

IBM

@server

IBM Systems - iSeries

Referințe privind securitatea

Versiunea 5 Ediția 4

SA12-6497-09





@server

IBM Systems - iSeries

Referințe privind securitatea

Versiunea 5 Ediția 4

SA12-6497-09

Notă

Înainte de a folosi aceste informații și produsul la care se referă, citiți informațiile din Anexa I, “Observații”, la pagina 633.

Ediția a zecea (februarie 2006)

Această ediție este valabilă pentru IBM i5/OS (număr de produs 5722-SS1) versiunea 5, ediția 4, modificarea 0 și pentru toate edițiile și modificările ulterioare până se specifică altceva în noile ediții. Această versiune nu rulează pe toate modelele RISC și nici pe modelele CISC.

Această ediție înlocuiește SC41-5302-08.

© Copyright International Business Machines Corporation 1996, 2006. Toate drepturile rezervate.

Cuprins

Figuri	ix
------------------	----

Tabele	xi
------------------	----

Despre Referințe privind securitatea (SC41-5302) xv

Cine ar trebui să citească această carte	xv
Convențiile și terminologia utilizate în această carte	xvi
Cerințe preliminare și informații înrudite	xvi
Cum să vă trimiteți comentariile	xvi

Ce este nou la V5R4 xix

Capitolul 1. Introducere în securitatea iSeries 1

Securitatea fizică	2
Securitatea privind cheia IPL	2
Nivelul de securitate	2
Valorile de sistem	3
Semnarea	3
Activarea pentru semnare unică	3
Profilurile de utilizator	4
Profilurile de grup	4
Securitatea resurselor	4
Jurnalul de auditare a securității	5
Securitate CC (Common Criteria - Criterii comune)	6
Pool-ul de discuri independent	6

Capitolul 2. Utilizarea valorii de sistem QSecurity (Securitate sistem) 7

Nivelul de securitate 10	10
Nivelul de securitate 20	10
Trecerea la nivelul 20 de la nivelul 10	10
Trecerea la nivelul 20 de la un nivel mai înalt	10
Nivelul de securitate 30	11
Trecerea la nivelul 30 de la un nivel mai scăzut	11
Nivelul de securitate 40	11
Împiedicarea utilizării interfețelor nesuportate	13
Protecția descrierilor de job	13
Semnarea fără ID de utilizator și parolă	14
Protecția hardware îmbunătățită a spațiului de stocare	14
Protecția spațiului asociat unui program	14
Protecția spațiului de adresă al unui job	14
Validarea parametrilor	14
Validarea programelor care sunt restaurate	15
Trecerea la nivelul de securitate 40	15
Dezactivarea nivelului de securitate 40	16
Nivelul de securitate 50	16
Restricționarea obiectelor de domeniu utilizator	16
Restricționarea tratării mesajelor	17
Împiedicarea modificării blocurilor de control interne	17
Trecerea la nivelul de securitate 50	17
Dezactivarea nivelului de securitate 50	18

Capitolul 3. Valorile de sistem privind securitatea 19

Valorile de sistem generale pentru securitate	20
Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)	21
Autorizarea pentru noile obiecte (QCRTAUT)	22
Afișarea informațiilor de semnare (QDPSGNINF)	22
Intervalul de timeout pentru job inactiv (QINACTITV)	23
Coada de mesaje pentru timeout-ul de job inactiv (QINACTMSGQ)	24
Limitarea sesiunilor de dispozitiv (QLMTDEVSSN)	25
Limitarea responsabilului cu securitatea (QLMTSECOFR)	25
Numărul maxim de încercări de semnare (QMAXSIGN)	25
Acțiunea când este depășit numărul maxim de încercări de semnare (QMAXSGNACN)	26
Reținerea informațiilor de securitate server (QRETSVRSEC)	27
Controlul semnării de la distanță (QRMTSIGN)	27
Scanarea sistemelor de fișiere (QSCANFS)	28
Controlul scanării sistemelor de fișiere (QSCANFSCNTL)	28
Controlul memoriei de partajare (QSHRMEMCTL)	29
Folosirea autorizării adoptate (QUSEADPAUT)	30
Valorile de sistem referitoare la securitate	31
Configurarea automată a dispozitivelor (QAUTOCFG)	31
Configurarea automată a dispozitivelor virtuale (QAUTOVRT)	32
Acțiunea la recuperarea dispozitivelor (QDEVRCYACN)	32
Intervalul de timeout pentru job deconectat (QDSCJOBITV)	33
Atributul de service la distanță (QRMTSRVATR)	33
Valorile de sistem pentru restaurare referitoare la securitate	34
Verificarea obiectului la restaurare (QVFYOBJRST)	34
Forțarea conversiei la restaurare (QFRCCVNRST)	36
Permiterea restaurării obiectelor sensibile la securitate (QALWOBJRST)	37
Valorile de sistem pentru parole	38
Intervalul de expirare a parolei (QPWDEXPITV)	39
Nivelul parolei (QPWDLVL)	40
Lungimea minimă a parolelor (QPWDMINLEN)	41
Lungimea maximă a parolelor (QPWDMAXLEN)	41
Necesitatea diferenței în parole (QPWDRQDDIF)	42
Restricționarea caracterelor pentru parole (QPWDLMTCHR)	42
Restricționarea cifrelor consecutive pentru parole (QPWDLMTAJC)	43
Restricționarea caracterelor repetate pentru parole (QPWDLMTREP)	43
Diferența poziției caracterelor pentru parole (QPWDPOSDIF)	44
Necesitatea caracterelor numerice în parole (QPWDRQDDGT)	44

Programul de aprobare a parolei (QPWDVLDPGM)	44
Valorile de sistem pentru controlul auditării	49
Controlul auditării (QAUDCTL)	50
Acțiunea pentru oprirea auditării (QAUDENDACN)	50
Nivelul de forțare a auditării (QAUDFRCLVL)	51
Nivelul de auditare (QAUDLVL)	51
Extensia nivelului de auditare (QAUDLVL2)	53
Auditarea noilor obiecte (QCRTOJAUD)	54

Capitolul 4. Profilurile de utilizator . . . 57

Rolurile profilului de utilizator	57
Profilurile de grup	57
Câmpuri parametru profil utilizator	58
Nume profil utilizator	59
Parolă	60
Setare parolă la Expirată	61
Stare	62
Clasă utilizator	62
Nivel de ajutorare	63
Bibliotecă curentă	64
Program inițial	65
Meniu inițial	66
Limitare capabilități	66
Text	67
Autorizare specială	68
Mediu special	72
Ecranul Informații semnare	73
Interval de expirare parolă	74
Gestiunea parolei locale	75
Limitare sesiuni dispozitiv	75
Punere în buffer tastatură	76
Spațiu de stocare maxim	76
Limită de prioritate	77
Descriere de job	78
Profil de grup	79
Proprietar	79
Autorizare de grup	80
Tip autorizare de grup	81
Grupuri suplimentare	81
Cod de contabilizare	82
Parolă document	83
Coadă de mesaje	83
Livrare	84
Gravitate	84
Dispozitiv de tipărire	85
Coadă de ieșire	85
Program de tratare tastă Attn.	86
Secvență de sortare	87
Identificator de limbă	87
Identificator de regiune sau țară	88
Identificator set de caractere codate	88
Control identificator de caracter	88
Atribute de job	89
Locale	89
Opțiuni utilizator	90
Numărul de identificare utilizator	90
Număr identificare grup	91
Directorul de bază	91
Asociere EIM	92
Autorizare	93
Auditare obiect	93

Acțiune de auditare	94
Informațiile suplimentare asociate cu un profil de utilizator	95
Autorizările private	95
Autorizările de grup primar	96
Informațiile privind obiectul deținut	96
Autentificarea prin ID digital	96
Gestionarea profilurilor de utilizator	96
Crearea profilurilor de utilizator	96
Copierea profilurilor de utilizator	99
Modificarea profilurilor de utilizator	101
Ștergerea profilurilor de utilizator	101
Lucrul cu obiecte după autorizare privată	103
Gestionarea obiectelor după grup primar	103
Activarea unui profil de utilizator	104
Listarea profilurilor de utilizator	104
Redenumirea unui profil de utilizator	106
Gestionarea auditării utilizatorilor	106
Gestionarea profilurilor în programele CL	107
Punctele de ieșire pentru profil de utilizator	107
Profilurile de utilizator furnizate de IBM	108

Capitolul 5. Securitatea resurselor . . . 111

Definirea celor care pot accesa informații	111
Definirea modului în care pot fi accesate informațiile	112
Autorizările folosite în mod obișnuit	113
Definirea informațiilor care pot fi accesate	114
Securitatea bibliotecii	114
Autorizările de câmp	115
Securitatea și mediul System/38	117
Securitatea directorului	117
Securitatea listei de autorizare	117
Autorizarea pentru obiectele noi dintr-o bibliotecă	118
Riscurile legate de crearea autorizării (CRTAUT)	119
Autorizarea pentru obiecte noi într-un director	119
Dreptul de proprietate asupra obiectului	122
Dreptul de proprietate al grupului asupra obiectelor	122
Grupul primar pentru un obiect	123
Profilul de utilizator proprietar implicit (QDFTOWN)	124
Asignarea autorizării și dreptului de proprietate pentru noile obiecte	124
Obiecte care adoptă autorizarea proprietarului	128
Riscurile și recomandările privind autorizarea adoptată	131
Programe care ignoră autorizarea adoptată	131
Deținătorii de autorizare	131
Deținătorii de autorizare și migrarea la System/36	132
Riscurile privind deținătorii de autorizare	133
Gestionarea autorizărilor	133
Ecrane pentru autorizare	133
Rapoarte pentru autorizare	136
Gestionarea bibliotecilor	136
Crearea obiectelor	137
Gestionarea autorizării de obiect individuale	138
Gestionarea autorizării pentru mai multe obiecte	141
Gestionarea proprietății asupra obiectelor	142
Gestionarea autorizării de grup primar	143
Folosirea unui obiect referit	144
Copierea autorizării de la un utilizator	144
Gestionarea listelor de autorizare	144
Cum verifică sistemul autorizarea	147
Diagramele de flux pentru verificarea autorizării	147
Exemple de verificare a autorizării	163

Cache-ul de autorizări	173
----------------------------------	-----

Capitolul 6. Securitate control funcționare 175

Inițiere job.	175
Pornirea unui job interactiv.	175
Pornirea unui job batch	176
Autorizarea adoptată și joburile batch.	176
Stații de lucru.	177
Proprietatea asupra descrierilor de dispozitiv	179
Fișierul de afișare pentru ecranul de semnare	180
Modificarea fișierului de afișare pentru semnare	180
Descrierile de subsistem	181
Controlarea felului în care intră joburile în subsistem	181
Descrieri de job	182
Coadă de mesaje operator sistem	182
Listele de biblioteci	183
Riscurile de securitate ale listelor de biblioteci	183
Recomandări pentru porțiunea de sistem a listei de biblioteci	184
Recomandări pentru bibliotecă de produs	185
Recomandări pentru bibliotecă curentă	185
Recomandări pentru porțiunea de utilizator a listei de biblioteci	185
Tipărirea	186
Securizarea fișierelor spool.	186
Coadă de ieșire și Parametrul Autorizării necesar pentru tipărire.	187
Exemple: Coadă de ieșire	188
Atributele de rețea	189
Atributul de rețea Acțiune job (JOBACN)	189
Atributul de rețea Acces Cerere client (PCSACC)	189
Atributul de rețea Acces cerere DDM (DDMACC)	190
Operațiile de salvare și restaurare	191
Restricționarea operațiilor de salvare și restaurare	191
Exemplu: Restricționarea comenzilor de salvare și restaurare	191
Ajustarea performanței	192
Restricționarea joburilor la batch	193

Capitolul 7. Proiectarea securității 195

Recomandări generale	196
Planificarea modificărilor nivelului de parolă	196
Considerente pentru modificarea QPWDLVL de la 0 la 1	197
Considerente pentru modificarea QPWDLVL de la 0 sau 1 la 2	197
Considerente pentru modificarea QPWDLVL de la 2 la 3	198
Trecerea la un nivel de parolă mai scăzut.	198
Planificarea bibliotecilor	199
Planificarea aplicațiilor pentru a împiedica profilurile mari	200
Listele de biblioteci	201
Descrierea securității bibliotecii	202
Planificarea meniurilor	203
Folosirea autorizării adoptate în proiectarea meniului	203
Descrierea securității meniului	206
Meniul Cerere sistem	207
Planificarea securității comenzii	208

Planificarea securității fișierului	209
Securizarea fișierelor logice	209
Înlocuirea fișierelor	212
Securitatea fișierului și SQL	212
Planificarea listelor de autorizări	212
Avantajele folosirii unei liste de autorizări	212
Planificarea profilurilor de grup	213
Planificarea grupurilor primare pentru obiecte	213
Planificarea profilurilor de grup multiple.	214
Folosirea unui profil individual ca profil de grup	214
Comparație între profilurile de grup și listele de autorizări	215
Planificarea securității pentru programatori	215
Gestionarea fișierelor sursă.	216
Protejarea fișierelor class și jar Java în sistemul de fișiere integrat	216
Planificarea securității pentru programatori de sistem sau manageri	216
Planificarea folosirii obiectelor din lista de validare	216
Limitarea accesului la funcția programului	217

Capitolul 8. Salvarea de rezervă și recuperarea informațiilor de securitate 219

Modul în care sunt stocate informațiile de securitate	220
Salvarea informațiilor de securitate	220
Recuperare informațiilor de securitate	221
Restaurarea profilurilor de utilizator	221
Restaurarea obiectelor	222
Restaurarea autorizării	224
Restaurarea programelor	225
Restaurarea programelor licențiate	225
Restaurarea listelor de autorizare	226
Restaurarea sistemului de operare	227
Autorizarea specială *SAVSYS	227
Auditarea operațiilor de salvare și restaurare.	228

Capitolul 9. Auditarea securității pe sistemul iSeries 229

Listă de verificare pentru responsabilii cu securitatea și auditori	229
Securitatea fizică	230
Valorile de sistem	230
Profilurile de utilizator furnizate de IBM.	230
Controlul parolei	231
Profilurile de utilizator și de grup	231
Controlul autorizării	232
Accesul neautorizat	233
Programele neautorizate.	233
Comunicațiile.	233
Utilizarea jurnalului de auditare a securității	233
Planificarea auditării securității	234
Folosirea CHGSECAUD pentru a seta auditarea securității	256
Setarea auditării securității	256
Gestionarea jurnalului de auditare și a receptorilor de jurnal	258
Oprirea funcției de auditare.	260
Analizarea intrărilor din jurnalul de auditare.	260
Relația Object Change Date/Time - Audit Records	264
Alte tehnici pentru monitorizarea securității	265
Monitorizarea mesajelor de securitate.	265

Utilizarea istoricului sistem.	265
Folosirea jurnalelor pentru monitorizarea activității obiectului	265
Analizarea profilurilor de utilizator	267
Analizarea autorizărilor pentru obiect.	268
Analizarea programelor care adoptă autorizarea.	268
Verificarea obiectelor ce au fost modificate	269
Verificarea sistemului de operare	269
Auditarea acțiunilor responsabilului cu securitatea	270

Anexa A. Comenzile de securitate. . . . 271

Anexa B. Profilurile de utilizator furnizate de IBM 279

Anexa C. Comenzile livrate cu autorizarea publică *EXCLUDE 287

Anexa D. Autorizarea cerută pentru obiectele folosite de comenzi 299

Obiect referențiat.	299
Autorizarea cerută pentru obiect	299
Autorizarea cerută pentru bibliotecă	299
Presupuneri privind utilizarea comenzii	301
Reguli generale privind autorizările pentru obiecte cerute de comenzi	301
Comenzi comune pentru majoritatea obiectelor	303
Comenzile de recuperare a căii de acces: autorizările necesare	310
Comenzile AFP: autorizările necesare	311
Comenzile pentru socket-uri AF_INET peste SNA: autorizările necesare	312
Alertele: autorizările necesare	312
Comenzi pentru dezvoltare de aplicații: autorizările necesare	312
Comenzi pentru dezvoltare de aplicații: autorizările necesare	314
Comenzile listei de autorizări: autorizările necesare	314
Comenzi pentru director de legare: autorizările necesare	314
Comenzi pentru descriere cerere de modificare	315
Comenzile pentru diagramă	315
Comenzi pentru clasă	316
Comenzile pentru clasă-de-serviciu	316
Comenzi pentru cluster	316
Comenzile pentru comandă (*CMD)	319
Comenzi pentru control comitere	320
Comenzile CSI (informații parte comunicații)	320
Comenzi de configurare.	321
Comenzi pentru listă de configurare	322
Comenzi pentru listă de conexiuni.	322
Comenzi pentru descriere controler	323
Comenzile pentru criptografie	324
Comenzi pentru zonă de date	325
Comenzi pentru coadă de date	326
Comenzi pentru descriere dispozitiv	326
Comenzi pentru emulare dispozitiv	328
Comenzi pentru director și ascundere director	329
Comenzi pentru disc	330
Comenzi pentru passthrough stație de afișare	330

Comenzi pentru distribuție	330
Comenzi pentru listă de distribuție	331
Comenzi pentru obiecte bibliotecă document	331
Comenzi pentru set de caractere pe doi octeți	335
Comenzi pentru descriere editare	336
Comenzi pentru variabile de mediu	336
Comenzi pentru configurație LAN extinsă prin comunicație fără fir	336
Comenzi pentru fișier	337
Comenzi pentru filtrare	344
Comenzi financiare	344
Operații grafice i5/OS	345
Comenzi pentru set de simboluri grafice	345
Comenzi pentru server gazdă	346
Comenzi pentru catalog imagini	346
Comenzi pentru sistem de fișiere integrat	347
Comenzi de definire interactivă a datelor.	366
Comenzile IPX (Intrare job la distanță)	366
Comenzi pentru index de căutare informații	366
Comenzile pentru attribute IPL	367
Comenzile pentru Java	367
Comenzi pentru job	367
Comenzi pentru descriere de job	370
Comenzi pentru coadă de joburi	371
Comenzi pentru planificare job	372
Comenzi pentru jurnal	372
Comenzi pentru receptor de jurnal.	376
Comenzi pentru limbaj	376
Comenzi pentru bibliotecă	382
Comenzi pentru cheie de licență	386
Comenzi pentru program cu licență	387
Comenzi pentru descriere de linie	387
Comenzi pentru rețea locală (LAN)	389
Comenzi pentru locale	389
Comenzi pentru cadru de lucru server de poștă	389
Comenzi pentru mediu	389
Comenzi pentru meniu și grup de panouri	390
Comenzile pentru mesaj.	391
Comenzi pentru descriere mesaj	392
Comenzi pentru fișier mesaj	392
Comenzi pentru coadă de mesaje	393
Comenzi pentru migrare	393
Comenzi pentru descriere mod.	394
Comenzi pentru modul	394
Comenzi pentru descriere NetBIOS	395
Comenzi pentru rețea	395
Comenzi NFS.	396
Comenzi pentru descriere interfață de rețea	397
Comenzi pentru server de rețea	397
Comenzi pentru configurație server de rețea	399
Comenzi pentru descriere server de rețea.	399
Comenzi pentru listă de noduri.	399
Comenzi pentru servicii de birou	400
Comenzi pentru educație online	400
Comenzi pentru asistent operațional	400
Comenzi pentru disc optic	401
Comenzi pentru coadă de ieșire	404
Comenzi pentru pachet	405
Comenzi pentru performanță	406
Comenzi pentru grup descriptori de tipărire	411
Comenzi pentru configurare Print Services Facility.	411

Comenzi pentru problemă	411
Comenzi pentru program	412
Comenzi pentru interpretor shell QSH	415
Comenzi pentru interogare	416
Comenzi pentru întrebare și răspuns	417
Comenzi pentru cititor	418
Comenzi pentru facilitatea de înregistrare	418
Comenzi pentru baze de date relaționale	419
Comenzi pentru resurse	419
Comenzi pentru RJE (Intrare job la distanță)	419
Comenzi pentru atribute de securitate	423
Comenzi pentru intrare autentificare server	424
Comenzi pentru service	424
Comenzi pentru dicționar ajutor corectare ortografică	428
Comenzi pentru sferă de control	429
Comenzi pentru fișier spool	429
Comenzi pentru descriere subsistem	431
Comenzi pentru sistem	433
Comenzi pentru listă replici sistem	433
Comenzi pentru valori sistem	433
Comenzile pentru mediul System/36	434
Comenzi pentru tabelă	436
Comenzi pentru TCP/IP	436
Comenzi pentru descriere fus orar	438
Comenzi pentru date comandă modernizare	438
Comenzi pentru index utilizator, coadă utilizator și spațiu utilizator	439
Comenzi pentru sistem de fișiere definit de utilizator	439
Comenzi pentru profil utilizator	440
Comenzi pentru listă de validare	443
Comenzi pentru personalizare stație de lucru	443
Comenzi pentru scriitor	443

**Anexa E. Operațiile și auditarea
obiectelor 447**

**Anexa F. Macheta intrărilor din jurnalul
de auditare 507**

**Anexa G. Comenzile și meniurile
pentru comenzi de securitate. 617**

Opțiunile din meniul cu unelte de securitate	617
Cum se folosește meniul batch securitate	620
Opțiunile din meniul batch securitate	621
Comenzile pentru personalizarea securității	625
Valorile setate de comanda Configurare securitate sistem	625
Modificarea programului	627
Ce face comanda Revocare autorizare publică	627
Modificarea programului	628

**Anexa H. Informații înrudite pentru
iSeriesSecurity Reference 629**

Securitatea avansată	629
Salvarea de rezervă și recuperarea	629
Informații privind securitatea de bază și securitatea fizică	629
Programul licențiat iSeries Access pentru Windows	629
Comunicațiile și lucrul în rețea	629
Criptografia	630
Operațiile de sistem generale	630
Instalarea programelor livrate de IBM și configurarea sistemului	630
Sistemul de fișiere integrat	630
Internetul	630
IBM Lotus Domino	630
Suportul optic	631
Tipărirea	631
Programarea	631
Utilitare	632

Anexa I. Observații 633

Informații privind interfața de programare	634
Mărci comerciale	634
Termenii și condițiile	635

Index 637

Figuri

1. Mesaj de expirare parolă	62	18. Organigrama 6: Verificarea autorizării de grup	157
2. Descriere mediu special	73	19. Organigrama 7: Verificarea autorizării publice	159
3. Ecranul Informații semnare	74	20. Organigrama 8 A: Verificarea autorizării adoptate	
4. Ecranul Display Object Authority care arată F16=Display field authorities. Această tastă funcțională va fi afișată când un fișier bază de date are autorizări de câmp.	116	Utilizator *ALLOBJ și Proprietar	160
5. Ecranul Display Field Authority. Când este apăsat F17=Position to” este afișat promptul Position the List. Dacă este apăsat F16, va fi repetată operația anterioară de poziționare.	116	21. Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private	162
6. Exemplu de obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare privată dată	125	22. Autorizarea pentru fișierul PRICES	163
7. Exemplu de obiect nou: Autorizare publică din valoare de sistem, Grup cu autorizare privată dată	126	23. Autorizarea pentru fișierul CREDIT	164
8. Exemplu de obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare de grup primar dată	127	24. Display Object Authority - Afișare autorizare obiect	168
9. Exemplu de obiect nou: Autorizare publică specificată, Grupul deține obiectul	128	25. Autorizarea pentru fișierul ARWRK01	169
10. Autorizare adoptată și comanda CALL	129	26. Autorizarea pentru lista de autorizare ARLST1	169
11. Comanda TFRCTL și Autorizare adoptată	129	27. Autorizarea pentru fișierul CRLIM	170
12. Ecranul Afișare autorizare obiect	133	28. Autorizarea pentru fișierul CRLIMWRK	171
13. Organigrama 1: Procesul principal de verificare a autorizării	148	29. Autorizarea pentru Lista de autorizare CRLST1	171
14. Organigrama 2: Calea rapidă pentru autorizarea obiectului	150	30. Verificare autorizare pentru Stații de lucru	178
15. Organigrama 3: Verificare autorizare utilizator	151	31. Lista de biblioteci–Mediu așteptat	184
16. Organigrama 4: Verificarea autorizării proprietarului	152	32. Lista de biblioteci–Mediu real	184
17. Organigrama 5: Calea rapidă pentru autorizarea utilizatorului	154	33. Aplicații exemplu	195
		34. Program pentru a înlocui și restaura lista de biblioteci	201
		35. Format pentru descrierea securității bibliotecii	202
		36. Exemplu de meniu de interogare	203
		37. Meniu exemplu inițial	204
		38. Program aplicație inițială exemplu	204
		39. Program exemplu pentru interogare cu autorizare adoptată	204
		40. Meniu de aplicație exemplu cu Query	206
		41. Cerințe format pentru securitate meniu	207
		42. Folosire fișier logic pentru securitate	210

Tabele

1. Niveluri de securitate: Comparație a funcțiilor	7	31. Valorile posibile pentru valoarea de sistem	
2. Autorizările speciale implicite pentru clasele utilizator, după nivelul de securitate	9	QPWDMINLEN:	41
3. Comparație a nivelurilor de securitate 30, 40 și 50	12	32. Valori posibile pentru valoarea de sistem	
4. Accesul în funcție de domeniu și stare	13	QPWDMAXLEN:	42
5. Valorile de sistem care pot fi blocate	19	33. Valorile posibile pentru valoarea de sistem	
6. Valorile posibile pentru valoarea de sistem		QPWDRQDDIF:	42
QALWUSRDMN:	21	34. Valori posibile pentru valoarea de sistem	
7. Valorile posibile pentru valoarea de sistem		QPWDLMTCHR:	43
QCRTAUT:	22	35. Valorile posibile pentru valoarea de sistem	
8. Valorile posibile pentru valoarea de sistem		QPWDLMTAJC:	43
QDSPSGNINF:	23	36. Valori posibile pentru valoarea de sistem	
9. Valorile posibile pentru valoarea de sistem		QPWDLMTREP:	43
QINACTITV:	24	37. Parole cu caractere ce se repetă cu QPWDLVL 0 sau	
10. Valorile posibile pentru valoarea de sistem		1	43
QINACTMSGQ:	24	38. Parole cu caractere ce se repetă cu QPWDLVL 2 sau	
11. Valorile posibile pentru valoarea de sistem		3	44
QLMTDEVSSN:	25	39. Valorile posibile pentru valoarea de sistem	
12. Valorile posibile pentru valoarea de sistem		QPWDDIF:	44
QLMTSECOFR:	25	40. Valori posibile pentru valoarea de sistem	
13. Valorile posibile pentru valoarea de sistem		QPWDRQDDGT:	44
QMAXSIGN:	26	41. Valorile posibile pentru valoarea de sistem	
14. Valorile posibile pentru valoarea de sistem		QPWDLVDPGM:	45
QMAXSGNACN:	26	42. Parametrii pentru programul de aprobare a parolei	45
15. Valorile posibile pentru valoarea de sistem		43. Valorile posibile pentru valoarea de sistem	
QRETSVRSEC:	27	QAUDCTL:	50
16. Valorile posibile pentru valoarea de sistem		44. Valori posibile pentru valoarea de sistem	
QRMTSIGN:	27	QAUDENDACN:	51
17. Valorile posibile pentru valoarea de sistem		45. Valorile posibile pentru valoarea de sistem	
QSCANFS:	28	QAUDFRCLVL:	51
18. Valorile posibile pentru valoarea de sistem		46. Valori posibile pentru valoarea de sistem	
QSCANFSCTL:	28	QAUDLVL:	52
19. Valori posibile pentru valoarea de sistem		47. Valorile posibile pentru valoarea de sistem	
QSHRMEMCTL:	30	QAUDLVL2:	53
20. Valorile posibile pentru valoarea de sistem		48. Valori posibile pentru valoarea de sistem	
QUSEADPAUT:	30	QCRTOBJAUD:	55
21. Valorile posibile pentru valoarea de sistem		49. Valori posibile pentru PASSWORD:	61
QAUTOCFG:	31	50. Valori posibile pentru PWDEXP:	62
22. Valorile posibile pentru valoarea de sistem		51. Valori posibile pentru STATUS:	62
QAUTOVRT:	32	52. Autorizările speciale implicite după clasa de	
23. Valorile posibile pentru valoarea de sistem		utilizator	63
QDEVRCYACN:	32	53. Cum sunt memorate și modificate nivelurile de	
24. Valorile posibile pentru valoarea de sistem		ajutorare	64
QDSCJOBITV:	33	54. Valori posibile pentru ASTLVL:	64
25. Valorile posibile pentru valoarea de sistem		55. Valori posibile pentru CURLIB:	65
QRMTSRVATR:	33	56. Valori posibile pentru INLPGM:	65
26. Valori posibile pentru valoarea de sistem		57. Valori posibile pentru Biblioteca INLPGM:	66
QVFYOBJRST:	35	58. Valori posibile pentru MENU:	66
27. Valori QFRCCVNRST	37	59. Valori posibile pentru Biblioteca MENU:	66
28. Valori posibile pentru valoarea de sistem		60. Funcții permise pentru valorile de limitare	
QALWOBJRST:	38	capabilități	67
29. Valorile posibile pentru valoarea de sistem		61. Valori posibile pentru text:	68
QPWDEXPITV:	40	62. Valori posibile pentru SPCAUT:	68
30. Valori posibile pentru valoarea de sistem		63.	70
QPWDLVL:	40	64. Valori posibile pentru SPCENV:	72
		65. Valori posibile pentru DSPSGNINF:	74
		66. Valori posibile pentru PWDEXPITV:	74

67. Valori posibile pentru LCLPMDMGT:	75	125. Valori auditare acțiune	235
68. Valori posibile pentru LMTDEVSSN:	75	126. Intrări jurnal auditare securitate.	239
69. Valori posibile pentru KBDBUF:	76	127. Cum lucrează împreună un obiect și o auditare utilizator.	253
70. Valori posibile pentru MAXSTG:	77	128. Comenzi pentru lucrul cu deținători de autorizare	271
71. Valori posibile pentru PTYLMT:	78	129. Comenzi pentru lucrul cu liste de autorizații	271
72. Valori posibile pentru JOBD:.	78	130. Comenzi pentru lucru cu autorizări și auditare de obiecte	272
73. Valori posibile pentru Biblioteca JOBD:	79	131. Comenzi pentru Gestionare parole	273
74. Valori posibile pentru GRPPRF:	79	132. Comenzi pentru lucru cu profiluri utilizator	274
75. Valori posibile pentru OWNER:	80	133. Comenzi înrudite pentru profil utilizator	275
76. Valori posibile pentru GRPAUT:	81	134. Comenzi pentru lucru cu auditare	275
77. Valori posibile pentru GRPAUTYP: ¹	81	135. Comenzi pentru lucrul cu obiecte de bibliotecă de documente	275
78. Valori posibile pentru SUPGRPPRF	82	136. Comenzi pentru lucru cu intrări de autentificare server	276
79. Valori posibile pentru ACGCDE:	82	137. Comenzi pentru lucru cu directorul de distribuție sistem	276
80. Valori posibile pentru DOCPWD:	83	138. Comenzi pentru lucru cu liste de validare	276
81. Valori posibile pentru MSGQ:	83	139. Comenzi pentru lucru cu informații de utilizare funcție	277
82. Valori posibile pentru Biblioteca MSGQ:	83	140. Unelte de securitate pentru Gestionare auditare	277
83. Valori posibile pentru DLVRY:	84	141. Unelte de securitate pentru Gestionare autorizări	277
84. Valori posibile pentru SEV:	85	142. Unelte de securitate pentru Gestionare securitate sistem	278
85. Valori posibile pentru PRTDEV:.	85	143. Valorile implicite pentru profilurile utilizator	279
86. Valori posibile pentru OUTQ:	86	144. Profiluri utilizator livrate de IBM	281
87. Valori posibile pentru biblioteca OUTQ:	86	145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate	287
88. Valori posibile pentru ATNPGM:	86	146. Descriere tipuri de autorizare	299
89. Valori posibile pentru Biblioteca ATNPGM:	86	147. Autorizare definită de sistem	300
90. Valori posibile pentru SRTSEQ:	87	148. Autorizare definită de sistem	300
91. Valori posibile pentru Biblioteca SRTSEQ:	87	149. Comenzi comune pentru majoritatea obiectelor	303
92. Valori posibile pentru LANGID:.	87	150. Câmpuri antet standard pentru Intrări de jurnal de auditare.	507
93. Valori posibile pentru CNTRYID:	88	151. Câmpuri antet standard pentru Intrări de jurnal de auditare.	509
94. Valori posibile pentru CCSID:	88	152. Câmpuri antet standard pentru Intrări de jurnal de auditare.	510
95. Valori posibile pentru CHRIDCTL:	89	153. Tipuri intrare jurnal auditare (QAUDJRN)	511
96. Valori posibile pentru SETJOBATR:	89	154. Intrări jurnal AD (auditare modificare)	512
97. Valori posibile pentru LOCALE:	90	155. Intrări jurnal AF (Eșuare autorizare)	514
98. Valori posibile pentru USROPT:.	90	156. Intrări jurnal AP (autorizare adoptată)	519
99. Valori posibile pentru UID:	91	157. Intrări jurnal AU (Modificări atribut)	519
100. Valori posibile pentru GID:	91	158. Intrări jurnal CA (Modificări autorizare)	520
101. Valori posibile pentru HOMEDIR:	91	159. Intrări jurnal CD (șir comenzi)	522
102. Valori posibile pentru EIMASSOC, valori singulare:	92	160. Intrări jurnal CO (Creare obiect)	523
103. Valori posibile pentru EIMASSOC, Elementul 1:	92	161. Intrări jurnal CP (Modificări profil utilizator)	525
104. Valori posibile pentru EIMASSOC, Elementul 2:	92	162. Intrări jurnal CQ (modificare *CRQD)	527
105. Valori posibile pentru EIMASSOC, Elementul 3:	92	163. Intrări jurnal CU (Operații cluster)	527
106. Valori posibile pentru EIMASSOC, Elementul 4:	93	164. Intrări jurnal CV (Verificare conexiune)	528
107. Valori posibile pentru AUT:	93	165. Intrări jurnal CY (Configurație criptografică)	530
108. Valori posibile pentru OBJAUD:	94	166. Intrări jurnal DI (Directory Server).	532
109. Auditarea realizată pentru accesul la obiect	94	167. Intrări jurnal DO (Operație ștergere)	536
110. Valori posibile pentru AUDLVL:	95	168. Intrări jurnal DS (Resetare ID utilizator unelte service furnizate de IBM)	538
111. Descriere tipuri de autorizare	112	169. Intrări jurnal EV (variabilă mediu)	539
112. Autorizare definită de sistem	113	170. Intrări jurnal GR (înregistrare generică)	539
113. Autorizare definită de sistem	113	171. Intrări jurnal GS (acordare descriptor)	544
114. Permisunile LAN Server	114	172. Intrări Jurnal IM (Intrusion Monitor - Monitorizare intruziuni)	544
115. Autorizarea publică contra autorizarea privată	155		
116. Autorizarea de grup acumulată	156		
117. Părți ale listei de biblioteci	183		
118. Autorizarea necesară pentru a realiza funcții de tipărire	188		
119. Profiluri utilizatori pentru sistem meniu	204		
120. Obiecte folosite de sistem meniu	205		
121. Opțiuni și comenzi pentru Meniul cerere sistem	208		
122. Exemplu fișier fizic: Fișier CUSTMAST	210		
123. Comparatie între lista de autorizații și profilul de grup	215		
124. Modul în care informațiile de securitate sunt salvate și restaurate	219		

173. Intrări jurnal IP (comunicații între procese)	545	203. Intrări jurnal SE (Modificare intrare rutare subsistem)	586
174. Intrări jurnal IR (Acțiuni reguli IP)	547	204. Intrări jurnal SF (Acțiune către fișierul spool)	586
175. Intrări jurnal IS (gestiune securitate internet)	548	205. Intrări jurnal SG (Semnale asincrone)	590
176. Intrări jurnal JD (modificare descriere job)	550	206. Intrări jurnal SK (Conexiuni socket securizate)	591
177. Intrări jurnal JS (modificare job)	550	207. Intrări jurnal SM (Modificare gestiune sisteme)	592
178. Intrări jurnal KF (Fișier inel de chei)	554	208. Intrări jurnal SO (Acțiuni informații utilizator de securitate server)	593
179. Intrări jurnal LD (director de căutare, legare, dezlegare)	557	209. Intrări jurnal ST (Acțiune unelte service)	593
180. Intrări jurnal ML (Acțiuni mail)	558	210. Intrări jurnal SV (Acțiune pentru valoarea sistem)	597
181. Intrări jurnal NA (Modificare atribut)	559	211. Intrări jurnal VA (Modificarea listei de control acces)	597
182. Intrări de jurnal ND (Filtru de căutare director APPN)	559	212. Intrări jurnal VC (Terminare și oprire conexiune)	598
183. Intrări de jurnal NE (Filtru punct final APPN)	560	213. Intrări jurnal VF (Închiderea fișierelor server)	598
184. Intrări jurnal OM (Modificare gestiune obiect)	560	214. Intrări jurnal VL (Limită cont depășită)	599
185. Intrări jurnal OR (restaurare obiect)	563	215. Intrări jurnal VN (Logare și delogare rețea)	599
186. Intrări jurnal OW (modificare drept de proprietate)	566	216. Intrări jurnal VO (Listă de validare)	600
187. Intrări jurnal O1 (Acces optic)	567	217. Intrări jurnal VP (Eroare parolă rețea)	601
188. Intrări jurnal O2 (Acces optic)	568	218. Intrări jurnal VR (Acces resursă rețea)	602
189. Intrări jurnal O3 (Acces optic)	569	219. Intrări jurnal VS (Sesiune server)	603
190. Intrări jurnal PA (Adoptare program)	570	220. Intrări jurnal VU (Modificare profil rețea)	603
191. Intrări jurnal PG (Modificare grup primar)	572	221. Intrări jurnal VV (modificare stare service)	604
192. Intrări jurnal PO (Ieșire imprimantă)	574	222. Intrări jurnal X0 (Autentificare rețea)	605
193. Intrări jurnal PS (Interschimbare profil)	575	223. Intrări jurnal X1 (Jeton identitate)	608
194. Intrări jurnal PW (Parolă)	576	224. Intrări jurnal YC (Modificarea obiectului DLO)	610
195. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat)	578	225. Intrări jurnal YR (Citirea obiectului DLO)	611
196. Intrări jurnal RJ (Restaurare descriere job)	579	226. Intrări jurnal ZC (Modificare obiect)	611
197. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat)	580	227. Intrări jurnal ZR (Citire obiect)	614
198. Intrări RP (Restaurare programe care adoptă autorizare)	581	228. Codurile numerice pentru tipurile de acces	616
199. Intrări jurnal RQ (Restaurare obiect descriptor de modificare cerere)	582	229. Comenzi unelte pentru Profiluri utilizatori	617
200. Intrări jurnal RU (Restaurare autorizare pentru profil utilizator)	583	230. Comenzi unelte pentru auditarea de securitate	619
201. Intrări jurnal RZ (Modificare grup primar pentru obiectul restaurat)	583	231. Comenzi pentru rapoarte securitate	621
202. Intrări jurnal SD (Modificare director de distribuție sistem)	585	232. Comenzi pentru Personalizarea sistemului dumneavoastră	625
		233. Valori setate de comanda CFGSYSSEC	625
		234. Comenzi ale căror autorizații publice sunt setate de comanda RVKPUBAUT.	628
		235. Programe ale căror autorizații publice sunt setate de comanda RVKPUBAUT.	628

Despre Referințe privind securitatea (SC41-5302)

Această carte furnizează informații despre planificarea, setarea, gestionarea și auditarea securității pe sistemul dumneavoastră iSeries. Ea descrie toate caracteristicile securității din sistem și discută cum se înrudesc caracteristicile securității cu alte aspecte ale sistemului, cum ar fi controlul funcționării, salvarea de rezervă și recuperarea și proiectarea aplicațiilor.

Această carte nu furnizează instrucțiuni operaționale complete pentru setarea securității pe sistemul dumneavoastră. Pentru un exemplu pas-cu-pas de setare a securității, consultați Centrul de informare iSeries (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi) și cartea *Tips and Tools for Securing Your iSeries*, SC41-5300-07. Informații despre Securitatea de bază a sistemului și planificarea pot fi de asemenea găsite în Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi).

Această carte nu furnizează informații complete despre planificare pentru utilizatorii de IBM Lotus Domino. Pentru utilizatorii Lotus Domino, vedeți URL <http://www.lotus.com/ldd/doc>. Acest sit Web oferă informații despre IBM Lotus Notes, Lotus Domino și IBM Lotus Domino for iSeries. De pe acest sit Web puteți descărca informații în formatul de bază de date Domino (.NSF) și în formatul Adobe Acrobat (.PDF), puteți căuta în baza de date și puteți afla cum puteți obține manuale tipărite.

Această carte nu conține informații complete despre API-urile (application programming interfaces - interfețe de programare de aplicații) care sunt disponibile pentru a accesa informațiile de securitate. Acest subiect nu conține informații despre Internet. Pentru informații despre considerentele privind conectarea sistemului dumneavoastră la Internet, vedeți IBM SecureWay: iSeries și Internet din Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi).

Pentru o listă de publicații înrudite, vedeți Anexa H, “Informații înrudite pentru iSeriesSecurity Reference”, la pagina 629.

Cine ar trebui să citească această carte

Ținta principală a acestei cărți este administratorul de securitate.

Capitolul 9, “Auditarea securității pe sistemul iSeries”, la pagina 229 este intenționată pentru oricine dorește să realizeze o auditare de securitate asupra sistemului.

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

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

Informațiile din următoarele capitole pot ajuta programatorii de aplicații și de sisteme să înțeleagă relația dintre securitate și aplicație și proiectarea sistemului:

Capitolul 5, “Securitatea resurselor”, la pagina 111

Capitolul 6, “Securitate control funcționare”, la pagina 175

Capitolul 7, “Proiectarea securității”, la pagina 195

Capitolul 8, “Salvarea de rezervă și recuperarea informațiilor de securitate”, la pagina 219

Convențiile și terminologia utilizate în această carte

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

Pentru informații suplimentare despre cum se utilizează Navigator iSeries, citiți Centrul de informare iSeries (vedeți “Cerințe preliminare și informații înrudite”).

Cerințe preliminare și informații înrudite

Utilizați Centrul de informare iSeries drept un punct de pornire pentru obținerea informațiilor tehnice referitoare la iSeries.

Puteți accesa Centrul de informare în două moduri:

- De pe următorul sit web:
<http://www.ibm.com/eserver/series/infocenter>
- De pe CD-ROM-ul *Centrul de informare iSeries*, SK3T-4091-04. Acest CD-ROM este trimis o dată cu noua dumneavoastră comandă de actualizare a hardware-ului iSeries sau software-ului IBM i5/OS. Puteți de asemenea comanda CD-ROM-ul la Centrul de publicații IBM:
<http://www.ibm.com/shop/publications/order>

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

Cu fiecare nouă comandă de hardware, primiți *CD-ROM-ul Setarea și operațiile iSeries*, SK3T-4098-02. Acest CD-ROM conține IBM eServer iSeries Access for Windows și vrăjitorul EZ-Setup. iSeries Access Family oferă un puternic set de capabilități de client și de server pentru conectarea PC-urilor la servere iSeries. Vrăjitorul EZ-Setup execută automat multe dintre operațiile de setare iSeries.

Pentru informații înrudite, vedeți subiectul Anexa H, “Informații înrudite pentru iSeriesSecurity Reference”, la pagina 629.

Cum să vă trimiteți comentariile

Reacția dumneavoastră este importantă, deoarece ne ajută să furnizăm informații cât mai exacte și de calitate înaltă. Dacă aveți comentarii cu privire la această carte sau orice altă documentație iSeries, completați formularul pentru comentariile cititorului, de la sfârșitul acestei cărți.

- Dacă preferați să trimiteți comentarii prin poștă, utilizați formularul pentru comentariile cititorului care are adresa tipărită pe spate. Dacă trimiteți prin poștă un formular cu comentarii de cititor dintr-o țară sau regiune diferită de Statele Unite, puteți să lăsați formularul la biroul reprezentanței IBM locale sau la reprezentantul IBM pentru a fi trimis gratuit prin poștă.
- Dacă preferați să trimiteți comentarii prin FAX, utilizați oricare dintre numerele următoare:
 - Statele Unite, Canada și Puerto Rico: 1-800-937-3430
 - Alte țări sau regiuni: 1-507-253-5192
- Dacă preferați să trimiteți comentarii pe cale electronică, utilizați una dintre aceste adrese de e-mail:
 - Comentarii despre cărți:
RCHCLERK@us.ibm.com
 - Comentarii despre Centrul de informare iSeries:
RCHINFOC@us.ibm.com

Aveți grijă să includeți următoarele informații:

- Numele cărții sau subiectul din Centrul de informare iSeries.
- Numărul de publicație al cărții.
- Numărul de pagină sau subiectul cărții la care se referă comentariile.

Ce este nou la V5R4

- l Cartea Referințe privind securitatea iSeries a fost modificată semnificativ în ediția V5R4. Această secțiune vă oferă un
l scurt sumar al principalelor modificări.
- l • De la capitolul 1 la capitolul 9, multe secțiuni au fost modificate, cum ar fi:
 - l – Secțiunea "Securitatea CC (Common Criteria)" a fost modificată în capitolul 1.
 - l – În capitolul 4 a fost adăugată o nouă secțiune, numită "Gestionarea obiectelor după autorizări private".
 - l – În capitolul 7 a fost adăugată o nouă secțiune, numită "Protejarea fișierelor class și jar Java în sistemul de fișiere
l integrat".
 - l – În capitolul 9 a fost adăugată secțiunea "Relația obiectului Modificare Dată/Timp cu Înregistrări de auditare".
 - l • În anexa A au fost actualizate două tabele, numite "Comenzi pentru lucrul cu autorizarea și auditarea obiectelor" și
l "Unelte de securitate pentru lucrul cu auditarea".
 - l • În anexa C, au fost adăugate 26 de comenzi noi.
 - l • Anexa D conține următoarele adăugiri și modificări:
 - l – Un nou tabel numit "Comenzi de configurare server rețea" a fost adăugat.
 - l – Multe tabele au fost modificate, cum ar fi tabelul "Comenzi pentru catalog de imagini", tabelul "Comenzi pentru
l sistem de fișiere integrat" și tabelul "Comenzi pentru cluster".
 - l • În anexa E, au fost actualizate următoarele tabele: "Operații comune tuturor tipurilor de obiecte", "Operații pentru
l biblioteci (*LIB)", "Operații pentru fișiere spool", "Operații pentru Query Manager Form (*QMFORM)" și "Operații
l pentru profil de utilizator (*USRPRF)".
 - l • Anexa F conține următoarele condiții și modificări:
 - l – A fost adăugat un tabel nou, numit "Intrări de jurnal IM (Intrusion Monitor)".
 - l – Multe tabele au fost modificate, cum ar fi "Intrări de jurnal AF (Authority Failure)", "Intrări de jurnal CA
l (Authority Changes)" și "Intrări de jurnal CO (Create Object)".
 - l • În anexa H au fost actualizate informațiile din Observații.
 - l • Anexa G conține următoarele condiții și modificări:
 - l – Tabelele actualizate includ "Comenzi pentru unelte pentru auditare de securitate", "Comenzi pentru rapoarte de
l securitate" și "Valorile setate de comanda CFGSYSSEC".
 - l – Secțiunile actualizate includ "Opțiuni în meniul unelte de securitate", "Modificarea programului" în "Ce face
l comanda Revocare autorizare publică" și "Valori care sunt setate de către comanda configurare securitate sistem".

Capitolul 1. Introducere în securitatea iSeries

Familia de sisteme @server acoperă un interval mare de utilizatori. Un sistem mic poate avea între trei și cinci utilizatori, iar un sistem mare poate avea câteva mii de utilizatori. Unele instalări își au toate stațiile de lucru într-o singură zonă, relativ sigură. Altele au utilizatori răspândiți pe distanțe mari, inclusiv utilizatori care se conectează prin apel telefonic și utilizatori indirecti, conectați prin calculatorul personal sau prin rețele de sisteme.

Securitatea sistemului iSeries este destul de flexibilă pentru a îndeplini cerințele acestei diversități de utilizatori și de situații. Trebuie să înțelegeți caracteristicile și opțiunile disponibile, astfel încât să le puteți adapta la cerințele dumneavoastră de securitate. Acest capitol conține o privire generală asupra opțiunilor de securitate din sistem.

Securitatea sistemului are trei obiective importante:

Confidențialitatea:

- Protejarea împotriva dezvăluirii de informații persoanelor neautorizate.
- Restricționarea accesului la informațiile confidențiale.
- Protejarea împotriva utilizatorilor de sistem curioși și împotriva celor din afară.

Integritatea:

- Protejarea împotriva modificărilor neautorizate ale datelor.
- Restricționarea manipulării datelor la programele autorizate.
- Furnizarea siguranței că datele sunt de încredere.

Disponibilitatea:

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

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

Cele mai bune funcții de sistem pentru securitate nu pot duce la rezultate bune fără o bună planificare. Securitatea setată pe bucăți mici, fără planificare, poate fi derutantă. Este dificil de întreținut și de auditat. Planificarea nu implică proiectarea în avans a securității pentru fiecare fișier, program și dispozitiv. Ea implică stabilirea unei abordări generale a securității sistemului și comunicarea acestei abordări dezvoltatorilor de aplicații, programatorilor și utilizatorilor sistemului.

Când planificați securitatea sistemului dumneavoastră și stabiliți gradul de securitate de care aveți nevoie, luați 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 protecția la eroare furnizată de caracteristicile de securitate?
- Care sunt cerințele de securitate ale companiei dumneavoastră pentru viitor?

Pentru a ușura instalarea, multe din capacitățile de securitate din sistemul dumneavoastră nu sunt activate la livrarea sistemului. În această carte sunt furnizate recomandări pentru a aduce sistemul dumneavoastră la un nivel rezonabil de securitate. Luați în considerare cerințele de securitate ale instalării dumneavoastră când evaluați recomandările.

Securitatea fizică

Securitatea fizică include protejarea unității de sistem, a dispozitivelor de sistem și a mediilor cu copii de rezervă pentru deteriorări accidentale sau intenționate. Majoritatea măsurilor pe care le luați pentru a asigura securitatea fizică a sistemului dumneavoastră sunt externe sistemului. Totuși, sistemul este echipat cu o cheie de IPL, care împiedică executarea funcțiilor neautorizate de la unitatea sistem.

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

Securitatea fizică este descrisă în Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Securitatea privind cheia IPL

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

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

Aceasta permite accesul utilizatorului de la distanță la funcțiile suplimentare pe care le oferă panoul de control. De exemplu, se poate controla de unde va realiza mașina IPL-ul și în ce mediu, fie în IBM i5/OSOS/400, fie în DST (Dedicated Service Tools - Unelte de service dedicate).

Valoarea de sistem i5/OS QRMTSRVATR controlează accesul la distanță. Această valoare este livrată implicit dezactivată, ceea ce nu va permite înlocuirea cheii IPL. Valoarea de sistem poate fi modificată pentru a permite accesul de la distanță, dar pentru aceasta este nevoie de autorizările speciale *SECADM și *ALLOBJ.

Nivelul de securitate

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

Nivelul 10:

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

Nivelul 20:

Sistemul necesită un ID de utilizator și o parolă pentru semnare. Toți utilizatorii primesc acces la toate obiectele.

Nivelul 30:

Sistemul necesită un ID de utilizator și o parolă pentru semnare. Este impusă securitatea resurselor.

Nivelul 40:

Sistemul necesită un ID de utilizator și o parolă pentru semnare. Este impusă securitatea resurselor. În plus, sunt impuse caracteristici suplimentare de protecție a integrității.

Nivelul 50:

Sistemul necesită un ID de utilizator și o parolă pentru semnare. Este impusă securitatea resurselor. Sunt impuse protecția integrității de nivel 40 și protecția integrității îmbunătățită. Nivelul de securitate 50 este conceput pentru sisteme iSeries cu cerințe înalte de securitate, fiind proiectat să îndeplinească cerințele de securitate CC.

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

Valorile de sistem

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

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

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

Semnarea

O componentă cheie a securității este integritatea: posibilitatea de a avea încredere că obiectele din sistem nu au fost utilizate sau modificate. Software-ul sistemului dumneavoastră de operare este protejat prin semnături digitale și acum puteți consolida integritatea prin semnarea obiectelor software pe care vă bazați. (Pentru informații suplimentare despre folosirea semnării pentru a vă proteja sistemul, vedeți *Tips and Tools for Securing Your iSeries*.) Acest lucru este important dacă obiectul a fost transmis prin Internet sau stocat într-un mediu de stocare care credeți că ar fi putut fi modificat. Semnătura digitală poate fi folosită pentru a detecta dacă obiectul a fost modificat.

Semnăturile digitale și utilizarea lor pentru verificarea integrității software-ului pot fi gestionate în conformitate cu politica dumneavoastră de securitate, folosind valoarea de sistem QVYOBJRST (Verify Object Restore - Verificare restaurare obiecte), comanda CHKOBJITG (Check Object Integrity - Verificare integritate obiect) și unealta DCM (Digital Certificate Manager - Manager certificate digitale). În plus, puteți alege să vă semnați programele (toate programele cu licență livrate împreună cu iSeries sunt semnate). DCM este descris în Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Puteți restricționa adăugarea semnăturilor digitale la un depozit de certificate digitale, folosind API-ul Adăugare verificator și puteți restricționa resetarea parolelor pentru rezerva de certificate digitale. SST (System Service Tools - Unelte de service sistem) furnizează o nouă opțiune de meniu, numită “Gestionare securitate sistem”, unde puteți restricționa adăugarea de certificate digitale.

Activarea pentru semnare unică

În rețele eterogene din prezent, cu servere partiționate și cu multiple platforme, administratorii trebuie să facă față complexității de a gestiona identificarea și autentificarea utilizatorilor din rețea. Noua infrastructură IBM și exploatarea ei în iSeries îi ajută pe administratori, utilizatori și programatorii de aplicații să gestioneze mult mai ieftin și mai ușor aceste identificări și autentificări.

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

În timp ce serviciul de autentificare în rețea permite unui sistem iSeries să participe în acea regiune Kerberos, EIM furnizează un mecanism pentru asocierea acestor principalii Kerberos la un singur identificator EIM, care reprezintă acel utilizator în întreaga întreprindere. Alte identități de utilizator, cum ar fi un nume de utilizator i5/OS, pot fi asociate cu acest identificator EIM. Când un utilizator semnează în rețea și accesează un sistem iSeries, nu i se cere ID-ul de utilizator și parola. Dacă autentificarea Kerberos a reușit, aplicațiile pot căuta asocierile cu identificatorul EIM pentru a găsi numele de utilizator i5/OS. Utilizatorul nu mai are nevoie de o parolă pentru aplicațiile și funcțiile iSeries, deoarece este deja autentificat prin intermediul protocolului Kerberos. Administratorii pot gestiona central identitățile

de utilizator cu EIM, în timp ce utilizatorii de rețea au nevoie să gestioneze doar o parolă. Puteți activa semnarea unică prin configurarea serviciului de autentificare în rețea și prin configurarea EIM (Enterprise Identity Mapping - Mapare de identitate în întreprindere) pe sistemul dumneavoastră iSeries. Pentru a examina un scenariu care ilustrează cum se face setarea unui mediu cu semnare unică, vedeți în Centrul de informare subiectul Scenariu: Activarea semnării unice. **(Securitate—>Serviciu de autentificare în rețea—>Scenarii serviciu de autentificare în rețea—>Scenariu: Activarea semnării unice)**. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru informații suplimentare asupra accesării, Centrul de informare.

Profilurile de utilizator

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

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

Autorizarea specială

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

Meniul inițial și programul inițial

Meniul inițial și programul inițial stabilesc ce vede utilizatorul după ce semnează pe sistem. Puteți limita un utilizator la un anumit set de operații prin restricționarea utilizatorului la un meniu inițial.

Limitarea capacităților

Câmpul Limitare capacități din profilul de utilizator stabilește dacă utilizatorul poate introduce comenzi și dacă poate modifica meniul inițial sau programul inițial când semnează.

Profilurile de utilizator sunt discutate în Capitolul 4, “Profilurile de utilizator”, la pagina 57.

Profilurile de grup

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

“Planificarea profilurilor de grup” la pagina 213 discută utilizarea autorizării de grup. “Dreptul de proprietate al grupului asupra obiectelor” la pagina 122 discută ce obiecte ar trebui deținute de profilurile de grup. “Grupul primar pentru un obiect” la pagina 123 discută utilizarea grupului primar și a autorizării de grup primar pentru un obiect. “Copierea profilurilor de utilizator” la pagina 99 descrie cum se face copierea unui profil de grup pentru a crea un profil de utilizator individual.

Securitatea resurselor

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

Fișierele, programele și bibliotecile sunt cele mai obișnuite obiecte care necesită protecția prin securitate, dar puteți specifica o autorizare pentru orice obiect din sistem. Urmează descrierile caracteristicilor securității de resurse:

Profiluri de grup

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

Listă de autorizare

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

Drept de proprietate obiect

Fiecare obiect din sistem are un proprietar. Obiectele pot fi deținute de un profil de utilizator individual sau de un profil de grup. Alocarea corespunzătoare a dreptului de proprietate asupra obiectului vă ajută să gestionați aplicațiile și să delegați responsabilitatea pentru securitatea informațiilor dumneavoastră.

Grup primar

Puteți specifica un grup primar pentru un obiect. Autorizarea grupului primar este memorată cu obiectul. Utilizarea grupurilor primare poate simplifica administrarea autorizărilor și poate îmbunătăți performanțele de verificare a autorizării.

Autorizare de bibliotecă

Puteți aduna fișiere și programe care au cerințe similare de protecție într-o bibliotecă și puteți restricționa accesul la acea bibliotecă. Aceasta se face de obicei mai ușor decât restricționarea accesului la fiecare obiect în parte.

Autorizare de director

Puteți utiliza autorizarea de director în același mod în care folosiți autorizarea de bibliotecă. Puteți grupa obiecte într-un director și puteți securiza directorul, nu obiecte individuale.

Autorizare de obiect

În cazurile în care restricționarea accesului la o bibliotecă sau la un director nu este destul de precisă, puteți restricționa autorizarea de accesare a obiectelor individuale.

Autorizare publică

Pentru fiecare obiect, puteți 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 informațiile și ea furnizează o bună performanță.

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 funcție de situație.

Deținător de autorizare

Un deținător de autorizare memorează informațiile de autorizare pentru un fișier de bază de date descris de program. Informațiile de autorizare rămân, chiar dacă fișierul este șters. Deținătorii de autorizare sunt utilizați de obicei la convertirea din System/36, deoarece aplicațiile System/36 șterg de obicei fișierele și le creează din nou.

Autorizare la nivel de câmp

Autorizările la nivel de câmp sunt acordate câmpurilor individuale dintr-un fișier de bază de date. Puteți folosi instrucțiunile SQL pentru a gestiona această autoritate.

Securitatea resurselor este descrisă în Capitolul 5, “Securitatea resurselor”, la pagina 111

Jurnalul de auditare a securității

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

Capitolul 9, “Auditarea securității pe sistemul iSeries”, la pagina 229 furnizează informații despre auditarea securității.

| **Securitate CC (Common Criteria - Criterii comune)**

| Pe 10 August 2005, IBM a primit certificare Common Criteria pentru i5/OS V5R3M0 la Evaluated Assurance Level (EAL) 4 augmented cu ALC_FLR.2 al CAPP, versiunea 1.d, 8 Octombrie 1999. Pentru a comanda sistemul evaluat, comandați Common Criteria FC 1930 sub 5722-SS1. Doar clienții care trebuie să ruleze sub a configurație Common Criteria ar trebui să comande acest număr de caracteristică.

| Produsul este postat pe pagina "Lista produselor validate" pe siteul Web Common Criteria Evaluation and Validation Scheme:

| http://niap.nist.gov/cc-scheme/vpl/vpl_type.html

Pool-ul de discuri independent

Pool-urile de discuri independente furnizează abilitatea de a grupa împreună spații de stocare care pot fi trecute în starea offline sau pot fi aduse online independent de datele de sistem sau de orice alte date înrudite. Termenii pool de memorie auxiliară (auxiliary storage pool - ASP) independent și pool de discuri independent sunt sinonimi. Un pool de discuri independent poate fi comutabil între mai multe sisteme dintr-un mediu cu funcționare în cluster sau conectat la un singur sistem. Pentru V5R2, modificările funcționale asupra pool-urilor de discuri independente au implicații asupra securității din sistemul dumneavoastră. De exemplu, când executați comanda CRTUSRPRF, nu puteți 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 și intrările de grup primar vor fi atașate la profilul cu același nume din sistemul destinație. Dacă nu există un profil în sistemul destinație, este creat un profil. Utilizatorul nu va avea nici o autorizare specială și parola va fi setată la *NONE.

| Pool-uri de disc independent suportă multe obiecte bazate pe biblioteci și sisteme de fișiere definite de utilizator. În i5/OS V5R1, puteți folosi pool-uri de disc independente doar cu sisteme de fișiere definite de utilizator. Există însă mai multe obiecte care nu sunt permise pe pool-urile de discuri independente. Pentru o listă completă cu obiectele suportate și nesuportate, vedeți în Centrul de informare subiectul Tipurile de obiecte i5/OS. (**Administrarea sistemelor**→**Pool-urile de discuri independente**→**Concepte**→**Restricții și considerente**→**Tipurile de obiecte i5/OS suportate și nesuportate**)

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

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

Privire generală:

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

Cum se face:

WRKSYSVAL *SEC (comanda Gestionare valori de sistem) sau meniul SETARE, opțiunea 1 (Modificare opțiuni sistem)

Autorizare:

*ALLOBJ și *SECADM

Intrare jurnal:

SV

Notă: Înainte de a face modificări într-un sistem de producție, citiți secțiunea corespunzătoare despre migrarea de la un nivel la altul.

Sistemul oferă cinci niveluri de securitate:

10 Nici o securitate impusă de sistem

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

20 Securitatea semnării

30 Securitatea semnării și resurselor

40 Securitatea semnării și resurselor; protecția integrității

50 Securitatea semnării și resurselor; protecție îmbunătățită a integrității

Sistemul dumneavoastră este livrat la nivelul 40, care furnizează securitatea semnării și resurselor și asigură protecția integrității. Pentru informații suplimentare, vedeți "Nivelul de securitate 40" la pagina 11.

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

Tabela 1. Niveluri de securitate: Comparație a funcțiilor

Funcție	Nivel 20	Nivel 30	Nivel 40	Nivel 50
Este necesar numele de utilizator pentru semnare.	Da	Da	Da	Da
Este necesară parola pentru semnare.	Da	Da	Da	Da
Securitatea de parolă activă.	Da	Da	Da	Da
Securitatea de meniuri și program inițial activă.	Da ¹	Da ¹	Da ¹	Da ¹
Suportul pentru limitarea capacităților activ.	Da	Da	Da	Da
Securitatea resurselor activă.	Nu	Da	Da	Da
Acces la toate obiectele.	Da	Nu	Nu	Nu
Profilul de utilizator este creat automat.	Nu	Nu	Nu	Nu
Capabilitățile de auditare securitate disponibile.	Da	Da	Da	Da

Tabela 1. Niveluri de securitate: Comparație a funcțiilor (continuare)

Funcție	Nivel 20	Nivel 30	Nivel 40	Nivel 50
Programele care conțin instrucțiuni restricționate nu pot fi create sau recompilate.	Da	Da	Da	Da
Programele care folosesc interfețe nesuportate eșuează la rulare.	Nu	Nu	Da	Da
Este suportată protecția hardware îmbunătățită a spațiului de stocare.	Nu	Nu	Da	Da
Biblioteca QTEMP este un obiect temporar.	Nu	Nu	Nu	Nu
Obiectele *USRSPC, *USRIDX și *USRQ pot fi create doar în bibliotecile specificate în valoarea de sistem QALWUSRDMN.	Da	Da	Da	Da
Pointer-ii utilizați în parametri sunt validați 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 și utilizator.	Nu	Nu	Nu	Da
Spațiul asociat unui program nu poate fi modificat direct.	Nu	Nu	Da	Da
Blocurile de control intern sunt protejate.	Nu	Nu	Da	Da ²

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

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

Nivelul de securitate al sistemului determină care sunt autorizările speciale implicite pentru fiecare clasă de utilizator. Când creați un profil de utilizator, puteți selecta autorizări speciale pe baza clasei de utilizator. Autorizările speciale sunt de asemenea adăugate și înlăturate din profilurile de utilizator când modificați 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 operațiile pe obiecte.

***AUDIT**

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

***IOSYSCFG**

Autorizarea specială de configurare sistem permite unui utilizator să configureze dispozitivele de intrare și de ieșire din sistem.

***JOBCTL**

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

***SAVSYS**

Autorizarea specială de salvare sistem permite unui utilizator să salveze și 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 funcții de service software în sistem.

***SPLCTL**

Autorizarea specială de control spool permite controlul nerestricționat asupra joburilor batch și asupra cozilor de ieșire din sistem.

Puteți de asemenea restricționa utilizatorii cu autorizările *SECADM și *ALLOBJ, astfel încât să nu poată modifica cu ajutorul comenzii CHGSYSVAL această valoare de sistem pentru securitate. Puteți specifica această restricție în SST (System Service Tools - Unelte de service sistem) cu opțiunea "Work with system security - Gestionare securitate sistem".

Notă: Această restricție se aplică și altor câteva valori de sistem.

Pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem referitoare la securitate și pentru o listă completă a valorilor de sistem afectate, vedeți Capitolul 3: "Valorile de sistem privind securitatea".

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

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

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

Notă: Subiectele "Clasă utilizator" la pagina 62 și "Autorizare specială" la pagina 68 furnizează informații suplimentare despre clasele de utilizator și despre autorizările speciale.

Recomandări:

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

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

Nivelul de securitate 40 furnizează protecție suplimentară a integrității, fără a afecta performanțele sistemului.

Aplicațiile care nu rulează la nivelul de securitate 40 au un efect negativ asupra performanței la nivelul de securitate 30. Ele determină sistemul să răspundă la violările de domeniu.

Nivelul de securitate 50 este conceput pentru sisteme cu cerințe de securitate foarte ridicate. Dacă vă rulați sistemul la nivelul de securitate 50, puteți observa un efect asupra performanței, din cauza verificării suplimentare pe care o realizează sistemul.

Chiar dacă doriți să acordați tuturor utilizatorilor acces la toate informațiile, luați în considerare rularea sistemului la nivelul de securitate 30. Puteți folosi capabilitatea de autorizare publică pentru a acorda utilizatorilor acces la informații. Utilizarea de la început a nivelului de securitate 30 vă oferă flexibilitatea de a securiza câteva resurse critice când este nevoie, fără a trebui să testați din nou toate aplicațiile.

Nivelul de securitate 10

La nivelul de securitate 10 nu aveți protecție prin securitate; de aceea, nivelul de securitate 10 **nu este recomandat** de IBM. Începând cu Versiunea 4 Ediția 3, nu vă puteți seta nivelul de securitate la 10. Dacă sistemul dumneavoastră se află la nivelul 10, el va rămâne la acest nivel când instalați Versiunea 4 Ediția 3. Dacă schimbați nivelul sistemului cu altă valoare, nu veți putea să îl schimbați 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 același utilizator semnează mai târziu cu un alt ID de utilizator, atunci este creat un nou profil de utilizator. Anexa B arată valorile implicite care sunt folosite când sistemul creează automat un profil de utilizator.

Sistemul realizează verificarea autorizării la toate nivelurile de securitate. Deoarece toate profilurile de utilizator create la nivelul de securitate 10 primesc autorizare specială *ALLOBJ, utilizatorii trec cu succes de orice verificare de autorizare și au acces la toate resursele. Dacă doriți să testați efectul mutării la un nivel de securitate mai înalt, puteți să înlăturați autorizarea specială *ALLOBJ din profilurile de utilizator și să acordați autorizarea de a folosi anumite resurse. Totuși, aceasta nu vă oferă nici o protecție prin securitate. Oricine poate semna cu un nou ID de utilizator și atunci este creat un nou profil, cu autorizarea specială *ALLOBJ. Nu puteți împiedica aceasta la nivelul de securitate 10.

Nivelul de securitate 20

Nivelul 20 furnizează următoarele funcții de securitate:

- Atât ID-ul utilizator, cât și 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 capabilităților.

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

Trecerea la nivelul 20 de la nivelul 10

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

Următoarea listă conține activitățile recomandate dacă doriți să treceți de la nivelul 10 la nivelul 20 după ce sistemul dumneavoastră a fost pus în funcțiune:

- Listați toate profilurile de utilizator din sistem folosind comanda DSPAUTUSR (Display Authorized User - Afișare utilizator autorizat).
- Creați noi profiluri de utilizator, cu nume standardizate sau copiați profilurile existente și dați-le nume noi, standardizate.
- Setează parola să expire în fiecare profil existent, forțând fiecare utilizator să seteze o nouă parolă.
- Setează valorile de sistem pentru formatul parolei astfel încât să împiedicați utilizatorii să seteze parole triviale.
- Revedeți valorile implicite în Tabela 143 din Anexa B pentru orice modificări pe care doriți să le faceți asupra profilurilor create automat la nivelul de securitate 10.

Trecerea la nivelul 20 de la un nivel mai înalt

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

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

Nivelul de securitate 30

Nivelul 30 furnizează următoarele funcții de securitate, în plus față de cele furnizate la nivelul 20:

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

Trecerea la nivelul 30 de la un nivel mai scăzut

Când treceți la nivelul de securitate 30 de la un nivel de securitate mai scăzut, sistemul modifică toate profilurile de utilizator următoarea dată când realizați 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 și 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 excepția acelor cu clasa de utilizator *SECOFR. Vedeți Tabela 2 la pagina 9 pentru o listă a autorizărilor speciale implicite și a diferențelor dintre nivelul 10 sau 20 și nivelurile de securitate mai înalte.

Dacă sistemul dumneavoastră a rulat aplicații la un nivel de securitate scăzut, atunci ar trebui să setați și să testați securitatea resurselor înainte de a trece la nivelul de securitate 30. Următoarea listă conține activitățile recomandate:

- Pentru fiecare aplicație, setați autorizările corespunzătoare pentru obiectele de aplicație.
- Testați fiecare aplicație folosind fie profilurile de utilizator reale, fie profiluri de utilizator speciale, de testare:
 - Înlăturați autorizarea specială *ALLOBJ din profilurile de utilizator folosite pentru testare.
 - Acordați autorizări de aplicație corespunzătoare pentru profilurile de utilizator.
 - Rulați aplicația folosind profilurile de utilizator.
 - Verificați dacă există eșuări ale autorizării fie căutând mesaje de eroare, fie folosind jurnalul de auditare a securității.
- Când toate aplicațiile rulează cu succes cu profilurile de testare, acordați autorizările corespunzătoare pentru obiectele de aplicație tuturor profilurilor de utilizator de producție.
- 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 autorizați asupra dispozitivelor la nivelul de securitate 30 sau mai înalt. Acordați acestor utilizatori autorizarea *CHANGE pentru dispozitivele selectate, acordați autorizarea QSECOFR *CHANGE dispozitivelor sau modificați valoarea de sistem QLMTSECOFR în 0.
- Modificați nivelul de securitate din sistemul dumneavoastră și realizați IPL (initial program load - Încărcare inițială de program).

Dacă doriți să treceți la nivelul 30 fără a defini autorizările fiecărui obiect, faceți autorizarea publică pentru obiectele de aplicație destul de înaltă ca să ruleze aplicația. Faceți testări ale aplicațiilor pentru a vă asigura că nu au loc eșuări ale autorizărilor.

Notă: Vedeți subiectul “Definirea modului în care pot fi accesate informațiile” la pagina 112 pentru informații suplimentare despre autorizările de obiect.

Nivelul de securitate 40

Nivelul de securitate 40 previne riscurile potențiale de integritate sau de securitate, cauzate de programe care pot trece peste măsurile de securitatea în anumite cazuri. Nivelul de securitate 50 furnizează protecție îmbunătățită a integrității pentru instalări cu cerințe de securitate stricte. Tabela 3 la pagina 12 compară modul în care sunt suportate funcțiile de securitate la nivelurile 30, 40 și 50. Aceste funcții sunt explicate mai detaliat în secțiunile care urmează.

Tabela 3. Comparație a nivelurilor de securitate 30, 40 și 50

Descriere scenariu	Nivel 30	Nivel 40	Nivel 50
Un program încearcă să acceseze obiecte folosind interfețe care nu sunt suportate.	Intrare jurnal AF ¹	Intrare jurnal AF ¹ ; operația eșuează.	Intrare jurnal AF ¹ ; operația eșuează.
Un program încearcă să folosească o instrucțiune restricționată.	Intrare jurnal AF ¹	Intrare jurnal AF ¹ ; operația eșuează.	Intrare jurnal AF ¹ ; operația eșuează.
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 și 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 reuși.	Intrare de jurnal AF; ^{1, 2} operația a eșuat. ²	Intrare de jurnal AF; ^{1, 2} operația a eșuat. ²
Este făcută o încercare de a restaura un program care nu are o valoare de validare. ³	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.
Este făcută o încercare de a restaura un program care are o valoare de validare.	Este făcută validarea programului.	Este făcută validarea programului.	Este făcută validarea programului.
Se încearcă modificarea spațiului asociat unui program.	Încercarea are succes.	Intrare jurnal AF; ¹ operația eșuează. ²	Intrare jurnal AF; ¹ operația eșuează. ²
Se încearcă modificarea spațiului de adresă al unui job.	Încercarea are succes.	Intrare jurnal AF; ¹ operația eșuează. ²	Intrare jurnal AF; ¹ operația eșuează. ²
Un program în stare utilizator încearcă să apeleze sau să transfere controlul unui program de domeniu sistem.	Încercarea are succes.	Intrare jurnal AF; ¹ operația eșuează. ²	Intrare jurnal AF; ¹ operația eșuează. ²
Este făcută o încercare de a crea un obiect de domeniu utilizator de tipul *USRSPC, *USRIDX sau *USRQ într-o bibliotecă ce nu este inclusă în valoarea de sistem QALWUSRDMN.	Operația eșuează.	Operația eșuează.	Operația eșuează.
Un program în starea utilizator trimite un mesaj de excepție la un program în starea sistem care nu se află imediat deasupra lui în stiva de program.	Încercarea are succes.	Încercarea are succes.	Operația eșuează.
Un parametru este transmis unui program de domeniu utilizator care rulează în starea sistem.	Încercarea are succes.	Este făcută validarea parametrului.	Este făcută validarea parametrului.
O comandă livrată de IBM* este modificată să ruleze un alt program folosind comanda CHGCMD. Comanda este modificată din nou să ruleze programul original livrat de IBM, care este un program de domeniu sistem. Un utilizator încearcă să ruleze comanda.	Încercarea are succes.	Intrare jurnal AF; ^{1, 2, 4} operația eșuează. ^{2, 4}	Intrare jurnal AF; ^{1, 2, 4} operația eșuează. ^{2, 4}
¹	Dacă funcția de auditare este activă atunci este scrisă o intrare de tipul AF (authority failure - eșuare autorizare) în jurnalul de auditare (QAUDJRN). Vedeți Capitolul 9 pentru informații suplimentare despre funcțiile de auditare.		
²	Dacă procesorul suportă protecție hardware îmbunătățită a spațiului de stocare.		
³	Programele create înainte de Versiunea 1 Ediția 3 nu au o valoare de validare.		
⁴	Când modificați o comandă livrată de IBM, ea nu mai poate apela un program de domeniu sistem.		

Dacă folosiți funcția de auditare la niveluri de securitate scăzute, sistemul înregistrează în istoric intrările de jurnal pentru majoritatea acțiunilor afișate în Tabela 3, cu excepția acelor detectate de funcția de protecție îmbunătățită hardware. Primiți avertizări sub formă de intrări de jurnal în cazul potențialelor violări ale integrității. La nivelul 40 sau mai înalt, violările de integritate determină sistemul să eșueze operația încercată.

Împiedicarea utilizării interfețelor nesuportate

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

Sistemul utilizează atributul de domeniu al unui obiect și atributul de stare al unui program pentru a impune această protecție:

- **Domeniu:**

Fiecare obiect aparține 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.

Puteți afișa domeniul unui obiect folosind comanda DSPOBJD (Display Object Description - Afișare descriere obiect) și specificând DETAIL(*FULL). Puteți de asemenea utiliza următoarele comenzi:

- DSPPGM (Display Program - Afișare program) pentru a afișa domeniul unui program
- DSPSRVPGM (Display Service Program - Afișare program serviciu) pentru a afișa domeniul unui program serviciu

- **Stare:**

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

Puteți afișa starea unui program folosind comanda DSPPGM (Display Program - Afișare program). Puteți afișa starea unui program serviciu folosind comanda DSPSRVPGM (Display Service Program - Afișare program serviciu).

Tabela 4 arată regulile de acces pentru domeniu și stare:

Tabela 4. Accesul în funcție de domeniu și stare

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

¹ O violare de domeniu sau de stare determină eșuarea operației la nivelul de securitate 40 și mai înalt. La toate nivelurile de securitate este scrisă o intrare de tipul AF în jurnalul de auditare dacă funcția de auditare este activă.

Intrare jurnal:

Dacă funcția de auditare este activă și valoarea de sistem QAUDLVL include *PGMFAIL atunci o intrare AF (authority failure - eșuare autorizare), violare de tipul D, este scrisă în jurnalul QAUDJRN când este făcută o încercare de a folosi o interfață nesuportată.

Protecția descrierilor de job

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

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

Intrare jurnal:

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

Semnarea fără ID de utilizator și parolă

La nivelul de securitate 30 și mai scăzut, pentru anumite descrieri de subsistem este posibilă semnarea prin apăsarea tastei Enter fără un ID de utilizator și parolă. La nivelul de securitate 40 și mai înalt, sistemul oprește orice încercare de semnarea fără ID de utilizator și o parolă. Vedeți subiectul “Descrierile de subsistem” la pagina 181 pentru informații suplimentare despre probleme privind securitatea asociate cu descrierile de subsistem.

Intrare jurnal:

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

Protecția hardware îmbunătățită a spațiului de stocare

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

Protecția hardware îmbunătățită a spațiului de stocare este suportată pe toate modelele iSeries, *cu excepția* următoarelor modele:

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

Intrare jurnal:

Dacă funcția de auditare este activă și valoarea de sistem QAUDLVL include *PGMFAIL, în jurnalul QAUDJRN este scrisă o intrare AF, violare de tipul R, atunci când un program încearcă să scrie într-o zonă a discului protejată de caracteristica de protecție hardware îmbunătățită a spațiului de stocare.

Protecția spațiului asociat unui program

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

Protecția spațiului de adresă al unui job

La nivelul de securitate 50, un program în starea utilizator nu poate obține 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

Interfețele pentru sistemul de operare sunt programe în starea sistem din domeniul utilizator. Cu alte cuvinte, ele sunt programe care pot fi apelate direct de un utilizator. Când parametrii sunt transmiși între programe în starea utilizator și sistem, acești parametri trebuie să fie verificați pentru a împiedica orice valoare neașteptată care ar periclita integritatea sistemului de operare.

Când vă rulați sistemul la nivelul de securitate 40 sau 50, sistemul verifică în mod specific toți parametrii transmiși între un program în starea utilizator și unul în starea sistem din domeniul utilizator. Această acțiune este necesară

pentru ca sistemul dumneavoastră să separe domeniul sistem de domeniul utilizator și pentru a îndeplini cerințele nivelului de securitate Common Criteria. Ați putea observa un efect asupra performanțelor din cauza acestei verificări suplimentare.

Validarea programelor care sunt restaurate

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

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

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

Programele create pentru iSeries pot conține informații care permit programului să fie creat din nou la restaurare, fără a fi necesară sursa programului. Programele create pentru iSeries Versiunea 5, Ediția 1 și mai recentă conțin informațiile necesare pentru re-creare chiar și când observabilitatea programului este înlăturată. Programele create pentru ediții înainte de Versiunea 5, Ediția 1 pot fi re-create la restaurare doar dacă informațiile de observabilitate ale programului nu au fost șterse.

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

Trecerea la nivelul de securitate 40

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

1. Activați funcția de auditare a securității, dacă nu ați făcut-o deja. Subiectul "Setarea auditării securității" la pagina 256 vă oferă instrucțiuni complete pentru setarea funcției de auditare.
2. Asigurați-vă că valoarea de sistem QAUDLVL include *AUTFAIL și *PGMFAIL. *PGMFAIL înregistrează în istoric intrări jurnal pentru orice încercare de acces care violează protecția integrității la nivelul de securitate 40.
3. Controlați jurnalul de auditare pentru intrări *AUTFAIL și *PGMFAIL în timp ce rulați toate aplicațiile dumneavoastră la nivelul de securitate 30. Fiți în special atent la următoarele coduri motiv din intrările de tipul AF:

- B** Violare de instrucțiune restricționată (blocată)
- C** Eșuare la validare obiect
- D** Violare de interfață (domeniu) nesuportată
- J** Eșuare autorizare descriere de job și profil de utilizator
- R** Încercare de accesare zonă protejată a discului (protecție hardware îmbunătățită a spațiului de stocare)
- S** Încercare de semnare implicită

Aceste coduri indică prezența expunerilor integrității din aplicațiile dumneavoastră. La nivelul de securitate 40, aceste programe eșuează.

4. Dacă aveți programe care au fost create înainte de Versiunea 1 Ediția 3, folosiți 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 crește considerabil durata procesului de restaurare. Vedeți subiectul “Validarea programelor care sunt restaurate” la pagina 15 pentru informații suplimentare despre validarea programelor.

Notă: Restaurați bibliotecile de program drept parte a testării dumneavoastră de aplicații. Controlați jurnalul de auditare pentru eșuări la validare.

5. Pe baza intrărilor din jurnalul de auditare, corectați-vă aplicațiile și împiedicați eșuările de program.
6. Modificați valoarea de sistem QSECURITY în 40 și realizați un IPL.

Dezactivarea nivelului de securitate 40

După trecerea la nivelul de securitate 40, ați putea descoperi că trebuie să vă întoarceți temporar la nivelul 30. De exemplu, ar putea fi necesar să testați de erori de integritate noile aplicații. Sau, ați putea descoperi că nu ați testat aplicațiile destul de bine înainte de a trece la nivelul de securitate 40.

Puteți trece de la nivelul de securitate 40 la nivelul 30 fără a vă periclita securitatea resurselor. Nu sunt făcute modificări asupra autorizărilor speciale din profilurile utilizator când treceți de la nivelul 40 la nivelul 30. După ce v-ați testat aplicațiile și ați rezolvat orice eroare din jurnalul de auditare, vă puteți întoarce la nivelul 40.

Atenție: Dacă treceți de la nivelul 40 la nivelul 20 atunci sunt adăugate unele autorizări speciale tuturor profilurilor utilizator. (Vedeți Tabela 2 la pagina 9.) Aceasta înlătură protecția de securitate a resurselor.

Nivelul de securitate 50

- | Nivelul de securitate 50 este proiectat pentru a asigura cerințele definite de Controlled Access Protection Profile (CAPP) pentru compatibilitate cu Common Criteria (CC). El furnizează protecție îmbunătățită a integrității în plus față de cea furnizată de nivelul de securitate 40.

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

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

Restricționarea obiectelor de domeniu utilizator

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

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

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

Obiectele de tipul *USRSPC, *USRIDX și *USRQ din il utilizator pot fi manevrate direct fără folosirea API-urilor și 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 și *SQLPKG se pot afla de asemenea în domeniul utilizator. Conținutul lor nu poate fi manevrat direct și ele nu sunt afectate de restricții.

La nivelul de securitate 50, unui utilizator nu trebuie să i se permită să transmită informații 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 obține 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 informații către un alt utilizator.
- Pentru a furniza compatibilitate cu aplicațiile existente care utilizează obiecte de domeniu utilizator, puteți specifica bibliotecă suplimentară în valoarea de sistem QALWUSRDMN. Valoarea de sistem QALWUSRDMN este impusă la toate nivelurile de securitate. Vedeți “Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)” la pagina 21 pentru informații suplimentare.

Restricționarea tratării mesajelor

Mesajele trimise între programe furnizează un potențial de expunere a integrității. 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-excepție către orice program în starea sistem.
- Un program în starea utilizator poate trimite un mesaj de tip excepție (stare, notificare sau ieșire) către un program în starea sistem dacă una din următoarele afirmații 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 excepție nu trebuie să fie programul apelat de programul în starea sistem. De exemplu, în această stivă de programe, un mesaj de excepție poate fi trimis către programul A de către programul B, C sau D:

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

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

Împiedicarea modificării blocurilor de control interne

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

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

Trecerea la nivelul de securitate 50

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

Acțiunile care pot cauza erori la nivelul de securitate 50 sunt neobișnuite în software-ul de aplicații normal. Majoritatea software-ului care rulează cu succes la nivelul de securitate 40 rulează de asemenea și la nivelul de securitate 50.

Dacă rulați sistemul dumneavoastră la nivelul de securitate 30, efectuați pașii descriși în “Trecerea la nivelul de securitate 40” la pagina 15 pentru a pregăti sistemul pentru trecerea la nivelul de securitate 50.

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

- Evaluați setarea valorii sistem QALWUSRDMN. Controlarea obiectelor de domeniu utilizator este importantă pentru integritatea sistemului. Vedeți “Restricționarea obiectelor de domeniu utilizator” la pagina 16.
- Recompilați toate programele COBOL care alocă dispozitivul din clauza SELECT unei STAȚII DE LUCRU dacă programele COBOL au fost compilate folosind un compilator anterior versiunii V2R3.
- Recompilați toate programele COBOL de mediu S/36 care au fost compilate folosind un compilator anterior versiunii V2R3.
- Recompilați toate programele RPG/400 sau RPG* ale mediului System/38 care folosesc fișiere de afișare dacă au fost compilate folosind un compilator anterior versiunii V2R3.

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

Dezactivarea nivelului de securitate 50

După trecerea la nivelul de securitate 50, ați putea descoperi că trebuie să vă întoarceți temporar la nivelul de securitate 30 sau 40. De exemplu, ar putea fi necesar să testați de erori de integritate noile aplicații. Sau, ați putea descoperi probleme de integritate care nu au apărut la nivelurile scăzute de securitate.

Puteți trece de la nivelul de securitate 50 la nivelul 30 sau 40 fără a vă periclita securitatea resurselor. Nu sunt făcute modificări asupra autorizărilor speciale din profilurile utilizator când treceți de la nivelul 50 la nivelul 30 sau 40. După ce v-ați testat aplicațiile și ați rezolvat orice eroare din jurnalul de auditare, vă puteți întoarce la nivelul 50.

Atenție: Dacă treceți de la nivelul 50 la nivelul 20 atunci sunt adăugate unele autorizări speciale tuturor profilurilor utilizator. Aceasta înlătură protecția de securitate a resurselor. (Vedeți Tabela 2 la pagina 9.)

Capitolul 3. Valorile de sistem privind securitatea

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

Puteți împiedica utilizatorii să modifice valorile de sistem referitoare la securitate. SST (system service tools - unelte de service sistem) și DST (dedicated service tools - unelte de service dedicate) furnizează o opțiune de a bloca aceste valori de sistem. Prin blocarea valorilor de sistem puteți să împiedicați chiar și un utilizator cu autorizare *SECADM și *ALLOBJ să modifice aceste valori de sistem cu comanda CHGSYSVAL. În plus față de restricționarea modificărilor asupra acestor de valori de sistem, puteți restricționa adăugarea de certificate digitale în depozitul de certificate digitale cu API-ul Add Verifier și puteți restricționa resetarea parolei pentru depozitul de certificate digitale.

Notă: Dacă blocați valorile de sistem referitoare la securitate și este nevoie să executați o operație de restaurare ca parte a unei restaurări de sistem, fiți atent că trebuie să deblocați valorile de sistem pentru a efectua operația de restaurare. Aceasta asigură faptul că valorile de sistem pot fi modificate în timpul IPL-ului.

Următoarele valori de sistem pot fi restricționate prin utilizarea opțiunii de blocare:

Tabela 5. Valorile de sistem care pot fi blocate

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

Puteți 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 folosiți DST dacă vă aflați în modul de recuperare, deoarece SST este indisponibil în timpul acestui mod. Altfel, utilizați 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), urmați acești pași:

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

1. Deschideți o interfață bazată pe caractere.
2. În linia de comandă, tastați **STRSST**.
3. Tastați ID-ul dumneavoastră utilizator unelte de service și parola.
4. Selectați opțiunea 7 (Gestionare securitate sistem).
5. Tastați 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, urmați acești pași:

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

Notă: Acest pas presupune că vă aflați în modul de recuperare și efectuați un IPL supravegheat.

2. Semnați pentru DST utilizând numele dumneavoastră de utilizator unelte de service și parola.
3. Selectați opțiunea 13 (Gestionare securitate sistem).
4. Tastați 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*.

Secțiunile următoare discută anumite valori de sistem de securitate. Pentru informații despre valorile de sistem referitoare la securitate pe care le puteți bloca, vedeți secțiunea lor corespondentă:

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

Valorile de sistem generale pentru securitate

Privire generală:

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

Cum se face:

WRKSYSVAL *SEC (comanda Gestionare valori de sistem)

Autorizare:

*ALLOBJ și *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 QPWDVLV).

Următoarele valori de sistem generale controlează securitatea în sistemul dumneavoastră:

QALWUSRDMN

Permitere obiecte de domeniu utilizator în biblioteci

QCRTAUT

Creare autorizare publică implicită

QDSPSGNINF

Afișare informații de semnare

QFRCCVNRST

Forțare conversație la restaurare

QINACTIV

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	Acțiune la depășirea numărului maxim de încercări de semnare
QRETSVRSEC	Păstrare securitate server
QRMTSIGN	Cereri de semnare la distanță
QSCANFS	Scanare sisteme de fișiere
QSCANFSCTL	Control scanare sisteme de fișiere
QSECURITY	Nivel de securitate
QSHRMEMCTL	Control memorie partajată
QUSEADPAUT	Utilizare autorizare adoptată
QVFYOBJRST	Verificare obiect la restaurare

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

Permiterea obiectelor din domeniul de utilizator (**QALWUSRDMN**)

Valoarea de sistem QALWUSRDMN specifică căror biblioteci le este permis să conțină obiecte din domeniul de utilizator de tipul *USRSPC, *USRIDX și *USRQ. Restricția nu se aplică obiectelor din domeniul de utilizator de tipul *PGM, *SRVPGM și *SQLPKG. Sistemele cu cerințe de securitate mari necesită restricționarea obiectelor de utilizator *USRSPC, *USRIDX și *USRQ. Sistemul nu poate audita transferul de informații către și de la obiectele din domeniul de utilizator.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 6. Valorile posibile pentru valoarea de sistem QALWUSRDMN:

*ALL	Obiectele de domeniu utilizator sunt permise în toate bibliotecile și directoarele din sistem.
*DIR	Obiectele de domeniu utilizator sunt permise în toate directoarele din sistem.
<i>nume-biblioteca</i>	Numele a până la 50 de biblioteci care pot conține obiecte de domeniu utilizator de tipul *USRSPC, *USRIDX și *USRQ. Dacă sunt afișate biblioteci individuale, atunci biblioteca QTEMP <i>trebuie</i> să fie inclusă în listă.

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

Unele sisteme au software de aplicație 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 aplicație. Autorizarea publică a oricărei biblioteci din QALWUSRDMN, cu excepția QTEMP, ar trebui setată la *EXCLUDE. În acest fel se limitează numărul utilizatorilor care pot folosi interfața MI (care nu poate fi auditată) pentru a citi sau modifica datele obiectelor din domeniul de utilizator aflate în aceste biblioteci.

Notă: Dacă rulați comanda RCLSTG (Reclaim Storage - pretindere spațiu de stocare), obiectele de domeniu utilizator ar putea necesita să fie mutate în și din bibliotecă QRCL (reclaim storage - pretindere spațiu de stocare). Pentru a rula cu succes comanda RCLSTG, ar trebui să adăugați biblioteca QRCL la valoarea de sistem QALWUSRDMN. Pentru a proteja securitatea de sistem, setați autorizarea publică pentru biblioteca QRCL la *EXCLUDE. Înlăturați biblioteca QRCL din valoarea de sistem QALWUSRDMN când ați terminat de rulat comanda RCLSTG.

Autorizarea pentru noile obiecte (QCRTAUT)

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

- 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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

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 funcție 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 fișiere îmbunătățit.

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

Afișarea informațiilor de semnare (QDSPSGNINF)

Valoarea de sistem QDSPSGNINF stabilește dacă după semnare este afișat ecranul Informații semnare. Ecranul Informații semnare afișează:

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

```

                                Sign-on Information
Previous sign-on . . . . . : 10/30/91 14:15:00
                                System:
Sign-on attempts not valid . . . . . : 3
Days until password expires . . . . . : 5

```

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 8. Valorile posibile pentru valoarea de sistem QDSPSGNINF:

<u>0</u>	Ecranul nu este afișat.
1	Ecranul este afișat.

Valoare recomandată: Este recomandată opțiunea 1 (Ecranul este afișat), pentru ca utilizatorii să poată monitoriza încercările de utilizare a profilului lor și să știe când este necesară o nouă parolă.

Notă: Afișarea informațiilor de semnare poate fi de asemenea specificată în profilurile de utilizator individuale.

Intervalul de timeout pentru job inactiv (QINACTITV)

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

- Utilizarea tastei Enter
- Utilizarea funcției de derulare pagină
- Utilizarea tastelor funcționale
- Utilizarea tastei Ajutor

Sunt incluse sesiunile de emulare prin iSeries Access. Joburile locale care sunt semnate pe un sistem la distanță sunt excluse. Joburile care sunt conectate prin FTP (file transfer protocol - protocol de transfer de fișiere) sunt excluse. Înainte de Versiunea 4, Ediția 2, erau excluse și joburile Telnet. Pentru a controla timeout-ul conexiunilor FTP, modificați parametrul INACTTIMO din comanda CHGFTP (Change FTP Attribute - Modificare atribut FTP). Pentru a controla timeout-ul sesiunilor Telnet mai vechi de V4R2, utilizați comanda CHGTELNA (Change Telnet Attribute - Modificare atribut Telnet).

Următoarele exemple arată cum stabilește sistemul ce joburi sunt inactice:

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

Valoarea de sistem QINACTMSGQ determină ce acțiune execută sistemul când jobul inactiv depășește intervalul specificat.

Când este pornit, sistemul verifică existența joburilor inactice în intervalul specificat de valoarea de sistem QINACTITV. De exemplu, dacă sistemul este pornit la 9:46 dimineața și valoarea de sistem QINACTITV este de 30 de minute, el verifică existența joburilor inactice la 10:16, 10:46, 11:16 și așa mai departe. Dacă descoperă un job care a fost inactiv 30 de minute sau mai mult, sistemul execută acțiunea 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 QINACTIV și QINACTMSGQ asigură securitatea împiedicând utilizatorii să lase semnate stații de lucru inactive. O stație de lucru inactivă ar putea permite unei persoane neautorizate să acceseze sistemul.

Tabela 9. Valorile posibile pentru valoarea de sistem QINACTIV:

*NONE:	Sistemul nu verifică dacă există joburi inactive.
<i>interval-în-minute</i>	Specificați o valoare între 5 și 300. Când un job a fost inactiv pentru acel număr de minute, sistemul execută acțiunea specificată în QINACTMSGQ.

Valoare recomandată: 60 de minute.

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 10. Valorile posibile pentru valoarea de sistem QINACTMSGQ:

*ENDJOB	Joburile inactive sunt oprite. Dacă jobul inactiv este un job de grup, ¹ atunci toate joburile asociate cu grupul sunt de asemenea oprite. Dacă jobul este o parte a unui job secundar, ¹ atunci ambele joburi sunt oprite. Acțiunea executată de *ENDJOB este echivalentă cu rularea comenzii ENDJOB JOB(num) OPTION (*IMMED) ADLINTJOBS(*ALL) pentru jobul inactiv.
*DSCJOB	Jobul inactiv este deconectat, la fel și eventualele joburi secundare sau joburi de grup ¹ asociate cu el. Valoarea de sistem QDSCJOBTV (disconnected job time-out interval - interval de timeout al jobului deconectat) controlează dacă sistemul, la sfârșit, termină joburile deconectate. Vedeți "Intervalul de timeout pentru job deconectat (QDSCJOBTV)" la pagina 33 pentru informații suplimentare.
<i>nume-coadă-de-mesaje</i>	<p>Atenție: Sistemul nu poate deconecta unele joburi, cum ar fi PC Organizer și funcția PCTA (PC text-assist - Asistent text PC). Dacă sistemul nu poate deconecta un job inactiv, el termină jobul respectiv.</p> <p>Mesajul CPI1126 este trimis cozii de mesaje specificate când este atins intervalul de timeout pentru job inactiv. Acest mesaj anunță că: Jobul &3/&2/&1; nu a fost activ.</p> <p>Coadă de mesaje trebuie să existe înainte să poată să fie specificată pentru valoarea de sistem QINACTMSGQ. Această coadă de mesaje este curățată automat în timpul unui IPL. Dacă asignați QINACTMSGQ drept coada de mesaje a utilizatorului, toate mesajele din coada de mesaje sunt pierdute în timpul unui IPL.</p>

¹ Cartea *Work Management* descrie joburile grup și joburile secundare.

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

Folosirea unei Cozi de mesaje: Un utilizator sau un program poate monitoriza coada de mesaje și să acționeze după cum este necesar, precum terminarea jobului sau trimiterea unui mesaj de avertisment utilizatorului. Folosirea unei cozi de mesaje vă permite să luați decizii în legătură cu anumite dispozitive și profiluri de utilizator, în loc să trataze toate dispozitivele inactive în același fel. Această metodă este recomandată când folosiți programul licențiat iSeries Access.

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

Limitarea sesiunilor de dispozitiv (QLMTDEVSSN)

Valoarea de sistem QLMTDEVSSN specifică dacă un utilizator are permisiunea să semneze pe mai multe dispozitive în același timp. Această valoare nu restricționează meniul Cerere sistem sau o a doua semnare de pe același 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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 11. Valorile posibile pentru valoarea de sistem QLMTDEVSSN:

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

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

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

Limitarea responsabilului cu securitatea (QLMTSECOFR)

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

Valoarea sistem QLMTSECOFR este forțată doar de la nivelul de securitate 30 în sus. "Stații de lucru" la pagina 177 furnizează mai multe informații despre autorizarea necesară pentru semnarea la o stație de lucru.

Puteți întotdeauna să semnați la consolă cu profilurile QSECOFR, QSRV și QSRVBAS, indiferent de modul în care este setată valoarea QLMTSECOFR.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 12. Valorile posibile pentru valoarea de sistem QLMTSECOFR:

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

Valoare recomandată: 1 (Da).

Numărul maxim de încercări de semnare (QMAXSIGN)

Valoarea de sistem QMAXSIGN controlează numărul de încercări consecutive de semnare care nu sunt corectate de utilizatorii locali și de la distanță. Încercările de semnare incorecte pot fi cauzate de un ID de utilizator care nu este corect, o parolă care nu este corectă sau de autorizare inadecvată pentru a folosi stația de lucru.

Când este atins numărul maxim de încercări de semnare, valoarea de sistem QMAXSGNACN este folosită pentru a determina acțiunea ce trebuie făcută. Un mesaj CPF1393 este trimis la coada de mesaje QSYSOPR (și coada de mesaje QSYSMSG dacă există în biblioteca QSYS) pentru a anunța responsabilul cu securitatea de un posibil intrus.

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 13. Valorile posibile pentru valoarea de sistem QMAXSIGN:

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

Valoare recomandată: 3.

Acțiunea când este depășit numărul maxim de încercări de semnare (QMAXSGNACN)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 14. Valorile posibile pentru valoarea de sistem QMAXSGNACN:

<u>3</u>	Dezactivați profilul de utilizator și dispozitivul.
1	Dezactivați doar dispozitivul.
2	Dezactivați doar profilul de utilizator.

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

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

Dacă creați coada de mesaje QSYSMSG în QSYS, mesajul trimis (CPF1397) conține numele utilizatorului și dispozitivului. De aceea, este posibil să controlați dezactivarea dispozitivului bazându-vă pe dispozitivul ce este folosit.

"Numărul maxim de încercări de semnare (QMAXSIGN)" la pagina 25 furnizează informații suplimentare despre coada de mesaje QSYSMSG.

Dacă profilul QSECOFR este dezactivat, puteți să semnați cu QSECOFR la consolă și să activați profilul. Dacă este dezactivată consola și nici un alt utilizator n-o poate activa, trebuie să executați un IPL de sistem pentru a face consola disponibilă.

Valoare recomandată: 3.

Reținerea informațiilor de securitate server (QRETSVRSEC)

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

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

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

Câmpul cu date criptate al unei intrări de listă de validare este folosit în mod tipic pentru a memora informații de autentificare. Aplicațiile specifică dacă să se memoreze datele criptate într-o formă decriptabilă sau nedecriptabilă. Dacă aplicațiile aleg o formă decriptabilă și valoarea QRETSVRSEC este modificată de pe 1 pe 0, informațiile 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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 15. Valorile posibile pentru valoarea de sistem QRETSVRSEC:

<u>0</u>	Datele de securitate server nu sunt reținute.
<u>1</u>	Datele de securitate server sunt reținute.

Valoare recomandată: 0.

Controlul semnării de la distanță (QRMTSIGN)

Valoarea de sistem QRMTSIGN specifică cum se tratează cererile de semnare la distanță. Exemple de semnări la distanță sunt stația de afișare passthrough de la un alt sistem, funcția stației de lucru a programului cu licență iSeries Access și accesul TELNET.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 16. Valorile posibile pentru valoarea de sistem QRMTSIGN:

*FRCSIGNON
*SAMEPRF

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

Ecranul de semnare apare pentru încercări passthrough care nu cer semnarea automată.

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

*VERIFY	Valoarea *VERIFY vă permite să ocoliți ecranul de semnare al sistemului destinație dacă, împreună cu cererea automată de semnare, sunt trimise informații valide de securitate. Dacă parola nu este validă pentru profilul specificat al utilizatorului destinație, atunci sesiunea passthrough se termină cu o eșuare de sistem. Dacă sistemul destinație are valoarea QSECURITY de 10, orice cerere automată de semnare este permisă.
*REJECT	Ecranul de semnare apare pentru încercări passthrough care nu cer semnarea automată. Nu este permisă nici o semnare de la distanță. Pentru acces TELNET, nu există acțiune pentru *REJECT.
<i>nume-program nume-biblioteca</i>	Programul specificat se rulează la pornirea și oprirea fiecărei sesiuni passthrough.

Valoarea recomandată: *REJECT dacă nu doriți să permiteți vreun acces passthrough sau iSeries Access. Dacă permiteți acces passthrough sau iSeries Access, folosiți *FRCSIGNON sau *SAMEPRF.

Cartea *Remote Work Station Support* conține informații detaliate despre valoarea de sistem QRMTSIGN. Conține de asemenea necesități pentru un program de semnare de la distanță și un exemplu.

Scanarea sistemelor de fișiere (QSCANFS)

Valoarea de sistem QSCANFS (Scan File Systems - Scanare sisteme de fișiere) vă permite să specificați sistemul de fișiere integrat în care vor fi scanate obiecte. De exemplu, puteți folosi această opțiune pentru a scana de viruși. Scanarea sistemului integrat de fișiere este activată când sunt înregistrate programele de ieșire cu oricare dintre punctele de ieșire referitoare la scanarea sistemului integrat de fișiere.

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

Punctele de ieșire referitoare la scanarea sistemului integrat de fișiere sunt:

- QIBM_QP0L_SCAN_OPEN — Ieșire scanare sistem integrat de fișiere la deschidere.
- QIBM_QP0L_SCAN_CLOSE — Ieșire scanare sistem integrat de fișiere la închidere.

Pentru informații suplimentare despre sistemele integrate de fișiere, vedeți subiectul sistemul integrat de fișiere.

Tabela 17. Valorile posibile pentru valoarea de sistem QSCANFS:

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

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

Pentru informații înrudite, vedeți subiectul “Controlul scanării sistemelor de fișiere (QSCANFSCTL)”.

Controlul scanării sistemelor de fișiere (QSCANFSCTL)

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

Tabela 18. Valorile posibile pentru valoarea de sistem QSCANFSCTL:

*NONE	Nu este specificat nici un control pentru punctele de ieșire referitoare la scanarea sistemului integrat de fișiere.
--------------	--

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

*ERRFAIL	Dacă există erori la apelarea programului de ieșire (de exemplu, programul nu a fost găsit sau programul de ieșire semnalează o eroare), sistemul va eșua cererea care a declanșat apelul programului de ieșire. Dacă aceasta nu este specificată, sistemul va sări peste programul de ieșire și îl va trata ca și cum obiectul nu a fost scanat.
*FSVROONLY	Vor fi scanate doar accesările prin serverele de fișiere. De exemplu, accesările prin Sistemul de fișiere rețea va fi scanat la fel ca și alte metode de servere de fișiere. Dacă nu este specificat, toate accesările vor fi scanate.
*NOFAILCLO	Sistemul nu vor eșua cererile de închidere cu o indicare de eșuare la scanare, chiar dacă obiectul a eșuat o scanare care a fost făcută ca parte a procesării de închidere. De asemenea, această valoare va înlocui specificația *ERRFAIL pentru procesarea de închidere, dar nu și pentru celelalte puncte de ieșire 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 scanat 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 puțin 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 restaurați obiecte fără să le scanați măcar o dată. Este cel mai bine să folosiți această opțiune doar când știți 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 ieșire pentru a include acces de scriere. Dacă nu este specificat, sistemul va încerca să actualizeze accesul de scriere.
*USEOCOATR	Sistemul va folosi specificațiile atributului "doar modificare obiect" doar pentru a scana obiectul dacă a fost modificat (de asemenea și 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 și când software-ul de scanare indică o actualizare.

Valoarea recomandată: Dacă doriți cele mai restricționate valori specificate pentru scanarea sistemului integrat de fișiere, atunci setările recomandate sunt *ERRFAIL și *NOWRTUPG. Aceasta asigură că orice eșec de la programele de ieșire de scanare vor preveni operațiile asociate și nu va da programului de ieșire niveluri de acces suplimentare. Totuși, valoarea *NONE este o bună opțiune 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.

Pentru informații înrudite, vedeți subiectul "Scanarea sistemelor de fișiere (QSCANFS)" la pagina 28.

Controlul memoriei de partajare (QSHRMEMCTL)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 19. Valori posibile pentru valoarea de sistem QSHRMEMCTL:

0	Utilizatorii nu pot folosi memorie partajată sau folosiți memorie mapată care are capacitate de scriere. Această valoare înseamnă că utilizatorii nu pot folosi API-uri de memorie partajată (de exemplu, shmat() — API Atașare memorie partajată) și nu pot folosi obiecte de memorie mapată care au capacitate de scriere (de exemplu, mmap() — API Memorie mapează un fișier furnizează această funcție). Folosiți această valoare în medii cu cereri mai mari de securitate.
<u>1</u>	Utilizatorii pot folosi memorie partajată sau mapată care are capacitate de scriere. Această valoare înseamnă că utilizatorii pot folosi API-uri de memorie partajată (de exemplu, shmat() — API Atașare memorie partajată) și pot folosi obiecte de memorie mapată care au capacitate de scriere (de exemplu, mmap() — API Memorie mapează un fișier furnizează această funcție).

Valoare recomandată: 1.

Folosirea autorizării adoptate (QUSEADPAUT)

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

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

Dacă o listă de autorizații este numită în valoarea de sistem și lista de autorizații lipsește, funcția 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 și valoarea *NOADPAUT este specificată în șablonul opțiune, programul creează cu succes chiar dacă lista de autorizații nu există.

Dacă sunt cerute mai multe funcții în comandă sau API și lista de autorizații lipsește, funcția nu este executată.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 20. Valorile posibile pentru valoarea de sistem QUSEADPAUT:

<i>nume listă de autorizații</i>	Este semnalat un mesaj diagnostic pentru a indica faptul că programul este creat cu USEADPAUT(*NO) dacă toate următoarele sunt adevărate: <ul style="list-style-type: none">• Utilizatorul nu are autorizare la lista de autorizări menționată.• Nu mai există și alte erori când programul sau programul serviciu este creat.
<u>*NONE</u>	Toți utilizatorii pot crea sau modifica programe și programe service pentru a folosi autorizare adoptată dacă utilizatorul are autorizarea necesară programului sau programului service.

Valoare recomandată: Pentru mașinile de producție, creați o listă de autorizații cu autorizarea *PUBLIC(*EXCLUDE). Specificați această listă de autorizații pentru valoarea de sistem QUSEADPAUT. Aceasta previne crearea programelor de către cineva care folosește autorizare adoptată.

Ar trebui să luați în considerare proiectarea securității înainte de creare unei liste de autorizații pentru valoarea de sistem QUSEADPAUT. Acest lucru este important în special pentru mediile de dezvoltare de aplicații.

Valorile de sistem referitoare la securitate

Privire generală:

Scop: Specificați 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 și *SECADM

Intrare jurnal:

SV

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

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

QAUTOCFG

Configurare automată dispozitiv

QAUTOVRT

Configurare automată dispozitive virtuale

QDEVRCYACN

Acțiune recuperare dispozitiv

QDSCJOBIV

Interval de timeout job deconectat

Notă: Această valoare de sistem este de asemenea discutată în Centrul de informații (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

QRMTSRVATR

Atribut service la distanță

În continuare sunt prezentate aceste valori de sistem. Sunt afișate opțiunile posibile. Opțiunile care sunt subliniate sunt valorile implicite ale sistemului.

Configurarea automată a dispozitivelor (QAUTOCFG)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: “Valorile de sistem privind securitatea” pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 21. Valorile posibile pentru valoarea de sistem QAUTOCFG:

<u>0</u>	Configurarea automată este dezactivată. Trebuie să configurați manual noile controlerele sau dispozitive locale pe care le adăugați sistemului dumneavoastră.
1	Configurarea automată este activată. Sistemul configurează automat noile controlere sau dispozitive locale pe care le adăugați sistemului dumneavoastră. Operatorul primește un mesaj care indică modificările din configurația sistemului.

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

Configurarea automată a dispozitivelor virtuale (QAUTOVRT)

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

Un **dispozitiv virtual** este o descriere de dispozitiv care nu are asociat hardware. Este folosit pentru a realiza o conexiune între un utilizator și o stație de lucru fizică atașată la un sistem de la distanță.

Dacă permiteți sistemului să configureze automat dispozitive virtuale, utilizatorii vor putea pătrunde mai ușor în sistemul dumneavoastră folosind pass-through sau telnet. Fără configurare automată, un utilizator care încearcă să pătrundă are la dispoziție 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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 22. Valorile posibile pentru valoarea de sistem QAUTOVRT:

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

Valoarea recomandată: 0

Cartea *Remote Work Station Support* conține mai multe informații despre folosirea pass-through pentru stația de afișare. Cartea *TCP/IP Configuration and Reference* conține mai multe informații despre folosirea TELNET.

Ațiunea la recuperarea dispozitivelor (QDEVRCYACN)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 23. Valorile posibile pentru valoarea de sistem QDEVRCYACN:

*DSCMSG	Deconectează jobul. Când semnează din nou, este trimis un mesaj de eroare programului aplicație al utilizatorului.
*MSG	Semnaleză mesajul de eroare I/O programului aplicație al utilizatorului. Programul aplicație execută recuperarea din eroare.
*DSCENDRQS	Deconectează jobul. Când semnează din nou, este executată o funcție 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 și 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 performanței al jobului care se termină, prioritatea jobului este scăzută cu 10, porțiunea de timp este setată la 100 milisecunde și atributul de epurare este setat la da.
*ENDJOBNO LIST	Termină jobul. Pentru job nu este produs un istoric de job. În istoricul QHST este trimis un mesaj indicând că jobul s-a terminat din cauza unei erori de dispozitiv.

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

Valoare recomandată:

*DSCMSG

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

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

Intervalul de timeout pentru job deconectat (QDSCJOBTV)

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

Dacă setați valoarea de sistem QINACTMSGQ pentru a deconecta joburile inactive (*DSCJOB), trebuie setată QDSCJOBTV pentru a termina, la sfârșit, joburile deconectate. Un job deconectat consumă resurse de sistem și păstrează blocări asupra obiectelor.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 24. Valorile posibile pentru valoarea de sistem QDSCJOBTV:

<u>240</u>	Sistemul termină un job deconectat după 240 de minute.
*NONE	Sistemul nu termină automat un job deconectat.
<i> timp-în-minute</i>	Specifică o valoare între 5 și 1440.

Valoare recomandată: 120

Atributul de service la distanță (QRMTSRVATR)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Valorile permise pentru valoarea de sistem QRMTSRVATR sunt:

Tabela 25. Valorile posibile pentru valoarea de sistem QRMTSRVATR:

<u>0</u>	Atributul service la distanță este dezactivat.
<u>1</u>	Atributul service la distanță este activat.

Valoarea recomandată: 0

Pentru informații despre accesul la distanță și valoarea de sistem QRMTSRVATR, vedeți "Securitatea privind cheia IPL" la pagina 2.

Valorile de sistem pentru restaurare referitoare la securitate

Privire generală:

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

Cum se face:

WRKSYSVAL*SEC (comanda Gestionare valori de sistem)

Autorizare:

*ALLOBJ și *SECADM

Intrare jurnal:

SV

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

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

QVfyOBJRST

Verificare obiect la restaurare

QFRCCVNRST

Forțare conversație la restaurare

QALWOBjRST

Permitere restaurare obiecte sensibile la securitate

În continuare sunt prezentate aceste valori de sistem. Sunt afișate opțiunile posibile. Opțiunile care sunt subliniate sunt valorile implicite ale sistemului.

Verificarea obiectului la restaurare (QVfyOBJRST)

Valoarea de sistem QVfyOBJRST determină dacă obiectele trebuie să aibă semnături digitale pentru a fi restaurate în sistemul dumneavoastră. Puteți 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 și *MODULE. Se aplică de asemenea obiectelor *STMF care conțin programe Java.

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

Dacă Digital Certificate Manager (i5/OS opțiunea 34) nu este instalat pe sistem, toate obiectele cu excepția celor semnate de o sursă sistem de încredere sunt tratate ca nesemnate când se determină efectele valorii de sistem QVfyOBJRST în timpul unei operații de restaurare.

Modificarea acestei valori de sistem devine imediat efectivă.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Atenție

Când vă este livrat sistemul, valoarea de sistem QVfyOBRST este setată pe 3. Dacă modificați valoarea QVfyOBRST, este important să o setați la 3 sau mai puțin înainte de a instala o nouă ediție de sistemului de operare i5/OS.

Tabela 26. Valori posibile pentru valoarea de sistem QVfyOBRST:

- | | |
|----------|---|
| 1 | <p>Nu verificați semnăturile la restaurare. Restaurați toate obiectele indiferent de semnătura lor.</p> <p>Această valoare nu ar trebui să fie folosită decât dacă aveți de restaurat obiecte semnate care vor eșua la verificarea semnăturii din unele motive acceptabile.</p> |
| 2 | <p>Verificați obiectele la restaurare. Restaurați comenzile și obiectele stare utilizator neseminate. Restaurați comenzile și obiectele stare utilizator semnate chiar dacă semnăturile nu sunt valide.</p> <p>Această valoare trebuie să fie folosită numai dacă există anumite obiecte cu semnături nevalide pe care doriți să le restaurați. În general, este periculos să restaurați obiecte cu semnături care nu sunt valide pe sistemul dumneavoastră.</p> |
| 3 | <p>Verificați semnăturile la restaurare. Restaurați comenzile și obiectele stare utilizator neseminate. Restaurați comenzile și obiectele stare utilizator semnate numai dacă semnăturile sunt valide.</p> <p>Această valoare poate fi folosită pentru operații normale, când vă așteptați ca unele dintre obiectele pe care le restaurați să nu fie semnate, dar doriți să vă asigurați că toate obiectele semnate au semnături valide. Comenzile și programele pe care le-ați creat sau cumpărat înainte ca semnăturile digitale să fie disponibile vor fi neseminate. Această valoare permite acelor comenzi și programe să fie restaurate. Aceasta este valoarea implicită.</p> |
| 4 | <p>Verificați semnăturile la restaurare. Nu restaurați comenzile și obiectele stare utilizator neseminate. Restaurați comenzile și obiectele stare utilizator semnate chiar dacă semnăturile nu sunt valide.</p> <p>Această valoare trebuie să fie folosită numai dacă există anumite obiecte cu semnături nevalide pe care doriți să le restaurați, dar nu doriți să existe posibilitatea de a fi restaurate obiectele neseminate. În general, este periculos să restaurați obiecte cu semnături care nu sunt valide pe sistemul dumneavoastră.</p> |
| 5 | <p>Verificați semnăturile la restaurare. Nu restaurați comenzile și obiectele stare utilizator neseminate. Restaurați comenzile și obiectele stare utilizator semnate numai dacă semnăturile sunt valide.</p> <p>Această valoare este cea mai restrictivă valoare și trebuie să fie folosită când singurele obiecte care doriți să fie restaurate sunt acelea care au fost semnate de surse de încredere.</p> |

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

Unele comenzi folosesc o semnătură care nu acoperă toate părțile obiectului. Unele părți de comandă nu sunt semnate, în timp ce alte părți sunt semnate doar când conțin 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 validității unei comenzi care nu are unul.
- Modificarea parametrului 'unde este permisă rularea'.
- Modificarea parametrului 'permitere utilizator limitat'.

Dacă doriți, puteți să adăugați propria dumneavoastră semnătură comenzilor care includ aceste zone ale obiectului comandă.

Valoare recomandată: 3.

Forțarea conversiei la restaurare (QFRCCVNRST)

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

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

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

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

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabelul de mai jos rezumă valorile permise pentru QFRCCVNRST:

Tabela 27. Valori QFRCCVNRST

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

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

Valoare recomandată: 3 sau mai mare.

Permiterea restaurării obiectelor sensibile la securitate (QALWOBJRST)

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

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

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

ATENȚIE: Este important să setați valoarea QALWOBJRST la *ALL înainte să realizați unele activități de sistem, precum:

- Instalarea unei noi ediții a programului cu licență i5/OS.
- Instalarea noilor programe cu licență.
- Recuperarea sistemului.

Aceste activități pot eșua dacă valoarea QALWOBJRST nu este *ALL. Pentru a asigura securitatea sistemului, readuceți valoarea QALWOBJRST la setarea dumneavoastră normală după efectuarea activității de sistem.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

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

Tabela 28. Valori posibile pentru valoarea de sistem QALWOBJRST:

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

Valoare recomandată: Valoarea de sistem QALWOBJRST furnizează o metodă de a proteja sistemul de programe care pot crea probleme serioase. Pentru operații normale, setați această valoare pe *NONE. Nu uitați s-o modificați pe *ALL înainte de a realiza activitățile menționate anterior. Dacă restaurați programe și aplicații în mod regulat pe sistemul dumneavoastră, s-ar putea să fie necesară setarea valorii de sistem QALWOBJRST la *ALWPGMADP.

Valorile de sistem pentru parole

Privire generală:

Scop: Specificați valori de sistem pentru a seta cerințele privind alocarea parolelor utilizatorilor.

Cum se face:

WRKSYSVAL *SEC (comanda Gestionare valori de sistem)

Autorizare:

*ALLOBJ și *SECADM

Intrare jurnal:

SV

Notă: Modificările au efect imediat (cu excepția QPWDLVL). IPL-ul nu este necesar.

Următoarele valori de sistem controlează parolele. Aceste valori de sistem obligă utilizatorii să modifice parolele regulat și ajută la împiedicarea utilizatorilor de a alocă parole triviale sau ușor de ghicit. De asemenea, ele pot asigura faptul că parolele respectă cerințele rețelei dumneavoastră de comunicații:

QPWDEXPITY¹

Interval de expirare

QPWDLVL

Nivel parolă

QPWDMINLEN¹

Lungime minimă

QPWDMAXLEN¹

Lungime maximă

QPWDRQDDIF¹

Diferență necesară

QPWDLMTCHR

Caractere restricționate

QPWDLMTAJC

Caractere adiacente restricționate

QPWDLMTREP

Caractere repetate restricționate

QPWDPOSDIF

Diferență poziție caracter

QPWDRQDDGT

Necesitate caracter numeric

QPWDVLDPGM

Program validare parolă

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

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

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

Intervalul de expirare a parolei (QPWDEXPITV)

Valoarea de sistem QPWDEXPITV controlează numărul de zile permise înainte a fi cerută schimbarea parolei. Dacă un utilizator încercă 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 : 10/30/91 14:15:00

Sign-on attempts not valid : 3

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

1. Aceste valori de sistem sunt discutate de asemenea în Centrul de informare (vedeți "Cerințe preliminare și informații înrudite" la pagina xvi pentru detalii).

Tabela 29. Valorile posibile pentru valoarea de sistem QPWDEXPITV:

*NOMAX	Utilizatorii nu trebuie să-și modifice parolele.
<i>limită-in-zile</i>	Specificați o valoare între 1 și 366.

Valoare recomandată: de la 30 până la 90.

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

Nivelul parolei (QPWDLVL)

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

Nivelul de parolă poate fi setat să permită 'passphrase' (frază-parolă) ca valoare a parolei. Termenul 'passphrase' este uneori folosit în industria calculatoarelor pentru a descrie o valoare de parolă care poate fi foarte lungă și are puține restricții (sau deloc) privind caracterele folosite în valoarea parolei. Într-o frază-parolă, pot fi folosite spații între litere, ceea ce vă permite să aveți ca valoare de parolă o propoziție sau un fragment de propoziție. Singurele restricții dintr-o frază-parolă sunt imposibilitatea de a începe cu un asterisc (*) și înlăturarea spațiilor din coadă. Înainte să modificați nivelul parolei pe sistemul dumneavoastră, revedeți secțiunea "Planificarea modificărilor nivelului de parolă" la pagina 196.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 30. Valori posibile pentru valoarea de sistem QPWDLVL:

0	Sistemul suportă parole de profil de utilizator cu o lungime de 1-10 caractere. Caracterele permise sunt A-Z, 0-9 și caracterele \$, @, # și liniuța de subliniere. Setarea QPWDLVL 0 ar trebui folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o rețea, iar acele sisteme rulează cu o valoare QPWDLVL de 0 sau cu o ediție de sistem de operare mai mică de V5R1M0. QPWDLVL 0 ar trebui folosită dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. Trebuie să folosiți QPWDLVL 0 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) și cu alte sisteme folosind parole de 1-10 caractere. Când valoarea QPWDLVL a sistemului este setată pe 0, sistemul de operare va crea parola codată pentru folosirea la QPWDLVL 2 și 3. Valoarea parolei care poate fi folosită la QPWDLVL 2 și 3 va fi aceeași parolă ca și cea folosită la QPWDLVL 0 sau 1.
1	QPWDLVL 1 este suportul echivalent al QPWDLVL 0 cu următoarea excepție: parolele iSeries NetServer pentru clienții Windows 95/98/ME vor fi înlăturate de pe sistem. Dacă folosiți suportul client pentru produsul iSeries NetServer, nu puteți folosi valoarea 1 a QPWDLVL. QPWDLVL 1 îmbunătățește securitatea sistemului iSeries prin înlăturarea tuturor parolelor iSeries NetServer de pe sistem.
2	Sistemul suportă parole de profil utilizator de 1-128 caractere. Sunt permise caractere cu litere mici sau mari. Parolele pot conține orice caracter, iar parola va fi sensibilă la majuscule. Setarea QPWDLVL 2 este văzută ca un nivel de compatibilitate. Acest nivel permite mutarea înapoi la QPWDLVL 0 sau 1 atât timp cât parola creată la QPWDLVL 2 sau 3 îndeplinește cerințele de lungime și sintaxă ale unei parole valide la QPWDLVL 0 sau 1. Se poate folosi QPWDLVL 2 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer), atât timp cât parola dumneavoastră este de 1-14 caractere lungime. Setarea QPWDLVL 2 nu poate fi folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o rețea, iar acele sisteme rulează cu o valoare QPWDLVL de 0 sau cu o ediție de sistem de operare mai mică de V5R1M0. QPWDLVL 2 nu poate fi folosită dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. Nu este înlăturată nici o parolă codată de pe sistem când se modifică QPWDLVL la 2.

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

3	Sistemul suportă parole de profil utilizator de 1-128 caractere. Sunt permise caractere cu litere mici sau mari. Parolele pot conține orice caracter, iar parola va fi sensibilă la majuscule. Setarea QPWLVL 3 nu poate fi folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o rețea, iar acele sisteme rulează cu o valoare QPWLVL de 0 sau cu o ediție de sistem de operare mai mică de V5R1M0. QPWLVL 3 nu poate fi folosit dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolilor de 1-10 caractere. Nu se poate folosi QPWLVL 3 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer). Toate parolele de profil de utilizator care sunt folosite la QPWLVL 0 și 1 sunt înlăturate de pe sistem când QPWLVL este 3. Modificarea de la QPWLVL 3 înapoi la QPWLVL 0 sau 1 necesită o modificare la QPWLVL 2 înainte de trecerea la 0 sau 1. QPWLVL 2 permite crearea parolilor de profil de utilizator care pot fi folosite la QPWLVL 0 sau 1 atât timp cât cerințele de lungime și sintaxă pentru parolă îndeplinesc regulile pentru QPWLVL 0 sau 1.
---	---

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

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

Lungimea minimă a parolilor (QPWDMINLEN)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 31. Valorile posibile pentru valoarea de sistem QPWDMINLEN:

<u>6</u> <i>număr-minim-de-caractere</i>	Sunt necesare cel puțin șase caractere pentru parole. Specificați o valoare de la 1 la 10 când valoarea de sistem a nivelului parolei (QPWLVL) este 0 sau 1. Specificați o valoare de la 1 la 128 când valoarea de sistem a nivelului parolei (QPWLVL) este 2 sau 3.
---	---

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

Lungimea maximă a parolilor (QPWDMAXLEN)

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

Unele rețele de comunicare necesită o parolă de 8 caractere sau mai puțin. Folosiți această valoare de sistem pentru a vă asigura că parolele îndeplinesc cerințele rețelei dumneavoastră.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 32. Valori posibile pentru valoarea de sistem QPWDMAXLEN:

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

Valoare recomandată: 8.

Necesitatea diferenței în parole (QPWDRQDDIF)

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 33. Valorile posibile pentru valoarea de sistem QPWDRQDDIF:

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

Valoare recomandată: Selectați valoarea 5 sau mai mică, pentru a împiedica folosirea de parole repetate. Folosiți o combinație a valorii de sistem QPWDRQDDIF și a valorii de sistem QPWDEXPITV (interval expirare parolă) pentru a împiedica refolosirea unei parole pentru cel puțin 6 luni. De exemplu, setați valoarea de sistem QPWDEXPITV la 30 (zile) și valoarea de sistem QPWDRQDDIF la 5 (10 parole unice). Aceasta înseamnă că un utilizator obișnuit, care modifică parola când este avertizat de sistem, nu va repeta o parolă timp de aproximativ 9 luni.

Restricționarea caracterelor pentru parole (QPWDLMTCHR)

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 34. Valori posibile pentru valoarea de sistem QPWDLMTCHR:

*NONE	Nu există caractere restricționate pentru parole.
<i>caractere-restricționate</i>	Specificați până la 10 caractere restricționate. Caracterele valide sunt de la A la Z, 0 la 9 și caracterele speciale liră sterlină (#), dolar (\$), a rond (@) și liniuța de subliniere (_).

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

Restricționarea cifrelor consecutive pentru parole (QPWDLMTAJC)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 35. Valorile posibile pentru valoarea de sistem QPWDLMTAJC:

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

Restricționarea caracterelor repetate pentru parole (QPWDLMTREP)

Valoarea de sistem QPWDLMTREP limitează folosirea caracterelor de repetare într-o parolă. Această valoare furnizează securitate suplimentară împiedicând utilizatorii să specifice parole care sunt ușor de ghicit, cum ar fi același 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 diferența între o literă mică 'a' și o literă mare 'A'.

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 36. Valori posibile pentru valoarea de sistem QPWDLMTREP:

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

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

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

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

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

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

Diferența poziției caracterelor pentru parole (QPWDPOSDIF)

Valoarea de sistem QPWDPOSDIF controlează fiecare poziție într-o nouă parolă. Aceasta furnizează securitate suplimentară împiedicând utilizatorii să folosească același caracter (alfabetic sau numeric) într-o poziție corespunzătoare aceleași poziții din parola anterioară.

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 39. Valorile posibile pentru valoarea de sistem QPWDPOSDIF:

0	Pot fi folosite aceleași caractere într-o poziție corespunzătoare aceleași poziții din parola anterioară.
1	Nu poate fi folosit același caracter într-o poziție corespunzătoare aceleași poziții din parola anterioară.

Necesitatea caracterelor numerice în parole (QPWDRQDDGT)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 40. Valori posibile pentru valoarea de sistem QPWDRQDDGT:

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

Valoare recomandată: 1.

Programul de aprobare a parolei (QPWDVLDPGM)

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

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 41. Valorile posibile pentru valoarea de sistem QPWDVLDPGM:

*NONE	Nu este folosit nici un program scris de utilizator. Aceasta include orice program de aprobare a parolei înregistrat în facilitatea de semnare ieșire.
*REGFAC	Programul de validare este extras din facilitatea de semnare, punctul de ieșire 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.
<i>nume-program</i>	Specificați 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 așteptare a valorii de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3.
<i>nume-biblioteca</i>	Specificați numele bibliotecii unde este localizat programul scris de utilizator. Dacă numele bibliotecii nu este specificat, programul este căutat folosind lista de biblioteci (*LIBL) a utilizatorului care modifică valoarea de sistem. QSYS este biblioteca recomandată.

Folosirea unui program de aprobare a parolei

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

În cazul în care este necesar să vă recuperați sistemul dintr-o eșuare de disc, puneți programul de aprobare a parolei în biblioteca QSYS. În acest fel, programul de aprobare a parolei este încărcat când restaurați biblioteca QSYS.

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

Tabela 42. Parametrii pentru programul de aprobare a parolei

Poziție	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 Poziția 4 este opțională.

Dacă în valoarea de sistem QPWDVLDPGM s-a specificat *REGFAC, consultați informațiile despre Programul de ieșire pentru securitate din manualul System API, pentru detalii despre parametrii transmiși programului de validare.

Dacă programul dumneavoastră determină că noua parolă nu este validă, puteți fie să trimiteți propriul dumneavoastră mesaj de excepție (folosind comanda SNDPGMMSG), fie să setați codul retur la o valoare diferită de 0 și să lăsați sistemul să afișeze un mesaj de eroare. Mesajele de excepție care sunt semnalate de programul dumneavoastră trebuie să fie create cu opțiunea DMPLST(*NONE) a comenzii ADDMSGD (Add Message Description - Adăugare descriere mesaj).

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

Atenție: Parola curentă și noua parolă sunt trimise programului de validare fără criptare. Programul de validare poate stoca parolele într-un fișier de bază de date, compromițând astfel securitatea sistemului. Asigurați-vă că funcțiile programului de validare sunt examinate de responsabilul cu securitatea și 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 aceeași zi. Pot fi adăugate calcule adiționale pentru a verifica parolele cu alte criterii:

```

/*****/
/* NAME:      PWDVALID - Password Validation      */
/*           */
/* FUNCTION:  Limit password change to one per   */
/*           day unless the password is expired */
/*****/
PGM (&NEW &OLD &RTNCD &USER)
DCL VAR(&NEW)      TYPE(*CHAR) LEN(10)
DCL VAR(&OLD)      TYPE(*CHAR) LEN(10)
DCL VAR(&RTNCD)    TYPE(*CHAR) LEN(1)
DCL VAR(&USER)     TYPE(*CHAR) LEN(10)
DCL VAR(&JOBDATE)  TYPE(*CHAR) LEN(6)
DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
DCL VAR(&PWDEXP)   TYPE(*CHAR) LEN(4)
/* Get the current date and convert to YMD format */
RTVJOBA      DATE(&JOBDATE)
CVTDATE      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, convertește noua parolă la CCSID 37), că parola nouă nu se termină într-un caracter numeric și că noua parolă nu conține numele profilului utilizatorului. Acest exemplu presupune că fost creat un fișier de mesaje (PWDERRORS) a și au fost adăugate descrierile de mesaj (PWD0001 și PWD0002) în fișierul de mesaje. Pot fi adăugate calcule adiționale 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.                               */

```

```

/*****/
I 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:;<=>?+
@ABCDEFGHIJKLMNPOQRSTUVWXYZ[\]^_+
`ABCDEFGHIJKLMNPOQRSTUVWXYZ{|}~.+
.....+
.....+
.....+
.....+')

DCL &XLATEC   *CHAR 255 VALUE('.....+
.....+
.....+
.....+
.ABCDEFGHI.....JKLMNOPQR.....+
..STUVWXYZ.....+
.....+
.....+')

/*****/
/* FORMAT OF EXINPUT IS: */

/* POSITION  DESCRIPTION */
/* 001 - 020 EXIT POINT NAME */
/* 021 - 028 EXIT POINT FORMAT NAME */
/* 029 - 032 PASSWORD LEVEL (binary) */
/* 033 - 042 USER PROFILE NAME */
/* 043 - 044 RESERVED */
/* 045 - 048 OFFSET TO OLD PASSWORD (binary) */
/* 049 - 052 LENGTH OF OLD PASSWORD (binary) */
/* 053 - 056 CCSID OF OLD PASSWORD (binary) */
/* 057 - 060 OFFSET TO NEW PASSWORD (binary) */
/* 061 - 064 LENGTH OF NEW PASSWORD (binary) */
/* 065 - 068 CCSID OF NEW PASSWORD (binary) */
/* ??? - ??? OLD PASSWORD */
/* ??? - ??? NEW PASSWORD */
/* */

/*****/

/* Establish a generic monitor for the program. */
/*****/

MONMSG      CPF0000
/* Assume new password is valid */
CHGVAR &RTN VALUE('0') /* accept */
/* Get new password length, offset and value. Also get user name */
CHGVAR &NPLEN VALUE(%BIN(&EXINPUT 61 4))
CHGVAR &NPOFF VALUE(%BIN(&EXINPUT 57 4) + 1)
CHGVAR &UNAME VALUE(%SST(&EXINPUT 33 10))

```

```

CHGVAR &NEWPW VALUE(%SST(&EXINPUT &NPOFF &NPLEN))
/* If CCSID is 13488, probably used the QSYCHGPW API which converts */
/* the passwords to UNICODE CCSID 13488. So convert to CCSID 37, if */
/* possible, else give an error */
IF COND(%BIN(&EXINPUT 65 4) = 13488) THEN(DO)
  CHGVAR &INDX2 VALUE(1)
  CHGVAR &INDX3 VALUE(1)
  CVT1:
    CHGVAR &XLTCHR VALUE(%BIN(&NEWPW &INDX2 2))
    IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
      CHGVAR &RTN VALUE('3') /* reject */
      SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
GOTO DONE
ENDDO
  CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEU &XLTCHR 1))
  CHGVAR &INDX2 VALUE(&INDX2 + 2)
  CHGVAR &INDX3 VALUE(&INDX3 + 1)
  IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
  GOTO CVT1
ECVT1:
  CHGVAR &NPLEN VALUE(&INDX3 - 1)
  CHGVAR %SST(&EXINPUT 65 4) VALUE(X'00000025')
ENDDO

/* Check the CCSID of the new password value - must be 37 */
IF COND(%BIN(&EXINPUT 65 4) *NE 37) THEN(DO)
  CHGVAR &RTN VALUE('3') /* reject */
  SNDPGMMSG MSG('CCSID OF NEW PASSWORD MUST BE 37')
GOTO DONE
ENDDO

/* UPPERCASE NEW PASSWORD VALUE */
CHGVAR &INDX2 VALUE(1)
CHGVAR &INDX3 VALUE(1)
CVT4:
  CHGVAR %SST(&XLTCHR2 2 1) VALUE(%SST(&NEWPW &INDX2 1))
  CHGVAR &XLTCHR VALUE(%BIN(&XLTCHR2 1 2))
  IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
    CHGVAR &RTN VALUE('3') /* reject */
    SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
GOTO DONE
ENDDO
  IF COND(%SST(&XLATEC &XLTCHR 1) *NE '.' ) +
  THEN(CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEC &XLTCHR 1)))
  CHGVAR &INDX2 VALUE(&INDX2 + 1)
  CHGVAR &INDX3 VALUE(&INDX3 + 1)
  IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT4)
  GOTO CVT4
ECVT4:

/* CHECK IF LAST POSITION OF NEW PASSWORD IS NUMERIC */
IF COND(%SST(&NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)

/* CHECK IF PASSWORD CONTAINS USER PROFILE NAME */
CHGVAR &UNLEN VALUE(1)
LOOP2: /* FIND LENGTH OF USER NAME */
  IF COND(%SST(&UNAME &UNLEN 1) *NE ' ') THEN(DO)
    CHGVAR &UNLEN VALUE(&UNLEN + 1)

```

```

        IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
        GOTO LOOP2
    ENDDO
ELOOP2:
    CHGVAR &UNLEN VALUE(&UNLEN - 1)

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

/* New Password is valid                          */
GOTO DONE

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

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

DONE:
ENDPGM

```

Valorile de sistem pentru controlul auditării

Privire generală:

Scop: Specificați valori de sistem pentru a controla auditarea securității 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

Acțiune de terminare auditare

QAUDFRCLVL

Nivel forțare auditare

QAUDLVL

Nivel de auditare

QAUDLVL2

Extensie nivel de auditare

QCRTOBJAUD

Creare auditare implicită

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

Controlul auditării (QAUDCTL)

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

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

Tabela 43. Valorile posibile pentru valoarea de sistem QAUDCTL:

<u>*NONE</u>	Nici o auditare nu este realizată pentru acțiuni utilizator și obiecte.
*NOTAVL	Indică faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Nu puteți seta valoarea sistemului la această valoare.
*OBJAUD	Auditarea este executată pentru obiectele care au fost selectate folosind comenzile CHGOBJAUD, CHGDLOAUD sau CHGAUD.
*AUDLVL	Auditarea este executată pentru orice funcții selectate în valorile de sistem QAUDLVL și QAUDLVL2 și în parametrul AUDLVL al profilurilor de utilizator individuale. Nivelul de auditare pentru un utilizator este specificat folosind comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator).
*NOQTEMP	Pentru majoritatea acțiunilor auditarea nu este realizată dacă obiectul este în biblioteca QTEMP. Vedeți Capitolul 9, "Auditarea securității pe sistemul iSeries", la pagina 229 pentru detalii suplimentare. Trebuie să specificați această valoare cu *OBJAUD sau *AUDLVL. Vedeți "Planificarea auditării securității" la pagina 234 pentru o descriere completă a procesului pentru controlarea auditării pe sistemul dumneavoastră.

Acțiunea pentru oprirea auditării (QAUDENDACN)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 44. Valori posibile pentru valoarea de sistem QAUDENDACN:

*NOTAVL	Această valoare este afișată 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.
<u>*NOTIFY</u>	Mesajul CPI2283 este trimis în coada de mesaje QSYSOPR și în coada de mesaje QSYSMSG (dacă există) din oră în oră, până când auditarea este repornită cu succes. Valoarea de sistem QAUDCTL este setată la *NONE pentru a împiedica sistemul să încerce să scrie intrări suplimentare în jurnalul de auditare. Continuă procesarea în sistem.
*PWRDWNSYS	Dacă este realizat un IPL înaintea repornirii auditării, este trimis mesajul CPI2284 în cozile de mesaje QSYSOPR și QSYSMSG în timpul IPL-ului. Dacă nu este capabil să scrie o intrare de jurnal de auditare, sistemul își oprește alimentarea imediat. Unitatea de sistem afișează codul de referință sistem (SRC) B900 3D10. Când este pornit din nou, sistemul este într-o stare restricționată. Această înseamnă că subsistemul de control este într-o stare restricționată, nici un alt subsistem nu este activ și 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 și *AUDIT.

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

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

Nivelul de forțare a auditării (QAUDFRCLVL)

Valoarea de sistem QAUDFRCLVL determină cât de des se forțează noi intrări de jurnal de auditare din memorie spre spațiul 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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 45. Valorile posibile pentru valoarea de sistem QAUDFRCLVL:

*NOTAVL	Această valoare este afișată 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.
<u>*SYS</u>	Sistemul determină când sunt scrise intrările de jurnal în spațiul de stocare auxiliar pe baza performanței de sistem interne.
număr-de-înregistrări	Specificați un număr între 1 și 100 pentru a determina câte intrări de auditare se pot acumula în memorie înainte de a fi scrise în spațiul de stocare auxiliar. Cu cât este mai mic numărul, cu atât este mai mare impactul asupra performanței sistemului.

Valoare recomandată: *SYS furnizează cea mai bună performanță de auditare. Totuși, dacă instalarea dumneavoastră necesită să nu fie pierdută nici o intrare de auditare când sistemul termină anormal, trebuie să specificați 1. Specificarea 1 poate scădea performanța.

Nivelul de auditare (QAUDLVL)

Valoarea de sistem QAUDLVL împreună cu valoarea de sistem QAUDLVL2 determină ce evenimente referitoare la securitatea sunt înregistrate în jurnalul de auditare a securității (QAUDJRN) pentru toți utilizatorii sistemului. Puteți specifica mai multe valori pentru valoarea de sistem QAUDLVL, în cazul în care nu specificați *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 restricționată. Vedeți Capitolul 3: "Valorile de sistem privind securitatea" pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 46. Valori posibile pentru valoarea de sistem QAUDLVL:

*NONE	Nici un eveniment controlat de valorile de sistem QAUDLVL sau QAUDLVL2 nu este înregistrat. Evenimentele sunt înregistrate pentru utilizatori individuali pe baza valorilor AUDLVL din profilurile de utilizator.
*NOTAVL	Această valoare este afișată 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 și QAUDLVL2, vor fi folosite pentru a determina acțiunile de securitate care vor fi auditate.
*ATNEVT	Sunt înregistrate evenimentele de atenționare
*AUTFAIL	Sunt înregistrate evenimentele de eșuare a autorizării.
*CREATE	Sunt înregistrate operațiile de creare obiecte.
*DELETE	Sunt înregistrate operațiile de ștergere obiecte.
*JOBDTA	Sunt înregistrate acțiunile care afectează un job.
*NETBAS	Sunt auditate funcțiile de bază ale rețelei.
*NETCLU	Sunt auditate operațiile de cluster și grup de resurse cluster.
*NETCMN	Sunt auditate funcțiile de comunicație și rețea.
	 *NETCMN este compus din câteva valori pentru a vă permite să vă personalizați mai bine auditarea. Următoarele valori formează *NETCMN:
	 *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Sunt auditate eșuările de rețea.
*NETSCK	Sunt auditate task-urile de socket.
*OBJMGT	Sunt înregistrate operațiile de redenumire și mutare obiecte.
*OFCSRV	Sunt înregistrate modificările aduse directorului de distribuție sistem și acțiunile de mail office.
*OPTICAL	Este înregistrată folosirea volumelor optice.
*PGMADP	Este înregistrată obținerea autorizării de la un program care adoptă autorizare.
*PGMFAIL	Sunt înregistrate violările de integritate a sistemului.
*PRTDTA	Sunt înregistrate tipărirea unui fișier spool, trimiterea ieșirii direct la o imprimantă și trimiterea ieșirii la o imprimantă la distanță.
*SAVRST	Sunt înregistrate operațiile de restaurare.
*SECCFG	Este auditată configurația de securitate.
*SECDIRSRV	Sunt înregistrate modificările sau actualizările când se execută funcții de serviciu de director.
*SECIPC	Sunt auditate modificările aduse comunicațiilor între procese.
*SECNAS	Sunt auditate acțiunile serviciului de autentificare în rețea.
*SECRUN	Sunt auditate funcțiile de timp de rulare securitate.
*SECCKD	Sunt auditați descriptorii de socket.

Tabela 46. Valori posibile pentru valoarea de sistem QAUDLVL: (continuare)

*SECURITY	Sunt înregistrate funcțiile referitoare la securitate.
	*SECURITY este compus din câteva valori pentru a vă permite să vă personalizați mai bine auditarea. Următoarele valori formează *SECURITY:
	*SECCFG
	*SEC DIRSRV
	*SECIPC
	*SECNAS
	*SECRUN
	*SEC SCKD
	*SECVFY
	*SECVL DL
*SECVFY	Este auditată folosirea funcțiilor de verificare.
*SECVL DL	Sunt auditate modificările aduse obiectelor din lista de validare.
*SERVICE	Este înregistrată folosirea uneltelor de service.
*SPLFDTA	Sunt înregistrate acțiunile executate asupra fișierelor spool.
*SYSMGT	Folosirea funcțiilor de gestionare sisteme este înregistrată în istoric.

Vedeți “Planificarea auditării acțiunilor” la pagina 234 pentru o descriere completă a tipurilor de intrare jurnal și valorile posibile pentru QAUDLVL.

Extensia nivelului de auditare (QAUDLVL2)

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: “Valorile de sistem privind securitatea” pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 47. Valorile posibile pentru valoarea de sistem QAUDLVL2:

*NONE	În această valoare de sistem nu este conținută nici o valoare de auditare.
*NOTAVL	Această valoare este afișată 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 atenționare
*AUTFAIL	Sunt înregistrate evenimentele de eșuare a autorizării.
*CREATE	Sunt înregistrate operațiile de creare obiecte.
*DELETE	Sunt înregistrate operațiile de ștergere obiecte.
*JOBDTA	Sunt înregistrate acțiunile care afectează un job.
*NETBAS	Sunt auditate funcțiile de bază ale rețelei.
*NETCLU	Sunt auditate operațiile de cluster și grup de resurse cluster.
*NETCMN	Sunt auditate funcțiile de comunicație și rețea.
	*NETCMN este compus din câteva valori pentru a vă permite să vă personalizați mai bine auditarea. Următoarele valori formează *NETCMN:
	*NETBAS
	*NETCLU
	*NETFAIL
	*NETSCK
*NETFAIL	Sunt auditate eșuările de rețea.
*NETSCK	Sunt auditate task-urile de socket.

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

*OBJMGT	Sunt înregistrate operațiile de redenumire și mutare obiecte.
*OFCSR	Sunt înregistrate modificările aduse directorului de distribuție sistem și acțiunile de mail office.
*OPTICAL	Este înregistrată folosirea volumelor optice.
*PGMADP	Este înregistrată obținerea autorizării de la un program care adoptă autorizare.
*PGMFAIL	Sunt înregistrate violările de integritate a sistemului.
*PRTDTA	Sunt înregistrate tipărirea unui fișier spool, trimiterea ieșirii direct la o imprimantă și trimiterea ieșirii la o imprimantă la distanță.
*SAVRST	Sunt înregistrate operațiile de restaurare.
*SECCFG	Este auditată configurația de securitate.
*SECDIRSRV	Sunt înregistrate modificările sau actualizările când se execută funcții de serviciu de director.
*SECIPC	Sunt auditate modificările aduse comunicațiilor între procese.
*SECNAS	Sunt auditate acțiunile serviciului de autentificare în rețea.
*SECRUN	Sunt auditate funcțiile de timp de rulare securitate.
*SECCKD	Sunt auditați descriptorii de socket.
*SECURITY	Sunt înregistrate funcțiile referitoare la securitate.
	*SECURITY este compus din câteva valori pentru a vă permite să vă personalizați mai bine auditarea. Următoarele valori formează *SECURITY:
	*SECCFG
	*SECDIRSRV
	*SECIPC
	*SECNAS
	*SECRUN
	*SECCKD
	*SECVFY
	*SECVLDL
*SECVFY	Este auditată folosirea funcțiilor de verificare.
*SECVLDL	Sunt auditate modificările aduse obiectelor din lista de validare.
*SERVICE	Este înregistrată folosirea uneltelor de service.
*SPLFDTA	Sunt înregistrate acțiunile executate asupra fișierelor spool.
*SYSMGT	Folosirea funcțiilor de gestionare sisteme este înregistrată în istoric.

Vedeți “Planificarea auditării acțiunilor” la pagina 234 pentru o descriere completă a tipurilor de intrare jurnal și valorile posibile pentru QAUDLVL2.

Auditarea noilor obiecte (QCRTOBJAUD)

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

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

Notă: Această valoare de sistem este o valoare restricționată. Vedeți Capitolul 3: “Valorile de sistem privind securitatea” pentru detalii despre cum se face restricționarea modificărilor asupra valorilor de sistem de securitate și pentru o listă completă a valorilor de sistem restricționate.

Tabela 48. Valori posibile pentru valoarea de sistem QCRTOBJAUD:

*NONE	Nu este realizată nici o auditare pentru obiect.
*NOTAVL	Această valoare este afișată 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 utilizatorului care accesează obiectul.
*CHANGE	Este scrisă o înregistrare de auditare atunci când obiectul este modificat.
*ALL	Este scrisă o înregistrare de auditare pentru orice acțiune care afectează conținutul obiectului. Este scrisă o înregistrare de auditare dacă se modifică conținutul obiectului.

Valoare recomandată: Valoarea pe care o selectați depinde de cerințele de auditare ale instalării dumneavoastră. Secțiunea “Planificarea auditării accesului la obiect” la pagina 252 furnizează mai multe informații despre metodele de setare a auditării de obiecte pe sistemul dumneavoastră. Puteți controla valoarea de auditare la nivel de director cu parametrul CRTOBJAUD la comanda Facere Director(CRTDIR) și valoarea *CRTOBJAUD la comanda Modificare atribute (CHGATR). Puteți de asemenea controla valoarea de auditare la nivelul bibliotecii cu parametrul CRTOBJAUD cu comanda CRTLIB și comanda CHGLIB.

Capitolul 4. Profilurile de utilizator

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

Privire generală:

Scop: Crearea și întreținerea profilurilor de utilizator și a profilurilor de grup în sistem

Cum se face:

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

Comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator)

Autorizare:

Autorizarea specială *SECADM

Autorizarea specială *AUDIT pentru modificarea auditării de utilizator

Intrare jurnal:

AD pentru modificări asupra auditării de utilizator

CO pentru crearea unui profil utilizator

CP pentru modificări asupra profilurilor de utilizator

DO pentru ștergerea unui profil utilizator

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

Rolurile profilului de utilizator

Profilul utilizator are mai multe roluri în sistem:

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

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

Tabela 143 din Anexa B arată valorile alocate când sistemul creează un profil de utilizator.

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

Profilurile de grup

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

Unealtă de securitate

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

Unealtă de personalizare

Un profil de grup poate fi folosit drept un model pentru crearea de profiluri de utilizator individuale. Majoritatea persoanelor care fac parte din același grup au aceleași necesități de personalizare, cum ar fi meniul inițial și imprimanta implicită. Puteți defini aceste lucruri în profilul de grup și puteți apoi copia profilul de grup pentru a crea profiluri de utilizator individuale.

Puteți crea profiluri de grup în același mod în care creați profiluri individuale. Sistemul recunoaște un profil de grup când adăugați primul membru la grup. În acel moment, sistemul setează informațiile 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. Puteți de asemenea să desemnați un profil drept un profil de grup în momentul în care îl creați specificând o valoare în parametrul GID. "Planificarea profilurilor de grup" la pagina 213 arată un exemplu de setare a unui profil de grup.

Câmpuri parametru profil utilizator

Când creați un profil de utilizator, profilului îi sunt date următoarele autorizări pentru el însuși: *OBJMGT, *CHANGE. Aceste autorizări sunt necesare pentru funcțiile sistemului și nu trebuie înlăturate.

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

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

- Nivelul de ajutorare elementar, care conține informații mai puține și nu folosește terminologie tehnică.
- Nivelul de ajutorare intermediar, care arată mai multe informații și folosește termeni tehnici.
- Nivelul de ajutorare avansat, care folosește termeni tehnici și arată cantitatea maximă de date, neafișând întotdeauna tasta funcțională și informațiile de opțiune.

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

Titlu câmp

Titlul secțiunii arată cum apare numele de câmp în promptul de comandă Creare profil utilizator, care apare când creați un profil de utilizator cu Nivelul de asistență intermediar pentru comanda Creare profil utilizator (CRTUSRPRF).

Promptul Adăugare utilizator:

Acesta arată cum apare numele de câmp în ecranul Adăugare utilizator și alte ecrane de profil utilizator care folosesc nivelul de ajutorare elementar. Ecranele la nivel de ajutorare elementar afișează un subset al câmpurilor din profilul de utilizator. *Neafișat* înseamnă că acel câmp nu apare în ecranul la nivel de ajutorare elementar. Când folosiți ecranul Adăugare utilizator pentru a crea un profil utilizator, sunt folosite valorile implicite pentru toate câmpurile care nu sunt afișate.

Parametru CL:

Folosiți numele de parametru CL pentru un câmp dintr-un program CL sau când introduceți o comandă de profil de utilizator fără promptare.

Lungime:

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

Autorizare:

Dacă un câmp se referă la un obiect separat, precum o bibliotecă sau un program, vi se spun necesitățile de autorizare pentru acel obiect. Pentru a specifica obiectul când creați sau modificați un profil de utilizator, trebuie să listați autorizările. Pentru a semna folosind profilul, utilizatorul trebuie să menționeze autorizarea. De exemplu, dacă creați profilul de utilizator USERA cu descrierea de job JOB1, trebuie să aveți autorizarea *USE pentru JOB1. USERA trebuie să aibă autorizarea *USE la JOB1 pentru a semna cu succes cu profilul.

În plus, fiecare secțiune descrie valorile posibile pentru câmp și o valoare recomandată.

Nume profil utilizator

Promptul Adăugare utilizator:

Utilizator

Parametru CL:

USRPRF

Lungime:

10

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

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

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

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

Numele profilului de utilizator nu poate începe cu o cifră.

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

Pentru informații suplimentare despre specificarea numelor în sistem, consultați cartea *CL Programming*.

Recomandări pentru denumirea profilurilor de utilizator: Țineți cont de următoarele când alegeți numele profilurilor de utilizator:

- Un nume de profil de utilizator poate avea până la 10 caractere lungime. Unele metode de comunicare limitează ID-ul de utilizator la 8 caractere. Ecranul Adăugare utilizator limitează și numele de profil de utilizator la 8 caractere.
- Folosiți o schemă de numire care face ID-urile de utilizator ușor de ținut minte.
- Sistemul nu face distincție între literele mari și cele mici într-un nume de profil de utilizator. Dacă introduceți caractere alfabetice mici la stația dumneavoastră de lucru, sistemul le traduce în majuscule.
- Ecranele și listele folosite pentru gestionarea profilurilor de utilizator le arată în ordine alfabetică, după numele de profil de utilizator.
- Evitați folosirea caracterelor speciale în numele de profiluri de utilizator. Caracterele speciale pot cauza probleme legate de maparea tastaturii pentru anumite stații de lucru sau de versiunile de limbă națională ale programului licențiat i5/OS.

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

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

Recomandări pentru denumirea profilurilor de grup: Dacă doriți să identificați ușor profilurile de grup în liste și ecrane, folosiți o convenție de numire. Începeți toate numele de profiluri de grup cu aceleași caractere, precum GRP (pentru grup) sau DPT (pentru departament).

Parolă

Promptul Adăugare utilizator:

Parolă

Parametru CL:

PAROLĂ

Lungime:

128

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

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

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

Când valoarea de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3, parola este sensibilă la majuscule și poate conține orice caracter, inclusiv caractere spațiu. Totuși, parola nu poate începe cu un caracter asterisc ('*') și caracterele spațiu de la sfârșit sunt înlăturate.

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

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

Puteți seta valori de sistem pentru a controla parolele pe care le alocă utilizatorii. Valorile de sistem pentru compoziția parolei se aplică doar când un utilizator modifică o parolă folosind comanda Modificare parolă (CHGPWD), opțiunea Modificare parolă din meniul ASSIST sau API-ul QSYCHGPW. Dacă valoarea de sistem QPWDMINLEN (lungime minimă parolă) nu este 1 sau valoarea de sistem lungime maximă parolă (QPWDMAXLEN) nu este 10 sau oricare dintre celelalte valori de sistem pentru compoziție parolă a fost modificată față de valoarea implicită, un utilizator nu poate seta parola egală cu numele profilului de utilizator folosind comanda CHGPWD, meniul ASSIST sau API-ul QSYCHGPW.

Consultați subiectul "Valorile de sistem pentru parole" la pagina 38 pentru informații despre setarea valorilor de sistem compoziție parolă.

Tabela 49. Valori posibile pentru PASSWORD:

*USRPRF	Parola pentru acest utilizator este numele profilului de utilizator. Când valoarea de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3, parola este numele profilului de utilizator scris cu majuscule. Pentru profilul JOHNDOE, parola va fi JOHNDOE, nu johndoe.
*NONE	Nici o parolă nu este alocată acestui profil de utilizator. Semnarea nu este permisă cu acest profil de utilizator. Puteți să lansați un job batch folosind un profil de utilizator cu parola *NONE dacă aveți autorizarea corespunzătoare pentru profilul de utilizator.
<i>parolă-utilizator</i>	Un șir de caractere (128 caractere sau mai puțin).

Recomandări pentru parole:

- Setati parola pentru un profil de grup la *NONE. Acest lucru împiedică pe oricine să semneze cu profilul de grup.
- Când creați un profil de utilizator individual, setati parola la o valoare inițială și cereți să fie alocată o parolă nouă când utilizatorul semnează (setati expirarea parolei la *YES). Parola implicită la crearea unui profil de utilizator este numele profilului de utilizator.
- Dacă folosiți o parolă trivială sau implicită la crearea unui nou profil de utilizator, asigurați-vă că utilizatorul intenționează să semneze imediat. Dacă vă așteptați ca utilizatorul să semneze mai târziu, setati starea profilului de utilizator la *DISABLED. Modificați starea în *ENABLED când utilizatorul este gata să semneze. Asta protejează noul profil de utilizator față de folosirea sa de către cineva neautorizat.
- Folosiți valorile de sistem pentru compoziția parolei pentru a împiedica alocarea de către utilizatori de parole triviale.
- Unele metode de comunicații trimit parole între sisteme și limitează lungimea parolei și caracterele pe care le pot conține parolele. Dacă sistemul dumneavoastră comunică cu alte sisteme, folosiți valoarea de sistem QPWDMAXLEN pentru a limita lungimea parolelor. La nivelurile de parolă 0 și 1, valoarea de sistem QPWDLMTCHR poate fi folosită pentru a specifica anumite caractere care nu pot fi folosite în parole.

Setare parolă la Expirată

Prompt adăugare utilizator:

Neafișat

Parametru CL:

PWDEXP

Lungime:

4

Câmpul *Setare parolă la expirată* permite unui administrator de securitate să indice în profilul de utilizator că parola utilizatorului este expirată și că trebuie modificată la următoarea semnare a utilizatorului. Această valoare este resetată la *NO când parola este modificată. Puteți 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 își amintește parola și un administrator de securitate trebuie să alocă una nouă. Dacă se cere utilizatorului să modifice parola alocată de administratorul de securitate, se împiedică cunoașterea de către administratorul de securitate a noii parole și semnarea acestuia în locul utilizatorului.

Când parola unui utilizator a expirat, utilizatorul primește un mesaj la semnare (vedeți Figura 1). Utilizatorul poate apăsa tasta Enter pentru a alocă o nouă parolă sau poate apăsa F3 (Ieșire) pentru a anula încercarea de semnare fără alocarea unei noi parole. Dacă utilizatorul alege să modifice parola, este arătat ecranul Modificare parolă și este rulat validarea parolei pentru noua parolă.

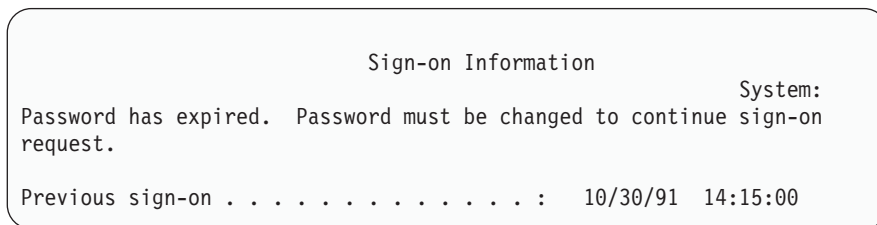


Figura 1. Mesaj de expirare parolă

Tabela 50. Valori posibile pentru PWDEXP:

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

Recomandări: Setati parola la expirată când creați un profil nou de utilizator sau alocați o parolă temporară utilizatorului.

Stare

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

STATUS

Lungime:

10

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

Puteți folosi comanda CHGUSRPRF pentru a activa un profil care a fost dezactivat. Trebuie să aveți autorizarea specială *SECADM și autorizările *OBJMGT și *USE la profil pentru a-i schimba starea. Subiectul “Activarea unui profil de utilizator” la pagina 104 prezintă un exemplu de program cu autorizare adoptată pentru a permite unui operator de sistem să activeze un profil.

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

Puteți întotdeauna să semnați cu profilul QSECOFR (responsabil cu securitatea) la consolă, chiar și când starea QSECOFR este *DISABLED. Dacă profilul de utilizator QSECOFR devine dezactivat, semnați cu QSECOFR la consolă și tastați CHGUSRPRF QSECOFR STATUS(*ENABLED).

Tabela 51. Valori posibile pentru STATUS:

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

Recomandări: Setati starea la *DISABLED dacă doriți să împiedicați semnarea cu un profil de utilizator. De exemplu, puteți dezactiva profilul unui utilizator care nu va lucra o perioadă mai lungă.

Clasă utilizator

Promptul Adăugare utilizator:

Tip de utilizator

Parametru CL:
USRCLS

Lungime:
10

Clasa de utilizator este folosită pentru controlul opțiunilor de meniu care sunt afișate utilizatorului în meniurile i5/OS. Aceasta nu limitează în mod necesar folosirea comenzilor. Câmpul *Limitare capabilități* controlează dacă utilizatorul poate introduce comenzi. Clasa de utilizator nu poate afecta opțiunile care sunt arătate în meniurile furnizate de alte programe licențiate.

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 și valoarea de sistem pentru nivelul de securitate (QSECURITY).

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

Valoarea implicită pentru clasa de utilizator este *USER.

Tabela 52. Autorizările speciale implicite după clasa de utilizator

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

Recomandări: Cei mai mulți utilizatori nu au nevoie să execute funcții de sistem. Setează clasa de utilizator la *USER, exceptând cazul în care pentru un utilizator există necesități specifice de folosire a funcțiilor de sistem.

Nivel de ajutorare

Promptul Adăugare utilizator:
Neafișat

Parametru CL:
ASTLVL

Lungime:
10

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

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

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

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

Tabela 53. Cum sunt memorate și modificate nivelurile de ajutorare

Acțiune executată	Versiunea ecranului arătat	Versiunea ecranului memorat
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nici o modificare (nivelul de asistență de bază)
Din ecranul Gestionare înrolare utilizator, apăsați F12 și selectați Nivelul de asistență intermediar.	Ecranul Gestionare profiluri utilizator	Modificat la Nivelul de asistență intermediar
Folosire comandă WRKUSRPRF	Ecranul Gestionare profiluri utilizator	Nici o modificare (intermediară)
Selectați opțiunea gestionare înrolare utilizator de la meniul SETUP.	Ecranul Gestionare profiluri utilizator	Nici o modificare (intermediară)
Tastați CHGUSRPRF USERA ASTLVL(*BASIC)		Modificat la nivelul de asistență de bază
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nici o modificare (elementară)
Tastare WRKUSRPRF ASTLVL(*INTERMED)	Ecranul Gestionare profiluri utilizator	Nici o modificare (elementară)

Notă: Câmpul *Opțiune utilizator* din profilul utilizator de asemenea afectează afișarea ecranelor de sistem. Acest câmp este descris la pagina 90.

Tabela 54. Valori posibile pentru ASTLVL:

*SYSVAL	Este folosit nivelul de ajutorare specificat în valoarea de sistem QASTLVL.
*BASIC	Este folosită interfața de utilizator Asistent operațional.
*INTERMED	Este folosită interfața de sistem.
*ADVANCED	Este folosită interfața de sistem expert. Pentru a permite mai multe intrări de listă, numerele de opțiune și tastele funcționale nu sunt întotdeauna afișate. Dacă o comandă nu are un nivel avansat (*ADVANCED), este folosit nivelul intermediar (*INTERMED).

Biblioteca curentă

Promptul Adăugare utilizator:

Biblioteca implicită

Parametru CL:

CURLIB

Lungime:

10

Autorizare

*USE

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

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

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

Subiectul “Listele de biblioteci” la pagina 183 furnizează informații suplimentare despre folosirea listelor de biblioteci și a bibliotecii curente.

Tabela 55. Valori posibile pentru CURLIB:

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

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

Program inițial

Promptul Adăugare utilizator:

Program de semnare

Parametru CL:

INLPGM

Lungime:

10 (nume program) 10 (nume bibliotecă)

Autorizare:

*USE pentru program *EXECUTE pentru bibliotecă

Puteți specifica numele unui program pentru a fi apelat când semnează un utilizator. Acest program rulează înainte de a fi afișat meniul inițial, dacă există. Dacă opțiunea din câmpul *Limitare capabilități* din profilul utilizatorului este *YES, utilizatorul nu poate specifica un program inițial pe ecranul Semnare.

Programul inițial este apelat numai dacă programul de rutare al utilizatorului este QCMD sau QCL. Consultați “Pornirea unui job interactiv” la pagina 175 pentru informații suplimentare despre secvența de procesare când semnează un utilizator.

Programele inițiale sunt folosite pentru două scopuri principale:

- Ca să restricționați un utilizator la un set specific de funcții.
- Ca să realizați unele procesări inițiale, cum ar fi deschiderea fișierelor sau stabilirea listei de biblioteci, când utilizatorul semnează prima dată.

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

Tabela 56. Valori posibile pentru INLPGM:

*NONE	Nici un program nu este apelat când utilizatorul semnează. Dacă este specificat un nume de meniu în parametrul de meniu inițial (INLMNU), este afișat acel meniu.
<i>nume-program</i>	Numele programului care este apelat când utilizatorul semnează.

Tabela 57. Valori posibile pentru Biblioteca INLPGM:

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

Meniu inițial

Promptul Adăugare utilizator:

Primul meniu

Parametru CL:

INLMNU

Lungime:

10 (nume meniu) 10 (nume bibliotecă)

Autorizare

*USE pentru meniu *EXECUTE pentru bibliotecă

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

Dacă doriți ca utilizatorul să ruleze numai programul inițial, puteți specifica *SIGNOFF pentru meniul inițial.

Dacă opțiunea din câmpul *Limitare capabilități* din profilul utilizatorului este *YES, utilizatorul nu poate specifica un meniu inițial diferit în ecranul Semnare. Dacă unui utilizator îi este permis să specifice un meniu inițial în ecranul Semnare, meniul specificat înlocuiește meniul din profilul utilizator.

Tabela 58. Valori posibile pentru MENU:

MAIN	Este arătat Meniul principal de sistem iSeries .
*SIGNOFF	Sistemul anulează semnarea utilizatorului când programul inițial se termină. Folosiți aceasta ca să limitați utilizatorii la rularea unui singur program.
<i>nume-meniu</i>	Numele meniului care este apelat când utilizatorul semnează.

Tabela 59. Valori posibile pentru Biblioteca MENU:

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

Limitare capabilități

Promptul Adăugare utilizator:

Restricționare folosire linie de comandă

Parametru CL:

LMTCPB

Lungime:

10

Puteți folosi câmpul *Limitare capabilități* pentru a limita abilitatea utilizatorului de a introduce comenzi și de a înlocui programul inițial, meniul inițial, biblioteca curentă și programul de tratare a tastei de atenționare, specificate în profilul de utilizator. Acest câmp este o unealtă pentru împiedicarea utilizatorilor de a experimenta pe sistem.

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

- Anulare semnare (SIGNOFF)
- Trimitere mesaj (SNDMSG)
- Afișare mesaje (DSPMSG)
- Afișare job (DSPJOB)
- Afișare istoric de job (DSPJOBLOG)
- Pornire Organizator PC (STRPCO)
- Gestionare mesaje (WRKMSG)

Câmpul *Limitare capabilități* din profilul de utilizator și 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 opțiune dintr-un meniu de grupare comandă. Utilizatorii nu au restricții în folosirea următoarelor:

- Rularea comenzilor în programe CL care rulează o comandă ca rezultat al alegerii unei opțiuni dintr-un meniu
- Rularea comenzilor la distanță prin aplicații.

Puteți permite utilizatorului cu capabilitate limitată să ruleze comenzi suplimentare sau să înlăturați câteva comenzi din listă, modificând parametrul ALWLMTUSR într-o comandă. Folosiți comanda Modificare comandă (CHGCMD). Dacă vă creați propriile comenzi, puteți specifica parametrul ALWLMTUSR din comanda Creare comandă (CRTCMD).

Valori posibile: Tabela 60 arată valorile posibile pentru *Limitare capabilități* și ce funcții sunt permise pentru fiecare valoare.

Tabela 60. Funcții permise pentru valorile de limitare capabilități

Funcție	*YES	*PARTIAL	*NO
Modificare program inițial	Nu	Nu	Da
Modificare meniu inițial	Nu	Da	Da
Modificare bibliotecă curentă	Nu	Nu	Da
Modificare program Attn	Nu	Nu	Da
Introducere comenzi	Câteva ¹	Da	Da

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

Recomandări: Folosirea un meniu inițial, restricționarea utilizării liniei de comandă și furnizarea de acces la meniu vă permit să setați un mediu pentru un utilizator care nu are nevoie sau nu dorește să acceseze funcții de sistem. Consultați subiectul “Planificarea meniurilor” la pagina 203 pentru informații suplimentare despre acest tip de mediu.

Text

Promptul Adăugare utilizator:

Descriere utilizator

Parametru CL:

TEXT

Lungime:

50

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

Tabela 61. Valori posibile pentru text:

*BLANK:	Nu este specificat nici un text.
<i>descriere</i>	Specificați cel mult 50 de caractere.

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

Autorizare specială

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

SPCAUT

Lungime:

100 (10 caractere pentru autorizare specială)

Autorizare:

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

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

Tabela 62. Valori posibile pentru SPCAUT:

*USRCLS	Autorizările speciale sunt acordate acestui utilizator pe baza câmpului de clasă utilizator (USRCLS) din profilul de utilizator și a valorii de sistem pentru nivelul de securitate (QSECURITY). Dacă se specifică *USRCLS, nici o autorizare specială adițională nu poate fi specificată pentru acest utilizator.
----------------	--

Dacă specificați *USRCLS când creați sau modificați un profil de utilizator, sistemul pune autorizările speciale corecte în profilul de utilizator, ca și cum le-ați fi introdus dumneavoastră. Când afișați profilurile, nu puteți preciza dacă autorizările speciale au fost introduse individual sau au fost introduse de sistem pe baza clasei de utilizator.

*NONE

nume-autorizare-specială

Tabela 52 la pagina 63 arată autorizările speciale implicite pentru fiecare clasă de utilizator. Nu este acordată nici o autorizare specială pentru acest utilizator. Specificați una sau mai multe autorizări speciale pentru utilizator. Autorizările speciale sunt descrise în secțiunile care urmează.

Autorizarea specială *ALLOBJ

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

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

Un utilizator cu autorizarea *ALLOBJ nu poate realiza direct operații 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. Totuși, un utilizator cu autorizarea specială *ALLOBJ poate lansa un job batch folosind un profil care are autorizarea specială necesară. În esență, acordarea autorizării speciale *ALLOBJ dă utilizatorului acces la toate funcțiile din sistem.

Autorizarea specială *SECADM

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

- Să adauge utilizatori la directorul de distribuire sistem.
- Să afișeze autorizarea pentru documente sau foldere.
- Să adauge și să înlătore coduri de acces la sistem.
- Să dea și să înlătore autorizarea unui utilizator pentru cod de acces '.
- Să dea și să înlătore permisiunea pentru utilizatori ca să lucreze în numele altor utilizatori '.
- Să șteargă documente și foldere.
- Să șteargă liste de documente.
- Să modifice liste de distribuție create de alți utilizatori.

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

Autorizarea specială *JOBCTL

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

- Modifice, șteargă, rețină și elibereze toate fișierele din orice coadă de ieșire specificată ca OPRCTL(*YES).
- Afișeze, trimită și copieze toate fișierele din orice coadă de ieșire specificată ca DSPDTA(*YES sau *NO) și OPRCTL(*YES).
- Rețină, elibereze și șteargă cozi de joburi specificate ca OPRCTL(*YES).
- Rețină, elibereze și șteargă cozi de ieșire specificate ca OPRCTL(*YES).
- Rețină, elibereze, modifice și anuleze joburile altor utilizatori.
- Pornească, modifice, oprească, reține și elibereze scriitori, dacă coada de ieșire 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 inițial (IPL).

Securizarea ieșirii de imprimantă și a cozilor de ieșire este discutată în “Tipărirea” la pagina 186.

Puteți modifica prioritatea de job (JOBPTY) și prioritatea de ieșire (OUTPTY) a jobului dumneavoastră fără autorizarea specială control de job. Trebuie să aveți autorizarea specială *JOBCTL pentru a modifica prioritatea de rulare (RUNPTY) a jobului dumneavoastră.

Modificările priorității de ieșire și a priorității de job a unui job sunt limitate de limita de prioritate (PTYLMT) din profilul utilizatorului care face modificările.

Riscuri: Un utilizator cu autorizarea specială *JOBCTL poate modifica prioritatea joburilor și a tipării, poate opri un job înainte de a se termina sau poate șterge ieșirea înainte de a fi tipărită. Autorizarea specială *JOBCTL poate de asemenea acorda acces unui utilizator la ieșiri spool confidențiale, dacă cozile de ieșire sunt specificate OPRCTL(*YES). Un utilizator care abuzează de autorizarea specială *JOBCTL poate cauza un impact negativ asupra joburilor individuale și asupra performanței generale a sistemului.

Autorizarea specială *SPLCTL

Autorizarea specială control spool (*SPLCTL) permite utilizatorului să realizeze toate funcțiile de control spool, precum modificarea, ștergerea, afișarea, reținerea și eliberarea de fișiere spool. Utilizatorul poate realiza aceste funcții în toate cozile de ieșire, indiferent de autorizările pentru coada de ieșire sau parametrul OPRCTL al cozii de ieșire.

De asemenea, autorizarea specială *SPLCTL permite utilizatorului să gestioneze cozi de joburi, inclusiv să rețină, să elibereze și să șteargă coada de joburi. Utilizatorul poate realiza aceste funcții 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 operații pe orice fișier spool din sistem. Fișierele spool confidențiale nu pot fi protejate de un utilizator cu autorizarea specială *SPLCTL.

Autorizarea specială *SAVSYS

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

Riscuri: Un utilizator cu autorizare specială *SAVSYS poate:

- Să salveze un obiect și să-l ducă pe un alt sistem iSeries pentru a fi restaurat.
- Să salveze un obiect și să afișeze banda pentru a vedea datele.
- Să salveze un obiect și să elibereze spațiu, astfel ștergând porțiuni din datele obiectului.
- Să salveze un document și să-l șteargă.

Autorizarea specială *SERVICE

Autorizarea specială service (*SERVICE) permite utilizatorului să pornească unelte de service sistem folosind comanda STRSST. Permite utilizatorului și depanarea unui program doar cu autorizarea *USE și realizarea funcțiilor de afișare și modificare serviciu. Funcția dump poate fi realizată fără autorizare *SERVICE. Permite utilizatorului și realizarea de diferite funcții de urmărire.

Riscuri: Un utilizator cu autorizarea specială *SERVICE poate afișa și modifica informații confidențiale folosind funcțiile de service. Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ pentru a modifica informațiile folosind funcții de service.

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

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

Tabela 63.

STRCMNTRC	Pornire urmărire comunicații
ENDCMNTRC	Oprire urmărire comunicații
PRTCMNTRC	Tipărire urmărire comunicații
DLTCMNTRC	Ștergere urmărire comunicații
CHKCMNTRC	Verificare urmărire comunicații
TRCCNN	Conexiune de urmărire (consultați "Acordarea accesului la urmăritori" la pagina 71)
TRCINT	Urmărire internă
STRTRC	Pornire job de urmărire
ENDTRC	Oprire job de urmărire
PRTRC	Tipărire job de urmărire
DLTRC	Ștergere job de urmărire
I TRCTCPAPP	Urmărire aplicație TCP/IP (Trace TCP/IP Application)
I WRKTRC	Gestionarea urmăririlor (Work with Traces)

| **Notă:** Aveți nevoie de *ALLOBJ pentru a fi capabil de modificare a datelor folosind funcții de service.

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

1. În Navigator iSeries, deschideți Utilizatori și grupuri.
2. Selectați Toți utilizatorii pentru a vedea o listă a profilurilor de utilizator.
3. Faceți clic dreapta pe profilul de utilizator de transformat.
4. Selectați Proprietăți.
5. Faceți clic pe Capabilități.
6. Deschideți fișa Aplicații.
7. Selectați Acces pentru.
8. Selectați Aplicații gazdă.
9. Selectați Sistem de operare.
10. Selectați Service.
11. Folosiți caseta de bifare ca să acordați sau să înlăturați accesul la comanda de urmărire.

| Alternativ, comanda Change Function Usage (CHGFCNUSG) poate fi folosită pentru a acorda acces utilizatorilor la comenzile de urmărire. Introduceți CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(profil utilizator) USAGE(*ALLOWED).

Autorizarea specială *AUDIT

Autorizarea specială de auditare (*AUDIT) oferă utilizatorului posibilitatea să vizualizeze și să modifice caracteristicilor de auditare. Utilizatorul poate:

- Să modifice valorile de sistem care controlează auditarea.
- Să utilizeze comenzile CHGOBJAUT, CHGDLOAUD și CHGAUD ca să modifice auditarea pentru obiecte.
- Să utilizeze comanda CHGUSRAUD ca să modifice auditarea pentru un utilizator.
- | • Să afișeze valorile de auditare ale unui obiect.
- | • Să afișeze valorile de auditare ale unui profil de utilizator.
- | • Să execute unele dintre comenzile pentru unelte de securitate (de exemplu PRTADPOBJ).

Riscuri: Un utilizator cu utilizare specială *AUDIT poate opri și porni auditarea pe sistem sau poate împiedica auditarea acțiunilor particulare. Dacă aveți o înregistrare de auditare a evenimentelor relevante de securitate este important pentru sistemul dumneavoastră să controlați cu atenție și să monitorizați folosirea autorizării speciale *AUDIT.

| Dacă este important ca informația de auditare să nu fie vizibilă de către utilizatorii generali, aplicați acțiuni suplimentare pentru a restricționa utilizatorii generali de a vizualiza următoarele informații:

- | • Jurnal auditare de securitate (QAUDJRN)
- | • Alte jurnale care conțin date de auditare
- | • Fișiere de salvare, fișiere de ieșire, fișiere spool și tipărituri care conțin informația de auditare

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

Autorizarea specială *IOSYSCFG

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

Recomandări pentru Autorizări speciale: Acordarea autorizărilor speciale pentru utilizatori reprezintă o expunere de securitate. Pentru fiecare utilizator, evaluați cu atenție nevoile pentru orice autorizare specială. Urmăriți îndeaproape care utilizatori au autorizări speciale și revedeți în mod periodic cerințele lor pentru autorizări.

În plus, ar trebui să controlați următoarele situații pentru profilurile utilizator și programe:

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

Programele adoptă autorizarea specială *ALLOBJ a deținătorului 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

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

SPCENV

Lungime:

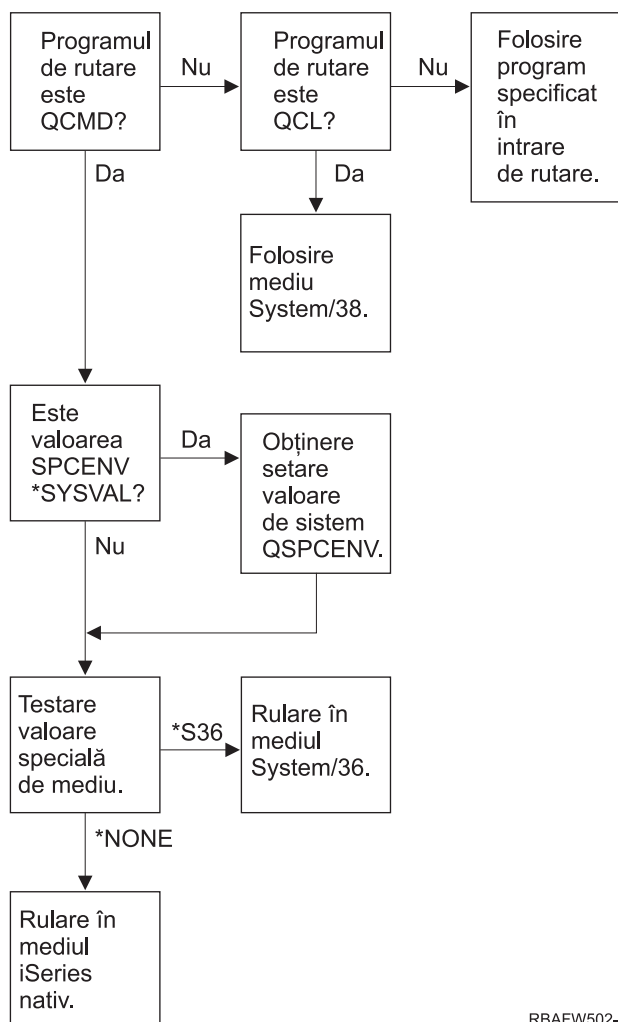
10

Mediul special determină mediul operării utilizatorului după semnare. Utilizatorul poate opera în mediul iSeries, System/36 sau System/38. Când utilizatorul semnează, sistemul folosește programul de rutare și mediul special din profilul utilizatorului pentru a determina mediul utilizatorului. Consultați Figura 2 la pagina 73.

Tabela 64. Valori posibile pentru SPCENV:

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

Recomandări: Dacă utilizatorul rulează o combinație de aplicații iSeries și System/36, folosiți comanda Pornire System/36 (STRS36) înaintea rulării aplicațiilor System/36 mai repede decât specificarea mediului System/36 în profilul utilizator. Aceasta furnizează performanță mai bună pentru aplicații iSeries .



RBAFW502-1

Figura 2. Descriere mediu special

Descriere mediu 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 folosește 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 și testează valoarea de mediu special. Dacă valoarea de sistem SPCENV nu este setată, atunci sistemul testează valoarea de mediu special.

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

Ecranul Informații semnare

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

DSPSGNINF

Lungime:

7

Câmpul *Afișare informații semnare* specifică dacă ecranul Informații semnare este arătat când utilizatorul semnează. Figura 3 arată ecranul. Informațiile de expirare parolă sunt afișate numai dacă parola expiră în șapte zile.

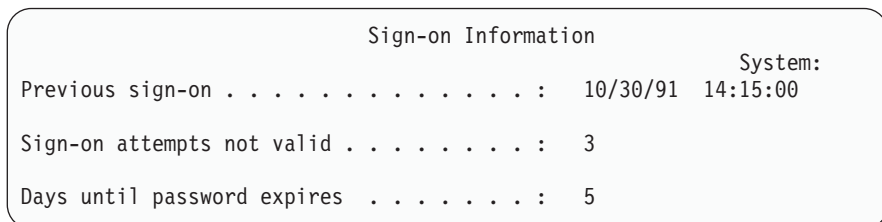


Figura 3. Ecranul Informații semnare

Tabela 65. Valori posibile pentru DSPSGNINF:

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

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

Interval de expirare parolă

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

PWDEXPITV

Lungime:

5,0

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

Când parola unui utilizator a expirat, utilizatorul primește un mesaj la semnare. Utilizatorul poate apăsa tasta Enter pentru a alocă o nouă parolă sau poate apăsa F3 (Ieșire) pentru a anula încercarea de semnare fără alocarea unei noi parole. Dacă utilizatorul alege să modifice parola, este arătat ecranul Modificare parolă și este rulat validarea parolei pline pentru noua parolă. Figura 1 la pagina 62 arată un exemplu de mesaj de expirare parolă.

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

Tabela 66. Valori posibile pentru PWDEXPITV:

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

Recomandări: Setati valoarea de sistem QPWDEXPTV pentru un interval corespunzător, cum ar fi 60 până la 90 de zile. Folosiți câmpul *Interval de expirare parolă* din profilul utilizator pentru utilizatorii individuali care ar trebui să-și modifice parolele mai frecvent, cum ar fi administratorii de securitate.

Gestiunea parolei locale

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

LCLPWDMGT

Lungime:

10

Câmpul de parametru Gestionare locală parolă specifică dacă parola profilului de utilizator trebuie să fie gestionată local. Dacă parola este gestionată local, atunci parola este memorată local cu profilul utilizator. Aceasta este metoda tradițională de memorare a parolei.

Dacă parola nu este gestionată local, atunci parola locală i5/OS este setată la *NONE. Valoarea specificată în parametrul de parolă va fi trimisă la alte produse IBM care fac sincronizare de parolă, cum ar fi serverul IBM iSeries Integration for Windows. Utilizatorul nu-și va putea modifica parola folosind comanda Modificare parolă (CHGPWD). În plus, el nu va putea semna direct pe sistem. Specificarea acestei valori va afecta alte produse IBM care fac sincronizare de parolă, cum ar fi serverul IBM Integration for Windows. Consultați-vă documentația de produs pentru detalii.

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

Tabela 67. Valori posibile pentru LCLPWDMGT:

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

Limitare sesiuni dispozitiv

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

LMTDEVSSN

Lungime:

7

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

Tabela 68. Valori posibile pentru LMTDEVSSN:

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

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

Punere în buffer tastatură

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

KBDBUF

Lungime:

10

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

Câmpul de punere în buffer tastatură controlează două funcții:

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 informațiilor la sistem chiar dacă altă intrare de la stația de lucru este inhibată.

Tabela 69. Valori posibile pentru KBDBUF:

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

Spațiu de stocare maxim

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

MAXSTG

Lungime:

11,0

Puteți specifica dimensiunea maximă a spațiului de stocare auxiliar care este utilizat la stocarea obiectelor permanente care sunt deținute de un profil utilizator, inclusiv obiecte plasate în biblioteca temporară (QTEMP) în timpul unui job. Spațiul maxim este specificat în kiloocteți (1024 octeți).

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

Valoarea maximă de spațiu 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 și 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 planificați memoria maximă pentru profilurile de utilizator, luați în considerare următoarele funcții de sistem, care pot afecta memoria maximă cerută de un utilizator:

- O operație de restaurare întâi alocă memoria utilizatorului care efectuează operația de restaurare și apoi transferă obiectele la OWNER. Utilizatorii care efectuează operații de restaurare mari ar trebui să aibă MAXSTG(*NOMAX) în profilurile lor de utilizatori.
- Profilul utilizator care deține un receptor jurnal este alocat memoriei pe măsură ce dimensiunea receptorului crește. Dacă sunt create noi receptoare, spațiul continuă să fie alocat profilului utilizator care deține receptorul de jurnal activ. Utilizatorii care dețin receptoare de jurnal active ar trebui să aibă MAXSTG(*NOMAX) în profilurile lor de utilizatori.
- Dacă un profil utilizator specifică OWNER(*GRPPRF), dreptul de proprietate al oricărui obiect creat de utilizator este transferat la profilul de grup după crearea obiectului. Totuși, utilizatorul care creează obiectul trebuie să aibă spațiu de stocare adecvat pentru a conține orice obiecte create anterior transferării dreptului de proprietate asupra obiectului la profilul de grup.
- Proprietarul unei biblioteci este alocat spațiului de stocare pentru descrierile obiectelor plasate în bibliotecă, chiar dacă obiectele sunt deținute de alt profil utilizator. Exemple ale unor asemenea descrieri sunt referințele text și de program.
- Spațiu de stocare este alocat profilului utilizator pentru obiecte temporare care sunt folosite în timpul procesării unui job. Exemple ale unor asemenea obiecte sunt blocurile de control comitere, spațiile de editare fișier și documentele.

Tabela 70. Valori posibile pentru MAXSTG:

*NOMAX	Poate fi alocat atâta spațiu cât este necesar acestui profil.
<i>maxim KB</i>	Specificați dimensiunea maximă de spațiu în kiloocteți (1 kilooctet are 1024 octeți) care poate fi alocată acestui profil utilizator.

Limită de prioritate

Prompt adăugare utilizator:

Neafișat

Parametru CL:

PTYLMT

Lungime:

1

Un job batch are trei valori de prioritate diferite:

Rulare prioritate:

Determină cum concurează jobul pentru resursele mașinii când rulează. Prioritatea de rulare este determinată de clasa jobului.

Prioritate job:

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

Prioritate ieșire:

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

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

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

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

Tabela 71. Valori posibile pentru PTYLMT:

<u>3</u>	Limita de prioritate implicită pentru profiluri utilizator este 3. Prioritatea implicită pentru prioritatea de job și cea de ieșire pe descrieri de job este 5. Setarea limitei de prioritate pentru profilul utilizator la 3 dă utilizatorului abilitatea de a muta unele joburi înaintea altora în cozi.
<i>limită de prioritate</i>	Specificați 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 și 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.

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

Descriere de job

Prompt adăugare utilizator:

Neafișat

Parametru CL:

JOBID

Lungime

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

Autorizare:

*USE pentru descriere de job, *READ și *EXECUTE pentru bibliotecă

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

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

O descriere de job conține un set specific de atribute legate de job, precum cozile de joburi pe care să le folosească, prioritatea de planificare, datele de rutare, gravitatea cozii de mesaje, lista de biblioteci și informațiile de ieșire. Atributele determină cum este rulat fiecare job în sistem.

Vedeți cartea *Work Management* pentru informații suplimentare despre descrierile de job și utilizările lor.

Tabela 72. Valori posibile pentru JOBID:

QDFTJOBID

Este folosită descrierea de job furnizată de sistem, găsită în biblioteca QGPL. Puteți folosi comanda Afișare descriere job (DSPJOBID) pentru a vedea atributele conținute în această descriere de job.

nume descriere de job

Specificați numele descrierii de job, 10 caractere sau mai puțin.

Tabela 73. Valori posibile pentru Biblioteca JOBD:

*LIBL	Este folosită lista de biblioteci pentru localizarea descrierii de job.
*CURLIB	Pentru localizarea descrierii de job este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se folosește QGPL.
<i>nume-biblioteca</i>	Specificați biblioteca unde este localizată descrierea de job, 10 caractere sau mai puțin.

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

Profil de grup

Prompt adăugare utilizator:

Profil grup

Parametru CL:

GRPPRF

Lungime:

10

Autorizare:

Pentru specificarea unui grup când creați sau modificați un profil de utilizator, trebuie să aveți autorizarea *OBJMGT, *OBJOPR, *READ, *ADD, *UPD și *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, consultați “Obiecte care adoptă autorizarea proprietarului” la pagina 128.

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

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

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

| Când este modificată valoarea GRPPRF, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau
| următoarea dată când un job face swap profilului utilizatorului folosind un manipulator sau jeton de profil care a fost
| obținut după ce a avut loc modificarea.

Consultați “Planificarea profilurilor de grup” la pagina 213 pentru informații suplimentare despre folosirea profilurilor de grup.

Tabela 74. Valori posibile pentru GRPPRF:

*NONE	Nici un profil de grup nu este folosit cu acest profil de utilizator.
<i>nume profil utilizator</i>	Specificați numele unui profil de grup în care acest profil de utilizator este membru.

Proprietar

Prompt adăugare utilizator:

Neafișat

Parametru CL:
OWNER

Lungime:
10

Dacă un utilizator este membrul unui grup, folosiți parametrul *proprietar* din profilul de utilizator ca să specificați cine deține obiectele nou create de utilizator. Obiectele pot fi deținute fie de utilizator, fie de primul grup al utilizatorului (valoarea parametrului GRPPRF). Puteți să specificați câmpul *OWNER* numai dacă ați specificat câmpul *Profil de grup*.

| Când este modificată valoarea OWNER, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau
| următoarea dată când un job face swap profilului utilizatorului folosind un manipulator sau jeton de profil care a fost
| obținut după ce a avut loc modificarea.

Tabela 75. Valori posibile pentru OWNER:

***USRPRF**

Acest profil de utilizator este OWNER pentru orice obiect nou pe care îl creează.

***GRPPRF**

Profilul de grup este făcut OWNER pentru toate obiectele create de utilizator și îi este dată autorizarea *ALL pentru obiecte. Profilului de utilizator nu îi este dată nici o autorizare specifică pentru noile obiecte create. Dacă este specificat *GRPPRF, trebuie să specificați un nume de profil de grup în parametrul GRPPRF și parametrul GRPAUT trebuie să fie *NONE.

Note:

1. Dacă dați drept de proprietate grupului, toți membrii acelui grup pot modifica, înlocui și șterge obiectul.
2. Parametrul *GRPPRF este ignorat pentru toate sistemele de fișiere cu excepția QSYS.LIB. În cazurile în care parametrul este ignorat, utilizatorul păstrează dreptul de proprietate asupra obiectului.

Autorizare de grup

Prompt adăugare utilizator:
Neafișat

Parametru CL:
GRPAUT

Lungime:
10

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

Autorizarea de grup poate fi specificată numai când GRPPRF nu este *NONE și 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 este modificată valoarea GRPAUT, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau
| următoarea dată când un job face swap profilului utilizatorului folosind un manipulator sau jeton de profil care a fost
| obținut după ce a avut loc modificarea.

Tabela 76. Valori posibile pentru GRPAUT:

*NONE	Nici o autorizare specifică nu este dată profilului de grup când utilizatorul creează obiecte.
*ALL	Profilului de grup îi sunt date toate autorizările de gestionare și 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.

Consultați “Definirea modului în care pot fi accesate informațiile” la pagina 112 pentru o explicație completă a autorizărilor care pot fi acordate.

Tip autorizare de grup

Prompt adăugare utilizator:

Neafișat

Parametru CL:

GRPAUTTYP

Lungime:

10

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

- | Când este modificată valoarea GRPAUTTYP, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau următoarea dată când un job face swap profilului utilizatorului folosind un manipulator sau jeton de profil care a fost obținut după ce a avut loc modificarea.

Tabela 77. Valori posibile pentru GRPAUTTYP: ¹

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

- | ¹ Autorizarea privată și autorizarea de grup primar furnizează același acces obiectului pentru membrii grupului, dar ele au caracteristici de performanță diferite. “Grupul primar pentru un obiect” la pagina 123 explică cum lucrează autorizarea de grup primar.

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

Grupuri suplimentare

Prompt adăugare utilizator:

Neafișat

Parametru CL:

SUPGRPPRF

Lungime:

150

Autorizare:

Pentru specificarea grupurilor suplimentare atunci când creați sau modificați un profil de utilizator, trebuie să aveți autorizarea *OBJMGT, *OBJOPR, *READ, *ADD, *UPD și *DLT la fiecare profil.

Notă: Autorizarea *OBJMGT nu poate veni de la autorizarea adoptată. Pentru detalii suplimentare, consultați “Obiecte care adoptă autorizarea proprietarului” la pagina 128.

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

Când profilurile de grup suplimentare sunt specificate într-un profil utilizator, utilizatorului îi sunt acordate în mod automat autorizările *OBJMGT, *OBJOPR, *READ, *ADD, *UPD și *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 funcțiile sistemului și nu trebuie înlăturate. Dacă un profil specificat în parametrul SUPGRPPRF nu este deja un profil de grup, sistemul setează informații în semnarea profilului ca și un profil de grup. De asemenea sistemul generează un gid pentru profilul de grup, dacă deja nu are unul.

! Când este modificată valoarea SUPGRPPRF, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau următoarea dată când un job face swap profilului utilizatorului folosind un manipulator sau jeton de profil care a fost obținut după ce a avut loc modificarea.

Consultați “Planificarea profilurilor de grup” la pagina 213 pentru informații suplimentare despre folosirea profilurilor de grup.

Tabela 78. Valori posibile pentru SUPGRPPRF

***NONE**

nume profil de grup

Nici un grup suplimentar nu este folosit cu acest profil utilizator.

Specificați până la 15 nume de profiluri de grup pentru a fi folosite cu acest profil de utilizator. Aceste profiluri, în plus față 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

Prompt adăugare utilizator:

Neafișat

Parametru CL:

ACGCDE

Lungime:

15

Contabilizarea jobului este o funcție opțională folosită la adunarea de informații 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 și când un job rulează, folosind comanda Modificare cod de contabilizare (CHGACGCDE).

Vedeți cartea *Work Management* pentru informații suplimentare despre contabilizarea de job.

Tabela 79. Valori posibile pentru ACGCDE:

***BLANK**

cod de contabilizare

Un cod de contabilizare de 15 spații este alocat acestui profil utilizator.

Specificați un cod de contabilizare de 15 caractere. Dacă sunt specificate mai puțin de 15 caractere, șirul este completat cu spații în partea dreaptă.

Parolă document

Prompt adăugare utilizator:

Neafișat

Parametru CL:

DOCPWD

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

Tabela 80. Valori posibile pentru DOCPWD:

***NONE**

parolă document

Nici o parolă de document nu este folosită de acest utilizator.

Specificați o parolă document pentru acest utilizator. Parola trebuie să aibă 1-8 caractere (litere de la A la Z și numere de la 0 la 9). Primul caracter al parolei de document trebuie să fie alfabetic; restul caracterelor pot fi alfanumerice. Nu sunt permise spații incluse, spații la început și caractere speciale.

Coadă de mesaje

Prompt adăugare utilizator:

Neafișat

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.

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

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

Tabela 81. Valori posibile pentru MSGQ:

***USRPRF**

nume coadă de mesaje

O coadă de mesaje cu același nume cu numele de profil utilizator este folosită ca și coadă de mesaje pentru acest utilizator. Dacă coada de mesaje nu există, ea este creată în biblioteca QUSRSYS.

Specificați numele cozii de mesaje care este folosit pentru acest utilizator. Dacă specificați un nume de coadă de mesaje, trebuie să specificați și parametrul de bibliotecă.

Tabela 82. Valori posibile pentru Biblioteca MSGQ:

***LIBL**

***CURLIB**

nume-bibliotecă

Lista de biblioteci este folosită pentru localizarea cozii de mesaje. Dacă coada de mesaje nu există, nu puteți specifica *LIBL.

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 folosește QGPL. Dacă nu există coada de mesaje, este creată în biblioteca curentă sau în QGPL.

Specificați biblioteca în care este localizată coada de mesaje. Dacă nu există coada de mesaje, este creată în această bibliotecă.

Recomandări: Când un utilizator semnează, coada de mesaje din profilul de utilizator este alocată aceluși job utilizator. În cazul în care coada de mesaje este deja alocată altui job, utilizatorul primește un mesaj de avertizare în timpul semnării. Pentru a evita aceasta, dați fiecărui utilizator o coadă de mesaje unică, de preferat cu același nume ca profilul de utilizator.

Livrare

Prompt adăugare utilizator:

Neafișat

Parametru CL:

DLVRY

Lungime:

10

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

Tabela 83. Valori posibile pentru DLVRY:

***NOTIFY**

Jobul la care este alocată coada de mesaje este anunțat când ajunge un mesaj la coada de mesaje. Pentru joburi interactive la o stație de lucru, alarma sonoră este pornită și este aprinsă lumina de așteptare mesaj. Tipul de livrare nu poate fi modificat în *NOTIFY dacă coada de mesaje este folosită și de un alt utilizator.

***BREAK**

Jobul la care este alocată coada de mesaje este întrerupt când ajunge un mesaj la coada de mesaje. Dacă jobul este interactiv, este sunată alarma sonoră (dacă alarma este instalată). Tipul de livrare nu poate fi modificat în *BREAK dacă coada de mesaje este folosită și de un alt utilizator.

***HOLD**

Mesajele sunt ținute în coada de mesaje până când sunt cerute de utilizator sau de program.

***DFT**

Mesajelor care necesită răspunsuri li se răspunde cu răspunsul implicit; mesajele care au doar caracter informativ sunt ignorate.

Gravitate

Prompt adăugare utilizator:

Neafișat

Parametru CL:

SEV

Lungime:

2,0

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

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

Tabela 84. Valori posibile pentru SEV:

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

Dispozitiv de tipărire

Prompt adăugare utilizator:

Imprimantă implicită

Parametru CL:

PRTDEV

Lungime:

10

Puteți specifica imprimanta folosită la tipărirea ieșirii pentru acest utilizator. Fișierele spool sunt plasate într-o coadă de ieșire cu același nume ca și imprimanta când coada de ieșire (OUTQ) este specificată ca dispozitiv de tipărire (*DEV).

Sunt folosite informațiile din profilul de utilizator pentru dispozitivul de tipărire și coada de ieșire numai dacă fișierul de imprimantă specifică *JOB și descrierea de job specifică *USRPRF. Pentru informații suplimentare despre directarea ieșirii imprimantă, vedeți cartea *Printer Device Programming*.

Tabela 85. Valori posibile pentru PRTDEV:

*WRKSTN	Este folosită imprimanta alocată stației de lucru a utilizatorului (în descrierea dispozitiv).
*SYSVAL	Este folosită imprimanta de sistem implicită în valoarea de sistem QPRTDEV.
<i>nume dispozitiv de tipărire</i>	Specificați numele imprimantei folosite la tipărirea ieșirii pentru acest utilizator.

Coadă de ieșire

Prompt adăugare utilizator:

Neafișat

Parametru CL:

OUTQ

Lungime:

10 (nume coadă de ieșire) 10 (nume bibliotecă)

Autorizare:

*USE pentru coadă de ieșire *EXECUTE pentru bibliotecă

Atât procesările interactive, cât și cele batch pot avea ca rezultat fișiere spool care sunt trimise la imprimantă. Fișierele spool sunt plasate într-o coadă de ieșire. Sistemul poate avea mai multe cozi de ieșire diferite. O coadă de ieșire nu trebuie neapărat să fie atașată la o imprimantă pentru a primi fișiere spool noi.

Sunt folosite informațiile din profilul de utilizator pentru dispozitivul de tipărire și coada de ieșire numai dacă fișierul de imprimantă specifică *JOB și descrierea de job specifică *USRPRF. Pentru informații suplimentare despre directarea ieșirii imprimantă, vedeți cartea *Printer Device Programming*.

Tabela 86. Valori posibile pentru OUTQ:

*WRKSTN	Este folosită coada de ieșire alocată stației de lucru a utilizatorului (în descrierea dispozitiv).
*DEV	Este folosită o coadă de ieșire cu același nume ca și dispozitivul de tipărire specificat în parametrul PRTDEV.
<i>nume coadă de ieșire</i>	Specificați numele cozii de ieșire care va fi folosită. Coada de ieșire trebuie să existe deja. Dacă este specificată o coadă de ieșire, trebuie să fie specificată și biblioteca.

Tabela 87. Valori posibile pentru biblioteca OUTQ:

*LIBL	Este folosită lista de biblioteci pentru localizarea cozii de ieșire.
*CURLIB	Pentru localizarea cozii de ieșire este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se folosește QGPL.
<i>nume-bibliotecă</i>	Specificați biblioteca în care se află coada de ieșire.

Program de tratare tastă Attn

Prompt adăugare utilizator:

Neafișat

Parametru CL:

ATNPGM

Lungime:

10 (nume program) 10 (nume bibliotecă)

Autorizare:

*USE pentru program

*EXECUTE pentru bibliotecă

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

ATNPGM este activat numai dacă programul de rutare al utilizatorului este QCMD. ATNPGM este activat înainte de apelarea programului inițial. Dacă programul inițial modifică ATNPGM, noul ATNPGM rămâne activ doar până când programul inițial se termină. Dacă se rulează comanda Setare program tratare tastă Atenție (SETATNPGM) dintr-o linie de comandă sau dintr-o aplicație, noul ATNPGM specificat înlocuiește ATNPGM din profilul de utilizator.

Notă: Consultați “Pornirea unui job interactiv” la pagina 175 pentru informații suplimentare despre secvența de procesare când semnează un utilizator.

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

Tabela 88. Valori posibile pentru ATNPGM:

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

Tabela 89. Valori posibile pentru Biblioteca ATNPGM:

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

Secvență de sortare

Prompt adăugare utilizator:

Neafișat

Parametru CL:

SRTSEQ

Lungime:

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

Autorizare:

*USE pentru tabelă *EXECUTE pentru bibliotecă

Puteți specifica secvența de sortare folosită pentru ieșirea utilizatorului. Puteți să folosiți tabela de sortare furnizată de sistem sau să vă creați una proprie. O tabelă de sortare poate fi asociată cu un identificator de limbă particular de pe sistem.

Tabela 90. Valori posibile pentru SRTSEQ:

*SYSVAL	Este folosită valoarea de sistem QSRTSEQ.
*HEX	Pentru utilizator este folosită secvența de sortare hexazecimală standard.
*LANGIDSHR	Este folosită tabela secvență de sortare asociată cu identificatorul de limbă al utilizatorului. Tabela poate conține aceeași pondere pentru mai multe caractere.
*LANGIDUNQ	Este folosită tabela secvență de sortare asociată cu identificatorul de limbă al utilizatorului. Tabela trebuie să conțină o pondere unică pentru fiecare caracter din pagina de cod.
<i>nume tabel</i>	Specificați numele tabelii secvență de sortare pentru acest utilizator.

Tabela 91. Valori posibile pentru Biblioteca SRTSEQ:

*LIBL	Este folosită lista de biblioteci pentru localizarea tabelii specificate pentru valoarea SRTSEQ.
*CURLIB	Pentru localizarea tabelii specificate pentru valoarea SRTSEQ este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se folosește QGPL.
<i>nume-bibliotecă</i>	Specificați bibliotecă în care se află tabela secvență de sortare.

Identificator de limbă

Prompt adăugare utilizator:

Neafișat

Parametru CL:

LANGID

Lungime:

10

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

Tabela 92. Valori posibile pentru LANGID:

*SYSVAL:	Este folosită valoarea de sistem QLANGID pentru determinarea identificatorului de limbă.
<i>identificator de limbă</i>	Specificați un identificator de limbă pentru acest utilizator.

Identificator de regiune sau țară

Prompt adăugare utilizator:

Neafișat

Parametru CL:

CNTRYID

Lungime:

10

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

Tabela 93. Valori posibile pentru CNTRYID:

<u>*SYSVAL</u>	Este folosită valoarea de sistem QCNTRYID pentru determinarea identificatorului de regiune sau țară.
<i>identificator de regiune sau țară</i>	Specificați identificatorul de regiune sau țară pentru acest utilizator.

Identificator set de caractere codate

Prompt adăugare utilizator:

Neafișat

Parametru CL:

CCSID

Lungime:

5,0

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

Tabela 94. Valori posibile pentru CCSID:

<u>*SYSVAL</u>	Este folosită valoarea de sistem QCCSID pentru determinarea identificatorului de set de caractere codate.
<i>identificator-set-caractere-codate</i>	Specificați identificatorul de set de caractere codate pentru acest utilizator.

Control identificator de caracter

Prompt adăugare utilizator:

Neafișat

Parametru CL:

CHRIDCTL

Lungime:

10

Atributele *CHRIDCTL* controlează tipul de conversie a setului de caractere codate care apare pentru fișierele de afișare, fișierele de imprimantă și grupurile de panouri. Informațiile 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 fișierele de afișare, fișierele de imprimantă și grupurile de panouri.

Tabela 95. Valori posibile pentru CHRIDCTL:

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

Atribute de job

Prompt adăugare utilizator:

Neafișat

Parametru CL:

SETJOBATR

Lungime:

160

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

Tabela 96. Valori posibile pentru SETJOBATR:

*SYSVAL	Este folosită valoarea de sistem QSETJOBATR ca să se determine ce atribute de job urmează să fie luate din Locale.
*NONE	Nici un atribut de job nu va fi luat din Locale.
*CCSID	Orice combinație a următoarelor valori poate fi specificată: 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 secvența de sortare din Locale. Secvența de sortare din Locale va înlocui secvența de sortare din profilul de utilizator.
*TIMSEP	Este folosit separatorul de timp din Locale.

Locale

Prompt adăugare utilizator:

Neafișat

Parametru CL:

LOCALE

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

Tabela 97. Valori posibile pentru LOCALE:

*SYSVAL	Este folosită valoarea de sistem QLOCALE este folosită pentru determinarea numelui de cale Locale spre a fi alocat pentru acest utilizator.
*NONE	Nici un Locale nu este alocat pentru acest utilizator.
*C	Utilizatorului ii este alocat Locale C.
*POSIX	Utilizatorului ii este alocat Locale POSIX.
<i>nume cale locale</i>	Utilizatorului ii este alocat numele de cale Locale specificat.

Opțiuni utilizator

Prompt adăugare utilizator:

Neafișat

Parametru CL:

USROPT

Lungime:

240 (10 caractere fiecare)

Câmpul *Opțiuni utilizator* vă permite să personalizați anumite ecrane de sistem și funcții pentru utilizator. Puteți specifica mai multe valori pentru parametrul opțiune utilizator.

Tabela 98. Valori posibile pentru USROPT:

*NONE	Nu este folosită nici o opțiune specială pentru acest utilizator. Este folosită interfața de sistem standard.
*CLKWD	Sunt afișate cuvinte cheie în loc de posibile valori de parametri când este promptată o comandă CL. Aceasta este echivalentul apăsării tastei F11 din ecranul de prompt normal pentru o comandă CL.
*EXPERT	Când utilizatorul vizualizează ecrane care arată autorizări de obiect, precum ecranul Editare autorizare obiect sau ecranul Editare listă autorizări, informațiile de autorizare detaliate sunt afișate fără ca utilizatorul să apese F11 (Afișare detalii). “Ecrane pentru autorizare” la pagina 133 prezintă un exemplu al versiunii experte a ecranului.
*HLPFULL	Utilizatorul vede informațiile de ajutor în ecran complet, nu într-o fereastră.
*PRTMSG	Un mesaj este trimis la coada de mesaje a utilizatorului când un fișier spool este tipărit pentru acest utilizator.
*ROLLKEY	Acțiunile tastelor Page Up și Page Down sunt inversate.
*NOSTMSG	Mesajele de stare afișate de obicei în partea de jos a ecranului nu sunt arătate utilizatorului.
*STMSG	Mesajele de stare sunt afișate când sunt trimise la utilizator.

Numărul de identificare utilizator

Prompt adăugare utilizator:

Neafișat

Parametru CL:

UID

Lungime:

10,0

Sistemul de fișiere integrat folosește numărul de identificare utilizator (uid) pentru a identifica un utilizator și verifică autorizarea utilizatorului. Fiecare utilizator din sistem trebuie să aibă un uid unic.

Tabela 99. Valori posibile pentru UID:

*GEN	Sistemul generează un unic uid pentru acest utilizator. Va fi generat un uid mai mare de 100.
<i>uid</i>	O valoare de la 1 la 4294967294 care va fi alocată ca uid pentru acest utilizator. Trebuie ca uid să nu fi fost deja alocat altui utilizator.

Recomandare: Pentru majoritatea instalărilor, lăsați sistemul să genereze un uid pentru utilizatorii noi specificând UID(*GEN). Totuși, dacă sistemul dumneavoastră este parte a unei rețele, ar putea fi necesar să alocați uid-uri care să se potrivească cu cele alocate altor sisteme din rețea. Consultați administratorul de rețea.

Număr identificare grup

Promptul Adăugare utilizator:

Neafișat

Parametru CL:

GID

Lungime:

10,0

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

Tabela 100. Valori posibile pentru GID:

*NONE	Acest profil nu are un gid.
*GEN	Sistemul generează un unic gid pentru acest profil. Va fi generat un gid mai mare de 100.
<i>gid</i>	O valoare de la 1 la 4294967294 care va fi alocată ca gid pentru acest profil. Trebuie ca gid să nu fi fost deja alocat altui profil.

Recomandare: Pentru majoritatea instalărilor, lăsați sistemul să genereze un gid pentru noi profiluri de grup specificând GID(*GEN). Totuși, dacă sistemul dumneavoastră este parte a unei rețele, ar putea fi necesar să alocați gid-uri care să se potrivească cu cele alocate altor sisteme din rețea. Consultați administratorul de rețea.

Nu alocați un gid unui profil de utilizator pe care nu intenționați să îl folosiți ca profil de grup. În unele medii, un utilizator care este semnat și are un gid are restricții asupra executării anumitor funcții.

Directorul de bază

Prompt adăugare utilizator:

Neafișat

Parametru CL:

HOMEDIR

Directorul de bază este directorul de lucru inițial al utilizatorului pentru Sistemul de fișiere integrat. Directorul de bază este directorul curent al utilizatorului dacă un alt director curent nu a fost specificat. Dacă directorul de bază specificat în profil nu există când utilizatorul semnează, directorul de bază al utilizatorului este directorul rădăcină (/).

Tabela 101. Valori posibile pentru HOMEDIR:

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

Asociere EIM

Prompt adăugare utilizator:

Neafișat

Parametru CL:

EIMASSOC

Câmpul de parametru Asociere EIM specifică dacă trebuie să fie adăugată o asociere EIM (Enterprise Identity Mapping) unui identificator EIM pentru utilizator. Opțional, identificatorul EIM poate fi creat dacă nu există deja.

Notă:

1. Aceste informații nu sunt stocate în profilul de utilizator. Aceste informații nu sunt salvate sau restaurate cu profilul de utilizator.
2. Dacă acest sistem nu este configurat pentru EIM, nu este făcută nici o procesare. Neputința de a realiza operații EIM nu cauzează eșuarea comenzii.

Tabela 102. Valori posibile pentru EIMASSOC, valori singulare:

Valori singulare

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

Tabela 103. Valori posibile pentru EIMASSOC, Elementul 1:

Elementul 1: identificatorul EIM

Specificați identificatorul EIM pentru această asociere.

***USRPRF** Numele identificatorului EIM este același cu numele profilului utilizator.
valoare caracter Specificați numele identificatorului EIM.

Tabela 104. Valori posibile pentru EIMASSOC, Elementul 2:

Elementul 2: Tip de asociere

Specifică tipul de asociere. Este recomandat ca o asociere destinație să fie adăugată pentru un utilizator i5/OS.

Asocierile destinație sunt în principal folosite pentru a securiza datele existente. Ele sunt găsite ca rezultat al mapării operației de căutare (de exemplu, `eimGetTargetFromSource()`), dar nu pot fi folosite ca identitatea sursă pentru o operație de căutare mapare.

Asocierile sursă sunt în principal folosite pentru scopuri de autentificare. Ele pot fi folosite ca identitate sursă a mapării operației de căutare, dar nu vor fi găsite ca destinație a operației 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, și nu vor fi găsite ca destinație a unei operații de căutare mapare.

***TARGET** Procesați o asociere destinație.
***SOURCE** Procesați o asociere sursă.
***TGTSRC** Procesați o asociere sursă și una destinație.
***ADMIN** Procesați o asociere administrativă.
***ALL** Procesați toate tipurile de asocieri.

Tabela 105. Valori posibile pentru EIMASSOC, Elementul 3:

Elementul 3: Acțiune de asociere

***REPLACE** Asocierile de tipul specificat vor fi înlăturate din identificatoarele EIM care au o asociere pentru acest profil utilizator și registru EIM local. O nouă asociere va fi adăugată la identificatorul EIM specificat.
***ADD** Adăugați o asociere.
***REMOVE** Înlăturați o asociere.

Tabela 106. Valori posibile pentru EIMASSOC, Elementul 4:

Elementul 4: Creare identificator EIM

Specifică dacă identificatorul EIM ar trebui să fie creat dacă nu există deja.

*NOCRTEIMID	Identificatorul EIM nu este creat.
*CRTEIMID	Identificatorul EIM este creat dacă nu există.

Autorizare

Prompt adăugare utilizator:

Neafișat

Parametru CL:

AUT

Câmpul *Autorizare* specifică autorizarea publică pentru profilul de utilizator. Autorizarea pentru un profil controlează multe funcții asociate cu profilul, precum:

- Modificarea lui
- Afișarea lui
- Ștergerea lui
- Lansarea unui job folosindu-l
- Specificarea lui într-o descriere de job
- Transferarea dreptului de proprietate a obiectului la el
- Adăugarea de membri, dacă este un profil de grup

Tabela 107. Valori posibile pentru AUT:

*EXCLUDE	Publicului îi este în mod explicit refuzat accesul la profilul de utilizator.
*ALL	Publicului îi sunt date toate autorizările de date și 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.

Consultați “Definirea modului în care pot fi accesate informațiile” la pagina 112 pentru o explicație completă a autorizărilor care pot fi acordate.

Recomandare: Pentru a preveni folosirea greșită a profilurilor de utilizator care au autorizare pentru obiecte critice, asigurați-vă că autorizarea publicului pentru profiluri este *EXCLUDE. Printre posibilele folosiri greșite ale unui profil se numără lansarea unui job care rulează sub acel profil de utilizator sau modificarea unui program astfel încât să adopte autorizarea acelui profil de utilizator.

Auditare obiect

Prompt adăugare utilizator:

Neafișat

Parametru CL:

OBJAUD

Lungime:

10

Valoarea de auditare obiect pentru un profil de utilizator lucrează împreună cu valoarea de auditare obiect pentru un obiect pentru a determina dacă accesul utilizatorului la un obiect este auditat. Auditarea de obiect pentru un profil de utilizator nu poate fi specificată în nici un ecran pentru profilul de utilizator. Folosiți comanda CHGUSRAUD pentru a specifica auditarea de obiect pentru un utilizator. Doar un utilizator cu autorizarea specială *AUDIT poate folosi

comanda CHGUSRAUD.

Tabela 108. Valori posibile pentru OBJAUD:

*NONE	Valoarea OBJAUD pentru obiecte determină dacă auditarea de obiect este efectuată pentru acest utilizator.
*ALL	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică sau citește obiectul.
*CHANGE	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică obiectul.
*NOTAVL	Această valoare este afișată 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.

Tabela 109 arată cum lucrează împreună valorile OBJAUD pentru utilizator și obiecte:

Tabela 109. Auditarea realizată pentru accesul la obiect

Valoare OBJAUD pentru obiect	Valoare OBJAUD pentru utilizator		
	*NONE	*CHANGE	*ALL
*ALL	Modificare și folosire	Modificare și folosire	Modificare și folosire
*CHANGE	Modificare	Modificare	Modificare
*NONE	Nimic	Nimic	Nimic
*NOTVAL	Nimic	Nimic	Nimic
*USRPRF	Nimic	Modificare	Modificare și folosire

“Planificarea auditării accesului la obiect” la pagina 252 furnizează informații despre cum se folosesc valorile de sistem și valorile de auditare obiect pentru a vă îndeplini nevoile de auditare securitate.

Acțiuni de auditare

Prompt adăugare utilizator:

Neafișat

Parametru CL:

AUDLVL

Lungime:

640

Pentru un utilizator individual, puteți să specificați ce acțiune relevantă de securitate ar trebui înregistrată în jurnalul de auditare. Acțiunile specificate pentru un utilizator individual se aplică în plus față de acțiunile specificate pentru toți utilizatorii de valorile de sistem QAUDLVL și QAUDLVL2. Acțiunea 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 110. Valori posibile pentru AUDLVL:

*NONE	Valoarea de sistem QAUDLVL controlează acțiunea de auditare pentru acest utilizator. Nu este terminată nici o auditare suplimentară.
*NOTAVL	Această valoare este afișată 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.
*CMD	Șirurile de comenzi sunt înregistrate în istoric. *CMD poate fi specificat numai pentru utilizatori individuali. Auditarea șirurilor de comenzi nu este disponibilă ca opțiune de sistem folosind valoarea de sistem QAUDLVL.
*CREATE	Operațiile de creare obiect sunt înregistrate în istoric.
*DELETE	Operațiile de ștergere obiect sunt înregistrate în istoric.
*JOBSTA	Modificările de job sunt înregistrate în istoric.
*OBJMGT	Operațiile de redenumire și mutare obiect sunt înregistrate în istoric.
*OFCSR	Modificările la directorul de distribuție sistem și acțiunile de poștă birou sunt înregistrate în istoric.
*PGMADP	Obținerea autorizării la un obiect printr-un program care adoptă autorizare este înregistrată în istoric.
*SAVRST	Operațiile de restaurare și salvare sunt înregistrate în istoric.
*SECURITY	Sunt înregistrate funcțiile referitoare la securitate.
*SERVICE	Folosirea uneltelor de service este înregistrată în istoric.
*SPLFDTA	Acțiunile efectuate pe fișierele spool sunt înregistrate în istoric.
*SYSMGT	Folosirea funcțiilor de gestionare sisteme este înregistrată în istoric.

“Planificarea auditării acțiunilor” la pagina 234 furnizează informații despre cum se folosesc valorile de sistem și acțiunile de auditare pentru utilizatori ca să vă îndepliniți nevoile de auditare securitate.

Informațiile suplimentare asociate cu un profil de utilizator

Secțiunile anterioare descriu câmpurile pe care le specificați atunci când creați sau modificați profiluri de utilizator. Și alte informații sunt asociate cu un profil de utilizator din sistem și sunt salvate cu el:

- Autorizări private
- Informații obiect deținut
- Informații obiect grup primar

Cantitatea acestor informații afectează timpul necesar pentru salvarea și restaurarea profilurilor și pentru construirea ecranelor de autorizare. “Modul în care sunt stocate informațiile de securitate” la pagina 220 furnizează detalii suplimentare despre cum profilurile de utilizator sunt memorate și salvate.

Autorizările private

Toate autorizările private ale unui utilizator pentru obiecte sunt memorate cu profilul de utilizator. Când un utilizator are nevoie de autorizare pentru un obiect, pot fi căutate autorizările private ale utilizatorului. “Organigrama 3: Cum este verificată autorizarea utilizatorului asupra unui obiect” la pagina 151 furnizează detalii suplimentare despre verificarea autorizării.

- | Puteți afișa o autorizare privată a utilizatorului la obiectele bazate pe bibliotecă folosind comanda Afișare profil
- | utilizator: `DSPUSRPRF nume profil utilizator TYPE(*OBJAUT)`. Puteți lucra cu autorizările private ale
- | utilizatorului asupra obiectelor bazate pe bibliotecă și directory folosind comanda Work with Objects by Private
- | Authority (`WRKOBJPVT`). Pentru modificarea autorizărilor private ale unui utilizator, puteți folosi comenzile care
- | lucrează cu autorizări de obiecte, cum ar fi Editare autorizare obiect (`EDTOBJAUT`).

Puteți copia toate autorizările private de la un profil de utilizator la altul folosind comanda Acordare autorizare utilizator (`GRTUSRAUT`). Consultați “Copierea autorizării de la un utilizator” la pagina 144 pentru informații suplimentare.

Autorizările de grup primar

Numele tuturor obiectelor pentru care profilul este grup primar sunt memorate cu profilul de utilizator. Puteți afișa obiectele pentru care profilul este grup primar folosind comanda DSPUSRPRF: DSPUSRPRF *nume profil grup* TYPE(*OBJPGP). De asemenea puteți folosi și comanda Gestionare obiecte după grup primar (WRKOBJPGP).

Informațiile privind obiectul deținut

Informațiile de autorizare privată pentru un obiect sunt memorate cu profilul utilizator care deține acel obiect. Aceste informații sunt folosite la construcția ecranelor de sistem care gestionează autorizările pentru obiecte. Dacă un profil deține un număr mare de obiecte care au multe autorizări private, performanța construirii ecranelor de autorizare pentru obiecte pentru aceste obiecte poate fi afectată. Mărimea unui profil proprietar afectează performanța când se afișează și se lucrează cu autorizări la obiectele deținute și când se salvează sau se restaurează profiluri. De asemenea, pot fi afectate operațiile de sistem. Pentru a preveni afectarea fie a performanței, fie a operațiilor de sistem, distribuiți dreptul de proprietate a obiectelor la mai multe profiluri. Deoarece mărimea unui profil de utilizator vă poate influența performanța, se recomandă să nu alocați toate obiectele (sau aproape toate) unui singur profil proprietar.

Autentificarea prin ID digital

Infrastructura de securitate iSeries vă permite folosirea pentru identificare a certificatelor digitale x.509. Certificatele digitale permit utilizatorilor să securizeze comunicațiile și să mențină integritatea mesajelor.

API-urile pentru ID digital creează, distribuie și gestionează certificate digitale asociate cu profiluri utilizator. Consultați subiectul API din Centrul de informare (consultați “Cerințe preliminare și informații înrudite” la pagina xvi) pentru informații despre următoarele API-uri:

- Adăugare certificat utilizator (QSYADDUC)
- Înlăturare certificat utilizator (QSYRMVUC)
- Listare certificat utilizator (QSYLSTUC)
- Găsire certificat utilizator (QSYFN Duc)
- Adăugare listă de validare certificat (QSYADDVC)
- Înlăturare listă de validare certificat (QSYRMVVC)
- Listare listă de validare certificat (QSYLSTVC)
- Verificare listă de validare certificat (QSYCHKVC)
- Analizare certificat (QSYPARSC)

Gestionarea profilurilor de utilizator

Această parte a capitolului descrie comenzile și ecranele pe care le folosiți ca să creați, modificați și ștergeți profiluri de utilizator. Nu sunt descrise toate câmpurile, opțiunile și tastele funcționale. Folosiți informațiile online pentru detalii.

Trebuie să aveți autorizarea specială *SECADM ca să creați, modificați sau ștergeți profiluri de utilizator.

Crearea profilurilor de utilizator

Puteți crea profiluri utilizator în mai multe căi:

- Folosind ecranul Gestionare profiluri utilizator (WRKUSRPRF).
- Folosind comanda Creare profil utilizator (CRTUSRPRF).
- Folosind opțiunea Gestionare înrolare utilizator din meniul Setare.
- Folosind ecranul Navigator iSeries de la folderul iSeries Access.

Utilizatorul care creează profilul utilizator îl deține și primește pentru el autorizarea *ALL. Profilului de utilizator îi este dată autorizarea *OBJMGT și *CHANGE pentru el însuși. Aceste autorizări sunt necesare pentru operații normale și nu trebuie înlăturate.

Un profil de utilizator nu poate fi creat cu mai multe autorizări sau capabilități decât acelea ale utilizatorului care creează profilul.

Notă: Când executați o comandă CRTUSRPRF, nu puteți 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 și intrările de grup primar vor fi atașate la profilul cu același nume din sistemul destinație. Dacă nu există un profil în sistemul destinație, este creat. Utilizatorul nu va avea nici o autorizare specială și parola va fi setată la *NONE.

Folosirea comenzii Gestionare profiluri utilizator

În comanda WRKUSRPRF puteți introduce un nume de profil specific, un set de profiluri generice sau *ALL. Nivelul de ajutorare determină ce listă de afișare vedeți. Când folosiți comanda WRKUSRPRF cu nivelul de ajutorare *BASIC, veți accesa ecranul Gestionare înrolare utilizator. Dacă este specificat nivelul de ajutorare *INTERMED, veți accesa ecranul Gestionare profiluri utilizator.

Puteți specifica parametrul ASTLVL (nivel de ajutorare) în comandă. Dacă nu specificați ASTLVL, sistemul va folosi nivelul de ajutorare memorat cu profilul dumneavoastră de utilizator.

În ecranul Gestionare profiluri utilizator, tastați 1 și numele profilului pe care doriți să-l creați:

```
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
```

Puteți vizualiza ecranul Creare profil utilizator:

```
Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . NEWUSER
User password . . . . . NEWUSER1
Set password to expired . . . . *YES
Status . . . . . *ENABLED
User class . . . . . *USER
Assistance level . . . . . *SYSVAL
Current library . . . . . *CRTDFT
Initial program to call . . . . *NONE
Library . . . . .
Initial menu . . . . . MAIN
Library . . . . . QSYS
Limit capabilities . . . . . *NO
Text 'description' . . . . .
```

Ecranul Creare profil utilizator afișează toate câmpurile din profilul utilizator. Folosiți tastele F10 (Parametri suplimentari) și Page Down ca să introduceți informații suplimentare. Folosiți F11 (Afișare cuvinte cheie) ca să vizualizați numele parametrilor.

Ecranul Creare profil utilizator nu adaugă utilizatorul la directorul de sistem.

Folosirea comenzii Creare profil utilizator

Puteți folosi comanda CRTUSRPRF ca să creați un profil de utilizator. Puteți introduce parametri prin comandă sau puteți cere promptarea (F4) și consulta ecranul Creare profil utilizator.

Folosirea opțiunii Gestionare înrolare utilizator

Selectați opțiunea Gestionare înrolare utilizator din meniul SETUP. Nivelul de ajutorare memorat cu profilul dumneavoastră determină dacă veți vedea ecranul Gestionare profiluri utilizator sau ecranul Gestionare înrolare utilizator. Puteți folosi F21 (Selectare nivel de ajutorare) ca să modificați nivelurile.

În ecranul Gestionare înrolare utilizator, folosiți opțiunea 1 (Adăugare) ca să adăugați un utilizator nou pe sistem.

```
Work with User Enrollment

Type options below, then press Enter.
1=Add 2=Change 3=Copy 4=Remove 5=Display

Opt  User      Description
1    NEWUSER
-    DPTSM      Sales and Marketing Departme
-    DPTWH      Warehouse Department
```

Apare ecranul Adăugare utilizator:

```
Add User

Type choices below, then press Enter.

User . . . . . NEWUSER
User description . . . .
Password . . . . . NEWUSER
Type of user . . . . . *USER
User group . . . . . *NONE

Restrict command line use  N

Default library . . . . .
Default printer . . . . . *WRKSTN
Sign on program . . . . . *NONE
Library . . . . .

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

F1=Help  F3=Exit  F5=Refresh  F12=Cancel
```

Ecranul Adăugare utilizator este proiectat pentru un administrator de securitate fără experiență tehnică. Nu afișează toate câmpurile din profilul de utilizator. Sunt folosite valorile implicite pentru toate câmpurile care nu sunt afișate.

Notă: Dacă folosiți ecranul Adăugare utilizator, aveți limitat numele de profil utilizator la 8 caractere.

Apăsați Page down ca să vedeți 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 același ID utilizator ca și numele de profil utilizator (primele opt caractere) și o adresă a numelui sistem.

Meniul principal include și Opțiunile de utilizator 51—59. Aceste opțiuni adiționale (Opțiunile 51--59) sunt procesate similar la Opțiunea 50, exceptând valorile implicite pentru următoarele câmpuri necompletate:

- Text pentru opțiuni de meniu
- Program utilizator
- Bibliotecă

Copierea profilurilor de utilizator

Puteți crea un profil de utilizator copiind alt profil de utilizator sau profil de grup. Ați putea dori să setați un profil dintr-un grup ca model. Copiați primul profil din grup pentru a crea profiluri adiționale.

Puteți copia un profil în mod interactiv din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Nici o comandă nu există pentru a copia un profil de utilizator.

Copierea dintr-un ecran Gestionare profiluri utilizator

În ecranul Gestionare profiluri utilizator, tastați 3 în fața profilului pe care doriți să îl copiați. Apare ecranul Creare profil utilizator:

```
                                Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . Name
User password . . . . . > *USRPRF Name
Set password to expired . . . . . > *NO *NO, *YES
Status . . . . . > *ENABLED *ENABLED,
User class . . . . . > *USER *USER,
Assistance level . . . . . > *SYSVAL *SYSVAL,
Current library . . . . . > DPTWH Name,
Initial program to call . . . . . > *NONE Name,
Library . . . . . Name,
Initial menu . . . . . > ICMAN Name,
Library . . . . . > ICPGLIB Name,
Limit capabilities . . . . . > *NO *NO,
Text 'description' . . . . . > 'Warehouse Department'
```

Toate valorile din profilul de utilizator de copiere sunt arătate în ecranul Creare profil utilizator, cu excepția acestor câmpuri:

Director de bază
*USRPRF

Atribute de job locale

Atribute de job locale

Locale Locale**Profil utilizator**

Spațiu liber. Trebuie completat.

Parolă *USRPRF**Coadă de mesaje**

*USRPRF

Parolă document

*NONE

Număr identificare utilizator

*GEN

Număr identificare grup

*NONE

Asociere EIM

*NOCHG

Autorizare

*EXCLUDE

6Puteți modifica orice câmpuri în ecranul Creare profil utilizator. Autorizările private ale profilului de copiere nu sunt copiate. În plus, obiectele interne care conțin preferințe de utilizator și alte informații despre utilizator nu vor fi copiate.

Copierea dintr-un ecran Gestionare înrolare utilizator

În ecranul Gestionare înrolare utilizator, tastați 3 în fața profilului pe care doriți să îl copiați. 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 de copiere apar în ecranul Adăugare utilizator, cu excepția următoarelor:

Utilizator

Spațiu liber. Trebuie completat. Limitat la 8 caractere.

Parolă Spațiu liber. Dacă nu introduceți o valoare, profilul este creat cu parola egală cu valoarea implicită specificată pentru parametrul PASSWORD al comenzii CRTUSRPRF.

Puteți modifica orice câmpuri din ecranul Copiere utilizator. Câmpurile profil utilizator care nu apar în versiunea nivelului de asistență de bază sunt copiate din profilul de copiere, cu următoarele excepții:

Coadă de mesaje

*USRPRF

Parolă document

*NONE

Număr identificare utilizator

*GEN

Număr identificare grup

*NONE

Asociere EIM

*NOCHG

Autorizare

*EXCLUDE

Autorizările private ale profilului de copiere nu sunt copiate.

Copierea autorizărilor private

Puteți copia autorizările private de la un profil utilizator la altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT). Această posibilitate poate fi de folos în unele situații, dar nu ar trebui folosită în locul profilurilor de grup sau a listelor de autorizare. Copierea autorizărilor nu ajută la gestionarea autorizărilor similare în viitor și poate cauza probleme de performanță în sistem.

Subiectul “Copierea autorizării de la un utilizator” la pagina 144 are informații suplimentare despre folosirea acestei comenzi.

Modificarea profilurilor de utilizator

Puteți modifica un profil utilizator folosind opțiunea 2 (Modificare) din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Puteți folosi și comanda Modificare profil utilizator (CHGUSRPRF).

Utilizatorilor cărora li se permite să introducă comenzi pot modifica unii parametri al propriului profil folosind comanda Modificare profil (CHGPRF).

Un utilizator nu poate modifica un profil de utilizator pentru a avea mai multe autorizări speciale sau capacități decât utilizatorul care modifică profilurile.

Ștergerea profilurilor de utilizator

Nu puteți șterge un profil de utilizator care deține obiecte. Trebuie să ștergeți orice obiecte deținute de profil sau să transferați dreptul de proprietate asupra acelor obiecte la alt profil. Nivelul de asistență de bază și Nivelul de asistență intermediar vă permit să manipulați obiectele deținute când ștergeți un profil.

Nu puteți șterge un profil de utilizator dacă este grupul primar pentru vreun obiect. Când folosiți Nivelul de asistență intermediar pentru a șterge un profil utilizator, puteți modifica sau înlătura grupul primar pentru obiecte. Puteți folosi comanda WRKOBJPGP cu opțiunea *OBJPGP (grup primar obiect) pentru a lista orice obiecte pentru care un profil este grupul primar.

Când ștergeți un profil utilizator, utilizatorul este înlăturat din toate listele de distribuire și din directorul sistem.

Trebuie să modificați dreptul de proprietate sau să ștergeți coada de mesaje a utilizatorului. Sistemul șterge automat coada de mesaje când profilul este șters.

Nu puteți șterge un profil grup care are membri. Pentru a lista membrii unui profil de grup, tastați DSPUSRPRF *nume-profil-grup* *GRPMBR. Modificați câmpul GRPPRF în fiecare profil de membru înainte de a șterge profilul de grup.

Folosirea comenzii Ștergere profil de utilizator

Puteți introduce direct comanda Ștergere profil utilizator (DLTUSRPRF) sau puteți folosi opțiunea 4 (Ștergere) din ecranul Gestionare profiluri utilizator. Comanda DLTUSRPRF are parametri care vă permit să tratați:

- Toate obiectele deținute 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 .

```

Puteți șterge toate obiectele deținute sau le puteți transfera unui nou utilizator. Dacă doriți să manipulați individual obiectele deținute, puteți folosi comanda Gestionare obiecte după proprietar (WRKOBJOWN). Puteți modifica grupul primar pentru toate obiectele pentru care profilul este grupul primar. Dacă doriți să manipulați individual obiectele, puteți 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

Opt  Object      Library  Type  Attribute  ASP
     HOGANR     QUSRSYS *MSGQ
     QUERY1     DPTWH   *PGM
     QUERY2     DPTWH   *PGM
Device
     *SYSBAS
     *SYSBAS
     *SYSBAS

```

Folosirea opțiunii Înlăturare utilizator

Din ecranul Gestionare înrolare utilizator, tastați 4 (Înlăturare) în fața profilului pe care doriți să îl ștergeți. Vedeți 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 șterge profilul, selectați opțiunea 1. Apare un ecran care vă cere noul utilizator.

Pentru a manipula obiecte individuale, selectați opțiunea 2. Vedeți un ecran detaliat Înălțurare 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

```

Folosiți opțiunile din ecran pentru a șterge obiectele sau a le transfera la un nou proprietar. Când toate obiectele au fost înlăturate din ecran, puteți șterge profilul.

Note:

1. Puteți folosi F13 pentru a șterge toate obiectele deținute de profilul utilizator.
2. Fișierele spool nu apar în ecranul Gestionare obiecte după proprietar. Puteți șterge un profil utilizator chiar dacă acel profil încă deține fișiere spool. După ce ați șters un profil de utilizator, folosiți comanda Gestionare fișiere spool (WRKSPLF) pentru a localiza și șterge orice fișier spool deținut de profilul de utilizator, dacă nu mai este necesar.
3. Obiectele pentru care profilul de utilizator șters a fost grupul primar vor avea un grup primar *NONE.

Lucrul cu obiecte după autorizare privată

- | Puteți folosi comanda Gestionare obiecte după autorizări private (WRKOBJPVT) pentru a lista și gestiona orice obiecte
- | pentru care un profil are autorizare primară.

Gestionarea obiectelor după grup primar

Puteți folosi comanda Gestionare obiecte după grup primar (WRKOBJPGP) pentru a lista și gestiona orice obiecte pentru care un profil este grupul primar. Puteți 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

Opt	Object	Library	Type	Attribute	ASP	Device
	CUSTMAST	CUSTLIB	*FILE			*SYSBAS
	CUSTWRK	CUSTLIB	*FILE			*SYSBAS
	CUSTLIB	QSYS	*LIB			*SYSBAS

Activarea unui profil de utilizator

Dacă valorile de sistem QMAXSIGN și QMAXSGNACN sunt setate să dezactiveze un profil de utilizator după prea multe încercări de semnare, ați putea dori ca o persoană, cum ar fi operatorul de sistem, să activeze profilul modificând starea în *ENABLED. Totuși, pentru a activa un profil utilizator, trebuie să aveți autorizare specială *SECADM și autorizare *OBJMGT și *USE la profil pentru profilul utilizator. În mod normal, un operator de sistem nu are autorizare specială *SECADM.

O soluție este de a folosi un program simplu care adoptă autorizare:

1. Creați un program CL deținut de un utilizator care are autorizare specială *SECADM și autorizare *OBJMGT și *USE la profilurile utilizator din sistem. Adoptați autorizarea proprietarului când programul este creat specificând USRPRF(*OWNER).
2. Folosiți comanda EDTOBJAUT pentru a face autorizare publică la programul *EXCLUDE și dați operatorilor de sistem autorizarea *USE.
3. Operatorul activează profilul introducând:

```
CALL ENABLEPGM nume-profil
```

4. Partea principală a programului ENABLEPGM arată astfel:

```
PGM &PROFILE  
DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)  
CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)  
ENDPGM
```

Listarea profilurilor de utilizator

Puteți afișa și tipări informații despre profilurile utilizator într-o varietate de formate.

Afișarea unui profil individual

Pentru a afișa valori pentru un profil utilizator individual, folosiți opțiunea 5 (Afișare) din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Sau, puteți folosi comanda Afișare profil utilizator (DSPUSRPRF).

Listarea tuturor profilurilor

Folosiți comanda Afișare utilizatori autorizați (DSPAUTUSR) pentru a tipări sau a afișa toate profilurile utilizator din sistem. Parametrul de secvență (SEQ) din comandă vă permite să sortați lista după numele de profil sau după profilul de grup.

Display Authorized Users				
Group Profile	User Profile	Password Last Changed	No 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, puteți vedea care profilurile utilizator au parole definite pentru folosire la diferite niveluri de parolă.

Display Authorized Users					
User Profile	Group Profile	Password Last Changed	Password for level 0 or 1	Password for level 2 or 3	Password for NetServer
ANGELA		04/21/0x	*YES	*NO	*YES
ARTHUR		07/07/0x	*YES	*YES	*YES
CAROL1		05/15/0x	*YES	*YES	*YES
CAROL2		05/15/0x	*NO	*NO	*NO
CHUCKE		05/18/0x	*YES	*NO	*YES
DENNISS		04/20/0x	*YES	*NO	*YES
DPORTER		03/30/0x	*YES	*NO	*YES
GARRY		08/04/0x	*YES	*YES	*YES
JANNY		03/16/0x	*YES	*NO	*YES

Tipuri de ecrane pentru profil de utilizator

Comanda Afișare profil utilizator (DSPUSRPRF) oferă câteva tipuri de listări și ecrane:

- Unele ecrane și listări sunt disponibile doar pentru profiluri individuale. Altele pot fi tipărite pentru toate profilurile sau un set generic de profiluri. Consultați informații online pentru detalii despre tipurile disponibile.
- Puteți crea un fișier de ieșire din câteva ecrane specificând ieșire(*OUTFILE). Folosiți o unealtă de interogare sau un program pentru a produce rapoarte personalizate din fișierul de ieșire. Subiectul “Analizarea profilurilor de utilizator” la pagina 267 dă sugestii pentru rapoarte.

Tipuri de rapoarte pentru profil de utilizator

Următoarele comenzi furnizează rapoarte profil utilizator.

- Tipărire profil utilizator (PRTUSRPRF)
Această comandă vă permite să tipăriți un raport care conține informații pentru profilurile utilizator din sistem. Pot fi tipărite patru rapoarte diferite. Unul conține informații de tip autorizare, unul conține informații de tip mediu, unul informații de tip parolă și unul informații de tip nivel parolă.
- Analizare parolă implicită (ANZDFTPWD)
Această comandă vă permite să tipăriți un raport al tuturor profilurilor utilizator din sistem care au o parolă implicită și să efectuați o acțiune împotriva profilurilor. Un profil are o parolă implicită când numele profil utilizator se potrivește parolei profilului.

Profilurile utilizator din sistem care au parolă implicită pot fi dezactivate și parolele lor pot fi setate să expire.

Redenumirea unui profil de utilizator

Sistemul nu oferă o metodă directă pentru redenumirea unui profil utilizator.

Un profil nou poate fi creat cu aceleași autorizări pentru un utilizator cu nume nou. Unele informații, totuși, nu pot fi transferate la noul profil. Următoarele sunt exemple de informații care nu pot fi transferate:

- Fișiere spool.
- obiecte interne care conțin preferințe utilizator și alte informații despre utilizator vor fi pierdute.
- Certificatele digitale care conțin numele utilizator nu vor fi validate.
- Informațiile uid și gid reținute de sistemul de fișiere integrat nu pot fi modificate.
- Nu veți putea să modificați informațiile care sunt memorate de aplicații și care conțin numele utilizator.

Aplicațiile care sunt rulate de utilizator pot avea "profiluri de aplicație". Crearea unui profil utilizator iSeries nou pentru redenumirea unui utilizator nu duce la redenumirea oricărui profil de aplicație pe care utilizatorul îl poate avea. Un profil Lotus Notes este un exemplu de profil de aplicație.

Următorul exemplu arată cum se creează un profil nou pentru un utilizator cu un nume nou și aceleași autorizări. Vechiul nume de profil este SMITHM. Noul nume de profil este JONESM:

1. Copiați vechiul profil (SMITHM) la un nou profil (JONESM) folosind opțiunea de copiere de la ecranul Gestionare înrolare utilizator.

2. Acordați lui JONESM toate autorizările private ale lui SMITHM folosind comanda Acordare autorizare utilizator (GRTUSRAUT):

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

3. Modificați grupul primar al tuturor obiectelor pentru care SMITHM este grup primar cu comanda Gestionare obiecte după grup primar (WRKOBJPGP):

```
WRKOBJPGP PGP(SMITHM)
```

Introduceți opțiunea 9 pentru toate obiectele care au nevoie de modificarea grupului primar și introduceți din linia de comandă NEWPGP (JONESM).

Notă: JONESM trebuie să aibă alocat un gid folosind parametrul GID din comanda Creare sau modificare profil utilizator (CRTUSRPRF sau CHGUSRPRF).

4. Afișați profilul de utilizator SMITHM folosind comanda Afișare profil utilizator (DSPUSRPRF):

```
DSPUSRPRF USRPRF(SMITHM)
```

Notați uid-ul și gid-ul pentru SMITHM.

5. Transferați dreptul de proprietate asupra tuturor celorlalte obiecte deținute la JONESM și înlăturați profilul de utilizator SMITHM, folosind opțiunea 4 (Înlăturare) din ecranul Gestionare înrolare utilizator.

6. Modificați valorile uid și gid ale lui JONESM la uid-ul și gid-ul care aparțineau lui SMITHM prin folosirea comenzii Modificare profil utilizator (CHGUSRPRF):

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

Dacă JONESM deține obiecte într-un director, nu poate fi folosită comanda CHGUSRPRF pentru a modifica uid-ul și gid-ul. Folosiți API-ul QSYCHGID pentru modificarea uid-ul și gid-ul profilului de utilizator JONESM.

Gestionarea auditării utilizatorilor

Folosiți comanda Modificare auditare utilizator (CHGUSRAUD) ca să setați caracteristicile de auditare pentru utilizatori. Ca să folosiți această comandă, trebuie să aveți 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

```

Puteți specifica simultan caracteristicile de auditare pentru mai mulți utilizatori prin listarea numelor de profil de utilizator.

Parametrul AUDLVL (acțiune de auditare utilizator) poate avea mai multe valori. Valoarea pe care o specificați în această comandă înlocuiește valoarea curentă AUDLVL pentru utilizatori. Valorile pe care le specificați nu sunt adăugate la valorile curente AUDLVL pentru utilizatori.

Dacă aveți autorizarea specială *ALLOBJ sau *AUDIT, puteți folosi comanda Afișare profil utilizator (DSPUSRPRF) ca să vedeți caracteristicile de auditare pentru un utilizator.

Gestionarea profilurilor în programele CL

Veți dori să extrageți informații despre profilul utilizator de la un program CL. Puteți folosi comanda Extragere profil utilizator (RTVUSRPRF) în programul dumneavoastră CL. Comanda întoarce atributele cerute ale profilului la variabilele pe care le-ați asociat cu numele de câmp profil utilizator. Descrierea câmpurilor profil utilizator din acest capitol arată lungimea câmpurilor așteptată de comanda RTVUSRPRF. În unele cazuri, un câmp zecimal poate să aibă o valoare care nu este numerică. De exemplu, câmpul spațiu de stocare maxim (MAXSTG) este definit ca și un câmp zecimal, dar poate avea o valoare de *NOMAX. Informațiile online pentru comanda RVTUSRPRF descriu valorile care sunt întoarse într-un câmp zecimal pentru valorile care nu sunt numerice.

Programul eșantion din “Folosirea unui program de aprobare a parolei” la pagina 45 arată un exemplu de utilizare a comenzii RTVUSRPRF.

Puteți de asemenea folosi comanda CRTUSRPRF sau CHGUSRPRF într-un program CL. Dacă folosiți variabile pentru parametrii acestor comenzi, definiți variabilele ca și câmpuri de caracter ca să le potriviți cu ecranul prompt Creare profil utilizator. Mărimea variabilei nu trebuie să se potrivească cu mărimea câmpului.

Nu puteți extrage o parolă de utilizator, deoarece parola este memorată cu criptare într-un singur sens. Dacă doriți ca utilizatorul să introducă parola din nou înainte să acceseze informații critice, puteți folosi comanda Verificare parolă Check Password (CHKPWD) din programul dumneavoastră. Sistemul compară parola introdusă cu parola utilizatorului și trimite un mesaj de scăpare la programul dumneavoastră dacă parola nu este corectă.

Punctele de ieșire pentru profil de utilizator

Punctele de ieșire sunt furnizate pentru crearea, modificarea, ștergerea sau restaurarea profilurilor de utilizator. Puteți să vă scrieți propriile programe de ieșire ca să realizeze funcții specifice pentru profilul de utilizator. Când vă înregistrați programele de ieșire cu puncte de ieșire pentru profil de utilizator, sunteți anunțat când un utilizator este creat, modificat, șters sau restaurat. În timpul notificării, programul dumneavoastră de ieșire poate realiza oricare dintre următoarele:

- Extragerea informațiilor 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 ieșire care sunt apelate. Aceasta înseamnă că programul de ieșire nu are autorizare de accesare obiect profil utilizator.

Pentru informații despre securitatea programelor de ieșire, consultați subiectul API din Centrul de informare (consultați “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Profilurile de utilizator furnizate de IBM

Un număr de profiluri utilizator este livrat cu software-ul dumneavoastră de sistem. Aceste profiluri utilizator furnizate de IBM sunt folosite ca și obiecte deținute pentru funcții de sistem variate. Unele funcții de sistem rulează și sub profiluri utilizator livrate de IBM specifice.

Profilurile de utilizator livrate de IBM, cu excepția QSECOFR, sunt furnizate cu parola *NONE și nu sunt destinate semnării. Cu excepția QSECOFR, nu semnați cu profilurile de utilizator livrate de IBM. Pentru a vă permite să instalați sistemul pentru prima dată, parola pentru profilul responsabil cu securitatea (QSECOFR) este aceeași pentru fiecare sistem livrat. Însă parola pentru QSECOFR este livrată ca expirată. În cazul sistemelor sistemele noi, vi se va cere să modificați parola prima dată când semnați cu QSECOFR.

Când instalați o nouă ediție de sistem de operare, parolele pentru profilurile livrate de IBM nu sunt modificate. Dacă profiluri cum ar fi QPGMR și QSYSOPR au parole, aceste parole nu se vor seta în mod automat la *NONE.

Anexa B, “Profilurile de utilizator furnizate de IBM”, la pagina 279 conține o listă completă a tuturor profilurilor utilizator livrate de IBM și valorile de câmp pentru fiecare profil.

Notă: Profilurile livrate de IBM sunt furnizate, dar sunt folosite de IBM i5/OS. Pri urmare, semnarea cu aceste profiluri sau folosirea profilurilor care dețin obiecte utilizator (nelivrate de IBM) **nu** este recomandată.

Modificarea parolelor pentru profilurile de utilizator livrate de IBM

Dacă doriți să semnați cu unul dintre profilurile furnizate de IBM, puteți modifica parola folosind comanda CHGUSRPRF. Puteți modifica aceste parole și folosind o opțiune de la meniul SETUP. Pentru a vă proteja sistemul, ar trebui să lăsați parola setată la *NONE pentru toate profilurile livrate de IBM cu excepția QSECOFR. Nu lăsați 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)

Apăsați Page down ca să modificați parole adiționale:

Change Passwords for IBM-Supplied

Type new password below for IBM-supplied user, type change, then press Enter.

New basic service (QSRVBAS) password
New password (to verify)

Gestionarea ID-urilor Unelte Utilizator

Sunt mai multe îmbunătățiri adăugate la uneltele de service pentru această ediție care le face mai ușor de folosit și de înțeles.

- **Unelte de service sistem (SST)**

Acum puteți gestiona și crea ID-uri utilizator unelte de service de la unelte de service sistem (SST) prin selectarea opțiunii 8 (Gestionare ID-uri utilizator unelte de service) de la ecranul SST principal. Nu mai aveți nevoie să mergeți în unelte de service dedicate (DST) ca să resetați parole, acordați sau revocați privilegiu, sau creați ID-uri utilizator unelte de service. **Note:** Informațiile privind Uneltele de service au fost mutate la Centrul de informare.

- **Îmbunătățiri de gestionare parolă**

Serverul este livrat cu abilitatea limitată de modificare implicită și parole expirate. Aceasta înseamnă faptul că nu puteți modifica ID-urile utilizator unelte de service care au implicate și parole expirate prin API-ul Modificare ID utilizator unelte de service (QSYCHGDS), nu puteți modifica parolele lor prin SST. Puteți modifica numai un ID utilizator unelte de service cu o implicită și parolă expirată prin DST. Și puteți modifica setările de permisiune implicită și parole expirate ca să fie modificate. De asemenea, puteți folosi noul privilegiu Pornire unelte de service (STRSST) ca să creați un ID utilizator unelte de service care poate accesa DST, dar poate fi restricționat de la accesarea SST.

- **Modificări de terminologie**

Datele textuale ale documentației au fost modificate ca să reflecte noua terminologie unelte de service. Specific, termenul ID-uri utilizator unelte de service înlocuiește termenii anteriori, cum ar fi profiluri utilizator DST, ID-uri utilizator, profiluri utilizator unelte de service, sau variații ale acestor nume.

Pentru informații despre cum se gestionează uneltele de service, consultați subiectul Centrului de informare, Unelte de service (**Securitate**—>**Unelte de service**). Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru informații suplimentare asupra accesării, Centrul de informare.

Parola de sistem

Parola de sistem este folosită ca să autorizeze modificările modelului de sistem, anumite condiții de service și modificări ale dreptului de proprietate. Dacă aceste modificări au survenit pe sistemul dumneavoastră, veți fi promptat pentru parola de sistem când veți realiza un IPL.

Capitolul 5. Securitatea resurselor

Securitate resursă definește căror utilizatori le este permis să utilizeze obiecte din sistem și care operație le este permis să realizeze pe aceste obiecte.

Acest capitol descrie fiecare din componentele de securitate resursă și cum lucrează ele împreună pentru a proteja informațiile din sistemul dvs. Explică de asemenea cum să se utilizeze comanda CL și afișează organizarea de securitate resursă pe sistemul dvs.

Capitolul 7 discuții tehnice pentru a proiecta securitatea resursă, inclusiv cum afectează aceasta și design aplicațiile și performanța sistemului.

Capitolul “Cum verifică sistemul autorizarea” la pagina 147 furnizează diagrame de flux detaliate și descrie cum sistemul verifică autorizarea. Puteți găsi util să consultați aceste informații pe măsură ce citiți explicațiile următoare.

Definirea celor care pot accesa informații

Puteți autoriza utilizatori individuali, grupuri de utilizatori și publicul.

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

Definiți cum puteți utiliza un obiect în mai multe modalități:

Autorizare publică:

Publicul este format din toți cei care sunt autorizați să semneze pe sistemul dumneavoastră. Autorizarea publică este definită pentru fiecare obiect din sistem, deși autorizarea publică pentru un obiect poate fi *EXCLUDE. Autorizarea publică la un obiect este utilizată dacă nici o altă autorizare specifică nu este găsită pentru obiect.

Autorizare publică:

Puteți defini autorizare specifică pentru a utiliza un (sau pentru a nu utiliza) obiect. Puteți acorda autorizare unui profil utilizator individual sau unui profil de grup. Un obiect are **autorizare privată** dacă orice autorizare, alta decât autorizarea publică, drept de proprietate obiect sau autorizare de grup primar este definită pentru obiect.

Autorizare utilizator:

Unor profiluri utilizator individuale le poate fi acordată autorizare să utilizeze obiecte în sistem. Acesta este un tip de autorizare privată.

Autorizare de grup:

Unor profiluri utilizator individuale le poate fi acordată autorizare să utilizeze obiecte în sistem. Un membru al grupului primește 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. Totuși, autorizarea proprietarului la obiect poate fi schimbată sau înlăturată. Autorizarea proprietarului la obiect nu este considerată autorizare privată.

Autorizare grup primar:

Puteți specifica un grup primar pentru un obiect și autorizarea pe care o are grupul primar la obiect. Autorizarea de grup primar este memorată cu obiectul și poate furniza performanțe mai bune decât autorizarea privată acordată unui profil de grup. Numai un profil utilizator cu un număr de identificare grup (gid) poate fi grupul primar pentru un obiect. Autorizarea de grup primar nu este considerată autorizare privată.

Definirea modului în care pot fi accesate informațiile

Autorizare înseamnă tipul de acces permis unui obiect. Operații 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** definește că operațiile pot fi realizate la obiect ca un întreg.
2. **Autorizare pentru date** definește că operațiile pot fi realizate în conținutul obiectului.
3. **Autorizare câmp** definește care operații pot fi realizate în câmpurile de date.

Tabela 111 descrie tipurile de autorizare disponibile și listează unele exemple despre cum sunt utilizate autorizările. În cele mai multe cazuri, accesarea unui obiect necesită o combinație de obiect, date, autorizări câmp. Anexa D furnizează informații despre autorizarea necesară pentru a realiza o funcție specifică.

Tabela 111. Descriere tipuri de autorizare

Autorizare	Nume	Funcții permise
<i>Autorizări obiect:</i>		
*OBJOPR	Obiect Operațional	Vedeți descrierea unui obiect. Folosiți obiectul așa cum este determinat de către autorizările de date ale utilizatorului.
*OBJMGT	Management Obiect	Specificați securitatea pentru obiect. Mutați sau redenumiți obiectul. Toate funcțiile definite pentru *OBJALTER și *OBJREF.
*OBJEXIST	Object Existence - Existență obiect	Șterge obiect. Eliberează spațiul ocupat de obiect. Efectuați operații de salvare și de restaurare a obiectului ¹ . Transfer proprietate asupra obiectului.
*OBJALTER	Object Alter - Modificare obiect	Adăugare, ștergere, inițializare și reorganizare membri ai fișierelor bază de date. Modificare și adăugare atribute ale fișierelor bază de date: adăugare și ștergere declanșatori. Modificare atribute ale pachetelor SQL.
*OBJREF	Object Reference - Referință la obiect	Specificați un fișier bază de date ca părinte într-o restricție referențiale. De exemplu, vreți să definiți o regulă conform căreia trebuie să existe o înregistrare despre client în fișierul CUSMAS înainte să poată fi adăugată o comandă pentru ale client în fișierul CUSORD. Vă trebuie autorizarea *OBJREF pentru fișierul CUSMAS pentru a defini această regulă.
*AUTLMGT	Authorization List Management - Gestionare listă de autorizare	Adăugați și eliminați utilizatori și autorizările lor din lista de autorizare ² .
<i>Autorizări asupra datelor:</i>		
*READ	Read - Citire	Afișarea conținutului obiectului, precum vizualizarea înregistrărilor dintr-un fișier.
*ADD	Add - Adăugare	Adăugare intrări la un obiect, precum este adăugarea de mesaje la o coadă de mesaje sau adăugarea de înregistrări la un fișier.
*UPD	Update - Actualizare	Modificarea intrărilor dintr-un obiect, precum este modificarea înregistrărilor dintr-un fișier.
*DLT	Delete - Ștergere	Ștergerea intrărilor dintr-un obiect, precum este ștergerea mesajelor dintr-o coadă de mesaje sau ștergerea înregistrărilor dintr-un fișier.
*EXECUTE	Execute - Execuție	Rularea unui program, unui program de serviciu sau a unui pachet SQL. Localizarea unui obiect într-o bibliotecă sau într-un director.

Tabela 111. Descriere tipuri de autorizare (continuare)

Autorizare	Nume	Funcții permise
<i>Autorizări asupra unui câmp:</i>		
*MGT	Management - Gestionare	Specificarea securității câmpului.
*ALTER	Alter - Modificare	Modificarea atributelor câmpului.
*REF	Reference - Referință	Specificarea câmpului ca parte a cheii părinte într-o restricție referențială.
*READ	Read - Citire	Accesarea conținutului unui câmp. De exemplu, afișarea conținutului câmpului.
*ADD	Add - Adăugare	Adăugarea de intrări la date, precum adăugarea de informații la un anumit câmp.
*UPDATE	Update - Actualizare	Modificarea conținutului unor intrări existente într-un câmp.
¹	Dacă un utilizator are autorizarea specială *SAVSYS (save system - salvare sistem), atunci nu este necesară autorizarea de existență obiect pentru a efectua operații de salvare și restaurare asupra obiectului.	
²	Vedeți capitolul "Gestionarea listei de autorizare" la pagina 118 pentru mai multe informații.	

Autorizările folosite în mod obișnuit

Anumite seturi de autorizări asupra datelor și obiectelor sunt necesare în mod normal pentru a efectua operații asupra obiectelor. Puteți 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 folosiți autorizarea publică definită pentru obiect. Tabela 112 arată autorizările definite de sistem disponibile la folosirea comenzilor și ecranelor de autorizare obiect.

Tabela 112. Autorizare definită de sistem

Autorizare	*ALL	*CHANGE	*USE	*EXCLUDE
<i>Autorizări obiect</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Autorizări de date</i>				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

Tabela 113 arată autorizări suplimentare definite de sistem care sunt disponibile la folosirea comenzilor WRKAUT și CHGAUT:

Tabela 113. Autorizare definită de sistem

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Autorizări obiect</i>							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							

Tabela 113. Autorizare definită de sistem (continuare)

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Autorizări de date</i>							
*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 licență LAN Server folosește liste de control al accesului pentru a gestiona autorizările. Autorizările unui utilizator sunt numite **permisii**. Tabela 114 arată cum sunt mapate permisiunile LAN Server către autorizările de obiect și de date:

Tabela 114. Permisuniile LAN Server

Autorizare	Permisuniile LAN Server
*EXCLUDE	nici una
<i>Autorizări de obiect</i>	
*OBJOPR	Vedeți nota 1
*OBJMGT	Permisuniunea
*OBJEXIST	Creare, Ștergere
*OBJALTER	Atribut
*OBJREF	Fără echivalent
<i>Autorizări de date</i>	
*READ	Read - Citire
*ADD	Create - Creare
*UPD	Write - Scriere
*DLT	Delete - Ștergere
*EXECUTE	Execute - Execuție

¹ Numai dacă nu este specificat NONE pentru un utilizator în lista de control al accesului, utilizatorul primește în mod implicit autorizarea *OBJOPR.

Definirea informațiilor care pot fi accesate

Puteți defini securitatea de resursă pentru obiecte individuale din sistem. De asemenea puteți defini securitatea pentru grupuri de obiecte folosind ori securitatea de bibliotecă, ori o listă de autorizare:

Securitatea bibliotecii

Majoritatea obiectelor din sistem se află în bibliotecă. Pentru a accesa un obiect, vă trebuie autorizarea atât pentru obiectul însuși, cât și pentru bibliotecă în care se află obiectul. Pentru majoritatea operațiilor, inclusiv ștergerea unui obiect, autorizarea *USE pentru bibliotecă este suficientă (în plus față de autorizarea necesară pentru obiect). Crearea unui nou obiect necesită autorizarea *ADD pentru bibliotecă. Anexa D arată ce autorizare este necesară pentru comenzile CL pentru obiecte și pentru bibliotecile de obiecte.

Folosirea securității de bibliotecă este o tehnică pentru protejarea informațiilor păstrând în același timp o schemă de securitate simplă. De exemplu, pentru a securiza informațiile confidențiale pentru un set de aplicații, puteți face următoarele:

- Să folosiți o bibliotecă pentru a stoca toate fișierele confidențiale pentru un anumit grup de aplicații.
- Să asigurați că autorizarea publică este suficientă pentru toate obiectele (din bibliotecă) care sunt folosite de către aplicații (*USE sau *CHANGE).

- Să restricționați autorizarea publică doar la biblioteca însăși (*EXCLUDE).
- Să dați grupurilor selectate sau indivizilor selectați autorizarea pentru bibliotecă (*USE, sau *ADD dacă aplicațiile o cer).

Deși securitatea de bibliotecă este o metodă simplă și eficientă pentru protejarea informațiilor, ea poate să nu fie adecvată pentru date cu cerințe de securitate mare. Obiectele foarte sensibile ar trebui să fie securizate individual sau cu o listă de autorizare, în loc de a vă baza pe securitatea bibliotecii.

Securitatea bibliotecii și listele de biblioteci

Când o bibliotecă este adăugată la lista de biblioteci a utilizatorului, autorizarea pe care o are utilizatorul asupra bibliotecii este stocată împreună cu informațiile de listă bibliotecii. Autorizarea utilizatorului asupra bibliotecii rămâne pentru întregul job, chiar dacă autorizarea utilizatorului pentru bibliotecă este revocată în timp ce jobul este activ.

Când este cerut accesul la un obiect și este specificat *LIBL pentru obiect, informațiile din lista de biblioteci sunt folosite pentru a verifica autorizarea pentru bibliotecă. Dacă este specificat un nume calificat, autorizarea pentru bibliotecă este verificată în mod special, chiar dacă biblioteca este inclusă în lista de biblioteci a utilizatorului.

Atenție: Dacă un utilizator rulează sub autorizarea adoptată când este adăugată o bibliotecă la lista de biblioteci, utilizatorul rămâne autorizat pentru bibliotecă chiar dacă el nu mai rulează sub autorizarea adoptată. Aceasta reprezintă un potențial risc pentru securitate. Orice intrări adăugate la lista de biblioteci utilizatorului de către un program care rulează sub autorizarea adoptată ar trebui eliminate înainte ca programul cu autorizarea adoptată să se termine.

În plus, aplicațiile care folosesc liste de biblioteci în locul numelor calificate de biblioteci au un potențial risc de securitate. Un utilizator care este autorizat pentru comenzile de lucru cu liste de biblioteci poate rula o versiune diferită a unui program. Vedeți "Listele de biblioteci" la pagina 183 pentru mai multe informații.

Autorizările de câmp

Autorizările de câmp sunt acum suportate pentru fișierele bază de date. Autorizările suportate sunt Reference și Update. Puteți administra aceste autorizări doar prin instrucțiunile SQL GRANT și REVOKE. Puteți afișa aceste autorizări prin comenzile DSPOBJAUT (Display Object Authority - Afișare autorizare obiect) și EDTOBJAUT (Edit Object Authority - Editare autorizare obiect). Puteți afișa numai autorizările de câmp cu comanda EDTOBJAUT; nu le puteți edita.

```

                                Display Object Authority
Object . . . . . : PLMITXT      Owner . . . . . : PGMR1
  Library. . . . : RLN          Primary group . . : DPTAR
Object type. . . : *FILE        ASP Device . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE
-----Data-----
User      Group      Object Authority  Read  Add  Update  Delete  Execute
*PUBLIC   *PUBLIC  *CHANGE      X     X   X       X       X
PGMR1     *PUBLIC  *ALL         X     X   X       X       X
USER1     *PUBLIC  *USE         X     X   X       X       X
USER2     *PUBLIC  USER DEF     X     X   X       X       X
USER3     *PUBLIC  USER DEF     X     X   X       X       X

Press Enter to continue

F3=Exit  F11=Nondisplay detail F12=Cancel F16=Display field authorities

```

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

```

                                Display Field Authority
Object . . . . . : PLMITXT      Owner . . . . . : PGMR1
  Library . . . . : RLN          Primary group . . : *NONE
Object type . . . : *FILE

-----Field Authorities-----
Field  User      Object Authority  Mgt  Alter  Ref  Read  Add  Update
Field3 PGMR1     *ALL         X     X   X   X     X   X
        USER1   *Use         X     X   X   X     X   X
        USER2   USER DEF     X     X   X   X     X   X
        USER3   USER DEF     X     X   X   X     X   X
        *PUBLIC *CHANGE     X     X   X   X     X   X
Field4 PGMR1     *ALL         X     X   X   X     X   X
        USER1   *Use         X     X   X   X     X   X
        USER2   USER DEF     X     X   X   X     X   X
        USER3   USER DEF     X     X   X   X     X   X
        *PUBLIC *CHANGE     X     X   X   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 afișat promptul Position the List. Dacă este apăsat F16, va fi repetată operația anterioară de poziționare.

Suportul pentru autorizările de câmp include următoarele opțiuni:

- Comanda PRTPVTAUT (Print Private Authority - Tipărire autorizare privată) are un nou câmp care indică atunci când un fișier are autorizări de câmp.
- Comanda DSPOBJAUT (Display Object Authority - Afișare autorizare obiect) are acum un nou parametru Authority Type pentru a permite afișarea autorizărilor de obiect, autorizărilor de câmp, sau a tuturor autorizărilor. Dacă tipul de obiect nu este *FILE, puteți afișa doar autorizările de obiect.
- Informațiile oferite de API-ul QSYLUSRA (List Users Authorized to Object - Listare utilizatori autorizați pentru obiect) indică acum dacă un fișier 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 referință este realizat utilizând comanda GRTOBJAUT și ambele obiecte (cel cu permisiune și cel la care ne referim) sunt fișiere baze de date, toate câmpurile autorizate vor fi acordate unde numele câmpului se potrivește.
- Dacă o autorizare de utilizator la un fișier de bază de date este înlăturată, orice autorizare de câmp pentru acel utilizator este înlăturată.

Securitatea și mediul System/38

System/38 mediu și program CL al tipului CLP38 reprezintă o potențială 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 și 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. Totuși, el poate fi creat de oricine cu suficientă autorizare pentru a crea o bibliotecă.

Vedeți manualul *System/38 Environment Programming* pentru informații suplimentare despre Mediu System/38.

Recomandare pentru mediul System/38

Utilizați aceste măsuri pentru a vă proteja sistemul pentru Mediu System/38 și programe CL ale tipului CLP38:

- Verificați autorizării publice a bibliotecii QSYS38 și dacă este *ALL sau *CHANGE, atunci schimbați-o în *USE.
- Verificați autorizarea publică a bibliotecii QUSER38 și dacă este *ALL sau *CHANGE, atunci schimbați-o în *USE.
- Dacă nu există QUSER38 și QSYS38 atunci creați-le și setați-le cu autorizare *USE publică. Aceasta va împiedica alte persoane să o creeze la un moment ulterior și să își dea lor sau publicului o autorizare prea mare la ea.

Securitatea directorului

La accesarea unui obiect dintr-un director, trebuie să aveți autorizare la toate directoarele din calea care conține obiectul. Trebuie de asemenea să aveți autorizarea necesară la obiect pentru a realiza operația pe care ați cerut-o.

Ați putea dori să folosiți securitatea director în același mod în care folosiți securitatea bibliotecă. Limitați accesul la directoare și folosiți autorizare publică la obiectele din cadrul directorului. Limitarea numărului de autorizări private definite pentru obiecte îmbunătățește performanța procesului de verificare autorizare.

Securitatea listei de autorizare

Puteți grupa obiecte cu cerințe de securitate similare folosind o listă de autorizare. O listă de autorizare, conceptual, conține o listă de utilizatori și autorizarea pe care o au utilizatorii pentru obiectele asigurate de listă. Fiecare utilizator poate avea o autorizare diferită la setul de obiecte pe care le asigură lista. Când dați unui utilizator autorizare la lista de autorizare, sistemul de operare efectiv permite o **autorizare privată pentru acel utilizator** la lista de autorizare.

Puteți de asemenea să folosiți o listă de autorizare pentru a defini o autorizare publică pentru obiectele din listă. Dacă autorizarea publică pentru un obiect este setată pe *AUTL, obiectul își obține autorizarea publică din lista sa de autorizare.

Obiectul din lista de autorizare este folosit ca o unealtă de gestionare de către sistem. Ea conține în realitate o listă a tuturor obiectelor care sunt asigurate de lista de autorizare. Această informație este folosită pentru a construi ecrane pentru vizualizarea sau editarea obiectelor din lista de autorizare.

Nu puteți folosi o listă de autorizare pentru a asigura un profil utilizator sau altă listă de autorizare. Poate fi specificată o singură listă de autorizare pentru un obiect.

Doar proprietarul obiectului, un utilizator cu autorizare specială toate obiectele (*ALLOBJ) sau un utilizator cu autorizare tot (*ALL) la obiect, poate adăuga sau șterge lista de autorizare pentru un obiect.

Obiectele din biblioteca sistem (QSYS) pot fi asigurate cu o listă de autorizare. Totuși, numele listei de autorizare care asigură un obiect este stocat cu obiectul. În unele cazuri, când instalați o nouă ediție a sistemului de operare, toate obiectele din biblioteca QSYS sunt înlocuite. Asocierea dintre obiecte și lista de autorizare se pierde.

Vedeți subiectul “Planificarea listelor de autorizări” la pagina 212 pentru exemple de moduri de utilizare a listelor de autorizare.

Gestionarea listei de autorizare

Puteți acorda o autorizare operațională specială numită Gestionare listă autorizare (*AUTLMGT) pentru liste de autorizare. Utilizatorii cu autorizare *AUTLMGT au permisiunea de a adăuga și șterge autorizarea utilizatorilor la lista de autorizare și 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 șterge obiecte din listă.

Un utilizator cu autorizarea *AUTLMGT poate oferi doar aceeași autorizare sau mai mică altor utilizatori. De exemplu, presupuneți că USERA are autorizare *CHANGE și *AUTLMGT la lista de autorizare CPLIST1. USERA poate adăuga USERB la CPLIST1 și 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 șterge autorizarea pentru un utilizator dacă utilizatorul *AUTLMGT are autorizare egală sau mai mare la listă decât numele profilului de utilizator care este șters. Dacă USERC are autorizare *ALL la CPLIST1, atunci USERA nu îl poate șterge pe USERC din listă, deoarece USERA are doar *CHANGE și *AUTLMGT.

Folosirea listelor de autorizare pentru a asigura obiectele furnizate de IBM

Puteți alege să folosiți o listă de autorizare pentru a asigura obiecte furnizate de IBM. De exemplu, poate doriți să restricționați folosirea unui grup de comenzi câtorva utilizatori.

Obiectele din bibliotecile furnizate de IBM, altele decât bibliotecile QUSRSYS și QGPL, sunt înlocuite de fiecare dată când instalați o nouă ediție a sistemului de operare. Așadar, legătura dintre obiectele din bibliotecile furnizate de IBM și listele de autorizare este pierdută. De asemenea, dacă o listă de autorizare asigură un obiect din QSYS și este necesară o refacere sistem completă, legătura dintre obiectele din QSYS și lista de autorizare este pierdută. După ce instalați o nouă ediție sau restaurare a sistemului dvs., folosiți comanda EDTOBJAUT sau GRTOBJAUT pentru a restabili legătura dintre obiectul furnizat de IBM și lista de autorizare.

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 creați un obiect, parametrul AUT din comanda de creare determină autorizarea publică pentru obiect. Dacă valoarea lui AUT din comanda de creare este *LIBCRTAUT, care este implicită, autorizarea publică pentru obiect este setată la valoarea CRTAUT pentru bibliotecă.

De exemplu, presupuneți 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:
CRTDARA DARA(CUSTLIB/DTA1) +
TYPE(*CHAR) AUT(*LIBCRTAUT)
- Permitearea parametrului AUT să ia valoarea implicită. *LIBCRTAUT este implicit:
CRTDARA DARA(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, presupuneți că biblioteca ITEMLIB are o valoare CRTAUT de *SYSVAL. Această comandă creează zona de date DTA2 cu autorizarea publică de modificare:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

“Asignarea autorizării și dreptului de proprietate pentru noile obiecte” la pagina 124 arată mai multe exemple de moduri în care sistemul asignează drept de proprietate și 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 (MOV OBJ), creării duplicat (CRTDUPOBJ) sau restaurării a unui obiect în bibliotecă. Autorizarea publică a obiectului existent este folosită.

Dacă parametrul REPLACE (*YES) este folosit în comanda de creare, atunci autorizarea obiectului existent este folosită în loc de valoarea CRTAUT a bibliotecii.

Riscurile legate de crearea autorizării (CRTAUT)

Dacă aplicațiile dvs. folosesc autorizarea implicită pentru obiectele noi create în timpul procesării aplicației, ar trebui să controlați cine are autorizarea să schimbe descrierile bibliotecii. Schimbarea autorizării CRTAUT pentru o bibliotecă de aplicație poate permite accesul neautorizat la obiectele noi create în bibliotecă.

Autorizarea pentru obiecte noi într-un director

Când creați un nou obiect într-un director folosind comenzile CRTDIR, MD sau MKDIR, specificați autorizarea datelor și a obiectelor pe care le primește publicul pentru noul director. Dacă folosiți opțiunea *INDIR, autorizarea pentru directorul creat este determinată de directorul în care este creat. Altfel, puteți specifica autorizarea dorită.

- | Când creați un nou director folosind API-ul mkdir()--Make Directory, proprietarul, grup primar și autorizările publice de obiect pentru directorul creat sunt determinate din directorul în care este creat dar proprietarul, grup primar și autorizările publice de obiect sunt determinate de modul specificat în apelul API-ului.
- | Următoarele 2 exemple arată diferite rezultate când creați un nou director cu diferite opțiuni.
- | Primul exemplu creează un nou director folosind comanda CRTDIR în sistemul de fișiere "root"(/) și specifică autoritatea *PUBLIC.
- |

Condiții inițiale: Autorizările directorului părinte:

```
Afișare autorizare

Obiect . . . . . : /sandern/mytest
Proprietar . . . . . : SANDERS
Grup primar . . . . . : SANDERSGP3
Listă de autorizare . . . . . : *NONE

User          Date          -----Autorități obiect-----
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(/sandern/mytest/deletemepub) DTAAUT(*R) OBJAUT(*NONE)
```

Rezultate: Autoritățile directorului creat:

```
Afișare autorizare

Obiect . . . . . : /sandern/mytest/deletemepub
Proprietar . . . . . : SANDERS
Grup primar . . . . . : SANDERSGP3
Listă de autorizare . . . . . : *NONE

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

Note:

1. Autorizările date *PUBLIC și obiect sunt bazate pe parametrii DTAAUT și OBJAUT.
2. Autorizările de date ale proprietarului (SANDERS) sunt setate la *RWX dar autorizările de obiect sunt moștenite 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 cum toate autorizările sunt moștenite de la directorul părinte când creai un director nou folosind comanda CRTDIR în sistemul de fișiere "root"(/).

Condiții inițiale: Autorizările directorului părinte:

```
Afișare autorizare
Obiect . . . . . : /sandern/mytest
Proprietar . . . . . : SANDERS
Grup primar . . . . . : SANDERSGP3
Listă de autorizare . . . . . : *NONE

User      Data      -----Object Authorities-----
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(/sandern/mytest/deletemepub')

Rezultate: Autorizările directorului creat:

```
Afișare autorizare
Obiect . . . . . : /sandern/mytest/deletemepub
Proprietar . . . . . : SANDERSUSR
Grup primar . . . . . : SANDERSGP3
Listă de autorizare . . . . . : *NONE

User      Data      -----Object Authorities-----
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
```

Note:

1. Autorizările date *PUBLIC și obiect sunt moștenite de la directorul părinte; prin urmare, autorizarea de date este setată la *RWX cu toate autorizările obiect.
2. Autorizările de date ale proprietarului (SANDERSUSR) sunt setate la *RWX dar autorizările de obiect sunt moștenite 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 autorizați privat părintelui director (QPGMR, QTCM) și proprietarului directorului părinte (SANDERS) li se acordă autorizare privată noului director.

Dreptul de proprietate asupra obiectului

Fiecărui obiect îi este asignat un proprietar când este creat. Proprietarul este fie utilizatorul care creează obiectul, fie profilul de grup dacă profilul utilizator membru a specificat că profilul de grup ar trebui să fie proprietarul obiectului. Când este creat obiectul, proprietarului îi sunt date toate autorizările de date și de obiect la obiect. “Asignarea autorizării și dreptului de proprietate pentru noile obiecte” la pagina 124 arată exemple de moduri în care sistemul asignează drept de proprietate noilor obiecte.

Proprietarul unui obiect are întotdeauna toate autorizările pentru obiect, doar dacă nu este ștearsă una sau toate autorizările. Ca proprietar de obiect, puteți alege să ștergeți unele autorizări ca o măsură de precauție. De exemplu, dacă un fișier există care conține informații critice, puteți șterge autorizarea de existență a obiectului dvs. pentru a împiedica ștergerea accidentală a fișierului de către dvs. Totuși, ca proprietar de fișier, vă puteți oferi orice autorizare obiect în orice moment. Proprietarul unui obiect sistem de fișiere integrat are aceleași autorizări de obiect pentru acel obiect sistem de fișiere integrat ca proprietarul directorului părinte asupra directorului părinte. Verificați “Unelte și sugestii pentru iSeries” pentru a vedea dacă regulile pentru autorizările obiect se aplică tuturor sistemelor de fișiere sau doar unora.

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 deține obiecte dacă grupul are membrii.

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

Când schimbați proprietarul unui obiect, aveți opțiunea să păstrați sau să revocați autorizarea proprietarului anterior. Un utilizator cu autorizare *ALLOBJ poate transfera dreptul de proprietate, așa cum poate orice utilizator care are următoarele:

- Autorizare de existență obiect pentru obiect (cu excepția unei liste de autorizare)
- Dreptul de proprietate al obiectului, dacă obiectul este o listă de autorizare
- Autorizarea de Adăugare pentru profilul de utilizator al noului proprietar
- Autorizarea de Ștergere pentru profilul de utilizator al proprietarului actual

Nu puteți șterge un profil care deține obiecte. Dreptul de proprietate al obiectelor trebuie să fie transferat către un nou proprietar sau obiectele trebuie șterse înainte ca profilul să poată fi șters. Comanda Ștergere profil utilizator (DLTUSRPRF) vă permite să manipulați obiecte deținute când ștergeți profilul.

Dreptul de proprietate al obiectului este folosit ca o unealtă de gestionare de către sistem. Profilul de proprietar pentru un obiect conține o listă a tuturor utilizatorilor care au autorizare privată la obiect. Aceste informații sunt folosite pentru a construi ecrane pentru editarea sau vizualizarea autorizării obiectelor.

Profilurile care dețin multe obiecte cu multe autorizări private pot deveni foarte mari. Dimensiunea unui profil care deține multe obiecte afectează performanța la afișarea și la lucrul cu autorizarea la obiectele pe care le deține și la salvarea sau restaurarea profilurilor. Operațiile sistem pot fi afectate de asemenea. Pentru a împiedica impacturi asupra performanței sau operațiilor sistem, nu asigurați obiecte unui singur profil proprietar pentru întregul dvs. sistem iSeries. Fiecare aplicație și obiectele aplicației ar trebui deținute de un profil separat. De asemenea, profilurile utilizator furnizate de IBM nu ar trebui să dețină date utilizator sau obiecte.

Proprietarul unui obiect necesită de asemenea spațiu de stocare suficient pentru obiect. Vedeți “Spațiu de stocare maxim” la pagina 76 pentru mai multe informații.

Dreptul de proprietate al grupului asupra obiectelor

Când este creat un obiect, sistemul verifică profilul utilizatorului care a creat obiectul pentru a determina dreptul de proprietate al obiectului. Dacă utilizatorul este un membru al unui profil de grup, câmpul OWNER din profilul utilizator specifică dacă utilizatorul sau grupul ar trebui să dețină noul obiect.

Dacă grupul deține obiectul (OWNER este *GRPPRF), utilizatorului care creează obiectul nu îi este dat automat nici o autorizare specifică la obiect. Utilizatorul primește autorizare la obiect prin grup. Dacă utilizatorul deține obiectul (OWNER este *USRPRF), autorizarea grupului la obiect este determinată de câmpul GRPAUT din profilul utilizator.

Câmpul *tip autorizare grup* (GRPAUTYP) din profilul utilizator determină dacă grupul 1) devine grupul primar pentru obiect sau 2) îi este dată autorizare privată la obiect. “Asignarea autorizării și dreptului de proprietate pentru noile obiecte” la pagina 124 arată câteva exemple.

Dacă utilizatorul care deține obiectul se schimbă la un alt grup utilizator, profilul de grup original încă reține autorizarea la orice obiect creat.

Chiar dacă câmpul *Proprietar* dintr-un profil utilizator este *GRPPRF, utilizatorul trebuie să aibă încă suficient spațiu de stocare pentru a reține un obiect nou cât timp este creat. După ce este creat, dreptul de proprietate este transferat profilului de grup. Parametrul MAXSTG din profilul utilizator determină cât spațiu de stocare auxiliar îi este permis unui utilizator.

Evalueați obiectele pe care le poate crea un utilizator, cum sunt programele interogare, când alegeți între drept de proprietate utilizator individual sau grup:

- Dacă utilizatorul se mută în alt departament și alt grup utilizator, ar trebui ca utilizatorul să mai dețină încă obiectul?
- Este important de știut cine creează obiecte? Ecranele de autorizare obiect arată proprietarul obiectului, nu utilizatorul care a creat obiectul.

Notă: Ecranul Afișare descriere obiect arată creatorul obiectului.

Dacă funcția de jurnal auditare este activă, este scrisă o intrare Creare obiect (CO) în jurnalul de auditare QAUDJRN în momentul creării unui obiect. Această intrare identifică profilul utilizator creator. Intrarea este scrisă doar dacă valoarea de sistem QAUDLVL specifică *CREATE și valoarea de sistem QAUDCTL include *AUDLVL.

Grupul primar pentru un obiect

Puteți specifica un grup primar pentru un obiect. Numele profilului de grup primar și autorizarea grupului primar la obiect sunt stocate cu obiectul. Folosirea autorizării de grup primar poate furniza o performanță 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. Același profil nu poate fi proprietarul obiectului și grupul său primar.

Când un utilizator creează un obiect nou, parametrii din profilul utilizator controlează dacă grupul utilizatorului are autorizare la obiect și tipul autorizării este dat. Parametrul *Tip autorizare grup* (GRPAUTYP) dintr-un profil utilizator poate fi folosit pentru a face grupul utilizatorului grupul primar pentru obiect. “Asignarea autorizării și dreptului de proprietate pentru noile obiecte” la pagina 124 arată exemple de cum este asignată autorizarea când sunt create noi obiecte. Pentru un obiect bazat pe director în unele sisteme de fișiere, obiectul moștenește 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 același profil nu poate fi în același timp profil proprietar și grup primar pentru același obiect.

Puteți modifica grupul primar pentru un obiect bazat pe bibliotecă sau director utilizând oricare dintre următoarele comenzi:

- Comanda Change Object Primary Group (CHGOBJPGP)
- Comanda Change Primary Group (CHGPGP)
- Opțiunea 9 din grupul primar Lucru cu obiecte (WRKOBJPGP)

Puteți schimba autorizarea pe care o are grupul primar folosind ecranul Editare autorizare obiect sau comenzile acordare sau revocare autorizare. Puteți modifica autorizarea grupului primar pentru un obiect bazat pe bibliotecă sau director folosind comanda Change Authority (CHGAUT) sau comanda Work with Authority (WRKAUT)

Profilul de utilizator proprietar implicit (QDFTOWN)

Profilul utilizator Proprietar implicit (QDFTOWN) este un profil utilizator livrat de IBM care este folosit când un obiect nu are proprietar sau când dreptul de proprietate al unui obiect poate ridica o expunere de securitate. Urmează situațiile care fac ca dreptul de proprietate al unui obiect să fie asignat profilului QDFTOWN:

- Dacă un profil deținător devine deteriorat și este șters, obiectele sale nu mai au proprietar. Folosirea comenzii Pretindere spațiu de stocare (RCLSTG) asignează dreptul de proprietate al acestor obiecte profilului utilizator proprietar implicit (QDFTOWN).
- Dacă un obiect este restaurat și 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. Vedeți subiectul “Validarea programelor care sunt restaurate” la pagina 15 pentru mai multe informații despre ce condiții fac ca dreptul de proprietate să fie asignat lui QDFTOWN.
- Dacă limita de stocare maximă este depășită pentru profilul utilizator care deține un deținător de autorizare care are același nume ca fișierul care este mutat, redenumit sau a cărui bibliotecă este redenumită.

Sistemul furnizează profilul utilizator QDFTOWN deoarece toate obiectele trebuie să aibă un proprietar. Când sistemul este livrat, doar un utilizator cu autorizare specială *ALLOBJ poate afișa și accesa acest profil utilizator și transfera dreptul de proprietate al obiectelor asociate cu profilul utilizator QDFTOWN. Puteți acorda alte autorizări utilizator profilului QDFTOWN. Profilul utilizator QDFTOWN este destinat folosirii doar de către sistem. Nu ar trebui să proiectați securitatea dvs. astfel încât QDFTOWN să dețină normal obiectul.

Asignarea autorizării și dreptului de proprietate pentru noile obiecte

Sistemul folosește câteva valori pentru a asigna autorizare și drept de proprietate când un obiect nou este creat pe sistem:

Parametrii din comanda CRTxxx

Valoarea de sistem QCRTAUT

Valoarea CRTAUT a bibliotecii

Valorile din profilul utilizator al creatorului

Figura 6 până la Figura 9 arată câteva exemple de cum sunt folosite aceste valori:

Valoarea de sistem QCRTAUT:

*CHANGE

Parametrul bibliotecii CRTAUT:

*USE

Valorile din profilul USERA (Creator):

GRPPRF:

DPT806

OWNER:

*USRPRF

GRPAUT:

*CHANGE

GRPAUTTYP:

*PRIVATE

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

sau

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR)
```

Valorile pentru noul obiect:

Autorizare publică:

*USE

Autorizare proprietar:

USERA *ALL

autorizare grup primar:

nici una

autorizare privată:

DPT806 *CHANGE

Notă:

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

Figura 6. Exemplu de obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare privată dată

Valoarea de sistem QCRTAUT:

*CHANGE

Parametrul bibliotecii CRTAUT:

*SYSVAL

Valorile din profilul USERA (Creator):

GRPPRF:

DPT806

OWNER:

*USRPRF

GRPAUT:

*CHANGE

GRPAUTTYP:

*PRIVATE

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valorile pentru noul obiect:

Autorizare publică:

*CHANGE

Autorizare proprietar:

USERA *ALL

autorizare grup primar:

nici una

autorizare privată:

DPT806 *CHANGE

Figura 7. Exemplu de obiect nou: Autorizare publică din valoare de sistem, Grup cu autorizare privată dată

Valoarea de sistem QCRTAUT:

*CHANGE

Parametrul bibliotecii CRTAUT:

*USE

Valorile din profilul USERA (Creator):

GRPPRF:

DPT806

OWNER:

*USRPRF

GRPAUT:

*CHANGE

GRPAUTTYP:

*PGP

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valorile pentru noul obiect:

Autorizare publică:

*USE

Autorizare proprietar:

USERA *ALL

autorizare grup primar:

DPT806 *CHANGE

autorizare privată:

nici una

Figura 8. Exemplu de obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare de grup primar dată

Valoarea de sistem QCRTAUT:

*CHANGE

Parametrul bibliotecii CRTAUT:

*USE

Valorile din profilul USERA (Creator):

GRPPRF:

DPT806

OWNER:

*GRPPRF

GRPAUT:

GRPAUTTYP:

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*CHANGE)
```

Valorile pentru noul obiect:

Autorizare publică:

*CHANGE

Autorizare proprietar:

DPT806 *ALL

autorizare grup primar:

nici una

autorizare privată:

nici una

Figura 9. Exemplu de obiect nou: Autorizare publică specificată, Grupul deține obiectul

Obiecte care adoptă autorizarea proprietarului

Uneori un utilizator are nevoie de diferite autorizări la un obiect sau o aplicație, în funcție de situație. De exemplu, un utilizator poate avea voie să schimbe informația dintr-un fișier client când folosește programul aplicație care furnizează acea funcție. Totuși, același utilizator ar trebui să aibă permisiunea să vizualizeze, dar să nu modifice, informațiile client când folosește o unealtă de suport decizie, cum este SQL.

O soluție la această situație este 1) să dea utilizatorului autorizare *USE la informațiile client pentru a permite interogarea fișierelor și 2) să folosească autorizare adoptată în programele de întreținere clienți pentru a permite utilizatorului să modifice fișierele.

Când un obiect folosește autorizarea proprietarului, aceasta este numită **autorizare adoptată**. Obiectele de tipul *PGM, *SRVPGM, *SQLPKG și programele Java pot adopta autorizare.

Când creați un program, specificați un parametru profil utilizator (USRPRF) în comanda CRTxxxPGM. Acest parametru determină dacă programul folosește autorizarea proprietarului programului în plus față de autorizarea utilizatorului care rulează programul.

Consultați Centrul de informare cu privire la considerente de securitate și autorizare adoptată când folosiți pachete SQL (vedeți "Cerințe preliminare și informații înrudite" la pagina xvi pentru detalii).

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 operația 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 fișierul CUSTMST:
 - Autorizarea publică la fișierul CUSTMST este *USE.
 - Autorizarea lui USER1 este *EXCLUDE.
 - USER2 deține programul LSTCUST, care adoptă autorizarea proprietarului.
 - USER2 nu deține fișierul CUSTMST și nu are autorizare privată la el.
 - Deși autorizarea publică este suficientă pentru a îi da lui USER2 acces la fișierul CUSTMST, USER1 nu obține accesul. Autorizarea utilizator, autorizarea grup primar și autorizarea privată sunt folosite pentru autorizare adoptată.
 - Doar autorizarea este adoptată. Nici un alt atribut de profil utilizator nu este adoptat. De exemplu, atributele cu capabilități limitate nu sunt adoptate.
- Autorizarea adoptată este activă atât timp cât programul care folosește autorizarea adoptată rămâne în stiva de programe. De exemplu, presupuneți că PGMA folosește autorizare adoptată:
 - Dacă PGMA pornește PGMB folosind comanda CALL, acestea sunt stivele cu programe înainte și după comanda CALL:

Stiva de programe înainte de comanda CALL:	Stiva de programe după comanda CALL:
QCMD ⋮ PGMA	QCMD ⋮ PGMA PGMB

Figura 10. Autorizare adoptată și comanda CALL

Deoarece PGMA rămâne în stiva de programe după ce este apelat PGMB, PGMB folosește autorizarea adoptată a PGMA. (Parametrul Folosire autorizare adoptată (USEADPAUT) poate înlocui aceasta. Vedeți “Programe care ignoră autorizarea adoptată” la pagina 131 pentru mai multe informații despre parametrul USEADPAUT.)

- Dacă PGMA pornește PGMB folosind comanda Transferare control (TFRCTL), stivele programului arată astfel:

Stiva de programe înainte de comanda TFRCTL:	Stiva de programe după comanda TFRCTL:
QCMD ⋮ PGMA	QCMD ⋮ PGMB

Figura 11. Comanda TFRCTL și Autorizare adoptată

PGMB nu folosește autorizarea adoptată a lui PGMA, deoarece PGMA nu mai este în stiva de programe.

- Dacă programul care rulează sub autorizare adoptată este întrerupt, folosirea autorizării adoptate este suspendată. Următoarele nu folosesc autorizarea adoptată:
 - Cerere sistem
 - Tasta Atenție (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

– Funcții de depanare

Notă: Autorizarea adoptată este imediat întreruptă de tasta Atenție sau de o cerere job grup. Utilizatorul trebuie să aibă autorizare pentru programul de tratare a tastei atenție sau programul inițial de job grup, altfel încercarea eșuează.

De exemplu, USERA rulează programul PGM1, care adoptă autorizarea USERB. PGM1 folosește comanda SETATNPGM și specifică PGM2. USERB are autorizare *USE la PGM2. USERA are autorizare *EXCLUDE la PGM2. Funcția SETATNPGM are succes deoarece este rulată folosind autorizare adoptată. USERA primește o eroare de autorizare când încearcă să folosească tasta de atenție deoarece autorizarea lui USERB nu mai este activă.

- Dacă un program care folosește autorizare adoptată lansează un job, acel job lansat nu are autorizarea adoptată a programului lansator.
- Când un program declanșator sau un program punct de ieșire este apelat, autorizarea adoptată de la programele anterioare din stiva de apel nu va fi folosită ca o sursă de autorizare pentru programul declanșator sau programul punct de ieșire.
- Autorizarea adoptată nu este folosită de către sistemele de fișiere integrate, incluzând rădăcina, QOpenSzs, QDLS și sisteme de fișiere definite de utilizator.
- Funcție de adoptare program nu este folosită când folosiți comanda Schimbare job (CHGJOB) pentru a schimba coada de ieșire pentru un job. Profilul utilizator care face modificarea trebuie să aibă autorizare la noua coadă de ieșire.
- Orice obiect creat, inclusiv fișierele spool care pot conține date confidențiale, sunt deținute 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 aceleași valori USRPRF, USEADPAUT și AUT ca programul înlocuit. Parametrii USRPRF și AUT specificați în parametrul CRTxxxPGM sunt ignorați.
- Doar proprietarul programului poate specifica REPLACE(*YES) în comanda CRTxxxPGM când este specificat USRPRF(*OWNER) în programul original.
- Doar un utilizator care deține programul sau are autorizări speciale *ALLOBJ și *SECADM poate schimba valoarea parametrului USRPRF.
- Trebuie să fiți semnat ca utilizator cu autorizările speciale *ALLOBJ și *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 și *SECADM restaurează un program care adoptă autorizare, toate autorizările publice și private la program sunt revocate pentru a împiedica o posibilă expunere de securitate.

Comenzile Afișare program (DSPPGM) și Afișare program service (DSPSRVPGM) arată dacă un program adoptă autorizare (prompt *profil utilizator*) și dacă folosește autorizare adoptată de la programele anterioare din stiva de programe (prompt *Folosire autorizare adoptată*). Comanda Afișare 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 informații despre obiectele care adoptă autorizare. Această comandă furnizează de asemenea o opțiune de a tipări un raport pentru obiectele care s-au modificat de ultima dată de când a fost rulată comanda.

“Organigrama 8: Cum este verificată autorizarea adoptată” la pagina 159 furnizează mai multe informații despre autorizarea adoptată. Subiectul “Folosirea autorizării adoptate în proiectarea meniului” la pagina 203 arată un exemplu de cum să folosiți autorizarea adoptată într-o aplicație.

Autorizare adoptată și Programe legate:

Un program ILE* (*PGM) este un obiect care conține 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 și la toate programele service la care este legat. Dacă un program ILE folosește autorizare adoptată de la un program de mai sus în stiva de apel programe, care adoptă autorizarea este folosit pentru a verifica autorizarea la toate programele service la care programul ILE este legat. Dacă programul ILE adoptă autorizare, autorizarea adoptată nu va fi verificată când sistemul verifică autorizarea utilizatorului la programele service la momentul activării programului.

Riscurile și recomandările privind autorizarea adoptată

Permiterea unui program să ruleze folosind autorizare adoptată este o eliberare intenționată de control. Permiteți utilizatorului să aibă autorizări la obiecte, și posibil autorizări speciale, pe care în mod normal utilizatorul nu le-ar fi avut. Autorizarea adoptată furnizează o unealtă importantă pentru întrunirea diverselor cerințe de autorizare, dar ar trebui să fie folosită cu grijă:

- Adoptați autorizarea minimă necesară pentru a întruni cerințele aplicației. Adoptarea autorizării unui proprietar de aplicație este de preferat față de adoptarea autorizării QSECOFR sau a unui utilizator cu autorizare specială *ALLOBJ.
- Monitorizați cu grijă funcția oferită de programele care adoptă autorizarea. Asigurați-vă că aceste programe nu oferă un mijloc prin care utilizatorul să acceseze obiecte dinafara controlului programului, precum capabilități de introducere comenzi.
- Asigurați-vă că programele care adoptă autorizarea și apelează alte programe trebuie să efectueze un apel de bibliotecă calificat. Nu folosiți lista de biblioteci (library list - *LIBL) în apel.
- Controlați ce utilizatori au voie să apeleze programe care adoptă autorizarea. Folosiți interfețe de tip meniu și securitate de bibliotecă pentru a împiedica aceste programe de a fi apelate fără suficient control.

Programe care ignoră autorizarea adoptată

Ați putea dori ca unele programe să nu folosească autorizarea adoptată a programelor anterioare din stiva program. De exemplu, dacă folosiți un program inițial de tip meniu care adoptă autorizarea proprietarului, ați putea dori ca unele dintre programele apelate din programul meniu să folosească acea autorizare.

Parametrul use adopted authority (USEADPAUT) al programului determină dacă sistemul folosește autorizarea adoptată a programelor anterioare din stivă la verificarea autorizării pentru obiecte.

Când creați un program, valoarea implicită este de a adopta autorizarea de la programele anterioare din stivă. Dacă nu vreți ca programul să folosească autorizarea adoptată, puteți 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 aceleași valori USRPRF, USEADPAUT AUT ca și programul înlocuit.

Subiectul "Ignorarea autorizării adoptate" la pagina 205 arată un exemplu a modului de folosire a acestui parametru în proiectarea meniului. Vedeți "Folosirea autorizării adoptate (QUSEADPAUT)" la pagina 30 pentru informații despre valoarea de sistem QUSEADPAUT.

Atenție: În unele situații, puteți folosi instrucțiunea MI MODINVAU pentru a împiedica pasarea autorizării adoptate către funcțiile apelate. Instrucțiunea MODINVAU poate fi folosită pentru a împiedica transmiterea oricărei autorizări adoptate din programele C și C++ către funcțiile apelate din alt program sau program de serviciu. Acest lucru poate fi folositor când nu cunoașteți setarea USEADPAUT a funcției care este apelată.

Deținătorii de autorizare

Un deținător de autorizare este o unealtă pentru păstrarea autorizărilor pentru un fișier bază de date descris prin program care nu există în sistem. Utilizarea lui principală este pentru aplicațiile din mediul System/36, care adesea șterg fișiere descrise prin program și le creează din nou.

Un deținător de autorizare poate fi creat pentru un fișier care există deja sau pentru un fișier care nu există, folosind comanda Create Authority Holder (CRTAUTHLR). Următoarele se aplică la deținătorii de autorizare:

- Deținătorii de autorizare pot securiza doar fișiere din spațiul de stocare auxiliar al sistemului (auxiliary storage pool - ASP) sau un ASP utilizator de bază. Ei nu pot securiza fișiere dintr-un ASP independent.
- Deținătorul de autorizare este asociat cu un anumit fișier și bibliotecă. El are același nume ca și fișierul.
- Deținătorii de autorizare pot fi folosiți doar pentru fișiere bază de date descrise prin program și fișiere logice.
- O dată ce deținătorul de autorizare este creat, puteți adăuga autorizări private pentru el la fel ca la un fișier. Folosiți comenzile pentru a acorda, revoca și afișa autorizările de obiect și pentru a specifica tipul de obiect *FILE. În ecranele de autorizare obiect, un deținător de autorizare nu poate fi deosebit de fișierul propriu-zis. Ecranele nu indică dacă fișierul există și nici nu arată dacă fișierul are un deținător de autorizare.
- Dacă un fișier este asociat cu un deținător de autorizare, autorizările definite pentru deținătorul de autorizare sunt folosite în timpul verificării autorizării. Orice autorizări private definite pentru fișier sunt ignorate.
- Folosiți comanda Display Authority Holder (DSPAUTHLR) pentru a afișa sau tipări toți deținătorii de autorizare din sistem. O puteți de asemenea folosi pentru a crea un fișier de ieșire (output file - OUTFILE) pentru procesare.
- Dacă creați un deținător de autorizare pentru un fișier care există:
 - Utilizatorul care creează deținătorul de autorizare trebuie să aibă autorizarea *ALL pentru fișier.
 - Proprietarul fișierului devine proprietarul deținătorului de autorizare indiferent de utilizatorul care creează deținătorul de autorizare.
 - Autorizarea publică pentru deținătorul de autorizare provine de la fișier. Parametrul public authority (AUT) din comanda CRTAUTHLR este ignorat.
 - Autorizarea fișierului existent este copiată la deținătorul de autorizare.
- Dacă creați un fișier și există deja un deținător de autorizare pentru acel fișier:
 - Utilizatorul care creează fișierul trebuie să aibă autorizarea *ALL pentru deținătorul de autorizare.
 - Proprietarul deținătorului de autorizare devine proprietarul fișierului indiferent de utilizatorul care creează fișierului.
 - Autorizarea publică pentru fișier provine de la deținătorul de autorizare. Parametrul public authority (AUT) din comanda CRTPF sau CRTLF este ignorat.
 - Deținătorul de autorizare este legat de fișier. Autorizarea specificată pentru deținătorul de autorizare este folosită pentru a securiza fișierul.
- Dacă un deținător de autorizare este șters, informațiile de autorizare sunt transferate către fișierul însuși.
- Dacă un fișier este redenumit și noul nume de fișier corespunde cu un deținător de autorizare existent, autorizarea și dreptul de proprietate asupra fișierului sunt schimbate pentru a corespunde cu deținătorul de autorizare. Utilizatorul care redenumeste fișierul trebuie să aibă autorizarea *ALL pentru deținătorul de autorizare.
- Dacă un fișier este mutat în altă bibliotecă și un deținător de autorizare există pentru acel nume de fișier și bibliotecă destinație, atunci autorizarea și dreptul de proprietate asupra fișierului sunt schimbate pentru a corespunde cu deținătorul de autorizare. Utilizatorul care mută fișierul trebuie să aibă autorizarea *ALL pentru deținătorul de autorizare.
- Dreptul de proprietate asupra deținătorului de autorizare și asupra fișierului corespund întotdeauna. Dacă schimbați dreptul de proprietate asupra fișierului, atunci se schimbă și dreptul de proprietate asupra deținătorului de autorizare.
- Când un fișier este restaurat, dacă există un deținător de autorizare pentru acel nume de fișier și biblioteca în care este restaurat, el este legat de deținătorul de autorizare.
- Deținătorii de autorizare nu pot fi creați pentru fișierele din bibliotecile: QSYS, QRCL, QRECOVERY, QSPL, QTEMP și QSPL0002 – QSPL0032.

Deținătorii de autorizare și migrarea la System/36

Ajutorul de migrare la System/36 creează un deținător de autorizare pentru fiecare fișier care este migrat. El creează de asemenea un deținător de autorizare pentru intrările din fișierul de securitate resurse System/36 dacă nu există un fișier corespunzător în System/36.

Vă trebuie deținători de autorizare doar pentru fișierele care sunt șterse și re-create de aplicațiile dvs. Folosiți comanda Delete Authority Holder (DLTAUTHLR) pentru a șterge orice deținători de autorizare de care nu aveți nevoie.

Riscurile privind deținătorii de autorizare

Un deținător de autorizare oferă capacitatea de a defini autorizarea pentru un fișier înainte ca acel fișier să existe. În unele circumstanțe, aceasta poate permite unui utilizator neautorizat să obțină acces la informații. Dacă un utilizator ar ști că o aplicație ar crea, muta, sau redenumi un fișier, utilizatorul ar putea crea un deținător de autorizare pentru noul fișier. Utilizatorul astfel primește acces la fișier.

Pentru a limita acest risc, comanda CRTAUTHLR este livrată cu autorizarea publică *EXCLUDE. Doar utilizatorii cu autorizarea *ALLOBJ pot folosi comanda, doar dacă nu acordați autorizarea și altora.

Gestionarea autorizărilor

Această parte a capitolului prezintă metodele folosite în mod obișnuit pentru setarea, întreținerea și afișarea informațiilor de autorizare ale sistemului dumneavoastră. Anexa A, “Comenzile de securitate”, la pagina 271 oferă o listă completă de comenzi disponibile pentru lucrul cu autorizări. Descrierile care urmează nu discută toți parametrii comenzilor sau toate câmpurile din ecrane. Consultați informațiile online pentru detalii complete.

Ecrane pentru autorizare

Patru ecrane arată autorizările de obiect:

- Ecranul Afișare autorizare obiect
- Ecranul Editare autorizare obiect
- Ecranul Afișare autorizare
- Ecranul Gestionare autorizări

Această secțiune descrie unele caracteristici ale acestor ecrane. Figura 12 arată versiunea de bază a ecranului Afișare 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

User      Group      Object
*PUBLIC
PGMR1
DPTAR
DPTSM
F3=Exit F11=Display detail object authorities F12=Cancel F17=Top
Authority
*EXCLUDE
*ALL
*CHANGE
*USE
```

Figura 12. Ecranul Afișare autorizare obiect

Numele definite de sistem ale autorizărilor sunt arătate în acest ecran. F11 acționează ca un comutator între aceasta și 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

User      Group      Object Authority -----Object-----
*PUBLIC   Group      *EXCLUDE  Opr  Mgt  Exist  Alter  Ref
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

User      Group      Object Authority -----Data-----
*PUBLIC   Group      *EXCLUDE  Read  Add  Update  Delete  Execute
PGMR1     *ALL          X    X    X      X      X
DPTAR     *CHANGE      X    X    X      X      X
DPTSM     *USE         X

```

Dacă aveți autorizarea *OBJMGT asupra unui obiect, vedeți toate autorizările private pentru acel obiect. Dacă nu aveți autorizarea *OBJMGT, vedeți doar propriile dvs. surse de autorizare pentru acel obiect.

De exemplu, dacă USERA afișează autorizarea pentru zona de date CUSTNO, este arătată doar autorizarea publică.

Dacă USERB, care este un membru al profilului de grup DPTAR, afișează 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

User      Group      Object Authority
*GROUP    DPTAR     *CHANGE

```

Dacă USERB rulează un program care adoptă autorizarea lui PGMR1 și afișează 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

User      Group      Object
*ADOPTED          Authority
*PUBLIC          USER DEF
PGMR1            *EXCLUDE
*GROUP          DPTAR  *ALL
DPTSM           *CHANGE
                *USE

```

Autorizarea *ADOPTED indică doar autorizarea suplimentară primită de la proprietarul programului. USERB primește 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

User      Group      Object      -----Object-----
Authority  Opr  Mgt  Exist  Alter  Ref
*ADOPTED          USER DEF      X    X    X    X
*PUBLIC          *EXCLUDEPGMR1
                *ALL          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 - opțiune utilizator) din profilul utilizatorului USERB include *EXPERT, atunci ecranul va arăta astfel:

Display Object Authority

```
Object . . . . . : CUSTNO      Owner . . . . . : PGMR1
Library. . . . . : CUSTLIB     Primary group . . . : DPTAR
Object type. . . . : *DTAARA   ASP device . . . . . : *SYSBAS

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

User	Group	OBJECT Authority	-----Object-----					-----Data-----				
			O	M	E	A	R	R	A	U	D	E
*ADOPTED		USER DEF		X	X	X	X					
*PUBLIC		*EXCLUDE										
PGMR1		*ALL	X	X	X	X	X	X	X	X	X	X
*GROUP	DPTAR	*CHANGE	X					X	X	X	X	X
DPTSM		*USE	X					X				X

Rapoarte pentru autorizare

Sunt disponibile mai multe rapoarte pentru a vă ajuta să monitorizați implementarea dvs. de securitate. De exemplu, puteți monitoriza obiectele cu autorizarea *PUBLIC diferită de *EXCLUDE și obiectele cu autorizările private cu următoarele comenzi:

- PRTPUBAUT (Print Public Authority - Tipărire autorizare publică)
- PRTPVTAUT (Print Private Authority - Tipărire autorizare privată)

Pentru mai multe informații despre unelte de securitate, vedeți *Tips and Tools for Securing Your iSeries*.

Gestionarea bibliotecilor

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 însăși, nu la obiectele din bibliotecă. Dacă specificați un nume de listă de autorizare, autorizarea publică pentru bibliotecă este setată la *AUTL.

Dacă nu specificați AUT când creați o bibliotecă, *LIBCRTAUT este valoarea implicită. Sistemul folosește 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 valoare numele unei liste de autorizare.

Notă: Puteți 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

User      Group      Object
*PUBLIC   Group      Authority
PGMR1     *PUBLIC   *AUTL
           PGMR1     *ALL

```

- Deoarece a fost specificată o listă de autorizare în parametrul AUT, autorizarea publică este setată la *AUTL.
- Utilizatorul care a introdus comanda CRTLIB este proprietarul bibliotecii, doar dacă profilul utilizatorului nu specifică OWNER(GRPPRF). Proprietarul primește în mod automat autorizarea *ALL.
- Valoarea CRTAUT nu este arătată în ecranele autorizării obiect. Folosiți comanda DSPLIBD (Display Library Description - Afisare descriere bibliotecă) pentru a vedea valoarea CRTAUT pentru o bibliotecă.

```

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

```

Crearea obiectelor

Când creați un nou obiect, puteți ori să specificați autorizarea (AUT), ori să folosiți 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

User      Group      Object
*PUBLIC   Group      Authority
PGMR1     *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      Proprietar . . . . . : PGMR1  
Library . . . . . : TESTLIB   Primary group . . . . : *NONE  
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS  
  
Object secured by authorization list . . . . . : *NONE  
  
User      Group      Object  
*PUBLIC   Group      Authority  
PGMR1    *CHANGE  
          *ALL
```

Gestionarea autorizării de obiect individuale

Pentru a schimba autorizarea pentru un obiect trebuie să aveți una dintre următoarele:

- Autorizarea *ALLOBJ sau apartenența la un profil de grup care are autorizarea specială *ALLOBJ.

Notă: Autorizarea grupului nu este folosită dacă aveți autorizare privată pentru obiect.

- Proprietatea asupra obiectului. Dacă un profil de grup deține obiectul, atunci orice membru al grupului poate acționa ca proprietar al obiectului, doar dacă membrul nu a primit o autorizare specifică și care nu îndeplinește cerințele pentru schimbarea autorizării obiectului.
- Autorizarea *OBJMGT pentru obiect și orice autorizări care sunt acordate sau revocate (cu excepția *EXCLUDE). Orice utilizator căruia îi este permis să lucreze cu autorizarea obiectului poate acorda sau revoca autorizarea *EXCLUDE.

Cea mai ușoară 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 opțiune 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  
  
User      Group      Object  
*PUBLIC   Group      Authority  
PGMR1    *AUTL  
          *ALL
```

De asemenea puteți 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 folosiți comenzile CHGAUT sau WRKAUT.

Specificarea unei autorizări definite de utilizator

Coloana Autorizare obiect din ecranul Editare autorizare obiect vă permite să specificați oricare dintre seturile de autorizări definite de sistem (*ALL, *CHANGE, *USE, *EXCLUDE). Dacă vreți să specificați o autorizare care nu este dintr-un set definit de sistem, folosiți F11 (Display detail - Afișare detalii).

Notă: Dacă valoarea câmpului *Opțiuni utilizator* (USROPT) din profilul dvs. de utilizator este setată pe *EXPERT, atunci veți vedea întotdeauna această versiune detaliată a ecranului fără a trebui să apăsați F11.

De exemplu, PGMR1 șterge autorizarea *OBJEXIST pentru fișierul CONTRACTS, pentru a împiedica ștergerea accidentală a fișierului. Deoarece PGMR1 are o combinație 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

User      Group      Object Authority  Opr Mgt Exist Alter Ref
*PUBLIC
PGMR1     USER DEF      X   X           X   X

```

Puteți apăsa F11 (Display data authorities - Afișare 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

User      Group      Object Authority  Read Add Update Delete Execute
*PUBLIC
PGMR1     USER DEF      X   X   X       X       X

```

Acordarea de autorizări noilor utilizatori

Pentru a acorda autorizare utilizatorilor suplimentari, apăsați F6 (Add new users - Adăugare noi utilizatori) din ecranul Editare autorizare obiect. Veți vedea fereastra de dialog Adăugare utilizatori noi, care vă permite să definiți autorizarea pentru mai mulți utilizatori:

```
                                Add New Users

Object . . . . . : DTA1
Library . . . . . : TESTLIB

Type new users, press Enter.

User      Object
          Authority
USER1     *USE
USER2     *CHANGE
PGMR2     *ALL
```

Ștergerea autorizării pentru un utilizator

Ștergerea 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 și 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.

Ștergerea autorizării unui utilizator înseamnă că utilizatorul nu are nici o autorizare specifică asupra obiectului. Utilizatorul poate obține 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.

Puteți șterge autorizarea unui utilizator prin folosirea ecranului Editare autorizare obiect. Tastați niște spații albe (blancuri) în câmpul Autorizare obiect pentru acel utilizator și apăsați tasta Enter. Utilizatorul este eliminat din ecran. De asemenea puteți folosi comanda Revoke Object Authority (RVKOBJAUT). Ori revocați autorizare specifică pe care o are utilizatorul, ori revocați autorizarea *ALL pentru acel utilizator.

Notă: Comanda RVKOBJAUT revocă doar autorizarea pe care o specificați. De exemplu, USERB are autorizarea *ALL pentru FILEB din biblioteca LIBB. Dvs. revocați 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

User      Group      Object
          Authority  -----Object-----
USERB     USER DEF    Opr Mgt Exist Alter Ref
X         X         X   X   X   X   X
```

```

Display Object Authority
Object . . . . . : FILEB   Owner . . . . . : PGMR1
Library. . . . . : LIBB    Primary group . . . : *NONE
Object type . . . : *FILE   ASP device . . . . . : *SYSBAS

Obiecte securizate printr-o listă de autorizații . . . . . *NONE

User   Group   Authority Read  Add Update Delete Execute
USERB          USER DEF

```

Gestionarea autorizării pentru mai multe obiecte

Ecranul Editare autorizare obiect vă permite să lucrați în mod interactiv cu autorizarea pentru un obiect la un moment dat. Comanda GRTOBJAUT (Grant Object Authority - Acordare autorizare obiect) vă permite să faceți schimbări de autorizare asupra mai multor obiecte la un moment dat. Puteți folosi comanda de autorizare GRTOBJAUT în mod interactiv sau în batch. De asemenea o puteți apela dintr-un program.

În continuare sunt date exemple de folosire a comenzii GRTOBJAUT, care arată ecranul prompt. Când este rulată comanda, dumneavoastră primiți un mesaj pentru fiecare obiect care indică dacă schimbarea a fost efectuată. Schimbările de autorizare necesită un lacăt exclusiv asupra obiectului și nu pot fi făcute atunci când obiectul este folosit deja. Tipăriți istoricul dvs. de job pentru evidența schimbărilor încercate și 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 specificați, dar nu șterge 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, folosiți comanda GRTOBJAUT cu parametrul REPLACE.

```

GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
USER(*PUBLIC) REPLACE(*YES)

```

Parametrul REPLACE indică dacă autorizările pe care le specificați înlocuiesc autorizarea existentă pentru acel utilizator. Valoarea implicită REPLACE(*NO) acordă autorizarea pe care o specificați, dar nu șterge nici o autorizare care este mai mare decât autorizarea specificată de dvs., decât dacă acordați 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, folosiți parametrul CRTAUT în descrierea bibliotecii.

- Pentru a da autorizarea *ALL fișierelor de lucru din biblioteca TESTLIB pentru utilizatorii AMES și SMITHR. În acest exemplu, numele fișierelor 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 folosește un nume generic pentru a specifica fișierele. Puteți specifica un nume generic prin tastarea unui șir de caractere urmat de un asterisc (*). Informațiile de ajutor online vă spun ce parametri ai unei comenzi acceptă ca valoare un nume generic.

- Pentru a securiza toate fișierele care încep caracterele AR* folosind o listă de autorizare numită ARLST1 și să faceți ca fișierele să își obțină autorizarea publică din acea listă, folosiți următoarele două comenzi:
 1. Securizarea fișierelor cu lista de autorizare folosind comanda GRTOBJAUT:

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
  Library . . . . . TESTLIB
Object type . . . . . *FILE
ASP device . . . . . *
:
Authorization list . . . . . ARLST1

```

2. Setarea autorizării publice pentru fișierele cu *AUTL, folosind comanda GRTOBJAUT:

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
  Library . . . . . TESTLIB
Object type . . . . . *FILE
ASP device . . . . . *
Users . . . . . *PUBLIC
                + for more values
Authority . . . . . *AUTL

```

Gestionarea proprietății asupra obiectelor

Pentru a schimba dreptul de proprietate asupra unui obiect, folosiți 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 deținute de un profil de utilizator. Puteți asigna obiecte individuale unui nou proprietar. De asemenea puteți schimba dreptul de proprietate pentru mai multe obiecte în același timp prin folosirea parametrului NEWOWN (new owner - nou proprietar) de la baza ecranului:

```
Work with Objects by Owner
User profile . . . . . : OLDDOWNER
Type options, press Enter.
  2=Edit authority      4=Delete   5=Display author
  8=Display description 9=Change owner
Opt Object      Library      Type      Attribute      ASP
COPGMMSG COPGMLIB *MSGQ
9 CUSTMAS      CUSTLIB *FILE
9 CUSTMSGQ     CUSTLIB *MSGQ
ITEMMSGQ  ITEMLIB *MSGQ
ASP
Device
*SYSBAS
*SYSBAS
*SYSBAS
*SYSBAS
Parameters or command
====> NEWOWN(OWNIC)
F3=Exit  F4=Prompt  F5=Refresh  F9=Retrieve
F18=Bottom
```

Când schimbați proprietatea folosind oricare dintre metode, puteți alege să ștergeți 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 aveți:

- Autorizarea existență 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 Ștergere pentru profilul de utilizator al proprietarului actual

Nu puteți șterge un profil de utilizator care deține obiecte. Subiectul “Ștergerea profilurilor de utilizator” la pagina 101 arată metode pentru manevrarea obiectelor deținute la ștergerea unui profil.

Ecranul Work with Objects by Owner (Gestionare obiecte după proprietar) include obiecte din sistemul de fișiere integrat. Pentru aceste obiecte, coloana *Object* din ecran arată primele 18 caractere ale numelui căii. Dacă numele căii este mai lung de 18 caractere, atunci apare un simbol mai mare (>) la sfârșitul numelui căii. Pentru a vedea întregul nume al căii, plasați cursorul oriunde în numele căii și apăsați tasta F22.

Gestionarea autorizării de grup primar

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

Change Object Primary Group (CHGOBJPGP)

Work with Objects by Primary Group (WRKOBJPGP)

Change Primary Group (CHGPGP)

Când schimbați grupul primar al unui obiect, specificați ce autorizare are noul grup primar. De asemenea, puteți revoca autorizarea vechiului grup primar. Dacă nu revocați 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 aveți următoarele:

- autorizarea *OBJEXIST pentru obiect.
- Dacă obiectul este un fișier, o bibliotecă sau o descriere subsistem, vă trebuie autorizările *OBJOPR și *OBJEXIST.
- Dacă obiectul este o listă de autorizare, vă trebuie autorizarea specială *ALLOBJ sau trebuie să fiți proprietarul listei de autorizare.
- Dacă revocați autorizarea pentru vechiul grup primar, vă trebuie autorizarea *OBJMGT.
- Dacă este specificată o valoare diferită de *PRIVATE, vă trebuie autorizarea *OBJMGT și toate autorizările care sunt date.

Folosirea unui obiect referit

Atât ecranul Edit Object Authority (Editare autorizare obiect) cât și comanda GRTOBJAUT vă permit să dați autorizare pentru un obiect (sau grup de obiecte) pe baza autorizării unui obiect referit. Acesta este un instrument folositor în unele situații, dar ar trebui să evaluați de asemenea folosirea unei liste de autorizare pentru îndeplinirea cerințelor dvs. Vedeti “Planificarea listelor de autorizări” la pagina 212 pentru informații despre avantajele folosirii unei liste de autorizare.

Copierea autorizării de la un utilizator

Puteți 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 situații. De exemplu, dacă sistemul nu vă permite să redenumiți un profil de utilizator. Pentru a crea un profil identic dar cu alt nume sunt implicați câțiva pași, incluzând copierea autorizărilor profilului original. “Redenumirea unui profil de utilizator” la pagina 106 arată un exemplu cum puteți face asta.

Comanda GRTUSRAUT copiază doar autorizările private. Ea nu copiază autorizările speciale; și 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 crește timpul necesar pentru a salva sistemul și face gestiunea autorizărilor mult mai dificilă. GRTUSRAUT copiază autorizările care există la un moment dat. Dacă este necesară autorizarea pentru noi obiecte pe viitor, atunci fiecare profil trebuie să primească autorizarea în mod individual. Profilul de grup oferă această funcție în mod automat.

Pentru a folosi comanda GRTUSRAUT, trebuie să aveți toate autorizările care sunt copiate. Dacă nu aveți o autorizare, atunci acea autorizare nu este acordată profilului destinație. Sistemul emite câte un mesaj pentru fiecare autorizare care este acordată sau nu este acordată profilului de utilizator destinație. Tipăriți istoricul de job pentru a avea evidența completă. Pentru a evita copierea unui set parțial de autorizări, comanda GRTUSRAUT ar trebui rulată de un utilizator care are autorizarea specială *ALLOBJ.

Gestionarea listelor de autorizare

Setarea unei liste de autorizare necesită trei pași:

1. Crearea listei de autorizare.
2. Adăugarea utilizatorilor la lista de autorizare.
3. Securizarea obiectelor cu lista de autorizare.

Pașii 2 și 3 pot fi făcuți în orice ordine.

Crearea unei liste de autorizare

Nu vă trebuie nici o autorizare pentru biblioteca QSYS pentru a crea o listă de autorizare în acea bibliotecă. Folosiți comanda Create Authorization List (CRTAUTL):

```

Create Authorization List (CRTAUTL)

Type choices, press Enter.

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

Additional Parameters

Authority . . . . . *use

```

Parametrul AUT setează autorizarea publică pentru orice obiecte securizate de către listă. Autorizarea publică din lista de autorizare este folosită doar atunci când autorizarea publică pentru un obiect securizat de listă este *AUTL.

Acordarea către utilizatori a autorizării pentru o listă de autorizare

Pentru a lucra cu autorizarea pe care o au utilizatorii asupra listei de autorizare, trebuie să aveți autorizarea *AUTLMGT (authorization list management - gestiune listă de autorizare), precum și autorizările specifice pe care le acordați. Vedeți subiectul “Gestionarea listei de autorizare” la pagina 118 pentru o descriere completă.

Puteți 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.

User      Object  List
          Authority Mgt
*PUBLIC   *USE
PGMR1     *ALL    X

```

Pentru a acorda noilor utilizatori autorizare asupra listei de autorizare, apăsați F6 (Adăugare noi utilizatori):

```

Add New Users

Object . . . . . : CUSTLST1      Owner . . . PGMR1
Library . . . . . : QSYS

Type new users, press Enter.

User      Object  List
          Authority Mgt
AMES      *CHANGE
SMITHR    *CHANGE

```

Autorizarea fiecărui utilizator asupra listei este de fapt stocată ca o autorizare privată în profilul celui utilizator. Puteți folosi de asemenea comenzi pentru a lucra cu utilizatori ai listei de autorizare, ori în mod interactiv, ori în lot (batch):

- Folosiți 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.
- Folosiți Remove Authorization List Entry (RMVAUTLE) pentru a șterge autorizarea unui utilizator asupra listei.
- Work with Authority (WRKAUT) pentru a arăta lista utilizatorilor autorizați 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 fiți proprietarul obiectului, să aveți autorizarea *ALL asupra lui, sau să aveți autorizarea specială *ALLOBJ .

Folosiți ecranul Edit Object Authority sau comanda GRTOBJAUT, sau comanda WRKAUT, sau comanda CHGAUT, sau comanda GRTOBJAUT pentru a securiza un obiect cu o listă de autorizare:

```

                                Edit Object Authority

Object . . . . . : ARWRK1      Owner . . . . . : PGMR1
Library . . . . . : TESTLIB    Primary group. . . . . : *NONE
Object type . . . . . : *FILE   ASP device . . . . . : *SYSBAS

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . ARLST1

User      Object
          Authority
*PUBLIC   *AUTL
PGMR1     *ALL

```

Setați autorizarea publică pentru obiect la *AUTL dacă vreți ca autorizarea publică să vină din lista de autorizare.

În ecranul Editare listă de autorizare, puteți folosi F15 (Display authorization list objects - Afișare obiecte din lista de autorizare) pentru a lista toate obiectele securizate de către listă:

```

                                Display Authorization List Objects

Authorization list . . . . . : CUSTLST1
Library . . . . . : CUSTLIB
Owner . . . . . : OWNAR
Primary group . . . . . : DPTAR

Object  Library  Type  Owner  Primary  Text
CUSTMAS CUSTLIB  *FILE OWNAR
CUSTADDR CUSTLIB  *FILE OWNAR

```

Aceasta este doar o listă informativă. Nu puteți adăuga sau șterge obiecte din listă. Puteți folosi de asemenea comanda Display Authorization List Objects (DSPAUTOBJ) pentru a vizualiza sau tipări o listă cu toate obiectele securizate de către listă.

Ștergerea unei liste de autorizare

Nu puteți șterge o listă de autorizare dacă este folosită pentru a securiza obiecte. Folosiți comanda DSPAUTOBJ pentru lista tuturor obiectelor securizate de către listă. Folosiți ori ecranul Editare autorizare obiect ori comanda

Revocare autorizare obiect (RVKOBJAUT) pentru a schimba autorizarea pentru fiecare obiect. Când lista de autorizare nu mai securizează nici un obiect, folosiți comanda DLTAUTL (Delete Authorization List - Ștergere listă de autorizare) pentru a o șterge.

Cum verifică sistemul autorizarea

Când un utilizator încearcă să efectueze o operație asupra unui obiect, sistemul verifică dacă utilizatorul are autorizarea adecvată pentru operație. Sistemul verifică mai întâi autorizarea pentru biblioteca sau calea director care conține obiectul. Dacă autorizarea pentru bibliotecă sau director este adecvată, sistemul verifică autorizarea asupra obiectului însuși. În cazul fișierelor bază de date, verificarea autorizării este făcută la momentul deschiderii fișierului, nu când este efectuată fiecare operație individuală asupra fișierului.

În timpul procesului de verificare a autorizării, când este găsită o autorizare (chiar dacă nu este adecvată pentru operația cerută) verificarea autorizării se oprește și accesul este acordat sau respins. Funcția de autorizare adoptată este o excepție de la această regulă. Autorizarea adoptată poate trece peste orice autorizare specifică (și inadecvată) care este găsită. Vedeți subiectul “Obiecte care adoptă autorizarea proprietarului” la pagina 128 pentru mai multe informații despre autorizarea adoptată.

Sistemul verifică autorizarea unui utilizator asupra unui obiect în următoarea ordine:

1. Autorizarea asupra obiectului - calea rapidă
2. Autorizarea specială *ALLOBJ a utilizatorului
3. Autorizarea specifică a utilizatorului asupra obiectului
4. Autorizarea utilizatorului asupra listei de autorizare care securizează obiectul
5. Autorizarea specială *ALLOBJ a grupurilor
6. Autorizarea grupurilor asupra obiectului
7. Autorizarea grupurilor asupra listei de autorizare care securizează obiectul
8. Autorizarea publică specificată pentru obiect sau pentru lista de autorizare care securizează obiectul
9. Autorizarea proprietarului programului, dacă este folosită autorizarea adoptată

Notă: Autorizarea de la unul sau mai multe dintre grupurile utilizatorului poate fi acumulată pentru a găsi o autorizare suficientă pentru obiectul accesat.

Diagramele de flux pentru verificarea autorizării

În continuare sunt date niște diagrame, descrieri și exemple legate de modul în care este verificată autorizarea. Folosiți-le pentru a răspunde la întrebări specifice legate de funcționarea unei scheme de autorizare particulară sau pentru a diagnostica probleme legate de definițiile dvs. de autorizare. Diagramele evidențiază de asemenea tipurile de autorizare care produc cel mai mare efect asupra performanțelor.

Procesul de verificare a autorizării este împărțit într-o diagramă de flux primară și mai multe diagrame de flux mai mici care arată părți specifice ale procesului. În funcție de combinația de autorizări pentru un obiect, pașii din unele diagrame de flux pot fi repetați 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.

Pașii care reprezintă căutarea autorizărilor private ale unui profil sunt evidențiați:

Pasul 6 din Organigrama 3 la pagina 151

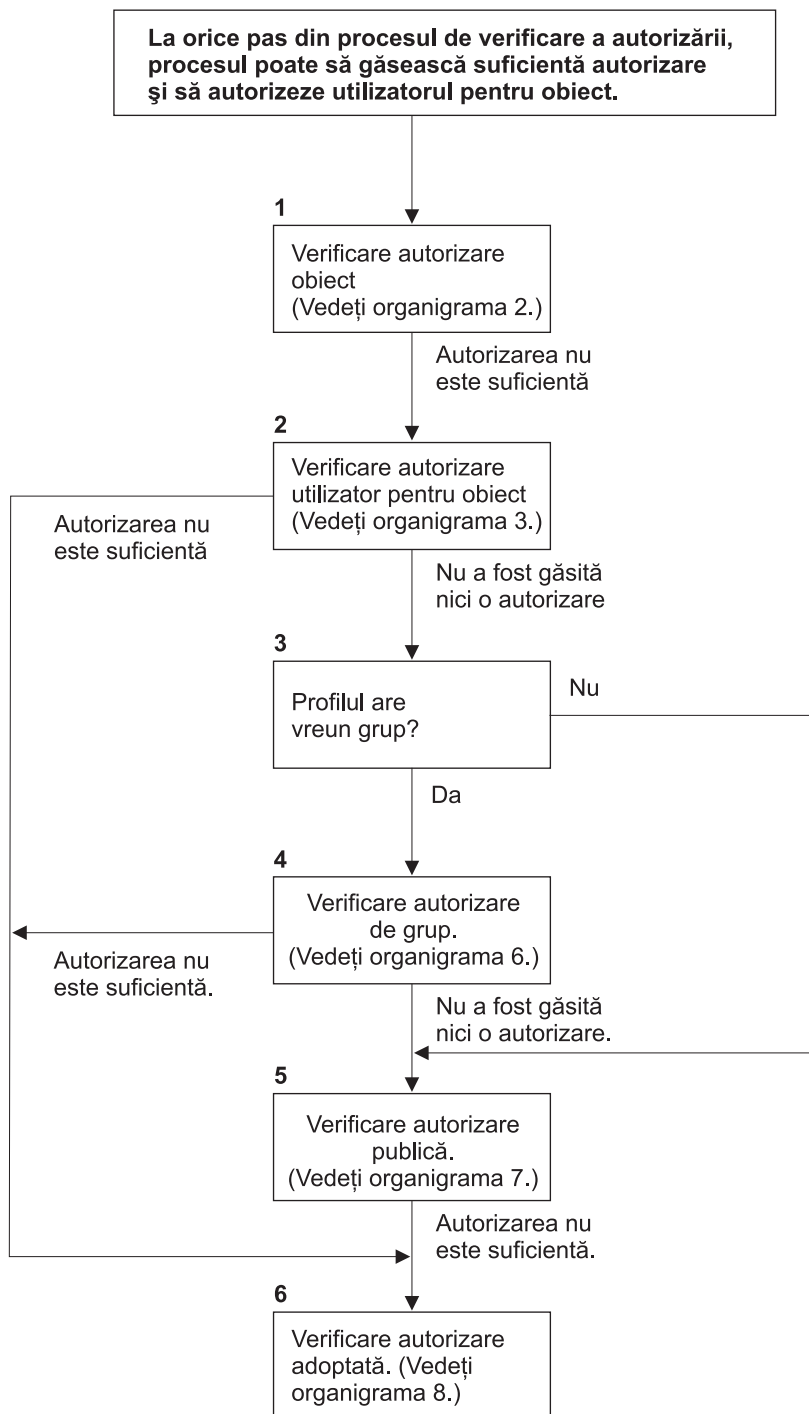
Pasul 6 din Organigrama 6 la pagina 157

Pasul 2 din Organigrama 8 B la pagina 162

Repetarea acestor pași este probabil să cauzeze probleme de performanță în procesul de verificare a autorizării.

Organigrama 1: Procesul principal de verificare a autorizării

Pașii din Organigrama 1 arată procesul principal pe care sistemul îl urmează 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 programului;
- 2) Programul eșuează;
- 3) Este scrisă o intrare AF jurnalul de auditare.

RBAFW508-0

Figura 13. Organigrama 1: Procesul principal de verificare a autorizării

Descrierea pentru Organigrama 1: Procesul principal de verificare a autorizării

Notă: La orice pas din cadrul procesului de verificare a autorizării, sistemul poate găsi o autorizare suficientă și poate autoriza utilizatorul să acceseze obiectul.

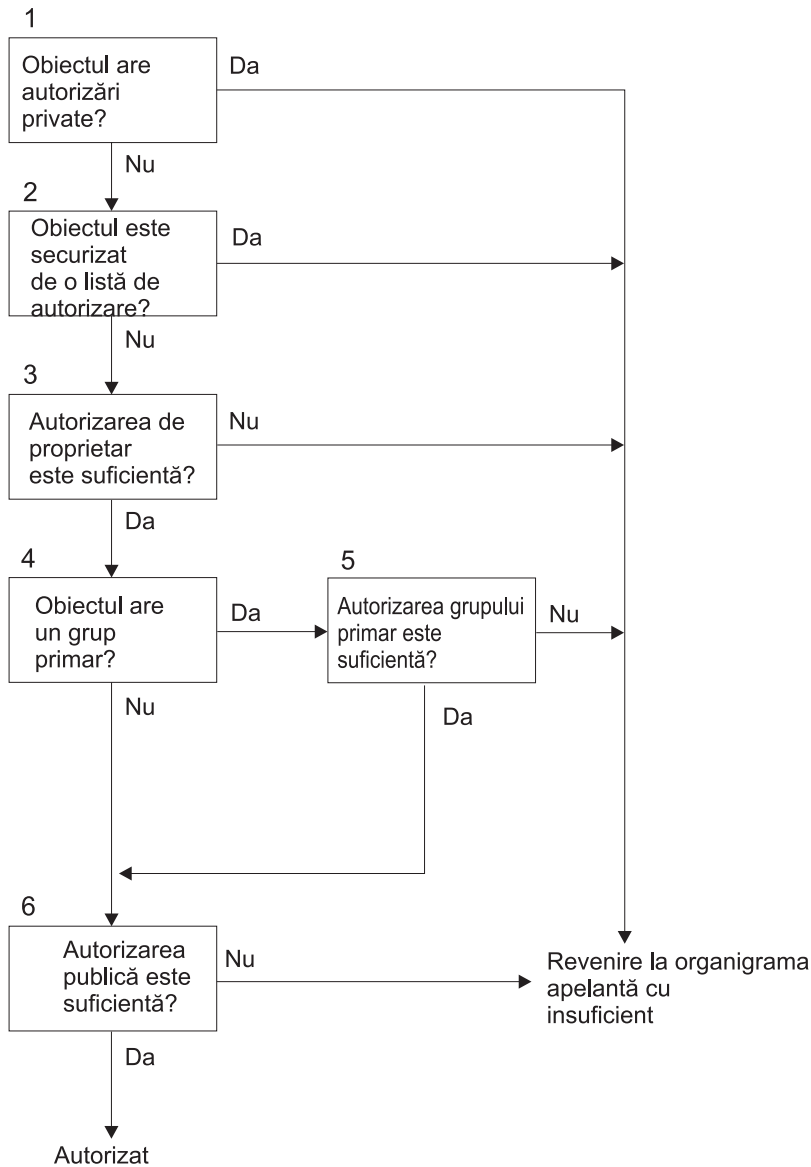
1. Sistemul verifică autorizarea obiectului. (Vedeți diagrama de flux 2: Calea rapidă pentru verificarea autorizării obiectului.) Dacă sistemul găsește că autorizarea este insuficientă, el continuă cu Pasul 2.
2. Sistemul verifică autorizarea utilizatorului asupra obiectului. (Vedeți diagrama de flux 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 găsește că autorizarea utilizatorului este insuficientă, el continuă cu Pasul 6.
3. Sistemul verifică dacă profilul de utilizator aparține vreunui grup. Dacă da, sistemul continuă cu Pasul 4. Dacă nu, sistemul continuă cu Pasul 5.
4. Sistemul determină autorizarea grupului. (Vedeți diagrama de flux 6). Dacă sistemul descoperă că grupul nu are autorizare pentru obiect, el continuă cu Pasul 5. Dacă sistemul determină că grupul nu are suficientă autorizare pentru obiect, el continuă cu Pasul 6.
5. Sistemul verifică autorizarea publică pentru obiect. (Vedeți diagrama de flux 7.) Dacă sistemul găsește că autorizarea publică este insuficientă, el continuă cu Pasul 6.
6. Sistemul verifică autorizarea adoptată pentru obiect. (Vedeți diagrama de flux 8.)

Dacă utilizatorul nu este autorizat, se întâmplă una sau mai multe dintre următoarele:

- Este trimis un mesaj către utilizator sau program
- Programul eșuează
- Este scrisă o intrare AF în jurnalul de audit

Organigrama 2: Calea rapidă pentru verificarea autorizării obiectului

Pașii din Organigrama 2 sunt efectuați folosind informațiile stocate cu obiectul. Aceasta este cea mai rapidă metodă de autorizare a unui utilizator pentru un obiect.



RBAFW522-0

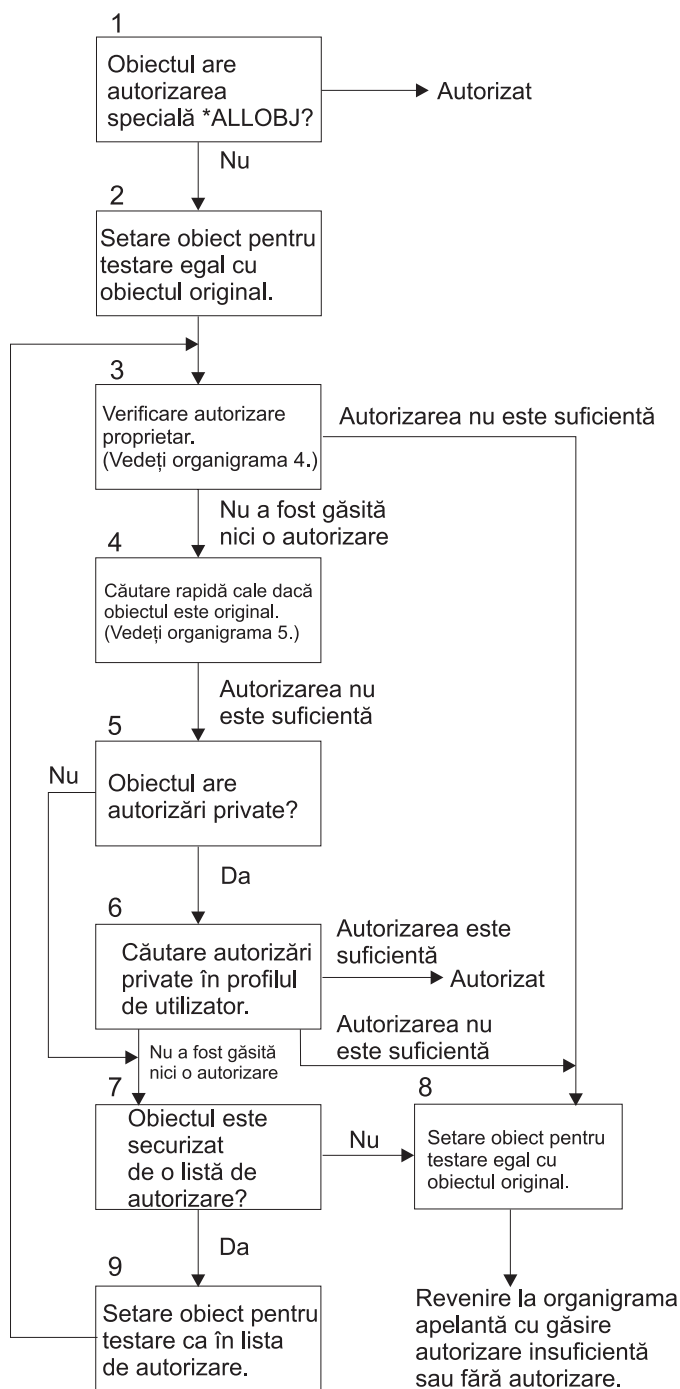
Figura 14. Organigrama 2: Calea rapidă pentru autorizarea obiectului

Descrierea lui Organigrama 2: Calea rapidă pentru autorizarea obiectului

1. Sistemul determină dacă obiectul are autorizări private. Dacă are, sistemul se întoarce la diagrama de flux apelantă cu insuficient. Dacă nu are, sistemul continuă cu Pasul 2.
2. Sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă 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.

Organigrama 3: Cum este verificată autorizarea utilizatorului asupra unui obiect

Pașii din Organigrama 3 sunt efectuați pentru profilul de utilizator individual.



RBAFW523-0

Figura 15. Organigrama 3: Verificare autorizare utilizator

Descrierea pentru Organigrama 3: Verificare autorizare utilizator

1. Sistemul determină dacă profilul de utilizator are autorizarea *ALLOBJ. Dacă profilul are autorizarea *ALLOBJ, atunci profilul este autorizat. Dacă nu are autorizarea *ALLOBJ, atunci verificarea autorizării continuă cu Pasul 2.
2. Sistemul setează autorizarea pentru obiect egală cu cea a obiectului original. Verificarea autorizării continuă cu Pasul 3.

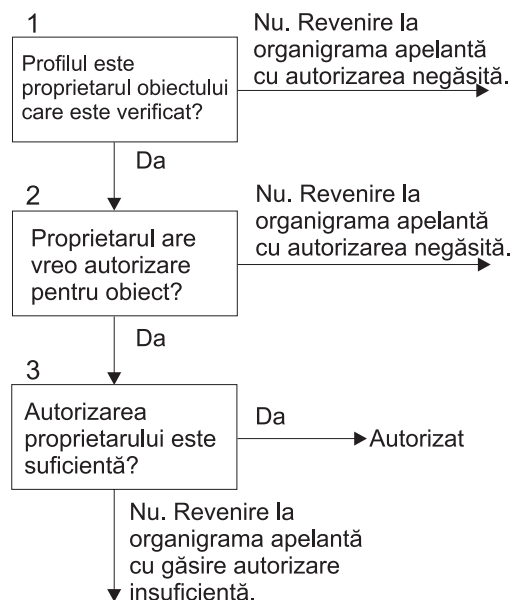
3. Sistemul verifică autorizarea proprietarului. Dacă autorizarea este insuficientă, atunci el continuă cu Pasul 8. Dacă nu este găsită nici o autorizare, atunci el continuă cu Pasul 4.
4. Sistemul efectuează o verificare a autorizării obiectului original pe calea rapidă. (Vedeți diagrama de flux 6). Dacă autorizarea este insuficientă, atunci verificarea autorizării continuă cu Pasul 5.
5. Sistemul determină dacă obiectul are autorizări private. Dacă are, atunci verificarea autorizării continuă cu Pasul 6. Dacă nu sunt autorizări private, atunci verificarea autorizării merge la Pasul 7.
6. Sistemul caută autorizări private pentru profilul de utilizator. Dacă autorizarea este suficientă, atunci utilizatorul este autorizat. Dacă autorizarea nu este suficientă, atunci verificarea autorizării continuă cu Pasul 8. Dacă nu este găsită nici o autorizare, atunci verificarea autorizării continuă cu Pasul 7.
7. Sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă nu este, atunci verificarea autorizării continuă cu Pasul 8. Dacă este securizat de o listă de autorizare, atunci verificarea autorizării continuă cu Pasul 9.
8. Sistemul setează obiectul pentru a fi testat egal cu obiectul original și 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 și se întoarce la Pasul 3.

Organigrama 4: Cum este verificată autorizarea proprietarului

Figura 16 arată procesul pentru verificarea autorizării proprietarului. Numele profilului de utilizator care este proprietar, precum și autorizarea proprietarului asupra unui obiect sunt stocate cu obiectul.

Există mai multe posibilități pentru utilizarea autorizării proprietarului pentru a accesa un obiect:

- Profilul de utilizator deține obiectul.
- Profilul de utilizator deține lista de autorizare.
- Profilul de grup al utilizatorului deține obiectul.
- Profilul de grup al utilizatorului deține lista de autorizare.
- Este folosită autorizarea adoptată și proprietarul programului deține obiectul.
- Este folosită autorizarea adoptată și proprietarul programului deține lista de autorizare.



RBAFW524-0

Figura 16. Organigrama 4: Verificarea autorizării proprietarului

Descrierea diagramei de flux 4: Verificarea autorizării proprietarului

1. Sistemul determină dacă profilul de utilizator deține obiectul care este verificat. Dacă profilul de utilizator deține într-adevăr obiectul, atunci sistemul trece la Pasul 2. Dacă profilul de utilizator nu deține obiectul, atunci sistemul revine la diagrama de flux apelantă cu nici o autorizare găsită.
2. Dacă profilul de utilizator nu deține obiectul, atunci sistemul determină dacă proprietarul are autorizare asupra obiectului. Dacă el sau ea este proprietarul, atunci verificarea autorizării continuă cu Pasul 3. Dacă sistemul descoperă că proprietarul nu are autorizare asupra obiectului, atunci sistemul se întoarce la diagrama de flux apelantă cu nici o autorizare găsită.
3. Dacă proprietarul are autorizare asupra obiectului, atunci sistemul determină dacă această autorizare este sau nu suficientă pentru a accesa obiectul. Dacă autorizarea este suficientă, atunci proprietarul este autorizat să acceseze obiectul. Dacă nu este suficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă găsită.

Organigrama 5: Calea rapidă pentru verificarea autorizării utilizatorului

Figura 17 la pagina 154 arată calea rapidă pentru testarea autorizării utilizatorului fără a căuta printre autorizările private.

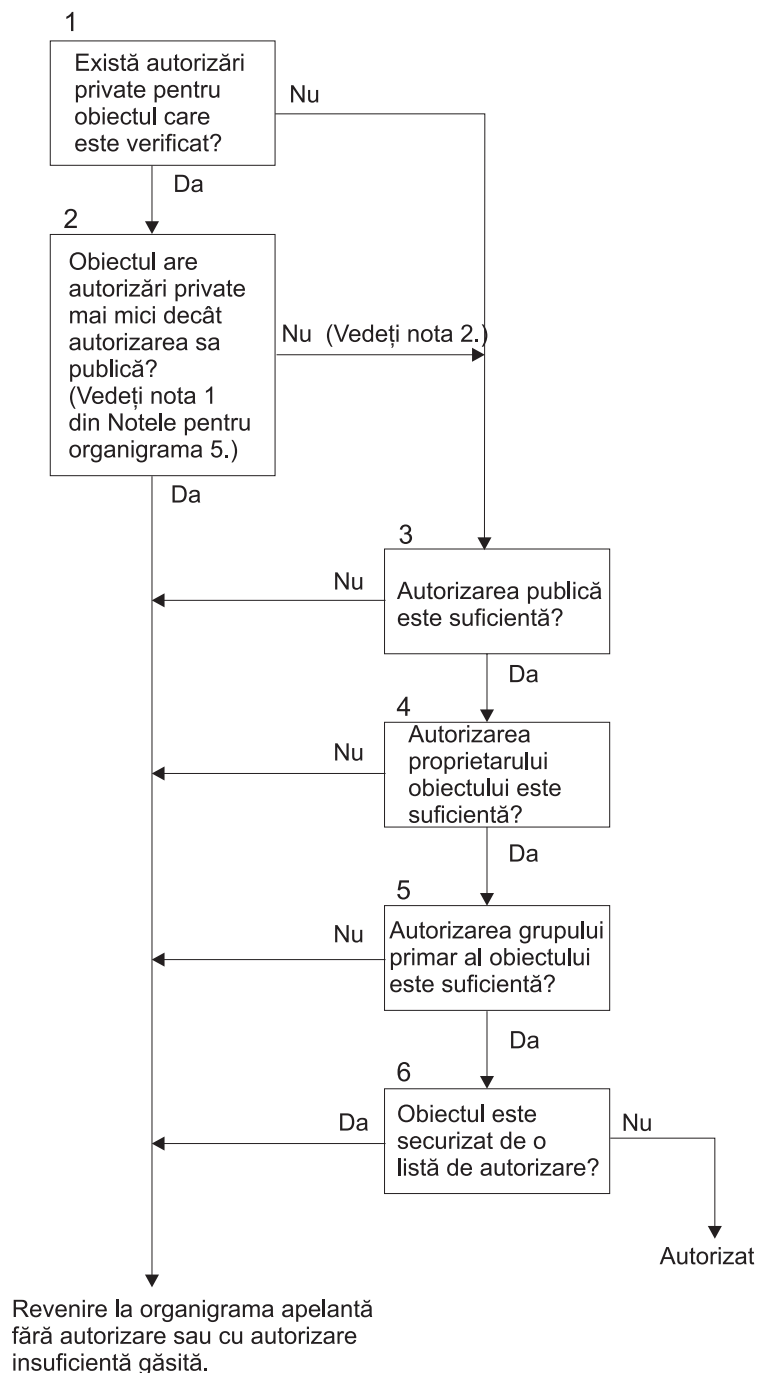


Figura 17. Organigrama 5: Calea rapidă pentru autorizarea utilizatorului

Organigrama 5 note:

1. Autorizarea este considerată mai mică decât publică dacă orice autorizare care este prezentă pentru *PUBLIC nu este prezentă pentru alt utilizator. În exemplul arătat în Tabela 115, publicul are autorizările *OBJOPR, *READ și *EXECUTE pentru obiect. WILSONJ are autorizarea *EXCLUDE și nu are nici una dintre autorizările pe care le are publicul. De aceea, acest obiect are o autorizare privată mai mică decât autorizarea publică. (OWNAR are de asemenea o autorizare mai mică decât publicul, dar autorizarea proprietarului este considerată autorizare privată.)

Tabela 115. Autorizarea publică contra autorizarea privată

Autorizare	Utilizatori			
	OWNAR	DPTMG	WILSONJ	*PUBLIC
<i>Autorizări obiect:</i>				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
<i>Autorizări de date</i>				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. Această cale oferă o metodă pentru folosirea autorizării publice, dacă este posibil, chiar dacă există autorizări private pentru un obiect. Sistemul se asigură să nu apară ceva mai târziu în procesul de verificare a autorizării care ar putea respinge accesul la obiect. Dacă rezultatul acestor teste este *Suficient*, atunci poate fi evitată căutarea printre autorizările private.

Descrierea diagramei de flux 5: Calea rapidă pentru autorizarea utilizatorului

Această diagramă de flux arată calea rapidă pentru testarea autorizării utilizatorului fără a căuta printre autorizările private.

1. Sistemul determină dacă există autorizări private pentru obiectul care este verificat. Dacă există autorizări private pentru obiect atunci verificarea autorizării continuă cu Pasul 2. Dacă nu există nici o autorizare privată, atunci verificarea autorizării continuă cu Pasul 3.
2. Dacă există autorizări private, atunci sistemul determină dacă obiectul are autorizări private care sunt mai mici decât autorizarea lui publică. (Vedeți 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, (vedeți nota 2), atunci verificarea autorizării continuă cu Pasul 3.
3. Dacă obiectul nu are autorizări private care sunt mai mici decât autorizarea lui publică, atunci sistemul determină dacă autorizarea publică este suficientă. Dacă autorizarea publică este suficientă, atunci verificarea autorizării continuă cu Pasul 4. Dacă autorizarea publică este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
4. Dacă autorizarea publică este suficientă, atunci sistemul determină dacă autorizarea proprietarului obiectului este suficientă. Dacă autorizarea proprietarului obiectului este suficientă, atunci verificarea autorizării continuă cu Pasul 5. Dacă autorizarea proprietarului obiectului este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
5. Dacă autorizarea proprietarului obiectului este suficientă, atunci sistemul determină dacă autorizarea grupului primar al obiectului este suficientă. Dacă autorizarea grupului primar al obiectului este suficientă, atunci verificarea autorizării continuă cu Pasul 6. Dacă autorizarea grupului primar al obiectului este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
6. Dacă autorizarea grupului primar al obiectului este suficientă, atunci sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă obiectul este securizat de o listă de autorizare, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă. Dacă obiectul nu este securizat de o listă de autorizare, atunci utilizatorul este autorizat să acceseze obiectul.

Organigrama 6: Cum este verificată autorizarea grupului

Un utilizator poate fi 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.

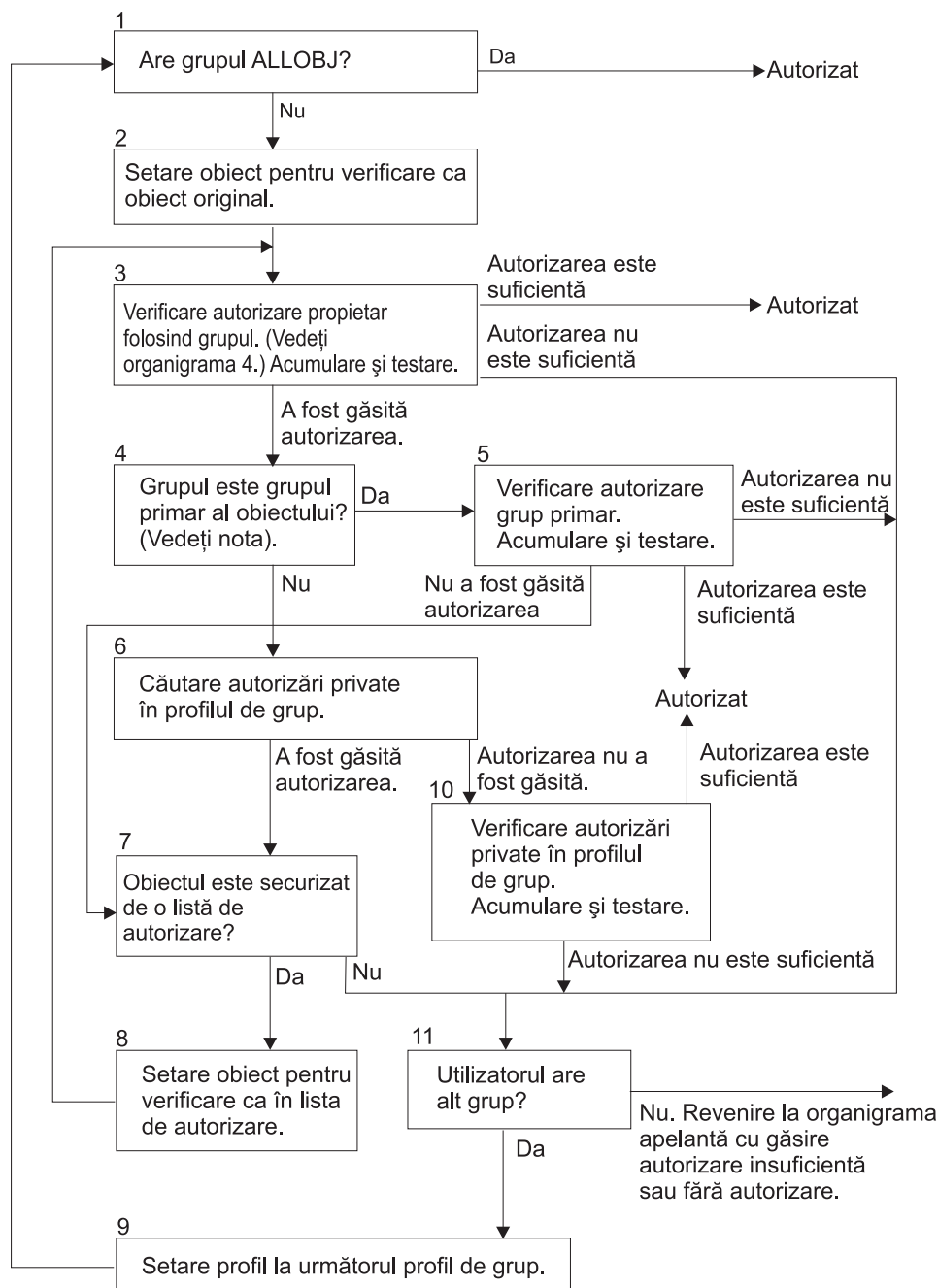
Autorizarea de la unul sau mai multe dintre grupurile utilizatorului poate fi acumulată pentru a găsi o autorizare suficientă pentru obiectul accesat. De exemplu, WAGNERB are nevoie de autorizarea *CHANGE pentru fișierul CRLIM. Autorizarea *CHANGE include *OBJOPR, *READ, *ADD, *UPD, *DLT și *EXECUTE. Tabela 116 arată autorizările pentru fișierul CRLIM:

Tabela 116. Autorizarea de grup acumulată

Autorizare	Utilizatori			
	OWNAR	DPT506	DPT702	*PUBLIC
<i>Autorizări obiect:</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Autorizări de date</i>				
*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 și DPT702 pentru a avea o autorizare suficientă pentru fișierul CRLIM. Lui DPT506 îi lipsește autorizarea *DLT, și lui DPT702 îi lipsește autorizarea *ADD.

Organigrama 6 la pagina 157 arată pașii de la verificarea autorizării de grup.



RBAFW509-0

Figura 18. Organigrama 6: Verificarea autorizării de grup

Notă: Dacă utilizatorul a intrat în sistem cu profilul care este grupul primar pentru un obiect, atunci utilizatorul nu poate primi autorizare asupra obiectului prin intermediul grupului primar.

Descrierea diagramei de flux 6: Verificarea autorizării de grup

1. Sistemul determină dacă grupul are autorizarea ALLOBJ. Dacă are, atunci grupul este autorizat. Dacă nu are, atunci verificarea autorizării continuă cu Pasul 2.
2. Dacă grupul nu are autorizarea ALLOBJ, atunci sistemul setează obiectul care este verificat să fie egal cu obiectul original.

3. După ce sistemul setează obiectul la original, el verifică autorizarea proprietarului. (Vedeți Diagrama de flux 4) Dacă autorizarea este suficientă, atunci grupul este autorizat. Dacă autorizarea nu este suficientă, atunci verificarea autorizării trece la Pasul 7. Dacă autorizarea nu este găsită, atunci verificarea autorizării continuă cu Pasul 4.
4. Dacă autorizarea proprietarului nu este găsită, atunci sistemul verifică dacă grupul este grupul primar al obiectului.

Notă: Dacă utilizatorul a intrat în sistem cu profilul care este grupul primar pentru un obiect, atunci utilizatorul nu poate primi autorizare asupra obiectului prin intermediul grupului primar.

Dacă grupul este grupul primar al obiectului, atunci verificarea autorizării continuă cu Pasul 5. Dacă grupul nu este grupul primar al obiectului, atunci verificarea autorizării continuă cu Pasul 6.

5. Dacă grupul este grupul primar al obiectului, atunci sistemul verifică și testează autorizarea grupului primar. Dacă autorizarea grupului primar este suficientă, atunci grupul este autorizat. Dacă autorizarea grupului primar este insuficientă sau nu este găsită, atunci verificarea autorizării trece la Pasul 7.
6. Dacă grupul nu este grupul primar al obiectului, atunci sistemul caută printre autorizările private din profilul de grup. Dacă este găsită autorizarea atunci verificarea autorizării merge la Pasul 10. Dacă nu este găsită autorizarea, atunci verificarea autorizării continuă cu Pasul 7.
7. Dacă nu este găsită nici o autorizare pentru autorizările private pentru profilul de grup atunci sistemul verifică dacă obiectul este securizat de o listă de autorizare. Dacă obiectul este securizat de o listă de autorizare, atunci verificarea autorizării continuă cu Pasul 8. Dacă obiectul nu este securizat de o listă de autorizare, atunci verificarea.
8. Dacă obiectul este securizat de o listă de autorizare, atunci sistemul setează obiectul de verificat să fie egal cu lista de autorizare și verificarea autorizării revine la Pasul 3.
9. Dacă utilizatorul aparține altui profil de grup, atunci sistemul setează acest profil la următorul profil de grup și revine la Pasul 1 pentru a porni din nou procesul de verificare a autorizării.
10. Dacă este găsită autorizarea pentru autorizările private din cadrul profilului de grup, atunci autorizările private sunt verificate și testate în profilul de grup. Dacă autorizările sunt suficiente, atunci profilul de grup este autorizat. Dacă nu sunt suficiente atunci verificarea autorizării merge la Pasul 7.
11. Dacă un obiect nu este securizat de o listă de autorizare, atunci sistemul verifică dacă utilizatorul este asociat cu alt profil de grup. Dacă utilizatorul aparține altui profil de grup, atunci sistemul merge la Pasul 9. Dacă utilizatorul nu aparține altui profil de grup, atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă sau nici o autorizare găsită.

Organigrama 7: Cum este verificată autorizarea publică

Când este verificată autorizarea publică, sistemul trebuie să determine dacă va folosi autorizarea publică pentru obiect sau va folosi lista de autorizare. Organigrama 7 arată procesul:

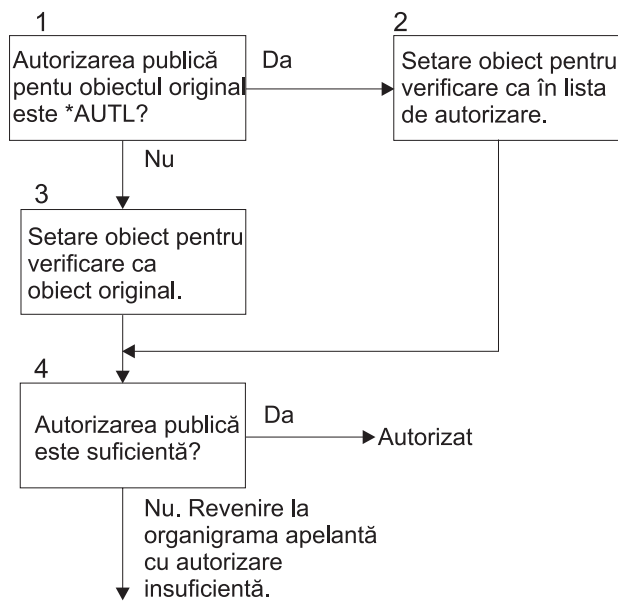


Figura 19. Organigrama 7: Verificarea autorizării publice

Descrierea pentru Organigrama 7: Verificarea autorizării publice

Diagrama de flux 7 arată cum trebuie sistemul să determine dacă va folosi autorizarea publică pentru obiect sau dacă va folosi lista de autorizare.

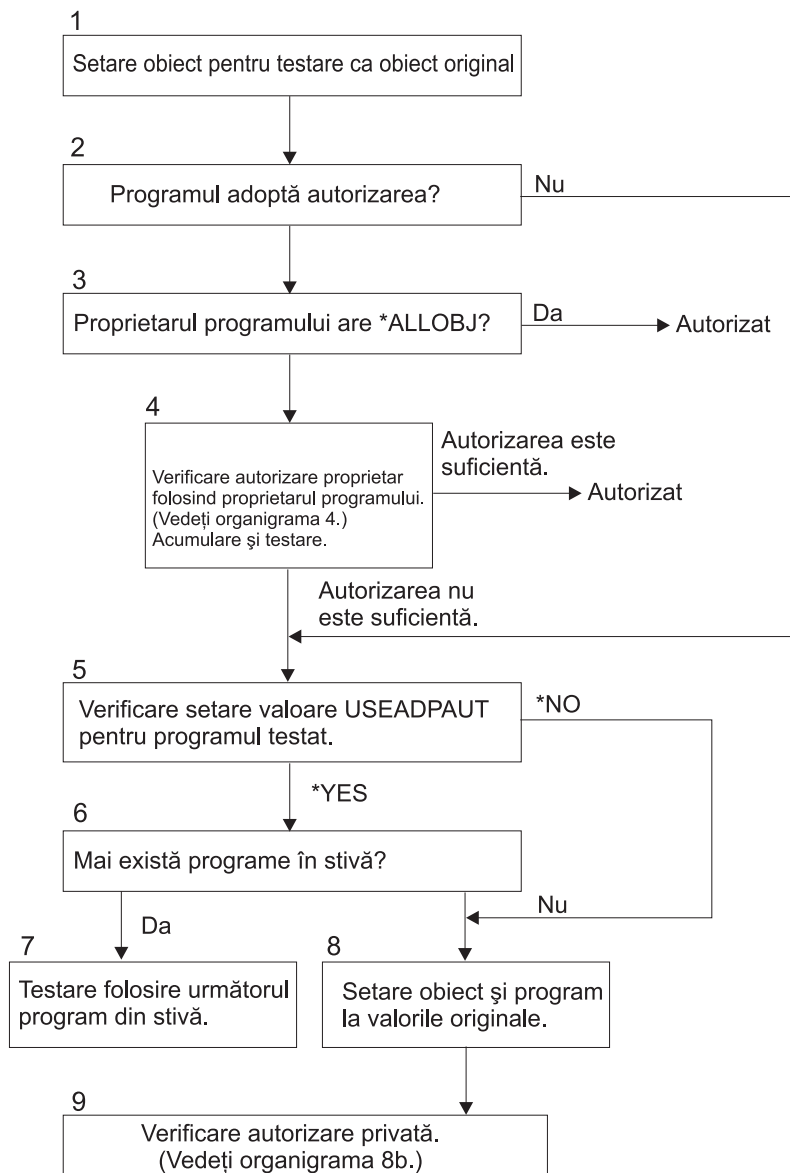
1. Sistemul determină dacă autorizarea publică pentru obiectul original este *AUTL. Dacă autorizarea publică pentru obiectul original este *AUTL, atunci sistemul continuă cu Pasul 2. Dacă autorizarea publică pentru obiectul original nu este *AUTL, atunci sistemul continuă cu Pasul 3.
2. Dacă autorizarea publică pentru obiectul original este *AUTL, atunci sistemul setează obiectul care este verificat să fie egal cu lista de autorizare și 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 și continuă cu Pasul 4.
4. Dacă obiectul care este verificat a fost setat egal cu lista de autorizare sau cu obiectul original, sistemul determină dacă autorizarea publică este suficientă. Dacă autorizarea publică este suficientă, atunci utilizatorul este autorizat pentru obiect. Dacă autorizarea publică nu este suficientă atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă.

Organigrama 8: Cum este verificată autorizarea adoptată

Dacă este găsită o autorizare insuficientă la verificarea autorizării utilizatorului, atunci sistemul verifică autorizarea adoptată. Sistemul poate folosi autorizarea adoptată de la programul original pe care utilizatorul l-a apelat sau de la programele anterioare din stiva program. Pentru a oferi cele mai bune performanțe și 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 deține obiectul care este testat. Aceasta este repetată pentru fiecare program din stivă care folosește autorizarea adoptată.

Dacă nu este găsită o autorizare suficientă, atunci sistemul verifică dacă proprietarul programului are autorizare privată pentru obiectul care este verificat. Aceasta este repetată pentru fiecare program din stivă care folosește autorizarea adoptată.

Figura 20 la pagina 160 și Figura 21 la pagina 162 arată procesul pentru verificarea autorizării adoptate.



RBAFW527-0

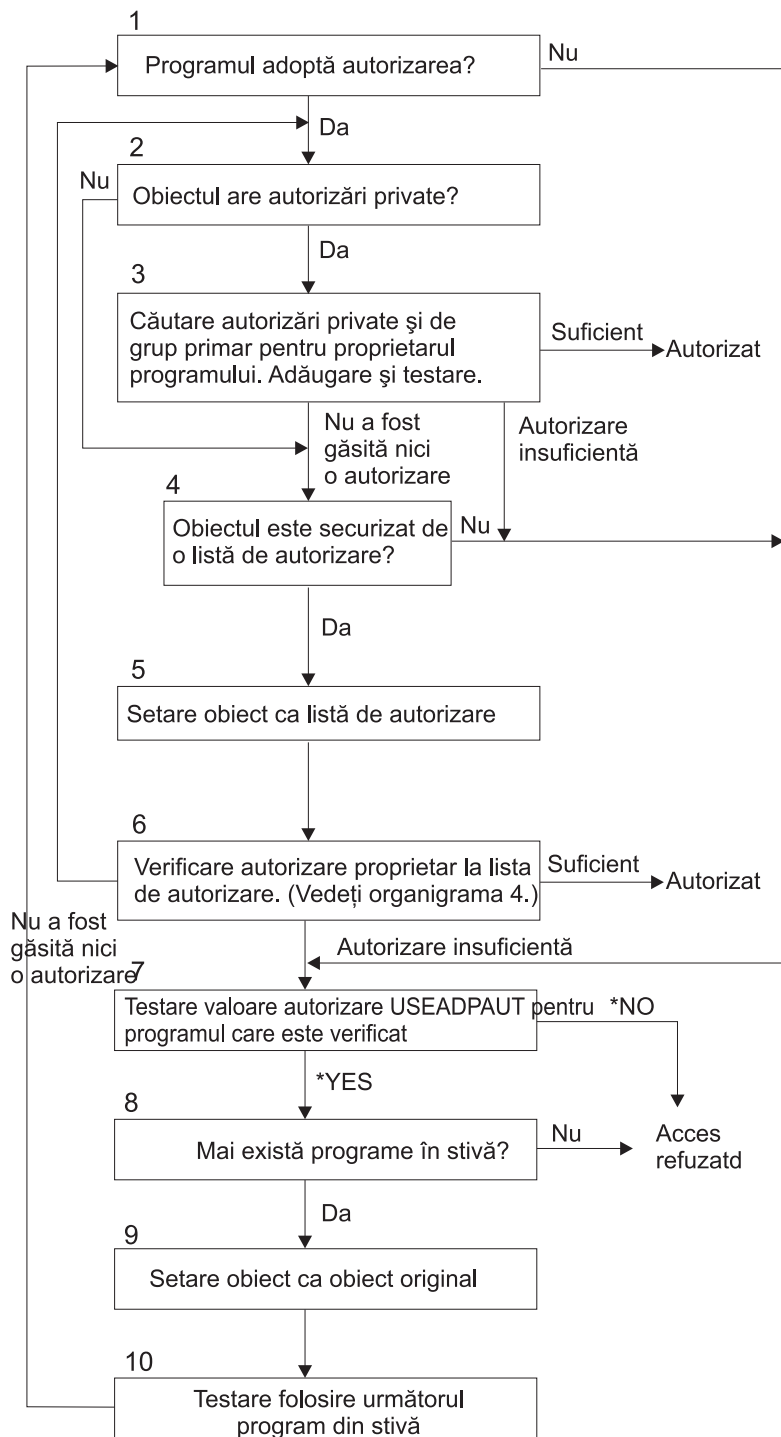
Figura 20. Organigrama 8 A: Verificarea autorizării adoptate Utilizator *ALLOBJ și Proprietar

Descrierea pentru Organigrama 8 A: Verificarea autorizării adoptate Utilizator *ALLOBJ și Proprietar

Organigrama 8 A descrie cum verifică sistemul autorizarea adoptată când a fost găsită o autorizare insuficientă la verificarea autorizării utilizatorului.

1. Sistemul setează obiectul care este verificat să fie egal cu obiectul original și 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 și 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 și 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 așteaptă în stivă. Dacă sunt mai multe programe în stivă, atunci verificarea autorizării continuă cu Pasul 7. Dacă nu mai sunt programe care așteaptă în stivă, atunci verificarea autorizării merge la Pasul 8.
7. Dacă sunt mai multe programe în stivă, sistemul testează următorul program din stivă.
8. Dacă nu mai sunt programe în stivă sau dacă valoarea USEADPAUT este egală cu *NO, atunci sistemul setează obiectul și programul la valorile originale și continuă cu Pasul 9.
9. Sistemul verifică autorizarea privată. Aceasta este descrisă în Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private.



RBAFW528-0

Figura 21. Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private

Descrierea pentru Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private

1. Sistemul determină dacă programul poate adopta autorizarea. Dacă da, continuă cu Pasul 2. Dacă nu, continuă cu Pasul 7.
2. Sistemul determină dacă obiectul are autorizări private. Dacă da, continuă cu Pasul 3. Dacă nu, continuă cu Pasul 4.

3. Sistemul verifică autorizările private și 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 și apoi continuă cu Pasul 6.
6. Sistemul verifică autorizarea proprietarului asupra listei de autorizare. (Vedeți 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 și continuă cu Pasul 10.
10. Text folosind următorul program din stivă și repornește de la Pasul 1.

Exemple de verificare a autorizării

În continuare sunt mai multe exemple de verificare a autorizării. Aceste exemple demonstrează pașii pe care sistemul îi folosește pentru a determina dacă unui utilizator îi este permis un acces cerut la un obiect. Aceste exemple sunt destinate să arate cum funcționează verificarea autorizării și unde pot apare potențiale probleme de performanță.

Figura 22 arată autorizările pentru fișierul PRICES. După figură urmează mai multe exemple de acces cerut la acest fișier și procesul de verificare a autorizării. În exemple, căutarea printre autorizările private (Organigrama 4, pasul 6) este evidențiată deoarece aceasta este partea din procesul de verificare a autorizării care poate produce probleme de performanță 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

User      Group      Object
OWNCP     Group      Authority
DPTSM     *CHANGE
DPTMG     *CHANGE
WILSONJ   *USE
*PUBLIC   *USE

```

Figura 22. Autorizarea pentru fișierul PRICES

Cazul 1: Folosirea autorizării private de grup

Utilizatorul ROSSM dorește accesul la fișierul PRICES folosind programul CPPGM01. CPPGM01 necesită autorizarea *CHANGE pentru fișier. ROSSM este un membru al profilului de grup DPTSM. Nici ROSSM nici DPTSM nu au autorizarea specială *ALLOBJ. Sistemul efectuează acești pași pentru a determina dacă să-i permită lui ROSSM accesul la fișierul PRICES:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 3, pasul 3.

- 1) Organigrama 4, pasul 1. Revenire la Organigrama 3 cu nici o autorizare găsită. ROSSM nu deține fișierul PRICES.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1, 2 și 3. Public nu este suficient.
 - d. Organigrama 3, pasul 5.
 - e. **Organigrama 3, pasul 6.** ROSSM nu are autorizare privată pentru fișierul PRICES.
 - f. Organigrama 3, pașii 7 și 8. Fișierul PRICES nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pașii 3 și 4. DPTSM este profilul de grup pentru ROSSM.
- a. Organigrama 6, pașii 1, 2 și 3.
 - 1) Organigrama 4, pasul 1. DPTSM nu deține fișierul PRICES.
 - b. Organigrama 6, pasul 4. DPTSM nu este grupul primar pentru fișierul PRICES.
 - c. **Organigrama 6, pasul 6.** Autorizat. (DPTSM are autorizarea *CHANGE.)

Rezultat: ROSSM este autorizat deoarece profilul de grup DPTSM are autorizarea *CHANGE.

Analiză: Folosirea autorizării de grup în acest exemplu este o bună metodă pentru gestiunea autorizărilor. Ea reduce numărul de autorizări private din sistem și este ușor de înțeles și de auditat. Însă folosirea autorizării private de grup cauzează de obicei două căutări de autorizări private (pentru utilizator și pentru grup) când autorizarea publică nu este adecvată. O căutare a autorizării private poate fi evitată făcând ca DPTSM să fie grupul primar pentru fișierul PRICES.

Cazul 2: Folosirea autorizării grupului primar

ANDERSJ are nevoie de autorizarea *CHANGE pentru fișierul CREDIT. ANDERSJ este un membru al grupului DPTAR. Nici ANDERSJ nici DPTAR nu au autorizarea specială *ALLOBJ. Figura 23 arată autorizările pentru fișierul CREDIT.

Display Object Authority			
Object	:	CREDIT	Owner : OWNER
Library	:	ACCTSRCV	Primary group : DPTAR
Object type	:	*FILE	ASP device : *SYSBAS
Object secured by authorization list			: *NONE
User	Group	Object Authority	
OWNER		*ALL	
DPTAR		*CHANGE	
*PUBLIC		*USE	

Figura 23. Autorizarea pentru fișierul CREDIT

Sistemul efectuează acești pași pentru a determina dacă să îi permită lui ANDERSJ accesul *CHANGE la fișierul CREDIT:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1. Autorizarea lui DPTAR este autorizarea de grup primar, nu autorizarea privată.
 - b. Organigrama 2, pașii 2, 3, 4, 5 și 6. Autorizarea publică nu este suficientă.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. ANDERSJ nu deține fișierul CREDIT. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.

- 1) Organigrama 5, pasul 1. Fișierul CREDIT nu are autorizări private.
- 2) Organigrama 5, pasul 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.
- d. Organigrama 3, pașii 5, 7 și 8. Fișierul CREDIT nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pașii 3 și 4. ANDERSJ este un membru al profilului de grup DPTAR.
 - a. Organigrama 6, pașii 1 și 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.
 - b. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPTAR nu deține fișierul CREDIT. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - c. Organigrama 6, pașii 4 și 5. Autorizat. DPTAR este grupul primar pentru fișierul CREDIT și are autorizarea *CHANGE.

Rezultat: ANDERSJ este autorizat deoarece DPTAR este grupul primar pentru fișierul CREDIT și are autorizarea *CHANGE.

Analiză: Dacă folosiți autorizarea de grup primar, atunci performanțele verificării autorizării sunt mai bune decât dacă specificați autorizare privată pentru grup. Acest exemplu nu necesită nici o căutare de autorizări private.

Cazul 3: Folosirea autorizării publice

Utilizatorul JONESP dorește accesul la fișierul CREDIT folosind programul CPPGM06. CPPGM06 necesită autorizarea *USE pentru fișier. JONESP este membru al profilului de grup DPTSM și nu are autorizarea specială *ALLOBJ. Sistemul efectuează acești pași pentru a determina dacă să-i permită lui JONESP accesul la fișierul CREDIT:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1. Fișierul CREDIT nu are autorizări private. Autorizarea lui DPTAR este autorizarea de grup primar, nu autorizarea privată.
 - b. Organigrama 2, pașii 2 și 3. Autorizarea proprietarului (OWNAR) este suficientă.
 - c. Organigrama 2, pașii 4 și 5. Autorizarea grupului primar (DPTAR) este suficientă.
 - d. Organigrama 2, pasul 6. Autorizat. Autorizarea publică este suficientă.

Analiză: Acest exemplu arată câștigul de performanță obținut când evitați definirea vreunei autorizări private pentru un obiect.

Cazul 4: Folosirea autorizării publice fără căutarea autorizării private

Utilizatorul JONESP dorește accesul la fișierul PRICES folosind programul CPPGM06. CPPGM06 necesită autorizarea *USE pentru fișier. JONESP este membru al profilului de grup DPTSM și nu are autorizarea specială *ALLOBJ. Sistemul efectuează acești pași pentru a determina dacă să-i permită lui JONESP accesul la fișierul PRICES:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1. Fișierul PRICES are autorizări private.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. JONESP nu deține fișierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1, 2 și 3. Autorizarea publică este suficientă.
 - 2) Organigrama 5, pasul 4. Autorizarea proprietarului este suficientă. (OWNCP are *ALL.)
 - 3) Organigrama 5, pasul 5. Fișierul PRICES nu are un grup primar.
 - 4) Organigrama 5, pasul 6. Autorizat. (Fișierul PRICES nu este securizat de o listă de autorizare.)

Analiză: Acest exemplu arată câștigul de performanță obținut când evitați definirea vreunor autorizări private pentru un obiect care sunt mai mici decât autorizarea publică. Deși există autorizări private pentru fișierul PRICES, autorizarea publică este suficientă pentru această cerere și poate fi folosită fără a căuta autorizări private.

Cazul 5: Folosirea autorizării adoptate

Utilizatorul SMITHG dorește accesul la fișierul PRICES folosind programul CPPGM08. SMITHG nu este membru al unui grup și nu are autorizarea specială *ALLOBJ. Programul CPPGM08 necesită autorizarea *CHANGE pentru fișier. CPPGM08 este deținut de profilul OWNCP și adoptă autorizarea proprietarului (USRPRF este *OWNER).

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. SMITHG nu deține fișierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1, 2 și 3. Public nu este suficient.
 - d. Organigrama 3, pasul 5.
 - e. **Organigrama 3, pasul 6.** SMITHG nu are autorizare privată.
 - f. Organigrama 3, pașii 7 și 8. Fișierul PRICES nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pasul 3. SMITHG nu are un grup.
4. Organigrama 1, pasul 5.
 - a. Organigrama 7, pasul 1. Autorizarea publică nu este *AUTL.
 - b. Organigrama 7, pasul 3. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - c. Organigrama 7, pasul 4. Autorizarea publică nu este suficientă.
5. Organigrama 1, pasul 6.
 - a. Organigrama 8 A, pasul 1. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 8 A, pașii 2 și 3. OWNCP nu are autorizarea *ALLOBJ.
 - c. Organigrama 8 A, pasul 4.
 - 1) Organigrama 4, pașii 1, 2 și 3. Autorizat. OWNCP deține fișierul PRICES și are suficientă autorizare.

Analiză: Acest exemplu demonstrează avantajele de performanță la folosirea autorizării adoptate când proprietarul programului deține de asemenea și obiectele aplicației.

Numărul de pași necesari pentru a efectua verificarea autorizării nu are aproape nici un efect asupra performanței, deoarece majoritatea pașilor nu necesită extragerea de noi informații. În acest exemplu, deși sunt efectuați mulți pași, autorizările private sunt căutate o singură dată (pentru utilizatorul SMITHG).

Comparați aceasta cu Cazul 1 de la pagina “Cazul 1: Folosirea autorizării private de grup” la pagina 163.

- Dacă ați schimba Cazul 1 astfel încât profilul de grup DPTSM deține fișierul PRICES și are autorizarea *ALL asupra lui, caracteristicile de performanță ale celor două exemple ar fi aceleași. Oricum, facerea ca un profil de grup să dețină obiecte aplicație poate reprezenta un risc de securitate. Membrii grupului au întotdeauna autorizarea grupului (proprietar), doar dacă nu acordați în mod specific membrilor grupului o autorizare mai mică. Când folosiți autorizarea adoptată, puteți controla situațiile în care este folosită autorizarea proprietarului.
- Puteți de asemenea schimba Cazul 1 astfel încât DPTSM este grupul primar pentru fișierul PRICES și 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 performanță ar fi la fel ca în Cazul 5.

Cazul 6: Autorizarea de utilizator și de grup

Utilizatorul WILSONJ dorește să acceseze fișierul PRICES folosind programul CPPGM01, care necesită autorizarea *CHANGE. WILSONJ este membru al profilului de grup DPTSM și nu are autorizarea specială *ALLOBJ. Programul CPPGM01 nu folosește autorizarea adoptată, și ignoră orice autorizare adoptată anterior (USEADPAUT este *NO).

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1. PRICES are autorizări private.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. WILSONJ nu deține fișierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1, 2 și 3. Public nu este suficient.
 - d. Organigrama 3, pasul 5.
 - e. **Organigrama 3, pasul 6.** WILSONJ are autorizarea *USE, care nu este suficientă.
 - f. Organigrama 3, pasul 8. Obiectul de testat = CONTRACTS/PRICES *FILE. Revenire la Organigrama 1 cu autorizare insuficientă.
3. Organigrama 1, pasul 6.
 - a. Organigrama 8 A, pasul 1. Obiectul de verificat = CONTRACTS/PRICES *FILE.
 - b. Organigrama 8 A, pasul 2. Programul CPPGM01 nu adoptă autorizarea.
 - c. Organigrama 8 A, pasul 5. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO.
 - d. Organigrama 8 A, pașii 8 și 9.
 - 1) Organigrama 8 B, pasul 1. Programul CPPGM01 nu adoptă autorizarea.
 - 2) Organigrama 8 B, pasul 7. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO. Accesul este interzis.

Analiză: Acest exemplu demonstrează că unui utilizator îi poate fi interzis accesul la un obiect chiar dacă grupul utilizatorului are autorizare suficientă.

Acordarea pentru un utilizator a aceleiași autorizării ca și publicul dar mai mică decât grupul utilizatorului nu afectează performanțele verificării autorizării pentru alți utilizatori. Oricum, dacă WILSONJ ar avea autorizarea *EXCLUDE (mai mică decât publicul), atunci ați pierde beneficiile de performanță arătate în Cazul 4.

Deși acest exemplu are mulți pași, autorizările private sunt căutate o singură dată. Aceasta ar oferi performanțe acceptabile.

Cazul 7: Autorizarea publică fără autorizare privată

Informațiile de autorizare pentru fișierul ITEM arată astfel:

Display Object Authority					
Object	:	ITEM	Owner	:	OWNIC
Library	:	ITEMLIB	Primary group	:	*NONE
Object type	:	*FILE	ASP device	:	*SYSBAS
Object secured by authorization list				:	*NONE
		Object			
User	Group	Authority			
OWNIC		*ALL			
*PUBLIC		*USE			

Figura 24. Display Object Authority - Afișare autorizare obiect

ROSSM are nevoie de autorizarea *USE pentru fișierul ITEM. ROSSM este membru al profilului de grup DPTSM. Aceștia sunt pașii verificării autorizării:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pașii 1, 2 și 3. Autorizarea lui OWNIC este suficientă.
 - b. Organigrama 2, pasul 4. Fișierul ITEM nu are un grup primar.
 - c. Organigrama 2, pasul 6. Autorizat. Autorizarea publică este suficientă.

Analiză: Autorizarea publică oferă cele mai bune performanțe când este folosită fără autorizări private. În acest exemplu, autorizările private nu sunt căutate deloc.

Cazul 8: Autorizarea adoptată fără autorizare privată

Pentru acest exemplu, toate programele din aplicație sunt deținute de profilul OWNIC. Orice program din aplicație care necesită o autorizare mai mare decât *USE adoptă autorizarea proprietarului. Aceștia sunt pașii pentru ca utilizatorul WILSONJ să obțină autorizarea *CHANGE pentru fișierul ITEM când folosește programul ICPGM10, care adoptă autorizarea:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pașii 1, 2, 3, 4 și 6. Autorizarea publică nu este suficientă.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = ITEMLIB/ITEM *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. WILSONJ nu deține fișierul ITEM. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1 și 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - d. Organigrama 3, pașii 5, 7 și 8. Fișierul ITEM nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pașii 3 și 5. (WILSONJ nu are un profil de grup.)
 - a. Organigrama 7, pașii 1, 3 și 4. Publicul are autorizarea *USE, care nu este suficientă.
4. Organigrama 1, pasul 6.
 - a. Organigrama 8 A, pasul 1. Obiectul de verificat = ITEMLIB/ITEM *FILE.
 - b. Organigrama 8 A, pașii 2, 3 și 4. Profilul OWNIC nu are autorizarea *ALLOBJ.
 - 1) Organigrama 4, pașii 1, 2 și 3. Autorizat. OWNIC are autorizare suficientă pentru fișierul ITEM.

Analiză: Acest exemplu arată beneficiile folosirii autorizării adoptate fără autorizarea privată, în special dacă proprietarul programelor deține de asemenea obiectele aplicației. Acest exemplu nu a necesitat căutarea de autorizări private.

Cazul 9: Folosirea unei liste de autorizare

Fișierul ARWRK01 din biblioteca CUSTLIB este securizat de lista de autorizare ARLST1. Figura 25 și Figura 26 arată autorizările:

```
Display Object Authority
Object . . . . . : ARWRK01      Owner . . . . . : OWNAR
Library . . . . . : CUSTLIB      Primary group . . . : *NONE
Object type . . . . : *FILE      ASP device . . . . . : *SYSBAS

Object secured by authorization list. . . . . : ARLST1

User      Group      Object
OWNCP
*PUBLIC   *PUBLIC   *ALL
          *PUBLIC   *USE
```

Figura 25. Autorizarea pentru fișierul ARWRK01

```
Display Authorization List
Object . . . . . : ARLST1      Owner . . . . . : OWNAR
Library . . . . . : QSYS        Primary group . . . : *NONE

User      Group      Object      List
OWNCP
AMESJ
*PUBLIC   *PUBLIC   *ALL
          *PUBLIC   *CHANGE
          *PUBLIC   *USE
```

Figura 26. Autorizarea pentru lista de autorizare ARLST1

Utilizatorul AMESJ, care nu este membru al unui profil de grup, necesită autorizarea *CHANGE pentru fișierul ARWRK01. Aceștia sunt pașii verificării autorizării:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pașii 1 și 2. Fișierul ARWRK01 este securizat de o listă de autorizare.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CUSTLIB/ARWRK01 *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. AMESJ nu deține fișierul ARWRK01. Revenire la Organigrama 2 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1 și 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - d. Organigrama 3, pașii 5, 7 și 9. Obiectul de verificat = ARLST1 *AUTL.
 - e. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. AMESJ nu deține lista de autorizare ARLST1. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - f. Organigrama 3, pașii 4 și 5.
 - g. **Organigrama 3, pasul 6.** Autorizat. AMESJ are autorizarea *CHANGE pentru lista de autorizare ARLST1.

Analiză: Acest exemplu demonstrează că listele de autorizare pot face ca autorizările să fie mai ușor de gestionat și oferă performanțe 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 pași suplimentari la acest exemplu, dar nu ar adăuga o căutare suplimentară a autorizărilor private, atâta vreme cât nu sunt definite autorizări private pentru fișierul ARWRK01. Problemele de performanță este cel mai probabil să apară când autorizările private, listele de autorizare și profilurile de grup sunt combinate, ca în “Cazul 11: Combinarea metodelor de autorizare” la pagina 171.

Cazul 10: Folosirea mai multor grupuri

WOODBC necesită autorizarea *CHANGE pentru fișierul CRLIM. WOODBC este membru al trei grupuri: DPTAR, DPTSM și DPTMG. DPTAR este primul profil de grup (GRPPRF). DPTSM și DPTMG sunt profiluri de grup suplimentare (supplemental group profiluris - SUPGRPPRF). Figura 27 arată autorizările pentru fișierul 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
User	Group	Object Authority		
OWNAR		*ALL		
DPTAR		*CHANGE		
DPTSM		*USE		
*PUBLIC		*EXCLUDE		

Figura 27. Autorizarea pentru fișierul CRLIM

Aceștia sunt pașii verificării autorizării:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1. Revenire la diagrama de flux apelantă cu autorizare insuficientă.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIM *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. WOODBC nu deține fișierul CRLIM. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1, 2 și 3. Autorizarea publică nu este suficientă.
 - d. Organigrama 3, pasul 5.
 - e. **Organigrama 3, pasul 6.** WOODBC nu are nici o autorizare pentru fișierul CRLIM.
 - f. Organigrama 3, pașii 7 și 8. Fișierul CRLIM nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pașii 3 și 4. Primul grup pentru WOODBC este DPTAR.
 - a. Organigrama 6, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIM *FILE.
 - b. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPTAR nu deține fișierul CRLIM. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - c. Organigrama 6, pașii 4 și 5. Autorizat. DPTAR este grupul primar și are autorizare suficientă.

Cazul 11: Combinarea metodelor de autorizare

WAGNERB necesită autorizarea *ALL pentru fișierul CRLIMWRK. WAGNERB este membru al acestor grupuri: DPTSM, DPT702 și DPTAR. Primul grup (first group - GRPPRF) al lui WAGNERB este DPTSM. Figura 28 arată autorizarea pentru fișierul 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
User	Group	Object Authority	
OWNAR		*ALL	
DPTSM		*USE	
WILSONJ		*EXCLUDE	
*PUBLIC		*USE	

Figura 28. Autorizarea pentru fișierul CRLIMWRK

Fișierul CRLIMWRK este securizat de lista de autorizare CRLST1. Figura 29 arată autorizarea pentru lista de autorizare CRLST1.

Display Authorization List			
Object	:	CRLST1	Owner : OWNAR
Library	:	QSYS	Primary Group . . . : DPTAR
User	Group	Object Authority	List Mgt
OWNAR		*ALL	X
DPTAR		*ALL	
*PUBLIC		*EXCLUDE	

Figura 29. Autorizarea pentru Lista de autorizare CRLST1

Acest exemplu arată multe dintre posibilitățile de verificare a autorizării. De asemenea el demonstrează cum folosirea a prea multe opțiuni de autorizare pentru un obiect poate conduce la performanțe scăzute.

În continuare sunt pașii necesari pentru a verifica autorizarea lui WAGNERB pentru fișierul CRLIMWRK:

1. Organigrama 1, pasul 1.
 - a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
 - a. Organigrama 3, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
 - b. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. WAGNERB nu deține fișierul CRLIMWRK. Revenire la Organigrama 3 cu nici o autorizare găsită.
 - c. Organigrama 3, pasul 4.
 - 1) Organigrama 5, pașii 1 și 2. WILSONJ are autorizarea *EXCLUDE, care este mai mică decât autorizarea publică *USE.
 - d. Organigrama 3, pașii 5 și 6 (**se caută mai întâi autorizările private**). WAGNERB nu are autorizare privată.
 - e. Organigrama 3, pașii 7 și 9. Obiectul de verificat = CRLST1 *AUTL.

- f. Organigrama 3, pasul 3.
 - 1) Organigrama 4, pasul 1. WILSONJ nu deține CRLST1. Revenire la Organigrama 3 cu nici o autorizare găsită.
- g. Organigrama 3, pașii 4 și 5.
- h. Organigrama 3, pasul 6 (**a doua căutare a autorizărilor private**). WAGNERB nu are autorizare privată pentru CRLST1.
- i. Organigrama 3, pașii 7 și 8. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
- 3. Organigrama 1, pașii 3 și 4. Primul profil de grup al lui WAGNERB este DPTSM.
 - a. Organigrama 6, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
 - b. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPTSM nu deține fișierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - c. Organigrama 6, pasul 4. DPTSM nu este grupul primar pentru fișierul CRLIMWRK.
 - d. Organigrama 6, pasul 6 (**a treia căutare a autorizărilor private**). DPTSM are autorizarea *USE pentru fișierul CRLIMWRK, care nu este suficientă.
 - e. Organigrama 6, pasul 6 continuat. Autorizarea *USE este adăugată la autorizările deja găsite pentru grupurile lui WAGNERB (nici una). Nu a fost încă găsită o autorizare suficientă.
 - f. Organigrama 6, pașii 9 și 10. Următorul grup al lui WAGNERB este DPT702.
 - g. Organigrama 6, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
 - h. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPT702 nu deține fișierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - i. Organigrama 6, pasul 4. DPT702 nu este grupul primar pentru fișierul CRLIMWRK.
 - j. Organigrama 6, pasul 6 (**a patra căutare a autorizărilor private**). DPT702 nu are autorizare pentru fișierul CRLIMWRK.
 - k. Organigrama 6, pașii 7 și 8. Obiectul de verificat = CRLST1 *AUTL
 - l. Organigrama 6, pasul 3.
 - 1) Organigrama 5, pasul 1. DPT702 nu deține lista de autorizare CRLST1. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - m. Organigrama 6, pașii 4 și 6. (**a cincea căutare a autorizărilor private**). DPT702 nu are autorizare pentru lista de autorizare CRLST1.
 - n. Organigrama 6, pașii 7, 9 și 10. DPTAR este următorul profil de grup al lui WAGNERB.
 - o. Organigrama 6, pașii 1 și 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
 - p. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPTAR nu deține fișierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - q. Organigrama 6, pașii 4 și 6. (**a șasea căutare a autorizărilor private**). DPTAR nu are autorizare pentru fișierul CRLIMWRK.
 - r. Organigrama 6, pașii 7 și 8. Obiectul de verificat = CRLST1 *AUTL
 - s. Organigrama 6, pasul 3.
 - 1) Organigrama 4, pasul 1. DPTAR nu deține lista de autorizare CRLST1. Revenire la Organigrama 6 cu nici o autorizare găsită.
 - t. Organigrama 6, pașii 4 și 5. Autorizat. DPTAR este grupul primar pentru lista de autorizare CRLST1 și are autorizarea *ALL.

Rezultat: WAGNERB este autorizat să efectueze operația cerută folosind autorizarea grupului primar al lui DPTAR pentru lista de autorizare CRLST1.

Analiză: Acest exemplu demonstrează o proiectare slabă a autorizărilor, atât din punct de vedere al gestiunii, cât și din punct de vedere al performanțelor. Sunt folosite prea multe opțiuni, ceea ce face dificilă înțelegerea, modificarea și auditarea. Autorizările private sunt căutate de 6 ori, ceea ce poate produce probleme de performanță 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 secvenței profilurilor de grup ale lui WAGNERB ar schimba caracteristicile de performanță 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 fișierul CRLIMWRK
- Autorizarea lui WAGNERB pentru lista de autorizare CRLST1
- Autorizarea lui DPTAR pentru fișierul CRLIMWRK

Planificarea cu grijă a profilurilor de grup și a listelor de autorizare este esențială pentru performanțe bune ale sistemului.

Cache-ul de autorizări

În Versiunea 3, Ediția 7, sistemul creează un cache de autorizări pentru un utilizator prima dată când utilizatorul accesează un obiect. De fiecare dată când obiectul este accesat, sistemul caută autorizarea în cache-ul utilizatorului înainte de a căuta în profilul utilizatorului. Aceasta rezultă într-o verificare mai rapidă a autorizării private.

Cache-ul de autorizare conține până la 32 autorizări private pentru obiecte și 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 curățate când este efectuat IPL-ul sistemului.

Cât timp este recomandată folosirea limitată a autorizărilor private, cache-ul oferă flexibilitate. De exemplu, puteți alege cum să securizați obiecte cu mai puțină grijă legată de impactul asupra performanțelor sistemului. Acest lucru este adevărat în mod special dacă utilizatorii accesează aceleași obiecte în mod repetat.

Capitolul 6. Securitate control funcționare

Acest capitol discută probleme de securitate asociate cu controlul funcționării în sistem:

- Inițiere job
- Stații de lucru
- Descrieri de subsistem
- Descrieri de job
- Liste de biblioteci
- Tipărire
- Atribute rețea
- Reglare performanță

Pentru informații complete despre subiectele de control funcționare, vedeți cartea *Work Management*.

Inițiere job

Când porniți un job în sistem, obiectele sunt asociate cu jobul, cum ar fi o coadă de ieșire, o descriere de job și bibliotecile din lista de biblioteci. Autorizarea pentru unele dintre aceste obiecte este verificată înainte de a se permite jobului să pornească și este verificată pentru alte obiecte după ce pornește jobul. Autorizarea necorespunzătoare poate cauza erori sau oprirea jobului.

Obiectele care sunt parte a structurii jobului pot fi specificate în descrierea de job, profilul utilizator și în comanda SBMJOB (Submit Job - Lansare job) pentru un job batch.

Pornirea unui job interactiv

Următoarea este o descriere a activității de securitate realizate când un job interactiv este pornit. Pentru că există multe posibilități pentru specificarea obiectelor folosite de către un job, acesta este doar un exemplu.

Când un eșec de autorizare survine în timpul procesului de semnare, în partea de jos a ecranului de Semnare apare un mesaj care descrie eroarea. Unele eșecuri de autorizare cauzează de asemenea scrierea în istoricul jobului. Dacă un utilizator nu poate să se semneze din cauza unui eșec de autorizare, modificați fie profilul utilizator pentru a specifica un obiect diferit sau acordați autorizarea utilizator pentru obiect.

După ce utilizatorul introduce un ID utilizator și parola, acești pași sunt realizați înainte de pornirea efectivă a unui job în sistem:

1. Sunt verificate profilul utilizator și parola. Starea profilului utilizator trebuie să fie *ENABLED. Profilul utilizator care este specificat pe ecranul de semnare trebuie să aibă autorizările *OBJOPR și *CHANGE.
2. Autorizarea utilizator de folosit la verificarea stației de lucru. Vedeți “Stații de lucru” la pagina 177 pentru detalii.
3. Sistemul verifică autorizarea pentru valorile din profilul utilizator și din descrierea de job utilizator care sunt folosite pentru a construi structura jobului, cum este:

- Descriere de job
- Coadă de ieșire
- Bibliotecă curentă
- Biblioteci în lista de biblioteci

Dacă oricare dintre aceste obiecte nu există sau utilizatorul nu are autorizarea corespunzătoare, este afișat un mesaj în partea de jos a ecranului de Semnare și 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 și coada de joburi nu este verificată până când utilizatorul nu încearcă să le folosească.

După ce este pornit jobul, sunt realizați acești pași 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 și orice obiecte folosite de către program. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului pe ecranul de Semnare și se oprește jobul.
2. Dacă intrare de rutare specifică comanda procesor (QCMD):
 - a. Verificarea de autorizare este făcută pentru programul procesor QCMD, biblioteca program și orice obiecte folosite așa cum este descris la pasul 1.
 - b. Autorizarea utilizator pentru programul și biblioteca tratare-tastă-atenție este verificată. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului și este scris în istoricul jobului. Procesarea continuă. Dacă autorizarea este corespunzătoare, programul tratare-tastă-atenție este activat. Programul nu este pornit până la prima apăsare a tastei Atenție 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 inițial (și obiectele sale asociate) specificate în profilul utilizator. Dacă autorizarea este corespunzătoare, programul este pornit. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului și este scris în istoricul jobului. Jobul se oprește.
 - d. Verificarea autorizării normale este făcută pentru meniul inițial (și obiectele sale asociate) specificate în profilul utilizator. Dacă autorizarea este corespunzătoare, meniul este afișat. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului și este scris în istoricul jobului. Jobul se oprește.

Pornirea unui job batch

Următoarea este o descriere a activității de securitate realizate când un job batch este pornit. Deoarece există mai multe metode pentru lansarea de joburi batch și pentru specificarea obiectelor folosite de către job, aceasta este doar linie de îndrumare. Acest exemplu folosește un job lansat de la un job interactiv folosind comanda SBMJOB (submit job - lansare job).

Când introduceți comanda SBMJOB, această verificare este realizată înainte ca jobul să fie adăugat în coada de joburi:

1. Dacă specificați un profil utilizator în comanda SBMJOB, trebuie să aveți autorizarea *USE pentru profilul utilizator.
2. Autorizarea este verificată pentru obiectele specificate ca parametrii în comanda SBMJOB și în descrierea de job. Autorizarea este verificată pentru profilul utilizator sub care rulează jobul.
3. Dacă nivelul de securitate este 40 și comanda SBMJOB specifică USER(*JOB), utilizatorul care lansează jobul trebuie să aibă autorizarea *USE pentru profilul utilizator din descrierea de job.
4. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului și jobul nu este lansat.

Când sistemul selectează jobul din coada de joburi și încearcă să pornească jobul, the job, secvența de verificare autorizare este similară cu secvența pentru pornirea unui job interactiv.

Autorizarea adoptată și joburile batch

Când este pornit un job nou, este creată o nouă stivă program pentru job. Autorizarea adoptată nu poate avea efect până când primul program este adăugat în stiva program. Autorizarea adoptată nu poate fi folosită pentru a obține acces la orice obiecte, cum este o coadă de ieșire 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 lanșați jobul, acea autorizare adoptată nu este folosită când autorizarea este verificată pentru obiectele din cererea dumneavoastră SBMJOB.

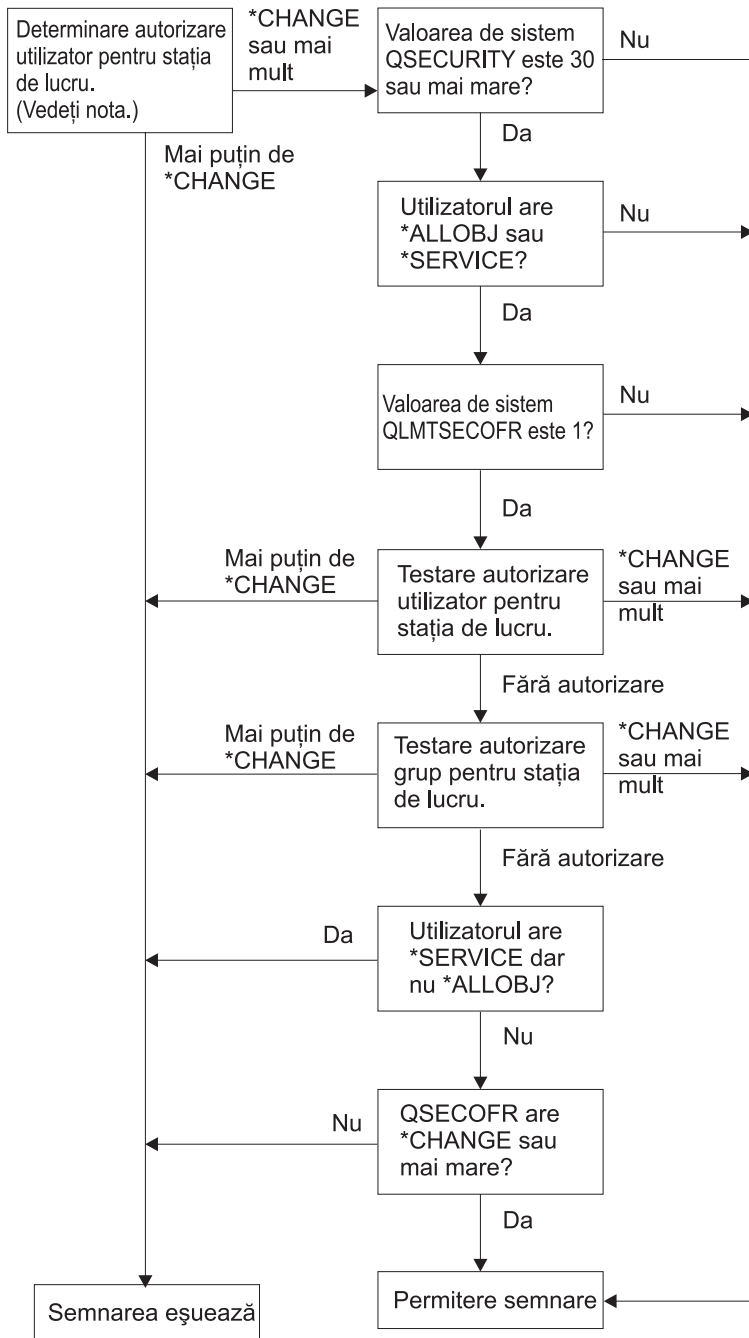
Puteți să modificați caracteristicile unui job batch când așteaptă să ruleze, folosind comanda CHGJOB (Change Job - Modifică job). Vedeți 368 pentru autorizarea care este necesară pentru a modifica parametrii pentru un job.

Stații de lucru

O *descriere de dispozitiv* conține informații despre un dispozitiv particular sau o unitate logică care este atașată sistemului. Când vă semnați în sistem, stația dumneavoastră de lucru este atașată fie la o descriere de dispozitiv fizic sau virtual. Pentru a semna cu succes, trebuie să aveți 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 autorizați specific pentru descrierile de dispozitiv.

Figura 30 la pagina 178 arată logica pentru a determina dacă unui utilizator îi este permis să se semneze la un dispozitiv:



RBAFW529-0

Figura 30. Verificare autorizare pentru Stații de lucru

Notă: Verificarea autorizării normale este realizată pentru a determina dacă un utilizator are cel puțin autorizarea *CHANGE pentru o descriere de dispozitiv. Autorizarea *CHANGE poate fi găsită utilizând următoarele:

- Autorizarea specială *ALLOBJ din profilul utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea privată pentru descrierea de dispozitiv din profilul utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea pentru o listă de autorizări folosită pentru a securiza descrierea de dispozitiv.
- Autorizarea pentru o listă de autorizări folosită pentru a securiza autorizarea publică.

Verificarea de autorizare pentru descrierea de dispozitiv este făcută înainte ca orice programe să fie în stiva program pentru job; de aceea autorizarea adoptată nu se aplică.

Descrierea Verificării autorizare pentru Stațiile de lucru

Sistemul determină autorizarea utilizator pentru stația de lucru. (Vedeți nota 1) Dacă autorizarea este mai puțin decât *CHANGE atunci semnarea eșuează. 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 stația de lucru. Dacă autorizarea utilizator este *CHANGE sau mai înaltă, atunci semnarea este permisă. Dacă autorizarea utilizator este mai puțin decât *CHANGE, semnarea eșuează. Dacă utilizatorul nu are nici o autorizare pentru stația de lucru, sistemul verifică autorizarea de grup utilizator pentru stația de lucru.

Dacă autorizarea de grup utilizator este *CHANGE sau mai înaltă, atunci semnarea este permisă. Dacă autorizarea de grup utilizator este mai puțin decât *CHANGE, semnarea eșuează. Dacă utilizatorul nu are nici o autorizare pentru stația de lucru, sistemul verifică dacă utilizatorul are sau nu autorizarea specială *SERVICE, dar nu și autorizarea specială *ALLOBJ.

Dacă utilizatorul are autorizarea specială *SERVICE, dar nu are autorizarea specială *ALLOBJ atunci semnarea eșuează. Dacă utilizatorul are autorizarea specială *SERVICE, dar nu are autorizarea specială *ALLOBJ, atunci sistemul verifică dacă QSECOFR are *CHANGE sau mai înaltă.

Dacă QSECOFR nu are *CHANGE sau mai înaltă, semnarea eșuează. Dacă QSECOFR are *CHANGE sau mai înaltă, atunci semnarea este permisă.

Profilurilor utilizator responsabil cu securitatea (QSECOFR), service (QSRV), service de bază (QSRVBAS) li se permite întotdeauna să se semneze la consolă. Valoarea de sistem QCONSOLE (consolă) este folosită pentru a determina care dispozitiv este consola. Dacă profilurile QSRV sau QSRVBAS încearcă să se semneze la consolă și nu au autorizarea *CHANGE, sistemul acordă autorizarea *CHANGE profilului și îi permite să se semneze.

Proprietatea asupra descrierilor de dispozitiv

- | 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 stație de lucru, setați autorizarea publică pentru stația de lucru la *EXCLUDE și dați 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 dați autorizarea responsabil cu securitatea *CHANGE dispozitivelor. Oricine cu autorizarea *OBJMGT și *CHANGE pentru un dispozitiv poate da autorizarea *CHANGE altui utilizator.

Dacă o descriere de dispozitiv este creată de către responsabilul cu securitatea, acesta deține acel dispozitiv și îi este data autorizarea specifică *ALL pentru acel dispozitiv. Când sistemul configurează automat dispozitive, cele mai multe dintre ele sunt deținute de către profilul QPGMR. Dispozitivele create de programul QLUS (dispozitive tip *APPC) sunt deținute de către profilul QSYS.

Dacă planificați să folosiți valoarea de sistem QLMTSECOFR pentru a limita unde să se poată semna responsabilul cu securitatea, orice dispozitive pe care le creați trebuie să fie deținute de un alt profil decât QSECOFR.

Pentru a modifica dreptul de proprietate al unei descrieri de dispozitiv afișare, dispozitivul trebuie să fie alimentat și activat. Semnați-vă la dispozitiv și modificați dreptul de proprietate folosind comanda CHGOBJOWN. Dacă nu sunteți semnat la dispozitiv, trebuie să alocați dispozitivul înainte să modificați dreptul de proprietate, folosind comanda ALCOBJ (Allocate Object - Alocare obiect). Puteți aloca dispozitivul doar dacă nimeni nu îl folosește. După ce ați modificat dreptul de proprietate, dezalocați dispozitivul folosind comanda DLCOBJ (Deallocate Object - Dezalocare obiect).

Fișierul de afișare pentru ecranul de semnare

Administratorul de sistem poate modifica ecranul de semnare sistem pentru a adăuga text sau logo-ul companiei. Trebuie să aveți grijă pentru a fi sigur că numele câmpului sau lungimile buffer-ului fișierului de afișare nu sunt modificate când se adaugă text la fișierul de afișare. Modificarea numelor câmpului sau a lungimilor buffer-ului poate cauza eșecul semnării.

Modificarea fișierului de afișare pentru semnare

Codul sursă pentru fișierul de afișare semnare este livrat cu sistemul de operare. Sursa este livrată în fișierul QSYS/QAWTSSRC. Acest cod sursă poate fi modificat pentru a adăuga text la afișarea ecranului de semnare. Numele de câmp și lungimile buffer-ului nu trebuie modificate.

Sursa fișierului de afișare pentru ecranul de semnare

Sursa pentru fișierul de afișare semnare este livrată ca un membru (QDSIGNON sau QDSIGNON2) în fișierul fizic QSYS/QAWTSSRC. QDSIGNON conține sursa pentru sursa ecranul de semnare folosit când valoarea de sistem QPWLVL este setată la 0 sau la 1. Membrul QDSIGNON2 conține sursa ecranului de semnare folosit când valoarea de sistem QPWLVL este setată la 2 sau la 3.

Fișierul QSYS/QAWTSSRC este **șters sau restaurat** de fiecare dată când sistemul de operare i5/OS este instalat. Dacă planificați să creați propria dumneavoastră versiune a ecranului de semnare, atunci trebuie mai întâi să copiați fișierul membru sursă corespunzător, fie QDSIGNON fie QDSIGNON2 în fișierul dumneavoastră sursă și să faceți modificări în copia din fișierul dumneavoastră sursă.

Modificarea fișierului de afișare pentru semnare

Pentru a modifica formatul ecranului de afișare:

1. Crearea unui fișier de afișare semnare modificat.

Un câmp ascuns în fișierul de afișare numit UBUFFER poate fi modificat pentru a gestiona câmpurile mai mici. UBUFFER are 128 de octeți lungime și este stabilit ca ultimul câmp din fișierul de afișare. Acest câmp poate fi modificat pentru a funcționa ca un buffer de intrare/ieșire astfel încât datele specificate în acest câmp al ecranului vor fi disponibile pentru programul aplicație când este pornit jobul interactiv. Puteți să modificați câmpul UBUFFER pentru a conține atâtea câmpuri mai mici câte aveți nevoie, dacă sunt îndeplinite următoarele cerințe:

- Noile câmpuri trebuie să urmeze toate celelalte câmpuri din fișierul de afișare. Locația câmpurilor din ecran nu contează atâta timp cât ordinea în care sunt puse în specificațiile descrierii de date (DDS) îndeplinește această cerință.
- Lungimea trebuie să fie în total 128. Dacă lungimea câmpurilor este mai mult de 128, unele date nu vor fi transmise.
- Toate câmpurile trebuie să fie de intrare/ieșire (tipul B în sursă DDS) sau ascunse (tipul H în sursă DDS).

2. Ordinea în care câmpurile din fișierul de afișare semnare sunt declarate nu trebuie modificată. Poziția în care ele sunt arătate pe ecran poate fi modificată. Nu modificați numele de câmp existente din sursa pentru fișierul de afișare ecran de semnare.

3. Nu modificați dimensiunea totală a buffer-lor de intrare sau ieșire. Pot apărea probleme serioase dacă ordinea sau dimensiunea buffer-lor este modificată.

4. Nu folosiți funcția de ajutor specificații descrierii de date (DDS) din fișierul de afișare semnare.

5. Modificați o descriere de subsistem pentru a folosi fișierul de afișare modificat în locul valorii implicite sistem a QSYS/QDSIGNON. Puteți modifica descrierile de subsistem pentru subsistemele pe care vreți să folosiți noul ecran. Pentru a modifica descrierea de subsistem:
 - a. Folosiți comanda CHGSBSD (Change Subsystem Description - Modificare descriere de subsistem).
 - b. Specificați noul fișier de afișare în parametrul SGNDSPF.
 - c. Folosiți o versiune de test a subsistemului pentru a verifica dacă ecranul este valid înainte de a încerca să modificați subsistemul de control.
6. Testați modificarea.
7. Modificați alte descrieri de subsistem.

Note:

1. Lungimea buffer-ului pentru fișierul de afișare trebuie să fie 318. Dacă este mai puțin decât 318, subsistemul folosește ecranul de afișare implicit QDSIGNON din biblioteca QSYS când valoarea de sistem QPWLVL este 0 sau 1 și QDSIGNON2 din biblioteca QSYS când QPWLVL este 2 sau 3.
2. Linia de copyright nu poate fi ștearsă.

Descrierile de subsistem

Control descrieri de subsistem:

- Cum intră joburi-le în sistemul dumneavoastră
- Cum sunt pornite joburi-le
- Caracteristici de performanță ale joburi-lor

Doar câțiva utilizatori trebuie să fie autorizați pentru a modifica descrieri de subsistem și modificările trebuie monitorizate cu atenție.

Controlarea felului în care intră joburile în subsistem

Mai multe descrieri de subsistem sunt livrate cu sistemul dumneavoastră. După ce ați modificat nivelul dumneavoastră de securitate (valoarea de sistem QSECURITY) la nivelul 20 sau mai sus, semnarea fără a introduce un ID utilizator și o parolă nu este permisă cu subsistemele livrate de IBM.

Totuși, definirea unei combinații de descriere de subsistem și descriere de job care permite semnarea implicită (nici un ID utilizator și nici o parolă) este posibilă și reprezintă o expunere de securitate. Când sistemul rutează un job interactiv, privește intrarea stației 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 (și parola) în ecranul de Semnare. Dacă descrierea de job specifică un profil utilizator în câmpul *Utilizator*, oricine poate apăsa tasta Enter pentru a se semna ca acel utilizator.

La nivelurile de securitate 30 sau mai înalte, sistemul înregistrează în istoric o intrare (tip AF, sub-tip S) în jurnalul de auditare, dacă este încercată semnarea implicită și funcția de auditare este activă. La nivelul de securitate 40 și mai sus, sistemul nu permite semnarea implicită, chiar dacă o combinație de intrare de stație de lucru și descriere de job există și ar permite semnarea implicită. Vedeți “Semnarea fără ID de utilizator și parolă” la pagina 14 pentru informații suplimentare.

Fiți siguri că toate intrările stației de lucru pentru subsistemele interactive se referă la descrierile de job cu USER(*RQD). Controlați autorizarea pentru modificarea descrierilor de job și monitorizați orice modificări care sunt făcute descrierilor de job. Dacă funcția 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 comunicații dintr-o descriere de subsistem controlează felul cum joburi-le de comunicații intră în sistemul dumneavoastră. O intrare de comunicații indică spre un profil utilizator implicit, care permite unui job să fie pornit fără un ID utilizator și o parolă. Aceasta reprezintă o potențială expunere de securitate. Evaluați intrările de comunicații

din sistemul dumneavoastră și folosiți atribute de rețea pentru a controla felul cum joburi-le de comunicații intră în sistemul dumneavoastră. "Atributele de rețea" la pagina 189 discutați atributele de rețea care sunt importante pentru securitate.

Descrieri de job

O descriere de job este o unealtă valoroasă pentru securitate și controlul funcționării. Puteți de asemenea să setați o descriere de job pentru un grup de utilizatori care necesită aceeași listă de biblioteci inițială, coadă de ieșire și coadă de job. Puteți seta o descriere de job pentru un grup de joburi batch care au cerințe similare.

O descriere de job reprezintă o potențială expunere de securitate. În unele cazuri, o descriere de job care specifică un nume de profil pentru parametrul USER poate permite unui job să intre în sistem fără verificări de securitate adecvate. "Controlarea felului în care intră joburile în subsistem" la pagina 181 discutați cum poate fi aceasta împiedicată pentru joburi-le interactive și de comunicații.

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 și pentru profilul utilizator specificat în descrierea de job. Aceasta reprezintă o expunere de securitate. La nivelul de securitate 40 și mai înalt, cel care lansează jobul necesită autorizare atât pentru descrierea de job cât și pentru profilul utilizator.

De exemplu:

- USERA nu este autorizat pentru fișierul PAYROLL.
- USERB are autorizarea *USE pentru fișierul PAYROLL și pentru programul PRLIST, care listează fișierul PAYROLL.
- Descrierea de job PRJOBDB specifică USER(USERB). Autorizarea publică pentru PRJOBDB este *USE.

La nivelul de securitate 30 sau mai jos, USERA poate lista fișierul stat de plată prin lansarea unui job batch:

```
SBMJOB RQSDTA("Ape1ați PRLIST") JOBDB(PRJOBDB) +  
USER(*JOBDB)
```

Puteți preveni aceasta prin folosirea nivelului de securitate 40 sau prin controlarea autorizării pentru descrierile de job care specifică un profil utilizator.

Uneori, un nume de profil utilizator specific într-o descriere de job este necesar pentru anumite tipuri de lucru batch pentru a funcționa 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 și are autorizarea *USE pentru descrierea de job QBATCH, poate lansa lucrul sub profilul utilizator programator (QPGMR), indiferent dacă utilizatorul are sau nu autorizarea pentru profilul utilizator QPGMR. La nivelul de securitate 40 sau mai înalt, autorizarea *USE pentru profilul QPGMR este de asemenea necesară.

Coadă de mesaje operator sistem

Meniul iSeries Asistent operațional (ASSIST) furnizează o opțiune pentru a gestiona sistemul dumneavoastră, utilizatorii și dispozitivele. Meniul Gestionare sistem, utilizatori și dispozitive furnizează o opțiune pentru a lucra cu mesajele operatorului sistem. S-ar putea să vreți să împiedicați 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 și *ADD pentru coada de mesaje. Înlăturarea mesajelor necesită autorizările *USE și *DLT. (Vedeți 391.) Dați autorizarea de a răspunde la mesaje și de a înlătura mesaje în QSYSOPR doar utilizatorilor cu responsabilitate operator sistem. Autorizarea publică pentru QSYSOPR trebuie să fie *OBJOPR și *ADD, care permit adăugarea de mesaje noi la QSYSOPR.

Atenție: Toate joburi-le necesită abilitatea de a adăuga mesaje noi în coada de mesaje QSYSOPR. Nu faceți autorizarea publică pentru QSYSOPR *EXCLUDE.

Listele de biblioteci

Lista de biblioteci pentru un job indică care biblioteci sunt căutate și 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 și numele bibliotecii. Sau bibliotecă pentru obiect poate fi specificată ca *LIBL (listă de biblioteci). Bibliotecile din lista de biblioteci sunt căutate în ordine până când este găsit obiectul.

Tabela 117 rezumă părțile din lista de biblioteci și cum sunt ele construite în timpul unui job. Secțiunile care urmează discută riscurile și măsurile de protecție pentru lista de biblioteci.

Tabela 117. Părți ale listei de biblioteci. Lista de biblioteci este căutată în această ordine:

Parte	Cum este construită
Porțiune sistem 15 intrări	Construită inițial folosind valoarea de sistem QSYSLIBL. Poate fi modificată în timpul unui job folosind comanda CHGSYSLIBL.
Porțiune bibliotecă produs 2 intrări	Blanc inițial. O bibliotecă este adăugată la porțiunea bibliotecă produs a listei de biblioteci când o comandă sau un meniu rulat au fost create cu o bibliotecă în parametrul PRDLIB. Bibliotecă rămâne în porțiunea bibliotecă produs a listei de biblioteci până când comanda sau meniul se termină.
Bibliotecă curentă 1 intrare	Specificată în profilul utilizator sau pe ecranul de semnare. Poate fi modificată când o comandă sau un meniu rulat specifică o bibliotecă pentru parametrul CURLIB. Poate fi modificată în timpul jobului cu comanda CHGCURLIB.
Porțiune utilizator 250 intrări	Construită inițial prin folosirea listei de biblioteci inițiale din descrierea jobului utilizatorului. Dacă descrierea de job specifică *SYSVAL, este folosită valoarea de sistem QUSRLIBL. În timpul unui job, porțiunea utilizator a listei de biblioteci poate fi modificată cu comenzile ADDLIBL, RMVLIBL, CHGLIBL și EDTLIBL.

Riscurile de securitate ale listelor de biblioteci

Listele de biblioteci reprezintă o potențială 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 funcții care să încalce cerințele dumneavoastră de securitate.

“Securitatea bibliotecii și listele de biblioteci” la pagina 115 furnizează unele informații generale despre problemele asociate cu listele de biblioteci. Acest subiect oferă mai multe exemple specifice de expuneri posibile și modul cum pot fi evitate.

Următoarele două exemple arată cum modificările dintr-o listă de biblioteci pot duce la încălcarea cerințelor de securitate:

Modificarea funcției

Figura 31 la pagina 184 arată o bibliotecă de aplicație. Programul A apelează Programul B, despre care se așteaptă să fie în LIBA. Programul B realizează actualizări în Fișierul A. Programul B este apelat fără un nume calificat, astfel încât lista de biblioteci este căutată până când este găsit Program B.

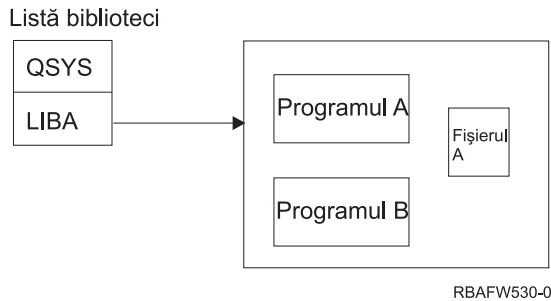


Figura 31. Lista de biblioteci—Mediu așteptat

Un programator sau alt utilizator informat poate pune alt Program B în biblioteca LIBB. Programul înlocuit poate realiza funcții diferite ca facerea unei copii a informațiilor confidențiale sau actualizarea fișierelor incorect. Dacă LIBB este plasată înainte de LIBA în lista de biblioteci, este rulat Program B înlocuit în locul Programului B original, deoarece programul este apelat fără un nume calificat:

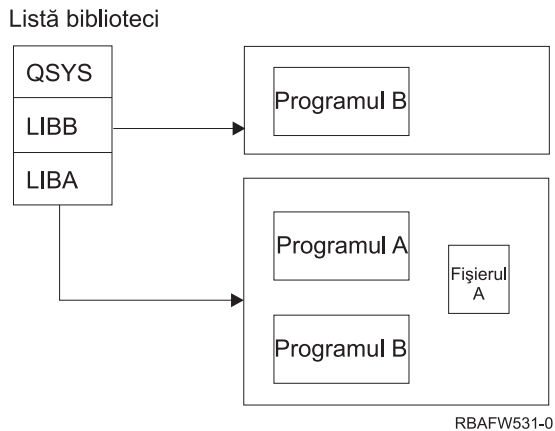


Figura 32. Lista de biblioteci—Mediu real

Acces neautorizat la informații

Să presupunem că Programul A din Figura 31 adoptă autorizarea USER1, care are autorizarea *ALL pentru Fișierul A. Să presupunem că Programul B este apelat de Programul A (autorizarea adoptată rămâne în vigoare). Un utilizator informat poate crea un Program B înlocuitor care apelează pur și simplu procesorul de comandă. Utilizatorul va avea o linie de comandă și acces total la Fișierul A.

Recomandări pentru porțiunea de sistem a listei de biblioteci

Porțiunea sistem a listei de biblioteci este intenționată pentru biblioteci livrate de IBM. Bibliotecile aplicație care sunt controlate cu grijă pot fi de asemenea plasate în porțiunea sistem a listei de biblioteci. Porțiunea 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 și *SECADM poate modifica valoarea sistem QSYSLIBL. Controlați și monitorizați orice modificări la porțiunea sistem a listei de biblioteci. Urmați aceste linii de ghidare când adăugați biblioteci:

- Doar bibliotecile care sunt controlate specific sunt plasate în această listă.
- Publicul nu trebuie să aibă autorizarea *ADD la aceste biblioteci.
- Puține biblioteci livrate de IBM cum este QGPL sunt livrate cu autorizarea publică *ADD din motive de producție. Monitorizați regulat ce obiecte (programe particulare, fișiere sursă și comenzi) sunt adăugate la aceste biblioteci.

Comanda CHGSYSLIBL este livrată cu autorizarea publică *EXCLUDE. Doar utilizatorii cu autorizarea *ALLOBJ sunt autorizați la comandă, doar dacă dumneavoastră acordați autorizare către alți utilizatori. Dacă lista de biblioteci sistem necesită să fie modificată temporar în timpul unui job, puteți folosi tehnica descrisă în subiectul “Modificarea listei de biblioteci de sistem” la pagina 202.

Recomandări pentru biblioteca de produs

Porțiunea bibliotecii de produs a listei de biblioteci este căutată înainte de porțiunea de utilizator. Un utilizator informat poate crea o comandă sau un meniu care înserează o bibliotecă produs în lista de biblioteci. De exemplu, această declarație creează CMDX, care rulează programul PGMA:

```
CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)
```

Cât timp CMDX rulează, LIBB este în porțiunea produs a listei de biblioteci.

Folosiți aceste măsuri pentru a proteja porțiunea produs a listei de biblioteci:

- Controlați autorizarea pentru comenzile CRTCMD (Create Command - Creare comandă), CHGCMD (Change Command - Modificare comandă), CRTMNU (Create Menu - Creare meniu) și CHGMNU (Change Menu - Modificare meniu).
- Când creați comenzi și meniuri, specificați PRDLIB(*NONE), ceea ce înlătură toate intrările prezente în porțiunea produs a listei de biblioteci. Aceasta vă protejează de la a avea căutate biblioteci necunoscute înaintea bibliotecii pe care o așteptați când comanda sau meniul dumneavoastră rulează.

Notă: Valoarea implicită când creați o comandă sau un meniu este PRDLIB(*NOCHG). *NOCHG înseamnă că atunci când comanda sau meniul rulează, porțiunea bibliotecă produs a listei de biblioteci nu este modificată.

Recomandări pentru biblioteca curentă

Biblioteca curentă poate fi utilizată de către unelte suport-decizie cum este Query/400. Orice programe de interogare create de către un utilizator sunt plasate implicit în biblioteca curentă a utilizatorului. Când creați un meniu sau o comandă, puteți specifica o bibliotecă curentă pentru a fi utilizată în timp ce meniul este activ.

Biblioteca curentă furnizează o metodă ușoară pentru utilizator și programator pentru a crea obiecte noi, cum sunt programele de interogare, fără a vă îngrijora despre unde vor fi ele localizate. Totuși, biblioteca curentă ridică un risc de securitate, deoarece este căutată înaintea porțiunii utilizator a listei de biblioteci. Puteți lua mai multe prevederi pentru a proteja securitatea sistemului dumneavoastră în timp ce încă vă folosiți de capacitățile bibliotecii curente:

- Specificați *YES pentru câmpul *Limitare capacități* din profilul utilizator. Aceasta împiedică un utilizator de a modifica biblioteca curentă în ecranul de Semnare sau de la a folosi comanda CHGPRF.
- Restricționați 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) și CHGCMD (Change Command - Modificare comandă).
- Folosiți tehnica descrisă în “Controlarea listei de biblioteci de utilizator” la pagina 201 pentru a seta biblioteca curentă în timpul procesării aplicației.

Recomandări pentru porțiunea de utilizator a listei de biblioteci

Porțiunea utilizator a listei de biblioteci modifică de obicei mai mult decât alte porțiuni și este mai dificil de controlat. Multe programe de aplicație modifică lista de biblioteci. Descrierile de job afectează de asemenea lista de biblioteci pentru un job.

Următoarele sunt unele sugestii alternative pentru controlarea porțiunii utilizator a listei de biblioteci pentru a fi sigur că biblioteci neautorizate cu programe și fișiere înlocuitoare nu sunt folosite în timpul procesării:

- Restricționarea utilizatorilor aplicațiilor de producție la un mediu meniu. Setează câmpul *Limitare capacități* din profilurile utilizator la *YES pentru a restricționa abilitatea lor de a introduce comenzi. “Planificarea meniurilor” la pagina 203 furnizează un exemplu al acestui mediu.
- Folosiți nume calificate (obiect sau bibliotecă) în aplicația dumneavoastră. Aceasta împiedică sistemul de la a căuta lista de biblioteci pentru a găsi un obiect.

- Controlați abilitatea de a modifica descrierile de job, deoarece descrierea de job setează lista de biblioteci inițială pentru un job.
- Folosiți comanda ADDLIBLE (Add Library List Entry - Adăugare intrare lista de biblioteci) la începutul programului pentru a vă asigura că obiectele dorite sunt la începutul porțiunii utilizator a listei de biblioteci. La sfârșitul programului, bibliotecă poate fi înlăturată.

Dacă bibliotecă este deja în lista de biblioteci, dar nu sunteți sigur că este la începutul listei, trebuie să înlăturați bibliotecă și să o adăugați. Dacă ordinea listei de biblioteci este importantă pentru alte aplicații din sistem, folosiți în locul ei următoarea metodă.

- Folosiți un program care extrage și salvează lista de biblioteci pentru un job. Înlocuiți lista de biblioteci cu lista dorită pentru aplicație. Când se termină aplicația, întoarceți lista de biblioteci la setarea originală. Vedeți “Controlarea listei de biblioteci de utilizator” la pagina 201 pentru un exemplu al acestei tehnici.

Tipărirea

Cele mai multe informații care sunt tipărite în sistemul dumneavoastră sunt memorate ca fișier spool într-o coadă de ieșire în timp ce se așteaptă tipărirea. Doar dacă controlați securitatea coșilor de ieșire din sistemul dumneavoastră, utilizatorii neautorizați pot afișa, tipări și chiar copia informații confidențiale care așteaptă să fie tipărite.

O metodă de a proteja ieșirea confidențială este de a crea o coadă de ieșire specială. Trimiteți ieșirea confidențială la coada de ieșire și controlați cine poate vizualiza și manevra fișierele spool în coada de ieșire.

Pentru a determina unde merge ieșirea, sistemul privește în ordine fișierul imprimantă, atributele jobului, profilul utilizator, descrierea dispozitivului stație de lucru și valoarea de sistem dispozitiv de tipărire (QPRTDEV). Dacă sunt folosite valori implicite, este folosită coada de ieșire asociată cu imprimanta QPRTDEV. Cartea *Printer Device Programming* furnizează exemple despre cum se face direcționarea ieșirii spre o anumită coadă de ieșire.

Securizarea fișierelor spool

Un fișier spool este un tip special de obiect în sistem. Nu puteți acorda direct și revoca autorizarea de a vizualiza și manevra un fișier spool. Autorizarea pentru un fișier spool este controlată de mai mulți parametri din coada de ieșire care păstrează fișierul spool.

Când creați un fișier spool, sunteți proprietarul aceluși fișier. Puteți vizualiza și manevra întotdeauna orice fișier spool pe care îl dețineți, indiferent cum este definită autorizarea pentru coada de ieșire. Trebuie să aveți autorizarea *READ pentru a adăuga intrări noi într-o coadă de ieșire. Dacă este înlăturată autorizarea pentru o coadă de ieșire, puteți accesa încă orice intrări pe care le dețineți în acea coadă folosind comanda WRKSPLF (Work with Spooled Files - Gestionare fișiere spool).

Parametrii de securitate pentru o coadă de ieșire sunt specificați folosind comanda CRTOUTQ (Create Output Queue - Creare coadă de ieșire) sau comanda CHGOUTQ (Change Output Queue - Modificare coadă de ieșire). Puteți afișa parametrii de securitate pentru o coadă de ieșire folosind comanda WRKOUTQD (Work with Output Queue Description - Gestionare descriere coadă de ieșire).

Atenție: Un utilizator cu autorizarea specială *SPLCTL poate realiza toate funcțiile pe toate intrările în ciuda felului cum este definită coada de ieșire. Unii parametrii din coada de ieșire permit unui utilizator cu autorizarea specială *JOBCTL să vizualizeze conținutul intrărilor din coada de ieșire.

Parametrul Afișare date (DSPDTA) al cozii de ieșire

Parametrul DSPDTA este proiectat pentru a proteja conținutul unui fișier spool. Determină ce autorizare este necesară pentru a realiza următoarele funcții pe fișierele spool deținute de alți utilizatori:

- comanda DSPSPLF (View the contents of a spooled file - Vizualizarea conținutului unui fișier spool)
- comanda CPYSPLF (Copy a spooled file - Copierea unui fișier spool)
- comanda SNDNETSPLF (Send a spooled file - Trimiterea unui fișier spool)
- comanda CHGSPLFA (Move a spooled file to another output queue - Mutarea unui fișier spool în altă coadă de ieșire)

Valori posibile pentru DSPDTA

*NO	Un utilizator nu poate afișa, trimite sau copia fișiere spool deținute de alți utilizatori decât dacă utilizatorul are una din următoarele: <ul style="list-style-type: none">• autorizarea specială *JOBCTL dacă parametrul OPRCTL este *YES.• autorizare *READ, *ADD și *DLT pentru coada de ieșire dacă parametrul *AUTCHK este *DTAAUT.• Dreptul de proprietate al cozii de ieșire dacă parametrul *AUTCHK este *OWNER.
*YES	Orice utilizator cu autorizarea *READ pentru coada de ieșire poate afișa, copia sau trimite datele fișierelor spool deținute de alții.
*OWNER	Doar proprietarul unui fișier spool sau un utilizator cu *SPLCTL (control spool) poate afișa, copia sau trimite fișierul. Dacă valoarea OPRCTL este *YES, utilizatorii cu autorizarea specială *JOBCTL pot reține, modifica, șterge și elibera fișierele spool din coada de ieșire, dar ei nu pot afișa, copia, trimite sau muta fișierele spool. Aceasta este concepută pentru a permite operatorilor să gestioneze o coadă de ieșire fără a fi capabili să vizualizeze conținutul.

Parametrul Autorizare pentru verificare (AUTCHK) al cozii de ieșire

Parametrul AUTCHK determină dacă autorizările *READ, *ADD și *DLT pentru coada de ieșire permit unui utilizator să modifice și să șteargă fișierele spool deținute de alți utilizatori.

Valori posibile pentru AUTCHK

*OWNER	Doar utilizatorul care deține coada de ieșire poate modifica sau șterge fișierele spool deținute de alții.
*DTAAUT	Specifică dacă orice utilizator cu autorizările *READ, *ADD și *DLT pentru coada de ieșire poate modifica sau șterge fișierele spool deținute de alții.

Parametrul Control operator (OPRCTL) al cozii de ieșire

Parametrul OPRCTL determină dacă un utilizator cu autorizarea specială *JOBCTL poate controla coada de ieșire.

Valori posibile pentru OPRCTL

*YES	Un utilizator cu autorizarea specială *JOBCTL poate realiza toate funcțiile pe fișierele spool doar dacă valoarea DSPDTA este *OWNER. Dacă valoarea DSPDTA este *OWNER, autorizarea specială *JOBCTL nu permite utilizatorului să afișeze, copieze, trimită sau să mute fișierele spool.
*NO	Autorizarea specială *JOBCTL nu dă utilizatorului orice autorizare de a realiza operații asupra cozii de ieșire. Regulile autorizării normale se aplică utilizatorului.

Coadă de ieșire și Parametrul Autorizări necesar pentru tipărire

Tabela 118 la pagina 188 arată ce combinație între parametrii cozii de ieșire și autorizarea pentru coada de ieșire este necesară pentru a realiza funcțiile de gestiune tipărire din sistem. Pentru unele funcții este menționată mai mult de o combinație. Proprietarul unui fișier spool poate realiza întotdeauna toate funcțiile pe acel fișier. Pentru informații suplimentare vedeți “Comenzi pentru scriitor” la pagina 443.

Autorizarea și parametrii cozii de ieșire pentru toate comenzile asociate cu fișiere spool sunt listate pe “Comenzi pentru fișier spool” la pagina 429. Comenzile cozii de ieșire sunt listate pe “Comenzi pentru coadă de ieșire” la pagina 404.

Atenție: Un utilizator cu autorizarea specială *SPLCTL (control spool) nu este subiectul nici unor restricții de autorizare asociate cu cozile de ieșire. Autorizarea specială *SPLCTL permite utilizatorului să realizeze toate operațiile pe toate cozile de ieșire. Evaluați cu grijă acordarea autorizării speciale *SPLCTL pentru orice utilizator.

Tabela 118. Autorizarea necesară pentru a realiza funcții de tipărire

Funcție de tipărire	Parametrii cozii de ieșire			Autorizarea coadă de ieșire	Autorizarea specială
	DSPDTA	AUTCHK	OPRCTL		
Adăugare fișiere spool în coadă ¹			*YES	*READ	Nimic *JOBCTL
Vizualizați lista de fișiere spool (comanda WRKOUTQ ²)			*YES	*READ	Nimic *JOBCTL
Afișare, copiere sau trimitere fișiere spool (DSPSPFL, CPYSPLF, SNDNETSPLF, SNDTCPSF ²)	*YES *NO	*DTAAUT		*READ *READ, *ADD, *DLT	Nimic Nimic
	*NO *YES *NO *OWNER	*OWNER	*YES *YES	Proprietar ³	Nimic *JOBCTL *JOBCTL
Modificare, ștergere, reținere și eliberare fișier spool (CHGSPLFA, DLTSPLF, HLDSPFL, RLSSPLF ²)		*DTAAUT		*READ, *ADD, *DLT	Nimic
		*OWNER	*YES	Proprietar ³	Nimic *JOBCTL
Modificare, curățare, reținere și eliberare coada de ieșire (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ ²)		*DTAAUT		*READ, *ADD, *DLT	Nimic
		*OWNER	*YES	Proprietar ³	Nimic *JOBCTL
Porniți un scriitor pentru coada de ieșire (STRPRTWTR, STRRMTWTR ²)		*DTAAUT	*YES	*CHANGE	Nimic *JOBCTL
			*YES		*JOBCTL

¹ Aceasta este autorizarea necesară pentru a direcționa ieșirea dumneavoastră spre o coadă de ieșire.

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

³ Trebuie să fiți proprietarul cozii de ieșire.

⁴ Necesită de asemenea autorizarea *USE pentru descrierea de dispozitiv de tipărire.

⁵ *CHGOUTQ necesită autorizarea *OBJMGT pentru coada de ieșire, în plus la autorizările *READ, *ADD și *DLT.

Exemple: Coada de ieșire

Următoarele sunt mai multe exemple de setare a parametrilor de securitate pentru cozile de ieșire astfel încât să îndeplinească cerințe diferite:

- Creați o coadă de ieșire cu scop-general. Toți utilizatorii au permisiunea de a afișa toate fișierele spool. Operatorilor sistem le este permis să gestioneze coada și să modifice fișierele spool:

```
CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
```

- Creați o coadă de ieșire pentru o aplicație. Doar membrilor profilului de grup GRPA le este permisă folosirea cozii de ieșire. Toți utilizatorii autorizați ai cozii de ieșire au permisiunea de a afișa toate fișierele spool. Operatorilor sistem nu le este permisă gestionarea cozii de ieșire:

```
CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
USER(GRPA) AUT(*CHANGE)
```

- Creați o coadă de ieșire confidențială pentru responsabilii cu securitatea pentru a o folosi când tipăriți informații despre profilurile și autorizările utilizator. Coada de ieșire este creată și deținută 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 fișierele spool deținute de alți utilizatori ai cozii de ieșire SECOUTQ.

- Creați o coadă de ieșire care este partajată de utilizatorii care tipăresc fișiere și documente confidențiale. Utilizatorii pot gestiona doar propriile fișiere spool. Operatorii sistem pot gestiona fișierele spool, dar nu pot afișa conținutul acestor fișiere.

```
CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +  
AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
```

Atributele de rețea

Atributele de rețea controlează felul cum sistemul dumneavoastră comunică cu alte sisteme. Unele atribute de rețea controlează felul cum sunt tratate cererile la distanță de procesare joburi și acces la informații. Aceste atribute de rețea afectează direct securitatea din sistemul dumneavoastră și sunt discutate în subiectele care urmează:

- Acțiune job (JOBACN)
- Cerere client acces (PCSACC)
- cerere DDM acces (DDMACC)

Sunt arătate valorile posibile pentru fiecare atribut de rețea. Valoarea implicită este subliniat. Pentru a seta valoarea unui atribut de rețea, folosiți comanda CHGNETA (Change Network Attribute - Modificare atribut rețea).

Atributul de rețea Acțiune job (JOBACN)

Atributul de rețea 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 și a fost refuzat, este trimis atât emițătorului cât și receptorului intenționat.
*FILE	Fluxul de intrare este introdus în coada fișierelor de rețea pentru utilizatorul ce recepționează. Acest utilizator poate afișa, anula sau recepționa fluxul de intrare într-un fișier de bază de date sau îl poate lansa într-o coadă de job. Un mesaj care pornește fluxul de intrare care a fost umplut, este trimis atât emițătorului cât și receptorului.
*SEARCH	Tabela job de rețea controlează acțiunile prin folosirea valorilor din tabelă.

Recomandări

Dacă nu vă așteptați să primiți cereri de joburi la distanță în sistemul dumneavoastră, setați atributul de rețea JOBACN la *REJECT.

Pentru informații suplimentare despre atributul JOBACN, vedeți cartea *SNA Distribution Services*.

Atributul de rețea Acces Cerere client (PCSACC)

Atributul de rețea PCSACC determină modul în care programul licențiat iSeries Access pentru Windows procesează cererile de la calculatoarele personale atașate pentru accesarea obiectelor. Atributul de rețea PCSACC controlează dacă joburile calculator personal pot accesa obiecte în sistem și nu dacă calculatorul personal iSeries poate folosi emularea stației de lucru.

Notă: Atributul de rețea PCSACC controlează doar clienții DOS și OS/2. Acest atribut nu are nici un efect pe alt client iSeries Access.

*REJECT	iSeries Access refuză toate cererile de la calculatorul personal pentru a accesa obiecte din sistem iSeries. Un mesaj de eroare este trimis aplicației PC.
*OBJAUT	Programele iSeries Access din sistem verifică autorizările obiect normal pentru fiecare obiect cerut de un program PC. De exemplu, dacă este cerut transferul fișierului, este verificată autorizarea de a copia date din fișierul bază de date.
*REGFAC	Sistemul folosește facilitatea de înregistrare a sistemului pentru a determina ce program de ieșire (dacă e vreunul) să ruleze. Dacă nu este definit nici un program de ieșire pentru un punct de ieșire și această valoare este specificată, este folosit *OBJAUT.
<i>nume program- calificat-</i>	Programul iSeries Access apelează acest program de ieșire scriitor-utilizator pentru a determina dacă cererea PC-ului trebuie să fie refuzată. Programul de ieșire este apelat doar dacă verificarea de autorizare normală pentru obiect are succes. Programul iSeries Access transmite informații despre utilizator și funcția cerută programului de ieșire. Programul întoarce un cod care indică dacă cererea trebuie permisă sau refuzată. Dacă codul retur indică că cererea trebuie refuzată sau dacă apare o eroare, un mesaj de eroare este trimis calculatorului personal.

Riscuri și recomandări

Măsurile de securitate normale în sistemul dumneavoastră s-ar putea să nu fie protecția suficientă dacă programul iSeries Access este instalat în sistemul dumneavoastră. De exemplu, dacă un utilizator are autorizarea *USE pentru un fișier și atributul de rețea PCSACC este *OBJAUT, utilizatorul poate folosi programul iSeries Access și un program din calculatorul personal pentru a transfera tot acel fișier pe calculatorul personal. Utilizatorul poate copia datele pe o dischetă sau o bandă PC și le poate înlătura din punctul de plecare.

Sunt disponibile mai multe metode pentru a împiedica iSeries ca un utilizator stație de lucru cu autorizarea *USE pentru un fișier, să copieze acel fișier:

- Setare LMTCPB(*YES) în profilul utilizator.
- Restricționați autorizarea pentru comenzile care copiază fișiere.
- Restricționați autorizarea pentru comenzile folosite de iSeries Access.
- Nu dați autorizarea utilizator *ADD pentru orice bibliotecă. Autorizarea *ADD este necesară pentru a crea un fișier nou într-o bibliotecă.
- Nu dați accesul utilizator pentru orice dispozitiv *SAVRST.

Nici una din aceste metode nu funcționează pentru utilizatorul PC al programul cu licență iSeries Access. Folosirea unui program de ieșire pentru a verifica toate cererile este singura măsură de protecție adecvată.

Programul iSeries Access transmite informații programului de ieșire utilizator apelat de atributul de rețea PCSACC, pentru următoarele tipuri de acces:

Transfer fișier
tipărire virtuală
Mesaj
Folder partajat

Pentru informații suplimentare despre iSeries Access, consultați Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Atributul de rețea Acces cerere DDM (DDMACC)

Atributul de rețea DDMACC determină cum procesează sistemul cererile de la alte sisteme pentru a accesa date folosind gestiunea de date distribuită (DDM) sau funcția bază de date relațională distribuită.

***REJECT**

Sistemul nu permite orice DDM sau orice cereri DRDA de la sistemele la distanță. *REJECT nu împiedică acest sistem de la a funcționa ca sistemul care cere și a trimite cereri către alte sisteme server.

***OBJAUT**

nume- program- calificat-

Cererile la distanță sunt controlate de autorizarea obiect din sistem.

Acest program scriitor-utilizator este apelat după ce a fost verificată autorizarea obiect normală. Programul de ieșire este apelat doar pentru fișierele DDM, nu pentru funcțiile bază de date relațională distribuită. Programul de ieșire este transmis parametru lista, construit de sistemul la distanță, care identifică utilizatorul sistem local și cererea. Programul evaluează cererea și trimite un cod retur, acordă sau refuză accesul cerut.

Pentru informații suplimentare despre atributul de rețea DDMACC și despre problemele de securitate asociate cu DDM, vedeți Centrul de informare (vedeți "Cerințe preliminare și informații înrudite" la pagina xvi pentru detalii).

Operațiile de salvare și 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 (și șterge 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 investiție financiară substanțială.

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 funcții diferite. De exemplu, presupuneți ca programul original a lucrat cu date confidențiale. Noua versiune poate realiza aceleași funcții, dar poate scrie de asemenea o copie a informațiilor confidențiale într-un fișier secret din biblioteca proprie a programatorului. Programatorul nu are nevoie de autorizare pentru datele confidențiale, deoarece utilizatorii obișnuiți ai programului vor accesa datele.

Restricționarea operațiilor de salvare și restaurare

Puteți controla abilitatea de a salva și restaura obiecte în mai multe căi:

- Restricționați accesul fizic de a salva și restaura dispozitive, cum sunt unități bandă, unități optice și unități de dischetă.
- Restricționați autorizarea pentru obiectele descrieri de dispozitiv pentru a salva și restaura dispozitive. Pentru a salva un obiect pe o unitate bandă, trebuie să aveți autorizarea *USE pentru descrierea de dispozitiv pentru unitatea bandă.
- Restricționați comenzile de salvare și restaurare. Aceasta vă permite să controlați ce este salvat din sistemul dumneavoastră și restaurat în sistemul dumneavoastră prin toate interfețele - prin includerea fișierelor de salvare. Vedeți "Exemplu: Restricționarea comenzilor de salvare și restaurare" pentru un exemplu de cum se face aceasta. Sistemul setează comenzile de restaurare la PUBLIC(*EXCLUDE) când vă instalați sistemul.
- Dați autorizarea specială *SAVSYS doar utilizatorilor de încredere.

Exemplu: Restricționarea comenzilor de salvare și restaurare

Puteți urma acești pași pentru a restricționa salvarea și restaurarea comenzilor pe sistemul dumneavoastră:

1. Pentru a crea o listă de autorizații pe care puteți să o folosiți pentru a da autorizare comenzilor pentru operatorii sistem, tastați următoarele:

```
CRTAUTL AUTL(SRLIST) TEXT('Listă salvare și restaurare')  
AUT(*EXCLUDE)
```

2. Pentru a folosi lista de autorizații pentru a securiza comenzile de salvare, tastați următoarele:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
```

3. Pentru a vă asigura că autorizarea *PUBLIC vine din lista de autorizații, tastați următoarele:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)
```

4. Pentru a folosi lista de autorizații pentru a securiza comenzile de restaurare, tastați următoarele:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
```

5. Pentru a vă asigura că autorizarea *PUBLIC vine din lista de autorizații, tastați următoarele:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)
```

6. Deși operatorii sistem care sunt responsabili pentru salvarea sistemului au autorizarea specială *SAVSYS, ei trebuie acum să aibă dată autorizare explicită pentru comenzile SAVxxx. Faceți aceasta prin adăugarea operatorilor sistem în lista de autorizații:

```
ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)
```

Notă: Puteți vrea ca operatorii sistem ai dumneavoastră să aibă autorizare doar pentru comenzile de salvare. În acest caz, securizați comenzile de salvare și restaurare cu două liste de autorizații separate.

7. Pentru a restricționa API-urile de salvare și restaurare și a le securiza cu lista de autorizații, tastați 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 performanței

Monitorizarea și ajustarea performanței nu este responsabilitatea unui responsabil cu securitatea. Totuși, responsabilul cu securitatea trebuie să se asigure că utilizatorii nu alterează caracteristicile de performanță ale sistemului pentru a mări viteza propriilor joburi pe socoteala altora.

Mai multe obiecte de control funcționare afectează performanța joburi-lor din sistem:

- Clasa setează prioritatea de rulare și felia de timp pentru un job.
- Intrarea de rutare din descrierea de subsistem determină clasa și pool-ul de stocare pe care le folosește jobul.
- Descrierea de job poate determina coada de ieșire, prioritatea de ieșire, coada de joburi și prioritatea job.

Utilizatorii informați cu autorizare corespunzătoare pot crea propriile lor medii în sistem și să-și dea singuri performanță mai bună decât alți utilizatori. Controlați aceasta prin limitarea autorizării de a crea și modifica obiecte de control funcționare. Setări autorizarea publică pentru comenzile de control funcționare la *EXCLUDE și acordați autorizarea pentru puțini utilizatori de încredere.

Caracteristicile de performanță 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 și a nivelurilor de activitate. De asemenea, un utilizator cu autorizarea specială *JOBCTL (job control) poate modifica prioritatea de planificare a oricărui job din sistem, subiect al limitei de prioritate (PTYLMT) din profilul utilizator. Alocați cu grijă autorizarea specială *JOBCTL și PTYLMT în profilurile utilizator.

Pentru a permite utilizatorilor să vizualizeze informațiile de performanță folosind comanda WRKSYSSTS, dar să nu o modifice, faceți următoarele:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
USER(*PUBLIC) AUT(*EXCLUDE)
```

Autorizați utilizatorii responsabili cu ajustarea sistemului să modifice caracteristicile de performanță:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +  
USER(USRRTUNE) AUT(*USE)
```

Restricționarea joburilor la batch

Puteți să creați sau să modificați comenzi pentru a restricționa anumite joburi, astfel încât să fie rulate doar într-un mediu batch. De exemplu, s-ar putea să vreți să rulați anumite rapoarte sau compilări de program în batch. Un job care rulează în batch afectează de obicei performanța sistemului mai puțin decât dacă ar rula interactiv.

De exemplu, pentru a restricționa la batch comanda care rulează programul RPTA, faceți următoarele:

- Creați o comandă pentru a rula RPTA și specificați că acea comandă poate fi rulată doar în batch:
CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)

Pentru a restricționa compilările la batch, faceți următoarele pentru a crea comanda pentru fiecare tip de program:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```


Capitolul 7. Proiectarea securității

Protejarea informațiilor este o parte importantă a majorității aplicațiilor. Securitatea ar trebui considerată, împreună cu alte cerințe, la momentul la care e proiectată aplicația. De exemplu, când vă decideți cum să organizați informațiile aplicației în biblioteci, încercați să echilibrați cerințele de securitate cu alte considerente, cum ar fi performanța aplicației și salvare de rezervă și recuperare.

Acest capitol conține linii de ghidare care să ajute dezvoltatorii de aplicație și managerii de sistem să includă securitatea ca parte a proiectării generale. De asemenea conține exemple de tehnici pe care le puteți folosi pentru a îndeplini obiectivele de securitate din sistemul dumneavoastră. Unele din exemplele din acest capitol conțin programe exemplu. Aceste programe sunt incluse doar cu scop ilustrativ. Multe dintre ele nu vor putea fi compilate sau rulate așa cum sunt, nici nu includ tratarea de mesaje și recuperarea erorii.

Subiectul Securitatea de bază a sistemului și planificarea din Centrul de informare este menit administratorului de securitate. El conține formulare, exemple și linii de ghidare pentru planificarea securității pentru aplicații care au fost deja dezvoltate. Dacă sunteți responsabil pentru proiectarea unei aplicații, veți găsi folositoare revederea formularelor și exemplelor din Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii). Vă pot ajuta să vă vedeți aplicația din perspectiva unui administrator de securitate și să înțelegeți ce informații e nevoie să furnizați.

Subiectul Securitatea de bază a sistemului și planificarea din Centrul de informare folosește de asemenea un set de aplicații exemplu pentru o companie fictivă numită Compania de jucării JKL. Acest capitol discută considerente de proiectare pentru același set de aplicații exemplu. Figura 33 arată relația dintre grupuri de utilizator, aplicații și biblioteci pentru Compania de jucării JKL:

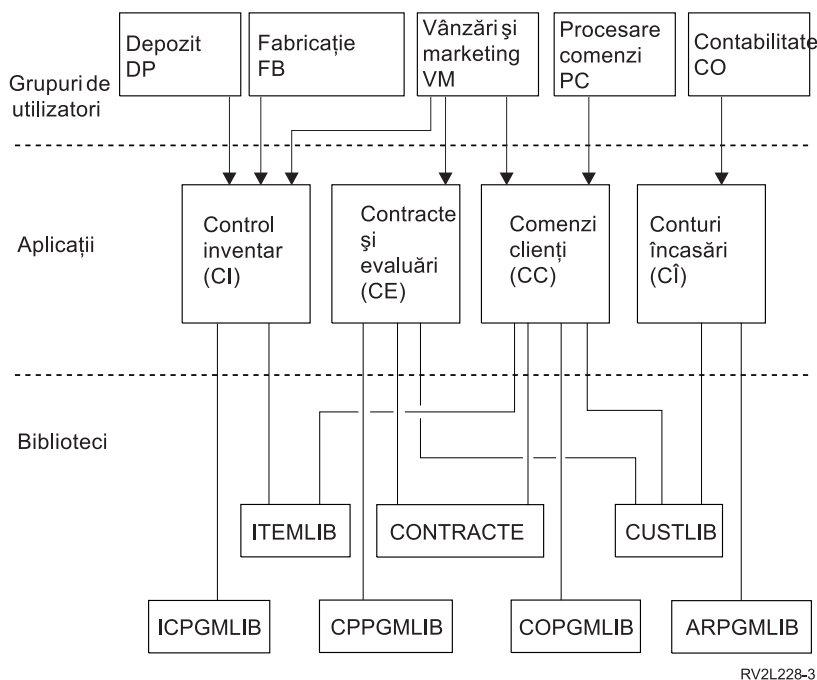


Figura 33. Aplicații exemplu

Descriere grafic

Acest grafic vă arată cum cinci seturi de grupuri de utilizatori accesează aplicații și biblioteci pe sistem la Compania JKL Toy. Grupurile de utilizatori includ Depozit, Producție, Vânzări și Marketing, Procesare comandă și Contabilitate.

Grupurile de utilizatori Depozit, Producție și Vânzări și Marketing pot accesa toate aplicațiile din Control inventar. Grupul de utilizatori Vânzări și Marketing au de asemenea acces la aplicația Contracte și Prețuri și la aplicația Personalizare comandă. Grupul de utilizatori Procesare comandă poate de asemenea accesa aplicația Personalizare comandă. Grupul de utilizatori Contabilitate folosește aplicația Conturi de primit.

Recomandări generale

Recomandările din acest capitol și din subiectul Securitatea de bază a sistemului și planificarea din Centrul de informare se bazează pe un principiu important: simplitatea. Păstrarea proiectării securității cât mai simple face mai ușoară gestionarea și auditarea ei. De asemenea îmbunătățește performanțele aplicației și ale copiei de rezervă.

Urmează o listă de recomandări generale pentru proiectarea securității:

- Folosiți securitatea resurselor împreună cu metodele disponibile, cum ar fi capabilități limitate în profilul utilizator și restricționarea utilizatorilor la un set de meniuri, pentru a proteja informațiile.

Atenție: Nu e suficient să folosiți doar capabilitățile limitate în profilul de utilizator și controlul accesului la meniu pentru a vă securiza sistemul dacă folosiți un produs cum ar fi iSeries Access sau aveți linii de comunicație atașate sistem. Trebuie să folosiți securitatea resurselor pentru a securiza acele obiecte care vreți să nu fie accesibile din aceste interfețe.

- Securizați doar acele obiecte care chiar necesită securitate. Analizați o bibliotecă pentru a determina care obiecte, cum ar fi fișierele de date, sunt confidențiale și securizați-le. Folosiți autorizare publică pentru alte obiecte, cum ar fi zone de date și cozi de mesaje.
- Mutați din general în specific:
 - Planificați securitatea pentru biblioteci și directoare. Lucrați cu obiecte individuale doar când e necesar.
 - Planificați autorizarea publică întâi, urmată de autorizarea de grup și cea individuală.
- Faceți autorizarea publică pentru obiecte noi într-o bibliotecă (parametrul CRTAUT) aceeași ca autorizarea publică pentru majoritatea obiectelor existente în bibliotecă.
- Pentru a face auditarea mai ușoară și a îmbunătăți performanța verificării autorizării, evitați definirea autorizării private care e mai puțin decât autorizarea publică pentru un obiect.
- Folosiți listele de autorizații pentru a grupa obiecte cu aceleași cerințe de securitate. Listele de autorizații sunt mai simple de gestionat decât autorizările individuale și ajută la recuperarea informațiilor de securitate.

Planificarea modificărilor nivelului de parolă

Modificarea nivelurilor parolei ar trebui planificată cu atenție. Operațiile cu alte sisteme pot eșua sau este posibil ca utilizatorii să nu se poată semna în sistem dacă nu ați planificat corespunzător modificarea nivelului parolei. Înainte de a modifica valoarea de sistem QPWDLVL, asigurați-vă că ați salvat datele de securitate folosind comanda SAVSECDTA sau SAVSYS. Dacă aveți o copie de rezervă curentă, veți putea reseta parolele pentru toate profilurile utilizator dacă trebuie să vă întoarceți la un nivel al parolei inferior.

Producele pe care le folosiți în sistem și pe clienții cu care sistemul interfațează, pot avea probleme când valoarea de sistem pentru nivelul parolei (QPWDLVL) este setată la 2 sau 3. Orice produs sau client care trimite parole la sistem într-o formă criptată, mai degrabă decât în forma necriptată în care le introduce un utilizator într-un ecran de semnare, trebuie modernizat pentru a lucra nu noile reguli de criptare a parolei pentru QPWDLVL 2 sau 3. Trimiterea parolei criptate este numită substituirea parolei. Substituirea parolei este folosită pentru a preveni capturarea parolei în timpul transmisiei prin rețea. Substituirile de parolă generate de clienți mai vechi, care nu suportă noul algoritm pentru QPWDLVL 2 sau 3, nu vor fi acceptate chiar dacă sunt corecte caracterele specifice introduse. Aceasta se aplică de asemenea în cazul oricărui acces peer iSeries la iSeries care folosește valorile criptate pentru autentificarea de la un sistem la altul.

Problema este generată de faptul că anumite produse afectate (cum ar fi IBM Toolbox pentru Java) sunt furnizate ca middleware. Un produs terț care încorporează 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 și alte scenarii, este ușor de văzut de ce e necesară planificarea cu atenție înainte de modificarea valorii de sistem QPWLVL.

Considerente pentru modificarea QPWLVL de la 0 la 1

Nivelul de parolă 1 permite ca pe un sistem care nu trebuie să comunice cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) să fie eliminate parolele NetServer. Eliminarea parolelor criptate necesare din sistem crește securitatea generală a sa.

La QPWLVL 1, toate mecanismele curente, pre-V5R1 de înlocuire și autorizare a parolei vor continua să funcționeze. Probabilitatea de a apărea probleme este foarte mică, cu excepția funcțiilor/serviciilor care necesită parola NetServer.

Printre funcțiile/serviciile care necesită parola NetServer se numără:

- iSeries Support for Windows Network Neighborhood, ediția Windows 95/98/ME, (NetServer)

Considerente pentru modificarea QPWLVL de la 0 sau 1 la 2

Nivelul de parolă 2 introduce folosirea parolelor sensibile la majuscule cu lungime de până la 128 de caractere (numite și passphrases) și furnizează abilitatea maximă de a reveni la QPWLVL 0 sau 1.

Indiferent de nivelul de parolă al sistemului, parolele din nivelul 2 și 3 sunt create oricând este modificată o parolă sau când semnează un utilizator în sistem. Deținerea unei parole de nivel 2 și 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 QPWLVL la 2, administratorul de sistem ar trebui să folosească comanda PRTUSRPRF TYPE(*QPWLVL) pentru a localiza toate profilurile utilizator care nu au o parolă care nu poate fi folosită la nivelul 2. În funcție de profilurile localizate, administratorul își poate dori să folosească unul din următoarele mecanisme pentru a adăuga un nivel de parolă 2 și 3 la profiluri.

- Modificați parola pentru profilul 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 și 1; și sistemul de asemenea creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 2 și 3. Sunt create versiuni doar de majuscule și 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 și c4d2rb4y de nivel 2.
- Semnați în sistem printr-un mecanism care prezintă parola în text clar (nu folosește înlocuirea parolei). Dacă parola e validă și profilul utilizator nu are o parolă care poate fi folosită la nivelurile 2 și 3, sistemul creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 2 și 3. Sunt create versiuni doar de majuscule și doar de litere mici pentru folosirea la nivelurile de parolă 2 sau 3.

Absența unei parole care poate fi folosită la nivelul 2 sau 3 poate fi o problemă oricând profilul utilizator nu are o parolă care poate fi folosită la nivelurile 0 și 1 sau când utilizatorul încearcă să semneze printr-un produs care folosește înlocuirea parolei. În aceste cazuri, utilizatorul nu va fi capabil să semneze când nivelul parolei este modificat la 2.

Dacă un profil de utilizator nu are o parolă care poate fi folosită la nivelurile 2 și 3, profilul de utilizator nu are o parolă care poate fi folosită la nivelurile 0 și 1 și utilizatorul semnează printr-un produs care trimite parole în text clar, atunci sistemul validează utilizatorul cu parola de la nivelul 0 de parolă și creează două parole de nivel 2 (așa cum au fost descrise mai sus) pentru profilul utilizator. Următoarele semnări vor fi validate cu parolele din nivelul 2.

Orice client/serviciu care folosește înlocuirea parolei nu va funcționa corect la QPWLVL 2 dacă clientul/serviciul nu a fost actualizat pentru a folosi noua schemă (passphrase) de înlocuire a parolei. Administratorul ar trebui să verifice dacă e necesar un client/serviciu care nu a fost actualizat pentru noua schemă de înlocuire a parolei.

Clientii/serviciile care folosesc înlocuirea parolei includ:

- TELNET
- iSeries Access

- iSeries Servere gazdă
- QFileSrv.400
- Suportul iSeries NetServer Print
- DDM
- DRDA
- SNA LU6.2

Se recomandă insistent ca datele de securitate să fie salvate înainte de a se modifica la QPWDLVL 2. Asta poate ajuta la facerea mai ușoară a tranziției înapoi la QPWDLVL 0 sau 1 dacă e necesar.

Se recomandă să nu fie modificate celelalte valori de sistem ale parolei, cum ar fi QPWDMINLEN și QPWDMAXLEN, decât după o testare a QPWDLVL 2. Asta va face mai ușoară tranziția înapoi la QPWDLVL 1 sau 0 dacă e necesar. Totuși, valoarea de sistem QPWDVLDPGM trebuie să specifice fie *REGFAC fie *NONE înainte ca sistemul să permită ca QPWDLVL să fie modificată la 2. Așadar, dacă folosiți un program de validare a parolei, veți dori să scrieți unul nou care poate fi înregistrat pentru punctul de ieșire QIBM_QSY_VLD_PASSWRD folosind comanda ADDEXITPGM.

Parolele NetServer sunt suportate în continuare la QPWDLVL 2, astfel că orice funcție/serviciu care necesită o parolă NetServer ar trebui de asemenea să funcționeze corect.

După ce administratorul s-a familiarizat cu rularea sistemului la QPWDLVL 2, puteți începe să modificați valorile de sistem ale parolei pentru a exploata parole mai lungi. Totuși, administratorul trebuie să știe că parolele mai lungi vor avea următoarele efecte:

- Dacă sunt specificate parole mai mari de 10 caractere, nivelurile de parolă 0 și 1 sunt curățate. Acest profil utilizator nu va putea semna dacă sistemul este returnat la nivelul de parolă 0 sau 1.
- Dacă parolele conțin caractere speciale sau nu urmează regulile de compoziție pentru nume de obiecte simple (excluzând sensibilitatea la majuscule), parola de nivel 0 și 1 e ștearsă.
- Dacă sunt specificate parole mai mari de 14 caractere, este ștearsă parola NetServer pentru profilul de utilizator.
- Valorile de sistem ale parolei se aplică doar la valoarea 2 a nivelului de parolă, nu și la parolele de nivel 0 și 1 generate de sistem sau valorile parolelor NetServer (dacă sunt generate).

Considerente pentru modificarea QPWDLVL de la 2 la 3

După ce rulați sistemul la QPWDLVL 2 pentru o perioadă de timp, administratorul poate lua în considerare mutarea la QPWDLVL 3 pentru a maximiza protecția securității prin parole.

La QPWDLVL 3, toate parolele NetServer sunt șterse, așa 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 și 1 sunt curățate. Administratorul poate folosi comenzile DSPAUTUSR sau PRTUSRPRF pentru a localiza profilurile utilizator care nu au parole de nivel 2 sau 3 asociate cu ele.

Trecerea la un nivel de parolă mai scăzut

Întoarcerea la o valoare QPWDLVL mai mică, chiar dacă e posibilă, nu e așteptată ca o operație lipsită de probleme. În general, ar trebui să fie un singur sens de la valori QPWDLVL mai mici la valori QPWDLVL mai mari. Totuși, pot fi cazuri în care o valoare QPWDLVL mai mică trebuie să fie refăcută.

Următoarele secțiuni discută munca necesară pentru a vă întoarce la un nivel de parolă mai mic.

Considerente pentru modificarea QPWDLVL de la 3 la 2

Această modificare e relativ ușoară. După ce s-a setat QPWDLVL la 2, administratorul trebuie să determine dacă este necesar ca vreun profil de utilizator să conțină parole NetServer sau parole de nivel 0 sau 1 și, dacă este așa, 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 și nivelul de parolă 0 sau 1, dacă sunt necesare aceste parole.

Considerente pentru modificarea QPWDLVL de la 3 la 1 sau 0

Din cauza potențialului foarte mare de a cauza probleme pentru sistem (cum ar fi faptul că nimeni nu poate semna deoarece toate parolele de nivel 0 și 1 au fost curățate), această modificare nu e suportată direct. Pentru a modifica de la QPWDLVL 3 la QPWDLVL 1 sau 0, sistemul trebuie să facă mai întâi modificarea intermediară la QPWDLVL 2.

Considerente pentru modificarea QPWDLVL de la 2 la 1

Înainte de la modifica QPWDLVL la 1, administratorul trebuie să folosească comanda DSPAUTUSR sau PRTUSRPRF TYPE(*PWDINFO) pentru a localiza profilurile de utilizator care nu au o parolă de nivel 0 sau 1. Dacă profilul de utilizator va necesita o parolă după ce se modifică QPWDLVL, administratorul trebuie să se asigure că e creată o parolă de nivel 0 și 1 pentru profil folosind unul din următoarele mecanisme:

- Modificați parola pentru profilul utilizator folosind comanda CHGUSRPRF sau CHGPWD CL sau API-ul QSYCHGPW API. Asta va face ca sistemul să modifice parola care poate fi folosită la nivelurile 2 și 3; și sistemul de asemenea creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 0 și 1. Sistemul e capabil să creeze parola de nivel 0 și 1 doar dacă sunt îndeplinite următoarele condiții:
 - Parola are o lungime de 10 caractere sau mai puțin.
 - Parola poate fi convertită la caractere cu majuscule EBCDIC A-Z, 0-9, @, #, \$ și liniuță de subliniere.
 - Parola nu începe cu un caracter numeric sau liniuță de subliniere.

De exemplu, modificarea parolei la o valoare de RainyDay va rezulta în generarea de către sistem a parolei de nivel 0 și 1 RAINYDAY. Dar modificarea valorii parolei la Rainy Days In April va face ca sistemul să curețe parola de nivel 0 și 1 (deoarece parola e prea lungă și conține spații).

Nu e produs nici un mesaj sau indicație dacă parola de nivel 0 sau 1 nu a putut fi creată.

- Semați în sistem printr-un mecanism care prezintă parola în text clar (nu folosește înlocuirea parolei). Dacă parola e validă și profilul utilizator nu are o parolă care poate fi folosită la nivelurile 0 și 1, sistemul creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 0 și 1. Sistemul e capabil să creeze parola de nivel 0 și 1 doar dacă condițiile de mai sus sunt îndeplinite.

Administratorul poate apoi modifica QPWDLVL la 1. Toate parolele NetServer sunt curățate când modificarea la QPWDLVL 1 devine efectivă (la următorul IPL).

Considerente pentru modificarea QPWDLVL de la 2 la 0

Considerentele sunt identice cu cele de la modificarea de la QPWDLVL 2 la 1, cu excepția că toate parolele NetServer sunt reținute când modificarea devine efectivă.

Considerente pentru modificarea QPWDLVL de la 1 la 0

După modificarea QPWDLVL la 0, administratorul trebuie să folosească comanda DSPAUTUSR sau PRTUSRPRF pentru a localiza profilurile de utilizator care nu au o parolă NetServer. Dacă profilul de utilizator necesită o parolă NetServer, ea poate fi creată modificând parola utilizatorului sau semnând printr-un mecanism care prezintă parola în text clar.

Administratorul poate apoi modifica QPWDLVL la 0.

Planificarea bibliotecilor

Mulți factori afectează modul în care alegeți să grupați informațiile aplicațiilor dumneavoastră în biblioteci și să le gestionați. Acest subiect adresează unele din problemele de securitate asociate proiectării bibliotecii.

Pentru a accesa un obiect, aveți nevoie de autorizare pentru obiectul respectiv și pentru bibliotecă în care se află. Puteți restricționa accesul la un obiect restricționând obiectul propriu-zis, bibliotecă în care se află sau ambele.

O bibliotecă este ca un director folosit pentru a localiza obiectele din ea. Autorizarea *USE pentru o bibliotecă vă permite să folosiți directorul pentru a găsi obiecte în ea. Autorizarea pentru obiectul însuși determină *cum* puteți folosi

obiectul. Autorizarea *USE pentru o bibliotecă e suficientă pentru a realiza majoritatea operațiilor asupra obiectelor din ea. Vedeți “Securitatea bibliotecii” la pagina 114 pentru informații suplimentare despre relația dintre autorizarea bibliotecă și obiect.

Folosirea autorizării publice pentru obiecte și restricționarea accesului la bibliotecă poate fi o tehnică de securitate simplă, eficientă. Punerea programelor într-o bibliotecă separată față de alte obiecte aplicație poate de asemenea simplifica panificarea securității. Aceasta este adevărată mai ales dacă fișierele sunt partajate de mai mult de o aplicație. Puteți utiliza autorizarea de folosire pentru bibliotecile care conțin programe aplicație pentru a controla cine poate realiza funcții asupra aplicațiilor.

Urmează două exemple de folosire a securității bibliotecii pentru aplicațiile Compania de jucării JKL. (Vedeți Figura 33 la pagina 195 pentru o diagramă a aplicațiilor.)

- Informațiile din biblioteca CONTRACTS sunt considerate confidențiale. Autorizarea publică pentru toate obiectele din bibliotecă este suficientă pentru a realiza funcțiile aplicației Preț și contracte (*CHANGE). Autorizarea publică pentru biblioteca CONTRACTS este *EXCLUDE. Doar utilizatorilor sau grupurilor autorizate pentru aplicația Preț și contracte le este acordată autorizare *USE pentru bibliotecă.
- Compania de jucării JKL este o companie mică cu o abordare nerestrictivă asupra securității, cu excepția informațiilor despre contracte și prețuri. Tuturor utilizatorilor sistemului le e permis să vadă informațiile despre client și inventar, deși doar utilizatorii autorizați le pot modifica. Bibliotecile CUSTLIB și ITEMLIB și obiectele din bibliotecă, au autorizarea publică *USE. Utilizatorii pot vedea informații din aceste biblioteci prin aplicația lor primară sau folosind Query. Bibliotecile programului au autorizarea publică *EXCLUDE. Doar utilizatorii cărora le e permis să modifice informațiile despre inventar au acces la ICPGMLIB. Programele care modifică informațiile despre inventar adoptă autorizarea proprietarului aplicației (OWNIC) și astfel au autorizare *ALL pentru câmpurile din biblioteca ITEMLIB.

Securitatea bibliotecii este eficientă doar când sunt urmate aceste reguli:

- Bibliotecile conțin obiecte cu cerințe de securitate similare.
- Utilizatorilor nu le e permis să adauge obiecte noi la bibliotecă restricționate. Modificările asupra programelor din bibliotecă sunt controlate. Bibliotecile aplicației trebuie să aibă autorizare publică *USE sau *EXCLUDE mai puțin în cazul în care utilizatorii au nevoie să creeze obiecte direct în bibliotecă.
- Listele de bibliotecă sunt controlate.

Planificarea aplicațiilor pentru a împiedica profilurile mari

Din cauza impactului potențial asupra performanțelor și securității, IBM **recomandă insistent** următoarele pentru ca profilurile să nu devină prea plin:

- Să nu aveți un profil care să dețină totul pe sistemul dumneavoastră.

Creați profiluri utilizator speciale pentru a deține aplicații. Profilurile proprietar care sunt specifice unei aplicații fac mai ușoară recuperarea lor și mutarea acestora între sisteme. De asemenea, informațiile despre autorizări private sunt dispersate în mai multe profiluri, ceea ce îmbunătățește performanța. Folosind mai multe profiluri de utilizator, puteți preveni creșterea excesivă a unui profil, din cauza prea multor obiecte. Profilurile de proprietar de asemenea vă permit să adoptați autorizarea profilului proprietar decât un profil mai puternic care furnizează autorizare nenecesară.

- Evitați deținerea de aplicații deținute de profiluri utilizator furnizate de IBM, cum ar fi QSECOFR sau QPGMR.

Aceste profiluri dețin un număr mare de obiecte furnizate de IBM și pot deveni foarte greu de gestionat. Păstrarea de aplicații deținute de profiluri utilizator livrate de IBM poate cauza de asemenea și probleme de securitate atunci când sunt mutate aplicațiile de pe un sistem pe altul. Aplicațiile deținute de profilurile de utilizator livrate de IBM pot afecta de asemenea performanțele comenzilor, cum ar fi CHKOBJITG și WRKOBJOWN.

- Folosiți liste de autorizații pentru a securiza obiecte.

Dacă acordați autorizări private multor obiecte pentru mai mulți utilizatori, ar trebui să considerați folosirea unei liste de autorizări pentru a securiza obiectele. Listele de autorizații vor cauza o intrare autorizare privată pentru lista de autorizații din profilul utilizatorului mai degrabă decât o intrare de autorizare privată pentru fiecare obiect. Din profilul proprietarului obiectului, listele de autorizări cauzează o intrare obiect autorizată pentru fiecare utilizator cărui i-a fost acordată autorizare la lista de autorizare mai degrabă decât o intrare obiect neautorizată pentru fiecare obiect multiplicat cu numărul utilizatorilor cărora le este acordată autorizarea privată.

Listele de biblioteci

Lista de biblioteci pentru un job furnizează flexibilitate. De asemenea reprezintă o expunere a securității. Această expunere este importantă mai ales dacă folosiți autorizare publică pentru obiecte și vă bazați pe securitatea bibliotecii ca principalul mijloc de protejare a informațiilor. În acest caz, un utilizator care primește acces la o bibliotecă are acces necontrolat la informațiile din ea. Subiectul “Listele de biblioteci” la pagina 183 furnizează o discuție despre problemele de securitate asociate listelor de biblioteci.

Pentru a evita riscurile de securitate ale listelor de biblioteci, aplicațiile dumneavoastră pot folosi nume calificate. Atunci când atât numele obiectului cât și bibliotecă sunt specificate, sistemul nu caută lista de biblioteci. Aceasta împiedică un potențial intrus de la folosirea listei de biblioteci pentru a dejuca securitatea.

Totuși, alte cerințe de proiectare a aplicației vă pot împiedica să folosiți nume calificate. Dacă aplicațiile dumneavoastră se bazează pe liste de biblioteci, tehnica descrisă în următoarea secțiune poate reduce expunerea securității.

Controlarea listei de biblioteci de utilizator

Ca o precauție de securitate, poate vreți să vă asigurați că porțiunea utilizator a listei de biblioteci are intrările corecte în secvența așteptată înainte de rularea unui job. O metodă de a face asta este să folosiți un program CL pentru a salva lista de biblioteci a utilizatorului, să o înlocuiți cu lista dorită și să o restaurați la sfârșitul aplicației. Urmează un program exemplu pentru a face asta:

```
PGM
DCL      &USRLIBL *CHAR LEN(2750)
DCL      &CURLIB  *CHAR LEN(10)
DCL      &ERROR  *LGL
DCL      &CMD    *CHAR LEN(2800)
MONMSG   MSGID(CPF0000) +
        EXEC(GOTO SETERROR)
RTVJOBA  USRLIBL(&USRLIBL) +
        CURLIB(&CURLIB)
IF COND(&CURLIB=('*NONE')) +
    THEN(CHGVAR &CURLIB '*CRTDFT ')
CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
/*****/
/*
/*      Normal processing      */
/*
/*
/*****/
GOTO     ENDPGM
SETERROR: CHGVAR  &ERROR '1'
ENDPGM:  CHGVAR  &CMD +
        ('CHGLIBL LIBL+
        (' *CAT &USRLIBL *CAT') +
        CURLIB(' *CAT &CURLIB *TCAT ' )')
        CALL     QCMDEXC PARM(&CMD 2800)
        IF      &ERROR SNDPGMMSG MSGID(CPF9898) +
        MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
        MSGDTA('The xxxx error occurred')
        ENDPGM
```

Figura 34. Program pentru a înlocui și restaura lista de biblioteci

Note:

1. Indiferent de modul în care se termină programul (normal sau anormal), lista de biblioteci este returnată la versiunea pe care o reține când programul a fost apelat, deoarece tratarea erorii include restaurarea listei de biblioteci.
2. Deoarece comanda CHGLIBL necesită o listă de nume de biblioteci, nu poate fi rulată direct. Comanda RTVJOBA, așadar, extrage bibliotecile folosite pentru a construi comanda CHGLIBL ca o variabilă. Variabile este pasată ca un parametru funcției QCMDEXC.

3. Dacă ieșiți într-o funcție necontrolată (de exemplu, un program utilizator, un meniu care permite introducerea de comenzi sau ecranul Introducere comanzi) în mijlocul unui program, acesta ar trebui să înlocuiască lista de biblioteci la întoarcere, pentru a asigura control adecvat.

Modificarea listei de biblioteci de sistem

Dacă aplicația dumneavoastră are nevoie să adauge intrări în porțiunea sistem a listei de biblioteci, puteți folosi un program CL similar celui arătat în Figura 34 la pagina 201, cu următoarele modificări:

- În loc să folosiți comanda RTVJOBA, folosiți comanda RTVSYSVAL (Retrieve System Values - Extragere valori de sistem) pentru a extrage valoarea de sistem QSYSLIBL.
- Folosiți comanda CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem) pentru a modifica porțiunea sistem a listei de biblioteci la valoarea dorită
- La sfârșitul programului dumneavoastră, folosiți comanda GSYSLIBL din nou pentru a restaura porțiunea sistem a listei de biblioteci la valoarea sa originală.
- Comanda CHGSYSLIBL este livrată cu autorizarea publică *EXCLUDE. Pentru a folosi această comandă în programul dumneavoastră, faceți una din următoarele:
 - Acordați proprietarului programului autorizare *USE pentru comanda CHGSYSLIBL și folosiți use autorizarea adoptată.
 - Acordați utilizatorilor care rulează programul autorizare *USE pentru comanda CHGSYSLIBL.

Descrierea securității bibliotecii

Ca un proiectant de aplicații, trebuie să furnizați informații despre o bibliotecă pentru administratorul de securitate. Administratorul de securitate folosește aceste informații pentru a decide cum să securizeze biblioteca și obiectele ei. Informațiile tipice necesare sunt:

- Orice funcții ale aplicației care adaugă obiecte în bibliotecă.
- Dacă sunt șterse obiecte din bibliotecă în timpul procesării aplicației.
- Ce profil deține biblioteca și obiectele sale.
- Dacă biblioteca ar trebui inclusă în lista de biblioteci.

Figura 35 furnizează un format exemplu pentru furnizarea acestor informații:

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 aplicație inițial sau programul de interogare inițial.

Listare orice funcții care necesită autorizare *ADD pentru bibliotecă:

Nu sunt adăugate obiecte în bibliotecă în timpul procesării normale a aplicației. Listați orice obiect care necesită autorizare *OBJMGT sau *OBJEXIST și ce funcții au nevoie de acea autorizare:

Toate fișierele de lucru, ale căror nume încep cu caracterele ICWRK, sunt curățate la sfârșit de lună. Asta necesită autorizare *OBJMGT.

Figura 35. Format pentru descrierea securității bibliotecii

Planificarea meniurilor

Meniurile sunt o metodă bună pentru furnizarea de acces controlat la sistemul dumneavoastră. Puteți folosi meniuri pentru a restricționa un utilizator la un set de funcții controlate strict specificând capabilități limitate și un meniu inițial în profilul utilizator.

Pentru a folosi meniuri ca o unealtă de control al accesului, urmați aceste linii la proiectarea lor:

- Nu furnizați o linie de comandă sau meniuri proiectate pentru utilizatori restricționați.
- Evitați să aveți funcții cu cerințe de securitate diferite în același meniu. De exemplu, dacă unor utilizatori ai unei aplicații le e permis doar să vadă informații, nu o modificați, furnizați un meniu care are doar opțiuni de vizualizare și tipărire pentru acei utilizatori.
- Asigurați-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.
- Furnizați acces la câteva funcții de sistem, cum ar fi vizualizarea ieșirii imprimantei. Meniul sistem ASSIST să această capabilitate și poate fi definit în profilul utilizator ca programul Attention-key-handling program. Dacă profilul utilizator are o clasă *USER și are capabilități limitate, utilizatorul nu poate vedea ieșirea sau joburile altor utilizatori.
- Furnizați acces la unelte de suport decizie din meniuri. Subiectul “Folosirea autorizării adoptate în proiectarea meniului” dă un exemplu cum să faceți asta.
- Considerați controlarea accesului la Meniul System Request sau la unele din opțiunile acestui meniu. Vedeți “Meniul Cerere sistem” la pagina 207 pentru informații suplimentare.
- Pentru utilizatorii cărora le e permis să ruleze doar o singură funcție, evitați complet meniurile și specificați un program inițial în profilul utilizator. Specificați *SIGNOFF ca meniu inițial.

La Compania de jucării JKL, toți utilizatorii văd un meniu de interogare care permite accesul la majoritatea fișierelor. Pentru utilizatorii cărora nu le e permis să modifice informații, acesta este meniul inițial. Opțiunea de întoarcere din meniu deconectează utilizatorul. Pentru alți utilizatori, acest meniu este apelat de o opțiune de interogare din meniurile aplicației. Apăsând F12 (Întoarcere), utilizatorul se întoarce la meniul de apelare. Deoarece se folosește securitatea bibliotecilor pentru bibliotecile program, acest meniu și programul pe care îl apelează sunt păstrate în biblioteca QGPL:

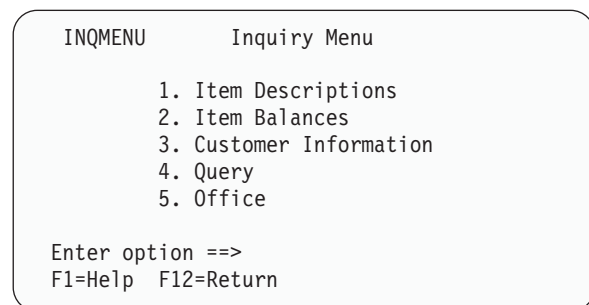


Figura 36. Exemplu de meniu de interogare

Folosirea autorizării adoptate în proiectarea meniului

Disponibilitatea uneltelor de suport decizie, cum ar fi Query/400, creează probleme la proiectarea securității. Poate vreți ca utilizatorii să fie capabili să vadă informații din fișiere folosind o unealtă de interogare, dar probabil vreți să vă asigurați că fișierele sunt modificate doar de programe aplicație testate.

Nu există nici o metodă în definițiile de securitate ale resursei pentru ca un utilizator să aibă autorizare diferită pentru un fișier în circumstanțe diferite. Totuși, folosirea autorizării adoptate vă permite să definiți autorizare pentru a îndeplini cerințe diferite.

Notă: “Obiecte care adoptă autorizarea proprietarului” la pagina 128 descrie cum funcționează autorizare adoptată. “Organigrama 8: Cum este verificată autorizarea adoptată” la pagina 159 descrie cum verifică sistemul autorizarea adoptată.

Figura 37 arată un exemplu de meniu inițial care folosește autorizare adoptată pentru a furniza acces controlat la fișiere folosind unelte de interogare:

```

MENU1          Initial Menu

      1. Inventory Control (ICSTART)
      2. Customer Orders  (COSTART)
      3. Query             (QRYSTART)
      4. Office            (OFCSTART)

(no command line)

```

Figura 37. Meniu exemplu inițial

Programele care pornesc aplicații (ICSTART și COSTART) adoptă autorizarea profilului care deține obiectele aplicație. Programele adaugă biblioteci aplicație la lista de biblioteci și afișează meniul aplicației inițiale. Urmează un exemplu de program de control inventar (ICSTART).

```

PGM
ADDLIBL  ITEMLIB
ADDLIBL  ICPGMLIB
GO  ICMENU
RMVLIBL  ITEMLIB
RMVLIBL  ICPGMLIB
      ENDPGM

```

Figura 38. Program aplicație inițială exemplu

Programul care pornește Query (QRYSTART) adoptă autorizarea unui profil (QRYUSR) furnizat pentru a permite acces la fișiere pentru interogări. Figura 39 arată programul QRYSTART:

```

PGM
ADDLIBL  ITEMLIB
ADDLIBL  CUSTLIB
STRQRY
RMVLIBL  ITEMLIB
RMVLIBL  CUSTLIB
      ENDPGM

```

Figura 39. Program exemplu pentru interogare cu autorizare adoptată

Sistemul meniu folosește trei tipuri de profiluri utilizator, arătate în Tabela 119. Tabela 120 la pagina 205 descrie obiectele folosite de sistemul meniu.

Tabela 119. Profiluri utilizatori pentru sistem meniu

Tip profil	Descriere	Parolă	Limitare capabilități	Autorizări speciale	Meniu inițial
Proprietar aplicație	Deține toate obiectele aplicație și are autorizare *ALL. OWNIC deține aplicația Control inventar.	*NONE	Nu se aplică	Așa cum e necesar aplicației	Nu se aplică
Utilizator aplicație ¹	Profil exemplu pentru oricine care folosește sistemul meniu	Da	*YES	Nimic	MENU1
Profil interogare	Folosit pentru a furniza acces la biblioteci pentru interogare	*NONE	Nu se aplică	Nimic	Nu se aplică

¹ Biblioteca curentă specificată în profilul utilizator al aplicației e folosită pentru a memora orice interogări create. Programul Attention-key-handling este *ASSIST, dându-i acces utilizatorului la funcțiile de bază ale sistemului.

Tabela 120. Obiecte folosite de sistem meniu

Nume obiect	Proprietar	Autorizare publică	Autorizări private	Informații suplimentare
MENU1 în biblioteca QGPL	Vedeți Nota	*EXCLUDE	Autorizare *USE pentru orice utilizator căruia îi e permis să folosească meniul	În biblioteca QGPL deoarece utilizatorii nu au autorizare pentru bibliotecile aplicației
Programul ICSTART din QGPL	OWNIC	*EXCLUDE	Autorizare *USE pentru utilizatorii autorizați pentru aplicația Control inventar	Creat cu USRPRF(*OWNER) pentru a adopta autorizare OWNIC
Programul QRYSTART din QGPL	QRYUSR	*EXCLUDE	Autorizare *USE pentru utilizatorii autorizați să creeze sau să ruleze interogări	Creat cu USRPRF(*OWNER) pentru a adopta autorizare QRYUSR
ITEMLIB	OWNIC	*EXCLUDE	QRYUSR are *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
Fișiere disponibile pentru Interogare în ITEMLIB	OWNIC	*USE		
Fișiere 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 aplicații multiple.

Când USERA selectează opțiunea 1 (Inventory Control) din MENU1, rulează programul ICSTART. Programul adoptă autorizarea lui OWNIC, dând autorizare *ALL obiectelor de control al inventarului din ITEMLIB și programelor din ICPGMLIB. USERA este astfel autorizată să facă modificări asupra fișierelor de control al inventarului în timp de folosesc opțiuni din ICMENU.

Când USERA iese din ICMENU și se întoarce la MENU1, bibliotecile ITEMLIB și ICPGMLIB sunt înlăturate din lista de biblioteci USERA și programul ICSTART este înlăturat din stiva de programe. USERA nu mai rulează sub autorizarea adoptată.

Când USERA selectează opțiunea 3 (Query) din MENU1, rulează programul QRYSTART. Programul adoptă autorizarea lui QRYUSR, dând autorizare *USE bibliotecii ITEMLIB. Autorizarea publică pentru fișierele din ITEMLIB determină care fișiere are voie USERA să le interogheze.

Această tehnică are avantajul de a minimiza numărul de autorizări private și de a furniza performanțe bune la verificarea autorizării:

- Obiectele din bibliotecile aplicației nu au autorizări private. Pentru unele funcții ale aplicației, autorizarea publică este adecvată. Dacă autorizarea publică nu e adecvată, e folosită autorizarea proprietar. “Cazul 8: Autorizarea adoptată fără autorizare privată” la pagina 168 arată pașii de verificare a autorizării.
- Accesul la fișierele pentru interogare folosește autorizare publică pentru fișiere. 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 deținută de utilizator și utilizatorul ar trebui să aibă autorizare *ALL.
- Utilizatorii individuali au nevoie doar să fie autorizați pentru MENU1, ICSTART și QRYSTART.

Considerați aceste riscuri și precauții când folosiți această tehnică:

- USERA are autorizare *ALL pentru toate obiectele de control inventar din ICMENU. Asigurați-vă că meniul nu permite acces la o linie de comandă sau permite funcții de ștergere și 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 funcții neautorizate.

Ignorarea autorizării adoptate

Folosirea autorizării adoptate în proiectarea meniului arată o tehnică pentru furnizarea capabilității de interogare fără a permite modificări necontrolate asupra fișierelor aplicației. Această tehnică necesită ca utilizatorul să se întoarcă la meniul inițial înainte de a rula interogări. Dacă vreți să furnizați oportunitatea de pornire a interogării din meniurile aplicației precum și din meniul inițial, puteți seta programul QRYSTART să ignore autorizarea adoptată.

Notă: “Programe care ignoră autorizarea adoptată” la pagina 131 furnizează informații suplimentară despre ignorarea autorizării adoptate. “Organigrama 8: Cum este verificată autorizarea adoptată” la pagina 159 descrie cum verifică sistemul autorizarea adoptată.

Figura 40 arată un meniu de aplicație care include programul QRYSTART:

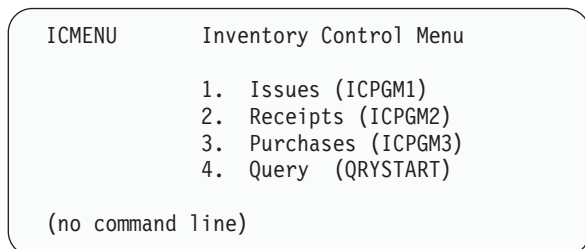


Figura 40. Meniu de aplicație exemplu cu Query

Informațiile de autorizare pentru programul QRYSTART sunt identice cu cele arătate în Tabela 120 la pagina 205. Programul este creat cu parametrul de autorizare adoptată de utilizare (USEADPAUT) setat pe *NO, pentru a ignora autorizarea adoptată a programelor anterioare din stivă.

Urmează comparații ale stivelor de programe când USERA selectează interogare din MENU1 (vedeți Figura 37 la pagina 204) și din ICMENU:

Stiva de programe când se selectează interogare din MENU1

MENU1 (fără autorizare adoptată)
QRYSTART (autorizare adoptată QRYUSR)

Stiva de programe când se selectează interogare din ICMENU

MENU1 (fără autorizare adoptată)
ICMENU (autorizare adoptată OWNIC)
QRYSTART (autorizare adoptată QRYUSR)

Specificând programul QRYSTART cu USEADPAUT(*NO), autorizarea oricărui program anterior din stivă nu e folosită. Asta permite USERA să ruleze interogare din ICMENU fără a avea abilitatea de a modifica și șterge fișiere, deoarece autorizarea lui OWNIC nu e folosită de programul QRYSTART.

Când USERA termină interogarea și se întoarce la ICMENU, autorizarea adoptată este din nou activă. Autorizarea adoptată este ignorată doar atâta timp cât programul QRYSTART este activ.

Dacă autorizarea publică pentru programul QRYSTART este *USE, specificați USEADPAUT(*NO) ca o precauție de securitate. Aceasta împiedică pe oricine care rulează sub autorizarea adoptată de la apelarea programului QRYSTART și realizarea funcțiilor neautorizate.

Meniul de interogare (Figura 36 la pagina 203) de la Compania de jucării JKL de asemenea folosește această tehnică, deoarece poate fi apelată din meniuri în bibliotecă aplicație diferite. Ea adoptă autorizarea lui QRYUSR și ignoră orice altă autorizare adoptată din stiva de programe.

Descrierea securității meniului

Ca un proiectant de aplicații, trebuie să furnizați informații despre un meniu pentru administratorul de securitate. Administratorul de securitate folosește aceste informații pentru a decide cine ar trebui să aibă acces la meniu și ce autorizări sunt necesare. Informațiile tipice necesare sunt:

- Dacă oricare din opțiunile din meniu necesită autorizări speciale, cum ar fi *SAVSYS sau *JOBCTL.
- Dacă opțiunile din meniu apelează programe care adoptă autorizare.

- Ce autorizare pentru obiecte e necesară pentru fiecare opțiune din meniu. Ar trebui să aveți nevoie doar să identificați acele autorizări care sunt mai mari decât autorizarea publică normală.

Figura 41 arată un format exemplu pentru furnizarea acestor informații.

Nume meniu: MENU1 Bibliotecă: QGPLNumăr opțiune: 3 Descriere: Query

Program apelat: QRYSTART Bibliotecă: QGPL

Autorizare adoptată: QRYUSR

Autorizare specială necesară: None

Autorizări obiect necesare: Utilizatorul trebuie să aibă autorizarea *USE pentru programul QRYSTART. QRYUSR trebuie să aibă autorizare *USE pentru bibliotecile conținând fișiere care vor fi interogate. Utilizatorul, QRYUSR sau public trebuie să aibă autorizare *USE pentru fișierele care sunt interogate.

Figura 41. Cerințe format pentru securitate meniu

Meniul Cerere sistem

Un utilizator poate folosi funcția de cerere sistem pentru a suspenda jobul curent și a afișa Meniul cerere sistem. Meniul cerere sistem permite utilizatorului să trimită și să afișeze mesaje, să transfere la un al doilea job sau să oprească jobul curent.

Când e livrat sistemul dumneavoastră, autorizarea publică pentru Meniul cerere sistem e *USE. Cea mai ușoară cale de a împiedica utilizatorii să acceseze acest meniu este prin restricționarea autorizării la grupul de panouri QGMNSYSR:

- Pentru a împiedica anumiți utilizatori să vadă Meniul cerere sistem, specificați 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, anulați autorizarea publică și acordați 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 fișierul 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 fișier de mesaje) ca să modifice comenzile pe care le folosesc opțiunile meniului cerere sistem.

| De fiecare dată când este apăsată tasta System Request, sistemul în mod automat modifică profilul utilizator curent al
 | jobului la profilul utilizator inițial al jobului. Acest lucru se întâmplă pentru ca utilizatorul să nu aibă nici o autoritate
 | adițională în meniul System Request sau în programul de ieșire Presystem Request Program. De fiecare dată când este
 | apăsată tasta System Request, sistemul în mod automat modifică profilul utilizator curent al jobului la profilul utilizator
 | inițial al jobului.

Puteți împiedica utilizatorii să selecteze opțiuni specifice din Meniul cerere sistem restricționând autorizarea pentru comenzile asociate. Tabela 121 la pagina 208 arată comenzile asociate cu opțiunile meniului:

Tabela 121. Opțiuni și comenzi pentru Meniul cerere sistem

Opțiune	Comandă
1	Transferare job secundar (TFRSECJOB)
2	Terminare cerere (ENDRQS)
3	Afișare job (DSPJOB)
4	Afișare mesaj (DSPMSG)
5	Trimitere mesaj (SNDMSG)
6	Afișare mesaj (DSPMSG)
7	Afișare utilizator stație de lucru (DSPWSUSR)
10	Pornire cerere sistem la sistemul precedent (TFRPASTHR). (Vedeți nota de mai jos.)
11	Transferare la sistemul anterior (TFRPASTHR). (Vedeți nota de mai jos.)
12	Afișare opțiuni de emulare 3270 (Vedeți nota de mai jos.)
13	Pornire cerere sistem pe sistemul home (TFRPASTHR). (Vedeți nota de mai jos.)
14	Transferare la sistemul home (TFRPASTHR). (Vedeți nota de mai jos.)
15	Transferare la sistemul capăt (TFRPASTHR). (Vedeți nota de mai jos.)
50	Terminare cerere pe sistemul la distanță (ENDRDBRQS). (Vedeți nota de mai jos.)
80	Deconectare job (DSCJOB)
90	Sign-Off (SIGNOFF)

Note:

- Opțiunile 10, 11, 13, 14 și 15 sunt afișate doar dacă passthrough-ul stației de afișare a fost pornit cu comanda STRPASTHR (Start Pass-Through - Pornire passthrough). Opțiunile 10, 13 și 14 sunt afișate doar pe sistemul destinație.
- Opțiunea 12 e afișată doar unde emularea 3270 este activă.
- Opțiunea 50 este afișată doar dacă un job la distanță e activ.
- Unele din opțiuni au restricții pentru mediul System/36.

De exemplu, pentru a împiedica utilizatorii să transfere la un job interactiv alternativ, anulați autorizarea publică pentru comanda TFRSECJOB (Transfer to Secondary Job - Transfer la un job secundar) și acordați 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 opțiune pentru care nu are autorizare, e afișat un mesaj.

Dacă vreți să împiedicați utilizatorii de la folosirea generală a comenzilor din meniul cerere sistem dar tot vreți să fie capabili să ruleze o comandă la un moment specific (cum ar fi la sign-off), puteți crea un program CL care adoptă autorizarea unui utilizator autorizat și rulează comanda.

Planificarea securității comenzii

Securitatea meniului e o tehnica buna pentru utilizatorii care au nevoie de aplicații și de funcții sistem limitate. Unii utilizatori au nevoie de un mediu mai flexibil și de capacitatea de a rula comenzi. Când sistemul dumneavoastră ajunge, abilitatea de folosire comenzi e setată să îndeplinească nevoile de securitate ale majorității 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.

Puteți modifica autorizarea pentru comenzi pentru a îndeplini cerințele dumneavoastră de securitate. De exemplu, poate vreți să împiedicați majoritatea utilizatorilor de pe sistemul dumneavoastră să lucreze cu comunicații. Puteți seta autorizarea publică pe *EXCLUDE pentru toate comenzile care lucrează cu obiecte de comunicație, cum ar fi comenzile CHGCTLxxx, CHGLINxxx, și CHGDEVxxx.

Dacă aveți nevoie să controlați care comenzi pot fi rulate de utilizatori, puteți folosi autorizarea de obiect pentru comenzile propriu-zise. Fiecare comandă de pe sistem are tipul obiect *CMD și poate fi autorizată pentru public sau orice utilizator specific. Pentru a rula o comandă, utilizatorul are nevoie de autorizare *USE pentru ea. Anexa C listează toate comenzile care sunt livrate cu autorizarea publică setată pe *EXCLUDE.

Dacă folosiți biblioteca System/38, aveți nevoie să restricționați comenzile relative pentru securitate de asemenea în acea bibliotecă. Sau, puteți restricționa accesul la întreaga bibliotecă. Dacă folosiți una sau mai multe versiuni de limbă națională i5/OS a programului licențiat pe sistemul dumneavoastră, aveți nevoie să restricționați comenzile în bibliotecile QSYSxxx suplimentare din sistemul dumneavoastră de asemenea.

O altă măsură de securitate folositoare este să modificați valorile implicite pentru unele comenzi. Comanda CHGCMDDFT (Change Command Default - Modificare valoare implicită a comenzii) vă permite să faceți asta.

Planificarea securității fișierului

Informațiile conținute în fișierele de bază de date sunt de obicei cele mai importante bunuri de pe sistemul dumneavoastră. Securitatea resursei vă permite să controlați cine poate vedea, modifica și șterge informații dintr-un fișier. Dacă utilizatorii necesită autorizări diferite pentru fișiere în funcție de situație, puteți folosi autorizarea adaptivă. “Folosirea autorizării adoptate în proiectarea meniului” la pagina 203 dă un exemplu pentru această metodă.

Pentru fișiere critice de pe sistemul dumneavoastră, păstrați o evidență a utilizatorilor care au autorizare pentru fișier. Dacă folosiți autorizare de grup și liste de autorizare, trebuie să țineți evidența utilizatorilor care au autorizare prin aceste metode, precum și a celor care sunt autorizați direct. Dacă folosiți autorizare adoptată, puteți lista programe care adoptă autorizarea unui utilizator particular folosind comanda DSPPGMADP (Display Program Adopt - Afișare program adoptare).

Puteți folosi de asemenea funcția de jurnalizare de pe sistem pentru a monitoriza activitatea unui fișier critic. Deși intenția primară a unui jurnal este să recupereze informații, poate fi folosit ca o unealtă de securitate. El conține o înregistrare a celor care au accesat un fișier și în ce fel. Puteți folosi comanda DSPJRN (Display Journal - Afișare jurnal) pentru a vedea un exemplu de intrări jurnal periodic.

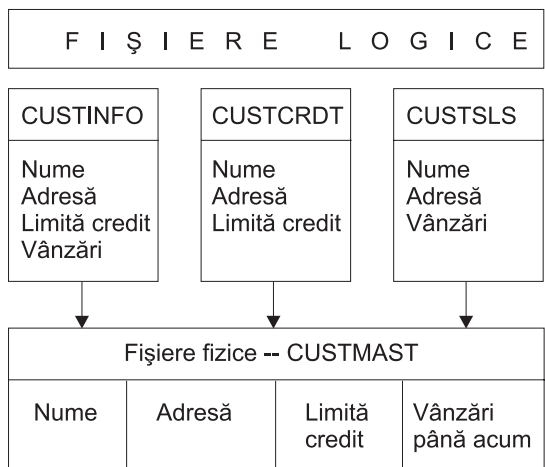
Securizarea fișierelor logice

Securitatea resursei din sistem suportă securitate la nivel de câmp a unui fișier. Puteți de asemenea folosi fișiere logice pentru a proteja câmpuri specifice sau înregistrări dintr-un fișier. Vedeți subiectul Baza de date universală DB2 pentru iSeries din Centrul de informare pentru informații suplimentare. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Un fișier logic poate fi folosit pentru a specifica un subset de *înregistrări* pe care un utilizator le poate accesa (folosind logică de selecție și omitere). Așadar, utilizatori specifici pot fi împiedicați să acceseze anumite tipuri de înregistrări. Un fișier logic poate fi folosit pentru a specifica un subset de *câmpuri* într-o înregistrare pe care o poate accesa un utilizator. Așadar, utilizatori specifici pot fi împiedicați să acceseze anumite câmpuri dintr-o înregistrare.

Un fișier logic nu conține nici o dată. Este o vizualizare particulară a unui sau mai multor fișiere care conțin datele. Furnizarea accesului la informațiile definite de un fișier logic necesită autorizare de date atât pentru fișierul logic cât și pentru fișierele fizice asociate.

Figura 42 la pagina 210 arată un exemplu de fișier fizic și trei fișiere logice diferite asociate cu el.



RBAFW532-0

Figura 42. Folosire fișier 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 fișierul fizic arată astfel:

Tabela 122. Exemplu fișier fizic: Fișier CUSTMAST

Autorizare	Utilizatori: *PUBLIC
<p><i>Autorizări obiect</i></p> <p>*OBJOPR</p> <p>*OBJMGT</p> <p>*OBJEXIST</p> <p>*OBJALTER</p> <p>*OBJREF</p> <p><i>Autorizări pentru date</i></p> <p>*READ</p> <p>*ADD</p> <p>*UPD</p> <p>*DLT</p> <p>*EXECUTE</p> <p>*EXCLUDE</p>	
	<p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p>

Publicul ar trebui să aibă toate autorizările pentru date, dar nu și autorizare de operare asupra obiectelor din fișierul fizic CUSTMAST. Publicul nu poate accesa fișierul CUSTMAST direct, deoarece este necesară autorizarea *OBJOPR pentru a deschide un fișier. Autorizarea publicului face ca toate drepturile asupra datelor să fie potențial disponibile pentru utilizatorii fișierului logic.

Autorizarea pentru fișierul 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

User      Group      Object
*PUBLIC   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

User      Group      Object
DPTAR     Group      Authority
*PUBLIC   *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

User      Group      Object
DPTSM     Group      Authority
*PUBLIC   *CHANGE
*PUBLIC   *USE

```

Pentru ca această schemă de autentificare să funcționeze nu este necesar ca profilul de grup, cum ar fi DPTSM, să fie făcut grup primar pentru fișierul logic. Totuși, folosirea autorizării de grup primar elimină căutarea autorizărilor private atât pentru utilizatorul care încearcă să acceseze fișierul, cât și pentru grupul utilizatorului. “Cazul 2: Folosirea autorizării grupului primar” la pagina 164 arată cum folosirea autorizării de grup primar afectează autorizarea care verifică procesul.

Puteți specifica autorizări de date pentru fișiere logice începând cu V3R1 a programului i5/OS licențiat. Când vă mutați la V3R1 de la o versiune anterioară, sistemul convertește fișierele dumneavoastră logice când e instalat. Prima dată când e accesat un fișier logic, sistemul dă toate autorizările de date.

Pentru a folosi fișiere logice ca unealtă de securitate, faceți următoarele:

- Acordați toate autorizările de date fișierelor fizice subliniate.
- Anulați *OBJOPR de la fișierele fizice. Asta împiedică utilizatorii să acceseze fișierele fizice direct.

- Acordați autorizările de date corespunzătoare pentru fișierele logice. Anulați orice autorizare pe care n-o vreți.
- Acordați *OBJOPR pentru fișierele logice.

Înlocuirea fișierelor

Comenzile de înlocuire pot fi folosite pentru ca un program să utilizeze un fișier diferit cu același format. De exemplu, presupuneți că un program din aplicația contracte și prețuri din Compania de jucării JKL scrie informații despre preț într-un fișier de lucru înainte de a face modificările de preț. Un utilizator cu acces la o linie de comandă care dorea să captureze informații confidențiale poate folosi o comandă de înlocuire pentru a face ca programul să scrie date într-un fișier diferit într-o bibliotecă controlată de utilizator. Vă puteți asigura că un program procesează fișierele corecte folosind comenzi de înlocuire cu SECURE(*YES) înainte ca programul să ruleze.

Securitatea fișierului și SQL

SQL (Structured Query Language) folosește fișiere cross-reference pentru a ține evidența fișierelor bază de date și relațiile dintre ele. La aceste fișiere se referă colectiv drept catalog SQL. Autorizarea publică pentru catalogul SQL este *READ. Asta înseamnă că orice utilizator care are acces la interfața SQL poate afișa numele și descrierile text pentru toate fișierele de pe sistemul dumneavoastră. Catalogul SQL nu afectează autorizarea normală necesară pentru a accesa conținutul fișierelor bază de date.

Ar trebui să aveți grijă când folosiți un program CL care adoptă autorizare pentru a porni SQL sau Query Manager. Aceste două programe de interogare permit utilizatorilor să specifice un nume de fișier. Utilizatorul poate, așadar, să acceseze orice fișier la care profilul adoptat are autorizare.

Planificarea listelor de autorizări

O listă de autorizații are aceste avantaje:

- Listele de autorizații simplifică gestionarea autorizațiilor. Autorizarea utilizatorului e definită pentru lista de autorizații, nu pentru obiectele individuale din listă. Dacă un obiect nou e securizat de lista de autorizații, utilizatorii din listă primesc autorizare pentru el.
- O operație poate fi folosită pentru a da unui utilizator autorizare pentru toate obiectele din listă.
- Listele de autorizații reduc numărul autorizărilor private din sistem. Fiecare utilizator are o autorizare privată pentru un obiect, lista de autorizații. Aceasta îi dă utilizatorului autorizare pentru toate obiectele din listă. Reducerea numărului de autorizări private din sistem are următoarele avantaje:
 - Reduce dimensiunea profilului utilizator.
 - Îmbunătățește performanțele la salvarea sistemului (SAVSYS) sau salvarea datelor de securitate (SAVSECDTA).
- Listele de autorizații furnizează o cale bună de a securiza fișiere. Dacă folosiți autorizări private, fiecare utilizator va avea o autorizare privată pentru fiecare membru fișier. Dacă folosiți o listă de autorizații, fiecare utilizator va avea doar o autorizare. De asemenea, fișierele care sunt deschise nu pot să aibă autorizare acordată sau anulată din fișier. Dacă securizați fișierul cu o listă de autorizații, puteți modifica autorizările, chiar când fișierul e deschis.
- Listele de autorizații furnizează o cale de a memora autorizările când este salvat un obiect. Când este salvat un obiect care e securizat de o listă de autorizații, numele listei e salvat cu obiectul. Dacă obiectul e șters și restaurat pe **același** sistem, e legat automat din nou la lista de autorizații. Dacă obiectul e restaurat pe un sistem diferit, lista de autorizații nu e legată, decât dacă se specifică ALWOBJDIF(*ALL) în comanda de restaurare.

Avantajele folosirii unei liste de autorizări

Din punctul de vedere al gestionării securității, o listă de autorizații este metoda preferată pentru a gestiona obiectele care au aceleași cerințe de securitate. Chiar și când sunt doar câteva obiecte care vor securizate de listă, mai e totuși un avantaj să folosiți o listă de autorizații în loc să folosiți autorizări private pentru obiect. Deoarece autorizările sunt într-un loc (lista de autorizații), este mai ușor să modificați cine e autorizat pentru obiecte. De asemenea e mai ușor să securizați orice obiecte noi cu aceleași autorizări ca obiectele existente.

Dacă folosiți liste de autorizații, atunci nu ar trebui să aveți autorizări private pentru obiect. Sunt necesare două căutări ale autorizărilor private ale utilizatorului în timpul verificării lor dacă obiectul are autorizări private și obiectul e de

asemenea securizat cu o listă de autorizații. Prima căutare este pentru autorizările private pentru obiect; cea de-a doua e pentru autorizările private din lista de autorizații. Două căutări necesită utilizarea resurselor sistemului; așadar, performanțele pot fi alterate. Dacă folosiți doar lista de autorizații, se realizează doar o căutare. De asemenea, din cauza folosirii cache-ului pentru autorizarea cu lista de autorizații, performanța pentru verificarea autorizării va fi identică cu cea pentru verificarea doar a autorizărilor private pentru obiect.

La Compania de jucării JKL, o listă de autorizații este folosită pentru a securiza toate fișierele de lucru folosite în procesare inventarului la sfârșit de lună. Aceste fișiere de lucru sunt curățate, ceea ce necesită autorizare *OBJMGT. Pe măsură ce cerințele aplicației se modifică, mai multe fișiere de lucru pot fi adăugate aplicației. De asemenea, pe măsură ce responsabilitățile jobului se modifică, utilizatori diferiți rulează procesarea de la sfârșit de lună. O listă de autorizații face mai simplă gestionarea acestor modificări.

Urmează pașii pentru a seta lista de autorizații:

1. Creați lista de autorizații:

```
CRTAUTL ICLIST1
```

2. Securizați toate fișierele de lucru cu lista de autorizații:

```
GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +  
OBJTYP(*FILE) AUTL(ICLIST1)
```

3. Adăugați utilizatori la listă care realizează procesare la sfârșit de lună:

```
ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)
```

Planificarea profilurilor de grup

Un profil de grup este o unealtă folositoare când mai mulți utilizatori au cerințe de securitate similare. Sunt folositoare în special când cerințele jobului și apartenența la grup se modifică. De exemplu, dacă membrii unui departament au responsabilitate pentru o aplicație, 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 ușor de gestionat decât înlăturarea autorizărilor individuale din profiluri utilizator.

Puteți crea profiluri specific pentru a fi profiluri de grup sau puteți face unul existent într-un profil de grup. Un profil de grup este un tip special de profil utilizator. El devine un profil de grup când se întâmplă una din următoarele:

- Alt profil îl desemnează ca profil de grup
- Îi asignați un număr de identificare a grupului (gid).

De exemplu:

1. Creați un profil numit GRPIC:

```
CRTUSRPRF GRPIC
```

2. Când profilul e creat, e un profil obișnuit, nu unul de grup.

3. Desemnați GRPIC ca profilul de grup pentru alt profilul de grup:

```
CHGUSRPRF USERA GRPPRF(GRPIC)
```

4. Sistemul acum tratează GRPIC ca un profil de grup și îi asignează un gid.

Planificarea grupurilor primare pentru obiecte

Orice obiect de pe sistem poate avea un grup primar. Autorizarea pentru grupul primar poate furniza un avantaj în performanțe dacă grupul primar este primul pentru majoritatea utilizatorilor unui obiect.

Deseori, un grup de utilizatori e responsabil pentru unele informații din sistem, cum ar fi informațiile despre client. Acel grup necesită mai multă autorizare pentru informații decât alți utilizatori ai sistemului. Folosind autorizare pentru grup primar, puteți seta acest tip de schemă de autorizare fără a afecta performanțele verificării autorizării. “Cazul 2: Folosirea autorizării grupului primar” la pagina 164 arată un exemplu pentru asta.

Planificarea profilurilor de grup multiple

Un utilizator poate fi membru a până la 16 grupuri: primul grup (parametrul GRPPRF din profilul utilizator) și 15 grupuri suplimentare (parametrul SUPGRPPRF din profilul utilizator). Folosind profiluri de grup, puteți gestiona autorizarea mai eficient și reduce numărul de autorizări private individuale pentru obiecte. Însă folosirea greșită a profilurilor de grup poate avea un efect negativ asupra performanțelor verificării autorizării.

Urmați aceste sugestii la folosirea profilurilor de grup multiple:

- Încercați să folosiți grupuri multiple în combinație cu autorizarea grupului primar și eliminați autorizarea privată pentru obiecte.
- Planificați cu atenție ordinea în care profilurile de grup sunt asignate unui utilizator. Primul grup al utilizatorului trebuie să se refere la asignarea primară a utilizatorului și la obiectele folosite mai des. De exemplu, să presupunem că un utilizator numit WAGNERB lucrează de obicei la inventariere și 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 performanțelor verificării autorizării.

- Dacă intenționați să folosiți grupuri multiple, studiați procesul de verificare a autorizării descris în “Cum verifică sistemul autorizarea” la pagina 147. Asigurați-vă că înțelegeți cum folosirea grupurilor multiple în combinație cu alte tehnici de autorizare, cum ar fi liste de autorizare, vă poate afecta performanța sistemului.

Acumularea autorizărilor speciale pentru membrii profilurilor de grup

Autorizările speciale ale profilurilor de grup sunt disponibile membrilor aceluși grup. Profilurile utilizator care sunt membri a unul sau mai multor grupuri au propriile autorizări speciale, plus autorizările speciale ale oricărui profil de grup pentru care utilizatorul e membru. Autorizările speciale sunt cumulative pentru utilizatorii care sunt membri ale grupurilor multiple. De exemplu, presupuneți că profilul GROUP1 are *JOBCTL, profilul GROUP3 are *AUDIT și profilul GROUP16 are autorizările speciale *IOSYSCFG. Un profil utilizator care are toate cele trei profiluri ca profilurile sale de grup are autorizările speciale *JOBCTL, *AUDIT și *IOSYSCFG.

Notă: Dacă un membru de grup deține un program, acesta adoptă doar autorizarea deținătorului. Autorizările grupului sunt **not** adoptate.

Folosirea unui profil individual ca profil de grup

Crearea profilurilor specific pentru a fi profiluri de grup este preferabilă transformării profilurilor existente în profiluri de grup. Puteți găsi că un utilizator specific are toate autorizările necesare pentru un grup de utilizatori și poate fi tentat să facă acel profil utilizator un profil de grup. Totuși, 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 responsabilitățile, un nou profil necesită să fie desemnat ca profil de grup, autorizările necesită să fie modificate și dreptul de proprietate necesită să fie transferat.
- Toți 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 alți utilizatori.

Încercați să planificați profiluri de grup în avans. Creați profiluri de grup specifice cu parola *NONE. Dacă descoperiți după ce o aplicație a rulat că un utilizator are autorizări care ar trebui să aparțină unui grup de utilizatori, faceți următoarele:

1. Creați un profil de grup.
2. Folosiți comanda GRTUSRAUT pentru a da autorizările utilizatorului pentru profilul de grup.
3. Înlăturați autorizările private din utilizator, deoarece ele nu mai sunt necesare. Folosiți comanda RVKOBJAUT sau EDTOBJAUT.

Comparație între profilurile de grup și listele de autorizări

Profilurile de grup sunt folosite pentru a simplifica gestionarea profilurilor utilizator care au cerințe de securitate similare. Listele de autorizări sunt folosite pentru a securiza obiecte cu cerințe de securitate similare. Tabela 123 arată caracteristicile celor două metode:

Tabela 123. Comparație între lista de autorizări și profilul de grup

Articolul comparat	Listă de autorizări	Profil de grup
Folosit pentru a securiza obiecte multiple	Da	Da
Utilizatorul poate aparține mai multora	Da	Da
Autorizarea privată înlocuiește altă autorizare	Da	Da
Utilizatorului trebuie să-i fie asignată autorizare independent	Da	Nu
Autorizările specificate sunt aceleași 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 ștersă când obiectul este șters	Da	Da
Asocierea cu obiectul este salvată când obiectul este salvat	Da	Nu ²

¹ Profilului de grup îi poate fi acordată autorizare când este crea un obiect folosind parametrul GRPAUT din profilul utilizatorului care îl creează.

² Autorizarea de grup primar este salvată cu obiectul.

- l Pentru lista de autorizări a elementului "Autorizarea poate fi specificată când este creat obiectul":
- l • Pentru a asigna o listă de autorizări unui obiect bazat pe bibliotecă, specificați AUT (*LIBCRTAUT) în comanda CRTxxxx și CRTAUT (authorization-list-name) pentru bibliotecă. Unele obiecte, cum ar fi listele de validare, nu pot folosi o valoare de *LIBCRTAUT în comanda CRT.
 - l • Pentru a asigna o listă de autorizări unui obiect bazat pe bibliotecă, specificați valoarea *INDIR pentru parametrii DTAAUT și OBJAUT ai comenzii MKDIR. În acest fel, lista de autorizări asigură și directorul părinte și pe cel nou. Sistemul nu permite ca o listă de autorizări arbitrară să fie specificată când este creat un obiect.

Planificarea securității pentru programatori

Programatorii reprezintă o problemă pentru responsabilul cu securitatea. Cunoștințele lor îi pot face să ocolească procedurile de securitate care nu sunt proiectate cu atenție. Ei pot ocoli securitatea pentru a accesa date de care au nevoie pentru testare. De asemenea ei pot dejuca procedurile normale care alocă resurse ale sistemului pentru a realiza performanțe mai bune pentru propriile joburi. Securitatea e deseori văzută de ei ca un obstacol pentru realizarea task-urilor cerute de jobul lor, cum ar fi testarea aplicațiilor. Totuși, 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.

Urmați aceste linii când setați un mediu pentru programatorii de aplicații:

- Nu acordați **toate** autorizările speciale programatorilor. Totuși, dacă trebuie să le dați autorizări speciale, dați-le **doar** autorizarea specială necesară pentru a realiza joburile sau task-urile asignate programatorului.
- Nu folosiți profilul utilizator QPGMR ca un profil de grup pentru programatori.
- Folosiți biblioteci de test și împiedicați accesul la bibliotecile de producție.
- Creați biblioteci ale programatorilor și folosiți un program care adoptă autorizare pentru a copia datele de producție selectate în bibliotecile programatorului pentru testare.
- Dacă performanțele interactive sunt o problemă, considerați modificarea comenzilor pentru crearea programelor să ruleze doar în batch:
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
- Realizați auditarea securității funcției aplicației înainte de mutarea aplicațiilor sau a modificărilor de program din bibliotecile de testare în cele de producție.

- Folosiți tehnica de profil de grup când e dezvoltată o aplicație. Toate programele aplicație să fie deținute de un profil de grup. Faceți programatorii care lucrează la aplicație membri ai grupului și definiți profilurile utilizator ale programatorului ca grupul să dețină orice obiecte noi create (OWNER(*GRPPRF)). Când un programator se mută de la un proiect la altul, puteți modifica informațiile de grup din profilul său. Vedeți “Dreptul de proprietate al grupului asupra obiectelor” la pagina 122 pentru informații suplimentare.
- Dezvoltați un plan pentru asignarea dreptului de proprietate asupra aplicațiilor când sunt mutate la producție. Pentru a controla modificările asupra unei aplicații de producție, toate obiectele aplicației, inclusiv programele trebuie să fie deținute de profilul utilizator proiectat pentru aplicație.

Obiectele aplicației nu ar trebui deținute de un programator deoarece acesta ar avea acces necontrolat la ele într-un mediu de producție. Profilul care deține aplicația poate fi cel al individului responsabil pentru aplicație sau poate fi profilul creat specific ca deținător al aplicației.

Gestionarea fișierelor sursă

Fișierele sursă sunt importante pentru integritatea sistemului dumneavoastră. Ele pot fi de asemenea un bun valoros al companiei, dacă ați dezvoltat sau obținut aplicații personalizate. Fișierele sursă ar trebui să fie protejate ca și alte fișiere importante de pe sistem. Considerați punerea fișierelor sursă în biblioteci separate și controlarea celor care le pot actualiza și muta la producție.

Când e creat un fișier sursă pe sistem, autorizarea publică implicită este *CHANGE, care permite oricărui utilizator să actualizeze orice membru sursă. Implicit, doar proprietarul fișierului sursă sau un utilizator cu autorizarea specială*ALLOBJ poate adăuga sau înlătura membri. În majoritatea cazurilor, această autorizare implicită pentru fișiere sursă fizice ar trebui modificată. Programatorii care lucrează la o aplicație au nevoie de autorizarea *OBJMGT pentru fișierele sursă pentru a adăuga membri noi. Autorizarea publică ar trebui probabil să fie redusă la *USE sau *EXCLUDE, doar dacă fișierele nu sunt într-o bibliotecă controlată.

Protejarea fișierelor class și jar Java în sistemul de fișiere integrat

Pentru a rula un program Java, aveți nevoie de autorizare de citire (*R) pentru fiecare fișier class și jar Java plus autorizare de execuție (*X) pentru fiecare director din calea fișierelor class și jar Java. Dacă folosiți fișiere class și jar Java în sistemul de fișiere integrat, trebuie să le protejați folosind autorizări normale de obiect. Pentru a proteja fișiere Java, folosiți comanda CHGAUT pentru a asigura directoarele din cale și fișierele cu attribute autorizare obiect. Un utilizator poate avea nevoie de autorizare de citire (*R) pentru fișierele class și jar Java pentru a rula un program Java. Pot primi acea autorizare de la autorizarea publică a fișierului sau de la autorizarea privată. O listă de autorizări este utilă în setarea autorizării private pentru un grup de utilizatori. Nu dați oricui autorizare de scriere (*W) asupra fișierului decât dacă au permisiunea de a modifica fișierul.

Puteți folosi parametrul Classpath Security Check Level din comanda RUNJVA pentru a vă asigura că o aplicație Java care rulează folosește fișierele corecte din CLASSPATH. Puteți folosi o valoare de CHKPATH(*SECURE).

Planificarea securității pentru programatori de sistem sau manageri

Majoritatea sistemelor au pe cineva responsabil pentru funcții de administrare. Această persoană monitorizează folosirea resurselor sistemului, în special spațiul de stocare de pe disc, pentru a se asigura că utilizatorii înlătură regulat obiectele nefolosite pentru a elibera spațiu. Programatorii de sistem au nevoie de autorizare mare pentru a observa toate obiectele din sistem. Totuși, nu au nevoie să vadă conținutul acelor obiecte.

Puteți folosi autorizare adoptată pentru a furniza un set de comenzi de afișare pentru programatorii de sistem, mai degrabă decât să dați autorizări speciale în profilurile lor utilizator.

Planificarea folosirii obiectelor din lista de validare

Obiectele listei de validare furnizează o metodă pentru aplicații de a stoca în siguranță informații de autentificare utilizatori.

De exemplu, ICS (Internet Connection Server) folosește liste de validare pentru a implementa conceptul de **utilizator Internet**. ICS poate realiza **autentificare de bază** înainte să fie servită o pagină Web. Autentificarea de bază necesită

ca utilizatorii să furnizeze un tip de informații de autentificare, cum ar fi parolă, PIN sau număr de cont. Numele utilizatorului și informațiile de autentificare pot fi memorate sigur într-o listă de validare. ICS poate folosi informațiile din listele de validare mai degrabă decât să ceară ca toți utilizatorii săi să aibă iSeries un id utilizator și o parolă.

Unui utilizator de internet îi poate fi permis sau refuzat accesul la iSeries de pe serverul Web. Utilizatorul, totuși, nu are nici o autorizare pentru iSeries nici o resursă sau autorizare să semneze sau să ruleze joburi. Un iSeries profil utilizator nu e niciodată creat pentru utilizatori internet.

Pentru a crea și șterge listele de validare, puteți folosi comenzile CL CRTVLDL (Create Validation List - Creare listă de validare) și DLTVLDL (Delete Validation List - Ștergere listă de validare). Sunt furnizate de asemenea API-uri (Application Programming Interfaces) pentru a permite aplicațiilor să adauge, modifice, înlăture, verifice (autentifice) și să găsească intrări într-o listă de validare. Pentru informații suplimentare și exemple, vedeți subiectul API-uri din Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Obiectele listei de validare sunt disponibile pentru folosirea de către toate aplicațiile. De exemplu, dacă o aplicație necesită o parolă, parolele aplicației pot fi memorate într-un obiect al listei de validare mai degrabă decât într-un fișier bază de date. Aplicația poate folosi API-urile listei de validare pentru a verifica parola unui utilizator, care e criptată, mai degrabă decât ca aplicația să realizeze verificarea însăși.

- | Puteți stoca informațiile de autentificare într-o formă decriptabilă. Dacă un utilizator are securitatea corespunzătoare, informațiile de autentificare pot fi descrise și returnate utilizatorului. Pentru informații despre controlarea memorării datelor decriptabile în liste de validare, vedeți “Reținerea informațiilor de securitate server (QRETSVRSEC)” la pagina 27.

Limitarea accesului la funcția programului

- | Limitarea accesului la funcția programului vă permite să definiți cine poate folosi o aplicație, părți din ea sau funcțiile dintr-un program. Acest suport **nu** e o înlocuire a securității resursei. Funcția de limitare a accesului la program nu împiedică un utilizator să acceseze o resursă (cum ar fi un fișier sau program) din altă interfață.
- | Limitarea accesului la program furnizează API-uri pentru a realiza următoarele task-uri:
 - Înregistrarea unei funcții
 - Extragerea informațiilor despre funcție
 - Definirea celor care pot sau nu să folosească funcția
 - Verifica dacă utilizatorului îi e permis să folosească funcția

Pentru a folosi acest suport în interiorul aplicației, furnizorul ei trebuie să înregistreze funcțiile când e instalată aplicația. Funcția înregistrată corespunde unui bloc de cod pentru funcții specifice din aplicație. Când utilizatorul rulează aplicația, ea apelează API-urile de folosire pentru a vedea dacă utilizatorului îi e permis să folosească funcția care e asociată cu blocul de cod, înainte de a-l apela. Dacă utilizatorului îi e permis să folosească funcția înregistrată, este rulat blocul de cod. Dacă utilizatorului nu îi e permis să folosească funcția, utilizatorul este împiedicat să ruleze blocul de cod.

Administratorul de sistem specifică cui îi e permis sau refuzat accesul la o funcție. Administratorul poate fie să folosească comanda WRKFCNUSG (Work with Function Usage Information - Gestionare informații folosire funcție) pentru a gestiona accesul la funcția programului fie să folosească Navigator iSeries.

Capitolul 8. Salvarea de rezervă și recuperarea informațiilor de securitate

În acest capitol este discutată relația dintre securitate și salvarea de rezervă și recuperarea pe sistemul dumneavoastră:

- Modul în care informațiile despre securitate sunt salvate și restaurate
- Modul în care securitatea afectează salvarea și restaurarea obiectelor
- Probleme de securitate asociate cu autorizarea speciale *SAVSYS

Această *Backup and Recovery* carte furnizează informații suplimentare despre copierea de rezervă și recuperare. Puteți de asemenea să consultați subiectele Copierea de rezervă și recuperarea din Centrul de informare iSeries (consultați “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Salvarea informațiilor dumneavoastră de securitate este la fel de importantă ca salvarea datelor dumneavoastră. În anumite situații, este posibil să fie nevoie să recuperați profiluri de utilizator, autorizări de obiecte și date pe sistemul dumneavoastră. În cazul în care nu aveți salvate informațiile dumneavoastră de securitate, va trebui să reconstruiți manual profilurile utilizator și autorizările de obiecte. Aceasta poate fi o activitate consumatoare de timp și poate duce la erori și la probleme de securitate.

Planificarea procedurilor corespunzătoare de copiere de rezervă și recuperare pentru informațiile de securitate necesită înțelegerea modului în care informațiile sunt stocate, salvate și restaurate.

Tabela 124 arată comenzile folosite pentru a salva și restaura informațiile de securitate. Această secțiune discută despre salvarea și recuperarea datelor de securitate în detaliu.

Tabela 124. Modul în care informațiile de securitate sunt salvate și restaurate

Informațiile de securitate salvate și restaurate	Comenzi de salvare și restaurare				
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT
Profiluri de utilizator	X		X		
Dreptul de proprietate ¹		X		X	
Grup primar ¹		X		X	
Autorizări publice ¹		X		X	
Autorizări private	X				X
Liste de autorizare	X		X		
Deținător de autorizare	X		X		
Legătura cu lista de autorizare și deținătorii de autorizare		X		X	
Valoare auditare obiect		X		X	
Informații înregistrare funcție ²		X		X	
Informații de folosire funcție	X		X		X
Liste de validare		X		X	

¹ Comenzile SAVSECDTA, SAVSYS și RSTUSRPRF salvează și restaurează drepturi de proprietate, grupuri primare, autorizări de grup primare și autorizări publice pentru aceste tipuri de obiecte: Profil utilizator (*USRPRF), listă de autorizare(*AUTL), și deținător de autorizare (*AUTHLR).

² Obiectul de salvat/restaurat este QUSEXRGOBJ, tip *EXITRG din biblioteca QUSRSYS.

Modul în care sunt stocate informațiile de securitate

Informațiile de securitate sunt stocate cu obiecte, profiluri utilizator și liste de autorizare:

Informații de autorizare stocate cu obiecte:

- Autorizare publică
- Nume proprietar
- Autorizarea proprietarului la obiect
- Nume grup primar
- Autorizarea grupului primar la obiect
- Nume listă autorizare
- Valoare auditare obiect
- Dacă există autorizare privată
- Dacă orice autorizare privată este mai puțin de public

Informații de autorizare stocate cu profilul utilizatorului:

Informații antet

Atributele profilului utilizator afișate în ecranul Create User Profile - Creare profil utilizator. uid și gid.

Informații autorizare privată

Autorizare privată la obiecte. Aceasta include autorizarea privată la liste de autorizare.

Informații despre proprietate

Lista obiectelor deținute

Pentru fiecare obiect, o listă a utilizatorilor cu autorizare privată la obiect.

Informații grup primar

Lista obiectelor pentru care profilul este grup primar.

Informații de auditare:

Valoare auditare acțiune

Valoare auditare obiect

Informații utilizare funcție:

Setările de utilizare pentru funcțiile înregistrate.

Informații de autorizare stocate cu liste de autorizare:

Informații de autorizare normală stocate cu orice obiect, cum ar fi autorizare publică și proprietar.

Lista obiectelor securizate de lista de autorizare.

Salvarea informațiilor de securitate

Informațiile de securitate sunt stocate diferențiat pe același mediu de stocare pe care este stocat sistemul dumneavoastră. Atunci când salvați profilurile utilizator, informațiile de autorizare privată stocate cu profilul utilizator sunt formate într-o tabelă de autorizare. O tabelă de autorizare este construită și salvată pentru fiecare profil utilizator care are autorizări private. Această reformatare și salvare a informațiilor de securitate poate fi de durată în cazul în care aveți multe autorizări private pe sistemul dumneavoastră.

Acesta este modul în care informațiile de securitate sunt stocate pe mediul de stocare:

Informații de autorizare salvate cu obiect:

Autorizare publică

Nume proprietar

Autorizarea proprietarului la obiect
Nume grup primar
Autorizarea grupului primar la obiect
Nume listă autorizare
Câmp nivel autorizări
Valoare auditare obiect
Dacă există autorizare privată
Dacă orice autorizare privată este mai puțin de public

Informații de autorizare salvate cu liste de autorizare:

Informații de autorizare normală stocate cu orice obiect, cum ar fi autorizare publică, proprietar și grup primar.

Informații de autorizare salvate cu profilul utilizatorului:

Atributele profilului utilizator afișate în ecranul Create User Profile - Creare profil utilizator.

Tabela de autorizare salvată asociată cu profilul utilizatorului:

Câte o înregistrare pentru fiecare autorizare privată a profilului utilizator, incluzând setări de folosire pentru funcțiile înregistrate.

Informații înregistrare funcție salvate cu obiectul QUSEXRGOBJ:

Informațiile de înregistrare a funcției pot fi salvate prin salvarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS.

Recuperare informațiilor de securitate

Recuperarea sistemului dumneavoastră înseamnă restaurarea datelor și a informațiilor de securitate asociate. Secvența obișnuită de recuperare este:

1. Restaurare profiluri de utilizator și liste de autorizare (RSTUSRPRF USRPRF(*ALL)).
2. Restaurare obiecte (RSTCFG, RSTLIB, RSTOBJ, RSTDLO sau RST).
3. Restaurare autorizări private la obiecte (RSTAUT).

Cartea *Backup and Recovery* furnizează mai multe informații despre planificarea recuperării.

Restaurarea profilurilor de utilizator

Unele modificări pot fi efectuate asupra unui profil utilizator atunci când este restaurat. Se aplică următoarele reguli:

- Dacă profilurile ce sunt restaurate individual (RSTUSRPRF USRPRF(*ALL) nu este specificat), SECDTA(*PWDGRP) nu este solicitat și profilul ce este restaurat nu există pe sistem, aceste câmpuri se modifică în *NONE:

- Nume profil grup (GRPPRF)
- Parolă (PASSWORD)
- Parolă a documentului (DOCPWD)
- Profiluri suplimentare de grup (SUPGRPPRF)

Parolele produsului sunt modificate în *NONE, astfel încât ele vor fi incorecte după restaurarea unui profil utilizator individual care nu există pe sistem.

- Dacă profilurile ce sunt restaurate individual (RSTUSRPRF USRPRF(*ALL) nu este specificat), SECDTA(*PWDGRP) nu este solicitat și profilul există pe sistem, parola, parola document și profilul grupului nu se modifică.

Profilurile utilizatorului pot fi restaurate individual cu parola și informațiile de grup restaurate de pe mediul de salvare, prin specificarea parametrului SECDTA(*PWDGRP) în comanda RSTUSRPRF. Autorizările speciale *ALLOBJ și *SECADM sunt cerute pentru a restaura parola și informațiile de grup, când se restaurează profilurile

individuale. Parolele produsului restaurate cu profilul utilizator vor fi incorecte după restaurarea unui profil utilizator individual care există pe sistem, doar dacă nu este specificat parametrul SECDDTA(*PWDGRP) în comanda RSTUSRPRF.

- Dacă toate profilurile utilizator sunt restaurate pe sistemul dumneavoastră, toate câmpurile din orice profil care există deja pe sistem, sunt restaurate de pe mediul de salvare, inclusiv parola.

Atenție: Profilurile utilizator salvate de pe sistem cu un nivel diferit de parolare (QPWDLVL variabilă de sistem) față de cel al sistemului ce este restaurat pot determina constituirea unei parole care nu este validă pe sistemul restaurat. De exemplu, dacă profilul utilizator ce este salvat vine de pe un sistem pe care rulează un nivel 2 de parolare, utilizatorul ar putea obține o parolă de tipul "Aceasta este parola mea". Această parolă nu ar fi validă pe un sistem pe care rulează nivelul de parolare 0 sau 1.

Atenție: Păstrați o înregistrare a parolei responsabilului cu securitatea (QSECOFR) asociată cu fiecare versiune a informațiilor dumneavoastră de securitate ce sunt salvate pentru a vă asigura că puteți să vă logați pe sistemul dumneavoastră, dacă trebuie să realizați o operație completă de restaurare.

Puteți folosi DST (Dedicated Service Tools - Instrumente dedicate de service) pentru a reseta parola pentru profilul QSECOFR. Consultați subiectul Instrumente pentru service din Centrul de informare, în legătură cu instrucțiunile. Vedeți "Cerințe preliminare și informații înrudite" la pagina xvi pentru informații suplimentare asupra accesării, Centrul de informare.

- Dacă există un profil pe sistem, operația de restaurare nu modifică uid sau gid.
- Dacă nu există un profil pe sistem, uid și gid pentru un profil sunt restaurate din mediul de salvare. Dacă atât uid cât și gid există deja pe sistem, sistemul generează o nouă valoare și compune un mesaj (CPI3810).
- Autorizarea specială *ALLOBJ este înlăturată din profilurile utilizator ce sunt restaurate pe un sistem la nivelul de securitate 30 sau mai înalt în oricare din situațiile acestea:
 - Profilul a fost salvat de pe un sistem diferit și utilizatorul ce realizează RSTUSRPRF nu are autorizările speciale *ALLOBJ și *SECADM.
 - Profilul a fost salvat de pe același sistem la nivelul de securitate 10 sau 20.

ATENȚIE: Sistemul folosește numărul de serie al mașinii de pe sistem și de pe mediul de salvare pentru a determina dacă obiectele sunt restaurate pe același sistem sau pe un alt sistem.

Autorizarea specială *ALLOBJ **nu** este înlăturată de pe aceste profiluri furnizate de IBM:

profil utilizator QSYS (sistem)

profil utilizator QSECOFR (responsabil de securitate)

profil utilizator QLPAUTO (instalare automată a programului licențiat)

profil utilizator QLPINSTALL (instalare a programului licențiat)

Restaurarea obiectelor

Când restaurați un obiect pe un sistem, sistemul folosește informațiile de autorizare stocate cu obiectul. Următoarele se aplică securității obiectului restaurat:

Drept de proprietate a obiectului:

- Dacă profilul care deține obiectul este pe sistem, dreptul de proprietate este restaurat pe acel profil.
- Dacă proprietarul profilului nu există pe sistem, dreptul de proprietate al obiectului este cedat profilului utilizator QDFTOWN (proprietar implicit).
- Dacă obiectul există pe sistem și proprietarul sistemului este diferit față de proprietarul mediului de salvare, obiectul nu este restaurat dacă nu este specificat ALWOBJDIF(*ALL). În acest caz, obiectul este restaurat și proprietarul sistemului este folosit.
- Vedeți "Restaurarea programelor" la pagina 225 pentru informații 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 și 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 operația de restaurare.

Autorizare publică:

- Dacă obiectul ce este restaurat nu există pe sistem, autorizarea publică este setată pe autorizarea publică a obiectului salvat.
- Dacă obiectul ce este restaurat nu există pe sistem și este înlocuit, autorizarea publică nu este modificată. Autorizarea publică de la versiunea salvată a obiectului nu este folosită.
- CRTAUT pentru bibliotecă nu este folosit când se face restaurarea obiectelor la bibliotecă.

Lista de autorizare:

- Dacă un obiect, altul decât un document sau fișier, există deja pe sistem și este legat de o listă de autorizare, parametrul ALWOBJDIF determină rezultatul:
 - Dacă este specificat ALWOBJDIF(*NONE), obiectul existent trebuie să aibă aceeași listă de autorizare precum obiectul salvat. Dacă nu, obiectul nu este restaurat.
 - Dacă este specificat ALWOBJDIF(*ALL), obiectul este restaurat. Obiectul este legat de lista de autorizare asociată cu obiectul existent.
- Dacă un document sau un fișier ce există deja pe sistem este restaurat, lista de autorizare asociată cu obiectul de pe sistem este folosită. Lista de autorizare de pe documentul sau fișierul salvat nu este folosită.
- Dacă nu există lista de autorizare pe sistem, obiectul este restaurat fără a fi legat de lista de autorizare și autorizarea publică este modificată la *EXCLUDE.
- Dacă obiectul ce este restaurat pe același 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 și autorizarea publică a obiectului este modificată la *EXCLUDE.

Autorizări private:

- Autorizarea privată este salvată cu profilurile utilizator, nu cu obiecte.
- Dacă profilurile utilizator au autorizare privată pentru un obiect ce se restaurează, acele autorizări private nu sunt, de obicei, afectate. Restaurarea anumitor tipuri de programe poate determina revocarea autorizărilor private. Vedeți “Restaurarea programelor” la pagina 225 pentru informații suplimentare.
- Dacă este șters un obiect din sistem și apoi restaurat din versiunea salvată, autorizarea privată a obiectului nu mai există deja pe sistem. Când este șters un obiect, toate autorizările private ale obiectului sunt înlăturate din profilul utilizator.
- Dacă autorizările private trebuie să fie recuperate, comanda RSTAUT (Restore Authority - Restaurare autorizare) trebuie folosită. Secvența obișnuită este:
 1. Restaurare profiluri utilizator
 2. Restaurare obiecte
 3. Restaurare autorizare

Auditare obiect:

- Dacă obiectul ce este restaurat nu există pe sistem, variabila auditare obiect (OBJAUD) a obiectului salvat este restaurată.
- Dacă obiectul ce este restaurat nu există pe sistem și este înlocuit, variabila auditare obiect nu este modificată. Valoarea OBJAUD de la versiunea salvată a obiectului nu este restaurată.
- Dacă obiectul ce este restaurat nu există pe sistem, variabila creare auditare obiect (CRTOBJAUD) pentru bibliotecă este restaurată.
- Dacă o bibliotecă ce este restaurată există și este înlocuită, variabila CRTOBJAUD pentru bibliotecă nu este restaurată. Variabila CRTOBJAUD pentru bibliotecă existentă este folosită.

Deținător de autorizare:

- Dacă un fișier este restaurat și un deținător de autorizare există pentru acel nume de fișier la care este restaurat, fișierul este legat la deținătorul de autorizare.
- Informațiile de autorizare asociate cu deținătorul de autorizare înlocuiesc autorizarea publică și informațiile deținătorului salvate cu fișierul.

Obiecte din domeniul utilizator:

- Pentru sisteme ce rulează Versiunea 2 Ediția 3 sau ulterioară a i5/OS programului licențiat, sistemul restricționează obiectele domeniu utilizator (*USRSPC, *USRIDX și *USRQ) la bibliotecile specificate în variabila 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.

Informații înregistrare funcție:

- Informațiile de înregistrare a funcției pot fi restaurate prin restaurarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS. Aceasta restaurează toate funcțiile înregistrate. Aceste informații de utilizare sunt asociate cu funcții și sunt restaurate când profilurile utilizator și autorizările sunt restaurate.

Aplicații care folosesc înregistrarea certificatelor

- Aplicațiile care folosesc informații de înregistrare a certificatelor pot fi restaurate prin restaurarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS. Aceasta restaurează toate aplicațiile înregistrate. Asocierea aplicației la informațiile ei de certificare poate fi restaurată prin restaurarea obiectului QYCDCERTI *USRIDX din QUSRSYS.

Restaurarea autorizării

Când este restaurată informația de securitate, autorizările private trebuie să fie reconstruite. Când se restaurează un profil de utilizator care are o tabelă de autorizare, este restaurată și tabela de autorizare pentru profil.

Comanda Restaurare autorizare (RSTAUT) reconstruiește autorizarea privată în profilul de utilizator folosind informațiile din tabela de autorizare. Operația de acordare a autorizării este rulată pentru fiecare autorizare privată din tabela de autorizare. Dacă autorizarea este restaurată pentru multe profile și multe autorizări private există în tabellele autorizare, acesta poate fi un proces de durată.

Comenzile RSTUSRPRF și RSTAUT pot fi rulate pentru un profil singular, o listă de profile, un nume generic de profil sau toate profilele. Sistemul caută mediul de salvare sau fișierele de salvare create de comanda SAVSECDTA sau SAVSYS sau API-ul QRSRAVO pentru a găsi profilele pe care doriți dumneavoastră să le restaurați.

Restaurare a autorizării câmpului:

Următorii pași se cer pentru a restaura autorizări câmp privat pentru fișiere bază de date care nu există încă pe sistem:

- Restaurați sau creați profilele utilizator necesare.
- Restaurare fișiere.
- Rulare a comenzii RSTAUT (Restore Authority - Restaurare autorizare)

Autorizările câmp privat nu sunt restaurate în totalitate până când autorizările obiect privat pe care ele le restricționează, nu sunt din nou restabilite.

Restaurarea programelor

Restaurarea programelor pe sistemul dumneavoastră ce sunt obținute de la o sursă necunoscută pun o problemă de securitate. Programele pot realiza operații care întrerup cererile de securitate. De o atenție deosebită se bucură programele care conțin instrucțiuni restricționate, programele care adoptă propria lor autorizare și programele care au fost dotate cu aceasta. Aceasta include tipurile de obiect *PGM, *SRVPGM, *MODULE și *CRQD. Puteți folosi variabilele de sistem QVfyOBRST, QFRCCVNRST și QALWOBJRST pentru a preveni aceste tipuri de obiecte de la a fi restaurate pe sistemul dumneavoastră. Consultați Variabile de sistem restaurare referitoare la securitate pentru informații suplimentare despre aceste variabile de sistem.

Sistemul folosește o variabilă de validare pentru a ajuta la protejarea programelor. Această variabilă este stocată cu un program și recalculată când este restaurat programul. Acțiunile sistemului sunt determinate de parametrul ALWOBJDIF din comanda de restaurare și forțează conversia pentru restaurarea variabilei de sistem (QFRCCVNRST).

Notă: Programele ce sunt create pentru Versiunea 5 Ediția 1 iSeries sau una ulterioară conțin informații care permit programului să fie recreat la momentul restaurării, dacă este necesar. Informațiile 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. Acțiunea de recreare a programului la momentul restaurării nu este ceva nou la iSeries V5R1. În edițiile anterioare, orice eroare de validare a programului întâlnită în momentul restaurării rezulta în recrearea programului dacă era posibil acest lucru (dacă exista observabilitate în programul de restaurat). Diferența dintre iSeries Version 5 Release 1 și programele ulterioare este aceea că informațiile necesare pentru recrearea programului rămân chiar și atunci când observabilitatea a fost înlăturată din program.

Restaurarea programelor care adoptă autorizarea proprietarului:

Atunci când un program este restaurat și adoptă autorizarea deținătorului, dreptul de proprietate și autorizarea la program pot fi modificate. Se aplică următoarele reguli:

- Profilul utilizatorului ce realizează operațiunea de restaurare trebuie fie să dețină programul, fie să aibă autorizările speciale *ALLOBJ și *SECADM.
- Profilul utilizatorului ce realizează operațiunea de restaurare poate primi autorizarea de a restaura programul dacă
 - Este deținătorul programului.
 - Este un membru al profilului de grup care deține programul (în cazul în care nu aveți autorizare privată asupra programului).
 - Are autorizările speciale *ALLOBJ și *SECADM.
 - Este un membru al profilului de grup care are autorizările speciale *ALLOBJ și *SECADM.
 - Rulează sub o autorizare adoptată care îndeplinește unul din testele de mai sus.
- În cazul în care profilul care restaurează nu are autorizarea adecvată, toate autorizările publice și private asupra programului sunt revocate și autorizarea publică este modificată în *EXCLUDE.
- În cazul în care deținătorul programului nu există în sistem, dreptul de proprietate este dat profilului utilizator QDFTOWN. Autorizarea publică este modificată în *EXCLUDE și lista de autorizare este înlăturată.

Restaurarea programelor licențiate

Comanda Restore Licensed Programs (RSTLICPGM) este folosită pentru a instala programele furnizate de IBM pe sistemul dumneavoastră. Poate fi folosită de asemenea pentru a instala programe non-IBM create folosind programul licențiat SystemViewSystem Manager/400.

La furnizarea sistemului dumneavoastră, doar utilizatorii cu autorizarea specială *ALLOBJ pot folosi comanda RSTLICPGM. Apelurile de procedură ale RSTLICPGM apelează un program ieșire pentru a instala programe care nu sunt furnizate de IBM.

Pentru a proteja securitatea pe sistemul dumneavoastră, programul de ieșire nu trebuie să ruleze folosind un profil cu autorizarea specială *ALLOBJ. Folosiți un program care adoptă autorizarea specială *ALLOBJ pentru a rula comanda RSTLICPGM, în loc de a avea un utilizator cu autorizarea *ALLOBJ care să ruleze direct comanda.

Urmează un exemplu pentru această tehnică. Programul de instalat folosind comanda RSTLICPGM este numit CPAPP (Contracts and Pricing).

1. Creați un profil de utilizator cu autorizare suficientă pentru a instala cu succes aplicația. Nu acordați acestui profil autorizarea specială *ALLOBJ. Pentru acest exemplu, profilul de utilizator este numit OWNCP.
2. Scrieți un program pentru a instala aplicația. De exemplu, programul este numit CPINST:
PGM
RSTLICPGM CPAPP
ENDPGM
3. Creați programul CPINST pentru a adopta autorizarea unui utilizator cu autorizarea specială *ALLOBJ, cum ar fi QSECOFR și autorizați OWNCP la program:
CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
AUT(*EXCLUDE)
GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
USER(OWNCP) AUT(*USE)
4. Semnați ca OWNCP și apelați programul CPINST. Atunci când programul CPINST rulează comanda RSTLICPGM, rulați sub autorizarea QSECOFR. Atunci când programul ieșire rulează pentru a instala programele CPAPP, aruncă autorizarea adoptată. Programele apelate de programul ieșire rulează sub autorizarea OWNCP.

Restaurarea listelor de autorizare

Listele de autorizare sunt salvate fie de comanda SAVSECDTA, fie de comanda SAVSYS. Listele de autorizare sunt restaurate de comanda:

```
RSTUSRPRF USRPRF(*ALL)
```

Nu există nici o metodă pentru restaurarea listelor de autorizare individuale.

La restaurarea unei liste de autorizare, autorizarea și dreptul de proprietate sunt stabilite așa cum sunt ele pentru orice alt obiect care este restaurat. Legătura dintre listele de autorizare și obiecte este stabilită dacă obiectele sunt restaurate după lista de autorizare. Consultați “Restaurarea obiectelor” la pagina 222 pentru mai multe informații. Autorizările private ale utilizatorilor pentru listă sunt restaurate folosind comanda RSTAUT.

Recuperarea dintr-o listă de autorizare deteriorată

Atunci când un obiect este securizat de o listă de autorizare și lista de autorizare este deteriorată, accesul la obiect este limitat la utilizatorii care au autorizarea specială *ALLOBJ.

Pentru a recupera dintr-o listă de autorizare deteriorată, sunt necesari doi pași.

1. Recuperarea utilizatorilor și a autorizărilor lor din lista de autorizare.
2. Recuperarea asociațiilor listei de autorizare cu obiecte.

Acești pași trebuie făcuți de un utilizator cu autorizarea specială *ALLOBJ.

Recuperarea listei de autorizare: În cazul în care autorizările utilizatorilor ’ la lista de autorizare sunt cunoscute, ștergeți lista de autorizare, creați-o din nou și apoi adăugați la ea utilizatori.

Dacă nu este posibil să creați din nou lista de autorizare pentru că nu știți toate autorizările utilizatorilor, lista de autorizare poate fi restaurată și utilizatorii restaurați la lista de autorizare folosind ultimele benzi SAVSYS sau SAVSECDTA. Pentru a restaura lista de autorizare, efectuați următoarele:

1. Ștergeți lista de autorizare deteriorată folosind comanda DLTAUTL (Delete Authorization List - Ștergere listă de autorizare).
2. Restaurați lista de autorizare prin restaurarea profilurilor utilizator:
RSTUSRPRF USRPRF(*ALL)

3. Restaurați autorizările private ale utilizatorilor la listă folosind comanda RSTAUT .

Atenție: Această procedură restaurează valorile profil utilizator de pe mediul de salvare. Consultați “Restaurarea profilurilor de utilizator” la pagina 221 pentru informații suplimentare.

Recuperarea asociațiilor de obiecte la lista de autorizare: Atunci când lista de autorizare deteriorată este ștearsă, obiectele securizate de lista de autorizare trebuie adăugate la noua listă de autorizare. Faceți următoarele acțiuni:

1. Găsiți obiectele care erau asociate cu lista de autorizare deteriorată folosind comanda Reclaim Storage (RCLSTG). Reclamarea spațiului de stocare asociază obiectele care erau asociate cu lista de autorizare la lista de autorizare QRCLAUTL.
2. Folosiți comanda DSPAUTLOBJ (Display Authorization List Objects - Afișare obiecte ale listei de autorizare) pentru a afișa obiectele asociate cu lista de autorizare QRCLAUTL.
3. Folosiți comanda GRTOBJAUT (Grant Object Authority - Acordare autorizare obiect) pentru a securiza fiecare obiect cu lista de autorizare corectă.

```
GRTOBJAUT OBJ(ume-biblioteca/ume-obiect) +  
           OBJTYPE(tip-obiect) +  
           AUTL(ume-lista-autorizare)
```

Notă: Dacă un număr mare de obiecte sunt asociate cu lista de autorizare QRCLAUTL, creați un fișier bază de date prin specificarea OUTPUT(*OUTFILE) în comanda DSPAUTLOBJ. Puteți scrie un program CL pentru a rula comanda GRTOBJAUT pentru fiecare obiect din fișier.

Restaurarea sistemului de operare

La efectuarea unui IPL manual pe sistemul dumneavoastră, meniul IPL sau Instalare sistem furnizează o opțiune de instalare a sistemului de operare. Funcția DST (dedicated service tools - unelte serviciu dedicat) furnizează abilitatea de a cere oricui care folosește acest meniu parola de securitate DST. Puteți folosi aceasta pentru a preveni situația în care cineva restaurează o copie neautorizată a sistemului de operare.

Pentru a securiza instalarea sistemului dumneavoastră de operare, faceți următoarele:

1. Realizați un IPL manual.
2. Selectați DST de la un IPL sau de la meniul Instalarea sistemului.
3. Din meniul Folosire DST, selectați opțiunea de lucru cu mediul DST.
4. Selectați opțiunea de modificare a parolelor.
5. Selectați opțiunea de modificare a securității de instalare a sistemului de operare.
6. Specificare 1 (securizare).
7. Apăsați F3 (ieșire) până când vă întoarceți la IPL sau la meniul Instalare a sistemului.
8. Completați manualul IPL și lăsați cheia IPL la poziția sa normală.

Note:

1. Dacă nu mai doriți să securizați instalarea sistemului de operare, faceți pașii următori și specificați 2 (necurizat).
2. Puteți, de asemenea, preveni instalarea sistemului de operare prin păstrarea întrerupătorului cheii dumneavoastră IPL în poziția normală și înlăturarea cheii.

Autorizarea specială *SAVSYS

Pentru a salva sau restaura un obiect, trebuie să aveți 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 capacitatea de a salva un obiect și de a-l lua pe un sistem diferit spre a fi restaurat sau pentru a afișa (dump) mediul ca să vadă datele. De asemenea, dă unui utilizator capacitatea de a

salva un obiect și de a face o memorare liberă chiar și ștergând datele din obiect. Când salvați documentele, un utilizator cu autorizarea specială *SAVSYS are opțiunea de a șterge acele documente. Autorizarea specială *SAVSYS trebuie să fie acordată cu atenție.

Auditarea operațiilor de salvare și restaurare

Este scrisă o înregistrare de auditare a securității pentru fiecare operație de restaurare dacă variabila de auditare acțiune (variabila de sistem QAUDLVL sau AUDLVL din profilul de utilizator) include *SAVRST. Când folosiți o comandă care restaurează un număr mare de obiecte, precum RSTLIB, este scrisă o înregistrare de auditare pentru fiecare obiect restaurat. Aceasta poate determina probleme legate de dimensiunea receptorului jurnalului de auditare, în particular, dacă restaurați mai multe biblioteci.

Comanda RSTCFG nu creează o înregistrare de auditare pentru fiecare obiect restaurat. Dacă doriți să aveți o înregistrare de auditare pentru această comandă, setați 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 și SAVCFG nu creează înregistrări individuale de auditare pentru obiectele salvate, chiar dacă obiectele salvate au activă auditarea. Pentru a monitoriza aceste comenzi, setați auditarea obiect pentru aceste comenzi.

Capitolul 9. Auditarea securității pe sistemul iSeries

Acest capitol descrie tehnici de auditare a eficienței securității pe sistem. Auditarea sistemului se face din mai multe motive:

- Pentru a se evalua dacă planul de securitate este complet.
- Pentru a se asigura că se află în locul potrivit controalele de securitate planificate și că funcționează. Acest tip de auditare este realizat de responsabilul cu securitatea ca parte a administrării zilnice a securității. Se realizează de asemenea, uneori și mai amănunțit, ca parte a examinării periodice a securității 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 admiși în sistem
 - Modificarea dreptului de proprietate a unui obiect (autorizare ne potrivită)
 - Modificarea a responsabilităților (grup de utilizatori modificat)
 - Autorizare temporară (nerevocată în timp)
 - Produse noi instalate
- Pentru a face pregătirea pentru un eveniment viitor, precum instalarea unei noi aplicații, mutarea spre un nivel mai ridicat de securitate sau setarea unei rețele de comunicare.

Tehnicile descrise în acest capitol sunt potrivite pentru toate aceste situații. Ce lucruri și cât de des le auditați, depinde de dimensiunea și nevoile de securitate ale organizației dumneavoastră. Scopul acestui capitol este, mai de grabă, de a discuta ce informații sunt disponibile, cum se obțin și de ce sunt necesare, decât de a oferi îndrumări pentru frecvența auditărilor.

Acest capitol are trei părți:

- O listă de elemente de securitate ce pot fi planificate și auditate.
- Informații despre setarea și utilizarea jurnalului de auditare furnizat de sistem.
- Alte tehnici care sunt disponibile pentru a culege informații de securitate privind sistemul.

Auditarea securității implică utilizarea comenzilor pe sistemul iSeries și accesarea informațiilor despre sistem din istoric și din jurnal. Este posibil să doriți să creați un profil special pentru a fi utilizat de cineva pentru realizarea unei auditări a securității sistemului dumneavoastră. Profilul de auditare va necesita autorizarea specială *AUDIT pentru a fi capabil să modifice caracteristicile de auditare ale sistemului dumneavoastră. Unele operații de auditare sugerate în acest capitol, necesită un profil utilizator cu autorizarea specială *ALLOBJ și *SECADM. Asigurați-vă că setați parola pentru profilul de auditare la *NONE, când s-a terminat perioada de auditare.

Listă de verificare pentru responsabilii cu securitatea și auditori

Această listă de verificare poate fi folosită, atât pentru planificare, cât și pentru auditare a securității sistemului. În timp ce planificați securitatea, alegeți elementele din listă, care împlinesc cererile dumneavoastră de securitatea. Când auditați securitatea sistemului dumneavoastră, folosiți lista pentru evaluarea controalelor pe care le aveți pe poziții și determinați dacă sunt necesare controale suplimentare.

Aceasta listează servere ca o sinteză a informației din această carte. Lista conține descrieri pe scurt ale modului în care se face fiecare element și cum se monitorizează ceea ce s-a făcut, inclusiv ce intrări se vor căuta în jurnalul QAUDJRN. Detalii despre elementele acestea se găsesc în carte.

Securitatea fizică

Notă: Subiectul Securitatea de bază a sistemului și planificarea din Centrul de informare conține o prezentare completă problemelor legate de securitatea fizică pe sistemul iSeries. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Unitatea sistem și consola se află într-o locație sigură.

Mediul cu copia de rezervă este protejat față de deteriorare și furt.

Comutatorul cheie IPL de pe unitatea procesor este în poziția Secure sau Auto. Cheia este înlăturată. Cheile se păstrează separat, amândouă, sub securitate fizică strictă. Consultați Centrul de informare pentru informații suplimentare despre comutatorul cheie IPL (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Accesul la stațiile de lucru localizate public și la consolă este restricționat. Utilizați comanda DSPOBJAUT pentru a vedea cine are autorizarea *CHANGE la stațiile de lucru. Căutați în jurnalul de auditare intrări AF ce au câmpul pentru tipul obiectului egal cu *DEVDD, pentru a găsi încercări de semnare pe stațiile de lucru restricționate.

Logarea pentru utilizatori cu autorizarea specială *ALLOBJ sau *SERVICE este limitată la câteva stații de lucru. Faceți verificarea pentru a vedea dacă variabila de sistem QLMTSECOFR este 1. Folosiți comanda DSPOBJAUT pentru dispozitive, în scopul de a afla dacă profilul QSECOFR are autorizare *CHANGE.

Valorile de sistem

Valorile de sistem pentru securitate urmează liniile generale recomandate. Pentru a tipări valorile de sistem pentru securitate, introduceți: 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 funcția de auditare este activă, o intrare SV este scrisă în jurnalul QAUDJRN, ori de câte ori este modificată o variabilă de sistem.

| Folosind comand Display Security Attributes (DSPSECA) pentru a verifica valorile curente și în așteptare ale
| nivelul de securitate (QSECURITY) și nivelul parolă (QPWDLVL), și setările curente ale sistemului înrudit de
| securitate (dacă valorile pot fi modificate)

Deciziile asupra variabilelor de sistem sunt revăzute periodic, mai ales când mediul de sistem se modifică, cum ar fi instalarea unei aplicații noi sau unei rețele de comunicație.

Profilurile de utilizator furnizate de IBM

Parola s-a modificat pentru profilul de utilizator QSECOFR. Acest profil este livrat cu parola setată pe QSECOFR, astfel încât dumneavoastră vă puteți loga pentru a instala sistemul dumneavoastră. Parola **trebuie** să fie modificată prima dată când vă logați pe sistemul dumneavoastră și, periodic, după instalare.

Verificați dacă a fost modificată controlând într-o listă DSPAUTUSR data la care parola QSECOFR a fost modificată și încercând să vă logați cu o parolă implicită diferită.

Notă: Vedeți “Profilurile de utilizator furnizate de IBM” la pagina 108 și Anexa B pentru informații suplimentare despre profiluri utilizator furnizate de IBM.

Parolele IBM pentru DST sunt modificate. ID-urile utilizator pentru unelte service nu apar într-o listă DSPAUTUSR. Pentru a verifica dacă ID-urile și parolele utilizator sunt modificate, porniți DST și încercați să folosiți valorile implicite. Vedeți subiectul “Gestionarea ID-urilor Unelte Utilizator” la pagina 109 pentru informații suplimentare.

| Cu excepția QSECOFR, nu semnați cu profilurile de utilizator livrate de IBM. Aceste profiluri furnizate de IBM
| sunt proiectate pentru a deține obiecte sau a rula funcții de sistem. Folosiți o listă DSPAUTUSR pentru a verifica
| dacă următoarele profiluri utilizator furnizate de IBM listate în Anexa B, “Profilurile de utilizator furnizate de
| IBM”, la pagina 279, cu excepția QSECOFR, au o parolă *NONE.

Controlul parolei

Utilizatorii pot schimba propriile parole. Permișiunea 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 funcția Modificare parolă din meniul Securitate (GO SECURITY - PORNIRE SECURITATE).

Este necesară modificare a parolei conform regulilor de securitate ale organizației, de exemplu la un interval între 30 și 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. Revedeți 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 și prin folosirea unui program de aprobare a parolelor. Folosiți comanda WRKSYSVAL *SEC și uitați-vă la setările pentru valori începând cu QPWD.

Profilurile de grup au parola *NONE. Utilizați comanda DSPAUTUSR pentru a verifica dacă există profiluri de grup care au parole.

Oricând sistemul nu operează la nivel de parolare 3 și utilizatorii își modifică parola lor, sistemul va încerca să creeze o parolă echivalentă care este utilizabilă la alte niveluri de parolare, dacă este posibil. Puteți 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 o parolă BbAaA3x este specificată la nivelul 2 de parolare, sistemul va crea o parolă echivalentă BBAAA3X pentru utilizare la nivelurile 0 și 1 de parolare. Aceasta ar fi adevărată chiar dacă variabila de sistem QPWDLMTCHR îl include pe 'A' ca pe unul din caracterele limitate (QPWDLMTCHR nu este impus la nivelul 2 de parolare) sau variabila de sistem QPWDLMTREP a specificat că nu pot fi caracterele consecutive la fel (deoarece verificarea este sensibilă la majuscule, la nivelul 2 de parolare dar insensibilă la majusculă la nivelurile 0 și 1 de parolare.)

Profilurile de utilizator și de grup

Fiecărui utilizator îi este alocat un profil de utilizator unic. Variabila de sistem QPMTDEVSSN trebuie setată la 1. Chiar dacă limitarea fiecărui utilizator la o sesiune dispozitiv la un moment dat nu previne partajarea profilurilor de utilizator, descurajează acest fapt.

Profilurile de utilizator cu autorizarea specială *ALLOBJ sunt limitate și nu sunt utilizate ca profiluri de grup. Comanda DSPUSRPRF poate fi utilizată pentru a verifica autorizările speciale pentru profilurile de utilizator și pentru a determina care profiluri sunt profiluri de grup. Subiectul "Tipărirea profilurilor de utilizator selectate" la pagina 267 arată cum se folosește un fișier de ieșire și o interogare pentru a determina aceasta.

Câmpul *Capabilități limită* este *YES în profilurile de utilizator, care ar trebui să fie restricționate la un set de meniuri. Subiectul "Tipărirea profilurilor de utilizator selectate" la pagina 267 oferă un exemplu despre modul în care se determină aceasta.

Programatorii sunt restricționați de bibliotecile de producție. Folosiți comanda DSPOBJAUT pentru a determina autorizările publice și private pentru bibliotecile de producție și obiectele critice din bibliotecă.

"Planificarea securității pentru programatori" la pagina 215 are mai multe informații despre securitate și mediul de programare.

Apartenența la un profil de grup este modificată când responsabilitățile de job se modifică. Pentru a verifica apartenența la grup, utilizați una din aceste comenzi:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF nume-profil *GRPMBR
```

Dumneavoastră trebuie să utilizați o convenție de denumire pentru un profil de grup. Când sunt afișate autorizările, puteți recunoaște atunci cu ușurință profilul de grup.

Administrarea profilurilor de utilizatori este organizată adecvat. Nici un profil de utilizator nu are numere mari ca autorizare privată. Subiectul “Examinarea profilurilor mari de utilizatori” la pagina 268 discută modul în care se găsește și se examinează profilurile mari de utilizatori de pe sistemul dumneavoastră.

Angajații sunt înlăturați din sistem imediat când sunt transferați sau eliberați. Revedeți în mod regulat lista DSPAUTUSR pentru a vă asigura de faptul că numai angajații activi au acces la sistem. Intrările DO (Delete Object - Ștergere obiect) din jurnalul de auditare pot fi revăzute pentru a vă asigura că profilurile de utilizator sunt șterse imediat după ce pleacă utilizatorii.

Gestionarea verifică în mod regulat utilizatorii autorizați pe sistem. Dumneavoastră puteți folosi comanda DSPAUTUSR pentru această informație.

Parola pentru un angajat inactiv este setată la *NONE. Utilizați 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 și autorizări speciale *AUDIT. Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 267 oferă un exemplu despre modul în care se determină aceasta.

Controlul autorizării

Proprietarii datelor înțeleg obligația lor de autorizare a utilizatorilor pe principiul nevoii-de-cunoaștere.

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 deținute de un profil 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 neautorizați să lanseze joburi care rulează folosind autorizarea altui profil.

Pentru a afla ce descrieri de job sunt pe sistem, introduceți:

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

Pentru a verifica parametrul *Utilizator* al descrierii de job, folosiți comanda DSPJOB (Display Job Description - Afășare descriere de job) Pentru a verifica autorizarea pentru o descriere de job, folosiți comanda DSPOBJAUT.

Notă: La nivelul de securitate 40 sau 50, un utilizator ce trimite un job folosind o descriere de job care specifică un nume de profil utilizator, trebuie să aibă autorizarea *USE atât pentru descrierea de job, cât și 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 intrare AF cu tipul de violare J din jurnalul de auditare.

Utilizatorilor nu li se permite să se logeze prin apăsarea tastei Introdere de pe ecranul Logare. Asigurați-vă că nici o intrare de stație de lucru din descrierile de subsistem nu specifică o descriere de job care are un nume de profil utilizator specificat pentru parametrul USER.

Logarea implicită este prevenită la nivelul 40 sau 50 de securitate, chiar dacă o descriere de subsistem o permite. La toate nivelurile de securitate, o intrare AF cu un tip de violare S este scrisă într-un jurnal de audit, dacă logarea implicită se încearcă și este definită o descriere de subsistem pentru a o permite.

Lista de biblioteci din programele aplicație este controlată pentru a preveni o bibliotecă ce conține un program similar de la a fi adăugat înainte de bibliotecile de producție. Subiectul “Listele de biblioteci” la pagina 183 discută metode pentru controlul listei de biblioteci.

Programele care adoptă autorizarea sunt folosite doar când sunt cerute și sunt controlate cu atenție. Vedeți subiectul “Analizarea programelor care adoptă autorizarea” la pagina 268 pentru o explicație a modului în care se evaluează utilizarea funcției de adoptare a programului.

Interfețele program aplicație (API-uri) sunt securizate.

Tehnicile bune de securitate a obiectului sunt folosite pentru a evita problemele de performanță.

Accesul neautorizat

Evenimentele referitoare la securitate sunt înregistrate în jurnalul de auditare a securității (QAUDJRN), când funcția de auditare este activă. Pentru a audita defectele de autorizare, folosiți următoarele variabile de sistem și setări:

- QAUDCTL trebuie să fie setat la *AUDLVL.
- QAUDLVL trebuie să includă valorile *PGMFAIL și *AUTFAIL.

Cea mai bună metodă de detectare a încercărilor neautorizate de a accesa informațiile 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 puțin. Variabila de sistem QMAXSGNACN setată la 2 sau 3.

Cooda mesaj QSYSMSG este creată și monitorizată.

Jurnalul de auditare este auditat pentru încercări repetate ale unui utilizator. (Eșecurile de autorizare determină intrări de tipul AF în jurnalul auditare.)

Programele care încearcă să acceseze obiecte, folosind interfețe care nu sunt suportate, eșuează. (Variabila de sistem QSECURITY este setată la 40 sau 50.)

ID-ul și parola utilizatorului sunt cerute pentru logare. Nivelurile de securitate 40 și 50 impun aceasta. La nivelul 20 sau 30, trebuie să vă asigurați că nici o descriere de subsistem nu are o intrare de stație de lucru care utilizează o descriere de job ce are un nume de profil utilizator.

Programele neautorizate

Variabila de sistem QALWOBJRST este setată la *NONE pentru a împiedica pe oricine de la restaurarea programelor sensibile la securitate în sistem.

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului) rulează periodic pentru a detecta modificări neautorizate în scopul programării obiectelor. Această comandă este descrisă “Verificarea obiectelor ce au fost modificate” la pagina 269

Comunicațiile

Comunicațiile telefonice sunt protejate de proceduri apel-înapoi.

Criptarea este utilizată cu date sensibile.

Logarea de la distanță este controlată. Variabila de sistem QRMTSIGN este setată la *FRCSIGNON sau este folosit un program de validare passthrough.

Datele de acces de la alte sisteme, inclusiv computere personale, sunt controlate folosind atributele de rețea JOBACN, PCSACC și DDMACC. Atributul de rețea JOBACN trebuie să fie *FILE.

Utilizarea jurnalului de auditare a securității

Jurnalul de auditare a securității este sursa primară de auditare a informațiilor despre sistem. Un auditor de securitate din interiorul sau din afara organizației dumneavoastră poate folosi funcția de auditare furnizată de sistem pentru a strânge informații despre evenimente referitoare la securitate, ce apar pe sistem.

Puteți defini auditarea pe sistemul dumneavoastră la trei niveluri diferite.

- Auditare largă a sistemului ce apare pentru toți utilizatorii.
- Auditare ce are loc pentru obiecte specifice.
- Auditare ce are loc pentru utilizatori specifici.

Folosiți variabile de sistem, parametrii profil utilizator și parametrii obiect pentru a defini auditarea. “Planificarea auditării securității” descrie cum se face aceasta

Când un eveniment referitor la securitate, care poate fi auditat, apare, sistemul verifică dacă dumneavoastră ați selectat acel eveniment pentru auditare. Dacă este așa, sistemul scrie o intrare de jurnal în receptorul curent pentru jurnalul de auditare securitate (QAUDJRN din biblioteca QSYS).

Cînd doriți să analizați informațiile de auditare pe care le-ați colectat în jurnalul QAUDJRN, puteți folosi comanda Afișare jurnal (DSPJRN). Cu această comandă, informațiile din jurnalul QAUDJRN pot fi scrise într-un fișier baze de date. Un program aplicație sau o unealtă de interogare pot fi folosite pentru a analiza datele.

Funcția de auditare securitate este opțională. Trebuie să faceți anumiți pași pentru a seta auditarea securității.

Următoarele secțiuni descriu modul în care se planifică, se setează și se gestionează auditarea securității, ce informații sunt înregistrate și cum se vizualizează acele informații. Anexa F arată machetele de înregistrare pentru intrările de jurnal de auditare. Anexa E prezintă operațiile sunt auditate pentru fiecare tip de obiect.

Planificarea auditării securității

Pentru a planifica folosirea auditării securității pe sistemul dumneavoastră:

- Determinați ce evenimente relevante de securitate doriți să înregistrați pentru toți utilizatorii sistemului. Auditarea evenimentelor relevante de securitate se numește *auditare acțiune*
- Verificați dacă aveți nevoie de auditare suplimentară pentru utilizatori particulari.
- Decideți dacă doriți să auditați utilizarea obiectelor specifice pe sistem.
- Determinați dacă auditarea obiectului ar trebui folosită pentru toți utilizatorii sau utilizatorii particulari.

Planificarea auditării acțiunilor

Variabila de sistem QAUDCTL (control audit), variabila de sistem QAUDLVL (nivel audit), variabila de sistem QAUDLVL2 (extensie nivel audit) și parametrul AUDLVL (auditare acțiune) din profilurile utilizator lucrează împreună pentru a controla auditarea acțiunii:

- Variabila de sistem QAUDLVL specifică ce acțiuni sunt auditate pentru toți utilizatorii sistemului.
- Variabila de sistem QAUDLVL2 specifică, de asemenea, ce acțiuni sunt auditate pentru toți utilizatorii sistemului și este folosită când mai mult de 16 valori de auditare sunt necesare.
- Parametrul AUDLVL din profilul utilizator determină ce acțiuni sunt auditate pentru un utilizator specific. Valorile pentru parametrul AUDLVL aplică *in addition to* valorile pentru variabilele de sistem QAUDLVL și QAUDLVL2.
- Variabila de sistem QAUDCTL pornește și oprește auditarea acțiune.

Evenimentele pe care le alegeți pentru înregistrare în istoric depind atât de obiectivele dumneavoastră de securitate, cât și de expunerile potențiale. Tabela 125 la pagina 235 descrie valorile posibile de nivel auditare și cum este posibil să le folosiți. Arată dacă acestea sunt disponibile ca variabilă de sistem, parametru profil utilizator sau ambele.

Tabela 126 la pagina 239 furnizează informații suplimentare despre intrările jurnal care sunt scrise pentru valorile auditare acțiune specificate în variabilele de sistem QAUDLVL și QAUDLVL2 și în profilul utilizator. Arată:

- Tipul intrării scrise pentru jurnalul QAUDJRN.
- Pentru a modela fișier bază de date de ieșire care poate fi folosit pentru a defini înregistrarea când creați un fișier de ieșire cu comanda DSPJRN. Machete complete pentru fișierele externe ale bazei de date model se găsesc în Anexa F.
- Tipul de intrare detaliat. Unele tipuri de intrare jurnal sunt folosite pentru a înregistra în istoric mai mult de un tip de eveniment. Câmpul tip de intrare detaliat din intrarea de jurnal identifică tipul de eveniment.
- ID-ul mesajului care poate fi utilizat pentru a defini informațiile specifice intrării în intrarea de jurnal.

Tabela 125. Valori auditare acțiune

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL și QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*NONE	Da	Da	Dacă variabila de sistem QAUDLVL este *NONE, nici o acțiune nu este înregistrată în istoric pe o bază lărgită a sistemului. Acțiunile sunt înregistrate în istoric pentru utilizatori individuali pe baza valorii AUDLVL din profilurile lor de utilizatori. Dacă valoarea AUDLVL dintr-un profil utilizator este *NONE, nu este realizată nici o auditare suplimentară de acțiune pentru acest utilizator. Orice acțiuni specificate pentru variabila de sistem QAUDLVL sunt înregistrate în sistem pentru acest utilizator.
*ATNEVT	Da	Nu	Evenimente atenționare: Sistemul scrie o intrare de jurnal pentru evenimente care necesită examinare ulterioară. Cu aceste informații, puteți determina semnificația potențială a evenimentului de atenționare asupra sistemului.
*AUTFAIL	Da	Nu	Autorizare eșecuri: Încercările fără succes de logare la sistem și de accesare a obiectelor sunt înregistrate în istoric. *AUTFAIL poate fi folosit în mod regulat pentru monitorizarea utilizatorilor ce încearcă să realizeze funcții neautorizate pe sistem. *AUTFAIL poate fi folosit, de asemenea, pentru a ajuta migrarea spre un nivel de securitate mai înalt și pentru a testa resursa de securitate pentru o nouă aplicație.
*CMD	Nu	Da	Comenzi: Șirurile de comandă pentru înregistrare în istoric, ale sistemului, rulate de un utilizator. Dacă o comandă rulează de la un program CL ce este creat cu LOG(*NO) și ALWRTVSR(*NO), doar numele comandă și numele de bibliotecă sunt înregistrate. *CMD poate fi utilizat pentru a înregistra acțiunile 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	Ștergere de obiecte: Sistemul scrie o intrare de jurnal când este șters un obiect.
*JOBDTA	Da	Da	Operații ale jobului: Acțiunile care afectează un job sunt înregistrate în istoric, precum pornirea și oprirea jobului, păstrarea, eliberarea, anularea sau modificarea lui. *JOBDTA poate fi folosit pentru a monitoriza cine rulează joburile batch.
*NETBAS	Da	Nu	Funcții de bază rețea: Acțiuni reguli IP, conexiuni socket-uri, filtru de căutare director APPN, filtru punct final APPN.

Tabela 125. Valori auditare acțiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL și QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*NETCLU	Da	Nu	<p>Operații cluster sau grup de resurse : Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • Un nod cluster sau un grup de resurse cluster este adăugat, creat sau șters. • Un nod cluster sau un grup de resurse cluster este pornit, oprit, actualizat sau înlăturat. • Eșecul automat al unui sistem care comută accesul la alt sistem. • Accesul este comutat manual de la un sistem la alt sistem, într-un cluster.
*NETCMN	Da	Nu	<p>Auditare comunicații rețea: Violările detectate de suportul pentru filtrare APPN sunt înregistrate în jurnalul de auditare a securității când sunt auditate Filtrul de căutare director și Filtrul de punct final.</p> <p>*NETCMN este compus din câteva valori pentru a vă permite să personalizați mai bine auditarea dumneavoastră. Următoarele valori compun *NETCMN:</p> <p>*NETBAS *NETCLU *NETFAIL *NETSCK</p>
*NETFAIL	Da	Nu	<p>Eșecuri de rețea : Este scrisă o intrare de jurnal de auditare când încercați să vă conectați la un port TCP/IP care nu există sau când încercați să trimiteți informații unui port TCP/IP care nu este deschis sau disponibil.</p>
*NETSCK	Da	Nu	<p>Operații socket-uri: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • Este acceptată o conexiune de intrare socket TCP/IP. • Este stabilită o conexiune de ieșire 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. • Pașta este filtrată sau refuzată.
*OBJMGT	Da	Da	<p>Operații 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 informațiilor confidențiale prin mutarea obiectului într-o bibliotecă diferită.</p>
*OPTICAL	Da	Da	<p>Funcții optice: Toate funcțiile optice sunt auditate, inclusiv funcțiile referitoare la fișierele optice, directoarele optice, volumele optice și cartușele optice. *OPTICAL poate fi utilizat pentru a detecta încercările de creare sau ștergere a unui director optic.</p>

Tabela 125. Valori auditare acțiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem		Descriere
	QAUDLVL și QAUDLVL2	Disponibil la comanda CHGUSRAUD	
*PGMADP	Da	Da	Autorizare adoptată: Sistemul scrie o intrare de jurnal când este folosită o autorizare adoptată pentru a câștiga accesul la un obiect. *PGMADP poate fi utilizat pentru a testa modul în care o aplicație nouă folosește o autorizare adoptată.
*PGMFAIL	Da	Nu	Eșecuri 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 și pentru a testa o nouă aplicație.
*PRTDTA	Da	Nu	Funcții de tipărire: Tipărirea unui fișier spool, tipărirea direct dintr-un program sau trimiterea unui fișier spool unei imprimante la distanță sunt înregistrate în istoric. *PRTDTA poate fi folosit pentru a detecta tipărirea informației confidențiale.
*SAVRST	Da	Da	Operații restaurare : *SAVRST poate fi folosit pentru a detecta încercările de restaurare a obiectelor neautorizate.
*SECCFG	Da	Nu	Configurare a securității: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: <ul style="list-style-type: none"> • Sunt create, modificate, șterse sau restaurate profiluri utilizator. • Se aduc modificări programelor, variabilelor de sistem, rutării de subsistem sau atributelor de auditare ale unui obiect. • Parola QSECOFR este resetată la valoarea livrată. • Parola responsabilului cu securitatea uneltelor de service este implicită.
*SECDIRSRV	Da	Nu	Funcții Directory Services: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: <ul style="list-style-type: none"> • Modificări sau actualizări se fac auditării, autorizării, parolelor și dreptului de proprietate. • Legări și dezlegări de succes. • Au fost făcute modificări asupra politicilor de securitate (de exemplu, politica de parolă)
*SECIPC	Da	Nu	Comunicații interproces: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: <ul style="list-style-type: none"> • Se fac modificări dreptului de proprietate sau autorizării unui obiect IPC. • O creare, ștergere sau obținere a unui obiect IPC. • Atașare de memorie partajată.

Tabela 125. Valori auditare acțiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL și QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*SECNAS	Da	Nu	<p>Acțiuni de service autentificare în rețea: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • Tichet de serviciu invalid. • Principalii serviciului nu se potrivesc. • Principalii clientului nu se potrivesc. • Nepotrivire adresă IP tichet. • Decriptarea tichetului a eșuat. • Decriptarea autorizării a eșuat. • Regiunea nu este în cadrul clientului și regiunilor locale. • Tichetul este o încercare de răspuns. • Tichetul nu este încă valid. • Nepotrivire adresă IP locală sau la distanță. • 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 secvenței. • Pentru acceptare GSS: acreditări expirate, eroare sumă de control sau legături de canal. • Pentru desfășurare GSS sau verificare GSS: context expirat, decriptare/ decodificare, eroare sumă de control sau eroare de secvență.
*SECRUN	Da	Nu	<p>Funcții de securitate la rulare: Modificările privind dreptul de proprietate, autorizarea și grupul primar al obiectului sunt scrise în jurnalul de auditare.</p>
*SECCKD	Da	Nu	<p>Descriptori socket: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • Un descriptor socket este acordat altui job. • Un descriptor socket este primit. • Un descriptor socket este inutilizabil.
*SECVFY	Da	Nu	<p>Funcții de verificare: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • Este generat un mâner de profil sau un jeton. • Toate jetoanele profil au fost invalidate. • Numărul maxim de jetoane profil a fost generat. • Toate jetoanele profil pentru un utilizator au fost înlăturate. • Un profil utilizator a fost autentificat. • Un profil destinație a fost modificat în timpul unei sesiuni passthrough.

Tabela 125. Valori auditare acțiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem		Descriere
	QAUDLVL și QAUDLVL2	Disponibil la comanda CHGUSRAUD	
*SECVLDL	Da	Nu	<p>Operații de validare a listei: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente:</p> <ul style="list-style-type: none"> • O adăugare, înlăturare sau găsim a intrării de listă de validare. • Verificare cu succes sau fără succes a intrării listei de validare.
*SECURITY	Da	Da	<p>Operații 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 activităților de securitate.</p> <p>*SECURITY este compus din câteva valori pentru a vă permite să personalizați mai bine auditarea dumneavoastră. Următoarele valori compun *SECURITY:</p> <p>*SECCFG *SEC DIRSRV *SECIPC *SECNAS *SECRUN *SEC SCKD *SECVFY *SECVLDL</p>
*SERVICE	Da	Da	<p>Operații de service: utilizarea uneltelor de service, precum DMPOBJ (Dump Object - Obiect dump) și 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.</p>
*SPLFDTA	Da	Da	<p>Operații în fișiere spool: Acțiunile realizate într-un fișier spool sunt înregistrate, inclusiv crearea, copierea și trimiterea. *SPLFDTA poate fi utilizat pentru a detecta încercările de tipărire sau trimitere a datelor confidențiale.</p>
*SYSMGT	Da	Da	<p>Operații de gestionare sisteme: Sistemul scrie o intrare de jurnal pentru activitățile 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 funcțiilor de gestionare a sistemelor pentru a trece peste controalele de securitate.</p>

Tabela 126. Intrări jurnal auditare securitate

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
Auditare acțiune:				

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
*ATNEVT	IM	QASYIMJ5	P	O intruziune potențială a fost detectată. Evaluări ulterioare sunt necesare pentru a determina dacă este vorba de o intruziune reală sau o acțiune așteptată și permisă.
*AUTFAIL ¹	AF	QASYAFJE/J4/J5	A	Încercare făcută pentru a accesa un obiect pentru a realiza o operație pentru care utilizatorul nu a fost autorizat.
			K	Încercarea făcută pentru a realiza o operație pentru care utilizatorul nu avea autorizarea specială necesară.
	X1	QASYX1J5	S	Încercare de semnătură implicită
			F	Delegare jeton identitate eșuată.
			U	Obținerea utilizatorului din jetonul identitate a eșuat.
			F	Eroare autorizare ICAPI.
			G	Eroare autentificare ICAPI.
			H	Final de scanare acțiune program.
			J	Încercare făcută pentru a lansa sau programa un job sub o descriere de job care are un profil utilizator specificat. Lansatorul nu are autorizarea la profilul utilizator.
			N	Jetonul profil nu este un jeton profil regenerabil.
			P	Încercare făcută pentru a folosi un mâner profil care nu este valid pe API QWTSETP.
			S	Încercare făcută pentru logare fără introducerea unei parole sau a unui ID utilizator.
			T	Neautorizat pentru port TCP/IP.
			U	O cerere de permisiune utilizator nu a fost validă.
			V	Jetonul profil nu este valid pentru generarea unui jeton profil nou.
			W	Jetonul profil nu este valid pentru swap.
			Y	Neautorizat pentru câmpul curent JUID în timpul unei operații de ștergere JUID.
			Z	Neautorizat pentru câmpul curent JUID în timpul unei operații de setare JUID.
	CV	QASYCVJ4/J5	E	Conexiune finalizată anormal.
	DI	QASYDIJ4/J5	AF	Eșuare autorizare.
			PW	Eșuare parolă.
			R	Conexiune refuzată.
	GR	QASYGRJ4/J5	F	Operații de înregistrare a funcției.
	KF	QASYKFJ4/J5	P	A fost introdusă o parolă incorectă.
	IP	QASYIPJE/J4/J5	F	Eșuare autorizare pentru o cerere IPC.
	PW	QASYPWJE/J4/J5	A	Eșuare legătură APPC.
			C	Eșuare CHKPWD.
			D	A fost introdus un nume utilizator DSTincorect.
			E	A fost introdus un nume utilizator DSTincorect.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere	
			P	A fost introdusă o parolă incorectă.	
			Q	Încercarea de autentificare utilizator a eșuat deoarece este dezactivat profilul utilizator.	
			R	Încercarea de autentificare utilizator a eșuat deoarece parola a expirat.	
			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.	
			U	Verificare fără succes a unei intrări a listei de validare.	
			R	O conexiune a fost refuzată din cauza parolei incorecte.	
	VO	QASYVOJ4/J5	R	O logare de rețea a fost refuzată din cauza contului expirat, a orelor incorecte, a id-ului utilizator incorect sau a parolei incorecte.	
	VC	QASYVCJE/J4/J5	P	A fost folosită parolă incorectă de rețea.	
	VN	QASYVNJE/J4/J5	C	Rula o comandă.	
	*CMD ²	VP CD	QASYVPJE/J4/J5 QASYCDJE/J4/J5	L	Rula o declarație 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 declarație de control utilitar S/36E.
				N	Creare de obiect nou, cu excepția creării obiectelor din biblioteca QTTEMP.
	*CREATE ³	CO	QASYCOJE/J4/J5	R	Înlocuirea obiectului existent.
CO				Obiect creat.	
A				Obiect șters.	
C				Comitere ștergere în așteptare.	
D				Creare în așteptare dată înapoi.	
P				Ștergere în așteptare.	
*DELETE ³	DI DO	QASYDIJ4/J5 QASYDOJE/J4/J5	R	Ștergere în așteptare dată înapoi.	
			DO	Obiect șters.	
			A	Comanda ENDJOBABN a fost folosită.	
			B	A fost trimis un job.	
			C	A fost modificat un job.	
			E	A fost oprit un job.	
*JOBDA	DI JS	QASYDIJ4/J5 QASYJSJE/J4/J5	H	A fost reținut un job.	
			I	A fost deconectat un job.	
			M	Modificare profil sau profil de grup.	
			N	Comanda ENDJOB a fost folosită.	
			P	A fost atașată o cerere de pornire a programului la jobul prestart.	

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
*NETBAS	SG	QASYSGJE/J4/J5	Q	Atributele interogării au fost modificate.
			R	A fost eliberat un job reținut.
			S	A pornit un job.
			T	Modificare profil sau profil de grup folosind un jeton de profil.
			U	Comanda CHGUSRTRC
			A	Proces de semnalizare asincron i5/OS.
	VC	QASYVCJE/J4/J5	P	Procesare de semnal asincron mediu de spațiu adresă privată (Private Address Space Environment -(PASE).
			S	A fost pornită o conexiune.
	VN	QASYVNJE/J4/J5	E	O conexiune a fost terminată.
			F	Cerere de delogare.
	VS	QASYVSJE/J4/J5	O	Cerere de logare.
			S	A pornit o sesiune de server.
	CV	QASYCVJE/J4/J5	E	A fost terminată o sesiune de server.
			C	Conexiune stabilită.
			E	Conexiune finalizată normal
			R	Conexiune refuzată.
			L	Au fost încărcate reguli IP de pe un fișier.
			N	Reguli IP au fost descărcate pentru o conexiune securitate IP.
IS	QASYISJ4/J5	P	Reguli IP au fost încărcate pentru o conexiune securitate IP.	
		R	Regulile IP au fost citite și copiate într-un fișier.	
		U	Au fost descărcate (înlăturate) reguli.	
		1	Negociere faza 1.	
		2	Negociere faza 2.	
		A	A fost detectată o violare la suportul de APPN Filter când a fost auditat filtrul de căutare director.	
ND	QASYNDJE/J4/J5	A	A fost detectată o violare la suportul APPN Filter când a fost auditat filtrul punct de oprire.	
		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 operația control cluster.
			R	Creare a unui obiect de către operația de gestiune Grup resursă cluster (*GRP).
*NETCMN	CU	QASYCUJE/J4/J5	M	Creare a unui obiect de către operația control cluster.
			R	Creare a unui obiect de către operația de gestiune Grup resursă cluster (*GRP).
	CV	QASYCVJ4/J5	C	Conexiune stabilită.
			E	Conexiune finalizată normal
	IR	QASYIRJ4/J5	L	Au fost încărcate reguli IP de pe un fișier.
			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 și copiate într-un fișier.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
			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	Poștă filtrată
			P	Port nedisponibil
			R	Refuzare poștă
			U	Adresă DHCP refuzată
*NETFAIL	SK	QASYSKJ4/J5	P	Port nedisponibil
*NETSCK	SK	QASYSKJ4/J5	A	Acceptare
			C	Conectare
			D	Adresă DHCP alocată
			F	Poștă filtrată
			R	Refuzare poștă
			U	Adresă DHCP refuzată
*OBJMGT ³	DI	QASYDIJ4/J5	OM	Redenumire obiect
	OM	QASYOMJE/J4/J5	M	A fost mutat un obiect la o altă bibliotecă.
			R	Un obiect a fost redenumit.
*OFCSRV	ML	QASYMLJE/J4/J5	O	A fost deschis un istoric de poștă.
	SD	QASYSDJE/J4/J5	S	A fost făcută o modificare directorului de distribuție sistem.
*OPTICAL	O1	QASYO1JE/J4/J5	R	Deschidere fișier sau director
			U	Modificare sau extragere atribute
			D	Ștergere director fișier
			C	Creare director
			X	Eliberare de fișier optic reținut
	O2	QASYO2JE/J4/J5	C	Copiere fișier sau director
			R	Redenumire fișier
			B	Copie de rezervă fișier sau director
			S	Salvare de fișier optic reținut
			M	Mutare fișier
	O3	QASYO3JE/J4/J5	I	Inițializare volum
			B	Volum copie de rezervă
			N	Redenumire volum
			C	Conversiune a volumului de rezervă la cel primar
			M	Importare
			E	Exportare
			L	Modificare listă de autorizare
			A	Modificare atribute ale volumului
			R	Citare absolută

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
*PGMADP	AP	QASYAPJE/J4/J5	S	A pornit un program care adoptă autorizarea proprietarului. Intrarea de pornire este scrisă prima dată când autorizarea adoptată este folosită pentru a câștiga accesul la un obiect, nu atunci când programul intră în stiva programului.
			E	A fost oprit un program care adoptă autorizarea proprietarului. Intrarea este scrisă când programul părăsește stiva de programe. Dacă același program apare de mai multe ori în stiva de programe, intrarea de oprire este scrisă atunci când cea mai înaltă (ultima) apariție a programului părăsește stiva.
			A	Autorizarea adoptată a fost folosită în timpul activării programului.
*PGMFAIL ¹	AF	QASYAFJE/J4/J5	B	Un program rula o instrucțiune restricționată de interfață de mașină.
			C	Un program care a eșuat verificările de validarea a programului de restaurare timp a fost restaurat. Informații despre eșec sunt în câmpul <i>Tip de violare valoare de validare</i> al înregistrării.
			D	Un program accesează un obiect printr-o interfață nesuportată sau programul apelabil nu este listat ca API apelabil.
			E	Violare protecție hardware spațiu de stocare.
			R	Încercare făcută să actualizeze un obiect care este definit numai citire. (Protecția hardware îmbunătățită a spațiului de stocare este înregistrată în istoric numai la nivelul de securitate 40 sau mai înalt)
*PRTDTA ¹	PO	QASYPOJE/J4/J5	D	Ieșirea imprimantei a fost tipărită direct la imprimantă.
			R	Ieșire trimisă sistemului de la distanță pentru tipărire.
			S	Ieșirea imprimantei a fost spool sau tipărită.
*SAVRST ³	OR	QASYORJE/J4/J5	N	Un obiect nou a fost restaurat pentru sistem.
			E	Un obiect a fost restaurat și înlocuiește un obiect existent.
	RA	QASYRAJE/J4/J5	A	Sistemul a modificat autorizarea unui obiect ce era restaurat. ⁴
	RJ	QASYRJJE/J4/J5	A	O descriere de job ce conține un nume de profil utilizator a fost restaurată.
	RO	QASYROJE/J4/J5	A	Proprietarul obiectului a fost modificat la QDFTOWN în timpul operației de restaurare.
	RP	QASYRPJE/J4/J5	A	A fost restaurat un program care adoptă autorizarea proprietarului.
	RQ	QASYRQJE/J4/J5	A	Un obiect *CRQD cu PROFILE(*OWNER) a fost restaurat.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
	RU	QASYRUJE/J4/J5	A	Autorizarea a fost restaurată pentru un profil utilizator folosind comanda RSTAUT.
	RZ	QASYRZJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat în timpul operației de restaurare.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
*SECCFG	AD	QASYADJE/J4/J5	D	Auditarea unui DLO a fost modificată cu comanda CHGDLOAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
	AU	QASYAUJ5	E	Modificare de configurație Mapare identitate întreprindere (Enterprise Identity Mapping - EIM)
	CP	QASYCPJE/J4/J5	A	Operația de creare, modificare sau restaurare a unui profil utilizator când API QSYSRESPA este folosit.
	CQ	QASYCQJE/J4/J5	A	Un obiect *CRQD a fost modificată.
	CY	QASYCYJ4/J5	A	Funcție de Control acces
			F	Funcție de Control facilitare
			M	Funcție Cheie master
	DO	QASYDOJE/J4/J5	A	Obiectul nu a fost șters sub controlul comiterii
			C	A fost comisă ștergere în așteptare a obiectului
			D	O creare în așteptare a obiectului a fost rulată înapoi.
			P	Ștergerea obiectului este în curs (ștergerea a fost realizată sub controlul comiterii)
			R	O ștergere 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	Ștergere.
	GR	QASYGRJ4/J5	A	Adăugare ieșire program
			D	Ieșire de program înlăturată.
			F	Operație de înregistrare a funcției.
			R	Ieșire de program înlocuită.
	JD	QASYJDJE/J4/J5	A	Parametrul USER al unei descrieri de job a fost modificat.
	KF	QASYKFJ4/J5	C	Certificare operație.
			K	Operație fișier inel de chei.
			T	Operație rădăcină de încredere.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
	NA	QASYNAJE/J4/J5	A	A fost modificat un atribut de rețea.
	PA	QASYPAJE/J4/J5	A	A fost modificat un program pentru a adopta autorizarea proprietarului.
	SE	QASYSEJE/J4/J5	A	A fost modificată o intrare rutare de subsistem.
	SO	QASYSOJ4/J5	A	Adăugare intrare.
			C	Modificare intrare.
			R	Înlăturare intrare.
	SV	QASYSVJE/J4/J5	A	A fost modificată o variabilă de sistem.
			B	Atributele service au fost modificate.
			C	Modificare la ceasul de sistem.
	VA	QASYVAJE/J4/J5	S	Lista de control al accesului a fost modificată cu succes.
			F	Modificarea listei de control al accesului a eșuat.
			V	Verificare cu succes a unei intrări a listei de validare.
	VU	QASYVUJE/J4/J5	G	A fost modificată o înregistrare de grup.
			M	Informația globală a profilului utilizator a fost modificată.
			U	A fost modificată o înregistrare utilizator.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Modificare auditare.
			BN	Legătură reușită.
			CA	Modificare autorizare
			CP	Modificare parolă
			OW	Modificare drept de proprietate
			PO	Modificare politică
			UB	Dezlegare reușită
*SECIPC	IP	QASYIPJE/J4/J5	A	A fost modificat dreptul de proprietate sau autorizarea unui obiect IPC.
			C	Creare a unui obiect IPC.
			D	Ștergere a unui obiect IPC.
			G	Obținere 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 eșuat.
			6	Decriptare a autentificatorului eșuat.
			7	Regiunea nu este în client și regiunile locale.
			8	Tichetul este o încercare de repunere în funcțiune.
			9	Tichetul nu este încă valid.
			A	Decriptare a erorii sumă de control KRB_AP_PRIV sau KRB_AP_SAFE.
			B	Nepotrivire de adresă IP la distanță
			C	Nepotrivire de adresă IP locală
			D	Eroare amprentă de timp KRB_AP_PRIV or KRB_AP_SAFE
			E	Eroare de repunere în funcțiune KRB_AP_PRIV or KRB_AP_SAFE

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
			F	Eroare de ordine secvențială 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 desfășurare GSS sau verificare GSS
			O	Decriptare/decodificare desfășurare GSS sau verificare GSS
			P	Eroare sumă de control desfășurare GSS sau verificare GSS
			Q	Eroare secvențială desfășurare 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 unui obiect a fost modificată cu comanda CHGOBJAUD.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
	X1	QASYADJE/J4/J5	D	Reușire delegare jeton de identitate
			G	Primire utilizator de la jetonul identitate reușit
	AU	QASYAUJ5	E	Modificare de configurație 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	Operația de creare, modificare sau restaurare a unui profil utilizator când API QSYRESPA este folosit.
	CQ	QASYCQJE/J4/J5	A	Un obiect *CRQD a fost modificată.
	CV	QASYCVJ4/J5	C	Conexiune stabilită.
			E	Conexiune finalizată normal
			R	Conexiune refuzată.
	CY	QASYCYJ4/J5	A	Funcție de Control acces
			F	Funcție de Control facilitate
			M	Funcție Cheie master
	DI	QASYDIJ4/J5	AD	Modificare audit
			BN	Legătură reușită.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
			CA	Modificare autorizare
			CP	Modificare parolă
			OW	Modificare drept de proprietate
			PO	Modificare politică
			UB	Dezlegare reușită
	DO	QASYDOJE/J4/J5	A	Obiectul nu a fost șters sub controlul comiterii
			C	A fost comisă ștergere în așteptare a obiectului
			D	O creare în așteptare a obiectului a fost rulată înapoi.
			P	Ștergerea obiectului este în curs (ștergerea a fost realizată sub controlul comiterii)
			R	O ștergere 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	Ștergere.
	GR	QASYGRJ4/J5	A	Adăugare ieșire program
			D	Ieșire de program înlăturată.
			F	Operație de înregistrare a funcției.
			R	Ieșire 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	Ștergere a unui obiect IPC.
			G	Obținere a unui obiect IPC.
	JD	QASYJDJE/J4/J5	A	Parametrul USER al unei descrieri de job a fost modificat.
	KF	QASYKFJ4/J5	C	Certificare operație.
			K	Operație fișier inel de chei.
			T	Operație rădăcină de încredere.
	NA	QASYNAJE/J4/J5	A	A fost modificat un atribut de rețea.
	OW	QASYOWJE/J4/J5	A	Dreptul de proprietate al obiectului a fost modificat.
	PA	QASYPAJE/J4/J5	A	A fost modificat un program pentru a adopta autorizarea proprietarului.
	PG	QASYPGJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat.
	PS	QASYPSJE/J4/J5	A	Un profil utilizator destinație a fost modificat în timpul unei sesiuni passthrough.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
			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 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.
VA		QASYVAJE/J4/J5	S	Lista de control al accesului a fost modificată cu succes.
			F	Modificarea listei de control al accesului a eșuat.
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	Informația globală a profilului utilizator a fost modificată.
			U	A fost modificată o înregistrare utilizator.
X0		QASYX0J4/J5	1	Tichet service valid.
			2	Principalii serviciului nu se potrivesc.
			3	Principalii clientului nu se potrivesc.
			4	Nepotrivire de adresă IP tichet.
			5	Decriptare a tichetului eșuat.
			6	Decriptare a autentificatorului eșuat.
			7	Regiunea nu este în client și regiunile locale.
			8	Tichetul este o încercare de repunere în funcțiune.
			9	Tichetul nu este încă valid.
			A	Decriptare a erorii sumă de control KRB_AP_PRIV sau KRB_AP_SAFE.
			B	Nepotrivire de adresă IP la distanță
			C	Nepotrivire de adresă IP locală
			D	Eroare amprentă de timp KRB_AP_PRIV or KRB_AP_SAFE
			E	Eroare de repunere în funcțiune KRB_AP_PRIV or KRB_AP_SAFE
			F	Eroare de ordine secvențială KRB_AP_PRIV KRB_AP_SAFE

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
			K	Acceptare GSS - acreditare expirată
			L	Acceptare GSS - eroare sumă de control
			M	Acceptare GSS - legături canal
			N	Context expirat desfășurare GSS sau verificare GSS
			O	Decriptare/decodificare desfășurare GSS sau verificare GSS
			P	Eroare sumă de control desfășurare GSS sau verificare GSS
			Q	Eroare secvențială desfășurare GSS sau verificare GSS
*SECVFY	PS	QASYPSJE/J4/J5	A	Un profil utilizator destinație a fost modificat în timpul unei sesiuni passthrough.
	X1	QASYX1J5	D	Reușire delegare jeton de identitate
			G	Primire utilizator de la jetonul identitate reușit
			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 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 fișier spool a fost citit de altcineva decât proprietarul.
			C	A fost creat un fișier spool.
			D	A fost șters un fișier spool.
			H	A fost reținut un fișier spool.
			I	An fost creat un fișier inline.
			R	A fost eliberat un fișier spool.
			U	A fost modificat un fișier spool.
*SYSMGT	DI	QASYDIJ4/J5	CF	Modificări de configurare
	SM	QASYSMJE/J4/J5	RM	Gestionarea replicărilor
			B	Opțiunile de copiere pentru rezervă au fost modificate foloisindxxxxxxxxxx
			C	Opțiunile de curățare automată au fost modificate foloisindxxxxxxxxxx

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
Auditare obiect: *CHANGE	VL	QASYVLJE/J4/J5	D	O modificare DRDA* a fost făcută.
			F	An fost modificat un fișier HFS.
			N	A fost realizată o operație fișier de rețea.
			O	O listă de copiere de rezervă a fost modificată foloindxxxxxxxxxxxx
			P	O programare pornire/oprire a fost modificată folosind xxxxxxxxxxxx.
			S	Lista de răspunsuri sistem a fost modificată.
			T	Orele de recuperare a căii de acces au fost modificate.
			A	Contul a expirat.
			D	Contul este dezactivat.
			L	Orele de logare au expirat.
	U	Necunoscut sau nedisponibil		
	W	Stație de lucru nevalidă		
	DI	QASYDIJ4/J5	IM	Import director LDAP
	ZC	QASYZCJ4/J5	ZC	Modificare obiect
	AD	QASYADJEJ4/J5	C	Modificări obiect
			U	Modernizare a accesului deschis către un obiect
			D	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
			E	Modificare de configurație Mapare identitate întreprindere (Enterprise Identity Mapping - EIM)
			A	Modificări ale listei de autorizare sau ale autorizării obiectului.
			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		E	Un obiect a fost restaurat și înlocuiește 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 operației de restaurare.	
RZ	QASYRZJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat în timpul operației de restaurare.	
GR	QASYGRJ4/J5	F	Operații de înregistrare a funcției ⁶	

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acțiune sau obiect	Tip de intrare jurnal	Model de fișier ieșire bază de date	Intrare detaliată	Descriere
	LD	QASYLDJE/J4/J5	L U K	Legătură la un director. Dezlegare de la un director. Căutare a unui director.
	VF	QASYVFJE/J4/J5	A N S	Fișierul a fost închis din cauza deconectării administrative. Fișierul a fost închis din cauza deconectării client normal. Fișierul a fost închis din cauza sesiunii deconectării.
	VO	QASYVOJ4/J5	A C F R	Adăugare intrare listă de validare. Modificare intrare listă de validare. Găsire intrare listă de validare. Înlăturare intrare listă de validare.
	VR	QASYVRJE/J4/J5	F S	Resursă de acces eşuată. Resursa de acces a fost reușită.
	YC	QASYYCJE/J4/J5	C	Un obiect bibliotecă document a fost modificat.
	ZC	QASYZCJE/J4/J5	C U	Un obiect a fost modificat. Modernizare a accesului deschis către un obiect.
*ALL ⁵	CD	QASYCDJ4/J5	C	Rulare comandă
	DI	QASYDIJ4/J5	EX ZR	Export director LDAP Citire obiect
	GR	QASYGRJ4/J5	F	Operații de înregistrare a funcției ⁶
	YR	QASYRJE/J4/J5	R	Un obiect bibliotecă document a fost citit.
	ZR	QASYZRJE/J4/J5	R	Un obiect a fost citit.

¹ Această valoare poate fi specificată numai pentru variabila de sistem QAUDLVL. Nu este o valoare pentru parametrul AUDLVL al unui profil utilizator.

² Această valoare poate fi specificată numai pentru parametrul AUDLVL al unui profil utilizator. Nu este o valoare pentru variabila de sistem QAUDLVL,

³ Dacă auditarea de obiect este activă pentru un obiect, este scrisă o înregistrare de auditare pentru o operație de creare, ștergere, gestionare obiect sau restaurare, chiar dacă aceste acțiuni nu sunt incluse în nivelul de auditare.

⁴ Vedeți acest subiect "Restaurarea obiectelor" la pagina 222 pentru informații despre modificările de autorizare care pot apărea când un obiect este restaurat.

⁵ Când este specificat *ALL, intrările pentru *CHANGE și *ALL sunt scrise.

⁶ Când obiectul QUSRSYS/QUSEXRGOBJ *EXITRG este auditat.

Planificarea auditării accesului la obiect

Sistemul furnizează abilitatea de a înregistra accesul la un obiect din jurnalul de auditare a securității. Aceasta se numește *auditare obiect*. Variabila de sistem QAUDCTL, valoarea OBJAUD pentru un obiect și valoarea OBJAUD pentru un profil utilizator lucrează împreună pentru a controla auditarea obiectului. Valoarea OBJAUD pentru obiectul și valoarea OBJAUD pentru utilizatorul care folosește acest obiect determină dacă un acces specific ar trebui să fie înregistrat. Variabila de sistem QAUDCTL pornește și oprește funcția de auditare a obiectului.

Tabela 127 arată cum lucrează împreună valorile OBJAUD pentru obiect și profilul utilizator.

Tabela 127. Cum lucrează împreună un obiect și o auditare utilizator.

Valoare pentru obiect OBJAUD	Valoare pentru utilizator OBJAUD		
	*NONE	*CHANGE	*ALL
*NONE	Nimic	Nimic	Nimic
*USRPRF	Nimic	Modificare	Modificare și utilizare
*CHANGE	Modificare	Modificare	Modificare
*ALL	Modificare și utilizare	Modificare și utilizare	Modificare și utilizare

Puteți folosi auditarea obiectului pentru a reține indicii despre toți utilizatorii ce accesează un obiect critic pe sistem. Puteți folosi, de asemenea, auditarea obiectului pentru a reține indicii despre toate accesările obiect ale unui utilizator particular. Auditarea obiectului este o unealtă flexibilă ce vă permite să monitorizați acele accesări obiecte care sunt importante pentru organizația dumneavoastră.

Folosirea capacităților de auditare a obiectelor necesită o planificare atentă. O auditare neglijent proiectată poate genera mult mai multe înregistrări de auditare decât puteți analiza și poate afecta semnificativ performanța sistemului. De exemplu, setarea unei valori OBJAUD la *ALL pentru o bibliotecă generează o intrare de auditare ce este scrisă de fiecare dată sistemul caută un obiect în acea bibliotecă. Pentru o bibliotecă utilizată des într-un sistem aglomerat, aceasta ar genera un foarte mare număr de intrări de jurnal de auditare.

Ceea ce urmează sunt câteva exemple asupra modului în care se folosește auditarea obiectului.

- Dacă anumite fișiere critice sunt folosite în organizația dumneavoastră, puteți revedea periodic cine le accesează, folosind o tehnică exemplu:
 1. Setări valoarea OBJAUD pentru fiecare fișier 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. Setări valoarea OBJAUD pentru fiecare utilizator în exemplul dumneavoastră la *CHANGE sau *ALL, folosind comanda CHGUSRAUD.
 3. Asigurați-vă că variabila de sistem QAUDCTL include *OBJAUD.
 4. După ce a trecut timp suficient pentru colectarea unui exemplu reprezentativ, setări valoarea OBJAUD din profilul utilizator la *NONE sau înlăturați *OBJAUD de la variabila de sistem QAUDCTL.
 5. Analizați intrările de jurnal de auditare folosind tehnicile descrise în “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 262
- Dacă sunteți interesat de cine folosește un fișier particular, puteți colecta informații despre toate accesările la acel fișier pentru o perioadă de timp:
 1. Setare auditare obiect pentru fișier, independent de valorile profilului utilizator:


```
CHGOBJAUD OBJECT(nume-biblioteca/nume-fișier)
OBJTYPE(*FILE) OBJAUD(*CHANGE sau *ALL)
```
 2. Asigurați-vă că variabila de sistem QAUDCTL include *OBJAUD.

3. După ce a trecut timp suficient pentru colectarea unui exemplu reprezentativ, setați valoarea OBJAUD în obiect la *NONE.
 4. Analizați intrările de jurnal de auditare folosind tehnicile descrise în “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 262
- Pentru a audita toate accesările obiect pentru un utilizator specific, faceți următoarele:
 1. Setați 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
```

Atenție: În funcție 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 și va degrada mult performanța. Selectarea unui subset de tipuri obiect și biblioteci pentru auditare este recomandată.

2. Setați valoarea OBJAUD pentru profilul utilizator specific la *CHANGE sau *ALL folosind comanda CHGUSRAUD.
3. Asigurați-vă că variabila de sistem QAUDCTL include *OBJAUD.
4. După ce ați colectat un exemplu particular, setați valoarea OBJAUD pentru profilul utilizator la *NONE.

Afișarea auditării obiectului: Folosiți comanda DSPOBJD pentru a afișa nivelul curent de auditare obiect pentru un obiect. Folosiți comanda DSPDLOAUD pentru a afișa nivelul curent de auditare obiect pentru un obiect bibliotecă document.

Setarea auditării implicite pentru obiecte: Puteți folosi variabila de sistem QCRTOBJAUD și valoarea CRTOBJAUD pentru biblioteci și directoare în scopul setării auditării obiectului pentru obiecte noi care sunt create. De exemplu, dacă doriți toate obiectele noi din biblioteca INVLIB pentru a avea valoarea de auditare *USRPRF, folosiți 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.

Folosiți valorile implicite de auditare cu atenție. Folosirea necorespunzătoare poate avea drept urmare multe intrări nedorite în jurnalul de auditare a securității. Folosirea efectivă a capacităților auditării obiectului ale sistemului cere o planificare atentă.

Împiedicarea pierderii informațiilor de auditare

Cele două variabile de sistem controlează ceea ce face sistemul când condițiile de eroare pot determina pierderea intrărilor de jurnal de auditare.

Nivelul de forțare a auditării: Variabila de sistem QAUDFRCLVL determină cât de des scrie sistemul intrări de jurnal de auditare din memorie în spațiul auxiliar de stocare. Variabila de sistem QAUDFRCLVL lucrează precum nivelul de forțare pentru fișierele bazei de date. Trebuie să urmați indicații similare pentru determinarea nivelului corect de forțare în cazul instalării dumneavoastră.

Dacă permiteți sistemului să determine când să scrie intrările pe spațiul auxiliar de stocare, el echilibrează impactul asupra performanței cu posibilitatea pierderii informațiilor la întreruperea alimentării. Alegerea implicită și recomandată este *SYS.

Dacă setați nivelul de forțare la un număr mic, minimizați posibilitatea pierderii înregistrărilor de audit, dar puteți sesiza o înrăutățire a performanței. Dacă instalarea dumneavoastră cere ca nici o înregistrare de auditare să nu fie pierdută la căderea alimentării, trebuie să setați QAUDFRCLVL la 1.

Acțiunea la oprirea auditării: Variabila de sistem QAUDENDACN determină ce face sistemul dacă nu poate scrie o intrare în jurnalul de auditare. Valoarea implicită este *NOTIFY. Sistemul realizează ceea ce urmează, dacă nu poate să scrie intrările de jurnal de auditare și 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 și 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 și QSYSMSG în timpul IPL-ului.

Notă: În majoritatea cazurilor, realizarea unui IPL rezolvă problema care a cauzat eșuarea auditării. După ce ați repornit sistemul, setați variabila de sistem QAUDCTL la valoarea corectă. Sistemul încearcă să scrie o înregistrare jurnal audit, oricând această variabilă de sistem se schimbă.

Puteți seta QAUDENDACN să oprească sistemul dacă eșuează auditarea (*PWRDWNSYS). Folosiți 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 și variabila de sistem QAUDENDACN este *PWRDWNSYS, se produc următoarele:

1. Sistemul se oprește imediat (echivalentul emiterii comenzii PWRDWNSYS *IMMED).
2. SRC cod B900 3D10 este afișat.

Mai departe, trebuie să faceți următoarele:

1. Porniți un IPL de la sistemul unitate. Asigurați-vă că este alimentat dispozitivul specificat în variabila de sistem pentru consolă (QCONSOLE).
2. Pentru a reliza IPL-ul, trebuie să se logeze un utilizator cu autorizarea specială *ALLOBJ și *AUDIT, la consolă.
3. Sistemul pornește într-o stare restricționată cu un mesaj ce indică faptul că eroarea de auditare a cauzat oprirea sistemului.
4. Variabila de sistem QAUDCTL este setată la *NONE.
5. Pentru a restaura sistemul la normal, setați variabila de sistem QAUDCTL la altă valoare decât nici una. Când modificați 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, folosiți un istoric de job pentru a determina de ce a eșuat auditarea. Corecțați problema și încercați să resetați din nou valoarea QAUDCTL.

Alegerea neauditării obiectelor din QTEMP

Valoarea *NOQTEMP poate fi specificată ca valoare pentru variabila de sistem QAUDCTL. Dacă este specificată, trebuie să specificați, de asemenea, atât *OBLAUD cât și *AUDLVL. Când este activă auditarea și este specificat *NOQTEMP, următoarele acțiuni 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 securității

Privire generală:

Folosind comanda CHGSECAUD, puteți activa auditarea sistemului de securitate pentru acțiuni asigurându-vă că jurnalul de securitate există, setând valoarea de sistem QAUDCTL la *AUDLVL și setând valoarea de sistem QAUDLVL la setul implicit de valori. Setul implicit include auditările de acțiune *AUTFAIL, *CREATE, *DELETE, *SECURITY și *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 și *AUDIT.

Intrare jurnal:

```
CO (creare obiect)  
SV (modificare variabilă de sistem)  
AD (modificare auditare obiect și utilizator)
```

Notă: Comanda CHGSECAUD creează jurnalul și receptorul jurnal, dacă acesta nu există. CHGSECAUD setează apoi variabilele de sistem QAUDCTL, QAUDLVL și QAUDLVL2.

Vedeți Tabela 230 la pagina 619 pentru informații suplimentare despre comanda CHGSECAUD.

Setarea auditării securității

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 și pentru jurnal
bibliotecă receptor
autorizare specială *AUDIT

Intrare jurnal:

```
CO (creare obiect)  
SV (modificare variabilă de sistem)  
AD (modificare auditare obiect și utilizator)
```

Notă: QSYS/QAUDJRN trebuie să existe înainte ca QAUDCTL să fie modificat.

Pentru a seta auditarea securității, faceți pașii următori. Setarea auditării cere autorizare specială *AUDIT.

1. Creați un receptor de jurnal într-o bibliotecă, la alegerea dumneavoastră, folosind comanda CRTJRNRCV (Create Journal Receiver - Creare receptor jurnal. Acest exemplu folosește o bibliotecă numită JRNLIB pentru receptori de jurnal.

```
CRTJRNRCV JRNRCV(JRNLIB/AUDRCV0001) +
          THRESHOLD(100000) AUT(*EXCLUDE) +
          TEXT('Auditare receptor jurnal')
```

- Puneți receptorul jurnal într-o bibliotecă salvată în mod regulat. **Nu** plasați receptorul jurnal în biblioteca QSYS, chiar dacă acolo este locul unde va fi jurnalul.
 - Alegeți un nume de receptor jurnal care poate fi folosit pentru a crea o convenție de denumire pentru viitorii receptori jurnale, precum AUDRCV0001. Puteți folosi opțiunea *GEN, când modificați receptorii jurnal pentru a continua convenția de denumire. Folosind acest tip de convenție de numire, este util, de asemenea, dacă alegeți ca sistemul dumneavoastră să gestioneze schimbarea receptorilor dumneavoastră jurnal.
 - Specificați un prag de receptor adecvat mărimii și activității sistemului dumneavoastră. Dimensiunea pe care o alegeți trebuie să se bazeze pe numărul de tranzacții de pe sistemul dumneavoastră și pe numărul de acțiuni pe care dumneavoastră le alegeți spre a le audita. Dacă folosiți suport de gestionare a jurnalului - modificare sistem, pragul receptorilor jurnal trebuie să fie de cel puțin 100 000 KB. Pentru informații suplimentare despre pragul receptorului de jurnal, consultați Gestionarea jurnalului.
 - Specificați *EXCLUDE pe parametrul AUT pentru a limita accesul la informațiile memorate în jurnal.
2. Creați jurnal QSYS/QAUDJRN prin folosirea comenzii CRTJRN (Create Journal - Creare jurnal):

```
CRTJRN JRN(QSYS/QAUDJRN) +
       JRNRCV(JRNLIB/AUDRCV0001) +
       MNGRCV(*SYSTEM) DLTRCV(*NO) +
       AUT(*EXCLUDE) TEXT('Auditare jurnal')
```

- Trebuie folosit numele QSYS/QAUDJRN.
- Specificați numele receptorului jurnal pe care l-ați creat la pasul anterior.
- Specificați *EXCLUDE pe parametrul AUT pentru a limita accesul la informațiile memorate în jurnal. Trebuie să aveți autorizarea de a adăuga obiecte la QSYS pentru a crea jurnalul.
- Folosiți parametrul *Gestionare receptor* (MNGRCV) pentru ca sistemul să schimbe receptorul jurnal și să atașeze unul nou receptorul atașat depășește pragul specificat când a fost creat receptorul jurnal. Dacă alegeți această opțiune, nu trebuie să folosiți comanda CHGJRN pentru a detașa receptorii și pentru a crea și atașa manual receptori noi.
- Nu trebuie ca sistemul să ștergă receptorii detașați. Specificați DLTRCV(*NO), care este implicit. Receptorii QAUDJRN reprezintă coada dumneavoastră de auditare a securității. Asigurați-vă că aceștia sunt salvați adecvat înainte de ștergerea lor din sistem.

Subiectul Gestionare jurnal furnizează mai multe informații despre lucrul cu jurnale și receptorii jurnal.

3. Setați valoarea de sistem pentru nivelul de auditare (QAUDLVL) sau valoarea de sistem pentru extensie nivel de auditare (QAUDLVL2), folosind comanda WRKSYSVAL. Variabilele de sistem QAUDLVL și QAUDLVL2 determină ce acțiuni sunt înregistrate în jurnalul de auditare pentru toți utilizatorii de pe sistem. Vedeți “Planificarea auditării acțiunilor” la pagina 234.
4. Setați acțiunea de auditare pentru utilizatori individuali, dacă este necesar folosind comanda CHGUSRAUD. Vedeți “Planificarea auditării acțiunilor” la pagina 234.
5. Setați auditarea de obiect pentru obiecte specifice, dacă este necesar, folosind comanda CHGOBJAUD și CHGDLOAUD. Vedeți “Planificarea auditării accesului la obiect” la pagina 252.
6. Setați auditarea de obiect pentru utilizatori specifici, dacă este necesar, folosind comanda CHGUSRAUD.
7. Setați valoarea de sistem QAUDENDACN pentru controlul a ceea ce se întâmplă dacă sistemul nu poate accesa jurnalul de auditare. Vedeți “Acțiunea la oprirea auditării” la pagina 255.
8. Setați variabila de sistem QAUDFRCLVL pentru a controla cât de des sunt scrise înregistrările de auditare în spațiul auxiliar de stocare. Vedeți “Împiedicarea pierderii informațiilor de auditare” la pagina 254.
9. Porniți auditarea prin setarea valorii de sistem QAUDCTL la altă valoare decât *NONE.

Jurnalul QSYS/QAUDJRN trebuie să existe înainte ca dumneavoastră să puteți modifica variabila de sistem QAUDCTL la altă valoare decât *NONE. Când porniți auditarea, sistemul încearcă să scrie o înregistrare în jurnalul de auditare. Dacă încercarea nu este reușită, dumneavoastră primiți un mesaj și auditarea nu pornește.

Gestionarea jurnalului de auditare și a receptorilor de jurnal

Jurnalul de auditare, QSYS/QAUDJRN, este destinat numai auditării securității. Obiectele nu trebuie să fie jurnalizate în jurnalul de auditare. Controlul obligațiilor nu trebuie să folosească jurnalul de auditare. Intrările utilizatorului nu trebuie trimise acestui jurnal folosind comanda SNDJRNE (Send Journal Entry - Trimitere intrare jurnal) sau API-ul QJOSJRNE (Send Journal Entry - Trimitere intrare jurnal).

Protecția specială de blocare este folosită pentru a asigura faptul că sistemul poate scrie intrări de auditare în jurnalul de auditare. Când auditarea este activă (variabila de sistem QAUDCTL nu este *NONE), jobul de arbitraj al sistemului (QSYSARB) reține un blocaj în jurnalul QSYS/QAUDJRN. Nu puteți realiza anumite operații în jurnalul de auditare când auditarea este activă, precum:

- comanda DLTJRN
- comenzile ENDJRNxxx (End Journaling - Final jurnalizare)
- comanda APYJRNCHG
- comanda RMVJRNCHG
- comanda DMPOBJ sau DMPSYSOBJ
- Mutare a jurnalului
- Restaurare a jurnalului
- Operații care lucrează cu autorizare, precum comanda GRTOBJAUT
- comanda WRKJRN

Informațiile înregistrate în intrările jurnal securitate sunt descrise în Anexa F. Toate intrările de securitate din jurnalul de auditare au codul de jurnal T. Pe lângă intrările de securitate, în jurnalul QAUDJRN apar de asemenea intrările de sistem. Acestea sunt intrări cu codul de jurnal J, care se referă la IPL (initial program load) și la operații 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 acțiune realizează sistemul. Recuperarea unui jurnal deteriorat sau a unui receptor jurnal este aceeași ca la alte jurnale.

Este posibil să doriți ca sistemul să gestioneze modificarea receptorilor jurnal. Specificați MNGRCV(*SYSTEM) când creați jurnalul QAUDJRN sau modificați jurnalul la acea valoare. Dacă specificați MNGRCV(*SYSTEM), sistemul dezatașează automat receptorul când atinge dimensiunea sa de prag și creează și atașează un nou receptor jurnal. Aceasta se numește *modificare sistem-gestionare jurnal*

Dacă specificați MNGRCV(*USER) pentru QAUDJRN, este trimis un mesaj cozii de mesaje prag specificată pentru jurnal când receptorul jurnal atinge un prag al spațiului de stocare. Mesajul indică faptul că receptorul a atins pragul său. Folosiți comanda CHGJRN pentru a detașa receptorul și a atașa un nou receptor jurnal. Aceasta împiedică condițiile eroare *Intare nejournalizată* Dacă primiți acest mesaj, trebuie să folosiți comanda CHGJRN pentru a continua auditarea securității.

Coadă implicită de mesaje pentru un jurnal este QSYSOPR. Dacă instalarea dumneavoastră are un volum mare de mesaje în coada de mesaje QSYSOPR, este posibil să doriți să asociați o coadă diferită de mesaje, precum AUDMSG, cu jurnalul QAUDJRN. Puteți folosi un program de tratare a mesajelor pentru a monitoriza coada de mesaje AUDMSG. Când este primit un avertisment al pragului jurnal (CPF7099), puteți atașa în mod automat un nou receptor. Dacă folosiți o modificare sistem-gestionare de jurnal, atunci mesajul CPF7020 este trimis cozii de mesaje jurnal când este completat un jurnal modificare sistem. Puteți monitoriza acest mesaj pentru a știți când să executați o salvare a receptorilor jurnal detașați.

Atenție: Funcția de ștergere automată furnizată folosind meniurile Asistent operațional nu șterge receptorii QAUDJRN. Trebuie să detașați în mod regulat, să salvați și să ștergeți receptorii QAUDJRN pentru a evita problemele cu spațiul pe disc.

Vedeți subiectul Gestionarea jurnalului pentru informații complete despre gestionarea jurnalelor și a receptorilor de jurnal.

Notă: Jurnalul QAUDJRN este creat în timpul unui IPL dacă nu există și variabila de sistem QAUDCTL este setată la o altă valoare decât *NONE. Aceasta se petrece doar după o situație neobișnuită, precum înlocuirea unui dispozitiv disc sau ștergerea unui pool de memorie auxiliară.

Salvarea și ștergerea receptorilor de jurnal de auditare

Privire generală:

Scop: Pentru a atașa un receptor nou jurnal audit; pentru a salva și șterge vechiul receptor

Cum se face:

- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- JRNRCV(*GEN) SAVOBJ (pentru a salva vechiul receptor)
- DLTJRNRCV (pentru a șterge 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 detașați în mod regulat receptorul de jurnal de auditare curent și să atașați unul nou pentru două motive:

- Analizarea intrărilor jurnal este mai facilă decât dacă fiecare receptor jurnal conține intrările pentru o perioadă de timp specifică, gestionabilă.
- Receptorii jurnal mari pot afecta performanța sistemului, în plus față de ocuparea unui spațiu folosit de pe spațiul de stocare auxiliar.

Gestionarea receptorilor în mod automat de către sistem este abordarea recomandată. Puteți specifica aceasta folosind parametrul *Gestionare receptor* când creați jurnalul.

Dacă ați setat auditarea acțiune și auditarea obiect pentru a înregistra multe evenimente diferite, este posibil să trebuiască să specificați o valoare mare de prag pentru receptorul jurnal. Dacă gestionați manual receptorii, este posibil să trebuiască să modificați zilnic receptorii jurnal. Dacă înregistrați doar câteva evenimente, este posibil să doriți să modificați receptorii pentru a corespunde programului de rezervă pentru biblioteca în care se află receptorul de jurnal.

Folosiți comanda CHGJRN pentru a detașa un receptor și a atașa un nou receptor jurnal.

Receptorii de jurnale gestionați de sistem: Dacă sistemul dumneavoastră gestionează receptorii, folosiți următoarea procedură pentru a salva toți receptorii detașați QAUDJRN și pentru a-i șterge:

1. Introduceți WRKJRNA QAUDJRN. Ecranul vă arată receptorul curent atașat. Nu salvați sau ștergeți acest receptor.
2. Folosiți F15 pentru a lucra cu directorul receptor. Aceasta arată toți receptorii care au fost asociați cu jurnalul și starea lor.
3. Folosiți comanda SAVOBJ pentru a salva fiecare receptor, cu excepția receptorului atașat în prezent, care nu a fost deja salvat.
4. Folosiți comanda DLTJRNRCV pentru a șterge fiecare receptor după ce este salvat.

Notă: O alternativă la procedura de mai sus ar putea fi realizată folosind coada de mesaje jurnal și monitorizând mesajul CPF7020 ceea ce indică faptul că jurnalul modificare sistem s-a terminat cu succes. Vedeți *Backup and Recovery* pentru informații suplimentare despre acest suport.

Receptorii de jurnale gestionati de utilizator: Dacă alegeți să gestionați manual receptorii jurnal, folosiți următoarea procedură pentru a detașa, salva și șterge un receptor jurnal:

1. Introduceți CHGJRN JRN(QAUDJRN) JRNRCV(*GEN). Această comandă:
 - a. Detașează receptorul atașat în prezent.
 - b. Creează un receptor nou cu numărul secvențial următor.
 - c. Atașează noul receptor la jurnal.De exemplu, dacă receptorul curent este AUDRCV0003, sistemul creează și atașează un nou receptor numit AUDRCV0004.
Comanda Gestionare atribute jurnal (Work with Journal Attributes - WRKJRNA) vă spune care receptor este atașat în prezent: WRKJRNA QAUDJRN.
2. Folosiți comanda Salvare obiect (SAVOBJ) pentru a salva receptorul jurnal detașat. Specificați tipul obiectului *JRNRCV.
3. Folosiți comanda DLTJRNRCV (Delete Journal Receiver - Ștergere receptor jurnal) pentru a șterge receptorul. Dacă încercați să ștergeți receptorul fără a-l salva, primiți un mesaj de avertizare.

Oprirea funcției de auditare

Este posibil să doriți să folosiți funcția de auditare în mod periodic, decât tot timpul. De exemplu, puteți dori să o folosiți când testați o aplicație nouă. Sau e posibil să o folosiți pentru a realiza o auditare de securitate în mod secvențial.

Pentru a opri funcția de auditare, faceți ceea ce urmează:

1. Folosiți comanda WRKSYSVAL pentru a modifica variabila de sistem QAUDCTL la *NONE. Aceasta oprește sistemul de la înregistrarea în continuare a altor evenimente.
2. Detașați receptorul jurnal curent folosind comanda CHGJRN.
3. Salvați și ștergeți receptorul detașat, folosind comenzile SAVOBJ și DLTJRNRCV.
4. Puteți șterge jurnalul QAUDJRN după ce l-ați modificat pe QAUDCTL la *NONE. Dacă plănuieți să continuați auditarea securității, în viitor, este posibil să doriți părăsirea jurnalului QAUDJRN pe sistem. Însă dacă jurnalul QAUDJRN este setat cu MNGRCV(*SYSTEM), sistemul detașează receptorul și atașează unul nou ori de câte ori realizați un IPL, chiar dacă auditarea securității este activă. Trebuie să ștergeți acești receptori jurnal. Salvarea lor înainte de a-i șterge nu trebuie să aibă loc neapărat, deoarece ei nu conțin nici o intrare de auditare.

Analizarea intrărilor din jurnalul de auditare

O dată ce ați setat funcția de auditare securitate, puteți folosi câteva metode diferite pentru a analiza evenimentele care sunt înregistrate:

- Vizualizare a intrărilor setate la stația dumneavoastră de lucru folosind comanda Afișare jurnal (DSPJRN)
- Copierea intrărilor selectate pe fișiere de ieșire folosind comanda CPYAUDJRNE sau comanda DSPJRN și apoi folosind o unealtă interogatoare sau un program pentru a analiza intrările
- Folosirea comenzii Afișare intrări jurnal auditare - Display Audit Journal Entries (DSPAUDJRNE)

Notă: IBM a încetat să furnizeze îmbunătățiri pentru comanda DSPAUDJRNE. Comanda nu suportă toate tipurile de înregistrări de auditare a securității și nu listează toate câmpurile pentru înregistrările pe care ea le suportă.

Puteți, de asemenea, să folosiți comanda RCVJRNE (Receive Journal Entry - Primire intrare jurnal) în jurnalul QAUDJRN pentru a primi intrările așa cum sunt ele scrise în jurnalul QAUDJRN.

Vizualizarea intrărilor din jurnalul de auditare

Privire generală:

Scop: Vizualizare intrări QAUDJRN

Cum se face:

Comanda DSPJRN (Display Journal - Afișare jurnal)

Autorizare:

Autorizare *USE pentru autorizare QSYS/QAUDJRN *USE receptor jurnal

Comanda Afișare jurnal (DSPJRN) vă permite să vedeți intrările jurnal selectate la stația dumneavoastră de lucru. Pentru a vedea intrările jurnal, faceți ceea ce urmează:

1. Introduceți DSPJRN QAUDJRN și apăsați F4. În ecranul prompt, puteți să introduceți informații pentru a selecta intervalul de intrări ce este arătat. De exemplu, puteți selecta toate intrările într-un interval specific de date sau puteți selecta doar un anumit tip de intrare, precum o încercare incorectă de logare (tip de intrare jurnal PW). Este implicită afișarea intrărilor doar din receptorul atașat. Puteți folosi RCVRNG(*CURCHAIN) pentru a vedea intrările din toți receptorii ce sunt în lanțul receptor pentru jurnalul QAUDJRN, până la a include receptorul care este atașat curent.
2. Când apăsați tasta Introdere, vedeți ecranul Afișare intrări jurnal:

```

Display Journal Entries

Journal . . . . . : QAUDJRN      Library . . . . . : QSYS
Largest sequence number on this screen . . . . . :000000000000000012
Type options, press Enter.
  5=Display entire entry

Opt   Sequence  Code  Type  Object      Library      Job       Time
     1         J    PR
     2         T    CA
     3         T    CO
     4         T    CA
     5         T    CO
     6         T    CA
     7         T    CO
     8         T    CA
     9         T    CO
    10        T    CA
    11        T    CO
    12        T    CA
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:55
                                     SCPF      10:24:56
                                     SCPF      10:24:56
                                     SCPF      10:24:57
                                     SCPF      10:24:57
                                     SCPF      10:24:57
                                     More...

F3=Exit  F12=Cancel

```

3. Folosiți opțiunea 5 (Afișare întreaga intrare) pentru a vedea informații despre o anumită intrare:

```

Display Journal Entry

Obiect . . . . . :                               Bibliotecă . . . . . :
Member . . . . . :                               Date intrare minimizezate : *None
Date incomplete . . : No                         Secvența . . . . . : 1198
Cod . . . . . : T - Auditare urmă intrare
Tip . . . . . : CO - Creare obiect

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=Ieșire F6=Afișare doar date specifice de intrare
F10=Afișare doar detalii intrări F12=Anulare F24=Mai multe taste

```

4. Puteți folosi F6 (Afișare doar a datelor specifice intrării) pentru intrări cu o mare cantitate de date specifice. Puteți selecta de asemenea o versiune hexazecimală a afișării. Puteți folosi F10 pentru a afișa detalii despre intrările din jurnal fără date specifice intrării.

Anexa F conține modelul pentru fiecare tip al intrării jurnal QAUDJRN.

Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program

Privire generală:

- Scop:** Afișare sau printare a informațiilor selectate din intrările jurnal.
- Cum se face:** DSPJRN OUTPUT(*OUTFILE), Creare a interogării și programului sau Rulare interogare sau program
- Autorizare:** Autorizare *USE pentru autorizare QSYS/QAUDJRN, autorizare *USE pentru receptor jurnal, autorizare *ADD pentru biblioteca pentru fișier ieșire

Puteți folosi comanda DSPJRN (Display Journal - Afișare jurnal) pentru a scrie intrările selectate din receptorii jurnalului de auditare într-un fișier de ieșire. Puteți folosi programul sau interogarea pentru a vedea informațiile din fișierul de ieșire.

Pentru parametrul ieșire al comenzii DSPJRN, specificați *OUTFILE. Vedeti parametrii suplimentari ce vă afișează informațiile despre fișierul ieșire:

```

                                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 conțin aceleași informații antet, ca și tipul intrării, data intrării și jobul care a determinat intrarea. QADSPJR5 (cu formatul înregistrare QJORDJE5) este furnizat pentru a defini aceste câmpuri când specificați *TYPE5 ca parametru format ieșire. Vedeți Tabela 150 la pagina 507 pentru informații suplimentare.

Pentru informații suplimentare despre alte înregistrări și formatele lor de ieșire, vedeți Anexa F.

Dacă doriți să realizați o analiză detaliată a unui tip particular de intrare, folosiți unul din fișierele bază de date model furnizate. De exemplu, pentru a crea un fișier ieșire numit AUDJRNAF5 în QGPL care include doar intrările eșec autorizare:

1. Creați un fișier ieșire gol cu formatul definit pentru intrările jurnal AF:
 CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
 OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)
2. Folosiți comanda DSPJRN pentru a scrie intrările jurnal selectate pentru fișierul ieșire:
 DSPJRN JRN(QAUDJRN) ... +
 JRNCD E(T) ENTYP(AF) OUTPUT(*OUTFILE) +
 OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)
3. Folosiți Interogare sau un program pentru a analiza informația din fișierul AUDJRNAF5.

Tabela 126 la pagina 239 arată numele fișierului bază de date model pentru fiecare tip de intrare. Anexa F arată dispunerile de fișiere pentru fiecare fișier de ieșire de tip bază de date.

Ceea ce urmează sunt câteva exemple despre cum puteți folosi informația QAUDJRN:

- Dacă suspectați că cineva încearcă să intre în sistemul dumneavoastră:
 1. Asigurați-vă că variabila de sistem QAUDLVL include *AUTFAIL.
 2. Folosiți comanda obiect CRTDUPOBJ pentru a crea un fișier ieșire gol cu formatul QASYPWJ5.
 3. O intrare jurnal de tip PW este înregistrată când introduce cineva un ID sau o parolă utilizator incorecte în ecranul Logare. Folosiți comanda DSPJRN pentru a scrie intrările jurnal de tip PW în fișierul ieșire.
 4. Creați un program interogare care afișează sau tipărește data, timpul și stația de lucru pentru fiecare intrare jurnal. Aceste informații vă ajută să determinați când și unde apar încercările.
- Dacă doriți să testați resursa de securitate pe care a-ți definit-o pentru o aplicație nouă:
 1. Asigurați-vă că variabila de sistem QAUDLVL include *AUTFAIL.
 2. Rulați testele aplicație cu ID-uri utilizator diferite.
 3. Folosiți comanda obiect CRTDUPOBJ pentru a crea un fișier ieșire gol cu formatul QASYAFJ5.
 4. Folosiți comanda DSPJRN pentru a scrie intrările jurnal de tip AF în fișierul ieșire.

5. Creați un program interogare care afișează sau tipărește informații despre obiect, job și utilizator. Această informație vă ajută să determinați ce utilizatori și funcții aplicație determină eșecurile de autorizare.
- Dacă planificați o migrare spre nivelul de securitate 40:
 1. Asigurați-vă că variabila de sistem QAUDLVL include *PGMFALL și *AUTFAIL.
 2. Folosiți comanda obiect CRTDUPOBJ pentru a crea un fișier ieșire gol cu formatul QASYAFJ5.
 3. Folosiți comanda DSPJRN pentru a scrie intrările jurnal de tip AF în fișierul ieșire.
 4. Creați un program de interogare ce selectează tipul de încălcări pe care le experimentați în timpul testului și tipărește informații despre jobul și programul ce determină fiecare intrare.

Notă: Tabela 126 la pagina 239 arată care intrare jurnal este scrisă pentru fiecare mesaj de încălcare a autorizării.

Relația Object Change Date/Time - Audit Records

Indicația principală folosită pentru a decide ce să se auditeze pentru i5/OS este să auditeze acțiunile utilizatorilor care au relevanță pentru securitate. A doua indicație este să nu se scrie înregistrări de auditare pentru operațiile pe care sistemul de operare le face automat. În unele cazuri, operațiile automate pot fi auditate dacă sistemul de operare realizează operația folosind o funcție care este de asemenea proiectată să fie folosită de către utilizatori.

Obiectivele pentru menținerea câmpului Change Date/Time al unui obiect sunt diferite față de obiectivele auditării. Scopul principal al câmpului Change Date/Time este de a indica dacă un obiect a fost modificat. 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 știe când a fost făcută ultima modificare, doar că obiectul a fost modificat de când a fost salvat ultima oară. Această caracteristică permite optimizarea performanțelor pentru fișiere baze de date. Câmpul Change Date/Time este actualizat doar prima oară când fișierul este modificat după ce a fost salvat ultima oară. Performanța ar fi afectată dacă câmpul Change Date/Time ar fi actualizat de fiecare dată când a fost actualizată, adăugată sau ștersă o înregistrare în fișier.

Rapoartele scrise pentru a detecta modificări în programe sau alte obiecte sunt uneori bazate pe câmpul Change Date/Time al obiectului în loc de informații din jurnalul audit de securitate. Următoarea listă descrie motivele pentru care ar putea fi o diferență între data de pe obiect și data de pe sursa obiectului:

- Comanda CHGPGM este folosită pentru a forța recrearea actualizărilor program pentru câmpul Change Date/Time al programului. Această operație scrie o înregistrare de auditare ZC (Modificare obiect)
- API-ul QYDOSGNO este folosit pentru a semna digital un program sau comandă actualizare asupra câmpului Change Date/Time pentru program sau comandă. Această operație scrie o înregistrare de auditare ZC.

Sistemul de operare poate de asemenea actualiza automat câmpul Change Date/Time al unui obiect în următoarele situații:

- Când un profil utilizator are autorizare privată asupra unui obiect și acel obiect este apoi șters, sistemul actualizează câmpul Change Date/Time al acelui profil utilizator pe măsură ce înlătură acea autorizare privată.
- Dacă auditarea de securitate este pornită când obiectul este șters, o înregistrare de auditare DO (Delete Operation) este scrisă pentru obiectul șters.
- Deoarece sistemul actualizează automat fiecare profil utilizator care are autorizare privată asupra obiectului șters, nu sunt scrise înregistrări de auditare pentru acele profile utilizator, chiar dacă câmpurile lor Change Date/Time sunt actualizate.

Pentru a depista când utilizatorii dumneavoastră au folosit interfețe de sistem normale pentru a modifica obiecte, puteți folosi jurnalul de auditare de securitate. Rapoartele de detectare modificări asupra obiectelor care sunt bazate doar pe câmpul Change Date/Time al unui obiect pot produce rezultate parțiale.

Alte tehnici pentru monitorizarea securității

Jurnalul auditare securitate (QAUDJRN) este sursa primară de informații despre evenimentele în legătură cu securitatea de pe sistemul dumneavoastră. Următoarele secțiuni discută alte moduri de observare a evenimentelor legate de securitate și a valorilor de securitate de pe sistemul dumneavoastră.

Veți găsi informații suplimentare în Anexa G, “Comenzile și meniurile pentru comenzi de securitate”, la pagina 617. Această anexă include exemple de folosire a comenzii și informațiilor despre meniuri pentru instrumente de securitate.

Monitorizarea mesajelor de securitate

Unele evenimente relevante de securitate, precum încercările de logare incorectă, realizează un mesaj în coada de mesaje QSYSOPR. Puteți crea separat, de asemenea, o coadă de mesaje numită QSYSMSG în biblioteca QSYS.

Dacă realizați coada de mesaje QSYSMSG în biblioteca QSYS, mesajele despre evenimentele critice de sistem sunt trimise atât către acea coadă de mesaje cât și către QSYSOPR. Coda de mesaje QSYSMSG poate fi monitorizată separat de un program sau un operator de sistem. Aceasta furnizează protecție suplimentară pentru resursele dumneavoastră de sistem. Mesajele critice de sistem din QSYSOPR sunt uneori ratate din cauza volumului de mesaje trimis la acea coadă de mesaje.

Utilizarea istoricului sistem

Unele evenimente în relație cu securitatea, precum depășirea încercărilor de logare incorectă în variabila de sistem QMAXSIGN, determină ca un mesaj să fie trimis istoricului QHST (istoric sistem-history). Mesajele de securitate sunt în intervalul 2200 - 22FF. Ele au prefixele CPI, CPF, CPC, CPD și CPA.

Începând cu Versiunea 2 Ediția 3 a programului licențiat i5/OS, unele mesaje privind eșecul autorizării și violarea integrității nu mai sunt trimise în istoricul (istoria) QHST. Toate informațiile care au fost disponibile în istoricul QHST pot fi obținute din jurnalul audit securitate. Înregistrarea informației în jurnalul audit furnizează o performanță mai bună a sistemului și informații complete despre aceste evenimente legate de securitate decât o face istoricul QHST. Istoricul QHST nu trebuie considerat o sursă completă de violări de securitate. Folosiți în schimb funcțiile 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 activității obiectului

Dacă includeți valoarea *AUTFAIL pentru auditarea acțiunii sistem (QAUDLVL variabilă de sistem), sistemul scrie o intrare jurnal audit pentru fiecare încercare nereușită de accesare a resursei. Pentru obiecte critice, puteți seta, de asemenea, o auditare obiect astfel încât sistemul scrie o intrare jurnal audit pentru fiecare acces reușit.

Jurnalul audit înregistrează doar faptul că obiectul a fost accesat. Nu înregistrează în istoric fiecare tranzacție către obiect. Pentru obiecte critice de pe sistemul dumneavoastră, este posibil să doriți informații mai detaliate despre datele specifice care au fost accesate și modificate. Jurnalizarea obiectului vă poate furniza aceste detalii. Jurnalizarea obiectului este folosită în mod primar pentru integritatea și recuperarea obiectului. Vedeți secțiunea Gestionarea jurnalului din Centrul de informare pentru o listă de tipuri de obiecte ce pot fi jurnalizate și ceea ce este jurnalizat

pentru fiecare tip de obiect. Un responsabil de securitate sau un auditor poate folosi, de asemenea, aceste intrări jurnal pentru a vedea modificările obiectului. A nu se jurnaliza orice obiecte în jurnalul QAUDJRN.

Intrările jurnal pot include:

- Identificarea jobului și utilizatorului și timpul de acces
- Imagini înainte și după modificările tuturor obiectelor
- Înregistrări despre când obiectul a fost deschis, închis, modificat, salvat și așa 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 șters, dar aceasta se descoperă ușor.

| Dacă jurnalizați un fișier bază de date, zonă de date, coadă de date sau un obiect sistem de fișiere integrat, puteți folosi
| comanda DSPJRN pentru a tipări toate modificările pentru acel obiect. Acestea sunt câteva exemple:

| Tastați următoarea comandă pentru un anumit fișier bază de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| FILE(biblioteca/fisier) OUTPUT(*PRINT)
```

| Tastați următoarea comandă pentru un anumit fișier zonă de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJ((biblioteca/nume obiect *DTAARA)) OUTPUT(*PRINT)
```

| Tastați următoarea comandă pentru un anumit fișier coadă de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJ((biblioteca/nume obiect *DTAQ) OUTPUT(*PRINT)
```

| Tastați următoarea comandă pentru un anumit sistem integrat de fișiere.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJPATH(('nume cale')) OUTPUT(*PRINT)
```

| De exemplu, dacă jurnalul JRNCUST din biblioteca CUSTLIB este folosit pentru a înregistra informații despre fișierul
| CUSTFILE (de asemenea în biblioteca CUSTLIB), comanda va fi:

```
| DSPJRN JRN(CUSTLIB/JRNCUST) +  
| FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

| Puteți atunci să faceți o interogare sau să folosiți SQL pentru a selecta toate înregistrările din acest fișier de ieșire
| pentru un anumit nume de obiect.

| Tastați următoarea comandă pentru a crea un fișier de ieșire pentru un anumit fișier.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| FILE(biblioteca/nume fisier) +  
| OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteca/fisier de iesire) ENTDTALEN(*CALC)
```

| Tastați următoarea comandă pentru a crea un fișier de ieșire pentru un anumit fișier zonă de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJ((biblioteca/nume obiect *DTAARA)) +  
| OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteca/fisier de iesire) ENTDTALEN(*CALC)
```

| Tastați următoarea comandă pentru a crea un fișier de ieșire pentru un anumit fișier coadă de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJ((biblioteca/nume obiect *DTAQ)) +  
| OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteca/fisier de iesire) ENTDTALEN(*CALC)
```

| Tastați următoarea comandă pentru a crea un fișier de ieșire pentru un anumit fișier coadă de date.

```
| DSPJRN JRN(biblioteca/jurnal) +  
| OBJPATH(('nume cale')) +  
| OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteca/fisier de iesire) ENTDTALEN(*CALC)
```


- I Dacă doriți să aflați ce jurnale sunt pe sistem, folosiți comanda WRKJRN (Work with Journals - Gestionare jurnale). Dacă doriți să aflați ce obiecte sunt jurnalizate pentru un jurnal particular, folosiți comanda WRKJRA (Work with Journal Attributes - Gestionare atribute jurnal).

Colecția de subiecte Gestionarea jurnalului furnizează informații complete despre jurnalizare.

Analizarea profilurilor de utilizator

Puteți afișa sau tipări o listă completă a tuturor utilizatorilor de pe sistemul dumneavoastră folosind comanda DSPAUTUSR (Display Authorized Users - Afișare utilizatori autorizați). Lista poate fi aranjată pe nume de profil sau nume de profil grup. Aici este un exemplu de secvență profil grup.

Display Authorized Users				
Group Profile	User Profile	Password Last Changed	No 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

Puteți folosi comanda DSPUSRPRF (Display User Profile - Afișare profil utilizator pentru a crea un fișier ieșire, pe care îl puteți procesa folosind o unealtă de interogare.

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

Puteți folosi o unealtă de interogare pentru a crea o varietate de rapoarte analiză ale fișierului dumneavoastră de ieșire, precum:

- O listă a tuturor utilizatorilor care au atât autorizarea specială *ALLOBJ cât și *SPLCTL.
- O listă a tuturor utilizatorilor ordonați secvențial de un câmp profil utilizator, precum un program inițial sau o clasă utilizator.

Puteți crea programe interogare pentru a produce rapoarte diferite de la fișierul dumneavoastră de ieșire. De exemplu:

- Listare a tuturor profilurilor utilizator care au orice tip de autorizări speciale prin selectarea înregistrărilor unde câmpul UPSPAU nu este egal cu *NONE.
- Listare a tuturor utilizatorilor cărora le este permis să introducă comenzi prin selectarea înregistrărilor unde câmpul *Capabilități limită* (numit UPLTCP în fișierul model bază de date) este egal cu *NO sau *PARTIAL.
- Listare a tuturor utilizatorilor care au un meniu inițial particular sau un program inițial.
- Listare a utilizatorilor inactivi prin cercetarea datei câmp de ultimă logare.
- Listare a tuturor utilizatorilor care nu au o parolă pentru folosire la nivelurile 0 și 1 de parolare prin selectarea înregistrărilor unde Parola prezentă pentru câmpul nivel 0 sau 1 (numit UPENPW în modelul de fișier ieșire) este egală cu N.

- Listare a tuturor utilizatorilor care au o parolă pentru folosire la nivelurile 2 și 3 prin selectarea înregistrărilor unde Parola prezentă pentru câmpul nivel 2 sau 3 (numit UPENPH în modelul de fișier ieșire) este egală cu Y.

Examinarea profilurilor mari de utilizatori

Profilurile de utilizator cu numere mari de autorizări, părând a fi răspândite la întâmplare în majoritatea sistemului, pot reflecta o lipsă de planificare a securității. Ceea ce urmează este o metodă de localizare a profilurilor mari de utilizatori și de evaluare a lor:

1. Folosiți comanda DSPOBJD (Display Object Description - Afășare descriere de obiect) pentru a crea un fișier de ieșire conținând informații despre toate profilurile utilizator de pe sistem:

```
DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
        DETAIL(*BASIC) OUTPUT(*OUTFILE)
```
2. Creați un program de interogare pentru a lista numele și dimensiunea fiecărui profil de utilizator, în ordine descrescătoare, după dimensiune.
3. Tipăriți informații detaliate despre cele mai mari profiluri de utilizator și evaluează autorizările și obiectele deținute 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 și obiectele bazate pe directoare nu sunt tipărite. Comenzile WRKOBJOWN și WRKOBJPVT pot fi folosite pentru a afișa obiecte bazate pe director și obiecte bazate pe bibliotecă, dar nu există o funcție de tipărire asociată cu aceste comenzi.

Unele profiluri de utilizator furnizate de IBM sunt foarte mari datorită numărului de obiecte pe care le dețin. Listarea și analizarea acestora nu este necesară. Oricum, trebuie să verificați dacă există programe de adoptare a autorizării profilurilor utilizator furnizate de IBM care au autorizare specială *ALLOBJ, precum QSECOFR și QSYS. Vedeți “Analizarea programelor care adoptă autorizarea”.

Anexa B furnizează informații despre toate profilurile utilizator furnizate de IBM și funcțiile acestora.

Analizarea autorizărilor pentru obiect

Puteți folosi următoarea metodă pentru a determina cine are autorizarea pentru bibliotecile de pe sistem:

1. Folosiți comanda DSPOBJD pentru a lista toate bibliotecile de pe sistem:

```
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```
2. Folosiți comanda DSPOBJAUT (Display Object Authority - Afășare autorizare obiect) pentru a lista autorizările unei anumite biblioteci:

```
DSPOBJAUT OBJ(nume-bibliotecă) OBJTYPE(*LIB) +
            ASPDEV(asp-nume-dispozitiv) OUTPUT(*PRINT)
```
3. Folosiți comanda DSPLIB (Display Library - Afășare bibliotecă) pentru a lista obiectele din bibliotecă:

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

Folosind aceste rapoarte, puteți determina ce este într-o bibliotecă și cine are acces la bibliotecă. Dacă este necesar, puteți folosi, de asemenea, comanda DSPOBJAUT pentru a vedea autorizarea pentru obiectele selectate în bibliotecă.

Analizarea programelor care adoptă autorizarea

Programe care adoptă autorizarea unui utilizator cu autorizarea specială *ALLOBJ reprezintă o expunere de securitate. Următoarea metodă poate fi folosită pentru a găsi și inspecta acele programe:

1. Pentru fiecare utilizator cu autorizarea specială *ALLOBJ, folosiți comanda DSPPGMADP (Display Programs That Adopt - Afășare programe care adoptă) pentru a lista programele care adoptă acea autorizare de utilizator:

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

Notă: Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 267 arată cum se listează utilizatori cu autorizarea *ALLOBJ.

2. Folosiți comanda DSPORTAUT pentru a determina cine este autorizat pentru a folosi fiecare program de adoptare și ce este autorizarea publică pentru program:

```
DSPORTAUT OBJ( nume-librărie/nume-program ) +  
          OBJTYPE(*PGM) ASPDEV(asp-nume-dispozitiv) OUTPUT(*PRINT)
```

Notă: Parametrul tip obiect ar putea trebui să fie *PGM, *SQLPKG sau *SRVPGM după cum indică raportul DSPPGMADP.

3. Inspectați codul sursă și descrierea de program pentru a evalua:
 - Dacă utilizatorul programului este împiedicat să folosească funcția exces, precum folosirea unei linii de comandă, în timpul rulării sub un profil adoptat.
 - Dacă programul adoptă nivelul minim de autorizare necesar pentru funcția dorită. Aplicații care folosesc eșuarea de program pot fi proiectate folosind același profil utilizator pentru obiecte și 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. Verificați când a fost modificat programul ultima dată, folosind comanda DSPORTBJD:

```
DSPORTBJD OBJ(nume-biblioteca/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 indică raportul DSPPGMADP.

Verificarea obiectelor ce au fost modificate

Puteți folosi comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului) pentru a căuta obiecte care au fost modificate. Un obiect transformat este, de obicei, un indiciu că cineva încearcă să facă modificări pe sistemul dumneavoastră. Este posibil să doriți să rulați această comandă după cineva:

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

Când rulați comanda, sistemul creează un fișier bază de date ce conține informații despre orice problemă potențială de integritate. Puteți verifica obiectele deținute de unul sau mai multe profiluri, obiectele care se potrivesc unui nume de cale sau toate obiectele de pe sistemul dumneavoastră. Puteți căuta obiecte ale cărui nume de domeniu a fost transformat și obiecte cu care au fost falsificate. Puteți recalcula valorile de validare ale programului pentru a căuta obiecte de tipul *PGM, *SRVPGM, *MODULE și *SQLPKG, care au fost transformate. Puteți verifica semnătura obiectelor care au fost semnate digital. Puteți verifica dacă bibliotecile și comenzile au fost falsificate. Puteți, de asemenea, porni o scanare de sistem fișier integrat sau să verificați dacă obiectele au eșuat unei scanări anterioare de sistem fișier.

Rularea programului CHKOBJITG cere autorizare specială *AUDIT. Comanda poate necesita mult timp pentru a rula, din cauza scanărilor și calculelor pe care le realizează. Trebuie să o rulați într-un moment când sistemul dumneavoastră nu este ocupat. Cele mai multe dintre comenzile IBM duplicat din edițiile apărute înainte de V5R2 vor fi înregistrate ca violări în istoric. Aceste comenzi trebuie să fie șterse și create din nou folosind comanda CRTDUPOBJ (Create Duplicate Object - Creare duplicat obiect), de fiecare dată când este încărcată o nouă ediție.

Verificarea sistemului de operare

Puteți 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 rulați într-un moment când sistemul dumneavoastră nu este ocupat.

Auditarea acțiunilor responsabilului cu securitatea

Este posibil să doriți să păstrați o înregistrare a tuturor acțiunilor realizate de utilizatori cu autorizarea specială *ALLOBJ și *SECADM. Puteți folosi valoarea de auditare a acțiunii în profilul utilizator pentru a face aceasta:

1. Pentru fiecare utilizator cu autorizarea specială *ALLOBJ și *SECADM, folosiți 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 și *SECURITY, folosiți această comandă pentru a seta AUDLVL pentru profilul utilizator responsabilul cu securitatea:

```
CHGUSRAUD USER(SECUSER) +
    AUDLVL(*CMD *CREATE *DELETE +
          *OBJMGT *OFCSRV *PGMADP +
          *SAVRST *SERVICE, +
          *SPLFDTA *SYSMTG)
```

Notă: Tabela 125 la pagina 235 arată toate valorile posibile pentru auditarea acțiunii.

2. Înlătură autorizarea specială *AUDIT din profilul utilizator cu autorizarea specială *ALLOBJ și *SECADM. Aceasta îi împiedică pe acești utilizatori să modifice caracteristicile de auditare ale profilurilor lor.

Notă: Nu puteți înlătura autorizările speciale din profilul QSECOFR. De aceea, nu puteți împiedica un utilizator logat ca QSECOFR de la modificarea caracteristicilor auditării aceluși profil. Oricum, dacă un utilizator logat ca QSECOFR folosește 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. Asigurați-vă că variabila de sistem QAUDCTL include *AUDLVL.
4. Folosiți comanda DSPJRN pentru a vedea intrările din jurnalul audit folosind tehnicile descrise. “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 262

Anexa A. Comenzile de securitate

Această anexă conține comenzile de sistem legate de securitate. Puteți folosi aceste comenzi în locul meniurilor de sistem, dacă doriți, tastând aceste comenzi la o linie de comandă. Comenzile sunt împărțite în grupuri orientate pe operații.

Subiectul CL din Centrul de informare informații mai detaliate despre aceste comenzi. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii. Tabelele din Anexa D arată ce autorizări de obiect sunt necesare pentru a folosi aceste comenzi.

Tabela 128. Comenzi pentru lucrul cu deținători de autorizare

Nume comandă	Nume descriptiv	Funcție
CRTAUTHLR	Creare deținător de autorizare	Vă permite să asigurați un fișier înainte ca fișierul să existe. Deținătorii de autorizare sunt valizi doar pentru fișiere bază de date descrise de program.
DLTAUTHLR	Ștergere deținător de autorizare	Vă permite să ștergeți un deținător de autorizare. Dacă fișierul asociat există, informațiile deținătorului de autorizare sunt copiate în fișier.
DSPAUTHLR	Afișare deținător de autorizare	Vă permite să afișați toți deținătorii de autorizare din sistem.

Tabela 129. Comenzi pentru lucrul cu liste de autorizații

Nume comandă	Nume descriptiv	Funcție
ADDAUTLE	Adăugare intrare listă de autorizații	Vă permite să adăugați un utilizator la o listă de autorizații. Dumneavoastră specificați ce autorizare are utilizatorul pentru toate obiectele din listă.
CHGAUTLE	Modificare intrare listă de autorizații	Vă permite să modificați autorizările de utilizator pentru obiectele din lista de autorizare.
CRTAUTL	Comanda Creare listă de autorizații	Vă permite să creați o listă de autorizații.
DLTAUTL	Ștergere listă de autorizații	Vă permite să ștergeți o întreagă listă de autorizații.
DSPAUTL	Afișare listă de autorizații	Vă permite să afișați o listă de utilizatori și autorizările lor pentru o listă de autorizații.
DSPAUTLOBJ	Afișare obiecte listă de autorizații	Vă permite să afișați o listă de obiecte asigurate de o listă de autorizații.
EDTAUTL	Editare listă de autorizații	Vă permite să adăugați, modificați și să înlăturați utilizatori și autorizările lor de la o listă de autorizații.
RMVAUTLE	Înlăturare intrare listă de autorizații	Vă permite să înlăturați un utilizator de la o listă de autorizații.
RTVAUTLE	Extragere intrare de listă de autorizații	Folosită într-un program în limbaj de control (CL) pentru a obține una sau mai multe valori asociate cu un utilizator din lista de autorizații. Comanda poate fi folosită împreună cu comanda CHGAUTLE pentru a acorda unui utilizator noi autorizări față de cele pe care le are deja.
WRKAUTL	Lucru cu liste de autorizație	Vă permite să lucrați cu liste de autorizații dintr-un ecran listă.

Tabela 130. Comenzi pentru lucru cu autorizări și auditare de obiecte

Nume comandă	Nume descriptiv	Funcție
CHGAUD	Modificare auditare	Vă permite să modificați valoarea de auditare pentru un obiect.
CHGAUT	Modificare autorizare	Vă permite să modificați autorizarea utilizatorilor pentru obiecte.
CHGOBJAUD	Modificare auditare obiect	Vă permite să specificați dacă accesul la un obiect este auditat.
CHGOBJOWN	Modificare proprietar obiect	Vă permite să modificați dreptul de proprietate pentru un obiect de la un utilizator la altul.
CHGOBJPGP	Modificare grup primar obiect	Vă permite să modificați grupul primar pentru un obiect la un alt utilizator sau la nici un grup primar.
CHGOWN	Modificare proprietar	Vă permite să modificați dreptul de proprietate al unui obiect de la un utilizator la altul.
CHGPGP	Modificare grup primar	Vă permite să modificați grupul primar pentru un obiect la un alt utilizator sau la nici un grup primar.
DSPAUT	Afișare autorizare	Vă permite să afișați autorizări ale utilizatorilor pentru un obiect.
DSPLNK	Afișare legături	Vă permite să arătați o listă de nume a obiectelor specificate în directoare și opțiuni pentru afișare informații despre obiecte.
DSPOBJAUT	Afișare autorizare obiect	Afișează proprietarul obiectului, autorizare publică pentru obiect, toate autorizările private pentru obiect și numele listei de autorizații folosite pentru a asigura obiectul.
DSPOBJD	Afișare descriere obiect	Afișează nivelul de auditare obiect pentru obiect.
EDTOBJAUT	Editare autorizare obiect	Vă permite să adăugați, să modificați sau să înlăturați o autorizare a unui utilizator pentru un obiect.
GRTOBJAUT	Acordare de autorizare obiect	Vă permite să acordați explicit autorizare către utilizatori numiți, tuturor utilizatorilor (*PUBLIC) sau utilizatorilor obiectului referit pentru obiectele numite în această comandă.
RVKOBJAUT	Revocare autorizare obiect	Vă permite să înlăturați una, mai multe sau toate autorizările acordate explicit unui utilizator pentru obiectele numite.
WRKAUT	Lucru cu autorizări	Vă permite să lucrați cu autorizări de obiect prin selectarea de opțiuni dintr-o listă afișată.
WRKLNK	Lucru cu legături	Vă permite să arătați o listă de nume a obiectelor specificate în directoare și opțiuni pentru afișare informații despre obiecte.
WRKOBJ	Lucru cu obiecte	Vă permite să lucrați cu autorizări de obiect prin selectarea de opțiuni dintr-o listă afișată.
WRKOBJOWN	Lucru cu obiecte după proprietar	Vă permite să lucrați cu obiectele deținute de un profil utilizator.
WRKOBJPGP	Lucru cu obiecte după grup primar	Vă permite să lucrați cu obiectele pentru care un profil este grupul primar folosind opțiuni dintr-un ecran listă.
WRKOBJPVT	Lucru cu obiecte după Private Authorities	Vă permite să lucrați cu obiectele pentru care un profil este autorizat privat folosind opțiuni dintr-un ecran listă.

Tabela 131. Comenzi pentru Gestionare parole

Nume comandă	Nume descriptiv	Funcție
CHGDSTPWD	Modificare parolă Unelte de service dedicate	Vă permite să resetați profilul cu capabilități de securitate DST la parola implicită livrată cu sistemul.
CHGPWD	Modificare parolă	Permite unui utilizator să își modifice parola proprie.
CHGUSRPRF	Modificare profil utilizator	Vă permite să modificați valorile specificate într-un profil de utilizator, inclusiv parola utilizatorului.
CHKPWD	Verificare parolă	Permite verificarea parolei unui utilizator. De exemplu, dacă doriți ca utilizatorul să introducă din nou parola pentru a rula o anumită aplicație, puteți folosi CHKPWD în programul dumneavoastră CL pentru a verifica parola.
CRTUSRPRF ¹	Creare profil utilizator	Când adăugați un utilizatorul în sistem, asigurați o parolă utilizatorului.

¹ Când se termină CRTUSRPRF, nu puteți să specificați crearea *USRPRF într-un pool de memorie auxiliară (ASP) independent. Totuși, când un utilizator este autorizat privat pentru un obiect pe un ASP independent, sau este proprietarul unui obiect de pe un ASP independent sau este grupul primar al unui obiect de pe un ASP independent, numele profilului este stocat pe ASP-ul independent. Dacă ASP-ul independent este mutat în alt sistem, autorizarea privată, dreptul de proprietate asupra obiectului și intrările de grup primar vor fi atașate la profilul cu același nume din sistemul destinație. Dacă nu există un profil pe sistemul destinație, va fi creat. Utilizatorul nu va avea nici o autorizare specială și parola va fi setată la *NONE.

Tabela 132. Comenzi pentru lucru cu profiluri utilizator

Nume comandă	Nume descriptiv	Funcție
CHGPRF	Modificare profil	Permite unui utilizator să modifice unele din atributele profilului propriu.
CHGUSRAUD	Modificare auditare utilizator	Vă permite să specificați acțiunea și auditarea de obiect pentru un profil utilizator.
CHGUSRPRF	Modificare profil utilizator	Vă permite să modificați valorile specificate într-un profil utilizator, cum ar fi parola utilizatorului, autorizări speciale, meniu inițial, program inițial, bibliotecă curentă și limită de prioritate.
CHKOBJTG	Verificare integritate obiect	Verificați obiectele deținute de unul sau mai mulți utilizatori sau verificați obiectele care corespund numelui de cale, pentru a vă asigura că obiectele nu au fost modificate.
CRTUSRPRF	Creare profil utilizator	Vă permite să adăugați un utilizator la sistem și să specificați valori cum ar fi parola utilizatorului, autorizări speciale, meniu inițial, bibliotecă curentă și limită de prioritate.
DLTUSRPRF	Ștergere profil utilizator	Vă permite să ștergeți un profil utilizator din sistem. Această comandă furnizează o opțiune de a șterge sau modifica dreptul de proprietate asupra obiectelor deținute de profilul utilizator.
DSPAUTUSR	Afișare utilizatori autorizați	Afișează sau tipărește 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 și textul profilului de utilizator.
DSPUSRPRF	Afișare profil utilizator	Vă permite să afișați un profil utilizator în câteva formate diferite.
GRTUSRAUT	Acordare autorizare utilizator	Vă permite să copiați autorizări private de la un profil utilizator la alt profil utilizator.
PRTPRFINT	Tipărire valori interne profil	Vă permite să tipăriți un raport de informații interne despre numărul de intrări.
PRTUSRPRF	Tipărire profil utilizator	Vă permite să analizați profiluri utilizator care îndeplinesc anumite criterii.
RTVUSRPRF	Extragere profil utilizator	Folosită într-un program în limbaj de control (CL) pentru a obține și utiliza una sau mai multe valori care sunt stocate și asociate cu un profil utilizator.
WRKUSRPRF	Lucru cu profiluri utilizator	Vă permite să lucrați cu profiluri utilizator prin introducerea de opțiuni într-o listă afișată.

Tabela 133. Comenzi înrudite pentru profil utilizator

Nume comandă	Nume descriptiv	Funcție
DSPPGMADP	Afișare programe care adoptă	Vă permite să afișați o listă de programe și pachete SQL care adoptă un anume profil utilizator.
RSTAUT	Restaurare autorizare	Vă permite să restaurați autorizări pentru obiecte conținute de un profil utilizator când acesta a fost salvat. Aceste autorizări pot fi restaurate doar ce un profil utilizator este restaurat cu comanda Restaurare profil utilizator (RSTUSRPRF).
RSTUSRPRF	Restaurare profil utilizator	Vă permite să restaurați un profil utilizator și atributele sale. Restaurarea autorizărilor specifice obiectelor se face cu comanda RSTAUT după ce este restaurat profilul. Comanda RSTUSRPRF restaurează de asemenea toate listele de autorizări și deținătorii de autorizări, dacă se specifică RSTUSRPRF(*ALL).
SAVSECDTA	Salvare date de securitate	Salvează toate profilurile utilizator, liste de autorizații și deținători de autorizare fără a folosi un sistem care este într-o stare restrictivă.
SAVSYS	Salvare sistem	Salvează toate profilurile utilizator, listele de autorizări și deținători de autorizare din sistem. Este necesar un sistem dedicat pentru a folosi această funcție.

Tabela 134. Comenzi pentru lucru cu auditare

Nume comandă	Nume descriptiv	Funcție
CHGAUD	Modificare auditare	Vă permite să specificați auditarea pentru un obiect.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Vă permite să specificați dacă se face auditare de acces pentru un obiect de bibliotecă de documente.
CHGOBJAUD	Modificare auditare obiect	Vă permite să specificați auditarea pentru un obiect.
CHGUSRAUD	Modificare auditare utilizator	Vă permite să specificați acțiunea și auditarea de obiect pentru un profil utilizator.

Tabela 135. Comenzi pentru lucrul cu obiecte de bibliotecă de documente

Nume comandă	Nume descriptiv	Funcție
ADDDLOAUT	Adăugare autorizare obiect de bibliotecă de documente	Vă permite să acordați acces unui utilizator la un document sau folder sau să asigurați un document sau folder cu o listă de autorizații sau un cod de acces.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Vă permite să specificați nivelul de auditare obiect pentru un obiect de bibliotecă de documente.
CHGDLOAUT	Modificare autorizare obiect de bibliotecă de documente	Vă permite să modificați autorizarea pentru un document sau un folder.
CHGDLOOWN	Modificare proprietar obiect de bibliotecă de documente	Transferă dreptul de proprietate asupra documentului sau folderului de la un utilizator la altul.
CHGDLOPGP	Modificare grup primar pentru obiect de bibliotecă de documente	Vă permite să modificați grupul primar pentru un obiect de bibliotecă de documente.
DSPAUTLDLO	Afișare obiecte de bibliotecă de documente pentru listă de autorizații	Vă permite să afișați documentele și folderele care sunt asigurate prin lista de autorizații specificată.
DSPDLOAUD	Afișare auditare obiect de bibliotecă de documente	Afișează nivelul de auditare pentru un obiect de bibliotecă de documente.
DSPDLOAUT	Afișare autorizare obiect de bibliotecă de documente	Vă permite să afișați informații de autorizare pentru un document sau un folder.
EDTDLOAUT	Editare autorizare obiect de bibliotecă de documente	Folosită pentru a adăuga, modifica sau înlătura autorizări utilizator pentru un document sau un folder.

Tabela 135. Comenzi pentru lucrul cu obiecte de bibliotecă de documente (continuare)

Nume comandă	Nume descriptiv	Funcție
GRTUSRPMN	Acordare permisiune utilizator	Dă permisiune unui utilizator de a manipula documente și foldere sau de a efectua operații de birou în numele altui utilizator.
RMVDLOAUT	Înlăturare autorizare obiect de bibliotecă de documente	Folosită pentru a înlătura autorizarea unui utilizator de la un document sau folder.
RVKUSRPMN	Revocare permisiune utilizator	Retrage de la un utilizator (sau toți utilizatorii) autorizarea de a accesa documente în numele unui alt utilizator.

Tabela 136. Comenzi pentru lucru cu intrări de autentificare server

Nume comandă	Nume descriptiv	Funcție
ADDSVRAUTE	Adăugare intrare de autentificare server	Vă permite să adăugați informații de autentificare server pentru un profil utilizator.
CHGSVRAUTE	Modificare intrare de autentificare server	Vă permite să modificați intrări de autentificare server existente pentru un profil utilizator.
DSPSVRAUTE	Afișare intrări de autentificare server	Vă permite să afișați intrări de autentificare server pentru un profil utilizator.
RMVSVRAUTE	Înlăturare intrare de autentificare server	Vă permite să înlăturați intrări de autentificare server din profilul utilizator specificat.

Aceste comenzi permit unui utilizator să specifice un nume de utilizator, parola asociată și numele unei mașini server la distanță. Distributed Relational Database Access (DRDA) folosește aceste intrări pentru a rula cereri de acces la baza de date ca utilizatorul specificat de pe serverul la distanță.

Tabela 137. Comenzi pentru lucru cu directorul de distribuție sistem

Nume comandă	Nume descriptiv	Funcție
ADDDIRE	Adăugare intrare director	Adaugă intrări noi la directorul de distribuție sistem. Directorul conține informații despre un utilizator, cum ar fi ID și adresă utilizator, numele sistemului, nume profil utilizator, adresă de poștă și număr de telefon.
CHGDIRE	Modificare intrare director	Modifică datele pentru o anumită intrare din directorul de distribuție sistem. Administratorul de sistem are autorizare de a actualiza orice date conținute într-o intrare de director, în afară de ID utilizator, adresă și descriere utilizator. Utilizatorii își pot actualiza propria intrare în director, dar nu și anumite câmpuri.
RMVDIRE	Înlăturare intrare director	Înlătură o anumită intrare din directorul de distribuție sistem. Când un ID utilizator și adresă este înlăturat din director, este de asemenea înlăturat din orice liste de distribuție.
WRKDIRE	Lucru cu directoare	Furnizează un set de ecrane care permit unui utilizator să vizualizeze, adauge, modifice și înlătore intrări din directorul de distribuție sistem.

Tabela 138. Comenzi pentru lucru cu liste de validare

Nume comandă	Nume descriptiv	Funcție
CRTVLDL	Creare liste de validare	Vă permite să creați un obiect listă de validare care conține intrări ce constau dintr-un identificator, date care vor fi criptate de sistem când sunt memorate și date în formă liberă.
DLTVLDL	Ștergere listă de validare	Vă permite să ștergeți lista de validate specificată dintr-o bibliotecă.

Tabela 139. Comenzi pentru lucru cu informații de utilizare funcție

Nume comandă	Nume descriptiv	Funcție
CHGFCNUSG	Modificare utilizare funcție	Vă permite să modificați informațiile de utilizare pentru o funcție înregistrată.
DSPFCNUSG	Afișare utilizare funcție	Vă permite să afișați o listă de identificatori de funcție și informațiile detaliate de utilizare pentru o anumită funcție.
WRKFCNUSG	Gestionare utilizare funcție	Vă permite să afișați o listă de identificatori de funcție și să modificați sau să afișați informațiile de utilizare de funcție.

Următoarele tabele descriu diferite tipuri de unelte de securitate. Pentru informații suplimentare despre uneltele de securitate, vedeți Anexa G, “Comenzile și meniurile pentru comenzi de securitate”.

Tabela 140. Unelte de securitate pentru Gestionare auditare

Nume comandă	Nume descriptiv	Funcție
CHGSECAUD	Modificare auditare de securitate	Vă permite să setați auditarea de securitate și să modificați valorile de sistem care controlează auditarea de securitate.
CPYAUDJRNE	Copiere intrări jurnal de auditare	Vă permit să copiați intrările din jurnalul auditat de securitate în fișiere de ieșire pe care le puteți interoga. Puteți să selectați anumite tipuri de intrări, anumiți utilizatori și o perioadă de timp.
DSPAUDJRNE	Afișare intrări jurnal de auditare	Vă permite să afișați sau să tipăriți informații despre intrările din jurnalul de auditare de securitate. Puteți să selectați anumite tipuri de intrare, anumiți utilizatori și o perioadă de timp.
DSPSECAUD	Afișare valori auditare de securitate	Vă permite să afișați informații despre jurnalul de auditare de securitate și valorile de sistem care controlează auditarea de securitate.

Notă: IBM a oprit furnizarea îmbunătățirilor pentru comanda DSPAUDJRNE. Comanda nu suportă toate tipurile de înregistrări de auditare a securității și nu listează toate câmpurile pentru înregistrările pe care ea le suportă.

Tabela 141. Unelte de securitate pentru Gestionare autorizări

Nume comandă	Nume descriptiv	Funcție
PRTJOBDAUT	Tipărire autorizare descriere de job	Vă permite să tipăriți o listă de descrieri de job a căror autorizare publică nu este *EXCLUDE. Puteți folosi această comandă pentru a tipări informații despre descrieri de job care specifică un profil utilizator care poate fi accesat de toți utilizatorii din sistem.
PRTPUBAUT	Tipărire obiecte autorizate public	Vă permite să tipăriți o listă de obiecte de tip specificat a căror autorizare publică nu este *EXCLUDE.
PRTPVTAUT	Tipărire autorizări private	Vă permite să tipăriți o listă de autorizări private pentru obiecte de tipul specificat.
PRTQAUT	Tipărire autorizare coadă	Vă permite să tipăriți setările de securitate pentru cozi de ieșire și cozi de job din sistemul dumneavoastră. Aceste setări controlează cine poate vizualiza și modifica intrări din coada de ieșire sau coada de joburi.
PRTSBSDAUT	Tipărire autorizare descriere subsistem	Vă permite să tipăriți o listă de descrieri de subsistem dintr-o bibliotecă care conține un utilizator implicit într-o intrare de subsistem.
PRTRGPGM	Tipărire programe de declanșare	Vă permite să tipăriți o listă de programe de declanșare care sunt asociate cu fișiere de bază de date de pe sistemul dumneavoastră.

Tabela 141. Unelte de securitate pentru Gestionare autorizări (continuare)

Nume comandă	Nume descriptiv	Funcție
PRTUSROBJ	Tipărire obiecte utilizator	Vă permite să tipăriți o listă cu obiectele utilizator (obiecte care nu sunt livrate de IBM) care sunt într-o bibliotecă.

Tabela 142. Unelte de securitate pentru Gestionare securitate sistem

Nume comandă	Nume descriptiv	Funcție
CHGSECA ¹	Modificare atribute de securitate	Vă permite să setați noi valori de pornire pentru generarea de numere de ID utilizator sau numere de ID de grup. Utilizatorii pot specifica un ID utilizator de pornire și un ID grup de pornire.
CFGSYSSEC	Configurare securitate sistem	Vă permite să setați valori sistem importante pentru securitate la setările lor recomandate. Comanda setează de asemenea auditarea de securitate pe sistemul dumneavoastră.
CLRSVRSEC	Curățare date de securitate server	Vă permite să curățați informații de autentificare decriptabile care sunt asociate cu profiluri utilizator și intrări de listă de validare (*VLDL). Notă: Acestea sunt aceleași informații care au fost curățate în ediții anterioare V5R2 când valoarea sistem QRETSVRSEC se schimba de '1' la '0'.
DSPSECA	Afișare atribute de securitate	Vă permite să afișați valorile curente și în așteptare ale unor atribute de securitate sistem.
PRTCMNSEC	Tipărire securitate comunicații	Vă permite să tipăriți atributele de securitate ale obiectelor *DEVD, *CTL și *LIND din sistem.
PRTSYSSECA	Tipărire atribute de securitate sistem	Vă permite să tipăriți o listă de valori sistem și atribute de rețea importante pentru securitate. Raportul arată valoarea curentă și valoarea recomandată.
RVKPUBAUT	Revocare autorizare publică	Vă permite să setați autorizarea publică la *EXCLUDE pentru un set de comenzi sensibile la securitate de pe sistemul dumneavoastră.

¹ Pentru a folosi această comandă, trebuie să aveți autorizare specială *SECADM.

Pentru informații suplimentare despre unelte și sugestii despre cum se folosesc uneltele de securitate, vedeți cartea *Tips for Making Your iSeries 400 Secure*, GC41-0615.

Anexa B. Profilurile de utilizator furnizate de IBM

Această anexă conține informații despre profilurile utilizator care sunt livrate cu sistemul. Aceste profiluri sunt folosite ca proprietari de obiecte pentru diferite funcții sistem. Unele funcții sistem de asemenea rulează sub anumite profiluri utilizator furnizate de IBM.

Tabela 143 arată valorile implicite care sunt folosite pentru toate profilurile utilizator furnizate de IBM și la comanda CRTUSRPRF (Create User Profile - Creare profil utilizator). Parametrii sunt ordonați în funcție de momentul apariției lor în ecranul Creare profil utilizator.

Tabela 144 menționează fiecare profil livrat de IBM, scopul lui și orice valoare pentru profil care este diferită de valorile implicite pentru profilurile utilizator livrate de IBM.

Notă:

Tabela 144 include acum profiluri utilizator adiționale care sunt livrate cu produsele de programe cu licență. Tabela include doar **unele**, dar nu toate profilurile utilizator pentru produsele de programe cu licență, de aceea, lista nu este completă.

Atenție:

- Parola pentru profilul QSECOFR

Trebuie să modificați parola pentru profilul QSECOFR după ce instalați sistemul dumneavoastră. Această parolă este aceeași pentru fiecare sistem iSeries și aduce o expunere de securitate până în momentul schimbării ei. Totuși, **nu** modificați nici o valoare pentru profilurile utilizator livrate de IBM. Modificarea acestor profiluri poate face ca funcțiile sistemului să eșueze.

- Autorizările pentru profilurile livrate de IBM

Manifestați **precauție** când îndepărtați autorizările deținute de profilurile livrate de IBM asupra obiectelor care sunt livrate cu sistemul de operare. Unor profiluri livrate de IBM le sunt acordate autorizări private care sunt livrate cu sistemul de operare. Îndepărtarea oricărei dintre aceste autorizări poate provoca funcțiile sistem să eșueze.

Tabela 143. Valorile implicite pentru profilurile utilizator

Parametru profil utilizator	Valori implicite	
	Profiluri utilizator livrate de IBM	Ecranul Creare profil utilizator
Parolă (PASSWORD)	*NONE	*USRPRF ⁴
Setare parolă ca să expire (PWDEXP)	*NO	*NO
Stare (STATUS)	*ENABLED	*ENABLED
Clasă utilizator (USRCLS)	*USER	*USER
Nivel de ajutorare (ASTLVL)	*SYSVAL	*SYSVAL
Biblioteca actuală (CURLIB)	*CRTDFT	*CRTDFT
Program inițial (INLPGM)	*NONE	*NONE
Meniu inițial (INLMNU)	MAIN	MAIN
Biblioteca meniu inițial	*LIBL	*LIBL
Capabilități limitate (LMTCPB)	*NO	*NO
Text (TEXT)	*BLANK	*BLANK
Autorizare specială (SPCAUT)	*ALLOBJ ¹ *SAVSYS ¹	*USRCLS ²
Mediu special (SPCENV)	*SYSVAL	*SYSVAL
Afișare informații de semnare (DSPSGNINF)	*SYSVAL	*SYSVAL
Interval de expirare parolă (PWDEXPITV)	*SYSVAL	*SYSVAL
Limitare sesiuni dispozitiv (LMTDEVSSN)	*SYSVAL	*SYSVAL

Tabela 143. Valorile implicite pentru profilurile utilizator (continuare)

Parametru profil utilizator	Valori implicite	
	Profiluri utilizator livrate de IBM	Ecranul Creare profil utilizator
Punere în buffer tastatură (KBDBUF)	*SYSVAL	*SYSVAL
Spațiu de stocare maxim (MAXSTG)	*NOMAX	*NOMAX
Limitare prioritate (PTYLMT)	0	3
Descriere de job (JOBID)	QDFTJOBID	QDFTJOBID
Biblioteca descriere de job	QGPL	*LIBL
Profil grup (GRPPRF)	*NONE	*NONE
Proprietar (OWNER)	*USRPRF	*USRPRF
Autorizare grup (GRPAUT)	*NONE	*NONE
Tip de autorizare grup (GRPAUTTYP)	*PRIVATE	*PRIVATE
Grupuri suplimentare (SUPGRPPRF)	*NONE	*NONE
Cod de contabilizare (ACGCDE)	*SYS	*BLANK
Parolă document (DOCPWD)	*NONE	*NONE
Coadă de mesaje (MSGQ)	*USRPRF	*USRPRF
Livrare (DLVRY)	*NOTIFY	*NOTIFY
Gravitate (SEV)	00	00
Dispozitiv imprimantă (PRTDEV)	*WRKSTN	*WRKSTN
Coadă de ieșire (OUTQ)	*WRKSTN	*WRKSTN
Programul Attention (ATNPGM)	*NONE	*SYSVAL
Secvență sortare (SRTSEQ)	*SYSVAL	*SYSVAL
Identificator limbă (LANGID)	*SYSVAL	*SYSVAL
Identificator regiune sau țară (CNTRYID)	*SYSVAL	*SYSVAL
Identificator set de caractere codat (CCSID)	*SYSVAL	*SYSVAL
Setare atribute job (SETJOBATR)	*SYSVAL	*SYSVAL
Locale (LOCALE)	*NONE	*SYSVAL
Opțiune utilizator (USROPT)	*NONE	*NONE
Număr identificare utilizator (UID)	*GEN	*GEN
Număr de identificare grup (GID)	*NONE	*NONE
Director inițial (HOMEDIR)	*USRPRF	*USRPRF
Autorizare (AUT)	*EXCLUDE	*EXCLUDE
Auditare acțiune (AUDLVL) ³	*NONE	*NONE
Auditare obiect (OBLAUD) ³	*NONE	*NONE

¹ Când nivelul de securitate sistem este modificat de la nivelul 10 sau 20 la nivelul 30 sau mai sus, această valoare este înlăturată.

² Când un profil utilizator este automat creat cu nivelul de securitate 10, clasa utilizator *USER dă autorizare specială *ALLOBJ și *SAVSYS.

³ Auditarea de obiecte și acțiuni este specificată folosind comanda CHGUSRAUD.

⁴ Când executați o comandă CRTUSRPRF, nu puteți 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 disc independent este mutat în alt sistem, autorizarea particulară, dreptul de proprietate asupra obiectului și intrările de grup primar vor fi atașate la profilul cu același nume din sistemul destinație. Dacă un profil nu exista pe sistemul destinație, va fi creat un profil. Utilizatorul nu va avea nici o autorizare specială și parola va fi setată la *NONE.

Tabela 144. Profiluri utilizator livrate de IBM

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QADSM	Profil utilizator ADSM	<ul style="list-style-type: none"> • USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: Profil ADSM folosit de serverul ADSM • SPCAUT: *JOBCTL, *SAVSYS • JOB: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	Profil utilizator APD	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *JOBCTL • JOB: QADSM/QADSM • TEXT: Profil utilizator intern APD
QAFUSR	Profil utilizator APD	<ul style="list-style-type: none"> • TEXT: Profil utilizator intern APD
QAFDFTUSR	Profil utilizator APD	<ul style="list-style-type: none"> • INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Profil utilizator intern APD
QAUTPROF	Profil utilizator autorizare IBM	
QBRMS	Profil utilizator BRM	
QCLUMGT	Profil gestiune cluster	<ul style="list-style-type: none"> • STARE: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	Profil cluster disponibilitate înaltă	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG
QCOLSRV	Profil utilizator servicii de colectare Administrare centrală	
QDBSHR	Profil partajare bază de date	<ul style="list-style-type: none"> • AUT: *ADD, *DELETE
QDBSHRDO	Profil partajare bază de date	<ul style="list-style-type: none"> • AUT: *ADD, *DELETE
QDFTOWN	Profil proprietar implicit	<ul style="list-style-type: none"> • PLYLMT: 3
QDIRSRV	Profilul utilizator server i5/OS Directory Server	<ul style="list-style-type: none"> • LMTCPB: *YES • JOB: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
QDLFM	Profil manager fișiere legături de date	<ul style="list-style-type: none"> • SRTSEQ: *HEX
QDOC	Profil document	<ul style="list-style-type: none"> • AUT: *CHANGE
QDSNX	Profil executiv nod sisteme distribuite	<ul style="list-style-type: none"> • PLYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QEJBSVR	Profil utilizator WebSphere Application Server	
QEJB	Profil utilizator Enterprise Java	
QFNC	Profil Finanțe	<ul style="list-style-type: none"> • PTYLMT: 3
QGATE	Profil punte VM/MVS*	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QIPP	Profil tipărire internet	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QIPP
QLPAUTO	Profil instalare automată program cu licență	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Profil instalare program cu licență	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG
QMGC	Profil Administrare centrală	<ul style="list-style-type: none"> • JOBID: QSYS/QYPSJOBID
QMSF	Profil cadru de lucru server de mail	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QMQM	Profil utilizator MQSeries	<ul style="list-style-type: none"> • USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: Utilizator MQM care deține biblioteca QMQM
QNFSANON	Profil utilizator NFS	
QNETSPLF	Profil de spool rețea	
QNETWARE	Profil utilizator ECS	<ul style="list-style-type: none"> • STARE: *DISABLED • TEXT: QFPNTWE USER PROFILE
QNTTP	Profil timp rețea	<ul style="list-style-type: none"> • JOBID: QTOTNTP • JOBID LIBRARY: QSYS
QOIUSER	Subsistem comunicații OSI	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG • CURLIB: QOSI • MSGQ: QOSI/QOIUSER • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profil utilizator subsistem de comunicații intern OSI

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QOSIFS	Profil utilizator server fișiere OSI	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Profil utilizator servicii fișiere intern OSI
QPGMR	Profil programator	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Profil utilizator Performance Explorer	<ul style="list-style-type: none"> • PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: Profil utilizator livrat de IBM
QPM400	IBM Performance Management pentru eServer iSeries (PM iSeries)	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Profil utilizator proprietar de proiecte și părți	<ul style="list-style-type: none"> • STARE: *DISABLED • CURLIB: QADM • TEXT: Profilul utilizator al proprietarului de proiecte și părți
QRDARSADM	Profil utilizator R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • TEXT: Profil administrație R/DARS
QRDAR	Profil de proprietar R/DARS	<ul style="list-style-type: none"> • USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: Profil proprietar R/DARS-400
QRDARS4001	Profil proprietar 1 R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 1 R/DARS-400
QRDARS4002	Profil proprietar 2 R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 2 R/DARS-400
QRDARS4003	Profil proprietar 3 R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 3 R/DARS-400
QRDARS4004	Profil proprietar 4 R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 4 R/DARS-400

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QRDARS4005	Profil proprietar 5 R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 5 R/DARS-400
QRMTCAL	Profil utilizator Calendar la distanță	<ul style="list-style-type: none"> • TEXT: Utilizator Calendar la distanță OfficeVision
QRJE	Profil intrare job la distanță	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ ¹ *SAVSYS ¹ *JOBCTL
QSECOFR	Profil responsabil cu securitatea	<ul style="list-style-type: none"> • PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PAROLĂ: QSECOFR
QSNADS	Profil servicii distribuție SNA	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QSOC	Profil utilizator OptiConnect	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Profil spool	
QSPLJOB	Profil job spool	<ul style="list-style-type: none"> • AUT: *USE
QSRV	Profil service	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ ¹, *SAVSYS ¹, *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profil utilizator agent service	
QSRVBAS	Profil service de bază	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ ¹ *SAVSYS ¹ *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Profil utilizator CC Server	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator CC Server
QSVCM	Profil utilizator Client Management Server	<ul style="list-style-type: none"> • TEXT: Profil utilizator Client Management Server

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QSVSM	Profil utilizator ECS	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • STARE: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator Manager sistem SystemView
QSVSMSS	Profil utilizator Managed System Service	<ul style="list-style-type: none"> • STARE: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator Managed System Service
QSYS	Profil sistem	<ul style="list-style-type: none"> • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG
QSYSOPR	Profil operator sistem	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *ALLOBJ¹, *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Profil TCM (Triggered Cache Manager)	<ul style="list-style-type: none"> • STARE: *DISABLED
QTCP	Profil TCP (Transmission control protocol)	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Profil TFTP (Trivial File Transfer Protocol)	
QTMPLPD	Profil suport tipărire TCP/IP	<ul style="list-style-type: none"> • PTYLMT: 3 • AUT: *USE
QTMPLPD	Profil utilizator LPR la distanță	<ul style="list-style-type: none"> • JOBID: QGPL/QDFTJOBID • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD
QTMTWSG	Profil utilizator HTML Workstation Gateway	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMTWSG • TEXT: Profil HTML Workstation Gateway
QTMHHTTP	Profil utilizator HTML Workstation Gateway	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil server HTTP
QTMHHTTP1	Profil utilizator HTML Workstation Gateway	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil CGI server HTTP
QTSTRQS	Profil cerere test	
QUMB	Profil utilizator Ultimedia System Facilities	

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiți din valorile implicite
QUMVUSER	Profil utilizator Ultimedia Business Conferencing	
QUSER	Profil utilizator stație de lucru	<ul style="list-style-type: none"> • PTYLMT: 3
QX400	Profil utilizator servicii fișier servicii mesaje OSI	<ul style="list-style-type: none"> • CURLIB: *QX400 • USRCLS: *SYSOPR • MSGQ: QX400/QX400 • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profil utilizator servicii mesaje interne OSI
QYCMCIMOM	Profil utilizator server	
QYPSJSVR	Profil server Administrare centrală Java	
QYPUOWN	Profil utilizator intern APU	<ul style="list-style-type: none"> • TEXT: Profil utilizator — Internal APU

¹ Când nivelul de securitate sistem este modificat de la nivelul 10 sau 20 la nivelul 30 sau mai sus, această valoare este înlăturată.

Anexa C. Comenzile livrate cu autorizarea publică *EXCLUDE

Tabela 145 identifică acele comenzi care au autorizare restricționată (autorizarea publică este *EXCLUDE) când sistemul dumneavoastră este livrat. Arată ce profiluri utilizator livrate de IBM sunt autorizate să folosească aceste comenzi restricționate. Pentru mai multe detalii despre profilurile utilizator, vedeți subiectul “Profilurile de utilizator furnizate de IBM” la pagina 108.

În Tabela 145, comenzile care sunt restricționate pentru responsabilul cu securitatea și pentru orice profil utilizator cu autorizare *ALLOBJ au un **R** în profilul QSECOFR. Comenzile care sunt autorizate special unuia sau mai multor profiluri utilizator livrate de IBM, în plus față de responsabilul cu securitatea, au un **S** sub numele de profil pentru care sunt autorizate.

Orice comenzi care nu sunt menționate aici sunt publice, ceea ce înseamnă că ele pot fi folosite de către toți utilizatorii. Oricum, unele comenzi necesită autorizare specială, precum *SERVICE sau *JOBCTL. Autorizările speciale necesare pentru o comandă sunt menționate în Anexa D, “Autorizarea cerută pentru obiectele folosite de comenzi”, la pagina 299

Dacă alegeți să acordați altor utilizatori sau autorizare publică *USE acestor comenzi, actualizați această tabelă pentru a indica ieșirea din starea restricționată pe sistemul dumneavoastră. Folosirea unor comenzi poate necesita autorizarea la anumite obiecte din sistem precum și la comenzile respective. Vedeți Anexa D, “Autorizarea cerută pentru obiectele folosite de comenzi”, la pagina 299 pentru autorizările de obiect necesare pentru comenzi.

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDCLUNODE	R				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	R				
ADDCRGNODE	R				
ADDCRSDMNK	R				
ADDDEVDMNE	R				
ADDSTQ		S	S		
ADDSTRTE		S	S		
ADDSTSYSN		S	S		
ADDEXITPGM	R				
ADDIMGCLGE	R				
ADDMFS	R				
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZPFRDTA	R				
ANZPGM	R				
ANZPRB		S	S	S	S
ANZPRFACT	R				
ANZS34OCL	R				
ANZS36OCL	R				
APYJRNCHG		S		S	
APYPTF				S	
APYRMTPTF		S	S	S	S
CFGDSTSRV		S	S		
CFGRPDS		S	S		
CFGSYSSEC	R				
CHGACTSCDE	R				
CHGASPA	R				
CHGCLUCFG	R				
CHGCLUNODE	R				
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDSTPWD ¹	R				
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
CHGGPHPKG	R				
CHGIMGCLG	R				
CHGIMGCLGE	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	S	S	
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	R				
CHGNETA	R				
CHGNETJOBE	R				
CHGNFSEXP	R				
CHGNWSA	R				
I 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	
CHKPRDOPT		S	S	S	S
CPHDTA	R				
CPYFCNARA	R				
CPYGPHFMT	R				
CPYGPHPKG	R				
CPYPFRDTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
I CRTADMDMN	R				
CRTAUTHLR	R				
CRTBESTMDL	R				
CRTCLS	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTIMGCLG	R				
CRTJOB	R				
I CRTNWSCFG	R				
CRTPFRTA	R				
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				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36CFG	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS36QRY	R				
CVTS38JOB	R				
CVTTCPL		S	S	S	S
I DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
I DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				
DLTGPHPKG	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DLTHSTDTA	R				
DLTIMGCLG	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
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
DMPYSOBY		S	S	S	S
DMPTRC	R	S		S	
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMFSINF	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				
DSPPFRTA	R				
DSPPFRGPH	R				
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
DSPUDFS	R				
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				
ENCTOMSTK	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ENDASPBAL	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDHOSTSVR		S	S	S	S
ENDIDXMN	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDNFSSVR	R		S	S	S
ENDPEX		S		S	
ENDPFRTRC	R			S	
ENDSRVJOB		S	S	S	S
ENDSYMGR		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				
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF ³				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				
LODIMGCLG	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

	Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
	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				
	PRTJOBTRPT	R				
	PRTJOBTRC	R				
	PRTLCKRPT	R				
	PRTPOLRPT	R				
	PRTRSCRPT	R				
	PRTSYSRPT	R				
	PRTTNSRPT	R				
	PRTTRCRPT	R				
	PRTDSKINF	R				
	PRERRLOG		S	S	S	S
	PRTINTDTA		S	S	S	S
	PRTPRFINT	R				
	PWRDWN SYS	R		S		
	RCLDBXREF	R				
	RCLOBJOWN	R				
	RCLOPT	R				
	RCLSPLSTG		S	S	S	S
	RCLSTG		S	S	S	S
	RCLTMPSTG		S	S	S	S

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
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				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVEXITPGM	R				
RMVIMGCLGE	R				
RMVJRNCHG		S		S	
RMVLANADP	R				
RMVMFS	R				
RMVNETJOBE	R				
RMVOPTCTG	R				
RMVOPTSVR	R				
RMVPEXDFN		S		S	
RMVPEXFTR		S		S	
RMVPTF				S	
RMVRMTPTF		S	S	S	S
RMVRPYLE		S			
RMVTRCFTR	R				
RSTAUT	R				
RST ⁴					
RSTCFG	R				
RSTDLO	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ ⁴					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				
RSTUSFCNR ⁵					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RSTUSRPRF	R				
RTVDSKINF	R				
I RTVIMGCLG	R				
RTVPRD		S	S	S	S
RTVPTF		S	S	S	S
RTVSMGOBJ		S	S	S	S
RUNLPDA		S	S	S	S
RUNSMGCMD		S	S	S	S
RUNSMGOBJ		S	S	S	S
RVKPUBAUT	R				
SAVAPARDTA		S	S	S	S
SAVLICPGM	R				
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
I STRASPBAL	R				
STRBEST	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJOBTRC	R				
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF ²			S	S	S
STRNFSSVR	R				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	R				
STRSRVJOB		S	S	S	S
STRSST				S	
STRSYSMGR		S	S	S	S
STRS36MGR	R				
STRS38MGR	R				
STRTCP		S	S	S	S
STRTCPIFC		S	S	S	S
STRTCP SVR		S	S	S	S
STRUPDIDX	R				
STRWCH	R				
TRCASPBAL	R				
TRCCPIC	R				
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	R				
UPDPTFINF	R				
VFYCMN		S	S	S	S
VFYIMGCLG	R				
VFYLNKLPDA		S	S	S	S
VFYMSTK	R				
VFYPIN	R				
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKCN TINF				S	S
WRKDEVTBL	R				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFCNARA	R				
WRKIMGCLGE	R				
WRKJRN		S	S	S	
WRKLIB					
WRKLIBPDM					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricționate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
WRKLCINF	R				
I WRKNWSCFG	R				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
I WRKTRC	R				
WRKTXIDX	R				
WRKUSRTBL	R				
I WRKWCH	R				
¹	Comanda CHGDSTPWD este livrată cu autorizare publică *USE, dar trebuie să fiți semnat ca QSECOFR pentru a folosi această comandă.				
²	Profilul utilizator QMSF este de asemenea autorizat la această comandă.				
³	QSRV poate să ruleze această comandă doar dacă nu se face un IPL.				
⁴	În plus la QSYS, profilul utilizator QRDARS400 are autorizare.				
⁵	În plus la QSYS, profilul utilizator QUMB are autorizare.				

Anexa D. Autorizarea cerută pentru obiectele folosite de comenzi

Tabelele din această anexă arată ce autorizare este necesară pentru obiectele referite de către comenzi. De exemplu, în intrarea pentru comanda CHGUSRPRF (Change User Profile - Modificare profil utilizator), tabela prezintă toate obiectele pentru care aveți nevoie de autorizare, cum ar fi coada de mesaje a utilizatorului, descrierea de job și programul inițial.

Tabelele sunt organizate în ordine alfabetică după tipul obiectului. În plus, sunt incluse tabele pentru elemente care nu sunt obiecte i5/OS (joburi, fișiere spool, atribute de rețea și valori de sistem) și pentru unele funcții (de emulare dispozitiv și financiare). Considerațiile suplimentare (dacă există) pentru comenzi sunt incluse ca note de subsol în tabel.

În continuare sunt descrise coloanele din tabele:

Obiect referențiat

Obiectele prezentate în coloana *Obiect referit* sunt obiectele pentru care utilizatorul are nevoie de autorizare pentru folosirea comenzii.

Autorizarea cerută pentru obiect

Autorizările specificate în tabele arată autorizările pentru obiect și autorizările pentru date care sunt necesare pentru obiect când folosiți comanda. Tabela următoare prezintă autorizările specificate în coloana *Autorizare necesară*. Descrierea include exemple ale modului în care este folosită autorizarea. În majoritatea cazurilor, accesarea unui obiect necesită o combinație de autorizări pentru obiect și pentru date.

Autorizarea cerută pentru bibliotecă

Această coloană arată ce autorizare este necesară pentru biblioteca în care se află obiectul. Pentru majoritatea operațiilor, este necesară autorizarea *EXECUTE pentru a localiza obiectul în bibliotecă. Pentru adăugarea unui obiect în bibliotecă sunt necesare autorizările *READ și *ADD. Această tabelă prezintă autorizările specificate în coloana *Autorizare necesară*.

Tabela 146. Descriere tipuri de autorizare

Autorizare	Nume	Funcții permise
<i>Autorizări obiect:</i>		
*OBJOPR	Operațional obiect	Vedeți descrierea unui obiect. Folosiți obiectul așa cum este determinat de către autorizările de date ale utilizatorului.
*OBJMGT	Gestionare obiect	Specificarea securității pentru un obiect. Mutați sau redenumiți obiectul. Toate funcțiile definite pentru *OBJALTER și *OBJREF.
*OBJEXIST	Existență obiect	Ștergere obiect. Eliberează spațiul ocupat de obiect. Efectuați operații de salvare și de restaurare a obiectului ¹ . Transfer proprietate asupra obiectului.
*OBJALTER	Transformare obiect	Adăugare, ștergere, inițializare și reorganizare membri ai fișierelor bază de date. Modificare și adăugare atribute ale fișierelor bază de date: adăugare și ștergere declanșatori. Modificarea atributelor pachetelor SQL. Mutarea bibliotecii sau folderului la un alt ASP.

Autorizarea cerută pentru bibliotecă

Tabela 146. Descriere tipuri de autorizare (continuare)

Autorizare	Nume	Funcții permise
*OBJREF	Referință obiect	Specificați un fișier bază de date ca părinte într-o restricție referențiale. De exemplu, vreți să definiți o regulă conform căreia trebuie să existe o înregistrare despre client în fișierul CUSMAS înainte să poată fi adăugată o comandă pentru ale client în fișierul CUSORD. Vă trebuie autorizarea *OBJREF pentru fișierul CUSMAS pentru a defini această regulă.
*AUTLMGT	Gestionare listă autorizații	Adăugați și eliminați utilizatori și autorizările lor din lista de autorizare ² .
<i>Autorizări date:</i>		
*READ	Citire	Afișarea conținutului obiectului, precum vizualizarea înregistrărilor dintr-un fișier.
*ADD	Adăugare	Adăugare intrări la un obiect, precum adăugarea de mesaje la o coadă de mesaje sau adăugarea de înregistrări la un fișier.
*UPD	Update - Actualizare	Modificarea intrărilor dintr-un obiect, precum este modificarea înregistrărilor dintr-un fișier.
*DLT	Ștergere	Ștergerea intrărilor dintr-un obiect, precum ștergerea mesajelor dintr-o coadă de mesaje sau ștergerea înregistrărilor dintr-un fișier.
*EXECUTE	Executare	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 existență obiect pentru a efectua operații de salvare și restaurare asupra obiectului.	
²	Pentru informații suplimentare, consultați Referințe de securitate iSeries.	

În plus față de aceste valori, coloanele *Autorizare necesară* ale tabelului pot arăta subseturi definite de sistem ale acestor autorizări. Tabela următoare prezintă subseturile autorizărilor pentru obiect și autorizărilor pentru date.

Tabela 147. Autorizare definită de sistem

Autorizare	*ALL	*CHANGE	*USE	*EXCLUDE
<i>Autorizări obiect</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Autorizări de date</i>				
*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 și WRKAUT.

Tabela 148. Autorizare definită de sistem

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Autorizări obiect</i>							

Tabela 148. Autorizare definită de sistem (continuare)

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
<i>Autorizări pentru date</i>							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Pentru informații suplimentare despre aceste autorizări și descrierile lor, consultați Referințe de securitate iSeries.

Presupuneri privind utilizarea comenzii

1. Pentru a folosi o comandă, este necesară autorizarea *USE pentru comanda respectivă. Această autorizare nu este menționată în tabele.
2. Pentru a introduce o comandă de afișare, aveți nevoie de autorizare de operare pentru fișierul de afișare furnizat de IBM, fișierul de ieșire pentru imprimantă sau grupul de panouri folosit de comandă. Aceste fișiere și grupuri de panouri sunt livrate cu autorizarea publică *USE.

Reguli generale privind autorizările pentru obiecte cerute de comenzi

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Modificare (CHG) cu F4 (Prompt) ⁷	Valori curente	Valorile curente sunt afișate 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	
Creare obiect în director	Directoarele din prefix cale	*X	
	Directorul care va conține obiecte noi	*WX	

Reguli generale privind autorizările pentru obiecte cerute de comenzi

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Copiere (CPY) unde fișierul în care se va copia este un fișier bază de date	Obiectul de copiat	*OBJOPR, *READ	*EXECUTE
	Comanda CRTPF, dacă se specifică CRTFILE (*YES)	*OBJOPR	*EXECUTE
	Fișier-destinație, dacă se specifică CRTFILE (*YES) ¹		*ADD, *EXECUTE
	Fișier-destinație, dacă el există și se adaugă un nou membru	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	Fișier-destinație, dacă el și membrul există și se specifică opțiunea *ADD	*OBJOPR, *ADD	*EXECUTE
	Fișier-destinație, dacă el și membrul există și se specifică opțiunea *REPLACE	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fișier-destinație, dacă el există, este adăugat un nou membru și este specificată opțiunea *UPDADD. ⁸	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
Creare (CRT)	Obiectul care va fi creat ²		*READ, *ADD
	Profilul utilizator care va deține obiectul creat (fie profilul utilizator care rulează jobul, fie profilul de grup al utilizatorului)	*ADD	
Creare (CRT) dacă se specifică REPLACE(*YES) ^{6, 9}	Obiectul care va fi creat (și înlocuit) ²	*OBJMGT, *OBJEXIST, *READ ⁵	*READ, *ADD
	Profilul de utilizator care va deține obiectul creat (fie profilul de utilizator care rulează jobul, fie profilul de grup al utilizatorului)	*ADD	
Afișare (DSP) sau altă operație care folosește fișierul ieșire (OUTPUT(*OUTFILE))	Obiectul care va fi afișat	*USE	*EXECUTE
	Fișierul de ieșire, dacă fișierul nu există ³		*ADD, *EXECUTE
	Fișierul de ieșire, dacă fișierul există și este adăugat un membru nou și dacă este specificată opțiunea *REPLACE și membrul nu există	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Fișierul de ieșire, dacă fișierul există și este adăugat un membru nou și dacă este specificată opțiunea *ADD și membrul nu există	OBJOPR, *OBJMGT sau *OBJALTER, *ADD	*ADD, *EXECUTE
	Fișier-destinație, dacă el și membrul există și se specifică opțiunea *ADD	*OBJOPR, *ADD	*EXECUTE
	Fișier-destinație, dacă el și membrul există și se specifică opțiunea *REPLACE	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*EXECUTE
	Fișier format (QAxxxx), dacă fișierul ieșire nu există	*OBJOPR	
Afișare (DSP) folosind *PRINT sau Lucru (WRK) folosind *PRINT	Obiectul care va fi afișat	*USE	*EXECUTE
	Coadă de ieșire ⁴	*READ	*EXECUTE
	Fișier imprimantă (QPxxxx în QSYS)	*USE	*EXECUTE
Salvare (SAV) sau altă operație care folosește descriere dispozitiv	Descriere dispozitiv	*USE	*EXECUTE
	Fișierul dispozitiv asociat cu descrierea dispozitivului, cum ar fi QSYSTAP pentru descrierea dispozitivului TAP01	*USE	*EXECUTE

Reguli generale privind autorizările pentru obiecte cerute de comenzi

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
1	Profilul utilizator care rulează comanda de copiere devine proprietarul fișierului-destinație, doar dacă utilizatorul nu este membru al unui profil de grup și are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fișierului destinație. În acest caz, utilizatorul care rulează comanda trebuie să aibă autorizarea *ADD pentru profilul de grup și autorizarea de a adăuga un membru și de a scrie date în noul fișier. Fișierului destinație îi este dată aceeași autorizare publică, autorizare de grup primar, autorizările private și listă de autorizare, ca și fișierului sursă.		
2	Profilul utilizator care rulează comanda de creare devine proprietarul noului obiect creat, doar dacă utilizatorul nu este membru al unui profil de grup și are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fișierului nou creat. Autorizarea publică pentru obiect este controlată de parametrul AUT.		
3	Profilul utilizator care rulează comanda de afișare devine proprietarul noului fișier ieșire creat, doar dacă utilizatorul nu este membru al unui profil de grup și are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fișierului de ieșire. Autorizarea publică pentru fișierul ieșire este controlată de parametrul CRTAUT al bibliotecii fișierului de ieșire.		
4	Dacă coada de ieșire este definită ca OPRCTL (*YES), un utilizator cu autorizarea specială *JOBCTL nu are nevoie de nici o autorizare pentru ea. Un utilizator cu autorizarea specială *SPLCTL nu are nevoie de nici o autorizare pentru coada de ieșire.		
5	Pentru fișiere 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 funcțională din meniul de programare pentru a șterge obiectul curent.		
7	E necesară de asemenea autorizare pentru comanda corespunzătoare (DSP).		
8	Opțiunea *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

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Tabela 149. Comenzi comune pentru majoritatea obiectelor

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ALCOBJ ^{1,2,11}	Obiect	*OBJOPR	*EXECUTE
ANZUSROBJ ²⁰			
CHGOBJAUD ¹⁸	Dispozitiv ASP (dacă este specificat)	*USE	
CHGOBJD ³	Obiect, dacă este un fișier	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect, dacă este un fișier	*OBJMGT	*EXECUTE

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGOBJOWN ^{3,4}	Obiect	*OBJEXIST	*EXECUTE
	Obiect (dacă avem fișier, bibliotecă, descriere subsistem)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiect (dacă este *AUTL)	Drept de proprietate sau *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	*EXECUTE
	Profil utilizator nou	*ADD	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	
CHGOBJPGP ³	Obiect	*OBJEXIST	*EXECUTE
	Obiect (dacă avem fișier, bibliotecă, descriere subsistem)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiect (dacă este *AUTL)	Drept de proprietate și *OBJEXIST sau *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	
	Profil utilizator nou	*ADD	
	Dispozitiv ASP (dacă este specificat)	*USE	
CHKOBJ ³	Obiect	Autorizare specificată de parametrul AUT ¹⁴	*EXECUTE
CPROBJ	Obiect	*OBJMGT	*EXECUTE
CHKOBJITG ^{11(Q)}			
CRTDUPOBJ ^{3,9,11,21}	Obiect nou		*USE, *ADD
	Obiectul copiat, dacă este *AUTL	*AUTLMGT	*USE, *ADD
	Obiect ce este copiat, toate celelalte tipuri	*OBJMGT, *USE	*USE
	comanda CRTSAVF (dacă obiectul este un fișier 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 informațiile de autorizare)	autorizare specială sau drept de proprietate *OBJMGT sau *ALLOBJ	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
	Dispozitiv ASP (dacă este specificat)	*USE	
DSPOBJD ^{2,28}	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
	Obiect	O autorizare, alta decât *EXCLUDE	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*EXECUTE	

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
EDTOBJAUT ^{3,5,6,15}	Obiect	*OBJMGT	*EXECUTE
	Obiect (dacă avem fișier)	*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 fișier)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, dacă s-a folosit pentru a securiza obiectul	Non *EXCLUDE	
	Dispozitiv ASP (dacă este specificat)	*USE	
	Dispozitiv ASP referință (dacă este specificat)	*EXECUTE	
	Obiect referință	*OBJMGT sau drept de proprietate	*EXECUTE
MOV OBJ ^{3,7,12}	Obiect	*OBJMGT	
	Obiect (dacă avem *FILE)	*ADD, *DLT, *EXECUTE	
	Obiect (nu *FILE),	*DLT, *EXECUTE	
	Bibliotecă sursă		*CHANGE
	Bibliotecă destinație		*READ, *ADD
	Dispozitiv ASP (dacă este specificat)	*USE	
PRTADPOBJ ^{26(Q)}			
P RTPUBAUT ²⁶			
PRTUSROBJ ²⁶			
P RTPVTAUT ²⁶			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Obiect	*OBJMGT	*EXECUTE
RNMOBJ ^{3,11}	Obiect	*OBJMGT	*UPD, *EXECUTE
	Obiect, dacă este *AUTL	*AUTLMGT	*EXECUTE
	Obiect (dacă avem *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RSTOBJ ^{3,13} (Q)	Obiect, dacă există deja în bibliotecă	*OBJEXIST ⁸	*EXECUTE, *ADD
	Obiect, dacă este *CFGL, *CNL, *CTLD, *DEVD, *LIND, sau *NWID	*CHANGE și *OBJMGT	*EXECUTE
	Definiție mediu de stocare	*USE	*EXECUTE
	Cozile de mesaje care sunt restaurate în bibliotecă unde există deja	*OBJOPR, *OBJEXIST ⁸	*EXECUTE, *ADD
	Profilul utilizator deține obiectele care sunt create	*ADD ⁸	
	Program care adoptă autorizare	Proprietar sau autorizare specială *SECADM și *ALLOBJ	*EXECUTE
	Bibliotecă destinație	*EXECUTE, *ADD ⁸	
	Bibliotecă pentru obiect salvat dacă VOL(*SAVVOL) este specificat	*USE ⁸	
	Fișier de salvare	*USE	*EXECUTE
RSTOBJ ^{3,13} (Q)	Unitate de bandă, unitate de dischetă sau unitate optică	*USE	*EXECUTE
	Fișier bandă (QSYSTAP) sau fișier dischetă (QSYSDKT)	*USE ⁸	*EXECUTE
	Fișier optic (OPTFILE) ²²	*R	Nu se aplică
	Director părinte sau fișier optic (OPTFILE) ²²	*X	Nu se aplică
	Prefix cale OPTFILE ²²	*X	Nu se aplică
	Volume optic ²⁴	*USE	Nu se aplică
	Ieșire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul referință de câmp QSYS/QASRRSTO pentru fișierul de ieșire, dacă un fișier de ieșire este specificat și nu există.	*USE	*EXECUTE
Descriere de dispozitiv ASP ²⁵	*USE		
RSTSYSINF	Fișier de salvare	*USE	*EXECUTE
	Unitate de bandă, unitate de dischetă sau unitate optică	*USE	*EXECUTE
	Fișier optic (OPTFILE) ²²	*R	N/A
	Director părinte sau fișier optic (OPTFILE) ²²	*X	N/A
	Prefix cale OPTFILE ²²	*X	N/A
	Volume optic ²⁴	*USE	N/A
RVKPUBAUT ²⁰	Fișier bandă (QSYSTAP) sau fișier dischetă (QSYSDKT)	*USE ⁸	*EXECUTE
RTVOBJD ^{2, 29}	Obiect	O autorizare alta decât *EXCLUDE	*EXECUTE

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RVKOBJAUT ^{3,5,15,27}	Prefix cale OPTFILE ²²	*X	Nu se aplică
	Volume optic ²⁴	*USE	Nu se aplică
	Ieșire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	
SAVCHGOBJ ³	Obiect (8)	*OBJEXIST	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
	Coadă de mesaje salvare active	*OBJOPR, *ADD	*EXECUTE
	Spațiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE
SAVCHGOBJ ³	Fișier optic (OPTFILE) ²²	*RW	Nu se aplică
	Director părinte sau fișier optic (OPTFILE) ²²	*WX	Nu se aplică
	Prefix cale sau fișier optic (OPTFILE) ²²	*X	Nu se aplică
	Director rădăcină (/) al volumului optic ^{22, 23}	*RWX	Nu se aplică
	Volume optic ²⁴	*CHANGE	
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul referință de câmp QSYS/QASAVOBJ pentru fișierul de ieșire, dacă un fișier de ieșire este specificat și nu există.	*USE ⁸	*EXECUTE
	Ieșire imprimantă QSYS/QPSAVOBJ	*USE ⁸	*EXECUTE
	Descriere de dispozitiv ASP ²⁵	*USE	
SAVOBJ ³	Obiect	*OBJEXIST ⁸	*EXECUTE
	Definiție mediu de stocare	*USE	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
	Coadă de mesaje salvare active	*OBJOPR, *ADD	*EXECUTE
	Spațiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SAVOBJ ³	Fișier optic (OPTFILE) ²²	*RW	Nu se aplică
	Director părinte sau fișier optic (OPTFILE) ²²	*WX	Nu se aplică
	Prefix cale OPTFILE ²²	*X	Nu se aplică
	Director rădăcină (/) al volumului optic ^{22, 23}	*RWX	Nu se aplică
	Volume optic ²⁴	*CHANGE	
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul referință de câmp QSYS/QASAVOBJ pentru fișierul de ieșire, dacă un fișier de ieșire este specificat și nu există.	*USE ⁸	*EXECUTE
	Ieșire 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	Nu se aplică
	Volume optic ²⁴	*CHANGE	Nu se aplică
SAVSYSINF	Definiție mediu de stocare	*USE	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
	Fișier optic (OPTFILE) ²²	*RW	N/A
	Director părinte sau fișier optic (OPTFILE) ²²	*WX	N/A
	Prefix cale OPTFILE ²²	*X	N/A
	Director rădăcină (/) al volumului optic ^{22, 23}	*RWX	N/A
	Volume optic ²⁴	*CHANGE	
SAVRSTCHG	Pe sistemul sursă, aceeași autorizare precum se cere prin comanda SAVCHGOBJ.		
	Pe sistemul destinație, aceeași autorizare precum se cere prin comanda RSTOBJ.		
	Descriere de dispozitiv ASP ²⁵	*USE	
SAVRSTOBJ	Pe sistemul sursă, aceeași autorizare precum se cere prin comanda SAVOBJ.		
	Pe sistemul destinație, aceeași autorizare precum se cere prin comanda RSTOBJ.		
	Descriere de dispozitiv ASP ²⁵	*USE	
SETOBJACC	Obiect	*OBJOPR	*EXECUTE
STROBJCVN (Q) ³⁰			
WRKOBJ ¹⁹	Obiect	Orice autorizație	*USE
WRKOBJLCK	Obiect		*EXECUTE
	Dispozitiv ASP	*EXECUTE	

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
WRKOBJOWN ¹⁷	Profil utilizator	*READ	*EXECUTE
WRKOBJPGP ¹⁷	Profil utilizator	*READ	*EXECUTE
WRKOBJPVT ¹⁷	Profil utilizator	*READ	*EXECUTE
1	Vedeți cuvântul cheie OBJTYPE al comenzii ALCOBJ pentru lista de tipuri de obiecte care pot fi alocate și dezalocate.		
2	Aceași autorizare pentru obiectul (altul când *EXCLUDE) este cerut.		
3	Această comandă nu poate fi utilizată pentru documente sau fișiere. Folosiți comanda echivalentă DLO (Document Library Object - Obiect bibliotecă document).		
4	Trebuie să aveți autorizarea specială *ALLOBJ și *SECADM pentru a modifica proprietarul obiect al unui program, programul service sau pachetul SQL care adoptă autorizarea.		
5	Trebuie să fiți proprietar sau să aveți autorizarea *OBJMGT și autorizările care sunt acordate sau revocate.		
6	Trebuie să fiți proprietarul sau să aveți autorizarea specială *ALLOBJ pentru a garanta autorizarea *OBJMGT sau *AUTLMGT.		
7	Această comandă nu poate fi utilizată pentru profiluri utilizator, descrieri de controller, descrieri de dispozitiv, descrieri linie, documente, biblioteci documente și fișiere.		
8	Dacă aveți autorizarea specială *SAVSYS, nu aveți nevoie de autorizarea specificată.		
9	Dacă utilizatorul rulează comanda CRTDUPOBJ are profilul utilizator OWNER(*GRPPRF), proprietarul unui obiect nou este profilul grup. Pentru a copia cu succes autorizările la un nou obiect deținut de un profil grup, au loc următoarele:		
	<ul style="list-style-type: none"> • Utilizatorul ce rulează comanda trebuie să aibă autorizare pentru obiectul sursă. Autorizările pot fi obținute prin adoptarea autorizării sau prin profilul de grup. • Dacă apare o eroare în timpul copierii autorizărilor pentru noul obiect, noul obiect creat este șters. 		
10	Trebuie să aveți autorizarea specială *SAVSYS.		
11	Această comandă nu poate fi utilizată pentru jurnale și receptori jurnale.		
12	Această comandă poate fi utilizată pentru jurnale și receptori jurnale, doar dacă bibliotecă-sursă este QRCL și bibliotecă-destinație este bibliotecă originală pentru jurnal sau receptorii jurnal.		
13	Trebuie să aveți 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 aveți autorizarea pe care o verificați. De exemplu, pentru a verifica dacă un utilizator are autorizarea *OBJEXIST pentru FILEB, trebuie să aveți 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 îndepliniți una dintre următoarele condiții:		
	<ul style="list-style-type: none"> • Să dețineți obiectul. • Să aveți autorizarea *ALL pentru obiect. • Să aveți autorizarea specială *ALLOBJ. 		
16	Dacă și fișierul original și fișierul redenumit are un deținător de autorizare asociată, autorizarea *ALL pentru deținătorul de autorizare este cerută.		
17	Această comandă nu suportă sistemul fișier QOPT.		
18	Trebuie să aveți autorizația specială *AUDIT.		
19	Pentru a folosi o operație individuală, trebuie să aveți autorizarea cerută de operația individuală.		
20	Trebuie să aveți autorizarea specială *ALLOBJ.		

Comenzi comune pentru majoritatea obiectelor

Tabela 149. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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 (GRPAUTYP) din profilul utilizator care rulează comanda. Dacă obiectul-sursă are un grup primar, noul obiect este posibil să nu aibă același grup primar, dar autorizarea pe care o are grupul primar asupra obiectului-sursă va fi duplicată la noul obiect.		
22	Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (format disc universal).		
23	Această verificare de autorizare este făcută doar când ștergeți volumul optic.		
24	Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția de suport optic.		
25	Autorizarea este necesară doar dacă operația de salvare sau restaurare necesită o comutare a spațiului de nume de bibliotecă.		
26	Trebuie să aveți autorizația 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 situație în care utilizatorul să aibă mai multe autorizări decât înainte de operația de revocare. Dacă utilizatorul are autorizarea *USE pentru un obiect și *CHANGE pentru lista de autorizare care securizează obiectul, revocarea autorizării *USE face ca utilizatorul să aibă autorizarea *CHANGE pentru obiect.		
28	Trebuie să aveți autorizarea specială *ALLOBJ sau *AUDIT pentru a fi afișată valoarea curentă de auditare a obiectului. În caz contrar va fi afișată valoarea *NOTAVL, pentru a indica faptul că valoarea nu este disponibilă pentru afișare.		
29	Trebuie să aveți 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	Vedeți comenzile CHGPGM, CHGSRVPGM și CHGMOD pentru a determina autorizarea necesară pentru a converti programe, programe service și module.		

Comenzile de recuperare a căii de acces: autorizările necesare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită nici o autorizare obiect.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGRCYAP ¹ (Q)	Dispozitiv ASP (dacă este specificat)	*USE	
DSPRCYAP ¹	Dispozitiv ASP (dacă este specificat)	*USE	
EDTRBDAP ² (Q)			
EDTRCYAP ¹ (Q)	Dispozitiv ASP (dacă este specificat)	*USE	
¹	Trebuie să aveți autorizația specială *JOBCTL pentru a folosi această comandă.		
²	Trebuie să aveți autorizația specială *ALLOBJ pentru a folosi această comandă.		

Comenzile AFP: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
CHGCDEFNT	Resursă fonturi	*CHANGE	*EXECUTE
CHGFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
CRTFNTRSC	Fișier sursă	*USE	*EXECUTE
	Resursă fonturi: REPLACE(*NO)		*READ, *ADD
	Resursă fonturi: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTFNNTBL	Tabel font DBCS		*READ, *ADD
CRTFORMDF	Fișier sursă	*USE	*EXECUTE
	Definiție formular: REPLACE(*NO)		*READ, *ADD
	Definiție formular: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTOVL	Fișier sursă	*USE	*EXECUTE
	Suprapunere: REPLACE(*NO)		*READ, *ADD
	Suprapunere: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTPAGDFN	Fișier sursă	*USE	*EXECUTE
	Definiție pagină: REPLACE(*NO)		*READ, *ADD
	Definiție pagină: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTPAGSEG	Fișier sursă	*USE	*EXECUTE
	Segment de pagină: REPLACE(*NO)		*READ, *ADD
	Segment de pagină: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
DLTFNTRSC	Resursă fonturi	*OBJEXIST	*EXECUTE
DLTFNNTBL	Tabel font DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Definiție formular	*OBJEXIST	*EXECUTE
DLTOVL	Suprapunere	*OBJEXIST	*EXECUTE
DLTPAGDFN	Definiție de pagină	*OBJEXIST	*EXECUTE
DLTPAGSEG	Segment pagină	*OBJEXIST	*EXECUTE
DSPCDEFNT	Resursă fonturi	*USE	*EXECUTE
DSPFNTRSCA	Resursă fonturi	*USE	*EXECUTE
DSPFNNTBL	Tabel font DBCS	*USE	*EXECUTE
RMVFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
WRKFNTRSC ¹	Resursă fonturi	*USE	*USE
WRKFORMDF ¹	Definiție formular	*USE	*USE
WRKOVL ¹	Suprapunere	*USE	*USE
WRKPAGDFN ¹	Definiție de pagină	Orice autorizație	*USE
WRKPAGSEG ¹	Segment pagină	*USE	Orice autorizație
¹ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.			

Comenzi pentru socket-uri AF_INET peste SNA

Comenzile pentru socket-uri AF_INET peste SNA: autorizările necesare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda autorizare *USE altora. Aceste comenzi nu necesită vreo autorizație obiect:

Aceste comenzi nu necesită vreo autorizație obiect:			
ADDIPSIFC ¹	CHGIPSIFC ¹	CVTIPSLOC	RMVIPSLOC ¹
ADDIPSRTE ¹	CHGIPSLOC ¹	ENDIPSIFC (Q)	RMVIPSRTE ¹
ADDIPSLOC ¹	CHGIPSTOS ¹	PRTIPSCFG	STRIPSIFC (Q)
CFGIPS	CVTIPSIFC	RMVIPSIFC ¹	
¹ Trebuie să aveți autorizația specială *IOSYSCFG pentru a folosi această comandă.			

Alertele: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDALRD	Tabel alertă	*USE, *ADD	*EXECUTE
CHGALRD	Tabel alertă	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Tabel alertă	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Tabel alertă		*READ, *ADD
DLTALR	Fișier fizic QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Tabel alertă	*OBJEXIST	*EXECUTE
RMVALRD	Tabel alertă	*USE, *DLT	*EXECUTE
WRKALR ¹	Fișier fizic QAALERT	*USE	*EXECUTE
WRKALRD ¹	Tabel alertă	*USE	*EXECUTE
WRKALRTBL ¹	Tabel alertă	*READ	*USE
¹ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.			

Comenzi pentru dezvoltare de aplicații: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
FNDSTRPDM	Parte sursă	*READ	*EXECUTE
MRGFORMD	Descriere formular	*READ	*EXECUTE
STRAPF ¹	Fișier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzile CRTPF, CRTLF, ADDPFM, ADDLFM și RMVM	*USE	*EXECUTE
STRBGU ¹	Grafic	*OBJMGT, *CHANGE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRDFU ¹	Program (dacă se creează opțiune program)		*READ, *ADD
	Program (dacă există opțiunea de modificare sau ștergere program)	*OBJEXIST	*EXECUTE
	Program (dacă se modifică sau afișează opțiune de date)	*USE	*EXECUTE
	Fișier bază de date (dacă se modifică opțiunea de date)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Fișier bază de date (dacă se afișează opțiunea de date)	*USE	*EXECUTE
	Fișier afișare (dacă se afișează sau modifică opțiunea de date)	*USE	*EXECUTE
	Fișier afișare (dacă se modifică opțiunea de program)	*USE	*EXECUTE
	Fișier afișare (dacă se șterge opțiunea de program)	*OBJEXIST	*EXECUTE
STRPDM ¹			
STRRLU	Fișier 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	Fișier sursă	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Actualizare și adăugare a unui nou membru	*CHANGE, *OBJMGT	*READ, *ADD
	Ștergere membru	*ALL	*EXECUTE
STRSEU ¹	Fișier 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	Fișier sursă	*USE	*EXECUTE
WRKOBJPDM ¹	Fișier	*READ sau drept de proprietate	*EXECUTE
¹	Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală.		
²	Un grup corespunde bibliotecii.		
³	Un proiect se alcătuiește din unul sau mai multe grupuri (biblioteci).		
⁴	Această comandă cere autorizarea specială *ALLOBJ.		

Comenzi pentru dezvoltare de aplicații: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTAUTHLR (Q)	Obiect asociat dacă acesta există	*ALL	*EXECUTE
DLTAUTHLR	Deținător de autorizare	*ALL	*EXECUTE
DSPAUTHLR	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.

Comenzile listei de autorizări: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QSYS
ADDAUTLE ¹	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
CHGAUTLE ¹	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Proprietar sau *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți 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 fiți proprietarul sau să aveți autorizarea gestionare listă și să aveți autorizările ce sunt date sau luate.

² Dacă nu aveți *OBJMGT sau *AUTLMGT, puteți extrage autorizarea *PUBLIC și autorizarea dumneavoastră proprie. Trebuie să aveți autorizarea *READ pentru profilul dumneavoastră pentru a extrage propria dumneavoastră autorizare.

³ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.

⁴ Nu trebuie să fiți exclus (*EXCLUDE) din lista autorizare.

⁵ O anumită autorizare pentru lista autorizare este cerută.

Comenzi pentru director de legare: autorizările necesare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
ADDBNDDIRE	Director legare	*OBJOPR, *ADD	*USE
CRTBNDDIR	Director legare		*READ, *ADD

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTBNDDIR	Director legare	*OBJEXIST	*EXECUTE
DSPBNDDIR	Director legare	*READ, *OBJOPR	*USE
RMVBND DIRE	Director legare	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBND DIR ¹	Director legare	Orice autorizație	*USE
WRKBND DIRE ¹	Director legare	*READ, *OBJOPR	*USE

¹ Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operație.

Comenzi pentru descriere cerere de modificare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCMDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDPRDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGCRQD	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 operație individuală, trebuie să aveți autorizația necesară de operație.

Comenzile pentru diagramă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTCHTFMT	Format diagramă	*OBJEXIST	*EXECUTE
DSPCHT	Format diagramă	*USE	*USE
	Fișier bază de date	*USE	*USE
DSPGDF	Fișier bază de date	*USE	*USE
STRBGU (Opțiunea 3) ²	Format diagramă	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT ¹	Format diagramă	Orice autorizație	*USE

Comenzi diagramă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
¹	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		
²	Opțiunea 3 din meniul BGU (afișat atunci când este rulat STRGBU) este opțiunea Modificare format diagramă.		

Comenzi pentru clasă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCLS	Clasă	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Clasă		*READ, *ADD
DLTCLS	Clasă	*OBJEXIST	*EXECUTE
DSPCLS	Clasă	*USE	*EXECUTE
WRKCLS ¹	Clasă	*OBJOPR	*USE
¹	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		

Comenzile pentru clasă-de-serviciu

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCOSD ³	Descriere clasă-de-serviciu	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD ³	Descriere clasă-de-serviciu		
DLTCOSD	Descriere clasă-de-serviciu	*OBJEXIST	*EXECUTE
DSPCOSD	Descriere clasă-de-serviciu	*USE	*EXECUTE
WRKOSD ^{1,2}	Descriere clasă-de-serviciu	*OBJOPR	*EXECUTE
¹	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
²	E necesară aceeași autorizare pentru obiect.		
³	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.		

Comenzi pentru cluster

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda *USE altora.

Comandă	Obiect referențiat	Autorizație necesară	
		Pentru obiecte	Pentru biblioteci
ADDCLUNODE (Q) ¹	Programul serviciu QCSTCTL	*USE	

Comandă	Obiect referențiat	Autorizație necesară	
		Pentru obiecte	Pentru biblioteci
ADDCRGDEVE (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
ADDCRGNODE (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Coadă de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
	Coadă utilizator informații distribuie	*OBJOPR, *ADD	*EXECUTE
ADDDEVMNE (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 funcția Urmărire service	
CHGCLUVER (Q) ¹	Programul serviciu QCSTCTL2	*USE	
CHGCRG (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Coadă de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
CHGCRGDEVE (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
CHGCRGPRI (Q) ¹	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Comanda VFYCFG (Vary configuration - Verificare configurare)	*USE	

Comenzi cluster

Comandă	Obiect referențiat	Autorizație necesară	
		Pentru obiecte	Pentru biblioteci
I CRTADMDMN (Q) ^{1, 3}	Profil 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 ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Coadă utilizator informații distribuie	*OBJOPR, *ADD	*EXECUTE
	Coadă de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
I 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)
DLTCRGCLU (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
DMPCLU TRC	Grup resursă cluster	*USE	
		*SERVICE sau funcția Urmărire service	
DSPCLUINF			
DSPCRGINF	Grup resursă cluster	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q) ¹	Programul serviciu QCSTCTL	*USE	
ENDCHTSVR (Q)	Listă de autorizații	*CHANGE	
ENDCRG (Q) ¹	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
RMVCLUNODE (Q) ¹	Programul serviciu QCSTCTL	*USE	
RMVCRGDEVE (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	

Comandă	Obiect referențiat	Autorizație necesară	
		Pentru obiecte	Pentru biblioteci
RMVCRGNODE (Q) ¹	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE, *OBJEXIST	*EXECUTE
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
RMVDEVDMNE (Q) ¹	Programul serviciu QCSTDD	*USE	
STRCHTSVR	Listă de autorizații	*CHANGE	
STRCLUNOD (Q) ¹	Programul serviciu QCSTCTL	*USE	
STRCRG (Q) ¹	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE
	Program ieșire	*EXECUTE ²	*EXECUTE ²
	Profil utilizator pentru rulare program de ieșire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
WRKCLU ⁴	Grup resursă cluster	*USE	*EXECUTE
<p>¹ Trebuie să aveți autorizația specială *IOSYSCFG pentru a folosi această comandă.</p> <p>² Se aplică pentru profilul utilizator apelator și profilul utilizator rulare program de ieșire.</p> <p>³ Profilului utilizator care apelează îi sunt garantate autorizări *CHANGE și *OBJEXIST asupra grupului de resurse cluster.</p> <p>⁴ Utilizatorul trebuie să fie autorizat pentru comandă și să aibă autorizarea specială *SERVICE sau să fie autorizat pentru funcția Urmărire serviciu a sistemului de operare prin suportul Administrare aplicație din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_SERVICE_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operații de urmărire.</p>			

Comenzile pentru comandă (*CMD)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCMD	Comandă	*OBJMGT	*EXECUTE
CHGCMDDFT	Comandă	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Comandă proxy	*OBJMGT	*EXECUTE
CRTCMD	Fișier sursă	*USE	*EXECUTE
	Comandă: REPLACE(*NO)		*READ, *ADD
	Comandă: REPLACE(*YES)	Vedeți regulile generale.	Vedeți regulile generale.
CRTPRCMD	Comandă proxy: REPLACE(*NO)		*READ, *ADD
	Comandă proxy: REPLACE(*YES)	Vedeți regulile generale la pagina D-2	Vedeți regulile generale la pagina D-2
DLTCMD	Comandă	*OBJEXIST	*EXECUTE
DSPCMD	Comandă	*USE	*EXECUTE

Comenzi comandă (*CMD)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
GENCMDDOC ³	Comandă	*USE	*EXECUTE
	Grup de panouri (asociat)	*USE	*EXECUTE
	Fișier ieșire: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Comandă	*OBJOPR	*EXECUTE
	Fișier DDM	*USE	*EXECUTE
SLTCMD ¹	Comandă	Orice autorizație	*USE
WRKCMD ²	Comandă	Orice autorizație	*USE
<p>¹ Drept de proprietate sau unele autorizații pentru obiect sunt necesare.</p> <p>² Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.</p> <p>³ Trebuie să aveți autorizare de execuție (*X) pentru directoarele din calea fișierului generat și autorizări de scriere și execuție (*WX) pentru directorul părinte al fișierului generat.</p>			

Comenzi pentru control comitere

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
COMMIT			
ENDCMTCTL	Coadă de mesaje, așa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Coadă de mesaje, când a fost specificată în cuvântul cheie NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Zona de date, așa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*CHANGE	*EXECUTE
	Fișierele, așa cum au fost specificate în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR *READ	*EXECUTE
WRKCMTDFN ¹			
<p>¹ Orice utilizator poate rula această comandă pentru definiții de comitere care aparțin 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 definiție de comitere.</p>			

Comenzile CSI (informații parte comunicații)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCSI	Obiect CSI	*USE, *OBJMGT	*EXECUTE
	Descriere dispozitiv ¹	*CHANGE	
CRTCSI	Obiect CSI		*READ, *ADD
	Descriere dispozitiv ¹	*CHANGE	

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTCSI	Obiect CSI	*OBJEXIST	*EXECUTE
DSPCSI	Obiect CSI	*READ	*EXECUTE
WRKCSI	Obiecte CSI	*USE	*EXECUTE

¹ Autorizarea este verificată când este folosit obiectul CSI (informații parte comunicații).

Comenzi de configurare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PRTDEVADR	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv	*USE	*EXECUTE
RSTCFG (Q) ⁵	Fiecare obiect care este restaurat peste, de o versiune salvată	*OBJEXIST ¹	*EXECUTE
	Bibliotecă destinație		*ADD, *EXECUTE ¹
	Profilul utilizator care deține obiectele care sunt create	*ADD ¹	
	Unitate bandă	*USE	*EXECUTE
	Fișier bandă (QSYSTAP)	*USE ¹	*EXECUTE
	Fișier salvare, dacă este specificat	*USE	*EXECUTE
	Ieșire imprimantă (QPSRLDSP), dacă s-a specificat output(*print)	*USE	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul referință câmp QSYS/QASRRSTO, dacă fișierul de ieșire este specificat și nu există	*USE	*EXECUTE
RTVCFGSTS	Obiect	*OBJOPR	*EXECUTE
RTVCFGSRC	Obiect	*USE	*EXECUTE
	Fișier sursă	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SAVCFG ²	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări în el	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	Pe sistemul sursă, aceeași autorizare ca și cea necesară pentru comanda SAVCFG.		
	Pe sistemul destinație, aceeași autorizare ca și cea necesară pentru comanda RSTCFG.		
VRYCFG ^{3, 5, 6, 7}	Obiect	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS ⁴	Obiect	*OBJOPR	*EXECUTE

Comenzi de configurare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
1	Dacă aveți autorizarea specială *SAVSYS, nu aveți nevoie de autorizarea specificată.		
2	Trebuie să aveți autorizarea specială *SAVSYS.		
3	Dacă un utilizator are autorizarea specială *JOBCTL, nu e necesară autorizarea pentru obiect.		
4	Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală.		
5	Trebuie să aveți autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF, sau RESETSYS(*YES).		
6	Trebuie să aveți autorizarea specială *IOSYSCFG pentru biblioteca mediu de stocare când starea e *ALLOCATE sau *DEALLOCATE.		
7	Trebuie să aveți autorizațiile speciale *IOSYSCFG și *SECADM pentru a specifica GENPTHCERT(*PWDGRP), USRPRF(*YES) sau OMITUSRPRF.		

Comenzi pentru listă de configurare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCFGLE ²	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL ²	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE ²	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL ²	Listă de configurare	*USE, *OBJMGT	*ADD
CRTCFGL ²	Listă de configurare		
DLTCFGL	Listă de configurare	*OBJEXIST	*EXECUTE
DSPCFGL ²	Listă de configurare	*USE, *OBJMGT	*EXECUTE
RMVCFGLE ²	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL ^{1, 2}	Listă de configurare	*OBJOPR	*EXECUTE
1	Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală.		
2	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.		

Comenzi pentru listă de conexiuni

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTCNNL	Listă de conexiuni	*OBJEXIST	*EXECUTE
DSPCNNL	Listă de conexiuni	*USE	*EXECUTE
WRKCNNL ¹	Listă de conexiuni	*OBJOPR	*EXECUTE
1	Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală.		

Comenzi pentru descriere controler

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCTLAPPC ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CHGCTLNET ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP ²	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS ²	Controler	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLASC ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLBSC ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLFNC ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		

Comenzi descriere controler

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTCTLHOST ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLLWS ²	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
	Program (INZPGM)	*USE	*EXECUTE
CRTCTLNET ²	Descriere de linie (LINE)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLRTL ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLRWS ²	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLTAP ²	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLVWS ²	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
DLTCTLD	Descriere controler	*OBJEXIST	*EXECUTE
DSPCTLD	Descriere controler	*USE	*EXECUTE
ENDCTLRCY	Descriere controler	*USE	*EXECUTE
PRTCMNSEC ³			
RSMCTLRCY	Descriere controler	*USE	*EXECUTE
WRKCTLD ¹	Descriere controler	*OBJOPR	*EXECUTE
¹ Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală. ² Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG. ³ Pentru a folosi această comandă trebuie să aveți autorizările speciale *ALLOBJ și *IOSYSCFG sau *AUDIT.			

Comenzile pentru criptografie

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
CPHDTA (Q)			
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGEX *FILE	*OBJOPR, *READ	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	Coadă de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE

Comenzi pentru zonă de date

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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 autorizație	*USE

Comenzi zonă de date

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
¹	Dacă comenzile de creare și modificare a zonei de date sunt rulate folosind funcții ale limbajului de nivel înalt, aceste autorizări sunt încă necesare deși autorizarea pentru comandă nu e necesară.		
²	Autorizarea este verificată în momentul rulării, dar nu și la momentul compilării.		
³	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		
⁴	Autorizarea este verificată când este folosită zona de date.		

Comenzi pentru coadă de date

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTDTAQ	Coadă de date		*READ, *ADD
	Coadă de date destinație pentru programul QSNDDTAQ	*OBJOPR, *ADD	*EXECUTE
	Coadă de date sursă pentru programul QRCVDTAQ	*OBJOPR, *READ	*EXECUTE
	Descriere dispozitiv APPC ²	*CHANGE	
DLTDTAQ	Coadă de date	*OBJEXIST	*EXECUTE
WRKDTAQ ¹	Coadă de date	*READ	*USE
¹	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
²	Autorizarea este verificată când este folosită zona de date.		

Comenzi pentru descriere dispozitiv

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CFGDEVMLB ⁴	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
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

Comenzi descriere dispozitiv

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGDEVNET ⁴	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNWSH ⁴	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT ⁴	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPR 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
CRTDEVASC ⁴	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVCRP ⁴	Descriere dispozitiv		*EXECUTE
CRTDEVDKT ⁴	Descriere dispozitiv		*EXECUTE
CRTDEVDS 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
CRTDEVPR 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		

Comenzi descriere dispozitiv

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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	
DSPCANNSTS	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
SETASGRP ⁶	Toate descrierile de dispozitive din grupul ASP	*USE	
	Toate bibliotecile specificate în lista de biblioteci înainte de spațiul nume bibliotecă și lista de biblioteci sunt modificate	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD ³	Descriere dispozitiv	*OBJOPR	*EXECUTE
<p>¹ Pentru a înlătura o coadă de ieșire asociată, sunt necesare autorizarea existență obiect (*OBJEXIST) pentru coada de ieșire și autorizarea de citire pentru bibliotecă QUSRSYS.</p> <p>² Trebuie să aveți autorizările specială control job (*JOBCTL) și cea operațională obiect pentru descrierea dispozitivului.</p> <p>³ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.</p> <p>⁴ Trebuie să aveți autorizarea specială *IOSYSCFG pentru a rula această comandă.</p> <p>⁵ Trebuie să aveți autorizarea specială *ALLOBJ pentru a rula această comandă.</p> <p>⁶ Când *CURUSR este specificat pentru grupul ASP (ASPGRP) sau parametrul Bibliotecă pentru firul de execuție curent (USRLIBL) trebuie de asemenea avută autorizare de citire (*READ) asupra descrierii jobului listat în profilul dumneavoastră utilizator și autorizare de execuție (*EXECUTE) asupra bibliotecii unde este localizată descrierea jobului.</p>			

Comenzi pentru emulare dispozitiv

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDEMLCFGE	Fișier de configurare emulare	*CHANGE	*EXECUTE
CHGEMLCFGE	Fișier de configurare emulare	*CHANGE	*EXECUTE
EJTEMLOUT	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locația e specificată	*OBJOPR	*EXECUTE

Comenzi emulare dispozitiv

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENDPRTEML	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locația e specificată	*OBJOPR	*EXECUTE
EMLPRTKEY	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locația e specificată	*OBJOPR	*EXECUTE
EML3270	Descriere dispozitiv emulare	*OBJOPR	*EXECUTE
	Descriere controler emulare	*OBJOPR	*EXECUTE
RMVEMLCFGE	Fișier de configurare emulare	*CHANGE	*EXECUTE
STREML3270	Fișier de configurare emulare	*OBJOPR	*EXECUTE
	Dispozitiv de emulare, descriere controler de emulare, dispozitiv stație de afișare și descriere controler stație de afișare	*OBJOPR	*EXECUTE
	Descriere dispozitiv imprimantă, program de ieșire utilizator și tabele de traducere când sunt specificate	*OBJOPR	*EXECUTE
STRPRTEML	Fișier de configurare emulare	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare și descriere controler emulare	*OBJOPR	*EXECUTE
	Descriere dispozitiv imprimantă, ieșire imprimantă, coadă de mesaje, descriere job, coadă de joburi și tabele de traducere când sunt specificate	*OBJOPR	*EXECUTE
SNDEMLIGC	Din-fișier	*OBJOPR	*EXECUTE
TRMPRTEML	Descriere dispozitiv emulare	*OBJOPR	*EXECUTE

Comenzi pentru director și ascundere director

Aceste comenzi nu necesită nici o autorizație obiect:			
ADDDIRE ²	CHGDIRSHD ¹	ENDDIRSHD ⁴	STRDIRSHD ⁴
ADDDIRSHD ¹	CPYFRMDIR ¹	RMVDIRE ¹	WRKDIRE ^{3,5}
CHGSYSDIRA ²	CPYTODIR ¹	RMVDIRSHD ¹	WRKDIRLOC ^{1,5}
CHGDIRE ³	DSPDIRE	RNMDIRE ²	WRKDIRSHD ^{1,5}
¹	Trebuie să aveți autorizarea specială *SECADM.		
²	Trebuie să aveți 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 aveți autorizația specială *JOBCTL.		
⁵	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		

Comenzi disc

Comenzi pentru disc

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită autorizarea pentru nici un obiect:		
ENDDSKRGZ (Q) ¹	STRDSKRGZ (Q) ¹	WRKDSKSTS
¹ Pentru a folosi această comandă, trebuie să aveți autorizarea specială *ALLOBJ.		

Comenzi pentru passthrough stație de afișare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENDPASTHR			
STRPASTHR	Dispozitiv APPC pe sistem sursă	*CHANGE	*EXECUTE
	Dispozitiv APPC pe sistem destinație	*CHANGE	*EXECUTE
	Controler virtual pe sistem destinație ¹	*USE	*EXECUTE
	Dispozitiv virtual pe sistem destinație ^{1, 2}	*CHANGE	*EXECUTE
	Program specificat în valoarea de sistem QRMTSIGN pe sistemul destinație, dacă există ¹	*USE	*USE
TFRPASTHR			
¹ Profilul utilizator care necesită această autorizare este cel care rulează jobul batch passthrough. Pentru un passthrough care ocolește ecranul de semnare, profilul de utilizator este cel specificat în parametrul de utilizator la distanță (RMTUSER). Pentru un passthrough care folosește procedura normală de semnare (RMTUSER(* NONE)), utilizatorul este profilul de utilizator implicit specificat în intrarea de comunicații a subsistemului care tratează cererea de passthrough. În general, acesta este QUSER.			
² Dacă passthrough-ul este unul care folosește procedura normală de semnare, profilul de utilizator specificat în ecranul de semnare pe sistemul destinație trebuie să aibă autorizare pentru acest obiect.			

Comenzi pentru distribuție

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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	Fișier cerut	*CHANGE	*EXECUTE
RCVDST ¹	Fișier cerut	*CHANGE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
RLSDSTQ (Q)			
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST ¹	Fișier sau document cerut	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			
¹ Dacă un utilizator cere distribuție pentru alt utilizator, el trebuie să aibă autorizarea de a lucra în numele celuiilalt. ² Când distribuția este plină.			

Comenzi pentru listă de distribuție

Aceste comenzi nu necesită nici o autorizare obiect:			
ADDDSTLE ¹	CRTDSTL	DSPDSTL	RNMDSTL ¹
CHGDSTL ¹	DLTDSTL ¹	RMVDSTLE ¹	WRKDSTL ²
¹ Trebuie să aveți autorizarea specială *SECADM sau să dețineți lista de distribuție. ² Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.			

Comenzi pentru obiecte bibliotecă document

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE
CHGDLOAUD ¹			
CHGDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE

Comenzi obiect bibliotecă document

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGDLOOWN	Obiect bibliotecă document	Proprietar sau autorizare specială *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	*EXECUTE
	Profil utilizator nou	*ADD	*EXECUTE
CHGDLOPGP	Obiect bibliotecă document	Proprietar sau autorizare specială *ALLOBJ	*EXECUTE
	Profil de grup primar vechi	*DLT	*EXECUTE
	Profil de grup primar nou	*ADD	*EXECUTE
CHGDOCD ²	Descriere document	*CHANGE	*EXECUTE
CHKDLO ²	Obiect bibliotecă document	Cum a fost cerut de cuvântul cheie AUT	*EXECUTE
CHKDOC	Document	*CHANGE	*EXECUTE
	Dicționar ajutător pentru corectare ortografică	*CHANGE	*EXECUTE
CPYDOC	Document-sursă	*USE	*EXECUTE
	Document-destinație, dacă se înlocuiește documentul existent	*CHANGE	*EXECUTE
	Folder-destinație dacă acesta e nou	*CHANGE	*EXECUTE
CRTDOC	Folder-destinație	*CHANGE	*EXECUTE
CRTFLR	Folder-destinație	*CHANGE	*EXECUTE
DLTDLO ³	Obiect bibliotecă document	*ALL	*EXECUTE
DLTDOCL ²⁰	Listă documente	*ALL ⁴	*EXECUTE
DMPDLO ¹⁵			
DSPAUTLDLO	Listă de autorizații	*USE	*EXECUTE
	Obiect bibliotecă document	*USE	*EXECUTE
DSPDLOAUD ²¹	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți 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	Fișier cerut	*USE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
MOVDOC	Folder-sursă, dacă documentul sursă este într-un folder	*CHANGE	*EXECUTE
	Document-sursă	*ALL	*EXECUTE
	În-fișier	*CHANGE	*EXECUTE
MRGDOC ⁵	Document	*USE	*EXECUTE
	Folder-sursă	*USE	*EXECUTE
	Document-destinație dacă acesta este înlocuit	Vedeți regulile generale.	Vedeți regulile generale.
	Folder-destinație dacă acesta e nou	Vedeți regulile generale.	Vedeți regulile generale.

Comenzi obiect bibliotecă document

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PAGDOC	Document	*CHANGE	*EXECUTE
PRTDOC	Folder	*USE	*EXECUTE
	Document	*USE	*EXECUTE
	Comenzile DLTPF, DLTF și DLTOVR, dacă e specificată o instrucțiune <i>INDEX</i>	*USE	*EXECUTE
	Comenzile CRTPF, OVRPRTF, DLTSPLF și DLTOVR, dacă se specifică o instrucțiune <i>RUN</i>	*USE	*EXECUTE
	Document salvare, dacă se specifică SAVOUTPUT (*YES)	*USE	*EXECUTE
	Folder salvare, dacă se specifică SAVOUTPUT (*YES)	*USE	*EXECUTE
QRYDOCLIB ^{2,6}	Fișier cerut	*USE	*EXECUTE
	Listă documente, dacă există	*CHANGE	*EXECUTE
RCLDLO	Obiect bibliotecă document		
	Documentele interne sau toate documentele și 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-destinație	*CHANGE	*EXECUTE
RPLDOC ²	Fișier cerut	*READ	*EXECUTE
	Document	*CHANGE	*EXECUTE
RSTDLO (Q) ^{7, 8, 9}	Obiect bibliotecă de documene, dacă se înlocuiește	*ALL ¹⁰	*EXECUTE
	Folderul părinte, dacă DLO este nou	*CHANGE ¹⁰	*EXECUTE
	Profilul utilizator proprietar, dacă DLO este nou	*ADD ¹⁰	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișier de salvare	*USE	*EXECUTE
	Fișier optic (OPTFILE) ¹⁷	*R	Nu se aplică
	Prefix cale al fișierului optic (OPTFILE) ¹⁷	*X	Nu se aplică
	Volum optic ¹⁹	*USE	Nu se aplică
RSTS36FLR ^{11,12,14}	Folder S/36	*USE	*EXECUTE
	În-fișier	*CHANGE	*EXECUTE
	Fișier 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
	Fișier cerut	*CHANGE	*EXECUTE

Comenzi obiect bibliotecă document

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SAVDLO ^{7,13}	Obiect bibliotecă document	*ALL ¹⁰	*EXECUTE
	Unitate de bandă, unitate de dischetă și unitate optică	*USE	*EXECUTE
	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări în el	*USE, *ADD, *OBJMGT	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișier optic (OPTFILE) ¹⁷	*RW	Nu se aplică
	Directorul părinte al fișierului optic (OPTFILE) ¹⁷	*WX	Nu se aplică
	Prefixul cale al fișierului optic (OPTFILE) ¹⁷	*X	Nu se aplică
	Directorul root (/) al volumului ^{17, 18}	*RWX	Nu se aplică
	Volum optic ¹⁹	*CHANGE	Nu se aplică
SAVRSTDLO	Pe sistemul sursă, aceeași autorizare ca și cea necesară pentru comanda SAVDLO.		
	Pe sistemul destinație, aceeași autorizare ca și cea necesară pentru comanda RSTDLO.		
WRKDOC	Folder	*USE	
WRKFLR	Folder	*USE	
1	Trebuie să aveți autorizația specială *AUDIT.		
2	Dacă utilizatorul lucrează în numele altui utilizator, este verificată autorizarea celui alt utilizator pentru obiect.		
3	Utilizatorul trebuie să aibă autorizarea *ALL pentru toate obiectele din folder pentru a șterge folderul și toate obiectele din el.		
4	Dacă aveți autorizarea specială *ALLOBJ sau *SECADM, nu aveți 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 și pentru care utilizatorul are cel puțin autorizarea *USE sunt returnate în lista de documente sau fișierul de ieșire.		
7	Trebuie să aveți autorizare specială *SAVSYS, *ALLOBJ sau să fiți înrolat în directorul de distribuție sistem.		
8	E necesară autorizarea specială *SAVSYS sau *ALLOBJ pentru a folosi următoarea combinație de parametri: RSTDLO DLO(*MAIL).		
9	Trebuie să aveți autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.		
10	Dacă aveți autorizarea specială *SAVSYS, nu aveți nevoie de autorizarea specificată.		

Comenzi obiect bibliotecă document

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
11	Aveți nevoie de autorizația *ALL pentru document dacă îl înlocuiți. Aveți nevoie de autorizații operaționale și pentru toate datele pentru folder dacă restaurați informații noi în aceste foldere, sau aveți nevoie de autorizația specială *ALLOBJ.		
12	Dacă este folosit pentru dicționar, este necesară doar autorizația pentru comandă.		
13	E necesară autorizarea specială *SAVSYS sau *ALLOBJ pentru a folosi următoarea combinație de parametri: SAVDLO DLO(*ALL) FLR(*ANY) SAVDLO DLO(*MAIL) SAVDLO DLO(*CHG) SAVDLO DLO(*SEARCH) OWNER(not *CURRENT)		
14	Trebuie să fiți înscris în directorul de distribuire sistem dacă folderul sursă este un folder document.		
15	Trebuie să aveți autorizarea specială *ALLOBJ pentru a face dump la obiectele bibliotecă document interne.		
16	Trebuie să aveți 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 ștergeți volumul optic.		
19	Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția de suport optic.		
20	Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ când s-a specificat OWNER (*ALL) sau OWNER (nume) și 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 pentru set de caractere pe doi octeți

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CPYIGCTBL	Tabelă de sortare DBCS (*IN)	*ALL	*EXECUTE
	Tabelă de sortare DBCS (*OUT)	*USE	*EXECUTE
CRTIGCDCT	Dicționar conversie DBCS		*READ, *ADD
DLTIGCDCT	Dicționar conversie DBCS	*OBJEXIST	*EXECUTE
DLTIGCSRT	Tabelă de sortare DBCS	*OBJEXIST	*EXECUTE
DLTIGCTBL	Tabel font DBCS	*OBJEXIST	*EXECUTE
DSPIGCDCT	Dicționar conversie DBCS	*USE	*EXECUTE
EDTIGCDCT	Dicționar conversie DBCS	*USE, *UPD	*EXECUTE
	Dicționar utilizator	*ADD, *DLT	*EXECUTE
STRCGU	Tabelă de sortare DBCS	*CHANGE	*EXECUTE
	Tabel font DBCS	*CHANGE	*EXECUTE

Comenzi pentru set de caracter pe doi octeți

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRFMA	Tabela de font DBCS, dacă e specificată opțiunea de copiere în	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	Tabela de font DBCS, dacă e specificată opțiunea de copiere din	*OBJOPR, *READ	*EXECUTE
	Fișierul de lucru de ajutor gestionare font (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

Comenzi pentru descriere editare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTEDTD	Descriere de editare		*EXECUTE, *ADD
DLTEDTD	Descriere de editare	*OBJEXIST	*EXECUTE
DSPEDTD	Descriere de editare	*OBJOPR	*EXECUTE
WRKEDTD ¹	Descriere de editare	Orice autorizație	*USE

¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.

Comenzi pentru variabile de mediu

Aceste comenzi nu necesită nici o autorizare obiect.			
ADDENVVAR ¹	CHGENVVAR ¹	RMVENVVAR ¹	WRKENVVAR ¹

¹ Pentru a actualiza variabile de mediu de nivel sistem, aveți nevoie de autorizarea specială *JOBCTL.

Comenzi pentru configurație LAN extinsă prin comunicație fără fir

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDEWCBCDE	Fișier sursă	*USE	*EXECUTE
ADDEWCM	Fișier sursă	*USE	*EXECUTE
ADDEWCPTCE	Fișier sursă	*USE	*EXECUTE
ADDEWLM	Fișier sursă	*USE	*EXECUTE
CHGEWCBCDE	Fișier sursă	*USE	*EXECUTE
CHGEWCM	Fișier sursă	*USE	*EXECUTE
CHGEWCPTCE	Fișier sursă	*USE	*EXECUTE
CHGEWLM	Fișier sursă	*USE	*EXECUTE
DSPEWCBCDE	Fișier sursă	*USE	*EXECUTE
DSPEWCM	Fișier sursă	*USE	*EXECUTE
DSPEWCPTCE	Fișier sursă	*USE	*EXECUTE
DSPEWLM	Fișier sursă	*USE	*EXECUTE
RMVEWCBCDE	Fișier sursă	*USE	*EXECUTE

Comenzi configurație LAN extinsă prin comunicație fără fir

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RMVEWCPTCE	Fișier sursă	*USE	*EXECUTE

Comenzi pentru fișier

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDICFDEVE	Fișier ICF	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	Fișier logic	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE, *ADD
	Fișierul la care se referă parametrul DTAMBRs, când fișierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fișierul la care se referă parametrul DTAMBRs, când fișierul logic nu este cu cheie	*OBJOPR	*EXECUTE
ADDPFCST	Fișier dependent, dacă se specifică TYPE(*REFCST)	*OBJMGT sau *OBJALTER	*EXECUTE
	Fișierul părinte, dacă se specifică TYPE(*REFCST)	*OBJMGT sau *OBJREF	*EXECUTE
	Fișierul, dacă se specifică TYPE(*UNQCST) sau TYPE(*PRIKEY)	*OBJMGT	*EXECUTE
ADDPFM	Fișier fizic	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Fișier fizic, pentru a insera declanșator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Fișier fizic, pentru a șterge declanșator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Fișier fizic, pentru a actualiza declanșator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Program declanșator	*EXECUTE	*EXECUTE
CHGD DMF	Fișier DDM	*OBJOPR, *OBJMGT	*EXECUTE
	Descriere dispozitiv ⁷	*CHANGE	
CHGDKTF	Fișier dischetă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat în comandă	*OBJOPR	*EXECUTE
CHGDSPF	Fișier afișare	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE

Comenzi fișier

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CHGDTA	Fișier date	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Program	*USE	*EXECUTE
	Fișier afișare	*USE	*EXECUTE
CHGICFDEVE	Fișier ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	Fișier ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Fișier logic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGLFM	Fișier logic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPF	Fișier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPF CST	Fișier dependent	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPFM	Fișier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPFTRG	Fișier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPRTF	Ieșire imprimantă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CHGSAVF	Fișier de salvare	*OBJOPR și (*OBJMGT sau *OBJALTER).	*EXECUTE
CHGSRCPF	Fișier fizic sursă	*OBJMGT sau *OBJALTER	*EXECUTE
CHGTAPF	Fișier bandă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CLRPFM	Fișier fizic	*OBJOPR, *OBJMGT sau *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Fișier de salvare	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Din-fișier	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
	Pe baza fișierului dacă fișier-sursă este unul logic	*READ	*EXECUTE
CPYFRMDKT	Din-fișier	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
CPYFRMIMPF	Din-fișier	*OBJOPR, *READ	*USE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*USE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
	Pe baza fișierului dacă fișier-sursă este unul logic	*READ	*USE
	comanda CRTDDMF	*USE	*USE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CPYFRMQRYF ¹	Din-fișier	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
CPYFRMSTMF	Fișier flux	*R	
	Directoarele din prefix nume cale al fișierului flux	*X	
	Fișierul bază de date destinație, dacă se specifică MBROPT(*ADD)	*X, *ADD	*X
	Fișierul bază de date destinație, dacă se specifică MBROPT(*REPLACE)	*X, *ADD, *DLT, *OBJMGT	*X
	Fișierul bază de date destinație, dacă este creat un nou membru)	*X, *OBJMGT, *ADD	*X, *ADD
	Tabela de conversie *TBL folosită pentru a translata datele	*OBJOPR	*X
	Fișierul de salvare destinație există	*RX, *ADD, *OBJMGT	*X
	Fișierul de salvare destinație este creat		*RX, *ADD
CPYFRMTAP	Din-fișier	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
CPYSRCF	Din-fișier	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
CPYTODKT	Fișier-destinație și din fișier	*OBJOPR, *READ	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat în comandă	*OBJOPR, *READ	*EXECUTE
	Pe baza fișierului fizic dacă fișier-sursă este unul logic	*READ	*EXECUTE
CPYTOIMPF	Din-fișier	*OBJOPR, *READ	*USE
	Fișier-destinație (fișier dispozitiv)	*OBJOPR, *READ	*USE
	Fișier-destinație (fișier fizic)	Vedeți regulile generale.	Vedeți regulile generale.
	Pe baza fișierului dacă fișier-sursă este unul logic	*READ	*USE
	comanda CRTDDMF	*USE	*USE
CPYTOSTMF	Fișier bază de date sau fișier de salvare	*RX	*X
	Fișier flux, dacă există deja	*W	
	Directorul părinte al fișierului flux, dacă fișierul flux nu există	*WX,	
	Prefixul numelui căii fișierului flux	*X	
	Tabela de conversie *TBL folosită pentru a translata datele	*OBJOPR	*X
CPYTOTAP	Fișier-destinație și din fișier	*OBJOPR, *READ	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR, *READ	*EXECUTE
	Pe baza fișierului fizic dacă fișier-sursă este unul logic	*READ	*EXECUTE

Comenzi fișier

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTDDMF	Fișier DDM: REPLACE(*NO)		*READ, *ADD
	Fișier DDM: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Descriere dispozitiv ⁷	*CHANGE	
CRTDKTF	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fișier dischetă: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Fișier dischetă: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD, *EXECUTE
CRTDSPF	Fișier sursă	*USE	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fișierul specificat în cuvintele cheie REF și REFFLD	*OBJOPR	*EXECUTE
	Fișier de afișare: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Fișier de afișare: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD, *EXECUTE
CRTICFF	Fișier sursă	*USE	*EXECUTE
	Fișierul specificat în cuvintele cheie REF și REFFLD	*OBJOPR	*EXECUTE
	Fișier ICF: REPLACE(*NO)		*READ, *ADD
	Fișier ICF: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTLF	Fișier sursă	*USE	*EXECUTE
	Fișierul specificat în cuvântul cheie PFILE sau JFILE, când fișierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fișierul specificat în cuvântul cheie PFILE sau JFILE, când fișierul logic nu este cu cheie	*OBJOPR	*EXECUTE
	Fișierele specificate în cuvintele cheie FORMAT și REFACCPH	*OBJOPR	*EXECUTE
	Tabele specificate în cuvântul cheie ALTSEQ	*OBJOPR	*EXECUTE
	Fișier logic		*EXECUTE, *ADD
	Fișierul la care se referă parametrul DTAMBRs, când fișierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fișierul la care se referă parametrul DTAMBRs, când fișierul logic nu este cu cheie	*OBJOPR	*EXECUTE
CRTPF	Fișier sursă	*USE	*EXECUTE
	Fișierele specificate în cuvintele cheie FORMAT și REFFLD și tabelele specificate în cuvântul cheie ALTSEQ	*OBJOPR	*EXECUTE
	Fișier fizic		*EXECUTE, *ADD

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTPRTF	Fișier sursă	*USE	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fișierele specificate în cuvintele cheie REF și REFFLD	*OBJOPR	*EXECUTE
	Ieșire imprimantă: Replace(*NO)		*READ, *ADD, *EXECUTE
	Ieșire imprimantă: Replace(*YES)	Vedeți regulile generale.	*READ, *ADD, *EXECUTE
CRTSAVF	Fișier de salvare		*READ, *ADD, *EXECUTE
CRTSRCPF	Fișier fizic sursă		*READ, *ADD, *EXECUTE
CRTS36DSPF	Fișier-destinație sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fișier sursă QS36SRC	*USE	*EXECUTE
	Fișier de afișare: REPLACE(*NO)		*READ, *ADD
	Fișier de afișare: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Comanda Creare fișier de afișare (CRTDSPF)	*OBJOPR	*EXECUTE
CRTTAPF	Fișier bandă: REPLACE(*NO)		*READ, *ADD
	Fișier bandă: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
DLTF	Fișier	*OBJOPR, *OBJEXIST	*EXECUTE
DSPCPCST	Fișierul bază de date care are constrângere în așteptare	*OBJOPR, *READ	*EXECUTE
DSPDBR	Fișier bază de date	*OBJOPR	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
DSPDDMF	Fișier DDM	*OBJOPR	
DSPDTA	Fișier date	*USE	*EXECUTE
	Program	*USE	*EXECUTE
	Fișier afișare	*USE	*EXECUTE
DSPFD ²	Fișier	*OBJOPR	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul este unul fizic și se specifică TYPE(*ALL, *MBR, SAU *MBRLST)	O autorizare alta decât *EXECUTE	*EXECUTE
DSPFFD	Fișier	*OBJOPR	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPPFM	Fișier fizic	*USE	*EXECUTE
DSPSAVF	Fișier de salvare	*USE	*EXECUTE

Comenzi fișier

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
EDTCPCST	Zona de date, așa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*CHANGE	*EXECUTE
	Fișierele, așa cum au fost specificate în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Fișier bază de date	*OBJOPR și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
INZPFM	Fișierul fizic, când se specifică RECORD(*DFT)	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD	*EXECUTE
	Fișierul fizic, când se specifică RECORD(*DLT)	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Fișier destinație	*CHANGE, *OBJMGT	*CHANGE
	Fișier întreținere	*USE	*EXECUTE
	Fișier rădăcină (root)	*USE	*EXECUTE
OPNDBF	Fișier bază de date	*OBJOPR și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
OPNQRYF	Fișier bază de date	*OBJOPR și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
PRTRGPGM ¹¹			
RGZPFM	Fișierul conținând membrul	*OBJOPR, *OBJMGT sau *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	Fișier ICF	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	Fișierul conținând membrul	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPCST	Fișier	*OBJMGT sau *OBJALTER	*EXECUTE
RMVPFTRG	Fișier fizic	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	Fișierul conținând membrul	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F ⁴ (Q)	În-fișier	*ALL	Vedeți regulile generale.
	Din-fișier	*USE	*EXECUTE
	Pe baza fișierului fizic, dacă fișierul care este restaurat este unul logic (alternativ)	*CHANGE	*EXECUTE
	Descrierea dispozitiv pentru dischetă sau bandă	*USE	*EXECUTE
RTVMBRD	Fișier	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
SAVSAVFDTA	Descriere bandă, dischetă sau unitate optică	*USE	*EXECUTE
	Fișier de salvare	*USE	*EXECUTE
	Fișier Salvare/Restaurare optic ⁸ (dacă cel anterior există)	*RW	Nu se aplică
	Directorul părinte al OPTFILE ⁸	*WX	Nu se aplică
	Prefixul căii lui OPTFILE ⁸	*X	Nu se aplică
	Director rădăcină (/) volum optic ^{8,9}	*RWX	Nu se aplică
	Volum optic ¹⁰	*CHANGE	Nu se aplică
SAVS36F	Din-fișier	*USE	*EXECUTE
	În-fișier, atunci când este fișier fizic	*ALL	Vedeți regulile generale.
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
SAVS36LIBM	În-fișier, atunci când este fișier fizic	*ALL	Vedeți regulile generale.
	Din-fișier	*USE	*EXECUTE
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
STRAPF ³	Fișier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzile CRTPF, CRTLF, ADDPFM, ADDLFM și RMVM	*USE	*EXECUTE
STRDFU ³	Program (dacă se creează opțiune program)		*READ, *ADD
	Program (dacă există opțiunea de modificare sau ștergere program)	*OBJEXIST	*READ, *ADD
	File (dacă există opțiunea de modificare sau afișare date)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Fișier (dacă există opțiunea de afișare date)	*READ	*EXECUTE
UPDDTA	Fișier	*CHANGE	*EXECUTE
WRKDDMF ³	Fișier DDM	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF ^{3,5}	Fișiere	*OBJOPR	*USE
WRKPCST ³			*EXECUTE

¹ Comanda CPYFRMQRYP folosește un parametru FROMOPNID, nu FROMFILE. Un utilizator trebuie să aibă suficientă autorizare pentru a executa comanda OPNQRYP înainte de a rula comanda CPYFRMQRYP. Dacă se specifică CRTFILE(*YES) în comanda CPYFRMQRYP, primul fișier specificat în parametrul corespondent OPNQRYP FILE este considerat a fi fișierul-sursă când se determină autorizările pentru noul fișier-destinație.

² Este necesar drept de proprietate sau autorizare operațională pentru fișier.

³ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.

⁴ Dacă se creează un nou fișier și există un deținător de autorizare pentru el, atunci utilizatorul trebuie să aibă autorizarea toate (*ALL) pentru deținătorul de autorizare sau să fie posesorul acestuia. Dacă nu există un deținător de autorizare, proprietarul fișierului este utilizatorul care a introdus comanda RSTS36F și autorizarea publică este *ALL.

⁵ E necesară aceeași autorizare pentru obiect.

Comenzi fișier

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
6	Trebuie să aveți autorizarea specială *ALLOBJ.		
7	Autorizarea este verificată când este folosit fișierul 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 ștergeți volumul optic.		
10	Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția de suport optic.		
11	Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.		

Comenzi pentru filtrare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDALRACNE	Filtru	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filtru	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filtru	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filtru	*USE, *ADD	*EXECUTE
CHGALRACNE	Filtru	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filtru	*USE, *UPD	*EXECUTE
CHGFTR	Filtru	*OBJMGT	*EXECUTE
CHGPRBACNE	Filtru	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filtru	*USE, *UPD	*EXECUTE
CRTFTR	Filtru		*READ, *ADD
DLTFTR	Filtru	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filtru	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filtru	*USE, *DLT	*EXECUTE
WRKFTR ¹	Filtru	Orice autorizație	*EXECUTE
WRKFTRACNE ¹	Filtru	*USE	*EXECUTE
WRKFTRSLTE ¹	Filtru	*USE	*EXECUTE

¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.

Comenzi financiare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SBMFNCJOB (Q)	Descriere job și coadă de mesaje ¹	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Descriere job și coadă de mesaje ¹	*OBJOPR	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
WRKDEVTBL (Q)	Descriere dispozitiv ¹	Cel puțin o autorizare pentru date	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			

¹ Profilul utilizator QFNC trebuie să aibă această autorizare.

Operații grafice i5/OS

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGFCNUSG ⁵			
DSPFCNUSG			
EDTWSOAUT	Obiect stație de lucru ¹	*OBJMGT ^{2,3,4}	*EXECUTE
GRTWSOAUT	Obiect stație de lucru ¹	*OBJMGT ^{2,3,4}	*EXECUTE
RVKWSOAUT	Obiect stație de lucru ¹	*OBJMGT ^{2,3,4}	*EXECUTE
SETCSTDTA	Profilul utilizator sursă copiere	*CHANGE	*EXECUTE
	Profilul utilizator destinație copiere	*CHANGE	*EXECUTE
WRKFCNUSG			

¹ Obiectul stație de lucru este un obiect intern care e creat când instalați opțiunea i5/OS Operații grafice. Este livrat cu autorizarea publică *USE.

² Trebuie să fiți proprietar sau să aveți autorizarea *OBJMGT și autorizările care sunt acordate sau revocate.

³ Trebuie să fiți proprietar sau să aveți autorizarea *ALLOBJ pentru a acorda autorizarea *OBJMGT sau *AUTLMGT.

⁴ Pentru a securiza obiectul stație de lucru cu o listă de autorizare sau pentru a o înlătura, trebuie să aveți una din următoarele:
 Să dețineți obiectul stație de lucru.
 Să aveți autorizare *ALL pentru obiectul stație de lucru.
 Să aveți autorizarea specială *ALLOBJ.

⁵ Trebuie să aveți autorizarea specială administrator de securitate (*SECADM) pentru a modifica utilizarea acestei funcții.

Comenzi pentru set de simboluri grafice

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTGSS	Fișier 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 autorizații pentru obiect sunt necesare.

Comenzi pentru server gazdă

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită nici o autorizare obiect.	
ENDHOSTSVR (Q)	STRHOSTSVR (Q)

Comenzi pentru catalog imagini

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Tip obiect	Autorizație necesară	
			Pentru obiecte	Pentru biblioteca ¹
ADDIMGCLGE (Q)	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	*X	
	Numele dispozitivul când FROMDEV este specificat	*DEV	*USE	
	Fișier imagine când FROMFILE este specificat	*STMF	*R, *OBJMGT	
	Prefix cale fișier imagine când FROMFILE este specificat	*DIR	*X	
	Director părinte fișier imagine când FROMFILE este specificat	*DIR	*RX	
CHGIMGCLG (Q)	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
	Prefix cale catalog imagini nou când parametrul DIR este specificat	*DIR	Vedeți regulile generale.	
CHGIMGCLGE (Q)	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
CRTIMGCLG (Q)	QUSRSYS	*LIB		*READ, *ADD
	Catalog imagini dacă se specifică DIR(*REFIMGCLG)	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Prefix cale director catalog imagini ²	*DIR	Vedeți regulile generale.	
DLTIMGCLG (Q)	Catalog imagini	*IMGCLG	*OBJEXIST	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
LODIMGCLG (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Catalog imagini când se specifică WRTPTC(*ALL) sau WRTPTC(*NONE)	*IMGCLG	*CHANGE	*EXECUTE
	dispozitiv virtual	*DEV	*USE	
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
LODIMGCLGE (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	

Comandă	Obiect referențiat	Tip obiect	Autorizație necesară	
			Pentru obiecte	Pentru biblioteca ¹
RMVIMGCLGE (Q)	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
RTVIMGCLG (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Descrierea dispozitiv dacă parametrul DEV este specificat	*DEV	*USE	
VFYIMGCLG (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	dispozitiv virtual	*DEV	*USE	
	Prefix cale director catalog imagini	*DIR	Vedeți regulile generale.	
WRKIMGCLG (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE (Q)	Catalog imagini	*IMGCLG	*USE	*EXECUTE
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 conține noul director.			

Comenzi pentru sistem de fișiere integrat

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	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	Vedeți regulile generale.		

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
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 moștenită de la *FILE părinte)
		alt	QSYS.LIB	*OBJMGT
	Obiect la setarea *ALWCKPWRT	Orice	Toate	*OBJMGT
	Directorul care conține obiecte când se specifică SUBTREE(*ALL)	Orice director	Toate	*RX
	Obiect la setarea următoarelor atribute: *CRTOBJSCAN sau *SCAN ²⁶	*DIR și *STMF	QOpenSys, "root" (/), UDFS	
	Obiect la setarea următoarelor atribute: *SETUID, *SETGID, *RSTRDRNMUNL	Orice	Toate exceptând QSYS.LIB și QLDS	Drept de proprietate ¹⁵
*CRTOBJAUD ²⁸				
Prefix cale ²⁸	Vedeți regulile generale.			
CHGAUD ⁴				
CHGAUT	Obiect	Toate	QOpenSys, "root" (/), UDFS	Drept de proprietate ¹⁵
			QSYS.LIB, QOPT ¹¹	Drept de proprietate sau *ALLOBJ
			QLDS	Drept de proprietate, *ALL sau *ALLOBJ
				*OBJMGT
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
Directorul care conține obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	Toate	*RX	
CHGCURDIR	Obiect	Orice director		*R
	Volum optic	*DDIR	QOPT ⁸	*X
	Prefix cale	Vedeți regulile generale.		

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
CHGOWN ²⁴	Obiect	Toate	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Toate	QOpenSys, "root" (/), UDFS	Drept de proprietate și *OBJEXIST ¹⁵
		Toate	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT ¹¹	Drept de proprietate sau *ALLOBJ
CHGOWN ²⁴	Profilul utilizator al vechiului proprietar—toate mai puțin QOPT, QDLS	*USRPRF	Toate	*DLT
	Profilul utilizator al noului proprietar—toate mai puțin QOPT, QDLS	*USRPRF	Toate	*ADD
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
	Directorul care conține obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	Toate	*RX
CHGPGP	Obiect	Toate	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Toate	QOpenSys, "root" (/), UDFS	Drept de proprietate ^{5, 15}
		Toate	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT ¹¹	Drept de proprietate sau *ALLOBJ
CHGPGP	Profilul utilizator al vechiului grup primar—toate exceptând QOPT, QDLS	*USRPRF	Toate	*DLT
	Profilul utilizator al noului grup primar—toate exceptând QOPT, QDLS	*USRPRF	Toate	*ADD
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
	Directorul care conține obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	Toate	*RX

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
CHKIN	Obiect, dacă utilizatorul i-a anulat înregistrarea (check out).	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Obiect, dacă nu utilizatorul i-a anulat înregistrarea (check out).	*STMF	QOpenSys, "root" (/), UDFS	*ALL sau *ALLOBJ sau Drept de proprietate
		*DOC	QDLS	*ALL sau *ALLOBJ sau Drept de proprietate
	Cale, dacă nu e utilizatorul care l-a verificat.	*DIR	QOpenSys, "root" (/), UDFS	*X
Prefix cale	Vedeți regulile generale.			
CHKOUT	Obiect	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Prefix cale	Vedeți regulile generale.		
CPY ²⁵	Obiectul care e copiat, obiectul origine	Orice	QOpenSys, "root" (/), UDFS	*R și *OBJMGT sau drept de proprietate
		*DOC	QDLS	*RWX și *ALL sau drept de proprietate
		*MBR	QSYS.LIB	Nimic
		alte	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT ¹¹	*R
	Obiect destinație când e specificat REPLACE(*YES) (dacă obiectul destinație există deja)	Orice	Toate ¹⁰	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT ¹¹	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF sau LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Directorul copiat care conține obiecte când e specificat SUBTREE(*ALL), ce duce la copierea conținutului său	*DIR	QOpenSys, "root" (/), UDFS	*RX, *OBJMGT

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
CPY ²⁵	Cale (destinație), directorul părinte al obiectului destinație	*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 destinație	*DDIR	QOPT ⁸	*CHANGE	
CPY ²⁵	Director părinte al obiectului origine	*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR	QDLS	*X
		Alte	QSYS.LIB	*RX
		*DDIR	QOPT ¹¹	*X
	Prefix cale (destinație țintă)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
	Prefix cale (obiect origine)	*DDIR	QOPT ¹¹	*X
	CRTDIR ^{21, 22}	Director părinte	*DIR	QOpenSys, "root" (/), UDFS
*FLR			QDLS	*CHANGE
*FILE			QSYS.LIB	*RX, *ADD
Orice				*ADD
*DDIR			QOPT ¹¹	*WX
CRTDIR	Prefix cale	Vedeți regulile generale.		
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
CVTDIR (Q) ¹⁶				
DSPAUT	Obiect	Toate	QDLS	*ALL
		Toate	Toate celelalte	*OBJMGT sau drept de proprietate
		ALL	QOPT ¹¹	Nimic
	Volum optic	*DDIR	QOPT ⁸	*USE
	Prefix cale	Vedeți regulile generale.		

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
DSPCURDIR	Prefix cale	*DIR	QOpenSys, "root" (/), UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT ¹¹	*RX
DSPCURDIR	Director curent	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT ¹¹	*X
	Volum optic	*DDIR*	QOPT ⁸	*USE
DSPF	Fișier bază de date	*FILE	QSYS.LIB	*USE
	Biblioteca fișierului bază de date	*LIB	QSYS.LIB	*EXECUTE
	Fișier flux	*STMF	QOpenSys, "root" (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
	Prefix cale	Vedeți regulile generale.		
DSPLNK	Orice	Orice	"root" (/), QOpenSys, UDFS QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	Nimic
	Fișier, opțiunea 12 (Afișare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	"root" (/), QOpenSys, UDFS	*R
DSPLNK	Obiect legătură simbolic	*SYMLNK	"root" (/), QOpenSys, UDFS	Nimic
	Volum optic	*DDIR	QOPT ⁸	*USE
	Directorul părinte al obiectului referință - 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 referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
DSPLNK	Directorul părinte al obiectului referință - 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 referință- opțiunea 8 (Afișare 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 referință - opțiunea 12 (Afișare 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 referință - 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 referință părinte - model specificat ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Comenzi sistem de fişiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect ¹
DSPLNK	Prefixul obiectului referință părinte - opțiunea 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 referință părinte - opțiunea 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 conține 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 conține 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 conține obiectul -Fără model ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
DSPLNK	Nume cale relativă ¹⁴ : Prefixul directorul curent de lucru care conține 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	Nimic
	Prefix cale	Vedeți regulile generale.		
EDTF	Fișier bază de date, membru existent	*FILE	QSYS.LIB	*CHANGE
	Biblioteca fișiere bază de date	*LIB	QSYS.LIB	*EXECUTE
	Fișier bază de date, membru nou	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Biblioteca fișiere bază de date, membru nou	*LIB	QSYS.LIB	*EXECUTE, *ADD
	Fișier flux, fișier existent	*STMF	QOpenSys, "root" (/), UDFS	*R
	Spațiu utilizator	*USRSPC	QSYS.LIB	*CHANGE
	Directorul părinte la crearea unui nou fișier flux	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Prefix cale	Vedeți regulile generale.		
ENDJRN	Obiect	*DIR dacă subarborele (*ALL)	QOpenSys, "root" (/), UDFS	*R, *X, *OBJMGT
		*DIR dacă subarborele (*NONE), *SYMLNK, *STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Director părinte	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Prefix cale	Vedeți regulile generale.		
	Jurnal			*OBJMGT, *OBJOPR

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
MOV ¹⁹	Obiect mutat în interiorul aceluiași sistem de fișiere	*DIR	QOpenSys, "root" (/)	*OBJMGT, *W
		non *DIR	QOpenSys, "root" (/)	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	Nimic
		alt	QSYS.LIB	Nimic
		*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 (destinație), 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 (destinație)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	alte	*X
		*DDIR	QOPT ¹¹	*X
	Obiect mutat între sistemele de fișiere în QOpenSys, root sau QDLS (fișier flux *STMF și *DOC, numai *MBR).	*STMF	QOpenSys, "root" (/), UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Nu se aplică
	*DSTMF	QOPT ¹¹	*RW	
MOV	Mutat în QSYS *MBR	*STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT ¹¹	*RW

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
MOV	Cale (sursă) mutat prin sistemele de fișiere, director părinte	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS.LIB	drept de proprietate, *RX, *OBJEXIST
		*DDIR	QOPT ¹¹	*WX
	Prefix cale	Vedeți regulile generale.		
	Volum optic (sursă și destinație)	*DDIR	QOPT ⁸	*CHANGE
RCLLNK ¹⁶				
RLSIFSLCK ¹⁸	<i>some_stmf</i>	*STMF	"root" (/), QOpenSys, UDFS	*R
	Prefix cale	Vedeți 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
	Prefix cale	Vedeți regulile generale.		
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
RMVLNK ¹⁹	Obiect	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		alt	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT ¹¹	*W
		orice	QOpenSys, "root" (/), UDFS	*OBJEXIST

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	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
	Prefix cale	Vedeți regulile generale.		
	Volum optic	*DDIR	QOPT ⁸	*CHANGE
RNM ¹⁹	Obiect	*DIR	QOpenSys, "root" (/), UDFS	*OBJMGT, *W
		Non *DIR	QOpenSys, "root" (/), UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Nu se aplică
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		alte	QSYS.LIB	*OBJMGT
		*DSTMF	QOPT ¹¹	*W
	Volum optic (sursă și destinație)	*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

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
RST (Q) ²³	Obiectul, dacă există ²	Orice	QOpenSys, "root" (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Variază ¹⁰
			QDLS	*ALL
	Prefix cale	Vedeți regulile generale.		
	Directorul părinte creat de către operația de restaurare datorită CRTPRNDIR(*YES) ²	*DIR	QOpenSys, "root" (/), UDFS	*WX
Proprietarul directorului 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 utilizator care deține obiectul nou restaurat ²	*USRPRF	QSYS.LIB	*ADD
	Unitate de bandă, unitate de dischetă, unitate optică sau fișier de salvare	*DEVD, *FILE	QSYS.LIB	*RX
Definiție mediu de stocare	*MEDDFN	QSYS.LIB	*USE	
RST (Q)	Bibliotecă pentru descrierea dispozitivului, definiția mediului de stocare, sau fișierul de salvare	*LIB	QSYS.LIB	*EXECUTE
	Fișier sursă, dacă este specificat	*STMF	QOpenSys, "root" (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefix cale al fișierului ieșire	*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 și părinte dacă se restaurează de pe un dispozitiv optic	*DDIR	QOPT ¹¹	*X
	Fișierul optic dacă se restaurează de pe un dispozitiv optic	*DSTMF	QOPT ¹¹	*R

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	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	Obiect ²	Orice	QOpenSys, "root" (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Variază ¹⁰
			QDLS	*ALL
	Prefix cale	Vedeți regulile generale.		
	Unitate de bandă, unitate de dischetă sau unitate optică	*DEVD	QSYS.LIB	*RX
	Definiție mediu de stocare	*MEDDFN	QSYS.LIB	*USE
SAV	Fișier de salvare, dacă e gol	*FILE	QSYS.LIB	*USE, *ADD
	Fișier 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, definiția mediului de stocare, sau fișierul de salvare sau coadă de mesaje salvare-când-este-activ	*LIB	QSYS.LIB	*EXECUTE
SAV	Fișier sursă, dacă este specificat	*STMF	QOpenSys, "root" (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefix cale al fișierului ieșire	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*RX

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	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
	Fișier optic (Dacă există deja)	*DSTMF	QOPT ¹¹	*RW
SAVRST	Pe sistemul sursă, aceeași autorizare ca și cea necesară pentru comanda SAV.			
	Pe sistemul destinație, aceeași autorizare ca și cea necesară pentru comanda RST.			
STATFS	Obiect	Orice	Orice	Nimic
	Prefix cale	Vedeți regulile generale.		
STRJRN	Obiect	*DIR dacă subarborele (*ALL)	QOpenSys, "root" (/), UDFS	*R, *X, *OBJMGT
		*DIR dacă subarborele (*NONE), *SYMLNK, *STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Director părinte	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Prefix cale	Vedeți regulile generale.		
	Jurnal	*JRN		*OBJMGT, *OBJOPR
WRKAUT ^{6,7}	Obiect	*DOC sau *FLR	QDLS	*ALL
		Toate	not QDLS	*OBJMGT sau drept de proprietate
		*DDIR și *DSTMF	QOPT ¹¹	*NONE
	Prefix cale	Vedeți regulile generale.		
	Volum optic	*DDIR	QOPT ⁸	*USE

Comenzi sistem de fişiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect ¹
WRKLNK	Orice	Orice	"root" (/), QOpenSys, UDFS QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	Nimic
	Fişier, opțiunea 12 (Gestionare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	"root" (/), QOpenSys, UDFS	*R
	Obiect legătură simbolic	*SYMLNK	"root" (/), QOpenSys, UDFS	Nimic
	Volum optic	*DDIR	QOPT ⁸	*USE
WRKLNK	Directorul părinte al obiectului referință - 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 referință - 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 referință - opțiunea 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 referință - opțiunea 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

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
WRKLNK	Directorul părinte al obiectului referință - 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 referință 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 referință părinte - opțiunea 8 (Afișare atribute)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Prefixul obiectului referință părinte - opțiunea 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

Comenzi sistem de fișiere integrat

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
WRKLNK	Nume cale relativă ¹⁴ : Directorul curent de lucru care conține 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 conține 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 conține 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 conține 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 fișiere integrat.

² Dacă aveți autorizare specială *SAVSYS, nu aveți nevoie de autorizarea specificată pentru sistemele de fișiere QSYS.LIB, QDLS, QOpenSys și "root".

³ Autorizarea necesară variază în funcție de tipul obiectului. Vedeți descrierea API-ului QLIRNMO în Centrul de informare. Dacă obiectul este un membru bază de date, vedeți autorizările pentru comanda RNMM (Rename Member - Redenumire membru).

⁴ Trebuie să aveți 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 referențiat	Tip obiect	Sistem fișier	Autorizare necesară pentru obiect ¹
6	Dacă profilul care este specificat folosind parametrul PRNDIROWN nu este utilizatorul făcând operația de restaurare, este necesară autorizare specială *SAVSYS sau *ALLOBJ.			
7	Aceste comenzi necesită ca autorizarea afișată plus autorizările necesare pentru comanda DSPCURDIR.			
8	Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția de suport optic.			
9	Pentru informații despre restricții privind această comandă, vedeți Capitolul 7 din cartea Suportul optic iSeries.			
10	Autorizarea necesară variază după comanda nativă folosită. Vedeți 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 și directorul curent de lucru este '/home/john', atunci obiectul accesat este '/home/john/a/b'.			
15	Dacă aveți autorizarea specială *ALLOBJ, nu aveți nevoie de autorizarea menționată.			
16	Trebuie să aveți autorizația specială *ALLOBJ pentru a folosi această comandă.			
17	În tabelul de mai sus, QSYS.LIB se referă la sistemul de fișiere QSYS.LIB al ASP-ului independent, precum și la sistemul de fișiere QSYS.LIB.			
18	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.			
19	Dacă atributul redenumiri și dezlegări restricționate (cunoscut de asemenea ca bit S_ISVTX) este activat pentru un director, va restricționa dezlegarea obiectelor de la acel director, numai dacă una din aceste autorizări nu e îndeplinită: *ALLOBJ; utilizatorul este deținătorul obiectului dezlegat; sau utilizatorul este proprietarul directorului.			
20	Dacă se specifică RMVLNK (*YES), utilizatorul trebuie să aibă autorizarea *OBJEXIST pentru toate obiectele din directorul specificat.			
21	Pentru QSYS.LIB, "root", QOpenSys și sisteme de fișiere 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) și *SECADM (administrator securitate) pentru a specifica o valoare pentru parametrul CRTOBJSCAN (opțiunea Scanare pentru obiecte) alta decât *PARENT.			
23	Trebuie să aveți autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.			
24	Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ și *SECADM când schimbă proprietarul unui fișier flux (*STMF) cu un program Java atașat a cărui verificare de autoritate în timpul rulării include utilizatorul și proprietarul.			
25	Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ și *SECADM când copiază un fișier flux (*STMF) cu un program Java atașat a cărui verificare de autoritate în timpul rulării include utilizatorul și proprietarul.			
26	Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ și *SECADM pentru a specifica atributele *CRTOBJSCAN și *SCAN.			
27	Când afișați conținutul directorului /QSYS.LIB, obiectele profil utilizator (*USRPRF) asupra cărora apelantul nu are nici o autorizare (cum ar fi *EXCLUDE) nu sunt returnate.			
28	Utilizatorul trebuie să aibă autorizare specială *AUDIT pentru a modifica noul atribut *CRTOBJAUD și utilizatorul nu are nevoie de autorizările normale de prefix nume cale (*X și *R).			

Comenzi de definire interactivă a datelor

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDTADFN	Dicționar de date	*CHANGE	*EXECUTE
	Fișier	*OBJOPR, *OBJMGT	*EXECUTE
CRTDTADCT	Dicționar de date		*READ, *ADD
DLTDTADCT ³	Dicționar de date	OBJEXIST, *USE	
DSPDTADCT	Dicționar de date	*USE	*EXECUTE
LNKDTADFN ¹	Dicționar de date	*USE	*EXECUTE
	Fișier	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT ²	Dicționar de date	*OBJOPR	*EXECUTE
WRKDBFIDD ²	Dicționar de date	*USE ⁴	*EXECUTE
	Fișier bază de date	*OBJOPR	*EXECUTE
WRKDTADFN ¹	Dicționar de date	*USE, *CHANGE	*EXECUTE
¹	Nu e necesară autorizare pentru dicționarul de date pentru a dezlega un fișier.		
²	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
³	Înainte ca dicționarul să fie șters, toate fișierele legate sunt dezlegate. Consultați comanda LNKDTADFN pentru autorizarea necesară pentru a dezlega un fișier.		
⁴	Aveți nevoie de autorizarea de utilizare pentru dicționarul de date pentru a crea un nou fișier. Nu e necesară nici o autorizare pentru dicționarul de date pentru a introduce date într-un fișier existent.		

Comenzile IPX (Intrare job la distanță)

Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTIPXD	Descriere IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Descriere IPX	*USE	*EXECUTE
WRKIPXD	Descriere IPX	*OBJOPR	*EXECUTE

Comenzi pentru index de căutare informații

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSCHIDX	Index de căutare	*CHANGE	*USE
	Grup de panouri	*USE	*EXECUTE
CHGSCHIDX	Index de căutare	*CHANGE	*USE
CRTSCHIDX	Index de căutare		*READ, *ADD
DLTSCHIDX	Index de căutare	*OBJEXIST	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RMVSCCHIDX	Index de căutare	*CHANGE	*USE
STRSCHIDX	Index de căutare	*USE	*EXECUTE
WRKSCCHIDX ¹	Index de căutare	*ANY	*USE
WRKSCCHIDX	Index de căutare	*USE	*USE

Comenzile pentru attribute IPL

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită autorizare pentru nici un obiect:
CHGIPLA (Q) ¹ DSPIPLA
¹ Pentru a folosi această comandă trebuie să aveți autorizările speciale *SECADM și *ALLOBJ.

Comenzile pentru Java

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZJVM	Comandă QSYS/STRSRVJOB	*USE	
	Comandă QSYS/STRDBG	*USE	
DSPJVMJOB ¹	Joburi Java Virtual Machine		
¹ Trebuie să aveți autorizația specială *JOBCTL pentru a folosi această comandă.			

Comenzi pentru job

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
BCHJOB	Descriere job ^{9,11}	*USE	*EXECUTE
	Bibliotecile din lista de biblioteci (sistem, curent și utilizator) ⁷	*USE	
	Profil utilizator din descrierea jobului ¹⁰	*USE	
	Tabelă secvență de sortare ⁷	*USE	*EXECUTE
	Coadă de mesaje ¹⁰	*USE, *ADD	*EXECUTE
	Coadă de joburi ^{10,11}	*USE	*EXECUTE
	Coadă de ieșire ⁷	*READ	*EXECUTE
CHGACGCDE ¹			

Comenzi job

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGGRPA ⁴	Coadă 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 ieșire, dacă se modifică coada de ieșire ⁷	*READ	*EXECUTE
	Coadă de ieșire curentă, dacă se modifică coada de ieșire	*READ	*EXECUTE
	Tabelă secvență de sortare ⁷	*USE	*EXECUTE
CHGPJ	Profil utilizator pentru pornire program necesită specificarea *PGMSTRRQS	*USE	*EXECUTE
	Profil utilizator și 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			
DMPUSRTRC	Buffer urmărire utilizator ¹⁵	*OBJOPR	*EXECUTE
DSCJOB ¹			
DSPACTPJ			
DSPJOB ¹			
DSPJOBTL			
DSPJOBLOG ^{1,5}	Fișierul de ieșire și membrul există	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Membrul nu există	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Fișierul de ieșire nu există	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB ¹			
ENDJOBABN ¹			
ENDLOGSVR ⁶			
ENDPJ ⁶			
HLDJOB ¹			
RLSJOB ¹			
RRTJOB			
RTVJOBA			
SBMDBJOB	Fișier bază de date	*USE	*EXECUTE
	Coadă joburi	*READ	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SBMDKTJOB	Coadă mesaje	*USE, *ADD	*EXECUTE
	Coadă de joburi și descriere dispozitiv	*READ	*EXECUTE
SBMJOB ^{2, 12}	Descriere job ^{9,11}	*USE	*EXECUTE
	Bibliotecile din lista de biblioteci (sistem, curent și utilizator) ⁷	*USE	
	Coadă de mesaje ¹⁰	*USE, *ADD	*EXECUTE
	Profilul utilizator ^{10,11}	*USE	
	Profil utilizator din descrierea jobului ¹⁰	*USE (la nivel 40)	
	Coadă de joburi ^{10,11}	*USE	*EXECUTE
	Coadă de ieșire ⁷	*READ	*EXECUTE
	Tabelă secvență de sortare ⁷	*USE	*EXECUTE
	Dispozitive ASP din grupul ASP inițial	*USE	
SBMNETJOB	Fișier bază de date	*USE	*EXECUTE
STRLOGSVR ⁶			
STRPJ ⁶	Descriere subsistem	*USE	
	Program	*USE	*EXECUTE
TFRBCHJOB	Coadă joburi	*READ	*EXECUTE
TFRGRPJOB	Program primul grup	*USE	*EXECUTE
TFRJOB ⁸	Coadă joburi	*USE	*EXECUTE
	Descrierea subsistemului la care e alocată coada de joburi	*USE	
TFRSECJOB			
WRKACTJOB			
WRKASPJOB	Descriere dispozitiv	*USE	
WRKJOB ¹			
WRKJOBLOG			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

Comenzi job

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
1	Orice utilizator poate rula aceste comenzi pentru joburi care rulează sub propriul său profil utilizator. Un utilizator cu autorizarea specială control job (*JOBCTL) poate rula aceste comenzi pentru orice job. Dacă aveți autorizarea specială *SPLCTL, nu aveți nevoie de nici o autorizare pentru coada de joburi. Totuși, aveți nevoie de autorizare pentru biblioteca în care se află coada de joburi.		
2	Trebuie să aveți autorizare (specificată în profilul dumneavoastră utilizator) pentru prioritatea de planificare și prioritatea de ieșire 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 și TSEPOOL.		
4	Această comandă afișează doar jobul în care a fost specificată.		
5	Pentru a afișa un istoric de job pentru un job care are autorizarea specială toate obiectele (*ALLOBJ), trebuie să aveți autorizarea specială *ALLOBJ sau să fiți autorizat pentru funcția Istoric job pentru toate obiectele i5/OS prin suportul de Administrare aplicație din Navigator iSeries. Se poate folosi comanda CHGFCNUSG (Change Function Usage), cu un ID funcție de QIBM_ACCESS_ALLOBJ_JOBLOG, pentru a modifica lista de utilizatori cărora le este permis să afișeze un istoric de job pentru un job cu autorizarea specială *ALLOBJ.		
6	Pentru a folosi această comandă, e necesară autorizarea specială control job *JOBCTL.		
7	Profilul utilizator sub care rulează jobul lansat este verificat pentru autorizare pentru obiectul referință. Autorizarea adoptată a utilizatorului care lansează sau modifică jobul nu e folosită.		
8	Dacă jobul transferat este unul interactiv, se aplică următoarele restricții: <ul style="list-style-type: none"> • Coada de joburi în care e plasat jobul trebuie să fie asociată cu un subsistem activ. • Stația de lucru asociată cu jobul trebuie să aibă o intrare de stație de lucru corespondentă în descrierea de subsistem asociată cu noul subsistem. • Stația 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 și profilul utilizator sub care rulează jobul sunt verificate pentru autorizare pentru obiectul referință.		
10	Utilizatorul care lansează jobul este verificat pentru autorizare pentru obiectul referință.		
11	E folosită autorizarea adoptată a utilizatorului care lansează comanda CHGJOB sau SBMJOB.		
12	Trebuie să fiți autorizat pentru profilul utilizator și descrierea jobului; profilul utilizator trebuie să fie de asemenea autorizat pentru descrierea jobului.		
13	Pentru a modifica anumite atribute ale jobului, chiar în propriul job al utilizatorului, sunt necesare autorizările speciale de control job (*JOBCTL) și toate obiectele (*ALLOBJ).		
14	Orice utilizator poate rula aceste comenzi pentru joburi care rulează sub propriul său profil utilizator. Un utilizator cu autorizarea specială control job (*JOBCTL) poate rula aceste comenzi pentru orice job.		
15	Un buffer de urmărire utilizator este un obiect spațiu utilizator (*USRSPC) din biblioteca QUSRSYS, cu numele QPOZnnnnnn, unde 'nnnnnn' este numărul jobului care folosește facilitatea de urmărire utilizator.		

Comenzi pentru descriere de job

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comenzi descriere de job

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGJOB	Descriere job	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil utilizator (USER)	*USE	
CPYAUDJRNE ⁸	Fișierul de ieșire deja există	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Fișierul de ieșire nu există		*EXECUTE *ADD
CRTJOB (Q)	Descriere job		*READ, *ADD
	Profil utilizator (USER)	*USE	
DLTJOB	Descriere job	*OBJEXIST	*EXECUTE
DSPJOB	Descriere job	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT ¹			
WRKJOB	Descriere job	Orice	*USE

¹ Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzi pentru coadă de joburi

Comandă	Obiect referențiat	Parametri coadă de joburi ⁴		Autorizare specială	Autorizație necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru biblioteci
CLRJOBQ ¹	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ ¹	Coadă joburi					*READ, *ADD
DLTJOBQ	Coadă joburi				*OBJEXIST	*EXECUTE
HLDJOBQ ¹	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT ⁵						
RLSJOBQ ¹	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ ^{1,3}	Coadă joburi	*DTAAUT			*READ	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

Comenzi coadă de joburi

Comandă	Obiect referențiat	Parametri coadă de joburi ⁴		Autorizare specială	Autorizație necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
¹	Dacă aveți autorizarea specială *SPLCTL, nu aveți nevoie de nici una pentru coada de joburi, dar aveți nevoie de autorizare pentru biblioteca în care se află coada de joburi.					
²	Trebuie să fiți proprietarul cozii de joburi.					
³	Dacă cereți să lucrați cu toate cozile de joburi, ecranul listă include toate cozile de joburi din bibliotecă pentru care aveți autorizare *EXECUTE.					
⁴	Pentru a afișa parametrii cozii de joburi, folosiți API-ul QSPRJOBQ.					
⁵	Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.					

Comenzi pentru planificare job

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
ADDJOBSCDE	Planificare job	*CHANGE	*EXECUTE
	Descriere job ¹	*USE	*EXECUTE
	Coadă de joburi ^{1,2}	*READ	*EXECUTE
	Profil 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 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 și cel sub care rulează jobul sunt verificate pentru autorizare pentru obiectul referință.		
²	Autorizarea pentru coada de joburi nu poate veni din autorizare adoptată.		
³	Trebuie să aveți autorizarea specială *JOBCTL sau să fi adăugat intrarea.		
⁴	Pentru a afișa detaliile unei intrări (opțiunea 5 sau formatul de tipărire *FULL), trebuie să aveți autorizarea specială *JOBCTL sau să fi adăugat intrarea.		

Comenzi pentru jurnal

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director
ADDRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal destinație		*EXEC, *ADD
APYJRNCHG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiecte non-IFS ale căror modificări jurnalizate sunt aplicate	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	Obiecte IFS ale căror modificări jurnalizate sunt aplicate	*RW, *OBJMGT	*RX dacă subarborele (*ALL)
APYJRNCHGX (Q)	Jurnal	*USE	
	Receptor jurnal	*USE	
	Fișier	*OBJMGT, *CHANGE, *OBJEXIST'	*EXECUTE, *ADD
CHGJRN (Q)	Receptor jurnal, dacă se specifică	*OBJMGT, *USE	*EXECUTE
	Receptor jurnal atașat	*OBJMGT, *USE	*EXECUTE
	Jurnal	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Jurnal dacă se specifică RCVSIZOPT(*MINFIXLEN).	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNOBJ ⁹		*OBJOPR, *OBJMGT	
	Obiecte non-IFS	*READ, *OBJMGT	
	Obiecte IFS *R	*OBJMGT	
	Cale obiect SUBTREE(*ALL) *RX	*OBJMGT	
	Cale obiect SUBTREE(*NONE) *R	*OBJMGT	
	Director părinte *X		
CHGRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal sursă	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fișier	*USE	*EXECUTE
CPYAUDJRNE ⁸	Fișierul de ieșire deja există	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fișierul de ieșire nu există		*EXECUTE, *ADD
CRTJRN	Jurnal		*READ, *ADD
	Receptor jurnal	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Jurnal	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE ⁸			

Comenzi jurnal

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director
DSPJRN ⁶	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fișierul specificat a fost șters din sistem sau se specifică *IGNOBSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanță.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Este specificat obiect sistem de fișiere neintegrat	*USE	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
	Este specificat obiect sistem de fișiere integrat	*R (Ar putea fi de asemenea *X dacă obiect este un director și SUBTREE (*ALL) este specificat)	*X
DSPJRNMNU ¹			
ENDJRN	Vedeți "Comenzi pentru sistem de fișiere integrat" la pagina 347.		
ENDJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fișier	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNOBJ	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fișier	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP ²			
JRNPF ³			
RCVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fișierul specificat a fost șters din sistem sau se specifică *IGNOBSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanță.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Este specificat obiect sistem de fișiere neintegrat	*USE	*EXECUTE
	Este specificat obiect sistem de fișiere integrat	*R (Ar putea fi de asemenea *X dacă obiect este un director și SUBTREE (*ALL) este specificat)	*X
	Program ieșire	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiecte non-IFS ale căror modificări jurnalizate sunt înlăturate	*OBJMGT, *CHANGE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director
RTVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fișierul specificat a fost șters din sistem sau se specifică *IGNOBSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanță.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Este specificat obiect sistem de fișiere neintegrat	*USE	*EXECUTE
	Este specificat obiect sistem de fișiere integrat	*R (Ar putea fi de asemenea *X dacă obiect este un director și 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	Vedeți "Comenzi pentru sistem de fișiere integrat" la pagina 347.		
STRJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fișier	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNPf	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fișier	*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 și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Receptor jurnal ⁵	*OBJOPR și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
¹	Vedeți comanda WRKJRN (această comandă are aceeași funcție)		
²	Vedeți comanda STRJRNAP.		
³	Vedeți comanda STRJRNPf.		
⁴	E necesară autorizare suplimentară pentru funcții specifice apelate în timpul operației selectate. De exemplu, pentru a restaura un obiect trebuie să aveți autorizarea necesară pentru comanda RSTOBJ sau RST.		
⁵	Sune necesare autorizările *OBJOPR și *OBJEXIST pentru receptori jurnal dacă opțiunea este aleasă pentru a șterge receptori.		

Comenzi jurnal

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director
6	Pentru a specifica JRN(*INTSYSJRN), trebuie să aveți autorizarea specială *ALLOBJ.		
7	E necesară autorizarea *READ pentru biblioteca jurnalului pentru a afișa meniul WRKJRN. E necesară autorizarea *EXECUTE pentru bibliotecă pentru a folosi o opțiune din meniu.		
8	Trebuie să aveți autorizația specială *AUDIT pentru a folosi această comandă.		
9	Pentru a specifica PTLNS(*ALWUSE), trebuie să aveți autorizarea specială *ALLOBJ.		

Comenzi pentru receptor de jurnal

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTJRNRCV	Receptor jurnal		*READ, *ADD
DLTJRNRCV	Receptor jurnal	*OBJOPR, *OBJEXIST și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Jurnal	*OBJOPR	*EXECUTE
DSPJRNRCVA	Receptor jurnal	*OBJOPR și o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Jurnal, dacă e atașat	*OBJOPR	*EXECUTE
WRKJRNRCV ^{1, 2, 3}	Receptor jurnal	Orice autorizație	*USE
1	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		
2	Sune necesare autorizările *OBJOPR și *OBJEXIST pentru receptori jurnal dacă opțiunea este aleasă pentru a șterge receptori.		
3	Sunt necesare *OBJOPR și altă autorizare de date decât *EXECUTE pentru receptorii de jurnal dacă este aleasă opțiunea de afișare descriere.		

Comenzi pentru limbaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTBNDC	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	*USE	*EXECUTE
	Fișierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	Vedeți regulile generale.	*READ, *ADD

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTBNDCL	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Director legare	*USE	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTBNDCL	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	Vedeți regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTBNDCL	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	*USE	*EXECUTE
	Fișierul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	Vedeți regulile generale.	*READ, *ADD
	Anteturi generate de parametrul TEMPLATE	*USE	*EXECUTE
CRTBNDCL	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Director legare	*USE	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTBNDCL	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCLD	Fișier sursă	*USE	*EXECUTE
	Obiect Locale - REPLACE(*NO)		*READ, *ADD
	Obiect Locale - REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD

Comenzi limbaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTCLMOD	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	Vedeți regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCLPGM	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	Vedeți regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCLPGM (COBOL/400* program licențiat sau mediu S/38)	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCMOD	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Fișierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	*USE	*EXECUTE
	Fișierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	Vedeți regulile generale.	*READ, *ADD
CRTCPMOD	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	*USE	*EXECUTE
	Fișierul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	Vedeți regulile generale.	*READ, *ADD
	Anteturi generate de parametrul TEMPLATE	*USE	*EXECUTE
CRTRPGMOD	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTRPGPGM (RPG/400* program licențiat sau mediu S/38)	Fișier sursă	*USE	*EXECUTE
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTRPTPGM (RPG/400 program licențiat și mediu S/38)	Fișier sursă	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Fișier sursă pentru program RPG generat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișiere dispozitiv descrise extern și fișiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTS36CBL (mediu S/36)	Fișier sursă	*USE	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTS36RPG	Fișier sursă	*USE	*READ, *ADD
	Program: REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTS36RPGR	Fișier sursă	*USE	*READ, *ADD
	Fișier de afișare: REPLACE(*NO)		*READ, *ADD
	Fișier de afișare: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTS36RPT	Fișier sursă	*USE	*EXECUTE
	Fișier sursă pentru program RPG generat	Vedeți regulile generale.	Vedeți regulile generale.
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
CRTSQLCI OS/400' (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comenzi limbaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTSQLCBL (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLCBLI (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLCPPI OS/400' (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLFTN (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecii
CRTSQLPLI OS/400' (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLRPG (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLRPGI OS/400' (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CVTRPGSRC	Fișier sursă	*USE	*EXECUTE
	Fișier ieșire	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Fișier istoric	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
CVTSQLCPP ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
	Fișier sursă destinație	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificații descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
ENDCBLDBG (COBOL/400 programul licențiat sau mediul S/38)	Program	*CHANGE	*EXECUTE

Comenzi limbaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENTCBLDBG (mediu S/38)	Program	*CHANGE	*EXECUTE
DLTCLD	Obiect Locale	*OBJEXIST, *OBJMGT	*EXECUTE
RTVCLDSRC	Obiect Locale	*USE	*EXECUTE
	În-fișier	Vedeți regulile generale.	Vedeți regulile generale.
RUNSQLSTM ¹	Fișier sursă	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRREXPRC	Fișier sursă	*USE	*EXECUTE
	Program ieșire	*USE	*EXECUTE
STRSQL (DB2 Query Manager și SQL Development pentru programul licențiat i5/OS) ¹	Tabelă secvență de sortare	*USE	*EXECUTE
	Descriere dispozitiv imprimantă	*USE	*EXECUTE
	Coadă de ieșire imprimantă	*USE	*EXECUTE
	Fișier imprimantă	*USE	*EXECUTE

¹ Vedeți informațiile **Autorizarea, privilegiile și proprietatea obiectului** din Referințe SQL DB2 for iSeries (în Centrul de informare iSeries) pentru informații suplimentare despre cerințele de securitate pentru instrucțiunile SQL.

Comenzi pentru bibliotecă

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă asupra căreia se acționează
ADDLIBLE	Bibliotecă		*USE
CHGCURLIB	Bibliotecă curentă nouă		*USE
CHGLIB ⁸	Bibliotecă		*OBJMGT
CHGLIBL	Fiecare bibliotecă care e pusă în lista de biblioteci		*USE
CHGSYSLIBL (Q)	Bibliotecile din noua listă		*USE
CLRLIB ³	Fiecare obiect care e șters din bibliotecă	*OBJEXIST	*USE
	Tipurile de obiecte *DTADCT ¹⁴ , *JRN ¹⁴ , *JRNRCV ¹⁴ , *MSGQ ¹⁴ , *SBSD ¹⁴	Vedeți autorizarea cerută de comanda DLTxxx pentru tipul de obiect	
	Dispozitiv ASP (dacă e specificat)	*USE	

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acționează
CPYLIB ⁴	Biblioteca sursă		*USE
	Biblioteca destinație, dacă ea există		*USE, *ADD
	Comenzile CHKOBJ, CRTDUPOBJ	*USE	
	Comanda CRTLIB, dacă biblioteca destinație este creată	*USE	
	Obiectul care e copiat	Autorizarea care e cerută când folosiți comanda CRTDUPOBJ pentru a copia tipul obiectului.	
CRTLIB ⁹	Dispozitiv ASP (dacă e specificat)	*USE	
DLTLIB ³	Fiecare obiect care e șters din bibliotecă	*OBJEXIST	*USE, *OBJEXIST
	Tipurile de obiecte *DTADCT ¹⁴ , *JRN ¹⁴ , *JRNRCV ¹⁴ , *MSGQ, *SBSD ¹⁴	Vedeți autorizarea cerută de comanda DLTxxx pentru tipul de obiect	
	Dispozitiv ASP (dacă e specificat)	*USE	
DSPLIB	Biblioteca		*READ
	Obiectele din biblioteca ⁵	O autorizare alta decât *EXCLUDE	
	Dispozitiv ASP (dacă e specificat)	*EXECUTE	
DSPLIBD	Biblioteca		O autorizare alta decât *EXCLUDE
EDTLIBL	Biblioteca de adăugat la listă		*USE
RCLLIB	Biblioteca		*USE, *OBJEXIST

Comenzi bibliotecă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acționează
RSTLIB ⁷ (Q)	Definiție mediu de stocare	*USE	*EXECUTE
	Biblioteca, dacă există		*READ, *ADD
	Cozile de mesaje care sunt restaurate în biblioteca unde există deja	*OBJOPR, *OBJEXIST ⁷	*EXECUTE. *READ, *ADD
	Programe care adoptă autorizarea	Proprietar sau *ALLOBJ și *SECADM	*EXECUTE
	Biblioteca salvată dacă se specifică VOL(*SAVVOL)		*USE ⁶
	Fiecare obiect care e restaurat peste în bibliotecă	*OBJEXIST ³	*EXECUTE, *READ, *ADD
	Profilul utilizator care deține obiectele care sunt create	*ADD ⁶	
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale	Vedeți regulile generale
	Fișierul referință de câmp QSYS/QASAVOBJ pentru fișierul de ieșire, dacă un fișier de ieșire este specificat și nu există.	*USE	*EXECUTE
RSTLIB ⁷ (Q)	Fișier bandă (QSYSTAP) sau dischetă (QSYSDKT)	*USE ⁶	*EXECUTE
	Ieșire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Fișier de salvare	*USE	*EXECUTE
	Fișier optic (OPTFILE) ¹²	*R	Nu se aplică
	Prefix cale al fișierului optic (OPTFILE) ¹²	*X	Nu se aplică
	Volum optic ¹¹	*USE	
	Descriere dispozitiv ASP ¹⁵	*USE	
RSTS36LIBM	Din-fișier	*USE	*EXECUTE
	În-fișier	*CHANGE	*EXECUTE
	Biblioteca destinație	*CHANGE	*EXECUTE
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVLIBD	Biblioteca		O autorizare alta decât *EXCLUDE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acționează
SAVLIB	Fiecare obiect din bibliotecă	*OBJEXIST ⁶	*READ, *EXECUTE
	Definiție mediu de stocare	*USE	*EXECUTE
	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier 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
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Fișierul referință câmp QSYS/QASAVOBJ, dacă fișierul de ieșire este specificat și nu există	*USE ⁶	*EXECUTE
	Ieșire imprimantă QSYS/QPSAVOBJ	*USE ⁶	*EXECUTE
	Spațiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE
SAVLIB	Fișier optic ¹²	*RW	Nu se aplică
	Directorul părinte al fișierului optic (OPTFILE) ¹²	*WX	Nu se aplică
	Prefix cale al fișierului optic (OPTFILE) ¹²	*X	Nu se aplică
	Director rădăcină (/) volum optic ^{12, 13}	*RWX	Nu se aplică
	Volum optic ¹¹	*CHANGE	
	Descriere dispozitiv ASP ¹⁵	*USE	
SAVRSTLIB	Pe sistemul sursă, aceeași autorizare precum se cere prin comanda SAVLIB.		
	Pe sistemul destinație, aceeași autorizare precum se cere prin comanda RSTLIB.		
SAVS36LIBM	Salvare într-un fișier fizic	*OBJOPR, *OBJMGT	*EXECUTE
	Fie QSYSDKT pentru dischetă fie QSYSTAP pentru bandă și toate comenzile au nevoie de autorizare pentru dispozitiv	*OBJOPR	*EXECUTE
	Salvare într-un fișier dacă e specificat MBROPT(*ADD)	*ADD	*READ, *ADD
	Salvare într-un fișier fizic dacă e specificat MBROPT(*REPLACE)	*ADD, *DLT	*EXECUTE
	Biblioteca sursă		*USE
WRKLIB ^{10, 16}	Biblioteca		*USE

Comenzi bibliotecă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acționează
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 șterse și bibliotecă nu e complet golită și ștearsă. Doar obiectele autorizate sunt șterse.		
4	Toate restricțiile care se aplică pentru comanda CRTDUPOBJ, se aplică de asemenea și la aceasta.		
5	Dacă nu aveți autorizare pentru un obiect din bibliotecă, textul pentru obiect spune *NOT AUTHORIZED.		
6	Dacă aveți autorizarea specială *SAVSYS, nu aveți nevoie de autorizarea specificată.		
7	Trebuie să aveți autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.		
8	Trebuie să aveți autorizarea specială *AUDIT pentru a modifica valoarea CRTOBLAUD pentru o bibliotecă. *OBJMGT nu e necesară dacă modificați doar valoarea CRTOBLAUD. *OBJMGT este necesară dacă modificați valoarea CRTOBLAUD și alte valori.		
9	Trebuie să aveți autorizarea specială *AUDIT pentru a specifica o valoare CRTOBLAUD alta decât *SYSVAL.		
10	Trebuie să aveți autorizarea cerută de operație pentru a folosi o operație individuală.		
11	Volumul optic nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția 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 ștergeți volumul optic.		
14	Acest obiect este permis pe ASP independent.		
15	Autorizarea este necesară doar dacă operația de salvare sau restaurare necesită o comutare a spațiului de nume de bibliotecă.		
16	Această comandă cere autorizarea specială *ALLOBJ.		

Comenzi pentru cheie de licență

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDLICKEY (Q)	Fișier ieșire	*USE	*EXECUTE
DSPLICKEY (Q)	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
RMVLICKEY (Q)	Fișier ieșire	*CHANGE	*EXECUTE

Comenzi pentru program cu licență

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGLICINF (Q)	Comanda WRKLCINF	*USE	*EXECUTE
DLTLICPGM ^{1,2} (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM ^{1,2} (Q)			
SAVLICPGM ^{1,2} (Q)			
WRKLCINF (Q)			
¹	Unele programe cu licență pot fi șterse, salvate sau restaurate doar dacă sunteți înscris în directorul de distribuție al sistemului.		
²	La ștergerea, restaurarea sau salvarea unui program cu licență care conține foldere, toate restricțiile care se aplică comenzii DLTDL0 se aplică de asemenea și acesteia.		
³	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		

Comenzi pentru descriere de linie

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGLINASC ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTIN sau CNNLSTOUT)	*USE	*EXECUTE
	Descriere interfață de rețea (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS ²	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE

Comenzi descriere de linie

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTLINASC ²	Descriere controler (CTL și SWTCTLLST)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINBSC ²	Descriere controler (SWTCTLLST și CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINDDI ²	Descriere de linie		*READ, *ADD
	Descriere interfață de rețea (NWI)	*USE	*EXECUTE
	Descriere controler (NETCTL)	*USE	*EXECUTE
CRTLINETH ²	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
	Descriere interfață de rețea (NWI)	*USE	*EXECUTE
	Descriere server de rețea (NWS)	*USE	*EXECUTE
CRTLINFAX ²	Descriere de linie		*READ, *ADD
	Descriere controler	*USE	*EXECUTE
CRTLINFR ²	Descriere de linie		*READ, *ADD
	Descriere interfață de rețea (NWI)	*USE	*EXECUTE
	Descriere controler (NETCTL)	*USE	*EXECUTE
CRTLINPPP ²	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINS DLC ²	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINTDLC ²	Descriere controler (WSC și CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINTRN ²	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
	Descriere interfață de rețea (NWI)	*USE	*EXECUTE
	Descriere server de rețea (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 interfață de rețea (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}			

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RSMLINRCY	Descriere de linie	*OBJOPR	*EXECUTE
WRKLIND ¹	Descriere de linie	*OBJOPR	*EXECUTE
¹	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
²	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.		
³	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *ALLOBJ.		

Comenzi pentru rețea locală (LAN)

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită nici o autorizație obiect:			
ADDLANADPI	DSPLANADPP	RMVLANADPT (Q)	WRKLANADPT
CHGLANADPI	DSPLANSTS	RMVLANADPI	

Comenzi pentru locale

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTLOCALE	Fișier sursă	*USE	*USE, *ADD
DLTLOCALE	Locale	*OBJEXIST	*USE

Comenzi pentru cadru de lucru server de poștă

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Această comandă nu necesită nici o autorizare pentru obiect:	
ENDMSF (Q)	STRMSF (Q)

Comenzi pentru mediu

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
CFGDEVMLB ¹	Descriere bibliotecă bandă	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Descriere bibliotecă bandă	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA ⁴	Descriere bibliotecă bandă	*CHANGE	*EXECUTE
CHGTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
CHKDKT	Descriere unitate de dischetă	*USE	*EXECUTE

Comenzi mediu

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHKTAP	Descriere dispozitiv bandă	*USE	*EXECUTE
CLRDKT	Descriere unitate de dischetă	*USE	*EXECUTE
CRTTAPCGY	Descriere bibliotecă bandă		
DLTDKTLBL	Descriere unitate de dischetă	*USE	*EXECUTE
DLTMEDDFN	Definiție mediu de stocare	*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
<p>¹ Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.</p> <p>² Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operație.</p> <p>³ Pentru a modifica atributele bibliotecii mediului de stocare sesiune trebuie să aveți autorizarea *CHANGE pentru descrierea bibliotecă bandă. Pentru a schimba prioritatea sau pentru a lucra cu alt job de utilizator, trebuie să aveți autorizarea specială *JOBCTL.</p> <p>⁴ Pentru a schimba prioritatea sau pentru a lucra cu alt job de utilizator, trebuie să aveți autorizarea specială *JOBCTL.</p> <p>⁵ Pentru a utiliza această comandă, trebuie să aveți autorizare specială *ALLOBJ când TYPE(*HEX) este specificat sau banda are setat steagul volum asigurat sau fișier asigurat.</p>			

Comenzi pentru meniu și grup de panouri

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMNU	Meniu	*CHANGE	*USE
CRTMNU	Fișier sursă	*USE	*EXECUTE
	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD

Comenzi meniu și grup de panouri

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTPNLGRP	Grup de panouri: Replace(*NO)		*READ, *ADD
	Grup de panouri: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Fișier sursă	*USE	*EXECUTE
	Fișier includere	*USE	*EXECUTE
CRTS36MNU	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Fișier sursă	*USE	*EXECUTE
	Fișiere de mesaje numite în sursă	*OBJOPR, *OBJEXIST	*EXECUTE
	Fișier-destinație sursă când TOMBR nu e *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	Fișier de afișare meniu când se specifică REPLACE(*YES)	*OBJOPR, *OBJEXIST	*EXECUTE
	Fișier mesaj text comandă	*OBJOPR, *OBJEXIST	*EXECUTE
	Comanda CRTMSGF (Create Message File - Creare fișier mesaj)	*OBJOPR	*EXECUTE
	Comanda ADDMSGD (Add Message Description - Adăugare descriere mesaj)	*OBJOPR	*EXECUTE
	Comanda Creare fișier de afișare (CRTDSPF)	*OBJOPR	*EXECUTE
DLTMNU	Meniu	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Grup de panouri	*OBJEXIST	*EXECUTE
DSPMNUA	Meniu	*USE	*USE
GO	Meniu	*USE	*USE
	Fișierul de afișare și fișierele mesaj cu *DSPF specificat	*USE	*EXECUTE
	Biblioteci curente și de produse	*USE	
	Program cu *PGM specificat	*USE	*EXECUTE
WRKMNU ¹	Meniu	Orice	*USE
WRKPNLGRP ¹	Grup de panouri	Orice	*EXECUTE

¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.

Comenzile pentru mesaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPMSG	Coadă mesaje	*USE	*USE
	Coadă de mesaje care primește replica la un mesaj de interogare	*USE, *ADD	*USE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*USE
RCVMSG	Coadă mesaje	*USE	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*EXECUTE
RMVMSG	Coadă mesaje	*OBJOPR, *DLT	*EXECUTE

Comenzi mesaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RTVMSG	Fișier de mesaje	*USE	*EXECUTE
SNDBRKMSG	Coadă de mesaje care primește replica la mesajele de interogare	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Coadă mesaje	*OBOPR, *ADD	*EXECUTE
	Coadă de mesaje care primește replica la mesajul de interogare	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Coadă mesaje	*OBJOPR, *ADD	*EXECUTE
	Fișierul mesaj, când se trimite mesaj predefinit	*USE	*EXECUTE
	Coadă de mesaje care primește replica la mesajul de interogare	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Coadă mesaje	*USE, *ADD	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Coadă mesaje	*OBJOPR, *ADD	*EXECUTE
	Fișierul mesaj, când se trimite mesaj predefinit	*USE	*EXECUTE
WRKMSG	Coadă mesaje	*USE	*USE
	Coadă de mesaje care primește replica la mesajul de interogare	*USE, *ADD	*USE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*USE

Comenzi pentru descriere mesaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDMSGD	Fișier de mesaje	*USE, *ADD	*EXECUTE
CHGMSGD	Fișier de mesaje	*USE, *UPD	*EXECUTE
DSPMSGD	Fișier de mesaje	*USE	*EXECUTE
RMVMSGD	Fișier de mesaje	*OBJOPR, *DLT	*EXECUTE
WRKMSGD ¹	Fișier de mesaje	*USE	*EXECUTE

¹ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.

Comenzi pentru fișier mesaj

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMSGF	Fișier de mesaje	*USE, *DLT	*EXECUTE
CRTMSGF	Fișier de mesaje		*READ, *ADD
DLTMSGF	Fișier de mesaje	*OBJEXIST	*EXECUTE
DSPMSGF	Fișier de mesaje	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
MRGMSGF	Fișier-sursă mesaj	*USE	*EXECUTE
	Fișier mesaje destinație	*USE, *ADD, *DLT	*EXECUTE
	Fișier mesaj înlocuire	*USE, *ADD	*EXECUTE
WRKMSGF ¹	Fișier de mesaje	Orice autorizație	*USE
¹ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.			

Comenzi pentru coadă de mesaje

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMSGQ	Coadă mesaje	*USE, *DLT	*EXECUTE
CLRMSGQ	Coadă mesaje	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Coadă mesaje		*READ, *ADD
DLTMSGQ	Coadă mesaje	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ ¹	Coadă mesaje	Orice autorizație	*USE
¹ Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.			

Comenzi pentru migrare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RCVMGRDTA	Fișier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
SNDMGRDTA	Fișier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
Acele comenzi nu necesită nici o autorizare obiect.			
Acele comenzi sunt livrate cu autorizația publică *EXCLUDE. Trebuie să aveți autorizare specială *ALLOBJ pentru a utiliza aceste comenzi.			
ANZS34OCL	CVTS36JOB	MGRS36DSPF	MIGRATE
ANZS36OCL	CVTS36QRY	MGRS36ITM	QMUS36
CHGS34LIBM	CVTS38JOB	MGRS36LIB	RESMGRNAM
CHKS36SRCA	GENS36RPT	MGRS36MNU	RSTS38AUT
CVTBASSTR	GENS38RPT	MGRS36MSGF	STRS36MGR
CVTBASUNF	MGRS36	MGRS36QRY ¹	STRS38MGR
CVTBGUDTA	MGRS36APF ¹	MGRS36RPG	
CVTS36CFG	MGRS36CBL	MGRS36SEC	
CVTS36FCT	MGRS36DFU ¹	MGRS38OBJ	
¹ Trebuie să aveți autorizarea specială *ALLOBJ și să aveți opțiunea 4 i5/OS instalată.			

Comenzi pentru descriere mod

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMODD ²	Descriere mod	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD ²	Descriere mod		*READ, *ADD
CHGSSNMAX	Descriere dispozitiv	*OBJOPR	*EXECUTE
DLTMODD	Descriere mod	*OBJEXIST	*EXECUTE
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 operații individuale, trebuie să aveți autorizația cerută de operații individuale. ² Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.			

Comenzi pentru modul

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMOD	Modul	*OBJMGT, *USE	*USE
	Modul, dacă se specifică OPTIMIZE	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modul, dacă se specifică FRCRT(*YES)	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modul, dacă se specifică ENBPRFCOL	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Modul	*OBJEXIST	*EXECUTE
DSPMOD	Modul	*USE	*EXECUTE
RTVBNDSRC ¹	Modul	*USE	*EXECUTE
	*SRVPGMs și module specificate cu *SRVPGMs	*USE	*EXECUTE
	Fișierul bază de date sursă dacă el și membrul există și se specifică MBROPT(*REPLACE).	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fișierul bază de date sursă dacă el și membrul există și se specifică MBROPT(*ADD).	*OBJOPR, *ADD	*EXECUTE
	Fișierul bază de date sursă dacă el există și membrul trebuie să fie creat.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Fișierul bază de date sursă dacă el există și membrul trebuie să fie creat.		*EXECUTE, *READ, *ADD
	Comanda CRTSCRPF dacă fișierul nu există		*EXECUTE
	Comanda ADDPFM dacă fișierul nu există		*EXECUTE
	Comanda RGZPFM pentru a reorganiza membrul fișier sursă	*OBJMGT	*EXECUTE
WRKMOD ²	Modul	Orice autorizație	*USE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
¹	Aveți nevoie de autorizare *USE pentru: <ul style="list-style-type: none"> • Comanda CRTSRCPF dacă fișierul nu există. • Comanda ADDPFM dacă membrul nu există. • Comanda RGZPFM astfel ca membrul fișier sursă să fie reorganizat. Sunt necesare fie autorizările *CHANGE și *OBJALTER sau *OBJMGT pentru a reorganiza membrul fișier sursă. Funcțiile comenzii RTVBNSRC se efectuează apoi cu membrul fișier sursă reorganizat cu numărul de ordine zero. 		
²	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		

Comenzi pentru descriere NetBIOS

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGNTBD ²	Descriere NetBIOS	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD ²	Descriere NetBIOS		*EXECUTE
DLTNTBD	Descriere NetBIOS	*OBJEXIST	*EXECUTE
DSPNTBD	Descriere NetBIOS	*USE	*EXECUTE
WKRNTBD ¹	Descriere NetBIOS	*OBJOPR	*EXECUTE
¹	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
²	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.		

Comenzi pentru rețea

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDNETJOBE (Q)	Profil utilizator în intrarea job rețea	*USE	
APING	Descriere dispozitiv	*CHANGE	
AREXEC	Descriere dispozitiv	*CHANGE	
CHGNETA (Q) ⁴			
CHGNETJOBE (Q)	Profil utilizator în intrarea job rețea	*USE	
DLTNETF ²	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPNETA			

Comenzi rețea

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RCVNETF ²	Fișierul destinație nu există, MBROPT(*ADD) specificat	*OBJMGT, *USE	*EXECUTE, *ADD
	Fișierul destinație nu există, MBROPT(*REPLACE) specificat	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	Fișierul destinație există, MBROPT(*ADD) specificat	*USE	*EXECUTE
	Fișierul destinație există, MBROPT(*REPLACE) specificat	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	Profil utilizator în intrarea job rețea	*USE	
RTVNETA			
RUNRMTCMD	Descriere dispozitiv	*CHANGE	
SNDNETF	Fișier fizic sau fișier de salvare	*USE	*EXECUTE
SNDNETMSG pentru un utilizator local	Coadă mesaje	*OBJOPR, *ADD	*EXECUTE
VFYAPCCNN	Descriere dispozitiv	*CHANGE	
WRKNETF ^{2,3}			
WRKNETJOBE ³	QUSRSYS/QANFNJE	*USE	*EXECUTE
¹	Trebuie să aveți autorizarea specială *ALLOBJ.		
²	Un utilizator poate rula aceste comenzi pe propriile sale fișiere rețea sau pe fișierele rețea deținute de profilul său de grup. E necesară autorizarea specială *ALLOBJ pentru a procesa fișiere rețea pentru alt utilizator.		
³	Pentru a folosi o operație individuală, trebuie să aveți autorizarea cerută de acea operație.		
⁴	Pentru a modifica unele atribute rețea, trebuie să aveți autorizarea specială *IOSYSCFG sau *ALLOBJ și *IOSYSCFG.		

Comenzi NFS

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
ADDMFS ^{1,3}	dir_pestre_care_se_montează	*DIR	"root" (/)	*W
CHGNFSEXP ^{1,2}	Prefix cale	Vedeți regulile generale.		
DSPMFSINF	unele_directoare	*DIR	"root" (/)	*RX
	Prefix cale	Vedeți regulile generale.		
ENDNFSSVR ^{1,4}	nimic			
EXPORTFS ^{1,2}	Prefix cale	Vedeți regulile generale.		
MOUNT ^{1,3}	dir_pestre_care_se_montează	*DIR	"root" (/)	*W
RLSIFSLCK ¹	obiect	*STMF	"root" (/), QOpenSys, UDFS	*R
	Prefix cale	Vedeți regulile generale.		
RMVMFS ¹				
STATFS	unele_directoare	*DIR	"root" (/)	*RX
	Prefix cale	Vedeți regulile generale.		

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
STRNFSSVR ¹	nimic			
UNMOUNT ¹				
<p>¹ Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.</p> <p>² Când e specificat stegulețul -F și fișierul /etc/exports nu există, trebuie să aveți autorizarea de scriere, executare (*WX) pentru directorul /etc. Când e specificat stegulețul -F și fișierul /etc/exports există, trebuie să aveți autorizare de citire, scriere (*RW) pentru fișierul /etc/exports și autorizare *X pentru directorul /etc.</p> <p>³ Directorul peste care se montează este orice director IFS peste care se poate monta.</p> <p>⁴ Pentru a opri orice joburi demon pornite de altcineva, trebuie să aveți autorizarea specială *JOBCTL.</p>				

Comenzi pentru descriere interfață de rețea

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGNWIFR ²	Descriere interfață de rețea	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR ²	Descriere interfață de rețea		*READ, *ADD
	Descriere de linie (DLCI)	*USE	*EXECUTE
DLTNWID	Descriere interfață de rețea	*OBJEXIST	*EXECUTE
DSPNWID	Descriere interfață de rețea	*USE	*EXECUTE
WRKNWID ¹	Descriere interfață de rețea	*OBJOPR	*EXECUTE
<p>¹ Pentru a folosi operații individuale, trebuie să aveți autorizarea cerută de operația individuală.</p> <p>² Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.</p>			

Comenzi pentru server de rețea

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
ADDNWSSTGL ²	Cale (/QFPNWSSTG)	*DIR	"root" (/)	*X
	Director părinte (numele spațiului de stocare)	*DIR	"root" (/)	*WX
	Fișierele care compun spațiul de stocare)	*FILE	"root" (/)	*RW
	Descriere server de rețea	*NWSG	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG ²	Cale (root și /QFPNWSSTG)	*DIR	"root" (/)	*WX
CHGNWSUSRA ⁴	Profil utilizator	*USRPRF		*OBJMGT, *USE
CRTNWSSTG ²	Cale (root și /QFPNWSSTG)	*DIR	"root" (/)	*WX
DLTNWSSTG ²	Cale (/QFPNWSSTG)	*DIR	"root" (/)	*WX
	Director părinte (numele spațiului de stocare)	*DIR	"root" (/)	*RWX, *OBJEXIST
	Fișierele care compun spațiul de stocare)	*FILE	"root" (/)	*OBJEXIST

Comenzi server de rețea

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
DLTWNTSVR ⁵	Descriere server de rețea (NWS)	*NWSD	QSYS.LIB	*OBJEXIST
	Descriere de linie	*LIND	QSYS.LIB	*OBJEXIST
	Descriere server de rețea	*NWSCFG	QSYS.LIB	*OBJEXIST
	Stocare server rețea - Cale (/QFPNWSSTG)	*DIR	"root" (/)	*WX
	Director părinte (numele spațiului de stocare)	*DIR	"root" (/)	*RWX, *OBJEXIST
	Fișierele care compun spațiul de stocare	*FILE	"root" (/)	*OBJEXIST
DSPNWSSTG	Cale la spațiul de stocare	*DIR	"root" (/)	*X
	Fișierele care compun spațiul de stocare)	*FILE	"root" (/)	*R
INSWNTSVR ^{6, 7}	Descriere server de rețea (NWS)	*NWSD	Neaplicabilă	*USE
	Descriere de linie	*LIND	Neaplicabilă	*USE
	Descriere server de rețea	*NWSCFG	Neaplicabilă	*USE
	Stocare server rețea - Cale (/QFPNWSSTG)	*DIR	"root" (/)	*WX
RMVNWSSTGL ²	Cale (/QFPNWSSTG)	*DIR	"root" (/)	*X
	Director părinte (numele spațiului de stocare)	*DIR	"root" (/)	*WX
	Fișierele care compun spațiul de stocare)	*FILE	"root" (/)	*RW
	Descriere server de rețea	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Cale la spațiul de stocare	*DIR	"root" (/)	*X
	Fișierele care compun spațiul de stocare)	*FILE	"root" (/)	*R
Aceste comenzi nu necesită nici o autorizație obiect:				
ADDRMTSVR	DSPNWSALS		SNDNWSMSG	
CHGNWSA ⁴ (Q)	DSPNWSASN		WRKNWSALS	
CHGNWSALS	DSPNWSSTC		WRKNWSENK	
CRTNWSALS	DSPNWSUSR		WRKNWSSN	
DLTNWSALS	DSPNWSUSRA		WRKNWSSTS	
DSPNWSA	SBMNWSCMD (Q) ³			
¹	Autorizarea necesară nu e folosită pentru comenzi ale serverului de rețea.			
²	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.			
³	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *JOBCTL.			
⁴	Trebuie să aveți autorizarea specială *SECADM pentru a specifica altă valoare decât *NONE pentru parametrii NDSTREELST și NTW3SVRLST.			
⁵	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *ALLOBJ.			
⁶	Pentru a folosi această comandă, aveți nevoie de autorizările speciale *IOSYSCFG, *ALLOBJ și *JOBCTL.			
⁷	Trebuie să aveți autorizarea specială *SECADM pentru a specifica altă valoare decât cea implicită pentru parametrii IPSECRULE, CHAPAUT sau SPCERTID.			

Comenzi pentru configurație server de rețea

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QUSRSYS
CHGNWSCFG ^{1,3}	configurație server de rețea	*CHANGE	*EXECUTE
CRTNWSCFG ^{1,3}	configurație server de rețea	*USE	*READ, *ADD
DLTNWSCFG ^{1,3}	configurație server de rețea	*OBJEXIST	*EXECUTE
DSPNWSCFG ^{1,3}	configurație server de rețea	*USE	*EXECUTE
INZNWSCFG ^{1,2}	configurație server de rețea	*CHANGE	*EXECUTE
WRKNWSCFG ¹	configurație server de rețea	*USE	*EXECUTE

¹ Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.

² Pentru a folosi această comandă, trebuie să aveți autorizare specială *SECADM.

³ Pentru a specifica altă valoare decât cea implicită pentru parametrii IPSECRULE, CHAPAUT sau SPCERTID trebuie să aveți autorizare de administrator (*SECADM).

Comenzi pentru descriere server de rețea

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QSYS
CHGNWSD ²	Descriere server de rețea	*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 rețea	*OBJEXIST	*EXECUTE
DSPNWSD	Descriere server de rețea	*USE	*EXECUTE
WRKNWSD ¹	Descriere server de rețea	*OBJOPR	*EXECUTE

¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.

² Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.

Comenzi pentru listă de noduri

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	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 operații individuale, trebuie să aveți autorizarea cerută de operația individuală.

Comenzi pentru listă de noduri

Comenzi pentru servicii de birou

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită nici o autorizare obiect.		
ADDACC (Q)	GRTACCAUT ^{2,3,6} (Q)	RVKUSRPMN ^{1,2}
DSPACC	GRTUSRPMN ^{1,2}	WRKDOCLIB ⁴
DSPACCAUT	RMVACC ¹ (Q)	WRKDOCPTQ ⁵
DSPUSRPMN	RVKACCAUT ¹	
¹	Trebuie să aveți autorizarea specială *ALLOBJ pentru a acorda sau revoca autorizarea cod de acces sau autorizarea document pentru alți utilizatori.	
²	Accesul e restricționat la documente, foldere și poștă 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 puteți acorda autorizare cod de acces. Utilizatorului căruia i se acordă autorizare cod de acces trebuie să fie înregistrat în directorul distribuție al sistemului.	
⁴	Trebuie să aveți autorizarea specială *SECADM.	
⁵	Sunt necesare autorizări suplimentare pentru funcții specifice apelate de operațiile selectată. Utilizatorul are de asemenea nevoie de autorizări speciale pentru orice comenzi apelate în timpul unei funcții specifice.	
⁶	Trebuie să aveți autorizarea specială *ALLOBJ sau *SECADM pentru a acorda autorizarea de acces la cod.	

Comenzi pentru educație online

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CVTEDU			
STREDU			

Comenzi pentru asistent operațional

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGBCKUP ¹	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP ²			
CHGPWRSCD ³			
CHGPWRSCDE ³			
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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 DSPPWRS CD	*USE	
RUNBCKUP ¹	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Comenzi: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP ⁴	Profil utilizator QPGMR	*USE	
	Coadă joburi	*USE	*EXECUTE
¹	Trebuie să aveți autorizările speciale *ALLOBJ sau *SAVSYS.		
²	Trebuie să aveți autorizările speciale *ALLOBJ, *SECADM și *JOBCTL.		
³	Trebuie să aveți autorizările speciale *ALLOBJ și *SECADM.		
⁴	Trebuie să aveți autorizația specială *JOBCTL.		
⁵	Trebuie să aveți autorizarea specială *ALLOBJ.		

Comenzi pentru disc optic

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare		
		Obiect	Bibliotecă	Volum optic ¹
ADDOPTCTG (Q)	Dispozitiv optic	*USE	*EXECUTE	
ADDOPTSVR (Q)	CSI server	*USE	*EXECUTE	
CHGDEVOPT ⁴	Dispozitiv optic	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				

Comenzi disc optic

Comandă	Obiect referențiat	Autorizări necesare		
		Obiect	Bibliotecă	Volum optic ¹
CHGOPTVOL	Directorul root (/) al volumului când se modifică descrierea text ⁵	*W	N/A	N/A
	Dispozitiv optic	*USE	*EXECUTE	*CHANGE ³
	CSI server	*USE	*EXECUTE	N/A
CHKOPTVOL	Dispozitiv optic	*USE	*EXECUTE	*USE
	Director rădăcină (/) al volumului	*RWX	N/A	N/A
CPYOPT	Dispozitiv optic	*USE	*EXECUTE	*USE - Volum sursă
				*ALL - Volum destinație
	Fiecare director precedent în calea fișierului sursă	*X	N/A	N/A
	Fiecare director precedent în calea fișierului destinație	*X	N/A	N/A
	Fișier sursă (*DSTMF) ⁵	*R	N/A	N/A
	Director părinte al fișierului destinație	*WX	N/A	N/A
	Părintele directorului părinte dacă se creează director	*WX	N/A	N/A
CPYOPT	Fișierul destinație dacă e înlocuit datorită SLTFILE(*ALL)	*W	N/A	N/A
	Fișierul destinație dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	N/A	N/A
	Fiecare director din cale care precede directorul sursă	*X	N/A	N/A
	Fiecare director din cale care precede directorul destinație	*X	N/A	N/A
CPYOPT	Directorul care e copiat ⁵	*R	N/A	N/A
	Directorul care e copiat dacă el conține intrări	*RX	N/A	N/A
	Părintele directorului destinație	*WX	N/A	N/A
	Directorul destinație dacă e înlocuit datorită SLTFILE(*ALL)	*W	N/A	N/A
	Directorul destinație dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	N/A	N/A
	Directorul destinație dacă intrările urmează să fie create	*WX	N/A	N/A

Comandă	Obiect referențiat	Autorizări necesare		
		Obiect	Biblioteca	Volum optic ¹
CPYOPT	Fișiere sursă	*R	N/A	N/A
	Fișierul destinație dacă e înlocuit datorită SLTFILE(*ALL)	*W	N/A	N/A
	Fișierul destinație dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	N/A	N/A
CRTDEVOPT ⁴	Dispozitiv optic		*EXECUTE	
CVTOPTBKU	Dispozitiv optic	*USE	*EXECUTE	*ALL
DSPOPT	Prefix cale când DATA (*SAVRST) ⁵	*X	N/A	N/A
	Prefix fișier când (*SAVRST) ²	*R	N/A	N/A
	Dispozitiv optic	*EXECUTE	*USE	
	CSI server	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	CSI server	*USE	*EXECUTE	
DUPOPT	Dispozitiv optic	*USE	*EXECUTE	*USE - Volum sursă
				*ALL - Volum destinație
INZOPT	Directorul root (/) al volumului	*RWX	N/A	N/A
	Dispozitiv optic	*USE	*EXECUTE	*ALL
LODOPTFMW	Fișier flux	*R	N/A	N/A
	Prefix cale	Vedeți 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	

Comenzi disc optic

Comandă	Obiect referențiat	Autorizări necesare		
		Obiect	Biblioteca	Volum optic ¹
¹	Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic și lista de autorizare folosită pentru a securiza volumul este menținută de funcția de suport optic.			
²	Sunt șapte opțiuni care pot fi invocate din utilitățile optice care nu sunt ele înseși comenzi. Aceste opțiuni și autorizările lor cerute pentru volumul optic sunt arătate mai jos. Ștergere fișier: *CHANGE Redenumire fișier: *CHANGE Ștergere director: *CHANGE Creare director: *CHANGE Redenumire volum: *ALL Eliberare fișier optic reținut: *CHANGE Salvare fișier optic reținut: *USE - Volum sursă, *Change - Volum destinație			
³	E necesară autorizare de gestionare listă de autorizații pentru lista care securizează curent volumul optic pentru a o modifica.			
⁴	Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.			
⁵	Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (Universal Disk Format).			

Comenzi pentru coadă de ieșire

Comandă	Obiect referențiat	Parametri coadă de ieșire		Autorizare specială	Autorizație necesară	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CHGOUTQ ¹	Coadă de date				*READ	*EXECUTE
	Coadă de ieșire	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă mesaje				*OBJOPR *ADD	*EXECUTE
	obiect de personalizare stație de lucru				*USE	*EXECUTE
	Program transformare date utilizator				*OBJOPR *EXECUTE	*EXECUTE
Program cu driver utilizator				*OBJOPR *EXECUTE	*EXECUTE	
CLROUTQ ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

Comandă	Obiect referențiat	Parametri coadă de ieșire		Autorizare specială	Autorizație necesară	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CRTOUTQ	Coadă de date				*READ	*EXECUTE
	Coadă de ieșire					*READ, *ADD
	Coadă de ieșire				*OBJOPR *ADD	*EXECUTE
	obiect de personalizare stație de lucru				*USE	*EXECUTE
DLTOUTQ	Coadă de ieșire				*OBJEXIST	*EXECUTE
HLDOUTQ ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT ⁴						
RLSOUTQ ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQ ^{1,3}	Coadă de ieșire				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQD ^{1,3}	Coadă de ieșire				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
<p>¹ Dacă aveți autorizarea specială *SPLCTL, nu aveți nevoie de nici o autorizare pentru coada de ieșire. Aveți nevoie de autorizarea specială *EXECUTE, totuși, pentru bibliotecă pentru coadă.</p> <p>² Trebuie să fiți proprietarul cozii de ieșire.</p> <p>³ Dacă cereți să lucrați cu toate cozile de ieșire, ecranul listă include toate cozile de ieșire din bibliotecă pentru care aveți autorizare *EXECUTE.</p> <p>⁴ Trebuie să aveți autorizația specială *ALLOBJ pentru a folosi această comandă.</p>						

Comenzi pentru pachet

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTSQLPKG	Program	*OBJOPR, *READ	*EXECUTE
	Pachet SQL: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	Pachet SQL: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Pachet	*OBJEXIST	*EXECUTE
PRTSQLINF	Pachet	*OBJOPR, *READ	*EXECUTE
	Program	*OBJOPR, *READ	*EXECUTE
	Program service	*OBJOPR, *READ	*EXECUTE

Comenzi pachet

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRSQL			

Comenzi pentru performanță

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda *USE altora.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPEXDFN (Q) ⁵	Bibliotecă PGM		*EXECUTE
ADDPEXFTR (Q) ⁵	Bibliotecă PGMTRG		*EXECUTE
	Bibliotecă PGMFTR		*EXECUTE
	Cale JVAFTR	*X pentru director	
	Cale PATHFTR	*X pentru director	
ANZBESTMDL (Q) ⁴	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Bibliotecile aplicație care conțin fișierele bază de date care vor fi analizate		*EXECUTE
	Descriere de job	*USE	*EXECUTE
ANZDBF (Q) ⁴	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Bibliotecile aplicație care conțin programele care vor fi analizate		*EXECUTE
	Descriere job	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	Date de performanță ²		*ADD, *READ
ANZPFRDTA (Q) ⁴	QPFR/QACVPP *PGM	*USE	*EXECUTE
	Date de performanță 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 colecție		*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

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGPEXDFN (Q) ⁵	Bibliotecă PGM		*EXECUTE
CHKPFCOL (Q)			
CPYFCNARA (Q) ⁴	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE din biblioteca "sursă"	*USE	*EXECUTE
	Biblioteca "destinație" (dacă QAPGGPHF *FILE nu există)		*EXECUTE, *ADD
	QAPGGPHF *FILE din biblioteca "destinație" (dacă se adaugă un nou format de grafic sau se înlocuiește unul existent)	*CHANGE	*EXECUTE
CPYGPHFMT (Q) ⁴	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE din biblioteca "sursă"	*USE	*EXECUTE
	Biblioteca "În" (dacă QAPGPKGF *FILE nu există)		*EXECUTE, *ADD
	QAPGPKGF *FILE din biblioteca "destinație" (dacă se adaugă un nou pachet grafic sau se înlocuiește unul existent)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE din biblioteca "destinație" (dacă se adaugă un nou pachet grafic sau se înlocuiește unul existent)	*USE	*EXECUTE
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinație		*EXECUTE, *ADD
	Descriere de job	*USE	*EXECUTE
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	Date de performanță (toate fișierele 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 funcțională este creată		*EXECUTE, *ADD
	QAPTAPGP *FILE din biblioteca destinație (dacă se adaugă o nouă zonă funcțională)	*CHANGE	*EXECUTE
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Biblioteca în care Formatul grafic este creat		*EXECUTE, *ADD
	QAPGGPHF *FILE din biblioteca destinație (dacă se adaugă o nou format de grafic)	*CHANGE	*EXECUTE

Comenzi performanță

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Biblioteca în care este creat Pachetul grafic		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE din biblioteca destinație (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 destinație		*ADD, *READ
CRTPEXDTA (Q) ⁵	Biblioteca *MGTCOL		*EXECUTE
	Biblioteca de date ¹		*READ, *ADD ²
CRTPFRDTA (Q)	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinație		*ADD, *READ
	Bibliotecă sursă		*USE
CVTPFRDTA (Q)	Descriere job	*USE	*EXECUTE
CVTPFRTHD (Q)	Date de performanță 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 funcționale	*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
DLTPFRDTA (Q) ⁴	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
I DMPMEMINF	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale
DMPTRC (Q) ⁵	Biblioteca în care vor fi memorate datele de urmărire		*EXECUTE, *ADD
	Fișier de ieșire (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPHSTGPH (Q) ⁴	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteca date istorice		*EXECUTE
DSPPFRDTA (Q) ⁴	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Biblioteca format sau pachet		*EXECUTE
	Date de performanță ²		*EXECUTE
	Biblioteca fișierului de ieșire		*EXECUTE, *ADD
	Coadă de ieșire	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
DSPPFRGPH (Q) ⁴	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteca fișierului de ieșire		*EXECUTE
	Descriere job	*USE	*EXECUTE
ENDJOBTRC (Q) ⁴	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDPEX (Q) ⁵	Biblioteca de date ¹		*READ, *ADD ²
ENDPFCOL (Q)			
PRTACTRPT (Q) ⁴	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Date de performanță ²	*USE	*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTCPTRPT (Q) ⁴	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	Date de performanță ²		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTJOBTRPT (Q) ⁴	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Date de performanță ²		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTJOBTRC (Q) ⁴	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Biblioteca fișier de urmărire job (QAPTRCJ)		*EXECUTE
	Descriere job	*USE	*EXECUTE
PRTLCKRPT (Q) ⁴	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE
PRTPEXRPT ⁵	Biblioteca de date ¹		*EXECUTE ²
	Fișier ieșire	*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 performanță ²		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTRSCRPT (Q) ⁴	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Date de performanță ²		*ADD, *READ
	Descriere job	*USE	*EXECUTE

Comenzi performanță

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PRTSYSRPT (Q) ⁴	QPFR/QPTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Descriere de job	*USE	*EXECUTE
PRTTNSRPT (Q) ⁴	QPFR/QPTNSRP *PGM	*USE	*EXECUTE
	Biblioteca fișier de urmărire (QTRJOB)		*EXECUTE
	Descriere job	*USE	*EXECUTE
PRTRCRPT (Q) ⁴	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVPEXDFN (Q) ⁵			
RMVPEXFTR (Q) ⁵			
STRBEST (Q) ⁴	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON ^{3, 4}	Fișier ieșire	*OBJOPR, *ADD	*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRPEX (Q) ⁵			
STRPFCOL (Q)			
STRPFRG (Q) ⁴	QPFR/QPGSTART *PGM	*USE	*EXECUTE
STRPFRT (Q) ⁴	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE din biblioteca zonei funcționale	*CHANGE	*EXECUTE
	Comanda CHGFCNARA (Q)	*USE	*EXECUTE
	Comanda CPYFCNARA (Q)	*USE	*EXECUTE
	Comanda CRTFCNARA (Q)	*USE	*EXECUTE
	Comanda DLTFNARA (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
	Fișier de ieșire (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q) ⁵			
WRKPEXFTR (Q) ⁵			
WRKSYSACT (Q) ^{3, 4}	QPFR/QITMONCP *PGM	*USE	*EXECUTE
<p>Aceste comenzi nu necesită nici o autorizație obiect:</p> <ul style="list-style-type: none"> • ENDDDBMON³ • ENDPFRTRC (Q) • STRPFRTRC (Q) 			

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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 fișiere bază de date. Nu e verificată autorizarea pentru setul individual de fișiere bază de date.		
3	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *JOBCTL.		
4	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE.		
5	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE sau trebuie să fiți autorizat pentru funcția Urmărire serviciu din i5/OS System/400 prin suportul Administrare aplicație din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_SERVICE_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operații de urmărire.		

Comenzi pentru grup descriptori de tipărire

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGPDGPRF	Profil utilizator	*OBJMGT	
CRTPDG	Grup descriptor tipărire		*READ, *ADD
DLTPDG	Grup descriptor tipărire	*OBJEXIST	*EXECUTE
DSPPDGPRF	Profil utilizator	*OBJMGT	
RTVPDGPRF	Profil utilizator	*READ	

Comenzi pentru configurare Print Services Facility

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGPSFCFG ^{1, 2}			
CRTGPSFCFG ^{1, 2}			*READ, *ADD
DLTPSFCFG ^{1, 2}	Configurare PSF	*OBJEXIST	*EXECUTE
DSPPSFCFG ¹	Configurare PSF	*USE	*EXECUTE
WRKPSFCFG ¹	Configurare PSF	*READ	*EXECUTE
1	Opțiunea PSF/400 este necesară pentru a folosi această comandă.		
2	Este necesară autorizarea specială *IOSYSCFG pentru a folosi această comandă.		

Comenzi pentru problemă

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPBACNE (Q)	Filtru	*USE, *ADD	*EXECUTE

Comenzi problemă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPBRLTE (Q)	Filtru	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Comanda SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filtru	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filtru	*USE, *UPD	*EXECUTE
DLTPRB (Q) ³	Comandă: DLTAPARDDTA	*USE	*EXECUTE
DSPPRB	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
PTRINTDDTA (Q)			
QRYPRBSTS (Q)			
VFYCMN (Q)	Descriere de linie ¹	*USE	*EXECUTE
	Descriere controler ¹	*USE	*EXECUTE
	ID rețea 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 rețea) și dispozitiv bazat pe acțiunea de analiză problemă	*USE	*EXECUTE
<p>¹ Aveți nevoie de autorizare *USE pentru obiectul de comunicații pe care îl verificați</p> <p>² Trebuie să aveți autorizare *USE pentru comanda SNDSRVRQS pentru a fi capabil să raportați o problemă.</p> <p>³ Trebuie să aveți autorizare pentru DLTAPARDDTA dacă vreți ca datele APAR asociate cu problema să fie de asemenea șterse. Vedeți DLTAPARDDTA din tabela de autorizări necesare pentru Comenzi de service pentru a determina autorizările suplimentare necesare.</p> <p>⁴ Trebuie să aveți autorizarea specială *IOSYSCFG când descrierea de dispozitiv este alocată de un dispozitiv bibliotecă de medii de stocare.</p>			

Comenzi pentru program

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Autorizările pentru obiect necesare pentru comenzile CRT:xxxPGM sunt afișate în tabela Limbaje din "Comenzi pentru limbaj" la pagina 376.			
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	Operația de depanare	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR ¹			

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CHGPGM	Program	*OBJMGT, *USE	*USE
	Programul, dacă opțiunea de recreare este specificată, nivelul de optimizare este modificat sau colectarea datelor de performanță s-a modificat	*OBJMGT, *USE	*USE, *ADD, *DLT
	Programul, dacă parametrul USRPRF sau USEADPAUT este modificat	Proprietarul ⁷	*USE, *ADD, *DLT
CHGPGMVAR ¹			
CHGPTR ¹			
CHGSRVPGM	Program service	*OBJMGT, *USE	*USE
	Programul service, dacă opțiunea de recreare este specificată, nivelul de optimizare este modificat sau colectarea datelor de performanță s-a modificat	*OBJMGT, *USE	*USE, *ADD, *DLT
	Program service, dacă parametrul USRPRF sau USEADPAUT este modificat.	Deținătorul ⁷ , *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA ¹			
CRTPGM	Program, Înlocuire(*NO)	Vedeți regulile generale.	*READ, *ADD
	Program, Înlocuire(*YES)	Vedeți regulile generale.	*READ, *ADD
	Programul service specificat în parametrul BNDSRVPGM.	*USE	*EXECUTE
	Modul	*USE	*EXECUTE
	Director legare	*USE	*EXECUTE
CRTSRVPGM	Program service, Înlocuire(*NO)	Vedeți regulile generale.	*READ, *ADD
	Program service, Înlocuire(*YES)	Vedeți regulile generale.	*READ, *ADD
	Modul	*USE	*EXECUTE
	Programul service specificat în parametrul BNDSRVPGM	*USE	*EXECUTE
	Export sursă fișier	*OBJOPR *READ	*EXECUTE
	Director legare	*USE	*EXECUTE
CVTCLSRC	Din-fișier	*USE	*EXECUTE
	În-fișier	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Program	*OBJEXIST	*EXECUTE
	Fișier afișare	*OBJEXIST	*EXECUTE
DLTPGM	Program	*OBJEXIST	*EXECUTE
DLTSRVPGM	Program service	*OBJEXIST	*EXECUTE
DMPCLPGM	Program CL	*USE	Nici unul ³
DSPBKP ¹			
DSPDBG ¹			
DSPDBGWCH			

Comenzi program

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPMODSRC ^{2, 4}	Fișier sursă	*USE	*USE
	Orice fișier inclus	*USE	*USE
	Program	*CHANGE	*EXECUTE
DSPPGM	Program	*READ	*EXECUTE
	Program, dacă este specificat DETAIL(*MODULE)	*USE	*EXECUTE
DSPPGMREF	Program	*OBJOPR	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPPGMVAR ¹			
DSPSRVPGM	Program service	*READ	*EXECUTE
	Program service, dacă este specificat DETAIL(*MODULE)	*USE	*EXECUTE
DSPTRC ¹			
DSPTRCDTA ¹			
ENDCBLDBG (COBOL/400 programul licențiat 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 fișier și fișierele bazei de date	*OBJOPR	*EXECUTE
	Informații program		*READ, *ADD
PRTCMDUSG	Program	*USE	*EXECUTE
RMVBKP ¹			
RMVPGM ¹			
RMVTRC ¹			
RSMBKP ¹			
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Fișier sursă bază de date	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	Program manevrare cheie de atenționare	*EXECUTE	*EXECUTE
SETPGMINF	Fișiere bază de date	*OBJOPR	*EXECUTE
	Fișier sursă	*USE	*EXECUTE
	Program root	*CHANGE	*READ, *ADD
	Subprogram	*USE	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRDBG	Program ²	*CHANGE	*EXECUTE
	Sursă fișier ⁴	*USE	*EXECUTE
	Orice fișiere 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 funcții 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 fișier	*OBJOPR *READ	*EXECUTE
WRKPGM ⁶	Program	Orice autorizație	*USE
WRKSRVPGM ⁶	Program service	Orice autorizație	*USE
¹	Când un program este într-o operație de depanare, nici o autorizare nu mai este necesară pentru comenzile de depanare.		
²	Dacă aveți 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 bibliotecă 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	Pentru informații suplimentare despre cerințele de securitate pentru instrucțiunile SQL, vedeți subiectul Autorizarea, privilegiile și proprietatea obiectului din Referințe SQL (în Centrul de informare iSeries).		
⁶	Pentru a folosi operațiile individuale, vă trebuie autorizarea necesară de către operațiile individuale.		
⁷	Trebuie să dețineți programul sau să aveți autorizările speciale *ALLOBJ și *SECADM.		

Comenzi pentru interpretor shell QSH

Comenzile listate în acest tabel nu necesită vreo autorizație pentru obiecte.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRQSH ^{1,2}			

Comenzi interpretor shell QSH

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
QSH ^{1, 2}			
<p>¹ QSH este un alias pentru comanda CL STRQSH.</p> <p>² Aveți nevoie de autorizarea *RX pentru toate scripturile și toate directoarele din calea scriptului.</p>			

Comenzi pentru interogare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZQRY	Definiție interogare	*USE	*EXECUTE
CHGQRYA ⁴			
CRTQMFORM	Formular Query Management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Formular Query Management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Fișier sursă	*USE	*EXECUTE
CRTQMQR	Interogare Query Management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Interogare Query Management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Fișier sursă	*USE	*EXECUTE
	Comandă OVRDBF	*USE	*EXECUTE
DLTQMFORM	Formular Query Management	OBJEXIST	*EXECUTE
DLTQMQR	Interogare Query Management	*OBJEXIST	*EXECUTE
DLTQR	Definiție interogare	*OBJEXIST	*EXECUTE
RTVQMFORM	Formular Query Manager	*OBJEXIST	*EXECUTE
	Fișier sursă destinație	*ALL	*READ, *ADD, *EXECUTE
	Comenzile ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQR	Interogare Query Manager	*USE	*EXECUTE
	Fișier sursă destinație	*ALL	*READ, *ADD
	Comenzile ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RUNQR	Definiție interogare	*USE	*USE
	Fișiere intrare	*USE	*EXECUTE
	Fișiere ieșire	Vedeți regulile generale.	Vedeți regulile generale.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
STRQMQRV ¹	Interogare Query Management	*USE	*EXECUTE
	Formular Query Management, dacă este specificat.	*USE	*EXECUTE
	Definiție interogare, dacă este specificat	*USE	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
	Comenzile ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM (dacă OUTPUT(*OUTFILE) este specificat)	*USE	*EXECUTE
STRQMPCR ¹	Fișier sursă care conține procedura managerului de interogări	*USE	*EXECUTE
	Fișier sursă care conține fișier sursă de comenzi, dacă este specificat	*USE	*EXECUTE
	Comandă OVRPRTF, dacă instrucțiunile au ca rezultat un raport tipărit sau un obiect interogare.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFOM ³	Formular Query Management	Orice autorizație	*USE
WRKQMQRV ³	Interogare Query Management	Orice autorizație	*USE
WRKQRY ³			
¹	Pentru a rula STRQM, trebuie să aveți autorizația cerută de declarațiile din interogare. De exemplu, pentru a insera o linie într-o tabelă este necesară autorizația *OBJOPR, *ADD și *EXECUTE pentru tabel.		
²	Drept de proprietate sau unele autorizații pentru obiect sunt necesare.		
³	Pentru a folosi operații individuale, trebuie să aveți autorizația cerută de operații individuale.		
⁴	Pentru a folosi comandă individuală, trebuie să aveți autorizația specială *JOBCTL.		

Comenzi pentru întrebare și răspuns

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
ANSQST (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ
ASKQST	Fișier bază de date QAQAxxBBPY ¹ or QAQAxxBQPY ¹	*READ	*READ
CHGQSTDB (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ
CRTQSTDB ² (Q)	Fișiere bază de date		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ
DLTQST (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ
DLTQSTDB (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ
EDTQST (Q)	Fișier bază de date QAQAxxBQPY ¹	*READ	*READ

Comenzi întrebare și răspuns

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
LODQSTDB ² (Q)	Fișier bază de date QAQAxxBQPY ^{1,3}	*READ	*READ, *ADD, *EXECUTE
STRQST ⁴	Fișier bază de date QAQAxxBBPY ¹ or QAQAxxBQPY ¹	*READ	*READ
WRKQST	Fișier bază de date QAQAxxBBPY ¹ QAQAxxBQPY ¹	*READ	*USE
WRKCNTINF			*EXECUTE

¹ Porțiunea "xx" a numelui fișierului este indexul bazei de date Întrebări și răspunsuri care este operată de către comandă. Indexul este un număr de două cifre de la 00 la 99. Pentru a obține indexul pentru o bază de date Întrebări și răspunsuri, folosiți comanda WRKCNTINF.

² Profilul de utilizator care rulează comanda devine proprietarul fișierelor nou create, cu excepția cazului în care parametrul OWNER al profilului de utilizator este *GRPPRF. Autorizarea publică a noilor fișiere, cu excepția QAQAxxBBPY, este setată la *EXCLUDE. Autorizarea publică pentru QAQAxxBBPY este setată la *READ.

³ Este necesară autorizația pentru fișier numai dacă se încarcă o bază de date Întrebări și Răspuns existentă.

⁴ Comanda afișează meniul Întrebări și răspunsuri. Pentru a folosi opțiuni individuale, trebuie să aveți autorizația necesară pentru aceste opțiuni.

Comenzi pentru cititor

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRDBRDR	Coadă mesaje	*OBJOPR, *ADD	*EXECUTE
	Fișier bază de date	*OBJOPR, *USE	*EXECUTE
	Coadă joburi	*READ	*EXECUTE
STRDKTRDR	Coadă mesaje	*OBJOPR, *ADD	*EXECUTE
	Coadă joburi	*READ	*EXECUTE
	Descriere dispozitiv	*OBJOPR, *READ	*EXECUTE

Aceste comenzi nu necesită vreo autorizație obiect:

ENDRDR ¹	HLDRDR ¹	RLSRDR ¹
---------------------	---------------------	---------------------

¹ Trebuie să fiți utilizatorul care a pornit cititorul sau să aveți autorizația specială (*ALLOBJ) sau control job (*JOBCTL).

Comenzi pentru facilitatea de înregistrare

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Comenzi pentru baze de date relaționale

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDRDBDIRE	Fișier sursă, dacă este specificat	*EXECUTE	*EXECUTE
CHGRDBDIRE	Fișier sursă, dacă este specificat	*EXECUTE	*EXECUTE
	Descriere dispozitiv locație la distanță ⁷	*CHANGE	
DSPRDBDIRE	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
Aceste comenzi nu necesită vreo autorizație obiect:			
RMVRDBDIRE WRKRDBDIRE			
¹ Autorizație verificată atunci când este folosită intrarea director RDB.			

Comenzi pentru resurse

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPHDWRSC			
DSPSFWRSC	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
EDTDEVRSC			
WRKHDWRSC ¹			
¹ Dacă folosiți opțiunea de a crea un obiect de configurație, trebuie să aveți autorizația de a folosi comanda CRT corespunzătoare.			

Comenzi pentru RJE (Intrare job la distanță)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDFCTE	Tabel de control formulare	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Fișier dispozitiv ^{1,2}	*USE	*READ, *EXECUTE
	Fișier fizic ^{1,2} (RJE generează membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fișier fizic ^{1,2} (membru specificat)	*USE, *ADD	*READ, *EXECUTE
	Program ^{1,2}	*USE	*READ, *EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
ADDRJECMNE	Descriere sesiune	*USE, *ADD, *DLT	*READ, *EXECUTE
	Fișier BSC/CMN ^{1,2}	*USE	*READ, *EXECUTE
	Descriere dispozitiv ²	*USE	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE

Comenzi RJE (Intrare job la distanță)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDRJERDRE	Descriere sesiune	*READ, *ADD, *DLT	*READ, *EXECUTE
	Coadă de joburi ²	*READ	*READ, *EXECUTE
	Coadă de mesaje ²	*READ, *ADD	*READ, *EXECUTE
ADDRJEW TRE	Descriere sesiune	*READ, *ADD, *DLT	*READ, *EXECUTE
	Fișier dispozitiv ^{1,2}	*USE	*READ, *EXECUTE
	Fișier fizic ^{1,2} (RJE generează membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fișier fizic ^{1,2} (membru specificat)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program ^{1,2}	*USE	*READ, *EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGFCT	Tabel de control formulare	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Tabel de control formulare	*USE	*READ, *EXECUTE
	Fișier dispozitiv ^{1,2}	*USE	*READ, *EXECUTE
	Fișier fizic ^{1,2} (RJE generează membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fișier fizic ^{1,2} (membru specificat)	*USE, *ADD	*READ, *EXECUTE
	Program ^{1,2}	*USE	*READ, *EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGRJECMNE	Descriere sesiune	*USE	*READ, *EXECUTE
	Fișier BSC/CMN ^{1,2}	*USE	*READ, *EXECUTE
	Descriere dispozitiv ²	*USE	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGRJERDRE	Descriere sesiune	*USE, *ADD, *DLT	*READ, *EXECUTE
	Coadă de joburi ²	*USE	*READ, *EXECUTE
	Coadă de mesaje ²	*USE, *ADD	*READ, *EXECUTE
CHGRJEW TRE	Descriere sesiune	*USE	*READ, *EXECUTE
	Fișier dispozitiv ^{1,2}	*USE	*READ, *EXECUTE
	Fișier fizic ^{1,2} (RJE generează membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fișier fizic ^{1,2} (membru specificat)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program ^{1,2}	*USE	*READ, *EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGSSND	Descriere sesiune	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Coadă de joburi ^{1,2}	*USE	*EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*EXECUTE
	Tabel de control formulare ^{1,2}	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE

Comenzi RJE (Intrare job la distanță)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CNLRJERDR	Descriere sesiune	*USE	*EXECUTE
	Coadă mesaje	*USE, *ADD	*EXECUTE
CNLRJEWTR	Descriere sesiune	*USE	*EXECUTE
	Coadă mesaje	*USE, *ADD	*EXECUTE
CRTFCT	Tabel de control formulare		*READ, *ADD
CRTRJEBSCF	Fișier BSC		*READ, *EXECUTE, *ADD
	Fișier fizic sursă(DDS)	*READ	*EXECUTE
	Descriere dispozitiv	*READ	*EXECUTE
CRTRJECFG	Descriere sesiune		*READ, *ADD, *UPD, *OBJOPR
	Coadă joburi		*READ, *ADD
	Descriere job		*READ, *OBJOPR, *ADD
	Descriere subsistem		*READ, *OBJOPR, *ADD
	Coadă mesaje		*READ, *ADD
	Fișier CMN		*READ, *EXECUTE, *ADD
	Fișier BSC		*READ, *EXECUTE, *ADD
	Fișier imprimantă		*USE, *ADD
CRTRJECFG	Fișier fizic		*EXECUTE, *ADD
	Profil utilizator QUSER ³	*USE	*EXECUTE
	Coadă de ieșire	*READ	*EXECUTE
	Tabel de control formulare	*READ	*READ
	Descriere dispozitiv		*EXECUTE
	Descriere controler		*EXECUTE
	Descriere de linie		*EXECUTE
CRTRJECMNF	Fișier de comunicație		*READ, *EXECUTE, *ADD
	Fișier fizic sursă(DDS)	*READ	*EXECUTE
	Descriere dispozitiv	*READ	*EXECUTE
CRTSSND	Descriere sesiune		*READ, *ADD, *UPD, *OBJOPR
	Coadă de joburi ^{1,2}	*USE	*EXECUTE
	Coadă de mesaje ^{1,2}	*USE, *ADD	*EXECUTE
	Tabel de control formulare ^{1,2}	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE

Comenzi RJE (Intrare job la distanță)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CVTRJEDTA	Tabel de control formulare	*USE	*EXECUTE
	Fișier de intrare	*USE, *UPD	*EXECUTE
	Fișier de ieșire (RJE generează membru)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fișier ieșire (membru specificat)	*USE, *ADD	*EXECUTE
DLTFCT	Tabel de control formulare	*OBJEXIST	*EXECUTE
DLTRJECFG	Descriere sesiune	*OBJEXIST	*EXECUTE
	Coadă joburi	*OBJEXIST	*EXECUTE
	Fișier BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	Fișier fizic	*OBJEXIST, *OBJOPR	*EXECUTE
	Fișier imprimantă	*OBJEXIST, OBJOPR	*EXECUTE
	Coadă 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	Tabel de control formulare	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJECMNE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Descriere sesiune	*USE	*EXECUTE
SBMRJEJOB	Descriere sesiune	*USE	*EXECUTE
	Fișier intrare ⁶	*USE	*EXECUTE
	Coadă mesaje	*USE, *ADD	*EXECUTE
	Obiecte legate de job ⁷		
SNDRJECMD	Descriere sesiune	*USE	*EXECUTE
STRRJCSL	Descriere sesiune	*USE	*EXECUTE
	Coadă mesaje	*USE	*EXECUTE
STRRJERDR	Descriere sesiune	*USE	*USE

Comenzi RJE (Intrare job la distanță)

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRRJESSN ⁵	Descriere sesiune	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE
	Obiecte legate de job ⁷		*EXECUTE
STRRJEWTR	Descriere sesiune	*USE	*USE
	Program ¹	*USE	*READ, *EXECUTE
	Fișier dispozitiv ¹	*USE, *ADD	*READ, *EXECUTE
	Fișier fizic ¹ (RJE generează membri)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Fișier fizic ¹ (membru specificat)	*READ, *ADD	*READ, *EXECUTE
	Coadă de mesaje ¹	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
WRKFCT ⁸	Tabel de control formulare	*USE	*EXECUTE
WRKRJESSN ⁸	Descriere sesiune	*USE	*EXECUTE
WRKSSND ⁸	Descriere sesiune	*CHANGE	*EXECUTE
¹	Profil utilizator QUSER necesită autorizație pentru acest obiect.		
²	Dacă obiectul nu este găsit sau nu este deținută autorizația necesară, un mesaj informațional este trimis și funcția comenzii este încă realizată.		
³	Această autorizație este necesară pentru a crea descrierea jobului QRJESSN.		
⁴	Această autorizație este necesară doar când DLTCMN(*YES) este specificat.		
⁵	Trebuie să aveți autorizația specială *JOBCTL.		
⁶	Fișierele de intrare au include acestea folosind declarația de control.. READFILE.		
⁷	Examinați autorizările necesare pentru comanda SBMJOB.		
⁸	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		

Comenzi pentru atribute de securitate

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGSECA ¹			
CHGSECAUD ^{2,3}			
CFGSYSSEC ^{1,2,3}			
DSPSECA			
DSPSECAUD ³			
PRTSYSSECA ⁴			
¹	Trebuie să aveți autorizația specială *SECADM pentru a folosi această comandă.		
²	Trebuie să aveți autorizația specială *ALLOBJ pentru a folosi această comandă.		
³	Trebuie să aveți autorizația specială *AUDIT pentru a folosi această comandă.		
⁴	Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.		

Comenzi pentru intrare autentificare server

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSVRAUTE ¹			
CHGSVRAUTE ¹			
DSPSVRAUTE	Profil utilizator	*READ	*EXECUTE
RMVSVRAUTE ¹			
¹ Dacă profilul utilizator pentru această operație nu este *CURRENT sau utilizatorul curent pentru job, trebuie să aveți autorizația specială *SECADM și autorizația *USE pentru profil.			

Comenzi pentru service

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTRCFTR ¹¹			
APYPTF (Q)	Bibliotecă produs	*OBJMGT	
CHGSRVA ³ (Q)			
CHKCMNTRC ³ (Q)			*EXECUTE
CHKPRDOPT (Q)	Toate obiectele din opțiunea produs ⁴		
CPYPTF ² (Q)	Fișier-sursă	*USE	*EXECUTE
	Fișier-destinație ⁸	Aceleași cerințe ca și comanda SAVOBJ	Aceleași cerințe ca și comanda SAVOBJ
	Descriere dispozitiv	*USE	*EXECUTE
	Program licențiat		*USE
	Comenzi: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF și OVRTAPF	*USE	*EXECUTE
	Biblioteca QSRV	*USE	*EXECUTE
CPYPTFGRP ² (Q)	Descriere dispozitiv	*USE	*EXECUTE
	În-fișier	*Aceleași cerințe ca și comanda SAVOBJ	*Aceleași cerințe ca și comanda SAVOBJ
	Din-fișier	*USE	*EXECUTE
	Comenzi: CHKTAP, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDA (Q)			
DLTCMNTRC ³ (Q)	NWID (ID rețea) sau descriere de linie	*USE	*EXECUTE
DLTPTF (Q)	Fișier scrisoare de copertă ⁴		*EXECUTE
	Fișier de salvare PTF ⁴		*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTTRC (Q)	Comanda RMVM	*USE	
	Bibliotecă	*EXECUTE	
	Fișier bază de date	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
ENDCMNTRC ³ (Q)	NWID sau descriere de linie	*USE	*EXECUTE
ENDCPYSCN (Q)	Descriere dispozitiv	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Bibliotecă	*ADD, *EXECUTE	
	Fișiere bază de date	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Comenzi: PTRTRC, DLTTRC	*USE	
EDNWCH ¹⁶ (Q)	Sesiune de urmărire urmărind un mesaj în într-un jurnal job ¹⁸		
INSPTF ⁹ (Q)			
LODPTF (Q)	Descriere dispozitiv	*USE	*EXECUTE
LODRUN ²	Comanda RSTOBJ	*USE	*EXECUTE
PRTCMNTRC ³ (Q)	NWID (ID rețea) sau descriere de linie	*USE	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
PRTERLOG (Q)	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
PRTINTDTA ^{12,13} (Q)			
PRTTRC ¹¹ (Q)	Bibliotecă	*EXECUTE	
	Fișier 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, PRTERLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB și WRKSYSVAL	*USE	*EXECUTE
	Problemă existentă ⁷	*CHANGE	*EXECUTE
SNDPTFORD ¹⁰ (Q)			
SNDSVRQS (Q)			

Comenzi service

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
STRCMNTRC ¹¹ (Q)	NWID (ID rețea) sau descriere de linie	*USE	*EXECUTE
	Job observat ¹⁷		
	Urmărire program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
STRCPYSCN	Coadă joburi	*USE	*EXECUTE
	Descriere dispozitiv	*USE	*EXECUTE
	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
STRSRVJOB (Q)	Profil utilizator al jobului	*USE	*EXECUTE
STRSST ³ (Q)			
STRTRC (Q) ^{11, 15}	Job observat ¹⁷		
	Urmărire program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
STRWCH ¹⁶ (Q)	Job observat ¹⁷		
	Observare program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCCNN ¹¹ (Q)	Job observat ¹⁷		
	Urmărire program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT ¹¹ (Q)	Job observat ¹⁷		
	Urmărire program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCJOB (Q)	Fișier sursă, dacă este specificat	Vedeți regulile generale.	Vedeți regulile generale.
	Program de ieșire, dacă există	*USE	*EXECUTE
TRCTCPAPP ¹¹ (Q)	Descriere de linie	*USE	
	Interfață rețea	*USE	
	Interfață rețea	*USE	
	Job observat ¹⁷		
	Urmărire program	*OBJOPR și *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
VFYCMN (Q)	Descriere de linie ⁵	*USE	*EXECUTE
	Descriere controler ⁵	*USE	*EXECUTE
	ID rețea ⁵	*USE	*EXECUTE
VFYLNKLPDA (Q)	Descriere de linie	*READ	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
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/QVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB ^{1, 10} (Q)	Linie, controler, NWID (ID rețea) și dispozitiv bazat pe acțiunea de analiză problemă	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKSRVPVD (Q)			
WRKTRC ¹¹ (Q)			
WRKWCH ¹⁹ (Q)			
1	Aveți nevoie de autorizație pentru comanda PRERRLOG pentru unele proceduri de analiză dacă înregistrările din istoricul de erori sunt salvate.		
2	Se aplică de asemenea toate restricțiile pentru comanda RSTOBJ.		
3	Autorizația specială Service (*SERVICE) este necesară pentru a rula această comandă.		
4	Obiectele listate sunt folosite de comandă, dar autorizația pentru obiecte nu este verificată. Autorizația pentru a folosi comanda este suficientă pentru a folosi obiectele.		
5	Aveți nevoie de autorizația *USE pentru obiectele de comunicații pe care le verificați.		
6	Trebuie să aveți autorizația specială *SPLCTL pentru a salva un fișier de spool.		
7	Atunci când SAVAPARDDTA este rulată pentru o problemă nouă, o bibliotecă unică APAR este creată pentru acea problemă. Dacă rulați din nou SAVAPARDDTA pentru aceeași problemă pentru a colecta mai multe informații, trebuie să aveți autorizația Use pentru bibliotecă APAR pentru acea problemă.		
8	Opțiunea de a adăuga un membru nou la un fișier de ieșire existent nu este validă pentru această comandă.		
9	Această comandă are aceleași autorizații și restricții ca și comenzile APYPTF și LODPTF.		
10	Pentru a accesa opțiunile 1 și 3 din ecranul "Selectare opțiune de raport" trebuie să aveți autorizația *USE pentru comanda SNDSRVRS. Următoarele restricții se aplică parametrului IMGDIR:		
	<ul style="list-style-type: none"> • Trebuie să aveți autorizare *X asupra fiecărui director din cale. • Trebuie să aveți autorizare *WX asupra directorului care conține imaginea optică. 		

Comenzi service

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
11	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE sau trebuie să fiți autorizat pentru funcția Urmărire serviciu din i5/OSi5/OS System/400 prin suportul Administrare aplicație din Navigator iSeries. Poate fi folosită de asemenea comanda Modificare informații de folosire funcție (CHGFCNUSG), cu ID-ul de funcție QIBM_SERVICE_TRACE, pentru a modifica lista de utilizatori care au permisunea de a realiza operații de urmărire.		
12	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE sau trebuie să fiți autorizat pentru funcția Urmărire serviciu din i5/OS prin suportul Administrare aplicație a Navigator iSeries. Se poate folosi de asemenea comanda Modificare informații de folosire funcție (CHGFCNUSG), cu un ID funcție de QIBM_SERVICE_DUMP, pentru a modifica lista utilizatorilor care au permisunea de a rula operații 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 aveți autorizarea specială *IOSYSCFG când descrierea de dispozitiv este alocată de un dispozitiv bibliotecă de medii de stocare.		
15	Dacă specificați un nume generic de utilizator pentru parametrul Nume job, aveți nevoie de autorizarea specială toate obiectele (*ALLOBJ) sau să fiți autorizat pentru funcția Istoric job pentru toate obiectele i5/OS prin suportul de Administrare aplicație din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_ALLOBJ_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operații de urmărire.		
16	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE sau trebuie să fiți autorizat pentru funcția Urmărire serviciu din sistemul de operare prin suportul Administrare aplicație din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_ALLOBJ_SERVICE pentru a modifica lista de utilizatori cărora le este permis să pornească și să oprească operații 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 funcția dacă sunt autorizați să folosească funcția Watch Any Job (Observă orice job) a sistemului de operare prin Administrarea aplicațiilor din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_ALLOBJ_SERVICE pentru a modifica lista de utilizatori cărora le este permis să pornească și să oprească operații de urmărire.		
18	Este necesară aceeași autorizare ca la comanda STRWCH.		
19	Pentru a folosi această comandă, trebuie să aveți autorizarea specială *SERVICE sau trebuie să fiți autorizat pentru funcția Urmărire serviciu și Observare serviciu din sistemul de operare prin suportul Administrare aplicație din Navigator iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcție) cu ID-ul de funcție QIBM_ACCESS_SERVICE_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operații de urmărire.		

Comenzi pentru dicționar ajutor corectare ortografică

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTSPADCT	Dicționar ajutător pentru corectare ortografică	*OBJEXIST	*EXECUTE
	Dicționar - REPLACE(*NO)		*READ, *ADD
	Dicționar - REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
DLTSPADCT	Dicționar ajutător pentru corectare ortografică	*OBJEXIST	*EXECUTE
WRKSPADCT ¹	Dicționar ajutător pentru corectare ortografică	Orice autorizație	*USE

Comenzi dicționar ajutor corectare ortografică

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.			

Comenzi pentru sferă de control

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSOCE	Sferă de control ¹	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sferă de control ¹	*USE, *DLT	*EXECUTE
WRKSOC	Sferă de control ¹	*USE	*EXECUTE
¹ Sfera de control este fișier fizic QUSRSYS/QAALSOC.			

Comenzi pentru fișier spool

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Parametri coadă de ieșire			Autorizare specială	Autorizație necesară		
		DSPDTA	AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci	
CHGSPLFA ^{1,2}	Coadă de ieșire ³		*DTAAUT			*READ, *DLT, *ADD		
			*OWNER			Proprietar ⁴		
				*YES	*JOBCTL			
CHGSPLFA ¹ , dacă se mută fișierul de spool	Coadă de ieșire originală ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Proprietar ⁴		
				*YES	*JOBCTL			
	Fișier spool	*OWNER				Proprietar ⁶		
	Coadă de ieșire destinație ⁷						*READ	*EXECUTE
				*YES	*JOBCTL			*EXECUTE
Dispozitiv destinație						*USE		

Comenzi fișier spool

Comandă	Obiect referențiat	Parametri coadă de ieșire			Autorizare specială	Autorizație necesară		
		DSPDTA	AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci	
CPYSPLF ¹	Fișier bază de date					Vedeți regulile generale pentru Afișare (DSP) sau altă operație care folosește fișierul ieșire (OUTPUT(*OUTFILE))	Vedeți regulile generale pentru Afișare (DSP) sau altă operație care folosește fișierul ieșire (OUTPUT(*OUTFILE))	
	Fișier spool	*OWNER				Proprietar ⁶		
	Coadă de ieșire ³	*YES					*READ	
		*NO	*DTAAUT				*READ, *ADD, *DLT	
		*NO	*OWNER				Proprietar ⁴	
	*YES sau *NO		*YES	*JOBCTL				
DLTEXPSPLF (Q)	Pool de discuri independent				*SPLCTL	*EXECUTE		
DLTSPLF ¹	Coadă de ieșire ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Proprietar ⁴		
				*YES	*JOBCTL			
DSPSPLF ¹	Coadă de ieșire ³	*YES				*READ		
		*NO	*DTAAUT			*READ, *ADD, *DLT		
		*NO	*OWNER			Proprietar ⁴		
		*YES sau *NO		*YES	*JOBCTL			
	Fișier spool	*OWNER				Proprietar ⁶		
HLDSPLF ¹	Coadă de ieșire ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Proprietar ⁴		
				*YES	*JOBCTL			
RCLSPLSTG (Q)								
RLSSPLF ^{1, 8}	Coadă de ieșire ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Proprietar ⁴		
				*YES	*JOBCTL			
SNDNETSPLF ^{1,5}	Coadă de ieșire ³	*YES				*READ		
		*NO	*DTAAUT			*READ, *ADD, *DLT		
		*NO	*OWNER			Proprietar ⁴		
		*YES sau *NO		*YES	*JOBCTL			
	Fișier spool	*OWNER				Proprietar ⁶		

Comandă	Obiect referențiat	Parametri coadă de ieșire			Autorizare specială	Autorizație necesară	
		DSPDTA	AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
SNDTCPSPLF 1,5	Coadă de ieșire ³	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar ⁴	
		*YES sau *NO		*YES	*JOBCTL		
	Fișier spool	*OWNER				Proprietar ⁶	
WRKSPLF							

¹ Utilizatorii sunt întotdeauna autorizați pentru a-și controla propriile fișier de spool.

² Pentru a muta un fișier spool în fața unei cozi de ieșire (PRTSEQ(*NEXT)) sau pentru a-i modifica prioritatea la o valoare mai mare decât limita specificată în profilul utilizator, trebuie să aveți una din autorizările arătate în coada de ieșire sau să aveți autorizația specială *SPLCTL.

³ Dacă aveți autorizarea specială *SPLCTL, nu aveți nevoie de nici o autorizare pentru coada de ieșire.

⁴ Trebuie să fiți proprietarul cozii de ieșire.

⁵ Trebuie să aveți autorizația *USE pentru coada de ieșire și bibliotecă de coadă de ieșire a destinatarului atunci când trimiteți un fișier unui utilizator de pe același subsistem.

⁶ Trebuie să fiți proprietarul fișierului spool.

⁷ Dacă aveți autorizația specială *SPLCTL, nu aveți nevoie de autorizație pentru coada de ieșire destinație dar trebuie să aveți autorizația *EXECUTE pentru bibliotecă.

⁸ Când fișierul spool a fost reținut cu HLDJOB SPLFILE(*YES) și fișierul spool a fost de asemenea decuplat de la job, utilizatorul trebuie să aibă autorizația *USE pentru comanda RLSJOB fie autorizația specială *JOBCTL sau să fie proprietarul fișierului spool.

Comenzi pentru descriere subsistem

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
	Profil utilizator	*USE	
ADDJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Comenzi descriere subsistem

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil utilizator	*USE	
	Descriere job	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
	Profil utilizator	*USE	
CHGJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil utilizator	*USE	
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD ⁵	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	fișier afișare semnare ⁴	*USE	*EXECUTE
CHGWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
CRTSBSD ⁵ (Q)	Descriere subsistem		*READ, *ADD
	fișier afișare semnare ⁴	*USE	*EXECUTE
DLTSBSD	Descriere subsistem	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Descriere subsistem	*OBJOPR, *READ	*EXECUTE
ENDSBS ¹			
PRTSBSDAUT ⁶			
RMVAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Comenzi descriere subsistem

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RMVRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
STRSBS ¹	Descriere subsistem	*USE	*EXECUTE
WRKSBS ^{2, 3}	Descriere subsistem	Orice autorizație	*USE
WRKSBSD ³	Descriere subsistem	Orice autorizație	*USE
¹	Trebuie să aveți autorizarea specială de control de joburi (*JOBCTL) pentru a folosi această comandă.		
²	Necesită unele autorizații (orice în afară de *EXCLUDE)		
³	Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.		
⁴	Autorizația este necesară pentru a realiza verificările de formă ale fișierului de afișare. Acest ajutor prezice că afișare va merge corect atunci când subsistemul este pornit. Atunci când nu sunteți autorizat pentru fișierul de afișare sau bibliotecă lui, aceste verificări de formă nu vor fi realizate.		
⁵	Trebuie să aveți autorizația specială *SECADM sau *ALLOBJ pentru a specifica o anumită bibliotecă pentru bibliotecă subsistem.		
⁶	Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.		

Comenzi pentru sistem

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PWRDWNYSYS ¹	Catalog de imagini (dacă este specificat)	*USE	
Aceste comenzi nu necesită nici o autorizație obiect:			
CHGSHRPOOL DSPSYSSTS ENDSYS ¹ RCLACTGRP ¹	RCLRSC RETURN RTVGRPA	SIGNOFF WRKSHRPOOL	WRKSYSSTS
¹	Trebuie să aveți autorizarea specială de control de joburi (*JOBCTL) pentru a folosi această comandă.		

Comenzi pentru listă replici sistem

Aceste comenzi nu necesită autorizații obiect:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Comenzi pentru valori sistem

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Aceste comenzi nu necesită vreo autorizație obiect:			
CHGSYSVAL (Q) ^{1,2}	DSPSYSVAL ³	RTVSYSVAL ³	WRKSYSVAL ^{1,2, 3}

Comenzi valori sistem

1	Pentru a modifica unele valori sistem, trebuie să aveți autorizările speciale *ALLOBJ, *ALLOBJ și *SECADM, *AUDIT, *IOSYSCFG sau *JOBCTL.
2	Pentru a folosi această comandă cum a fost livrată de IBM, trebuie să fiți semnat ca QPGMR, QSYSOPR sau QSRV sau să aveți autorizarea specială *ALLOBJ.
3	Pentru a afișa sau extrage valori de sistem referitoare la auditare, trebuie să aveți autorizarea specială *AUDIT sau *ALLOBJ.

Comenzile pentru mediul System/36

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGS36	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
CHGS36A	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Program	*OBJMGT, *USE	*EXECUTE
CHGS36PRCA	Fișier QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Sursă	*OBJMGT, *USE	*EXECUTE
CRTMSGFMNU	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD
	Fișier de afișare dacă există	*ALL	*EXECUTE
	Fișier de mesaje	*USE	*CHANGE
	Fișier sursă QS36SRC	*ALL	*EXECUTE
CRTS36DSPF	Fișier de afișare: REPLACE(*NO)		*READ, *ADD
	Fișier de afișare: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD, *CHANGE
	Fișier-destinație sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fișier sursă QS36SRC	*USE	*EXECUTE
	Comanda Creare fișier de afișare (CRTDSPF)	*OBJOPR	*EXECUTE
CRTS36MNU	Meniu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Meniu: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD, *CHANGE
	Fișier-destinație sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fișier sursă QS36SRC	*USE	*EXECUTE
	Fișier de afișare când REPLACE(*YES) este specificat	*ALL	*EXECUTE
	Fișiere de mesaje numite în sursă	*ALL	*EXECUTE
	Fișier afișare		*CHANGE
	Comanda CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Comanda ADDMSGD	*OBJOPR	*EXECUTE
	Comanda CRTDSPF	*OBJOPR	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
CRTS36MSGF	Fișier de mesaje: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Fișier de mesaje: REPLACE(*YES)	Vedeți regulile generale.	*READ, *ADD, *CHANGE
	Fișier-destinație sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fișier sursă QS36SRC	*USE	*EXECUTE
	Fișier de afișare când REPLACE(*YES) este specificat	*ALL	*EXECUTE
	Fișier de afișare numite în sursă	*ALL	*EXECUTE
	Fișier de mesaje numite în sursă când OPTION este *ADD sau *CHANGE	*CHANGE	*EXECUTE
	Fișiere 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
DS36	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	Fișier QS36PRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fișier QS36PRC, pentru a vedea atribute	*USE	*EXECUTE
EDTS36SRCA	Fișier sursă QS36SRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fișier sursă QS36SRC, pentru a vedea atribute	*USE	*EXECUTE
RSTS36F (Q)	Din-fișier	*USE	*EXECUTE
	În-fișier	*ALL	Vedeți regulile generale.
	Bazat pe fișier fizic, dacă fișierul care este restaurat este fișier (alternativ) logic	*CHANGE	*EXECUTE
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RSTS36FLR ^{1,2,3} (Q)	Folder S/36	*USE	*EXECUTE
	În-fișier	*CHANGE	*EXECUTE
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RSTS36LIBM (Q)	Din-fișier	*USE	*EXECUTE
	În-fișier	*ALL	Vedeți regulile generale.
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVS36A	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
SAVS36F	Din-fișier	*USE	*EXECUTE
	În-fișier, atunci când este fișier fizic	*ALL	Vedeți regulile generale.
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
SAVS36LIBM	Din-fișier	*USE	*EXECUTE
	În-fișier, atunci când este fișier fizic	*ALL	Vedeți regulile generale.
	Fișier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE

Comenzi mediu System/36

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
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	Fișier QS36PRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fișier QS36PRC, pentru a vedea atribute	*USE	*EXECUTE
WRKS36SRCA	Fișier sursă QS36SRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fișier sursă QS36SRC, pentru a vedea atribute	*USE	*EXECUTE
<p>¹ Aveți nevoie de autorizația *ALL pentru document dacă îl înlocuiți. Aveți nevoie de autorizații operaționale și pentru toate datele pentru folder dacă restaurați informații noi în aceste foldere, sau aveți nevoie de autorizația specială *ALLOBJ.</p> <p>² Dacă este folosit pentru dicționar, este necesară doar autorizația pentru comandă.</p> <p>³ Trebuie să fiți înscris în directorul de distribuire sistem dacă folderul sursă este un folder document.</p>			

Comenzi pentru tabelă

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTTBL	Tabelă		*READ, *ADD, *EXECUTE
	Fișier sursă	*USE	*EXECUTE
DLTTBL	Tabelă	*OBJEXIST	*EXECUTE
WRKTBL ¹	Tabelă	Orice autorizație	*USE
<p>¹ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.</p>			

Comenzi pentru TCP/IP

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTCPSVR ¹	Program de apelat	*EXECUTE	*EXECUTE
CHGTCPSVR ¹	Program de apelat	*EXECUTE	*EXECUTE
CVTTCPCL (Q)	Obiecte fișier	*USE	*EXECUTE
ENDTCP (Q)	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENDTCPIFC (Q)	Obiecte fișier	*USE	*EXECUTE
	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
ENDTCPPTP	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
ENDTCPSRV (Q)	Obiecte fișier	*USE	*EXECUTE
FTP	Obiecte fișier	*USE	*EXECUTE
	Obiecte tabel	*USE	*EXECUTE
LPR ²	Obiecte de personalizare stație de lucru	*USE	*EXECUTE
SETVTTBL	Obiecte tabel	*USE	*EXECUTE
SNDTCPSPLF ²	Obiecte de personalizare stație de lucru	*USE	*EXECUTE
STRTCP (Q)	Obiecte fișier	*USE	*EXECUTE
	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
STRTCPFTP	Obiecte tabel	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
STRTCPIFC (Q)	Obiecte fișier	*USE	*EXECUTE
	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
STRTCPPTP	Descriere de linie ⁴	*USE	*EXECUTE
	Descriere controler ⁴	*USE	*EXECUTE
	Descriere de dispozitiv ⁴	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
STRTCPSVR (Q)	Obiecte tabel	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
STRTCPTELN	Obiecte tabel	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
	Dispozitiv virtual stație de lucru ⁵	*USE	*EXECUTE
TELNET	Obiecte tabel	*USE	*EXECUTE
	Obiecte fișier	*USE	*EXECUTE
	Dispozitiv virtual stație de lucru ⁵	*USE	*EXECUTE
Aceste comenzi nu necesită nici o autorizație obiect:			

Comenzi TCP/IP

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCOMSNMP ¹	CFGTCPSMTP	CHGVTMAP	RMVTCPRSI ¹
ADDNETBLE ¹	CFGTCPSNMP	DSPVTMAP	RMVTCPRTE ¹
ADDPCLTBLE ¹	CFGTCPTLN	ENDTCPCNN	RMVTCPSVR ¹
ADDSRVTBLE ¹	CHGCOMSNMP ¹	MGRTCPHT ¹	RNMTCPHTE ¹
ADDTCPHTE ¹	CHGFTPA ¹	NETSTAT	SETVTMAP
ADDTCPIFC ¹	CHGLPDA ¹	PING	VFYTCPCNN
ADDTCPPORT ¹	CHGSMTA ¹	RMVCOMSNMP ¹	WRKNAMSMTP ³
ADDTCPRSI ¹	CHGSNMPA ¹	RMVNETTBLE ¹	WRKNETTBLE ¹
ADDTCPRTE ¹	CHGTCPA ¹	RMVPCLTBLE ¹	WRKPCLTBLE ¹
CFGTCP	CHGTCPHTE ¹	RMVSRVTBLE ¹	WRKSRVTBLE ¹
CFGTCPAPP	CHGTCPIFC ¹	RMVTCPHTE ¹	WRKTCPSTS
CFGTCPFTP ¹	CHGTCPRTE ¹	RMVTCPIFC ¹	
CFGTCPPLD ¹	CHGTELNA ¹	RMVTCPPORT ¹	
¹	Trebuie să aveți autorizația specială *IOSYSCFG pentru a folosi această comandă.		
²	Comanda SNDTCPSPLF și comanda LPR folosesc aceleași combinații de autorizații obiect referențiat ca și comanda SNDNETSPLF.		
³	Trebuie să aveți autorizația specială *SECADM pentru a modifica tabelul sistem alias sau alt tabel alias al unui profil utilizator.		
⁴	Dacă aveți autorizația specială *JOBCTL, nu aveți nevoie de autorizația specificată pentru obiect.		
⁵	Dacă aveți autorizația specială *JOBCTL, nu aveți nevoie de autorizația specificată pentru obiectul de pe sistemul la distanță.		

Comenzi pentru descriere fus orar

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGTIMZON	Descriere fus orar	*CHANGE	*EXECUTE
CRTTIMZON	Descriere fus orar		*READ, *ADD
DLTIMZON ¹	Descriere fus orar	*OBJEXIST	*EXECUTE
WRKTIMZON ²	Descriere fus orar	*USE	*USE
¹	Descrierea fus orar specificată în valoare sistem QTIMZON nu poate fi ștearsă.		
²	Dacă un mesaj este folosit pentru a specifica numele abreviate și complete ale descrierii de fus orar, trebuie să aveți autorizația *USE pentru fișierul de mesaje și autorizația *EXECUTE pentru biblioteca fișierului de mesaje pentru a vedea numele complete și abreviate.		

Comenzi pentru date comandă modernizare

Aceste comenzi sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
WRKORDINF	Fișier QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Comenzi pentru index utilizator, coadă utilizator și spațiu utilizator

Comanda	Obiect referențiat	Autorizație necesară	
		Pentru obiect	Pentru bibliotecă
DLTUSRIDX	Index utilizator	*OBJEXIST	*EXECUTE
DLTUSRQ	Coadă utilizator	*OBJEXIST	*EXECUTE
DLTUSRSPC	Spațiu utilizator	*OBJEXIST	*EXECUTE

Comenzi pentru sistem de fișiere definit de utilizator

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
ADDMFS ^{1,2,3}	dir_pestă_care_se_montează	*DIR	"root" (/)	*W
	Prefix cale	Vedeți regulile generale.		
CRTUDFS ^{1,2,6,7} (Q)	/dev/QASPxx sau /dev/IASPname	*DIR	"root" (/)	*RWX
DLTUDFS ^{1,2,4,5,8,9} (Q)	/dev/QASPxx sau /dev/IASPname	*DIR	"root" (/)	*RWX
	orice_obiect_epfs		"root" (/)	*RWX, *OBJEXIST
DSPUDFS	unele_dirxx	*DIR	"root" (/)	*RX
MOUNT ^{1,2,3}	dir_pestă_care_se_montează	*DIR	"root" (/)	*W
	Prefix cale	Vedeți regulile generale.		
RMVMFS ¹				
UNMOUNT ¹				

¹ Pentru a folosi această comandă, trebuie să aveți autorizația specială *IOSYSCFG.

² Există două convenții de numire directoare, care depind de locația sistemului de fișiere definit de utilizator (UDFS). Folosiți una din convențiile 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 conține *BLKSF care este montat.

³ Directorul peste care se montează este orice director IFS peste care se poate monta.

⁴ Un UDFS poate conține un întreg subarbore de obiecte, astfel atunci când ștergeți un UDFS, ștergeți obiecte de toate tipurile care pot fi stocate în sistemul de fișiere definit de utilizator.

⁵ Atunci când folosiți comenzi DLTUDFS, trebuie să aveți autorizația *OBJEXIST pentru fiecare obiect din UDFS altfel nici un obiect nu este șters.

Comenzi sistem de fișiere definit de utilizator

Comandă	Obiect referențiat	Tip obiect	Sistem fișier	Autorizație necesară pentru obiect
6	Trebuie să aveți autorizările speciale *ALLOBJ (toate obiectele) și *SECADM (administrator securitate) pentru a specifica o valoare pentru parametrul CRTOBJSCAN (opțiunea Scanare pentru obiecte) alta decât *PARENT.			
7	Autorizația specială (*AUDIT) este necesară atunci când specificați o valoare alta decât *SYSVAL pentru valoare Auditare pentru parametrul (CRTOBJAUD) al obiectelor.			
8	Trebuie să aveți autorizări de scriere (*W) și execuție (*X) asupra tuturor obiectelor director care nu sunt goale din UDFS.			
9	<p>Dacă un obiect director care nu este gol din UDFS are atributul "restricție de redenumire și dezlegare" setat Yes (acest atribut este echivalent cu bitul de mod S_ISVTX), atunci una sau mai multe din următoarele condiții trebuie să fie adevărate:</p> <ul style="list-style-type: none"> • Trebuie să fiți proprietarul tuturor obiectelor conținute în director. • Trebuie să fiți proprietarul directorului. • Trebuie să aveți autorizare specială *ALLOBJ. 			

Comenzi pentru profil utilizator

Comenzile identificate cu (Q) sunt livrate cu autorizația publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalți.

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZDFTPWD ^{3, 14,} 15(Q)			
ANZPRFACT ^{3, 14,} 15(Q)			
CHGACTPRFL ¹⁴ (Q)			
CHGACTSCDE ^{3, 14,} 15(Q)			
CHGDSTPWD ¹			
CHGEXPSCDE ^{3, 14,} 15(Q)			
CHGPRF	Profil utilizator	*OBJMGT, *USE	
	Program inițial ²	*USE	*EXECUTE
	Meniu inițial ²	*USE	*EXECUTE
	Descriere job ²	*USE	*EXECUTE
	Coadă de mesaje ²	*USE	*EXECUTE
	Coadă de mesaje ²	*USE	*EXECUTE
	Program de tratare tastă Attn ²	*USE	*EXECUTE
	Bibliotecă curentă ²	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD ¹¹ (Q)			

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGUSRPRF ³	Profil utilizator	*OBJMGT, *USE	*EXECUTE
	Program inițial ²	*USE	*EXECUTE
	Meniu inițial ²	*USE	*EXECUTE
	Descriere job ²	*USE	*EXECUTE
	Coadă de mesaje ²	*USE	*EXECUTE
	Coadă de mesaje ²	*USE	*EXECUTE
	Program de tratare tastă Attn ²	*USE	*EXECUTE
	Bibliotecă curentă ²	*USE	*EXECUTE
	Profil grup (GRPPRF sau SUPGRPPRF) ^{2,4}	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPTI	Profil utilizator	*CHANGE	
CHKPWD			
CRTUSRPRF ^{3, 12, 17}	Program inițial	*USE	*EXECUTE
	Meniu inițial	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
	Coadă mesaje	*USE	*EXECUTE
	Coadă de ieșire	*USE	*EXECUTE
	Program de tratare tastă Attn	*USE	*EXECUTE
	Bibliotecă curentă	*USE	*EXECUTE
	Profil grup (GRPPRF sau SUPGRPPRF) ⁴	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT ^{3, 14}			
DLTUSRPRF ^{3,9}	Profil utilizator	*OBJEXIST, *USE	*EXECUTE
	Coadă de mesaje ⁵	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPACTPRFL ^{14(Q)}			
DSPACTSCD ^{14(Q)}			
DSPAUTUSR ⁶	Profil utilizator	*READ	
DSPEXPSCD ^{14(Q)}			
DSPPGMADP	Profil utilizator	*OBJMGT	
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPUSRPRF ¹⁹	Profil utilizator	*READ	*EXECUTE
	Fișier ieșire	Vedeți regulile generale.	Vedeți regulile generale.
DSPUSRPTI	Profil utilizator	*USE	
GRTUSRAUT ⁷	Profil utilizator referențiat	*READ	
	Obiecte pentru care acordați autorizație	*OBJMGT	*EXECUTE
PRTPRFINT ^{14(Q)}			
PRTUSRPRF ¹⁸			
RSTAUT (Q) ⁸			

Comenzi profil utilizator

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă
RSTUSRPRF (Q) ^{8,10, 16}			
RTVUSRPRF ²⁰	Profil utilizator	*READ	
RTVUSRPRTI	Profil utilizator	*USE	
SAVSECDTA ⁸	Fișier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fișier de salvare, dacă există înregistrări	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF ¹³	Profil utilizator	Orice autorizație	

- ¹ Această comandă poate rula doar dacă sunteți înregistrat ca QSECOFR.
- ² Aveți nevoie de autorizație obiect doar pentru câmpurile pe care le modificați în profilul utilizator.
- ³ Autorizația specială *SECADM este necesară.
- ⁴ Autorizația *OBJMGT pentru profilul utilizator nu poate veni de la autorizația adoptată.
- ⁵ Coadă de mesaje asociată cu profilul utilizator este ștearsă dacă este deținută de acel profil utilizator. Pentru a șterge coada de mesaje, utilizatorul care rulează DLTUSRPRF trebuie să aibă autorizațiile specificate.
- ⁶ Afișare include doar profilurile utilizator pe care utilizatorul care rulează comanda are autorizația specificată.
- ⁷ Vedeți autorizările necesare pentru comanda GRTOBJAUT.
- ⁸ Autorizația specială *SAVSYS este necesară.
- ⁹ Dacă selectați opțiunea de a șterge obiectele deținute de profilul utilizator, trebuie să aveți autorizația necesară operației de ștergere. Dacă selectați opțiunea de transfer proprietate către alt profil utilizator, trebuie să aveți autorizația necesară pentru obiecte și pentru profilul de utilizator destinație. Vedeți informațiile pentru comanda CHGOBJOWN.
- ¹⁰ Trebuie să aveți autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.
- ¹¹ Trebuie să aveți autorizația specială *AUDIT.
- ¹² Utilizatorului al cărui profil este creat îi sunt date aceste autorizații: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.
- ¹³ Pentru a folosi o operație individuală, trebuie să aveți autorizația necesară de operație.
- ¹⁴ Trebuie să aveți autorizația specială *ALLOBJ pentru a folosi această comandă.
- ¹⁵ Trebuie să aveți autorizația specială *JOBCTL pentru a folosi această comandă.
- ¹⁶ Trebuie să aveți autorizațiile speciale *ALLOBJ și *SECADM pentru a specifica SECDTA(*PWDGRP), USRPRF(*ALL) sau OMITUSRPRF.
- ¹⁷ Când executați o comandă CRTUSRPRF, nu puteți crea un profil de utilizator (*USRPRF) într-un pool de discuri independent. Totuși, când un utilizator este autorizat în particular asupra unui obiect din pool-ul de disc independent, este proprietarul unui obiect dintr-un pool de disc independent sau este grupul primar al unui obiect dintr-un pool de disc independent atunci numele profilului este memorat în pool-ul de disc independent. Dacă pool-ul de disc independent este mutat în alt sistem, autorizația privată, proprietatea asupra obiectului și intrările din grupul primar vor fi atașate profilului cu același nume de pe sistemul destinație. Dacă nu există un profil pe sistemul destinație, va fi creat. Utilizatorul nu va avea nici o autorizație specială și parola va fi setată la *NONE.
- ¹⁸ Trebuie să aveți autorizația specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.
- ¹⁹ Trebuie să aveți ori autorizarea specială *ALLOBJ sau *AUDIT pentru a fi afișată valoarea curentă de auditare a obiectului și a acțiunii afișate. În caz contrar va fi afișată valoarea *NOTAVL, pentru a indica faptul că valorile nu sunt disponibile pentru afișare.
- ²⁰ Trebuie să aveți autorizarea specială *ALLOBJ sau *AUDIT pentru a extrage valorile curente OBJAUD și AUDLVL. În caz contrar va fi returnată valoarea *NOTAVL, pentru a indica faptul că valorile nu sunt disponibile pentru extragere.

Comenzi pentru listă de validare

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTVLDL	Listă de validare		*ADD, *READ
DLTVLDL	Listă de validare	*OBJEXIST	*EXECUTE

Comenzi pentru personalizare stație de lucru

Comandă	Obiect referențiat	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTWSCST	Fișier sursă	*USE	*EXECUTE
	Obiect de personalizare stație de lucru, dacă REPLACE(*NO)		*READ, *ADD
	Obiect personalizare stație de lucru, dacă REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Obiecte de personalizare stație de lucru	*OBJEXIST	*EXECUTE
RTVWSCST	Fișier-destinație, dacă el există și se adaugă un nou membru	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Fișier-destinație, dacă fișierul și membru există	*OBJOPR, *ADD, *DLT	*EXECUTE
	Fișier-destinație, dacă fișierul nu există		*READ, *ADD

Comenzi pentru scriitor

Comandă	Obiect referențiat	Parametri coadă de ieșire		Autorizare specială	Autorizări necesare	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CHGWTR ^{2, 4}	Coadă de ieșire curentă ¹	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar ³	
			*YES	*JOBCTL		
	Crearea unei noi cozi de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
*OWNER				Proprietar	*EXECUTE	
		*YES	*JOBCTL		*EXECUTE	
ENDWTR ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar ³	
			*YES	*JOBCTL		
HLDWTR ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar ³	
			*YES	*JOBCTL		

Comenzi scriitor

Comandă	Obiect referențiat	Parametri coadă de ieșire		Autorizare specială	Autorizări necesare	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
RLSWTR ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar ³	
			*YES	*JOBCTL		
STRDKTWTR ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă mesaje				*OBJOPR, *ADD	*EXECUTE
	Descriere dispozitiv				*OBJOPR, *READ	
STRPRTWTR ¹	Coadă de ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă mesaje				*OBJOPR, *ADD	*EXECUTE
	obiect de personalizare stație 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 ieșire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă mesaje				*OBJOPR, *ADD	*EXECUTE
	obiect de personalizare stație de lucru				*USE	*EXECUTE
	Program cu driver utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Program transformare date utilizator				*OBJOPR *EXECUTE	*EXECUTE
WRKWTR						

Comandă	Obiect referențiat	Parametri coadă de ieșire		Autorizare specială	Autorizări necesare	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
¹						Dacă aveți autorizarea specială *SPLCTL, nu aveți nevoie de nici o autorizare pentru coada de ieșire.
²						Pentru modificarea cozii de ieșire pentru scriitor, aveți nevoie de autorizările specificate pentru noua coadă de ieșire.
³						Trebuie să fiți proprietarul cozii de ieșire.
⁴						Trebuie să aveți autorizația *EXECUTE pentru biblioteca noii cozi de ieșire chiar dacă utilizatorul are autorizația specială *SPLCTL.

Anexa E. Operațiile și auditarea obiectelor

Această anexă listează operațiile care pot fi executate asupra obiectelor din sistem și dacă aceste operații sunt auditate. Listele sunt organizate după tipul de obiect. Operațiile sunt grupate în funcție de faptul că ele sunt auditate când este specificat *ALL sau *CHANGE pentru valoarea OBJAUD a comenzii CHGOBJAUD sau CHGDLOAD.

Dacă o înregistrare de auditare este scrisă pentru o acțiune depinde de o combinație de valori sistem, inclusiv o valoare din profilul utilizator al utilizatorului care execută acțiunea și o valoare definită pentru obiect. "Planificarea auditării accesului la obiect" la pagina 252 descrie modul în care se setează auditarea pentru obiecte.

Operațiile arătate în tabele cu litere mari, precum CPYF, se referă la comenzi CL, aceasta dacă nu sunt etichetate ca API (interfață de programare aplicație).

Operații obișnuite tuturor tipurilor de obiecte:

- Operația 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

SAVSAVFTA

Salvare date fișier de salvare

SAVDLO

Salvare obiect DLO

SAVLICPGM

Salvare program licențiat

SAVSHF

Salvare raft de cărți

Notă: Înregistrarea de auditare pentru operația de salvare va identifica dacă salvarea a fost făcută cu STG(*FREE).

- Operație de modificare

Auditare obiect

APYJRNCHG

Aplicare modificări jurnalizate

CHGJRNOBJ

Modificare obiect jurnalizat

CHGOBJD

Modificare descriere obiect

CHGOBJOWN

Modificare proprietar obiect

CRTxxxxxx

Creare obiect

Note:

1. Dacă este specificat *ALL sau *CHANGE pentru biblioteca destinație, este scrisă o intrare ZC când este creat un obiect.
2. Dacă este activ *CREATE pentru auditarea de acțiune, este scrisă o intrare CO când este creat un obiect.

DLTxxxxxx

Ștergere obiect

Note:

1. Dacă este specificat *ALL sau *CHANGE pentru biblioteca în care se află obiectul, este scrisă o intrare ZC când este șters un obiect.
2. Dacă este specificat *ALL sau *CHANGE pentru obiect, este scrisă o intrare ZC când este șters.
3. Dacă este activ *DELETE pentru auditarea de acțiune, este scrisă o intrare DO când este șters un obiect.

ENDJRNxxx

Terminare jurnalizare

GRTOBJAUT

Acordare autorizare obiect

Notă: Dacă este acordată o autorizare pe baza unui obiect referențiat, nu este scrisă o înregistrare de auditare pentru obiectul referențiat.

MOV OBJ

Mutare obiect

QjoEndJournal

Terminare jurnalizare

QjoStartJournal

Pornire jurnalizare

QSRRSTO

Restaurare API obiect

QsrRestore

Restaurare obiect în API-ul director

RCLSTG

Revendicare spațiu de stocare:

- Dacă un obiect este securizat printr-un *AUTL deteriorat, este scrisă o înregistrare de auditare când obiectul este securizat de lista de autorizații 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 configurație

RSTLIB

Restaurare bibliotecă

RSTLICPGM

Restaurare program licențiat

RSTOBJ

Restaurare obiect

RVKOBJAUT

Revocare autorizare obiect

STRJRNxxx

Pornire jurnalizare

- Operațiile care nu sunt auditate

Prompt²

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

Afișare descriere obiect

DSPOBJAUT

Afișare autorizare obiect

EDTOBJAUT

Editare autorizare obiect

Notă: Dacă autorizarea de obiect este modificată și auditarea acțiunii include *SECURITY sau dacă obiectul este auditat, este scrisă o înregistrare de auditare.

QSYCUSRA

Verificare autorizare utilizator pentru un API obiect

QSYLUSRA

Listează utilizatorii autorizați 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 spațiul utilizator folosit pentru a conține informații.

2. Apare un prompt care afișează valorile curente când este cerută avertizarea pentru o comandă. De exemplu, dacă introduceți CHGURSPRF USERA și apăsați F4 (prompt), ecranul Modificare profil utilizator arată valorile curente pentru profilul utilizator USERA.

Auditare obiect

QSYRUSRA

Extragere autorizare utilizator pentru un API obiect

RCLTMPSTG

Revendicare spațiu de stocare temporar

RTVOBJD

Extragere descriere obiect

SAVSTG

Salvare spațiu de stocare (auditare doar pentru comanda SAVSTG)

WRKOBJLCK

Gestionare blocare obiect

WRKOBJOWN

Gestionare obiecte după proprietar

WRKxxx

Gestionare comenzi de obiecte

Operațiile pentru Timpii de recuperare cale de acces:

Notă: Modificările timpilor de recuperare cale de acces sunt auditate dacă valoarea de sistem acțiune de auditare (QAUDLVL) sau parametrul de auditare acțiune (AUDLVL) din profilul utilizator include *SYSMGT.

- Operațiile care sunt auditate

CHGRCYAP

Recuperare modificări pentru căile de acces

EDTRCYAP

Editare modificări pentru căile de acces

- Operațiile care nu sunt auditate

DSPRCYAP

Afișare modificări pentru căile de acces

Operațiile pentru tabela de alertă (*ALRTBL):

- Citire operație

Nimic

- Operație de modificare

ADDALRD

Adăugare descriere alertă

CHGALRD

Modificare descriere alertă

CHGALRTBL

Modificare tabelă alertă

RMVALRD

Înlăturare descriere alertă

- Operațiile care nu sunt auditate

Tipărire

Tipărire descriere alertă

WRKALRD

Gestionare descriere alertă

WRKALRTBL

Gestionare tabelă alertă

Operațiile pentru lista de autorizații (*AUTL):

- Citire operație

Nimic

- Operație de modificare

ADDAUTLE

Adăugare intrare listă de autorizații

CHGAUTLE

Modificare intrare listă de autorizații

EDTAUTL

Editare listă de autorizații

RMVAUTLE

Înlăturare intrare listă de autorizații

- Operațiile care nu sunt auditate

DSPAUTL

Afișare listă de autorizații

DSPAUTLOBJ

Afișare obiecte din lista de autorizații

DSPAUTLDLO

Afișare DLO listă de autorizații

RTVAUTLE

Extragere intrare listă de autorizații

QSYLATLO

Obiecte listă securizate de API-ul *AUTL

WRKAUTL

Gestionare listă de autorizații

Operațiile pentru deținător de autorizare (*AUTHLR):

- Citire operație

Nimic

- Operație de modificare

Asociat

Când este folosit pentru a securiza un obiect.

- Operațiile care nu sunt auditate

DSPAUTHLR

Afișare deținător de autorizare

Operațiile pentru directorul de legături (*BNDDIR):

- Citire operație

CRTPGM

Creare program

CRTSRVPGM

Creare program service

Auditare obiect

RTVBNSRC

Extragere sursă binder

UPDPGM

Actualizare program

UPDSRVPGM

Actualizare program service

- Operație de modificare

ADDBNDDIRE

Adăugare intrare director de legături

RMVBNDDIRE

Înlăturare intrare director de legături

- Operațiile care nu sunt auditate

DSPBNDDIR

Afișare conținut pentru un director de legături

WRKBNDDIR

Gestionare director de legături

WRKBNDDIRE

Gestionare intrare director de legături

Operații pentru lista de configurație (*CFGL):

- Citire operație

CPYCFGL

Copiere listă de configurație. O intrare este scrisă pentru *din-lista-configurație*

- Operație de modificare

ADDCFGL

Adăugare intrări listă de configurație

CHGCFGL

Modificare listă de configurație

CHGCFGLE

Modificare intrare listă de configurație

RMVCFGLE

Înlăturare intrare listă de configurație

- Operațiile care nu sunt auditate

DSPCFGL

Afișare listă de configurație

WRKCFGL

Gestionare listă de configurație

Operații pentru fișiere speciale (*CHRSF):

Vedeți Operații pentru fișierul flux (*STMF) pentru auditare *CHRSF.

Operații pentru format diagramă (*CHTFMT):

- Citire operație

Afișare

comanda DSPCHT sau opțiunea F10 din meniul BGU

Tipărire/Plotare

comanda DSPCHT sau opțiunea F15 din meniul BGU

Salvare/Creare

Salvarea sau crearea fișierelor de date grafice (GDF) folosind comanda CRTGDF sau opțiunea F13 din meniul BGU

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

Nimic

Operațiile pentru descrierile C Locale (*CLD):

- Citire operație

RTVCLDSRC

Extragere sursă C Locale

Setlocale

Folosiți obiectul C locale în timpul rulării programului C folosind funcția Setare locale.

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

Nimic

Operații pentru Modificare descriere cerere (*CRQD):

- Citire operație

QFVLSTA

API-ul Listare activități de modificare descriere cerere

QFVRTVCD

API-ul Extragere modificare descriere cerere

SBMCRQ

Lansare modificare cerere

- Operație 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

Auditare obiect

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

- Operațiile care nu sunt auditate

WRKCRQD

Gestionare descrieri cerere modificare

Operațiile pentru clasă (*CLS):

- Citire operație

Nimic

- Operație de modificare

CHGCLS

Modificare clasă

- Operațiile care nu sunt auditate

Pornire job

Când este folosit de gestiunea de lucru pentru a porni un job

DSPCLS

Afișare clasă

WRKCLS

Gestionare clasă

Operații pentru comandă (*CMD):

- Citire operație

Rulare Când comanda rulează

- Operație de modificare

CHGCMD

Modificare comandă

CHGCMDDFT

Modificare valoare implicită comandă

- Operațiile care nu sunt auditate

DSPCMD

Afișare comandă

PRTCMDUSG

Tipărire folosire comandă

QCDRCMDI

API-ul Extragere informații comandă

WRKCMD

Gestionare comandă

Următoarele comenzi sunt folosite în programele CL pentru a controla procesarea și pentru a manipula date în interiorul programului. Utilizarea acestor comenzi nu este auditată.

CALL ¹	ENDPGM	RCVF
CALLPRC	ENDRCV	RETURN
CHGVAR	GOTO	SNDF
COPYRIGHT	IF	SNDRCVF
DCL	MONMSG	TFRCTL
DCLF	PGM	WAIT
DO		
ELSE		
ENDDO		

¹ CALL este auditată dacă este rulată interactiv. Nu este auditată dacă este rulată într-un program CL.

Operațiile pentru lista de conexiuni (*CNNL):

- Citire operație

Nimic

- Operație 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

- Operațiile care nu sunt auditate

Copiere

Opțiunea 3 din WRKCNNL

DSPCNNL

Afișare listă conexiuni

RTVCFGSRC

Extragere sursă a listei de conexiuni

WRKCNNL

Gestionare listă de conexiuni

WRKCNNLE

Gestionare intrări listă de conexiuni

Operațiile pentru descrierea clasă de serviciu (*COSD):

- Citire operație

Nimic

- Operație de modificare

Auditare obiect

CHGCOSD

Modificare descriere clasă de serviciu

- Operațiile care nu sunt auditate

DSPCOSD

Afișare descriere clasă de serviciu

RTVCFGSRC

Extragere sursă a descrierii clasă de serviciu

WRKOSD

Copiere descriere clasă-de-serviciu

WRKOSD

Gestionare descriere clasă-de-serviciu

Operațiile pentru Informațiile parte comunicații (*CSI):

- Citire operație

DSPCSI

Afișare informații parte comunicații

Inițializare

Inițializare conversație

- Operație de modificare

CHGCSI

Modificare informații parte comunicații

- Operațiile care nu sunt auditate

WRKCSI

Gestionare informații parte comunicații

Operațiile pentru harta de produse sistem încrucișate (*CSPMAP):

- Citire operație

Referință

Când este referit într-o aplicație CSP

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

DSPCSPOBJ

Afișare obiect CSP

WRKOBJCSP

Gestionare obiecte pentru CSP

Operații pentru tabela de produse sistem încrucișate (*CSPTBL):

- Citire operație

Referință

Când este referit într-o aplicație CSP

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

DSPCSPOBJ

Afișare obiect CSP

WRKOBJCSP

Gestionare obiecte pentru CSP

Operații pentru Descrierea controler (*CTLD):

- Citire operație

SAVCFG

Salvare configurație

VFYCMN

Test legătură

- Operație de modificare

CHGCTLxxx

Modificare descriere controler

VRYCFG

Activare sau dezactivare descriere controler

- Operațiile care nu sunt auditate

DSPCTLD

Afișare 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

Operațiile pentru descrierea dispozitiv (*DEVd):

- Citire operație

Achiziție

Prima achiziție a dispozitivului în timpul operației de deschidere sau cea de achiziție explicită

Alocare

Alocare conversație

SAVCFG

Salvare configurație

STRPASTHR

Pornire sesiune Pass-Through

Pornirea celei de-a doua sesiuni pentru pass-through intermediar

VFYCMN

Test legătură

- Operație de modificare

Auditare obiect

CHGDEVxxx

Modificare descriere dispozitiv

HLDDEVxxx

Reținere descriere dispozitiv

RLSDEVxxx

Eliberare descriere dispozitiv

QWSSETWS

Modificare setare type-ahead (tastare-înainte) pentru un dispozitiv

VRFCFG

Activare sau dezactivare descriere dispozitiv

- Operațiile care nu sunt auditate

DSPDEVD

Afișare descriere dispozitiv

DSPMODSTS

Afișare stare mod

ENDDEVRCY

Terminare recuperare dispozitiv

HLDCMNDEV

Reținere dispozitiv comunicații

RLSCMNDEV

Eliberare dispozitiv comunicații

RSMDEVRCY

Reluare recuperare dispozitiv

RTVCFGSRC

Extragere sursă a descrierii dispozitiv

RTVCFGSTS

Extragere stare descriere dispozitiv

WRKCFGSTS

Gestionare stare configurație

WRKDEVD

Copiere descriere dispozitiv

WRKDEVD

Gestionare descriere dispozitiv

Operațiile pentru director (*DIR):

- Operații citire/căutare

access, accessx, QlgAccess, QlgAccessx

Determinare accesabilitate fișier

CHGATR

Modificare atribut

CPY Copiere obiect

DSPCURDIR

Afișare director curent

DSPLNK

Afișare legături obiect

- facessx**
Determinare accesibilitate fișier pentru o clasă de utilizatori după descriptor
- getcwd, qlgGetcwd**
API-ul de obținere nume cale pentru directorul curent
- Qp0lGetAttr, QlgGetAttr**
API-uri de obținere atribute
- Qp0lGetPathFromFileID, QlgGetPathFromFileID**
API-uri de obținere cale din identificatorul de fișier
- Qp0lProcessSubtree, QlgProcessSubtree**
API-uri de procesare nume cale
- open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
API-uri de deschidere fișier
- Qp0lSetAttr, QlgSetAttr**
API-uri de setare atribute
- opendir, QlgOpendir**
API-uri de deschidere director
- RTVCURDIR**
Extragere director curent
- SAV** Salvare obiect
- WRKLNK**
Gestionare legături
- Operație de modificare
- CHGATR**
Modificare atribute
- CHGAUD**
Modificare valoare de auditare
- CHGAUT**
Modificare autorizare
- CHGOWN**
Modificare proprietar
- CHGPGP**
Modificare grup primar
- chmod, QlgChmod**
API-ul de modificare autorizații fișier
- chown, QlgChown**
API-ul de modificare proprietar și grup
- CPY** Copiere obiect
- CRTDIR**
Creare director
- fchmod**
API-ul de modificare autorizații fișier după descriptor
- fchown**
API-ul de modificare proprietar și grup după descriptor
- mkdir, QlgMkdir**
API-ul de creare director

Auditare obiect

MOV Mutare obiect

Qp0IRenameKeep, QlgRenameKeep

API-uri de redenumire fișier sau director, păstrare nou

Qp0IRenameUnlink, QlgRenameUnlink

API-uri de redenumire fișier sau director, dezlegare nou

Qp0ISetAttr, 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 fișier și timpi de modificare

WRKAUT

Gestionare autorizare

WRKLNK

Lucru cu legături obiect

- Operațiile care nu sunt auditate

chdir, QlgChdir

API-ul de modificare director

CHGCURDIR

Modificare director curent

close API-ul de închidere descriptor fișier

closedir

API-ul de închidere director

DSPAUT

Afișare autorizare

dup API-ul de deschidere duplicată descriptor fișier

dup2 API-ul de deschidere duplicată de descriptor fișier la un alt descriptor

faccessx

Determinare accesabilitate fișier pentru o clasă de utilizatori după descriptor

fchdir Modificare director curent după descriptor

fctl API-ul de executare comandă de control fișier

fpathconf

API-ul de obținere variabile de nume cale configurabile după descriptor

fstat, fstat64

API-uri de obținere informații fișier după descriptor

givedescriptor

API-ul de acordare acces fișier

ioctl API-ul de executare cereri de control I/O

lseek, lseek64

API-uri de setare offset citire/scriere fișier

lstat, lstat64, QlgLstat, QlgLstat64

API-uri de obținere informații de legătură sau fișier

pathconf, QlgPathconf

API-ul de obținere variabile de nume cale configurabile

readdir

API-ul de citire intrare director

rewinddir

API-ul de resetare flux director

select API-ul de verificare stare I/O ale descriptorilor de fișier multipli

stat, QlgStat

API-ul de obținere informații fișier

takedescriptor

API-ul de preluare acces fișier

Operațiunile pentru Directory Server:

Notă: Acțiunile Directory Server sunt auditate dacă valoarea de sistem pentru auditare acțiune (QAUDLVL) sau parametrul de auditare acțiune (AUDLVL) din profilul de utilizator conține *OFCSRV.

- Operațiile care sunt auditate

Adăugare

Adăugarea unor noi intrări director

Modificare

Modificarea detaliilor intrare director

Ștergere

Ștergerea de intrări director

Redenumire

Redenumirea de intrări director

Tipărire

Afișarea sau tipărirea detaliilor intrare director

Afișarea sau tipărirea detaliilor departament

Afișarea sau tipărirea intrărilor director ca rezultat al unei căutări

RTVDIRE

Extragere intrare director

Colectare

Colectarea datelor de intrare director folosind umbrirea de director

Furnizare

Furnizarea datelor de intrare director folosind umbrirea de director

- Operațiile care nu sunt auditate

comenzi CL

Comenzile CL care lucrează pe director pot fi auditate separat folosind funcția de auditare obiect.

Notă: Unele comenzi de director CL provoacă o înregistrare de auditare pentru că ele execută o funcție care este auditată de auditarea de acțiune *OFCSRV, precum adăugarea unei intrări director.

Auditare obiect

CHGSYSDIRA

Modificare atribute director sistem

Departamente

Adăugarea, modificarea, ștergerea sau afișarea datelor departament director

Descrieri

Asignarea unei descrieri unei intrări de director diferite folosind opțiunea 8 din panoul WRKDIR.

Adăugarea, modificarea sau ștergerea descrierilor departament director

Liste de distribuție

Adăugarea, modificarea, redenumirea sau ștergerea listelor de distribuție

ENDDIRSHD

Terminare umbrire director

Listă Afișarea 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.

Locații Adăugarea, modificarea, ștergerea sau afișarea datelor de locație director

Poreclă

Adăugarea, modificarea, redenumirea sau ștergerea poreclelor

Căutare

Căutarea intrărilor director

STRDIRSHD

Pornire umbrire director

Operații pentru obiectul de bibliotecă documente (*DOC sau *FLR):

- Operație de citire

CHKDOC

Verificare scriere document

CPYDOC

Copiere document

DMPDLO

Abandon DLO

DSPDLOAUD

Afișare auditare DLO

Notă: Dacă informații de auditare sunt afișate pentru toate documentele dintr-un folder și auditare de obiect este specificată pentru folder, este scrisă o înregistrare de auditare. Afișarea auditării de obiect pentru documente individuale nu provoacă o înregistrare de auditare.

DSPDLOAUT

Afișare autorizare DLO

DSPDOC

Afișare document

DSPHLPDOC

Afișare document ajutor

EDTDLOAUT

Editare autorizare DLO

MRGDOC

Combinare document

PRTDOC

Tipărire document

QHFCPYSF

API-ul de copiere fișier flux

QHFGETSZ

API-ul de obținere dimensiune fișier flux

QHFRDDR

API-ul de citire intrare director

QHFRDSF

API-ul de citire fișier flux

RTVDOC

Extragere document

SAVDLO

Salvare DLO

SAVSHF

Salvare raft de cărți

SNDDOC

Trimitere document

SNDDST

Trimitere distribuție

WRKDOC

Gestionare documente

Notă: O intrare de citire este scrisă pentru folderul care conține documentele.

- Operație de modificare

ADDLOAUT

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 distribuție

CPYDOC³

Copiere document

Auditare obiect

Notă: O intrare de modificare este scrisă dacă documentul destinație există deja.

CRTFLR

Creare folder

CVTTOFLR³

Convertire la folder

DLTDLO³

Ștergere DLO

DLTSHF

Ștergere raft de cărți

DTLDOCL³

Ștergere listă de documente

DLTDST³

Ștergere distribuție

EDTDLOAUT

Editare autorizare DLO

EDTDOC

Editare document

FILDOC³

Document fișier

GRTACCAUT

Acordare autorizare cod acces

GRTUSRPMN

Acordare permisiune utilizator

MOVDOC³

Mutare document

MRGDOC³

Combinare document

PAGDOC

Paginare document

QHFCHGAT

API-ul de modificare atribute intrare director

QHFSETSZ

API-ul de setare dimensiune fișier flux

QHFWRTSF

API-ul de scriere fișier flux

QRYDOCLIB³

Cerere bibliotecă documente

Notă: O intrare de modificare este scrisă dacă un document existent rezultat dintr-o căutare este înlocuit.

RCVDST³

Primire distribuție

RGZDLO

Reorganizare DLO

3. O intrare de modificare este scrisă pentru document și pentru folder dacă destinația operației este într-un folder.

- RMVACC**
Înlăturare cod acces pentru orice DLO la care este atașat codul de acces
- RMVDLOAUT**
Înlăturare autorizare DLO
- RNMDLO**³
Redenumire DLO
- RPLDOC**
Înlocuire document
- RSTDLO**³
Restaurare DLO
- RSTSHF**
Restaurare raft de cărți
- RTVDOC**
Extragere document (verificare)
- RVKACCAUT**
Revocare autorizare cod acces
- RVKUSRPMN**
Revocare permisiune utilizator
- SAVDLO**³
Salvare DLO
- Operațiile care nu sunt auditate
- ADDACC**
Adăugare cod acces
- DSPACC**
Afișare cod acces
- DSPUSRPMN**
Afișare permisiune utilizator
- QHFCHGFP**
API-ul de modificare cursor fișier
- QHFCLODR**
API-ul de închidere director
- QHFCLOSF**
API-ul de închidere fișier flux
- QHFFRCSE**
API-ul de forțare date din buffer
- QHFLULSF**
API-ul de blocare/deblocare interval fișier flux
- QHFRVAT**
API-ul de extragere atribute intrare director
- RCLDLO**
Revendicare DLO (*ALL sau *INT)
- WRKDOCLIB**
Gestionare biblioteci de documente
- WRKDOCPRTQ**
Gestionare coadă de tipărire documente

Auditare obiect

Operațiile pentru zonă de date (*DTAARA):

- Operație de citire

DSPDTAARA

Afișare zonă de date

RCVDTAARA

Primire zonă de date (comanda S/38)

RTVDTAARA

Extragere zonă de date

QWCRDTAA

API-ul de extragere zonă de date

- Operație de modificare

CHGDTAARA

Modificare zonă de date

SNDDTAARA

Trimitere zonă de date

- Operațiile care nu sunt auditate

Zone de date

Zonă de date locală, Zonă de date grup, Zonă de date PIP (Parametrul de inițializare program)

WRKDTAARA

Gestionare zonă de date

Operațiile pentru utilizatorul Interactive Data Definition (*DTADCT):

- Operație de citire

Nimic

- Operație de modificare

Creare Dicționar de date și definiții de date

Modificare

Dicționar de date și definiții de date

Copiere

Definiții de date (înregistrate cu creare)

Ștergere

Dicționar de date și definiții de date

Redenumire

Definiții de date

- Operațiile care nu sunt auditate

Afișare

Dicționar de date și definiții de date

LNKDTADFN

Legarea și dezlegarea definițiilor de fișier

Tipărire

Dicționar de date, definiții de date și informații loc-folosire pentru definițiile de date

Operațiile pentru coada de date (*DTAQ):

- Operație de citire

QMHRDQM

API-ul de extragere mesaje din coada de date

- Operație de modificare

QRCVDTAQ

API-ul de primire coadă de date

QSNDDTAQ

API-ul de trimitere coadă de date

QCLRDTAQ

API-ul de curățare coadă de date

- Operațiile care nu sunt auditate

WRKDTAQ

Gestionare coadă de date

QMHQRDQD

API-ul de extragere descrieri din coada de date

Operații pentru descrieri editare (*EDTD):

- Operație de citire

DSPEDTD

Afișare descriere editare

QECCVTEC

API-ul de editare expansiune cod (prin rutina QECEDITU)

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

WRKEDTD

Gestionare descrieri editare

QECEDT

API-ul de editare

QECCVTEW

API pentru translatarea Lucru editare în Mască editare

Operații pentru înregistrare ieșire (*EXITRG):

- Operație de citire

QUSRTVEI

API-ul Extragere informații ieșire

QusRetrieveExitInformation

API-ul Extragere informații ieșire

- Operație de modificare

ADDEXITPGM

Adăugare program ieșire

QUSADDEP

API-ul de adăugare program ieșire

QusAddExitProgram

API-ul de adăugare program ieșire

QUSDRGPT

API-ul de anulare înregistrare punct de ieșire

Auditare obiect

QusDeregisterExitPoint

API-ul de anulare înregistrare punct de ieșire

QUSRGPT

API-ul de înregistrare punct de ieșire

QusRegisterExitPoint

API-ul de înregistrare punct de ieșire

QUSRMVEP

API-ul de înlăturare program ieșire

QusRemoveExitProgram

API-ul de înlăturare program ieșire

RMVEXITPGM

Înlăturare program ieșire

WRKREGINF

Gestionare informații de înregistrare

- Operațiile care nu sunt auditate

Nimic

Operații pentru tabela de control formulare (*FCT):

- Nici o operație de citire sau modificare nu este auditată pentru tipul de obiect *FCT.

Operații pentru fișier (*FILE):

- Operație de citire

CPYF Copiere fișier (folosește operația deschidere)

Deschidere

Deschide un fișier pentru citire

DSPPFM

Afișare membru fișier fizic (folosește operația deschidere)

Deschidere

Deschidere MRT-uri după deschiderea inițială

CRTBSCF

Creare fișier BSC (folosește operația deschidere)

CRTC MNF

Creare fișier comunicații (folosește operația deschidere)

CRTDSPF

Creare fișier de afișare (folosește operația deschidere)

CRTICFF

Creare fișier ICF (folosește operația deschidere)

CRTMXDF

Creare fișier MXD (folosește operația deschidere)

CRTPRTF

Creare fișier imprimantă (folosește operația deschidere)

CRTPF

Creare fișier fizic (folosește operația deschidere)

CRTL F

Creare fișier logic (folosește operația deschidere)

DSPMODSRC

Afișare sursă modul (folosește operația deschidere)

STRDBG

Pornire depanare (folosește operația deschidere)

QTEDBGS

API-ul de extragere text de vizualizare

- Operație de modificare

Deschidere

Deschide un fișier pentru modificare

ADDBSCDEVE

(S/38E) Adăugare intrare dispozitiv Bisync unui fișier dispozitiv mixt

ADDCMNDEVE

(S/38E) Adăugare intrare dispozitiv de comunicații unui fișier dispozitiv mixt

ADDDSPDEVE

(S/38E) Adăugare intrare dispozitiv de afișare unui fișier dispozitiv mixt

ADDICFDEVE

(S/38E) Adăugare intrare dispozitiv ICF unui fișier dispozitiv mixt

ADDLFM

Adăugare membru fișier logic

ADDPFCST

Adăugare constrângere fișier fizic

ADDPFM

Adăugare membru fișier fizic

ADDPFTRG

Adăugare declanșator fișier fizic

ADDPFVLM

Adăugare membru de lungime variabilă fișier fizic

APYJRNCHGX

Aplicare extindere modificări jurnal

CHGBSCF

Funcția de modificare Bisync

CHGCMNF

(S/38E) Modificare fișier de comunicații

CHGDDMF

Modificare fișier DDM

CHGDKTF

Modificare fișier dischetă

CHGDSPF

Modificare fișier de afișare

CHGICFDEVE

Modificare intrare fișier dispozitiv ICF

CHGICFF

Modificare fișier ICF

CHGMXDF

(S/38E) Modificare fișier dispozitiv mixt

Auditare obiect

CHGLF

Modificare fișier logic

CHGLFM

Modificare membru fișier logic

CHGPF

Modificare fișier fizic

CHGPFCST

Modificare constrângere fișier fizic

CHGPFM

Modificare membru fișier fizic

CHGPRTF

Modificare fișier imprimantă GQle

CHGSAVF

Modificare fișier salvare

CHGS36PRCA

Modificare attribute procedură S/36

CHGS36SRCA

Modificare attribute sursă S/36

CHGTAPF

Modificare fișier bandă

CLRPFM

Curățare membru fișier fizic

CPYF

Copiere fișier (deschidere fișier pentru modificare, precum adăugare de înregistrări, curățare membru sau salvare membru)

EDTS36PRCA

Editare attribute procedură S/36

EDTS36SRCA

Editare attribute sursă S/36

INZPFM

Inițializare membru fișier fizic

JRNAP

(S/38E) Pornire cale de acces jurnal (intrare per fișier)

JRNPF

(S/38E) Pornire fișier fizic jurnal (intrare per fișier)

RGZPFM

Reorganizare membru fișier fizic

RMVBSCDEVE

(S/38E) Înlăturare intrare dispozitiv BSC dintr-un fișier dev mixt

RMVCMNDEVE

(S/38E) Înlăturare intrare dispozitiv CMN dintr-un fișier dev mixt

RMVDSPDEVE

(S/38E) Înlăturare intrare dispozitiv DSP dintr-un fișier dev mixt

RMVICFDEVE

(S/38E) Înlăturare intrare dispozitiv ICF dintr-un fișier dev ICM

RMVM

Înlăturare membru

RMVPCST

Înlăturare constrângere fișier fizic

RMVPFTGR

Înlăturare declanșator fișier fizic

RNMM

Redenumire membru

WRKS36PRCA

Gestionare attribute procedură System/36

WRKS36SRCA

Gestionare attribute sursă System/36

- Operațiile care nu sunt auditate

DSPCPCST

Afișare constrângeri de verificare în așteptare

DSPFD

Afișare descriere fișier

DSPFFD

Afișare descriere câmp fișier

DSPDBR

Afișare relații bază de date

DSPPGMREF

Afișare referințe program fișier

EDTCPCST

Editare constrângeri de verificare în așteptare

OVRxxx

Înlocuire fișier

RTVMBRD

Extragere descriere membru

WRKPCST

Gestionare constrângeri fișier fizic

WRKF

Gestionare fișier

Operații pentru fișierele primul intrat primul ieșit (*FIFO):

- Vedeți Operații pentru fișier flux (*STMF) pentru auditare *FIFO.

Operații pentru folder (*FLR):

- Vedeți operații pentru obiect bibliotecă documente (*DOC sau *FLR)

Operații pentru Resursă font (*FNTRSC):

- Operație de citire

Tipărire

Tipărirea unui fișier spool care referă la o resursă font

- Operație de modificare

Nimic

Auditare obiect

- Operațiile care nu sunt auditate

WRKFNTRSC

Gestionare resurse font

Tipărire

Referirea la resursa font la crearea unui fișier spool

Operații pentru definiția de formular (*FORMDF):

- Operație de citire

Tipărire

Tipărirea unui fișier spool care referă la o definiție de formular

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

WRKFORMDF

Gestionare definiții de formular

Tipărire

Referirea la definiția de formular la crearea unui fișier spool

Operațiile pentru obiectul filtrare (*FTR):

- Operație de citire

Nimic

- Operație de modificare

ADDALRACNE

Adăugare intrare acțiune alertă

ADDALRSLTE

Adăugare intrare selecție alertă

ADDPRBACNE

Adăugare intrare acțiune problemă

ADDPRBSLTE

Adăugare intrare selecție problemă

CHGALRACNE

Modificare intrare acțiune alertă

CHGALRSLTE

Modificare intrare selecție alertă

CHGPRBACNE

Modificare intrare acțiune problemă

CHGPRBSLTE

Modificare intrare selecție problemă

CHGFTR

Modificare filtru

RMVFTRACNE

Înlăturare intrare acțiune filtru

RMVFTRSLTE

Înlăturare intrare selecție alertă

WRKFTRACNE

Gestionare intrări acțiune filtru

WRKFTRSLTE

Gestionare intrări selecție filtru

- Operațiile care nu sunt auditate

WRKFTR

Gestionare filtre

WRKFTRACNE

Gestionare intrări acțiune filtru

WRKFTRSLTE

Gestionare intrări selecție filtru

Operațiile cu setul de simboluri grafice (*GSS):

- Operație de citire

Încărcat

Când este încărcat

Font Când este folosit ca font dintr-o imprimantă descrisă extern

- Operație de modificare

Nimic.

- Operațiile care nu sunt auditate

WRKGSS

Gestionare setul de simboluri grafice

Operații pentru dicționarul set de caractere pe doi octeți (*IGCDCT):

- Operație de citire

DSPIGCDCT

Afișare dicționar IGC

- Operație de modificare

EDTIGCDCT

Editare dicționar IGC

Operații pentru sortare set de caractere pe doi octeți (*IGCSRT):

- Operație de citire

CPYIGCSRT

Copiere sortare IGC (*din-obiectul-IGCSRT*)

Conversie

Conversia la formatul V3R1, dacă este necesar

Tipărire

Tipărire caracter pentru înregistrarea în tabela de sortare (opțiunea 1 din meniul CGU)

Tipăriți înainte de a șterge caracterul din tabela de sortare (opțiunea 2 din meniul CGU)

- Operație de modificare

CPYIGCSRT

Copiere sortare IGC (*la-obiectul-IGCSRT*)

Conversie

Conversia la formatul V3R1, dacă este necesar

Auditare obiect

Creare Crearea unui caracter definit de utilizator (opțiune 1 din meniul CGU)

Ștergere

Ștergerea unui caracter definit de utilizator (opțiune 2 din meniul CGU)

Actualizare

Actualizare tabelă de sortare activă (opțiunea 5 din meniul CGU)

- Operațiile care nu sunt auditate

FMTDTA

Sortare înregistrări sau câmpuri dintr-un fișier

Operații pentru tabela set de caractere pe doi octeți (*IGCTBL):

- Operație de citire

CPYIGCTBL

Copiere tabelă IGC

STRFMA

Pornire ajutor gestiune fonturi

- Operație de modificare

STRFMA

Pornire ajutor gestiune fonturi

- Operațiile care nu sunt auditate

CHKIGCTBL

Verificare tabelă IGC

Operații pentru descriere job (*JOB):

- Operație de citire

Nimic

- Operație de modificare

CHGJOB

Modificare descriere job

- Operațiile care nu sunt auditate

DSPJOB

Afișare descriere job

WRKJOB

Gestionare descrieri de job

QWDRJOB

API-ul de extragere descriere job

Job batch

Când este folosit pentru a stabili un job

Operații pentru coada de joburi (*JOBQ):

- Operație de citire

Nimic

- Operație de modificare

Intrare

Când o intrare este plasată sau îndepărtată din coadă

CLRJOBQ

Curățare coadă joburi

- HLDJOBQ**
Blocare coadă joburi
- RLSJOBQ**
Eliberare coadă joburi
- Operațiile care nu sunt auditate
 - ADDJOBQE “Descrierile de subsistem” la pagina 181**
Adăugare intrare coadă joburi
 - CHGJOB**
Modificare job dintr-un JOBQ în alt JOBQ
 - CHGJOBQE “Descrierile de subsistem” la pagina 181**
Modificare intrare coadă joburi
 - QSPRJOBQ**
Extragere informații coadă joburi
 - RMVJOBQE “Descrierile de subsistem” la pagina 181**
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

Operațiile pentru obiectul de planificare job (*JOBSCD):

- Operație de citire
 - Nimic**
- Operație 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
- Operațiile care nu sunt auditate
 - Afișare**
Afișare detalii intrare job planificat
 - WRKJOBSCDE**
Gestionare intrări planificare job

4. O înregistrare de auditare este scrisă dacă este specificată o auditare de obiect pentru descrierea subsistem (*SBSD).

Auditare obiect

Gestionare ...

Gestionare joburi lansate anterior din intrarea de planificare job

QWCLSCDE

API-ul de listare intrare planificare job

Operații pentru jurnal (*JRN):

- Operație de citire

CMPJRNIMG

Comparație imagini jurnal

DSPJRN

Afișare intrare jurnal pentru jurnale utilizator

QJORJIDI

Extragere informații de identificator jurnal (JID)

QjoRetrieveJournalEntries

Extragere intrări jurnal

RCVJRNE

Primire intrare jurnal

RTVJRNE

Extragere intrare jurnal

- Operație de modificare

ADDRMTJRN

Adăugare jurnal la distanță

APYJRNCHG

Aplicare modificări jurnalizate

APYJRNCHGX

Aplicare extindere modificări jurnal

CHGJRN

Modificare jurnal

CHGRMTJRN

Modificare jurnal la distanță

ENDJRNxxx

Terminare jurnalizare

JRNAP

(S/38E) Pornire cale acces jurnal

JRNPF

(S/38E) Pornire fișier fizic jurnal

QjoAddRemoteJournal

API-ul de adăugare jurnal la distanță

QjoChangeJournalState

API-ul de modificare stare jurnal

QjoEndJournal

API-ul de terminare jurnalizare

QjoRemoveRemoteJournal

API-ul de înlăturare jurnal la distanță

QJOSJRNE

API-ul trimitere intrare jurnal (intrări utilizator doar prin API-ul QJOSJRNE)

QjoStartJournal

API-ul Pornire jurnalizare

RMVJRNCHG

Înlăturare schimbări jurnalizate

RMVRMTJRN

Înlătuare jurnal la distanță

SNDJRNE

Trimitere intrare jurnal (intrări utilizator doar prin comanda SNDJRNE)

STRJRNxxx

Pornire jurnalizare

- Operațiile care nu sunt auditate

DSPJRN

Afișare intrare jurnal pentru jurnalele sistem interne, JRN(*INTSYSJRN)

DSPJRNA

(S/38E) Gestionare atribute jurnal

DSPJRNMNU

(S/38E) Gestionare jurnal

QjoRetrieveJournalInformation

API-ul de extragere informații jurnal

WRKJRN

Gestionare jurnal (DSPJRNMNU în mediu S/38)

WRKJRNA

Gestionare atribute jurnal (DSPJRNA în mediu S/38)

Operații pentru Receptorul jurnal (*JRNRCV):

- Operație de citire

Nimic

- Operație de modificare

CHGJRN

Modificare jurnal (când se atașează noi receptoare)

- Operațiile care nu sunt auditate

DSPJRNRCVA

Afișare atribute receptor jurnal

QjoRtvJrnReceiverInformation

API-ul de extragere informații receptor jurnal

WRKJRNRCV

Gestionare receptor jurnal

Operații pentru bibliotecă (*LIB):

- Operație de citire

DSPLIB

Afișare bibliotecă (când nu este goală). Dacă bibliotecă este goală, nu este executată nici o auditare.)

Localizare

Când un dispozitiv este adăugat la o tabelă de configurație

Auditare obiect

Note:

1. Câteva intrări de auditare pot să fi fost scrise pentru o bibliotecă pentru o singură comandă. De exemplu, când deschideți un fișier, este scrisă o intrare jurnal de auditare ZR pentru bibliotecă atunci când sistemul localizează fișierul și fiecare membru din fișier.
2. Nu este scrisă nici o intrare de auditare dacă funcția de localizare nu are succes. De exemplu, rulați o comandă folosind un parametru generic precum:

```
DSP0BJD OBJ(AR/WRK*) OBJTYPE(*FILE)
```

Dacă o bibliotecă numită "AR" nu conține nume de fișiere care încep cu "WRK", nu este scrisă nici o înregistrare de auditare pentru acea bibliotecă.

Listă de biblioteci

Adăugare bibliotecă la lista de biblioteci

- Operație de modificare

CHGLIB

Modificare bibliotecă

CLRLIB

Curățare bibliotecă

MOVOBJ

Mutare obiect

RNMOBJ

Redenumire obiect

Adăugare

Adăugare obiect la bibliotecă

Ștergere

Ștergere obiect din bibliotecă

- Operațiile care nu sunt auditate

Nimic

Operații pentru descrierea de linie (*LIND):

- Operație de citire

SAVCFG

Salvare configurație

RUNLPDA

Rulare comenzi operaționale LPDA-2

VFYCMN

Test legătură

VFYLNKLPDA

Test legătură LPDA-2

- Operație de modificare

CHGLINxxx

Modificare descriere linie

VRYCFG

Activare/dezactivare descriere de linie

- Operațiile care nu sunt auditate

ANSLIN

Linie răspuns

Copiere

Opțiunea 3 din WRKLIND

DSPLIND

Afișare descriere de linie

ENDLINRCY

Terminare recuperare linie

RLSCMNDEV

Eliberare dispozitiv comunicații

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

Operațiile pentru serviciile de mail:

Notă: Acțiunile servicii mail sunt auditate dacă valoarea de sistem acțiune de auditare (QAUDLVL) sau parametrul de auditare acțiune (AUDLVL) din profilul utilizator include *OFCSR.V.

- Operațiile care sunt auditate

Modificare

Modificările aduse directorului de distribuție sistem

În numele

Lucrul în numele altui utilizator

Notă: Lucrul în numele altui utilizator este auditat dacă AUDLVL din profilul utilizator sau valoarea sistem QAUDLVL include *SECURITY.

Deschidere

Este scrisă o înregistrare de auditare când istoricul de mail este deschis

- Operațiile care nu sunt auditate

Modificare

Modificare detalii pentru un element de mail

Ștergere

Ștergere element de mail

Disponere

Disponere 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

Auditare obiect

Notă: Tipărirea de elemente mail poate fi auditată folosind nivelul de auditare *SPLFDTA sau *PRTDTA.

Primire

Primire element mail

Răspuns

Răspuns unui element mail

Trimitere

Trimitere element mail

Vizualizare

Vizualizare element mail

Operații pentru meniu (*MENU):

- Operație de citire

Afișare

Afișarea unui meniu cu comanda GO MENU sau cu comanda din caseta de dialog UIM

- Operație de modificare

CHGMNU

Modificare meniu

- Operațiile care nu sunt auditate

Întoarcerea

Întoarcerea la un meniu din stiva de meniuri care a fost deja afișată

DSPMNUA

Afișare atribute meniu

WRKMNU

Lucru cu meniu

Operații pentru descriere mod (*MODD):

- Operație de citire

Nimic

- Operație de modificare

CHGMODD

Modificare descriere mod

- Operațiile care nu sunt auditate

CHGSSNMAX

Modificare maxim sesiuni

DSPMODD

Afișare descriere mod

ENDMOD

Terminare mod

STRMOD

Pornire mod

WRKMODD

Gestionare descrieri mod

Operații pentru obiectul modul (*MODULE):

- Operație de citire

CRTPGM

O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi CRTPGM

CRTSRVPGM

O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi CRTSRVPGM

UPDPGM

O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi UPDPGM

UPDSRVPGM

O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi UPDSRVPGM

- Operație de modificare

CHGMOD

Modificare modul

- Operațiile care nu sunt auditate

DSPMOD

Afișare modul

RTVBNSRC

Extragere sursă legătură

WRKMOD

Gestionare module

Operații pentru fișier de mesaje (*MSGF):

- Operație de citire

DSPMSGD

Afișare descriere mesaj

MRGMSGF

Fișier sursă combinare fișiere de mesaje

Tipărire

Tipărire descriere mesaj

RTVMSG

Extragere informații dintr-un fișier de mesaje

QMHRTVM

API-ul de extragere mesaj

WRKMSGD

Gestionare descriere de mesaj

- Operație de modificare

ADDMSGD

Adăugare descriere mesaj

CHGMSGD

Modificare descriere mesaj

CHGMSGF

Modificare fișier de mesaje

MRGMSGF

Combinare fișier de mesaje (fișier-destinație și înlocuire MSGF)

RMVMSGD

Înlăturare descriere mesaj

- Operațiile care nu sunt auditate

Auditare obiect

OVRMSGF

Înlocuire fișier de mesaje

WRKMSGF

Gestionare fișiere de mesaje

QMHRMFAT

API-ul de extragere atribute fișier de mesaje

Operații pentru coada de mesaje (*MSGQ):

- Operație de citire

QMHLSTM

API-ul de listare mesaje nonprogram

QMHRMQAT

API-ul de extragere atribute coadă de mesaje nonprogram

DSPLOG

Afișare istoric

DSPMSG

Afișare mesaj

Tipărire

Tipărire mesaje

RCVMSG

Primire mesaj RMV(*NO)

QMHRMVM

API-ul de primire mesaje nonprogram când acțiunea de mesaj nu este *REMOVE.

- Operație de modificare

CHGMSGQ

Modificare coadă de mesaje

CLRMSGQ

Curățare coadă de mesaje

RCVMSG

Primire mesaj RMV(*YES)

QMHRMVM

API-ul de primire mesaje nonprogram când acțiunea 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

- Operațiile care nu sunt auditate

WRKMSGQ

Gestionare cozi de mesaje

Programare

Programare operații coadă de mesaje

Operații pentru grupul de noduri (*NODGRP):

- Operație de citire

DSPNODGRP

Afișare grup de noduri

- Operație de modificare

CHGNODGRPA

Modificare grup de noduri

Operațiile pentru lista de noduri (*NODL):

- Operație de citire

QFVLSTNL

Listare intrări listă de noduri

- Operație de modificare

ADDNODLE

Adăugare intrare listă de noduri

RMVNODLE

Înlăturare intrare listă de noduri

- Operațiile care nu sunt auditate

WRKNODL

Gestionare listă de noduri

WRKNODLE

Gestionare intrări listă de noduri

Operații pentru descriere NetBIOS (*NTBD):

- Operație de citire

SAVCFG

Salvare configurație

- Operație de modificare

CHGNTBD

Modificare descriere NetBIOS

- Operațiile care nu sunt auditate

Copiere

Opțiunea 3 din WRKNTBD

DSPNTBD

Afișare descriere NetBIOS

Auditare obiect

RTVCFGSRC

Extragere sursă de configurație pentru descrierea NetBIOS

WRKNTBD

Gestionare descriere NetBIOS

Operații pentru interfața de rețea (*NWID):

- Operație de citire

SAVCFG

Salvare configurație

- Operație de modificare

CHGNWIISDN

Modificare descriere interfață de rețea

VRYCFG

Activare sau dezactivare descriere interfață de rețea

- Operațiile care nu sunt auditate

Copiere

Opțiunea 3 din WRKNWID

DSPNWID

Afișare descriere interfață de rețea

ENDNWIRCY

Terminare recuperare interfață de rețea

RSMNWIRCY

Reluare recuperare interfață de rețea

RTVCFGSRC

Extragere descriere interfață de rețea

RTVCFGSTS

Extragere stare descriere interfață de rețea

WRKNWID

Gestionare descriere interfață de rețea

WRKCFGSTS

Gestionare stare descriere interfață de rețea

Operații pentru descrierea server de rețea (*NWSD):

- Operație de citire

SAVCFG

Salvare configurație

- Operație de modificare

CHGNWSD

Modificare descriere server de rețea

VRYCFG

Modificare configurație

- Operațiile care nu sunt auditate

Copiere

Opțiunea 3 din WRKNWSD

DSPNWSD

Afișare descriere server de rețea

RTVCFGSRC

Extragere sursă de configurație pentru *NWSD

RTVCFGSTS

Extragere stare de configurație pentru *NWSD

WRKNWSD

Gestionare descriere server de rețea

Operații pentru coada de ieșire (*OUTQ):

- Operație de citire

STRPRTWTR

Pornire scriitor imprimantă la o coadă de ieșire

STRMTWTR

Pornire scriitor la distanță la o coadă de ieșire

- Operație de modificare

Plasare

Când o intrare este plasată sau îndepărtată din coadă

CHGOUTQ

Modificare coadă de ieșire

CHGSPLFA⁵

Modificați atributele fișierului spool, dacă este mutat într-o coadă de ieșire diferită sau dacă coada de ieșire este auditată

CLROUTQ

Curățare coadă de ieșire

DLTSPLF⁵

Ștergere fișier spool

HLDOUTQ

Reținere coadă de ieșire

RLSOUTQ

Eliberare coadă de ieșire

- Operațiile care nu sunt auditate

CHGSPLFA⁵

Modificare atribute fișier spool

CPYSPLF⁵

Copiere fișier spool

Creare⁵

Creare fișier spool

DSPSPLF⁵

Afișare fișier spool

HLDSPLF⁵

Reținere fișier spool

QSPROUTQ

Extragere informații coadă de ieșire

5. Aceasta este de asemenea auditată dacă auditarea de acțiuni (valoarea sistem QAUDLVL sau valoarea profil utilizator AUDLVL) include *SPLFDA.

Auditare obiect

RLSSPLF ⁵

Eliberare fișier spool

SNDNETSPLF ⁵

Trimitere fișier spool rețea

WRKOUTQ

Gestionare coadă de ieșire

WRKOUTQD

Gestionare descriere coadă de ieșire

WRKSPLF

Gestionare fișier spool

WRKSPLFA

Gestionare atribute fișier spool

Operații pentru suprapunere (*OVL):

- Operație de citire

Tipărire

Tipărire fișier spool care referă o suprapunere

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

WRKOVL

Gestionare suprapuneri

Tipărire

Referirea la suprapunere când se creează un fișier spool

Operații pentru definiția de pagină (*PAGDFN):

- Operație de citire

Tipărire

Tipărirea unui fișier spool care referă la o definiție de pagină

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

WRKPAGDFN

Gestionare definiții de pagină

Tipărire

Referirea la definiția de formular la crearea unui fișier spool

Operații pentru segment de pagină (*PAGSEG):

- Operație de citire

Tipărire

Tipărirea unui fișier spool care referă la un segment de pagină

- Operație de modificare

Nimic

- Operațiile care nu sunt auditate

WRKPAGSEG

Gestionare segmente de pagină

Tipărire

Referirea la segmentul de pagină la crearea unui fișier spool

Operații pentru grupul de descriptori tipărire (*PDG):

- Operație de citire

Deschidere

Când grupul de descriptori tipărire este deschis pentru citire de către un API PrintManager sau verb CPI.

- Operație de modificare

Deschidere

Când grupul de descriptori tipărire este deschis pentru modificare de către un API PrintManager* sau verb CPI.

- Operațiile care nu sunt auditate

CHGPDGPRF

Modificare profil grup de descriptori tipărire

WRKPDG

Gestionare grup de descriptori tipărire

Operații pentru program (*PGM):

- Operație de citire

Activare

Activare program

Apel Apelare program care nu este deja activat

ADDPGM

Adăugare program pentru depanare

QTEDBGS

API-ul de înregistrare vizualizare depanare Qte

QTEDBGS

API-ul de extragere vederi modul Qte

// **RUN** Rulare program în mediu S/36

RTVCLSRC

Extragere sursă CL

STRDBG

Pornire depanare

- Creare operație

CRTPGM

Creare program

UPDPGM

Actualizare program

- Operație de modificare

CHGCSPPGM

Modificare program CSP/AE

CHGPGM

Modificare program

CHGS36PGMA

Modificare attribute program System/36

Auditare obiect

EDTS36PGMA

Editare atribute program System/36

WRKS36PGMA

Gestionare atribute program System/36

- Operațiile care nu sunt auditate

ANZPGM

Analiză program

DMPCLPGM

Abandon program CL

DSPCSPOBJ

Afișare obiect CSP

DSPPGM

Afișare program

PRTCMDUSG

Tipărire folosire comandă

PRTCSPAPP

Tipărire aplicație CSP/AE

PRTSQLINF

Tipărire informații SQL

QBNLPGMI

API-ul de listare informații program

QCLRPGMI

API-ul de extragere informații program

STRCSP

Pornire utilitare CSP

TRCCSP

Urmărire aplicație CSP

WRKOBJCSP

Gestionare obiecte pentru CSP

WRKPGM

Gestionare programe

Operații pentru Panoul de grup (*PNLGRP):

- Operație citire

ADDSCHIDX

Adăugare intrare index de căutare

QUIOPNDA

Deschidere Grup panouri pentru API-ul de afișare

QUIOPNPA

Deschidere Grup panouri pentru API-ul de afișare

QUHDSPH

API de afișare ajutor

- Operația de modificare

Nimic

- Operațiile care nu sunt auditate

WRKPNLGRP

Gestionare grupuri de panouri

Operațiile pentru Disponibilitatea produsului (*PRDAVL):

- Operația de modificare

WRKSPTPRD

Gestionare produse suportate, când este adăugat sau înlăturat suportul

- Operațiile care nu sunt auditate

Citire Nici o operație de citire nu este auditată

Operațiile pentru Definiția de produs (*PRDDFN):

- Operația de modificare

ADDPRDLICI

Adăugare informații de licență produs

WRKSPTPRD

Gestionare produse suportate, când este adăugat sau înlăturat suportul

- Operațiile care nu sunt auditate

Citire Nici o operație de citire nu este auditată

Operații pentru Încărcarea de produse (*PRDLOD):

- Operația de modificare

Modificare

Stare de încărcare produs, listă de biblioteci pentru încărcare produs, listă directoare pentru încărcare produs, limbă principală

- Operațiile care nu sunt auditate

Citire Nici o operație de citire nu este auditată

Operații pentru Formular Query Manager (*QMFORM):

- Operație citire

STRQMORY

Pornire cerere Query Management

RTVQMFORM

Extragere formular Query Management

Rulare Rulare cerere

Exportare

Exportare formular Query Management

Tipărire

Tipărire formular Query Management

Tipărire formular Query Management folosind formularul

Folosire

Accesarea formularului folosind opțiunea 2, 5, 6, sau 9 sau funcția F13 din DB2 UDB pentru iSeries Query Manger și SQL Development Kit.

- Operația de modificare

CRTQMFORM

Creare formular Query Management

Auditare obiect

IMPORTARE

Importare formular Query Management

Salvare

Salvare formular folosind o opțiune meniul sau o comandă

Copiere

Opțiunea 3 din funcția Gestionare formulare Query Manager

- Operațiile care nu sunt auditate

Gestionare

Când sunt menționate *QMFORM-urile în ecranul Gestionare

Activ Orice operație formular care este făcută pentru formularul 'activ'.

Operații pentru Cerere Query Manager (*QMQRV):

- Operație citire

RTVQMQRV

Extragere cerere Query Management

Rulare Rulare cerere Query Manager

STRQMQRV

Pornire cerere Query Manager

Exportare

Exportare cerere Query Manager

Tipărire

Tipărire cerere Query Manager

Folosire

Accesați cererea folosind funcția F13 sau opțiunea 2, 5, 6 sau 9 din funcția Gestionare cereri Query Manager

- Operația de modificare

CRTQMQRV

Creare cerere Query Management

Convertire

Opțiunea 10 (Convertire la SQL) din funcția Gestionare cereri Query Manager

Copiere

Opțiunea 3 din funcția Gestionare cereri Query Manager

Salvare

Salvare cerere folosind un meniu sau comandă

- Operațiile care nu sunt auditate

Gestionare

Când sunt menționate *QMQRV-urile în ecranul Gestionare

Active Orice operație cerere care este făcută pentru cererea 'activă'.

Operațiile pentru Definiția cerere (*QRYDFN):

- Operație citire

ANZQRY

Analiză cerere

Modificare

Modificare cerere folosind un ecran prompt prezentat de WRKQRY sau QRY.

Afișare

Afișare cerere folosind ecranul prompt WRKQRY

Exportare

Exportare formular folosind Query Manager

Exportare

Exportare cerere folosind Query Manager

Tipărire

Tipărire definiție 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

RTVQMORY

Extragere cerere Query Management

Rulare Rulare cerere folosind ecranul prompt WRKQRY

Rulare (comanda Query Management)

RUNQRY

Rulare cerere

STRQMORY

Pornire cerere Query Management

Lansare

Lansare cerere (rulare cerere) în batch folosind ecranul prompt WRKQRY sau sau ecranul Ieșire cerere curentă

- Operația de modificare

Modificare

Salvare cerere modificată folosind programul cu licență Query/400

- Operațiile care nu sunt auditate

Copiere

Copiați o cerere folosind opțiunea 3 din ecranul “Gestionare cereri”

Creare Creați o cerere folosind opțiunea 1 din ecranul “Gestionare cereri”

Ștergere

Ștergeți o cerere folosind opțiunea 4 din ecranul “Gestionare cereri”

Rulare Rulați o cerere folosind opțiunea 1 din ecranul “Ieșire cerere curentă” când creați sau modificați o cerere folosind programul cu licență Query/400; Rulați o cerere interactiv folosind PF5 când creați, afișați sau modificați o cerere folosind programul cu licență Query/400

DLTQRY

Ștergere cerere

Operații pentru Tabela de translație cod referință (*RCT):

- Operație citire

Nimic

Auditare obiect

- Operația de modificare

Nimic

- Operațiile care nu sunt auditate

Nimic

Operații pentru Lista de răspuns:

Notă: Acțiunile listei de răspuns sunt auditate dacă valoarea sistem de auditare acțiune (QAUDLVL) sau parametrul de auditare acțiune (AUDLVL) din profilul utilizator includ *SYSMGT.

- Operațiile care sunt auditate

ADDRPYLE

Adăugare intrare listă răspuns

CHGRPYLE

Modificare intrare listă răspuns

RMVRPYLE

Înlăturare intrare listă răspuns

WRKRPYLE

Gestionare intrări listă răspuns sistem

- Operațiile care nu sunt auditate

Nimic

Operații pentru descrierea subsistem (*SBSD):

- Operație citire

ENDSBS

Terminare subsistem

STRSBS

Pornire subsistem

- Operația de modificare

ADDAJE

Adăugare intrare job autostart

ADDCMNE

Adăugare intrare comunicații

ADDJOBQE

Adăugare intrare coadă joburi

ADDPJE

Adăugare intrare job prestart

ADDRTGE

Adăugare intrare rutare

ADDWSE

Adăugare intrare stație de lucru

CHGAJE

Modificare intrare job autostart

CHGCMNE

Modificare intrare comunicații

CHGJOBQE

Modificare intrare coadă joburi

CHGPJE
Modificare intrare job prestart

CHGRTGE
Modificare intrare rutare

CHGSBSD
Modificare descriere subsistem

CHGWSE
Modificare intrare stație de lucru

RMVAJE
Înlăturare intrare job autostart

RMVCMNE
Înlăturare intrare comunicații

RMVJOBQE
Înlăturare intrare coadă joburi

RMVPJE
Înlăturare intrare job prestart

RMVRTGE
Înlăturare intrare rutare

RMVWSE
Înlăturare intrare stație de lucru

- Operațiile care nu sunt auditate

DSPSBSD
Afișare descriere subsistem

QWCLASBS
API-ul de listare subsistem activ

QWDL SJBQ
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

Operațiile pentru indexul de căutare informații (*SCHIDX):

- Operație citire

STRSCHIDX
Pornire index de căutare

WRKSCHIDX
Gestionare intrare index de căutare

- Operația de modificare (auditată dacă OBJAUD este *CHANGE sau *ALL)

ADDSCHIDX
Adăugare intrare index de căutare

Auditare obiect

CHGSCHIDX

Modificare index de căutare

RMVSCIDX

Înlăturare intrare index de căutare

- Operațiile care nu sunt auditate

WRKSCIDX

Gestionare index de căutare

Operațiile pentru socket-ul local (*SOCKET):

- Operație citire

connect

Legăți o destinație permanentă la un socket și stabiliți o conexiune.

DSPLNK

Afișare legături

givedescriptor

API-ul de acordare acces fișier

Qp01GetPathFromFileID

API-ul de obținere nume cale sau obiect din ID-ul de fișier

Qp01RenameKeep

API-ul Redenumire fișier sau director, păstrare nou

Qp01RenameUnlink

API-ul Redenumire fișier 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

- Operația de modificare

ADDLNK

Adăugare legătură

bind Stabilirea unei adrese locale pentru un socket.

CHGAUD

Auditare modificare

CHGAUT

Modificare autorizare

CHGOWN

Modificare proprietar

CHGPGP

Modificare grup primar

CHKIN

Înregistrare

CHKOUT

Debifare

chmod API-ul Modificare autorizații fișier

chown API-ul Modificare grup și proprietar

givedescriptor

API-ul de acordare acces fișier

link API-ul Creare legătură la fișier**Qp0IRenameKeep**

API-ul Redenumire fișier sau director, păstrare nou

Qp0IRenameUnlink

API-ul Redenumire fișier sau director, dezlegare nou

RMVLNK

Înlăturare legătură

RNM Redenumire**RST** Restaurare**unlink** API-ul Înlăturare legătură la fișier**utime** API-ul de Setare acces fișier și timpi de modificare**WRKAUT**

Gestionare autorizare

WRKLNK

Gestionare legături

- Operațiile care nu sunt auditate

close API-ul de închidere fișier

Notă: Închiderea nu este auditată, dar dacă apare o eșuare de modificare într-un program de ieșire scan_related de închidere, atunci este scrisă o înregistrare de auditare.

DSPAUT

Afișare autorizare

dup API-ul de duplicare descriptor fișier deschis**dup2** API-ul de duplicare descriptor fișier deschis la un alt descriptor**fcntl** API-ul de executare comandă control fișier**fstat** API-ul de obținere informații fișier după descriptor**fsync** API-ul de sincronizare modificări în fișier**ioctl** API-ul executare cerere control I/O**lstat** API-ul de obținere fișier sau informații de legătură**pathconf**

API-ul de obținere variabile nume cale configurabile

read API-ul de citire din fișier**readv** API-ul de citire din fișier (Vector)**select** API-ul de verificare stare I/O a descriptorilor fișier multipli**stat** API-ul de obținere informații fișier**takedescriptor**

API-ul de luare acces fișier

write API-ul de scriere în fișier**writev** API-ul de scriere în fișier (Vector)

Auditare obiect

Operații pentru scriere dicționar ajutor (*SPADCT):

- Operație citire

Verificare

Funcția silabisire verificare

Ajutor Funcția de ajutor silabisire

Despărțire

Funcția de despărțire

Legare Funcția de legare

Sinonime

Funcția sinonim

Bază Folosire dicționar ca bază la crearea unui alt dicționar

Verificare

Folosire ca dicționar de verificare la crearea unui alt dicționar

Extragere

Extragere sursă listă de cuvinte de stop

Tipărire

Tipărire sursă listă de cuvinte de stop

- Operația de modificare

CRTSPADCT

Creare dicționar de adăugare silabisire

- Operațiile care nu sunt auditate

Nimic

Operații pentru Fișierele spool:

Notă: Acțiunile fișierului spool sunt auditate dacă valoarea sistem de auditare a acțiunii (QAUDLVL) sau parametrul de auditare acțiune (AUDLVL) din profilul utilizator include *SPLFDTA.

- Operațiile care sunt auditate

Acces Fiecare acces pentru fiecare utilizator care nu este proprietarul fișierului spool, incluzând:

- CPYSPLF
- DSPSPLF
- SNDNETSPLF
- SNDTCPSPLF
- STRRMTWTR
- API-ul QSPOPNSP

Modificare

Modificarea oricăruia din următoarele atribute fișier spool cu CHGSPLFA:

- COPIES
- DEV
- FORMTYPE
- RESTART
- PAGERANGE
- OUTQ
- DRAWER
- PAGDFN

- | – FORMDF
- | – USRDFNOPT
- | – USRDFNOBJ
- | – USRDFNDTA
- | – EXPDATE
- | – SAVE
- | Modificarea oricăruia din următoarele atribute fișier spool cu CHGSPLFA:

Creare Crearea unui fișier spool folosind operațiile de tipărire

Crearea unui fișier spool folosind API-ul QSPCRTSP

Ștergere

Ștergerea unui fișier spool folosind oricare din următoarele operații:

- | – Tipărirea unui fișier spool de pe o imprimantă sau scriitor de dischetă
- | – Curățarea cozii de ieșire (CLROUTQ)
- | – Ștergerea fișierului spool folosind comanda DLTSPFL sau opțiunea de ștergere dintr-un ecran de fișiere spool
- | – Ștergerea fișierelor spool când un job se termină (ENDJOB SPLFILE(*YES))
- | – Ștergerea de fișiere spool când se termină un job tipărire (ENDPJ SPLFILE(*YES))
- | – Trimiterea unui fișier spool la un sistem la distanță de pe un scriitor la distanță
- | – Ștergerea fișierelor spool care au expirat folosind comanda DLTEXPSPLF
- | – Ștergerea fișierelor spool prin funcția operațională curățare asistată

Reținere

Reținerea unui fișier spool prin oricare din următoarele operații:

- | – Folosirea comenzii HLDSPLF
- | – Folosirea opțiunii de reținere dintr-un ecran cu fișiere spool
- | – Tipărirea unui fișier spool care specifică SAVE(*YES)
- | – Trimiterea unui fișier spool la un sistem la distanță de pe un scriitor la distanță când fișierul spool specifică SAVE(*YES)
- | – Cum reține un scriitor un fișier spool după ce apare o eroare la procesarea fișierului spool

Read Citirea unui fișier spool de pe o imprimantă sau scriitor de dischetă

Eliberare

Eliberarea unui fișier spool

Restaurare

Restaurare fișier spool

Salvare

Salvare fișier spool

Operații pentru pachet SQL (*SQLPKG):

- Operație citire

Rulare Când este rulat obiectul *SQLPKG

- Operația de modificare

Nimic

- Operațiile care nu sunt auditate

PRTSQLINF

Tipărire informații SQL

Auditare obiect

Operații pentru Programul service (*SRVPGM):

- Operație 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 operație

CRTSRVPGM

Creare program service

UPDSRVPGM

Actualizare program service

- Operația de modificare

CHGSRVPGM

Modificare program service

- Operațiile care nu sunt auditate

DSPSRVPGM

Afișare program service

PRTSQLINF

Tipărire informații SQL

QBNLSPGM

API-ul de listare informații de program service

QBNRSPGM

API-ul de extragere informații de program service

WRKSRVPGM

Gestionare programe serviciu

Operații pentru descriere de sesiune (*SSND):

- Nici o operație de citire sau modificare nu este auditată pentru tipul de obiect *SSND.

Operații pentru Spațiul de stocare server (*SVRSTG):

- Nici o operație de citire sau modificare nu este auditată pentru tipul de obiect *SVRSTG.

Operații pentru fișier flux (*STMF):

- Operație citire

CPY Copiere obiect

- DSPLNK**
Afișare legături obiect
- givedescriptor**
API-ul de acordare acces fișier
- MOV** Mutare obiect
- open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
API-uri de deschidere fișier
- SAV** Salvare obiect
- WRKLNK**
Lucru cu legături obiect
- Operația de modificare
- ADDLNK**
Adăugare legătură
- CHGAUD**
Auditare modificare
- CHGAUT**
Modificare autorizare
- CHGOWN**
Modificare proprietar
- CHGPGP**
Modificare grup primar
- CHKIN**
Obiect înregistrat la intrare
- CHKOUT**
Obiect înregistrat la ieșire
- chmod, QlgChmod**
API-uri de modificare autorizări fișier
- chown, QlgChown**
API-uri de modificare proprietar și grup
- CPY** Copiere obiect
- creat, creat64, QlgCreat, QlgCreat64**
API-uri de creare fișier nou sau rescriere fișier existent
- fchmod**
API-ul de modificare autorizări fișier după descriptor
- fchown**
API-ul de modificare grup și proprietar după descriptor
- givedescriptor**
API-ul de acordare acces fișier
- legătură**
API-ul Creare legătură la fișier
- MOV** Mutare obiect
- open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
API-uri la deschiderea pentru scriere

Auditare obiect

Qp0lGetPathFromFileID, QlgGetPathFromFileID

API-uri de obținere nume cale sau obiect din ID-ul de fișier

Qp0lRenameKeep, QlgRenameKeep

API-uri de redenumire fișier sau director, păstrare nou

Qp0lRenameUnlink, QlgRenameUnlink

API-uri Redenumire fișier sau director, dezlegare nou

RMVLNK

Înlăturare legătură

RNM Redenumire obiect

RST Restaurare obiect

unlink, QlgUnlink

API-uri de înlăturare legătură la fișier

utime, QlgUtime

API-uri de Setare acces fișier și timpi de modificare

WRKAUT

Gestionare autorizare

WRKLNK

Gestionare legături

- Operațiile care nu sunt auditate

închidere

API-ul de închidere fișier

DSPAUT

Afișare autorizare

dup API-ul de duplicare descriptor fișier deschis

dup2 API-ul de duplicare descriptor fișier deschis la un alt descriptor

faccessx

Determinați accesibilitate fișier

fclear, fclear64

Curățarea unui fișier

fcntl API-ul de executare comandă control fișier

fpathconf

API-uri de obținere variabile nume cale configurabile

fstat, fstat64

API-uri de obținere informații fișier după descriptor

fsync API-ul de sincronizare modificări în fișier

ftruncate, ftruncate64

API-uri de tăiere fișier

ioctl API-ul executare cerere control I/O

lseek, lseek64

API-uri de setare offset citire/scriere

lstat, lstat64

API-uri de obținere fișier sau informații de legătură

pathconf, QlgPathconf

API-uri de obținere variabile nume cale configurabile

pread, pread64

API-uri de citire din descriptor cu offset

pwrite, pwrite64

API-uri de scriere în descriptor cu offset

read API-ul de citire din fișier

readv API-ul de citire din fișier (Vector)

select API-ul de verificare stare I/O a descriptorilor fișier multipli

stat, stat64, QlgStat, QlgStat64

API-uri de obținere informații fișier

takedescriptor

API-ul de luare acces fișier

write API-ul de scriere în fișier

writev API-ul de scriere în fișier (Vector)

Operații pentru legătura simbolică (*SYMLNK):

- Operație citire

CPY Copiere obiect

DSPLNK

Afișare legături obiect

MOV Mutare obiect

readlink

API-ul de citire valoare a legăturii simbolice

SAV Salvare obiect

WRKLNK

Lucru cu legături obiect

- Operația de modificare

CHGOWN

Modificare proprietar

CHGPGP

Modificare grup primar

CPY Copiere obiect

MOV Mutare obiect

Qp0IRenameKeep, QlgRenameKeep

API-uri de redenumire fișier sau director, păstrare nou

Qp0IRenameUnlink, QlgRenameUnlink

API-uri Redenumire fișier sau director, dezlegare nou

RMVLNK

Înlăturare legătură

RNM Redenumire obiect

RST Restaurare obiect

symlink, QlgSymlink

API-uri realizare legătură simbolică

Auditare obiect

unlink, QlgUnlink

API-uri de înlăturare legătură la fișier

WRKLNK

Lucru cu legături obiect

- Operațiile care nu sunt auditate

Istat, Istat64, QlgLstat, QlgLstat64

API-uri legătură stare

Operații pentru descrierea mașină S/36 (*S36):

- Operație citire

Nimic

- Operația de modificare

CHGS36

Modificare configurație S/36

CHGS36A

Modificare atribute configurație S/36

SET Procedură SET

CRTDEVXXX

Când un dispozitiv este adăugat la o tabelă de configurație

DLTDEVD

Când un dispozitiv este șters dintr-o tabelă de configurație

RNMOBJ

Redenumire descriere dispozitiv

- Operațiile care nu sunt auditate

DSPS36

Afișare configurație System/36

RTVS36A

Extragere atribute configurație S/36

STRS36

Pornire S/36

ENDS36

Terminare S/36

Operații pentru tabelă (*TBL):

- Operație citire

QDCXLATE

Translatare șir de caractere

QTBXLATE

Translatare șir de caractere

QLGRTVSS

Extragere tabelă secvență de sortare

CRTL F

Translatarea tabelii în timpul comenzii CTRL F

Read Folosirea Tabelii de secvențe sortare când se rulează orice comandă care poate specifica o secvență de sortare

- Operația de modificare

Nimic

- Operațiile care nu sunt auditate

WRKTBL

Gestionare tabelă

Operații pentru indexul utilizator (*USRIDX):

- Operație citire

QUSRTVUI

API-ul de extragere intrări indexul utilizator

- Operația de modificare

QUSADDUI

API-ul de adăugare intrări în indexul utilizator

QUSRMVUI

API-ul de înlăturare intrări în indexul utilizator

- Operațiile care nu sunt auditate

Acces Accesul direct la un index utilizator folosind instrucțiunile 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 attribute index utilizator

Operațiuni pentru profilul utilizator (*USRPRF):

- Operație citire

RCLOBJOWN

Recuperare obiecte după proprietar

- Operația de modificare

CHGPRF

Modificare profil utilizator

CHGPWD

Modificare parolă

CHGUSRPRF

Modificare profil utilizator

CHKPWD

Verificare parolă

DLTUSRPRF

Ștergere profil utilizator

GRTUSRAUT

Acordare autorizare utilizator (*la-profil-utilizator*)

QSYCHGPW

API-ul de modificare parolă

RSTUSRPRF

Restaurare profil utilizator

- Operațiile care nu sunt auditate

DSPPGMADP

Afișare programe care adoptă

Auditare obiect

DSPUSRPRF

Afișare profil utilizator

GRTUSRAUT

Acordare autorizare utilizator (*de-la-profil-utilizator*)

PRTPRFINT

Tipărire valori interne profil

PRTUSRPRF

Tipărire profil utilizator

QSYCUSRS

API-ul de verificare autorizări speciale utilizator

QSYLOBJA

API-ul de listare obiecte autorizate

QSYLOBJP

API-ul de listare obiecte care adoptă

QSYRUSRI

API-ul de extragere informații utilizator

RTVUSRPRF

Extragere profil utilizator

WRKOBJOWN

Gestionare obiecte deținute

WRKUSRPRF

Gestionare profiluri utilizator

Operații pentru coada utilizator (*USRQ):

- Nici o operație de citire sau modificare nu este auditată pentru tipul de obiect *USRQ.
- Operațiile care nu sunt auditate

Acces Accesul direct la cozi utilizator folosind instrucțiunile MI (permise doar pentru o coadă utilizator a unui domeniu de utilizatori dintr-o bibliotecă specificată în valoarea sistem QALWUSRDMN.

Operații pentru spațiu utilizator (*USRSPC):

- Operație citire

QUSRTVUS

API-ul de extragere informații spațiu utilizator

- Operația de modificare

QUSCHGUS

API-ul de modificare informații spațiu utilizator

QUSCUSAT

API-ul de modificare atribute spațiu utilizator

- Operațiile care nu sunt auditate

Acces Accesul direct la spațiu utilizator folosind instrucțiunile MI (permise doar pentru spații utilizator ale unui domeniu de utilizatori din bibliotecile specificate în valoarea sistem QALWUSRDMN.

QUSRUSAT

API-ul de extragere atribute spațiu utilizator

Operații pentru lista de validare (*VLDL):

- Operație citire

QSYFDVLE

API-ul de găsire intrare listă de validare

- Operația 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

Operații pentru obiectul de personalizare stație de lucru

- Operație citire

Activare

Când un dispozitiv personalizat este activat

RTVWSCST

Extragere obiect de personalizare stație de lucru (doar când *TRANSFORM este specificat pentru tipul de dispozitiv)

SNDTCPSPLF

Trimitere fișier spool TCP/IP (doar când este specificat TRANSFORM(*YES))

STRPRTWTR

Pornire scriitor imprimantă (doar pentru fișierele spool care sunt tipărite la o imprimantă personalizată folosind funcția de transformare tipărire gazdă)

STRRMTWTR

Pornire scriitor la distanță (doar când coada de ieșire este configurată cu CNNTYPE(*IP) și TRANSFORM(*YES))

Tipărire

Când ieșirea este tipărită direct (nu prin spool) la o imprimantă personalizată folosind funcția de transformare tipărire gazdă

- Operația de modificare

Nimic

- Operațiile care nu sunt auditate

Nimic

Auditare obiect

Anexa F. Macheta intrărilor din jurnalul de auditare

Această anexă conține informații de dispunere pentru toate tipurile de intrări cu cod de jurnal T din jurnalul de auditare (QAUDJRN). Aceste intrări sunt controlate de auditarea de acțiune și de obiect pe care o definiți dumneavoastră. Sistemul scrie intrări suplimentare în jurnalul de auditare pentru evenimente ca un IPL sistem sau salvarea receptorului de jurnal. Dispunerea pentru aceste tipuri de intrări poate fi găsită în subiectul Gestionare jurnal din centrul de informare.

Tabela 152 la pagina 510 conține dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE2) în comanda DSPJRN. Această dispunere, numită QJORDJE2, este definită în fișierul QADSPJR2 din biblioteca QSYS.

Notă: Formatele de ieșire TYPE2 și *TYPE 4 nu mai sunt actualizate, prin urmare IBM vă recomandă să nu mai folosiți formatele *TYPE2 și *TYPE4 și să folosiți numai formate *TYPE5.

Tabela 151 la pagina 509 conține dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE4) în comanda DSPJRN. Această dispunere, numită QJORDJE4, este definită în fișierul QADSPJR4 din biblioteca QSYS. Ieșirea *TYPE4 include toate informațiile *TYPE2 plus informații despre identificatori de jurnal, declanșatoare și restricții referențiale.

Tabela 154 la pagina 512 la Tabela 227 la pagina 614 conțin dispuneri pentru fișierele de ieșire de bază de date de model furnizate pentru a defini date care depind de intrare. Puteți folosi comanda CRTDUPOBJ pentru a crea orice fișier de ieșire gol cu aceeași dispunere ca unul din fișierele de ieșire de bază de date de modele. Puteți folosi comanda DSPJRN pentru a copia intrările selectate din jurnalul de auditare la fișierul de ieșire pentru analizare. “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 262 furnizează exemple de folosire a fișierelor de ieșire de bază de date de modele. Vedeți de asemenea subiectul Gestionare jurnal.

Tabela 150 conține dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE5) în comanda DSPJRN. Această dispunere, numită QJORDJE5, este definită în fișierul QADSPJR5 din biblioteca QSYS. Ieșirea *TYPE5 include toate informațiile *TYPE4, plus informații 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 braț, ID fir de execuție, familie de adrese, port la distanță și adresă la distanță.

*Tabela 150. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format înregistrare QJORDJE5 (*TYPE5)*

Offset	Câmp	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea totală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr de ordine	Char(20)	Aplicat la fiecare intrare de jurnal. Setat inițial la 1 pentru fiecare jurnal nou sau restaurat. Opțional, resetat la 1 când este atașat un nou receptor.
26	Cod jurnal	Char(1)	Întotdeauna T.
27	Tip intrare	Char(2)	Vedeți Tabela 153 la pagina 511 pentru o listă de tipuri de intrări și descrieri.
29	Amprentă de timp pentru intrare	Char(26)	Data și ora la care intrarea a fost creată în format amprentă de timp SAA.
55	Nume job	Char(10)	Numele jobului care a provocat generarea intrării.
65	Nume utilizator	Char(10)	Numele profilului utilizator asociat cu jobul ¹ .
75	Număr de job	Zoned(6,0)	Numărul jobului.

Disponere intrări jurnal de auditare

Tabela 150. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE5 (*TYPE5)

Offset	Câmp	Format	Descriere
81	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parțial al unui fișier clasă folosit într-un program Java compilat. Dacă un program aplicație sau un program CL nu au provocat intrarea, câmpul conține numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevărată una din următoarele condiții: <ul style="list-style-type: none"> • Numele programului nu se aplică la acest tip de intrare. • Numele programului nu a fost disponibil.
91	Biblioteca program	Char(10)	Numele bibliotecii care conține programul care a adăugat intrarea de jurnal.
101	Dispozitiv ASP program	Char(10)	Numele dispozitivului ASP care conține programul care a adăugat intrarea de jurnal.
111	Număr ASP program	Zoned(5,0)	Numărul dispozitivului ASP care conține 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	Biblioteca obiecte	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
136	Nume membru	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
146	Contor/RRN	Char(20)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
166	Indicator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
167	Identificator ciclu de permanentizare	Char(20)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
187	Profil utilizator	Char(10)	Numele profilului utilizator curent. ¹ .
197	Nume sistem	Char(8)	Numele sistemului.
205	Identificator jurnal	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
215	Restricție referențială	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
216	Declanșator	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.
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	Secvență sistem	Char(20)	Un număr asignat de sistem pentru fiecare intrare de jurnal.
241	Receptor	Char(10)	Numele receptorului care conține intrarea de jurnal.
251	Biblioteca receptor	Char(10)	Numele bibliotecii care conține receptorul care conține intrarea de jurnal.
261	Dispozitiv ASP receptor	Char(10)	Numele dispozitivului ASP care conține receptorul.
271	Număr ASP receptor	Zoned(5,0)	Numărul ASP-ului care conține receptorul care conține intrarea de jurnal.
276	Număr braț	Zoned(5,0)	Numărul brațului de disc care conține intrarea de jurnal.
281	Identificator fir de execuție	Hex(8)	Identifică firul de execuție din procesul care a adăugat intrarea de jurnal.
289	Identificator hex fir de execuție	Char(16)	Versiune afișabilă în hex a identificatorului de fir de execuție.

Tabela 150. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE5 (*TYPE5)

Offset	Câmp	Format	Descriere
305	Familie de adrese	Char(1)	Formatul adresei la distanță pentru această intrare de jurnal.
306	Port la distanță	Zoned(5,0)	Numărul de port al adresei la distanță asociate cu intrarea de jurnal.
311	Adresă la distanță	Char(46)	Adresa la distanță 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 tranzacție	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 și numele profil utilizator de la offset 187 au aceeași valoare. Pentru joburi prestart, câmpul nume profil utilizator conține numele utilizatorului care pornește tranzacția. Pentru unele joburi, ambele câmpuri conțin QSYS ca nume utilizator. Câmpul nume profil utilizator din datele specifice intrării conține utilizatorul care a provocat intrarea. Dacă se folosește un API pentru a interschimba profilurile utilizator, câmpul nume profil utilizator conține numele profilului utilizator nou (interschimbat).

Tabela 151. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format înregistrare QJORDJE4 (*TYPE4)

Offset	Câmp	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea totală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr de ordine	Zoned(10,0)	Aplicat la fiecare intrare de jurnal. Setat inițial la 1 pentru fiecare jurnal nou sau restaurat. Opțional, resetăți la 1 când este atașat un nou receptor.
16	Cod jurnal	Char(1)	Întotdeauna T.
17	Tip intrare	Char(2)	Vedeți Tabela 153 la pagina 511 pentru o listă de tipuri de intrări și descrieri.
19	Amprentă de timp pentru intrare	Char(26)	Data și ora la care intrarea a fost creată în format amprentă de timp SAA.
45	Nume job	Char(10)	Numele jobului care a provocat generarea intrării.
55	Nume utilizator	Char(10)	Numele profilului utilizator asociat cu jobul ¹ .
65	Număr de job	Zoned(6,0)	Numărul jobului.
71	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parțial al unui fișier clasă folosit într-un program Java compilat. Dacă un program aplicație sau un program CL nu au provocat intrarea, câmpul conține numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevărată una din următoarele: <ul style="list-style-type: none"> • Numele programului nu se aplică la acest tip de intrare. • Numele programului nu a fost disponibil.
81	Nume obiect	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
91	Nume bibliotecă	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
101	Nume membru	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
111	Contor/RRN	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
121	Indicator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
122	ID ciclului de permanentizare	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
132	Profil utilizator	Char(10)	Numele profilului utilizator curent. ¹ .

Disponere intrări jurnal de auditare

Tabela 151. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE4 (*TYPE4)

Offset	Câmp	Format	Descriere
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	Restricție referențială	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
161	Declanșator	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.

Notă: Cele trei câmpuri care încep la offset 45 alcătuiesc numele de job sistem. În majoritatea cazurilor, câmpul nume utilizator de la offset 55 și numele profil utilizator de la offset 132 au aceeași valoare. Pentru joburi prestart, câmpul nume profil utilizator conține numele utilizatorului care pornește tranzacția. Pentru unele joburi, ambele câmpuri conțin QSYS ca nume utilizator. Câmpul nume profil utilizator din datele specifice intrării conține utilizatorul care a provocat intrarea. Dacă se folosește un API pentru a interschimba profilurile utilizator, câmpul nume profil utilizator conține numele profilului utilizator nou (interschimbat).

Tabela 152. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea totală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr secvență	Zoned(10,0)	Aplicat la fiecare intrare de jurnal. Setat inițial la 1 pentru fiecare jurnal nou sau restaurat. Opțional, resetată la 1 când este atașat un nou receptor.
16	Cod jurnal	Char(1)	Întotdeauna T.
17	Tip intrare	Char(2)	Vedeti Tabela 153 la pagina 511 pentru o listă de tipuri de intrări și 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 utilizator asociat cu jobul ¹ .
51	Număr de job	Zoned(6,0)	Numărul jobului.
57	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parțial al unui fișier clasă folosit într-un program Java compilat. Dacă un program aplicație sau un program CL nu au provocat intrarea, câmpul conține numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevărată una din următoarele: <ul style="list-style-type: none"> 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 ciclului de permanentizare	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
118	Profil utilizator	Char(10)	Numele profilului utilizator curent. ¹ .

Tabela 152. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	Format	Descriere
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 <i>Nume utilizator</i> de la offset-ul 41 și câmpul <i>Nume profil utilizator</i> de la offset-ul 118 au aceeași valoare. Pentru joburi prestart, câmpul <i>nume profil utilizator</i> conține numele utilizatorului care pornește tranzacția. Pentru unele joburi, ambele câmpuri conțin QSYS ca nume utilizator. Câmpul <i>nume profil utilizator</i> din datele specifice intrării conține utilizatorul care a provocat intrarea. Dacă se folosește un API pentru a interschimba profilurile utilizator, câmpul <i>nume profil utilizator</i> conține numele profilului utilizator nou (interschimbat).		

Tabela 153. Tipuri intrare jurnal auditare (QAUDJRN)

Tip intrare	Descriere
AD	Auditare modificări
AF	Eșuare autorizare
AP	Obținere autorizare adoptată
AU	Modificări atribut
CA	Modificări autorizare
CD	Auditare șir comandă
CO	Creare obiect
CP	Profil utilizator modificat, creat sau restaurat
CQ	Modificare obiect *CRQD
CU	Operații cluster
CV	Verificare conexiune
CY	Conexiune criptografică
DI	Directory Server
DO	Ștergere 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	Comunicație între procese
IR	Acțiuni reguli IP
IS	Gestionare securitate internet
JD	Modificare parametru utilizator pentru o descriere job
JS	Acțiuni care afectează joburile
KF	Fișierul inel de chei
LD	Legare, dezlegare sau căutare intrare director
ML	Acțiuni mail servicii office
NA	Atribut rețea 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) Fișier unic sau director
O2	(Acces optic) Fișier dual sau director
O3	(Acces optic) Volum
PA	Program modificat pentru adoptare autorizare
PG	Modificare grup primar pentru un obiect
PO	Ieșire tipărită

Disponere intrări jurnal de auditare

Tabela 153. Tipuri intrare jurnal auditare (QAUDJRN) (continuare)

Tip intrare	Descriere
PS	Comutare (swap) profil
PW	Parolă nevalidă
RA	Modificare autorizare în timpul restaurării
RJ	Restaurare descriere job cu profil utilizator specificat
RO	Modificare proprietar obiect în timpul restaurării
RP	Restaurare program cu autorizare adoptată
RQ	Restaurare obiect *CRQD
RU	Restaurare autorizare profil utilizator
RZ	Modificare grup primar în timpul restaurării
SD	Modificări aduse directorului de distribuție sistem
SE	Intrare de rutare subsistem modificată
SF	Acțiuni la fișierele spool
SG	Semnale asincrone
SK	Securizare conexiuni socket
SM	Modificări gestiune sisteme
SO	Acțiuni informații 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 fișiere server
VL	Limită cont depășită
VN	Conectare sau deconectare rețea
VO	Acțiuni listă de validare
VP	Eroare parolă rețea
VR	Acces resursă rețea
VS	Pornire sau terminare sesiune server
VU	Modificare profil rețea
VV	Modificare stare serviciu
X0	Autentificare rețea
X1	Jeton de identificare
YC	Obiect DLO accesat (modificare)
YR	Obiect DLO accesat (citire)
ZC	Obiect accesat (modificare)
ZR	Obiect accesat (citire)

Tabela 154. Intrări jurnal AD (auditare modificare). Fișier descriere câmp QASYADJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	D comanda CHGDLOAUD O comanda CHGAUD S Atributul de scanare a fost modificat folosind comanda CHGATR sau API-ul Qp01SetAttr API sau când obiectul a fost creat. U comanda CHGUSRAUD

Tabela 154. Intrări jurnal AD (auditare modificare) (continuare). Fișier descriere câmp QASYADJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
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 conține valoarea de auditare specificată. Dacă tipul intrării este S, câmpul conține valoarea atributului de scanare.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = Comenzi de auditare pentru acest utilizator.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator creează un obiect.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator șterge un obiect.
198	266	652	CHGUSRAUD *JOBSTA	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 redenumeste un obiect.
200	268	654	CHGUSRAUD *OFCSRVR	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator execută funcții office.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator obține 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 acțiuni relevante pentru securitate.
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator execută funcții service.
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator manipulează fișiere spool.
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = Se scrie o înregistrare de auditare când acest utilizator face modificări de gestiune sisteme.
207	275	661	CHGUSRAUD *OPTICAL	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator accesează dispozitive optice.
208	276	662	(Zonă rezervată)	Char(19)	
227	295	681	Nume DLO	Char(12)	Numele obiectului DLO pentru care auditarea a fost modificată.
239	307	693	(Zonă rezervată)	Char(8)	
247	315	701	Cale folder	Char(63)	Calea folderului.
310			(Zonă rezervată)	Char(20)	
	378	764	(Zonă rezervată)	Char(18)	
	396	782	Lungime nume obiect ¹	Binary(4)	Lungimea numelui obiectului.
330	398	784	CCSID nume obiect ¹	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
334	402	788	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.
336	404	790	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
339	407	793	(Zonă rezervată)	Char(3)	
342	410	796	ID fișier părinte ^{1,2}	Char(16)	ID-ul fișierului directorului părinte.
358	426	812	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.

Disponere intrări jurnal de auditare

Tabela 154. Intrări jurnal AD (auditare modificare) (continuare). Fișier descriere câmp QASYADJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
374	442	828	Nume obiect ¹	Char(512)	Numele obiectului.
	954	1340	ID fișier obiect ¹	Char(16)	ID-ul fișier 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.
	989	1375	ID regiune sau țară nume cale ¹	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	991	1377	ID limbă nume cale ¹	Char(3)	ID-ul limbă pentru numele de cale absolută.
	994	1380	Lungime nume cale ¹	Binary(4)	Lungimea numelui căii absolute.
	996	1382	Indicator nume cale ¹	Char(1)	Indicator nume cale: Y Câmpul Nume cale conține numele căii absolute complete pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	997	1383	ID fișier înrudit ^{1,3}	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
1013	1399	Nume cale ^{1,4}	Char(5002)	Numele căii obiectului.	

¹ Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.

² Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

⁵ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 155. Intrări jurnal AF (Eșuare autorizare). Fișier descriere câmp QASYAFJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 155. Intrări jurnal AF (Eșuare autorizare) (continuare). Fișier descriere câmp QASYAFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip violare ¹	Char(1)	<p>A Neautorizat la obiect</p> <p>B Instrucțiunea restricționată</p> <p>C Eșuare validare (vedeți J5 offset 639)</p> <p>D Folosire interfață nesuportată, eșuare domeniu obiect</p> <p>E Eroare de protecție spațiu de stocare hardware, violare spațiu constant program</p> <p>F Eroare autorizare ICAP</p> <p>G Eroare autentificare ICAP</p> <p>H Scanare acțiune program de ieșire (vedeți J5 offset 639)</p> <p>I⁷ Moștenirea sistem Java nu este permisă</p> <p>J Eroare lansare profil job</p> <p>K Violare specială a autorizării</p> <p>N Jetonul profil nu este un jeton regenerabil</p> <p>O Eșuare autorizare obiect optic</p> <p>P Eroare comutare (swap) profil</p> <p>R Eroare de protecție hardware</p> <p>S Încercare de semnare implicită</p> <p>T Neautorizat la portul TCP/IP</p> <p>U Cerere de permisiune utilizator nevalidă</p> <p>V Jetonul profil nu este valid pentru generarea unui nou jeton profil</p> <p>W Jetonul profil nu este valid pentru comutare (swap)</p> <p>X Violare sistem — vedeți J5 offset 723 pentru codurile de violare</p> <p>Y Neautorizat pentru câmpul curent JUID în timpul unei operații de ștergere JUID.</p> <p>Z Neautorizat pentru câmpul curent JUID în timpul unei operații de setare JUID.</p>
157	225	611	Nume obiect ^{1, 5, 12}	Char(10)	Numele obiectului.
167	235	621	Numele bibliotecii ¹³	Char(10)	Numele bibliotecii în care este obiectul sau numărul corecției de LIC care a eșuat la aplicare. ¹¹
177	245	631	Tip obiect ¹⁴	Char(8)	Tipul obiectului.

Disponere intrări jurnal de auditare

Tabela 155. Intrări jurnal AF (Eșuare autorizare) (continuare). Fișier descriere câmp QASYAFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
185	253	639	Acțiune eroare validare	Char(1)	<p>Acțiunea luată după eroarea de validare detectată, setată doar dacă tipul de violare (J5 offset 610) este C sau H.</p> <p>A Translatarea obiectului nu a fost încercată sau a eșuat. Setarea valoare sistem QALWOBJRST a permis obiectului să fie restaurat. Utilizatorul care face restaurarea nu a avut autorizare specială *ALLOBJ și nivelul de securitate sistem este setat la 10, 20 sau 30. De aceea, toate autorizările la obiect au fost reținute.</p> <p>B Translatarea obiectului nu a fost încercată sau a eșuat. Setarea valoare sistem QALWOBJRST a permis obiectului să fie restaurat. Utilizatorul care face restaurarea nu a avut autorizare specială *ALLOBJ și nivelul de securitate sistem este setat la 40 sau mai mult. De aceea, toate autorizările la obiect au fost revocate.</p> <p>C Translatarea obiectului a avut succes. Copia translatată a fost restaurată în sistem.</p> <p>D Translatarea obiectului nu a fost încercată sau a eșuat. 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 reținute.</p> <p>E Eroare detectată de timp instalare sistem.</p> <p>F Obiectul nu a fost restaurat din cauza semnăturii care nu este în format i5/OS.</p> <p>G Sistem neassignat sau obiect în stare de moștenire găsite la verificarea sistemului.</p> <p>H Obiect în stare utilizator neassignat găsită la verificarea sistemului.</p> <p>I Nepotrivire între obiect și semnătura sa găsită la verificarea sistemului.</p> <p>J Certificatul IBM nu a fost găsit la verificarea sistemului.</p> <p>K Format de semnătură nevalid găsit la verificarea sistemului.</p> <p>M Programul de ieșire scanare a modificat obiectul care a fost scanat</p> <p>X Programul de ieșire scanare a dorit marcarea obiectului ca având o eșuare la scanare</p>
186	254	640	Nume job	Char(10)	Numele jobului.
196	264	650	Nume utilizator	Char(10)	Numele utilizator job.
206	274	660	Număr job	Zoned(6,0)	Număr job.
212	280	666	Nume program	Char(10)	Numele programului.

Tabela 155. Intrări jurnal AF (Eșuare autorizare) (continuare). Fișier descriere câmp QASYAFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
222	290	676	Biblioteca program	Char(10)	Numele bibliotecii unde este găsit programul.
232	300	686	Profil utilizator ²	Char(10)	Numele utilizatorului care a cauzat eșuarea de autorizare.
242	310	696	Nume stație de lucru	Char(10)	Numele stației de lucru sau tipul stației de lucru.
252	320	706	Număr instrucțiune program	Zoned(7,0)	Numărul instrucțiunii programului.
259	327	713	Nume câmp	Char(10)	Numele câmpului.
269	337	723	Cod violare operație	Char(3)	Tipul violării de operație care a apărut, setat doar dacă tipul violării (J5 offset 610) este X. HCA Profilul utilizator unelte service nu este autorizat să execute operația de configurare hardware (QYHCHCOP). LIC LIC indică faptul că nu a fost aplicată corecția de LIC din cauza unei violări de semnătură. SFA Neautorizat să activeze atributul de mediu pentru accesul fișierului 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	Char(63)	Calea folderului.
365	433	819	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
375			(Zonă rezervată)	Char(20)	
	443	829	(Zonă rezervată)	Char(18)	
	461	847	Lungime nume obiect ³	Binary(4)	Lungimea numelui obiectului.
395	463	849	CCSID nume obiect ³	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
399	467	853	ID regiune sau țară nume obiect ³	Char(2)	ID-ul regiunii sau țării 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 fișier părinte ^{3,4}	Char(16)	ID-ul fișierului directorului părinte.
423	491	877	ID fișier obiect ^{3,4}	Char(16)	ID-ul fișier al obiectului.
439	507	893	Nume obiect ^{3,6}	Char(512)	Numele obiectului.
	1019	1405	ID fișier obiect ³	Char(16)	ID-ul fișier 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 țară nume cale ³	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.

Disponere intrări jurnal de auditare

Tabela 155. Intrări jurnal AF (Eșuare autorizare) (continuare). Fișier descriere câmp QASYAFJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1056	1442	ID limbă nume cale ³	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1059	1445	Lungime nume cale ³	Binary(4)	Lungimea numelui căii absolute.
	1061	1447	Indicator nume cale ³	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1062	1448	ID fișier director înrudit ^{3, 8}	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	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 violării este pentru descrierea "G", numele obiectului conține numele *SRVPGM care a conținut ieșirea care a detectat eroarea. Pentru mai multe detalii despre tipurile de violări, vedeți Tabela 126 la pagina 239.

² Acest câmp conține numele utilizatorului care a cauzat intrarea. QSYS poate fi utilizator pentru următoarele:

- offset-urile 41 și 118 pentru înregistrările *TYPE2
- offset-urile 55 și 132 pentru înregistrările *TYPE4
- offset-urile 65 și 187 pentru înregistrările *TYPE5

³ Aceste câmpuri sunt folosite doar pentru obiectele din sistemul de fișiere QOpenSys, din sistemul de fișiere "rădăcină" (/), din sistemele de fișiere definite de utilizator și QFileSvr.400.

⁴ Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.

⁵ Când tipul violării este "T", numele obiectului conține portul TCP/IP pe care utilizatorul nu are autorizarea să îl acceseze. Valoarea este lăsată aliniată la stânga și goală. Câmpurile bibliotecă obiect și tip obiect vor fi goale.

⁶ Când tipul de violare este O, numele obiectului optic este conținut în câmpul de nume obiect al sistemului de fișiere integrat. Câmpurile ID regiune sau țară, ID limbă, ID fișier părinte și ID fișier obiect vor conține toate spații goale.

⁷ Obiectul clasă Java care a fost creat nu-și poate extinde clasa sa de bază pentru că ea are attribute sistem Java.

⁸ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁹ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

¹⁰ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 155. Intrări jurnal AF (Eșuare autorizare) (continuare). Fișier descriere câmp QASYAFJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
11					Când Tip violare este X și valoarea codului Violare operație este LIC, aceasta indică faptul că nu a fost aplicată o corecție LIC din cauza unei violări de semnătură. Acest câmp va conține numărul corecției LIC a cărei aplicare a eșuat.
12					Când tipul violării este "K", numele obiectului conține 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 instrucțiune de mașină a detectat eroarea.
13					Când tipul violării este "K", numele bibliotecii conține numele bibliotecii programului sau "*N" pentru biblioteca în care se afișă comanda care a detectat eroarea.
14					Când tipul violării este "K", numele obiectului conține tipul obiectului comenzii sau programului care a detectat eroarea.
15					Când tipul violării este "K", calea folderului poate conține întregul nume API al API-ului sau numele punctului de ieșire care a detectat eroarea.

Tabela 156. Intrări jurnal AP (autorizare adoptată). Fișier descriere câmp QASYAPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	S Pornire E Terminare A Autorizarea adoptată folosită în timpul activării program
157	225	611	Nume obiect	Char(10)	Numele programului, programului de serviciu sau a unui pachet SQL.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Deținerea profilului utilizator	Char(10)	Numele profilului utilizator a cărui autorizare este adoptată.
195	263	649	ID fișier obiect	Char(16)	ID-ul fișier al obiectului.
	279	665	Nume ASP ¹	Char(10)	Numele dispozitivului ASP.
	289	675	Număr ASP ¹	Char(5)	Numărul dispozitivului ASP.
1					Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 157. Intrări jurnal AU (Modificări atribut). Fișier descriere câmp QASYAUJ5

Offset			
J5	Câmp	Format	Descriere
610	Tip intrare	Char(1)	Tipul intrării.
611	Acțiune	Char(3)	E Atribute de configurație EIM Acțiune CHG Atribute modificate

Disponere intrări jurnal de auditare

Tabela 157. Intrări jurnal AU (Modificări atribut) (continuare). Fișier descriere câmp QASYAUJ5

Offset			
J5	Câmp	Format	Descriere
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 țară valoare nouă	Char(2)	ID regiune sau țară 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 țară valoare veche	Char(2)	ID regiune sau țară 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 octeți conțin lungimea câmpului.

Tabela 158. Intrări jurnal CA (Modificări autorizare). Fișier descriere câmp QASYCAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
157	225	611	Nume obiect	Char(10)	A Modificările pentru autorizare 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 utilizator a cărui autorizare este revocată.
195	263	649	Nume listă de autorizații	Char(10)	Numele listei de autorizații.
205	273	659	Existență obiect	Char(1)	Autorizările acordate sau înlăturate: Y *OBJEXIST
206	274	660	Management obiect	Char(1)	Y *OBJMGT
207	275	661	Operare obiect	Char(1)	Y *OBJOPR
208	276	662	Gestionare liste de autorizare	Char(1)	Y *AUTLMGT
209	277	663	Listă de autorizații	Char(1)	Y Autorizare publică *AUTL
210	278	664	Autorizare citire	Char(1)	Y *READ
211	279	665	Autorizare adăugare	Char(1)	Y *ADD

Tabela 158. Intrări jurnal CA (Modificări autorizare) (continuare). Fișier descriere câmp QASYCAJE/J4/J5

Offset			Câmp	Format	Descriere	
JE	J4	J5				
212	280	666	Autorizare actualizare	Char(1)	Y	*UPD
213	281	667	Autorizare ștergere	Char(1)	Y	*DLT
214	282	668	Autorizare excludere	Char(1)	Y	*EXCLUDE
215	283	669	Autorizare execuție	Char(1)	Y	*EXECUTE
216	284	670	Autorizare de alterare obiect	Char(1)	Y	*OBJALTER
217	285	671	Autorizare de referire la obiect	Char(1)	Y	*OBJREF
218	286	672	(Zonă rezervată)	Char(4)		
222	290	676	Tip comandă	Char(3)		Tipul comenzii folosite. GRT Acordare RPL Acordare cu înlocuire RVK Revocare USR Operația GRTUSRAUT
225	293	679	Nume câmp	Char(10)		Numele câmpului.
235	303		(Zonă rezervată)	Char(10)		
		689	Atributul obiectului	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 setului de caractere codate pentru numele obiect.
378	446	832	ID regiune sau țară nume obiect ¹	Char(2)		ID-ul regiunii sau țării pentru numele obiectului.
380	448	834	ID limbă nume obiect ¹	Char(3)		ID-ul limbă pentru numele obiectului.
383	451	837	(Zonă rezervată)	Char(3)		
386	454	840	ID fișier părinte ^{1,2}	Char(16)		ID-ul fișierului directorului părinte.
402	470	856	ID fișier obiect ^{1,2}	Char(16)		ID-ul fișier al obiectului.
418	486	872	Nume obiect ¹	Char(512)		Numele obiectului.
	998	1384	ID fișier obiect	Char(16)		ID-ul fișier al obiectului.

Disponere intrări jurnal de auditare

Tabela 158. Intrări jurnal CA (Modificări autorizare) (continuare). Fișier descriere câmp QASYCAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	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 țară nume cale	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	1035	1421	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1038	1424	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1040	1426	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1041	1427	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1057	1443	Nume cale ⁴	Char(5002)	Numele căii obiectului.

¹ Aceste câmpuri sunt folosite doar pentru obiectele din sistemul de fișiere QOpenSys, din sistemul de fișiere "rădăcină", din sistemele de fișiere definite de utilizator și QFileSvr.400.

² Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

⁵ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 159. Intrări jurnal CD (șir comenzi). Fișier descriere câmp QASYCDJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 159. Intrări jurnal CD (șir comenzi) (continuare). Fișier descriere câmp QASYCDJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare	Char(1)	Tipul intrării. C Rulare comandă L Instrucțiune OCL O Control operator. P procedură S/36 S Rulare comandă după ce substituția comenzii a avut loc U Instrucțiune 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	Rulare dintr-un program CL	Char(1)	Y Da N Nu
186	254	640	Șir 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

Tabela 160. Intrări jurnal CO (Creare obiect). Fișier descriere câmp QASYCOJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. N Creare de noi obiecte R Înlocuirea unui obiect existent
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	(Zonă rezervată) Atribut obiect	Char(20)	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)	

Disponere intrări jurnal de auditare

Tabela 160. Intrări jurnal CO (Creare obiect) (continuare). Fișier descriere câmp QASYCOJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	394	780	Lungime nume cale	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect ¹	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
332	400	786	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.
334	402	788	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fișier părinte ^{1,2}	Char(16)	ID-ul fișierului directorului părinte.
356	424	810	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
372	440	826	Nume obiect ¹	Char(512)	Numele obiectului.
	952	1338	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1011	1397	Nume cale ⁴	Char(5002)	Numele căii obiectului.

¹ Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.

² Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

⁵ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 161. Intrări jurnal CP (Modificări profil utilizator). Fișier descriere câmp QASYCPJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
157	225	611	Nume profil utilizator	Char(10)	A Modificare la un profil utilizator Numele profilului utilizator care a fost modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	256	639	Nume comandă	Char(3)	Tipul comenzii folosite.
					CRT CRTUSRPRF
					CHG CHGUSRPRF
					RST RSTUSRPRF
					DST Resetare parolă QSECOFR folosind DST
					RPA API-ul QSYRESPA
188	256	642	Parolă modificată	Char(1)	Y Parolă modificată
189	257	643	Parolă *NONE	Char(1)	Y Parola este *NONE.
190	258	644	Parolă expirată	Char(1)	Y Parola expirată este *YES N Parola expirată este *NO
191	259	645	Autorizare specială la toate obiectele	Char(1)	Y Autorizare specială *ALLOBJ
192	260	646	Autorizare specială control job	Char(1)	Y Autorizare specială *JOBCTL
193	261	647	Autorizare specială salvare sistem	Char(1)	Y Autorizare specială *SAVSYS
194	262	648	Autorizare specială administrator securitate	Char(1)	Y Autorizare specială *SECADM
195	263	649	Autorizare specială control spool	Char(1)	Y Autorizare specială *SPLCTL
196	264	650	Autorizare specială service	Char(1)	Y Autorizare specială *SERVICE
197	265	651	Autorizare specială auditare	Char(1)	Y Autorizare specială *AUDIT
198	266	652	Autorizare specială configurație sistem	Char(1)	Y Autorizare specială *IOSYSCFG
199	267	653	(Zonă rezervată)	Char(13)	
212	280	666	Profil grup	Char(10)	Numele unui profil grup.
222	290	676	Proprietar	Char(10)	Proprietarul obiectelor create ca membru al unui profil grup.

Disponere intrări jurnal de auditare

Tabela 161. Intrări jurnal CP (Modificări profil utilizator) (continuare). Fișier descriere câmp QASYCPJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
232	300	686	Autorizare grup	Char(10)	Autorizare profil grup.
242	310	696	Program inițial	Char(10)	Numele programului inițial al utilizatorului.
252	320	706	Biblioteca program inițial	Char(10)	Numele bibliotecii unde este găsit programul inițial.
262	330	716	Meniu inițial	Char(10)	Numele meniului inițial al utilizatorului.
272	340	726	Bibliotecă meniu inițial	Char(10)	Numele bibliotecii unde este găsit meniul inițial.
282	350	736	Biblioteca actuală	Char(10)	Numele bibliotecii actuale a utilizatorului.
292	360	746	Capabilități limitate	Char(10)	Valoarea parametrului de capabilități limitate.
302	370	756	Clasă utilizator	Char(10)	Clasa utilizator a utilizatorului.
312	380	766	Limită prioritate	Char(1)	Valoarea parametrului limită prioritate.
313	381	767	Stare profil	Char(10)	Stare profil utilizator.
323	391	777	Tip autorizare grup	Char(10)	Valoarea parametrului GRPAUTTYP.
333	401	787	Profiluri grup suplimentare	Char(150)	Numele a până la 15 profiluri grup suplimentar pentru utilizator.
483	551	937	Identificare utilizator	Char(10)	uid pentru utilizator.
493	561	947	Identificare grup	Char(10)	gid pentru utilizator.
503	571	957	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 și este în concordanță.
					*SYSVAL Verificată dar nu este în concordanță din cauza unei reguli bazate pe valori sistem.
					*EXITPGM Verificată dar nu este în concordanță din cauza unui răspuns de ieșire al unui program.
					*NONE Neverificată; drept noua parolă a fost specificat *NONE.
					*NOCHECK Neverificată; parola a fost schimbată. Acest câmp are semnificație numai când câmpul Parolă schimbată conține 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.
					număr Dimensiunea intervalului de expirare în zile.

Tabela 162. Intrări jurnal CQ (modificare *CRQD). Fișier descriere câmp QASYCQJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificare obiect *CRQD
157	225	611	Nume obiect	Char(10)	Numele obiectului care a fost modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii obiect.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
		639	Nume ASP	Char(10)	Nume ASP pentru biblioteca CRQD
		649	Număr ASP	Char(5)	Număr ASP pentru biblioteca CRQD

Tabela 163. Intrări jurnal CU (Operații cluster). Fișier descriere câmp QASYCUJ4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru menționarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. M Operație control cluster R operație de gestiune grup resurse cluster (*GRP)
	225	611	Acțiune intrare	Char(3)	Tipul acțiunii. ADD Adăugare CRT Creare DLT Ștergere DST Distribuire END Terminare FLO Preluare la eroare LST Listare informații RMV Înlăturare STR Pornire SWT Comutare UPC Actualizare attribute
	228	614	Stare	Char(3)	Starea cererii. ABN Cererea s-a terminat anormal AUT Eșuare autorizare, *IOSYSCFG este necesară END Cererea s-a terminat cu succes STR Cererea a fost pornită

Disponere intrări jurnal de auditare

Tabela 163. Intrări jurnal CU (Operații cluster) (continuare). Fișier descriere câmp QASYCUJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	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 inițiat cererea.
	287	673	Nume coadă utilizator	Char(10)	Numele cozii utilizator unde sunt trimise răspunsurile.
	297	683	Biblioteca 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.

Tabela 164. Intrări jurnal CV (Verificare conexiune). Fișier descriere câmp QASYCVJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru menționarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. C Conexiune stabilită E Conexiune terminată R Conexiune refuzată

Tabela 164. Intrări jurnal CV (Verificare conexiune) (continuare). Fișier descriere câmp QASYCVJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	225	611	Acțiune	Char(1)	Acțiune 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 configurație 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 configurație 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. Tipul intrării. CHAP Protocolul de autentificare dialog de confirmare cerere PAP Protocol de autentificare parolă. SCRIPT Metodă script.
	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 distanță	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 utilizator *VLDL	Char(100)	Nume utilizator *VLDL.

Disponere intrări jurnal de auditare

Tabela 164. Intrări jurnal CV (Verificare conexiune) (continuare). Fișier descriere câmp QASYCVJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	386	772	Adresă IP locală	Char(40)	Adresa IP locală.
	426	812	Adresă IP la distanță	Char(40)	Adresa IP la distanță.
	466	852	Înaintare IP	Char(1)	Tipul intrării. Y Înaintarea IP este activă. N Înaintarea IP este inactivă.
	467	853	Proxy ARP	Char(1)	Tipul intrării. Y Proxy ARP este activat. N Proxy ARP nu este activat.
	468	854	Nume radius	Char(10)	Numele profil AAA.
	478	864	Autentificare adresă IP	Char(40)	Autentificare adresă IP.
	518	904	ID sesiune cont	Char(14)	ID sesiune cont.
	532	918	ID multi-sesiune cont	Char(14)	ID multi-sesiune cont.
	546	932	Număr legătură cont	Binary(4)	Număr legătură cont.
	548	934	Tip tunel	Char(1)	Tip tunel: 0 Netunelat 3 L2TP 6 AH 9 ESP
	549	935	Punct final client tunel	Char(40)	Punct final client tunel
	589	975	Punct final server tunel	Char(40)	Punct final server tunel
	629	1015	Timp sesiune cont	Char(8)	Timp sesiune cont. Folosit pentru Tipul de intrare E sau R.
	637	1023	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

Tabela 165. Intrări jurnal CY (Configurație criptografică). Fișier descriere câmp QASYCYJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 165. Intrări jurnal CY (Configurație criptografică) (continuare). Fișier descriere câmp QASYCYJ4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	224	610	Tip intrare	Char(1)	Tipul intrării. A Funcție de control acces coprocesor Cryptographic F Funcție de control facilitate coprocesor Cryptographic K Funcție cheie master servicii Cryptographic M Funcție cheie master coprocesor Cryptographic
	225	611	Acțiune	Char(3)	Funcția configurație criptografică executată: CCP Definire profil card. CCR Definire rol card. CLK Setare ceas. CLR Ștergere chei primare. CRT Creare chei primare. DCP Ștergere profil card. DCR Ștergere rol card. DST Distribuie chei primare. EID Setare ID mediu. FCV Încărcare/curățare FCV. INI Reinițializare card. LOD Încărcare cheie master. QRY Cerere rol sau informații 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
		640	ID-ul cheii master ¹	Binary(4)	Cheia master a serviciilor criptografice ID. ³
¹	Când tipul intrării (J5 offset 610) este K, profilul card (J5 offset 614), rolul cardului (J5 offset 622) și numele dispozitivului (J5 offset 630) este făcut câmp gol.				
²	Când tipul intrării este "K", acest câmp este gol.				
³	Când tipul intrării nu este "K", acest câmp este gol.				

Disponere intrări jurnal de auditare

Tabela 166. Intrări jurnal DI (Directory Server). fișier descriere câmp QASYDIJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
	224	610	Tip intrare	Char(1)	Tipul intrării.
	225	611	Tip operație	Char(2)	<p>L Operație LDAP</p> <p>Tipul operației LDAP:</p> <p>AD Modificare atribut auditare.</p> <p>AF Eșuare autorizare.</p> <p>BN Legătură cu succes.</p> <p>CA Modificare autorizare obiect.</p> <p>CF Modificare configurație.</p> <p>CO Creare obiect.</p> <p>CP Modificare parolă.</p> <p>DO Obiect ștergere.</p> <p>EX Exportare director LDAP.</p> <p>IM Importare director LDAP.</p> <p>OM Obiect gestiune (redenumire).</p> <p>OW Modificare drept de proprietate.</p> <p>PO Modificare politică.</p> <p>PW Parolă eșuată.</p> <p>RM Gestionarea replicărilor</p> <p>UB Dezlegare cu succes.</p> <p>ZC Obiect modificare.</p> <p>ZR Obiect citire.</p>

Tabela 166. Intrări jurnal DI (Directory Server) (continuare). fișier descriere câmp QASYDIJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	227	613	Cod eșuare autorizare	Char(1)	Cod pentru eșuările de autorizare. Acest câmp este folosit doar dacă tipul operației (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 ștergere obiect neautorizată.
					E Încercare de exportare neautorizată.
					F Modificare configurație neautorizată (administrator, modificare istoric, bibliotecă backend, publicare)
					G Încercare de gestiune 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 configurație de auditare.
					X Încercare neautorizată de autorizare proxy.
	228	614	Modificare configurație	Char(1)	Modificări configurație. Acest câmp este folosit doar dacă tipul operației (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 operației este (J5 offset 611) RM următoarele valori pot fi prezente:
					U Suspendare replicare.
					V Reluare replicare.
					W Replicare modificări aflate în așteptare acum.
					X Ocolire una sau mai multe modificări aflate în așteptare.
					Y Dezactivare context replicare.
					Z Dezactivare context replicare.
	229	615	Cod modificare configurație	Char(1)	Cod pentru modificările configurației. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este CF.
					A Element adăugat la configurație
					D Element șters din configurație
					M Element modificat

Disponere intrări jurnal de auditare

Tabela 166. Intrări jurnal DI (Directory Server) (continuare). fișier descriere câmp QASYDIJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	230	616	Propagare steguleț	Char(1)	Indică setarea nouă a proprietarului sau valorii de propagare ACL. Acest câmp este folosit doar dacă tipul operației (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 operației (J5 offset 611) este BN.
	251	637	Versiune LDAP	Char(4)	Versiunea clientului care face cererea. Acest câmp este folosit doar dacă operația 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 operația a fost făcută prin serverul LDAP. 0 Nu 1 Da
	256	642	Tip cerere	Char(1)	Tipul cererii. Acest câmp este folosit doar dacă operația 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 operația a fost făcută prin serverul LDAP.
	277	663	Adresă IP client	Char(50)	Adresa IP și numărul de port al cererii client. Acest câmp este folosit doar dacă operația a fost făcută prin serverul LDAP.
	327	713	CCSID nume utilizator	Bin(5)	Identificatorul de set de caractere codat al numelui utilizator.
	331	717	Lungime nume utilizator	Bin(4)	Lungimea numelui utilizator.
	333	719	Nume utilizator ¹	Char(2002)	Numele utilizatorului LDAP.
	2335	2721	CCSID nume obiect	Bin(5)	Identificatorul set de caractere codat pentru numele obiectului.
	2339	2725	Lungime nume cale	Bin(4)	Lungimea numelui obiectului.
	2341	2727	Nume obiect ¹	Char(2002)	Numele obiectului LDAP.
	4343	4729	CCSID nume proprietar	Bin(5)	Identificatorul de set de caractere codat al numelui proprietarului. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este OW.
	4347	4733	Lungime nume proprietar	Bin(4)	Lungimea numelui proprietarului. Acest câmp este folosit doar dacă tipul operației este OW.
	4349	4735	Nume proprietar ¹	Char(2002)	Numele proprietarului. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este OW.

Tabela 166. Intrări jurnal DI (Directory Server) (continuare). fișier descriere câmp QASYDIJ4/J5

Offset		JE	J4	J5	Câmp	Format	Descriere
			6351	6737	CCSID nume nou	Bin(5)	<p>Identificatorul set de caractere codat pentru numele nou. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este OM, OW, PO, ZC, AF+M, sau AF+P.</p> <ul style="list-style-type: none"> • Pentru tipul operație OM, acest câmp va conține CCSID-ul numelui obiect nou. • Pentru tipul operație OW, acest câmp va conține CCSID-ul numelui proprietar nou. • Pentru tipurile de operații PO, ZC, AF+M, sau AF+P, acest câmp va conține CCSID-ul listei de tipuri de attribute modificate din câmpul Nume nou.
			6355	6741	Lungime nume nou	Bin(4)	<p>Lungimea numelui nou. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este OM, OW, PO, ZC, AF+M, sau AF+P.</p> <ul style="list-style-type: none"> • Pentru tipul operație OM, acest câmp va conține lungimea numelui obiect nou. • Pentru tipul operație OW, acest câmp va conține lungimea numelui proprietar nou. • Pentru tipurile de operație PO, ZC, AF+M, sau AF+P, acest câmp va conține lungimea listei de tipuri de attribute modificate din câmpul Nume nou.
			6357	6743	Nume nou ¹	Char(2002)	<p>Numele nou. Acest câmp este folosit doar dacă tipul operației (J5 offset 611) este OM, OW, PO, ZC, AF+M sau AF+P.</p> <ul style="list-style-type: none"> • Pentru tipul operație OM, acest câmp va conține numele obiect nou. • Pentru tipul operație OW, acest câmp va conține numele proprietar nou. • Pentru tipurile de operație PO, ZC, AF+M sau AF+P, acest câmp va conține lungimea listei de tipuri de attribute modificate.
			8359	8745	ID fișier obiect ²	Char(16)	ID-ul fișier al obiectului pentru exportare.
			8375	8761	Nume ASP ²	Char(10)	Numele dispozitivului ASP.
			8385	8771	Număr ASP ²	Char(5)	Numărul dispozitivului ASP.
			8390	8776	Nume cale CCSID ²	Bin(5)	Identificatorul de set de caractere codat al numelui de cale absolută.
			8394	8780	ID regiune sau țară nume cale ²	Char(2)	ID regiune sau țară al numelui de cale absolută.
			8396	8782	ID limbă nume cale ²	Char(3)	ID-ul limbă pentru numele de cale absolută.
			8399	8785	Lungime nume cale ²	Bin(4)	Lungimea numelui căii absolute.
			8401	8787	Indicator nume cale ²	Char(1)	Indicator nume cale.
						Y	Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect.
						N	Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.

Disponere intrări jurnal de auditare

Tabela 166. Intrări jurnal DI (Directory Server) (continuare). Fișier descriere câmp QASYDIJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	8402	8788	ID fișier înrudit ^{2,3}	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	8418	8804	Nume cale ^{1,2}	Char(5002)	Numele căii obiectului.
		13806	Profil utilizator local	Char(10)	Numele profil utilizator local care este mapat la numele utilizator LDAP (J5 offset 719). Spațiul gol indică faptul că nici un profil utilizator nu este mapat.
		13816	Indicator administrator	Char(1)	Indicatorului administrator pentru numele utilizator LDAP (J5 offset 719). Y Utilizatorul LDAP este un administrator. N Utilizatorul LDAP nu este un administrator. U Nu este cunoscut acum dacă utilizatorul LDAP este un administrator.
		13817	Proxy ID CCSID	Bin(5)	identificator set de caractere codate (CCSID) al ID-ului proxy.
		13822	Lungime ID proxy	Bin(4)	Lungimea ID-ului proxy.
		13826	ID proxy ¹	Char(2002)	Numele ID-ului proxy. Acest câmp este folosit când controlul autorizației proxy est folosit pentru a cere ca o operație să fie făcută sub autorizația ID-ului proxy sau pentru un bind SASL în care clientul a specificat un ID de autorizare diferit de ID-ul bind.
	¹ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea valorii din câmp.				
	² Aceste câmpuri sunt folosite doar dacă tipul operației (J5 offset 611) este EX sau IM.				
	³ Dacă câmpul indicator nume de cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				

Tabela 167. Intrări jurnal DO (Operație ștergere). Fișier descriere câmp QASYDOJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Obiectul a fost șters sub controlul comiterii C A fost comisă ștergere în așteptare a obiectului D O creare în așteptare a obiectului a fost rulată înapoi. P Ștergerea obiectului este în curs (ștergerea a fost realizată sub controlul comiterii) R O ștergere în așteptare a obiectului a fost rulată înapoi.
157	225	611	Nume obiect	Char(10)	Numele obiectului.

Tabela 167. Intrări jurnal DO (Operație ștergere) (continuare). Fișier descriere câmp QASYDOJE/J4/J5

Offset			Câmp	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		(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.
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 setului de caractere codate pentru numele obiect.
332	400	786	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.
334	402	788	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fișier părinte ^{1,2}	Char(16)	ID-ul fișierului directorului părinte.
356	424	810	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
372	440	826	Nume obiect ¹	Char(512)	Numele obiectului.
	952	1338	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1011	1397	Nume cale ⁴	Char(5002)	Numele căii obiectului.

Disponere intrări jurnal de auditare

Tabela 167. Intrări jurnal DO (Operație ștergere) (continuare). Fișier descriere câmp QASYDOJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1					Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.
2					Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.
3					Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.
4					Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.
5					Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este în bibliotecă, acestea sunt informațiile ASP pentru obiect.

Tabela 168. Intrări jurnal DS (Resetare ID utilizator unelte service furnizate de IBM). Fișier descriere câmp QASYDSJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Resetare parolă ID utilizator unelte service. C Modificat cu un ID utilizator unelte service. P Parola ID utilizator unelte service a fost modificată.
157	225	611	Resetare ID utilizator unelte service furnizate de IBM	Char(1)	Y Cerere pentru resetare ID utilizator unelte service furnizate de IBM
158	226	612	Tip ID utilizator unelte service	Char(10)	Tipul ID utilizator unelte service *SECURITY *FULL *BASIC
168	236	622	Nume nou ID utilizator unelte service	Char(8)	Numele ID utilizator unelte service.
176	244	630	Modificare parolă ID utilizator unelte service	Char(1)	Cerere pentru modificarea parolei ID utilizator unelte service. Y Cerere de modificare parolă ID utilizator unelte service.
	245	631	Nume nou ID utilizator unelte service	Char(10)	Numele ID utilizator unelte service.
	255	641	Profil care cere ID utilizator unelte service	Char(10)	Numele ID-ului utilizator unelte service care a cerut modificarea.

Tabela 169. Intrări jurnal EV (variabilă mediu). Fișier descriere câmp QASYEVJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
	224	610	Tip intrare	Char(1)	Tipul intrării. A Adăugare C Modificare D Ștergere
	225	611	Nume trunchiat	Char(1)	Indică dacă este trunchiat numele variabilei de mediu (offset 232). Y Numele variabilă de mediu trunchiat. N Numele variabilă de mediu netrunchiat.
	226	612	CCSID	Binary(5)	CCSID-ul numelui variabilei de mediu.
	230	616	Lungime	Binary(4)	Lungimea numelui variabilei de mediu.
	232	618	Nume variabilă de mediu ²	Char(1002)	Numele variabilei de mediu.
	1234	1620	Nume nou trunchiat ¹	Char(1)	Indică dacă este trunchiat numele nou al variabilei de mediu (offset 1241). Y Valoare variabilă de mediu trunchiată. N Valoare variabilă de mediu netrunchiată.
	1235	1621	Nume nou CCSID ¹	Binary(5)	CCSID-ul numelui variabilă de mediu nou.
	1239	1625	Lungime nume nou ¹	Binary(4)	Lungimea numelui noii variabilei de mediu.
	1241	1627	Nume nou variabilă de mediu ^{1,2}	Char (1002)	Numele nou variabilă de mediu.

¹ Aceste câmpuri sunt folosite când tipul intrării este C.

² Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui variabilei de mediu.

Tabela 170. Intrări jurnal GR (înregistrare generică). Fișier descriere câmp QASYGRJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru menționarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. A Adăugare ieșire program C Monitorizare operații resursă și operații de control D Ieșire de program înlăturată. F Operații de înregistrare funcție. R Ieșire de program înlocuită.

Disponere intrări jurnal de auditare

Tabela 170. Intrări jurnal GR (înregistrare generică) (continuare). Fișier descriere câmp QASYGRJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	225	611	Acțiune	Char(2)	Acțiune executată. ZC Modificare
	227	613	Nume utilizator	Char(10)	ZR Citire Nume profil utilizator Pentru tipul de intrare F, acest câmp conține numele utilizatorului pentru care a fost executată funcția de înregistrare funcție.
	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 170. Intrări jurnal GR (înregistrare generică) (continuare). Fișier descriere câmp QASYGRJ4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	243	629	Câmp 1	Char(102) ¹	<p>Date câmp 1</p> <p>Pentru tipul de intrare F, acest câmp conține descrierea operației de înregistrare funcție care a fost executată. Valorile posibile sunt:</p> <p>*REGISTER: Funcția a fost înregistrată</p> <p>*REREGISTER: Funcția a fost actualizată</p> <p>*DEREGISTER: A fost anulată înregistrarea funcției</p> <p>*CHGUSAGE: Informațiile de folosire funcție au fost modificate</p> <p>*CHKUSAGE: Folosirea de funcție a fost verificată pentru un utilizator și verificarea a avut succes</p> <p>*USAGEFAILURE: Folosirea de funcție a fost verificată pentru un utilizator și verificarea nu a avut succes</p> <p>Pentru tipurile de intrare A, D și R, acest câmp va conține informațiile program de ieșire pentru respectiva funcție care a fost executată.</p> <p>Pentru tipul de intrare C, acest câmp conține numele funcției RMC care este încercat. Valorile posibile sunt:</p> <ul style="list-style-type: none"> • mc_reg_event_select Înregistrează eveniment folosind selecția 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 Definește resursă nouă • mc_undefine_resource Nedefinește resursă • mc_set_select Setează valorile atribut resursă folosind selecția 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 selecția de atribute • mc_query_d_select Cerere atribute dinamice resursă folosind selecția de atribute

Disponere intrări jurnal de auditare

Tabela 170. Intrări jurnal GR (înregistrare generică) (continuare). Fișier descriere câmp QASYGRJ4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
243 (cont)					<ul style="list-style-type: none"> • 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 persistente clasă de resurse mc_class_query_d Cerere atribute dinamice clasă de resurse mc_qdef_resource_class Cerere definiție clasă de resurse mc_qdef_p_attribute Cerere definiție atribut persistent mc_qdef_d_attribute Cerere definiție atribut dinamic mc_qdef_sd Cerere de date structurate mc_qdef_valid_values Cerere definiție pentru valori valide de atribut persistent mc_qdef_actions Cerere definiție acțiuni resursă mc_invoke_action Invocare acțiune pentru resursă mc_invoke_class_action Invocare acțiune 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 conține numele funcției pe care s-a lucrat.
					Pentru tipul de intrare C, acest câmp conține numele resursei sau clasei de resurse pentru care a fost încercată operația.
	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 170. Intrări jurnal GR (înregistrare generică) (continuare). Fișier descriere câmp QASYGRJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	459	845	Câmp 3	Char(102) ¹	<p>Date câmp 3.</p> <p>Pentru tipul de intrare F, acest câmp conține setarea de folosire pentru un utilizator. Există o valoare pentru acest câmp doar dacă operația de înregistrare funcție este una din următoarele valori:</p> <p>*REGISTER: Când operația este *REGISTER, acest câmp conține valoarea de folosire implicită. Numele utilizator va fi *DEFAULT.</p> <p>*REREGISTER: Când operația este *REREGISTER, acest câmp conține valoarea de folosire implicită. Numele utilizator va fi *DEFAULT.</p> <p>*CHGUSAGE: Când operația este *CHGUSAGE, acest câmp conține valoarea de folosire pentru utilizatorului specificat în câmpul nume utilizator.</p> <p>Pentru tipul de intrare C, acest câmp conține rezultatul pentru orice verificare de autorizații care a fost făcută pentru operația indicată la câmpul 1. Următoarele sunt valori posibile:</p> <ul style="list-style-type: none"> • *NOAUTHORITYCHECKED: Dacă operația indicată la câmpul 1 nu necesită o verificare de autorizație sau dacă, dintr-un motiv oarecare, nu a fost încercată nici o verificare de autorizație. • *AUTHORITYPASSED: Când ID-ul utilizator mapat indicat în Nume profil utilizator a fost admis cu succes de către verificarea de autorizație corespunzătoare pentru operația indicată în câmpul 1 pentru resursa sau clasa de resurse indicate în câmpul 2. • *AUTHORITYFAILED: Când ID-ul utilizator mapat indicat în Nume profil utilizator a eșuat verificarea de autorizație corespunzătoare pentru operația 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	<p>Date câmp 4.</p> <p>Pentru tipul de intrare F, acest câmp conține setarea de permitere *ALLJOB pentru funcție. Există o valoare pentru acest câmp doar dacă operația de înregistrare funcție este una din următoarele valori:</p> <p>*REGISTER</p> <p>*REREGISTER</p>

¹ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea câmpului.

Disponere intrări jurnal de auditare

Tabela 171. Intrări jurnal GS (acordare descriptor). Fișier descriere câmp QASYGSJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. G Acordare descriptor R Primire descriptor U Nu se poate folosi descriptor
157	225	611	Nume job	Char(10)	Numele jobului.
167	235	621	Nume utilizator	Char(10)	Numele utilizatorului.
177	245	631	Număr job	Zoned (6,0)	Numărul jobului.
183	251	637	Nume profil utilizator	Char (10)	Numele profilului utilizator.
	261	647	JUID	Char (10)	Identitatea utilizator job al jobului destinație. (Această valoare se aplică doar la înregistrările de auditare subtipul G)

Tabela 172. Intrări Jurnal IM (Intrusion Monitor - Monitorizare intruziuni). QASYIMJE/J4/J5 Fișier descriere de câmp

Offset			Câmp	Format	Descriere
JE	J4	J5			
		1			Câmpurile antet comune pentru toate tipurile de intrări.
		610	Tip intrare	Char(1)	Tipul intrării. P Detectare potențial 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 locația 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.
		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 distanță	Char(1)	Adresă de familie la distanță asociată cu evenimentul detectat.
		694	Număr port la distanță	Zoned(5, 0)	Număr port la distanță asociat cu evenimentul detectat.
		699	Adresă IP la distanță	Char(46)	Adresă IP la distanță asociată cu evenimentul detectat.

Tabela 172. Intrări Jurnal IM (Intrusion Monitor - Monitorizare intruziuni) (continuare). QASYIMJE/J4/J5 Fișier descriere de câmp

Offset					
JE	J4	J5	Câmp	Format	Descriere
		745	Identificator de tip Probe	Char(6)	Identifică tipul de probe folosit pentru a detecta potențiale intruziuni. Valorile posibile includ: ATTACK Eveniment detectat de acțiunea Attack TR Eveniment detectat de acțiunea TR (trace - urmărire) SCANG Eveniment detectat de acțiunea scanare globală (global Scan) SCANE Eveniment detectat de acțiunea Scan
		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 informații despre detectarea intruziunilor.
		755	Tip eveniment	Char(8)	Identifică tipul de intruziune potențială care a fost detectată. Valorile posibile sunt: MALFPKT Pachet format greșit FLOOD Eveniment inundație (flood) ICMPRED redirecționare ICMP (Internet Control Message Protocol) PERPECH Ecou continuu IPFRAG fragment IP RESTPROT Protocol IP restricționat
		763	Rezervat	Char(20)	
		783	Pachet suspectat	Char(1002) ¹	Un câmp de lungime variabilă care poate conține până la primii 1000 de octeți ai pachetului IP asociat cu evenimentul detectat. Acest câmp conține date binare și ar trebui tratat ca și cum ar avea un CCSID de 65535.

¹ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea informației pachetului suspectat.

Tabela 173. Intrări jurnal IP (comunicații între procese). Fișier descriere câmp QASYIPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Disponere intrări jurnal de auditare

Tabela 173. Intrări jurnal IP (comunicații între procese) (continuare). Fișier descriere câmp QASYIPJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificări de autorizare și/sau proprietate C Creare D Ștergere F Eșuare autorizare G Obținere M Atașare memorie partajată Z Semafor normal închis sau detașare memorie partajată
157	225	611	Tip IPC	Char(1)	Tip IPC M Memorie partajată N Semafor normal Q Coadă 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 și 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 și scriere
208	276	662	Autorizare publică	Char(3)	Autorizare publică la entitatea IPC *R citire *W scriere *RW citire și 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 conțin lungimea numelui semaforului.

Tabela 174. Intrări jurnal IR (Acțiuni reguli IP). Fișier descriere câmp QASYIRJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. L Au fost încărcate reguli IP de pe un fișier. 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 și copiate într-un fișier. U Au fost descărcate (înlăturate) reguli.
	225	611	Nume fișier	Char(10)	Numele fișierului QSYS folosit pentru a încărca sau primi regulile IP. Această valoare este goală dacă fișierul folosit nu a fost în sistemul de fișiere QSYS.
	235	621	Biblioteca fișiere	Char(10)	Numele bibliotecii fișiere QSYS.
	245	631	Rezervat	Char(18)	
	263	649	Lungime nume fișier	Binary (4)	Lungimea numelui fișier.
	265	651	CCSID nume fișier ¹	Binary (5)	Identificatorul set de caractere codat pentru numele fișier.
	269	655	ID fișier regiune sau țară ¹	Char(2)	ID-ul de regiune sau țară pentru numele fișier.
	271	657	ID limbă fișier ¹	Char(3)	ID-ul limbă pentru numele fișierului.
	274	660	Rezervat	Char(3)	
	277	663	ID fișier părinte ^{1, 2}	Char(16)	ID-ul fișierului directorului părinte.
	293	679	ID fișier obiect ^{1, 2}	Char(16)	ID-ul fișier al fișierului.
	309	695	Nume fișier ¹	Char(512)	Numele fișierului.
	821	1207	Secvență conexiune	Char(40)	Numele conexiunii.
	861	1247	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	898	1284	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	901	1287	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.

Disponere intrări jurnal de auditare

Tabela 174. Intrări jurnal IR (Acțiuni reguli IP) (continuare). Fișier descriere câmp QASYIRJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	903	1289	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	904	1290	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	920	1306	Nume cale ⁴	Char(5002)	Numele căii obiectului.
¹	Aceste câmpuri sunt folosite doar pentru obiectele din QOpenSys și sistemul de fișiere "root".				
²	Dacă ID-ul are cel mai din stânga bit setat și restul de biți zero, ID-ul nu este setat.				
³	Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				
⁴	Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea câmpului.				
⁵	Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.				

Tabela 175. Intrări jurnal IS (gestiune securitate internet). Fișier descriere câmp QASYISJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru menționarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. A Eșuare (acest tip nu mai este folosit) C Normal (acest tip nu mai este folosit) U Utilizator mobil (acest tip nu mai este folosit) 1 Negociere IKE fază 1 SA 2 Negociere IKE fază 2 SA
	225	611	Adresă IP locală	Char(15)	Adresă IP locală.
	240	626	Port ID client local	Char(5)	Port ID client local.
	245	631	Adresă IP la distanță	Char (15)	Adresă IP la distanță.
	260	646	Port ID client la distanță	Char (5)	Port ID client la distanță (valid pentru faza 2).
	265	651	ID mobil	Char(256)	ID mobil. Acest câmp nu mai este folosit.

Tabela 175. Intrări jurnal IS (gestiune securitate internet) (continuare). Fișier descriere câmp QASYISJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	521	907	Codul rezultat	Char(4)	Rezultat negociere: 0 Cu succes 1–30 Erori specifice protocol (documentate în ISAKMP RFC2408, găsit la: http://www.ietf.org) 82xx erori specifice iSeries VPN Key Manager
	525	911	CCSID	Bin(5)	Identificatorul set de caractere codat • ID local • Valoare ID client local • ID la distanță • Valoare ID client la distanță
	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 Subrețea IP versiunea 4 7 Interval adresă IP versiunea 4 9 Nume distinctiv 11 Identificator cheie
	787	1173	Valoare ID client local	Char(256)	ID client local (valid pentru faza 2)
	1043	1429	Protocol ID client local	Char(4)	Protocol ID client local (valid pentru faza 2)
	1047	1433	ID la distanță	Char(256)	Identificator IKE la distanță
	1303	1689	Tip ID client la distanță	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 Subrețea IP versiunea 4 7 Interval adresă IP versiunea 4 9 Nume distinctiv 11 Identificator cheie
	1305	1691	Valoare ID client la distanță	Char(256)	ID client la distanță (valid pentru faza 2)
	1561	1947	Protocol ID client la distanță	Char(4)	Protocol ID client la distanță (valid pentru faza 2)

Disponere intrări jurnal de auditare

Tabela 176. Intrări jurnal JD (modificare descriere job). Fișier descriere câmp QASYJDJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Profilul utilizator specificat pentru parametrul USER al descrierii de job
157	225	611	Descriere job	Char(10)	Numele descrierii de job modificate care a avut parametrul USER modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii 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 CHGJOB (Change Job Description - Modificare descriere job) CRT comanda CRTJOB (Create Job Description - Creare descriere job)
188	256	642	Utilizator vechi	Char(10)	Numele profilului utilizator specificat pentru parametrul USER înainte ca descrierea de job să se fi modificat.
198	266	652	Utilizator nou	Char(10)	Numele profilului USER specificat pentru parametrul utilizator înainte ca descrierea de job să se fi modificat.
		662	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOB
		672	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOB

Tabela 177. Intrări jurnal JS (modificare job). Fișier descriere câmp QASYJSJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 177. Intrări jurnal JS (modificare job) (continuare). Fișier descriere câmp QASYJSJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare	Char(1)	Tipul intrării. A comanda ENDJOBABN B Lansare C Modificare E Terminare H Reținere 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 Atașare 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

Disponere intrări jurnal de auditare

Tabela 177. Intrări jurnal JS (modificare job) (continuare). Fișier descriere câmp QASYJSJE/J4/J5

Offset			Câmp	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 Cerere T MRT U Utilizator spool alternativ
159	227	613	Nume job	Char(10)	Prima parte a numelui de job calificat pe care se operează.
169	237	623	Nume utilizator job	Char(10)	A doua parte a numelui de job calificat pe care se operează.
179	247	633	Număr job	Char(6)	A treia parte a numelui de job calificat pe care se operează.
185	253	639	Nume dispozitiv	Char(10)	Numele dispozitivului
195	263	649	Profil utilizator efectiv ²	Char(10)	Numele profilului utilizator efectiv pentru firul de execuție
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 ieșire	Char(10)	Numele cozii de ieșire pentru job
255	323	709	Bibliotecă coadă ieșire	Char(10)	Numele bibliotecii pentru coada de ieșire
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 execuție
715	783	1169	Profiluri grup suplimentare ²	Char(150)	Numele profilurilor grup suplimentare pentru firul de execuție.
	933	1319	Descriere JUID	Char(1)	Descrie înțelesul câmpului JUID: ' ' Câmpul JUID conține valoarea pentru JOB. C API-ul JUID de curățare a fost apelat. Câmpul JUID conține noua valoare. S API-ul JUID de setare a fost apelat. Câmpul JUID conține noua valoare.
	934	1320	Câmp JUID	Char(10)	Conține valoarea JUID
	944	1330	Profil utilizator real	Char(10)	Numele profilului utilizator real pentru firul de execuție.
	954	1340	Profil utilizator salvat	Char(10)	Numele profilului utilizator salvat pentru firul de execuție.

Tabela 177. Intrări jurnal JS (modificare job) (continuare). Fișier descriere câmp QASYJSJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	964	1350	Profil grup real	Char(10)	Numele profilului de grup real pentru firul de execuție.
	974	1360	Profil grup salvat	Char(10)	Numele profilului de grup salvat pentru firul de execuție.
	984	1370	Utilizator real modificat ³	Char(1)	Profilul utilizator real a fost modificat. Y Da N Nu
	985	1371	Utilizator efectiv modificat ³	Char(1)	Profilul utilizator efectiv a fost modificat. Y Da N Nu
	986	1372	Utilizator salvat modificat ³	Char(1)	Profilul utilizator salvat a fost modificat Y Da N Nu
	987	1373	Grup real modificat ³	Char(1)	Profilul grup real a fost modificat. Y Da N Nu
	988	1374	Grup efectiv modificat ³	Char(1)	Profilul grup efectiv a fost modificat. Y Da N Nu
	989	1375	Grup salvat modificat ³	Char(1)	Profilul grup salvat a fost modificat. Y Da N Nu
	990	1376	Grupuri suplimentare modificate ³	Char(1)	Profilurile grup suplimentare au fost modificate. Y Da N Nu
	991	1377	Numărul listă biblioteci ⁴	Bin(4)	Numărul de biblioteci din câmpul extensie listă de biblioteci (offset 993).
	993	1379	Extensie listă de biblioteci ^{4,5}	Char(2252)	Extensia la lista de biblioteci pentru job.
		3631	Grup ASP ASP de biblioteci	Char(10)	Grup ASP ASP de biblioteci
		3641	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOB
		3651	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOB
		3656	Nume fus orar	Char(10)	Nume descriere fus orar
		3666	Nume job ieșire	Char(10)	Numele jobului care a întrerupt jobul curent sau numele jobului care a fost întrerupt de către jobul curent
		3676	Utilizator job ieșire	Char(10)	Numele utilizatorului care a întrerupt jobul curent sau numele jobului care a fost întrerupt de către jobul curent
		3686	Număr job ieșire ^{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 ieșire ⁶	Char(10)	Programul de ieșire întrerupea jobul
		3702	Biblioteca program ieșire ⁶	Char(10)	Numele de bibliotecă al programului de ieșire întrerupea jobul

Disponere intrări jurnal de auditare

Tabela 177. Intrări jurnal JS (modificare job) (continuare). Fișier descriere câmp QASYJSJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1					Acest câmp este gol dacă jobul este în coada de mesaje și nu rulează.
2					Când înregistrarea de auditare JS este generată din cauză că un job execută o operație într-un alt job, atunci acest câmp va conține date din firul de execuție inițial al jobului pe care se operează. În toate celelalte cazuri, câmpul va conține date din firul de execuție care a executat operația.
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 depășește dimensiunea câmpului la offset-ul 729.
5					Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin 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 conține informații despre jobul care va fi întrerupt. Când tipul intrării este K sau L acest câmp conține informații despre jobul care a cerut întreruperea jobului curent.

Tabela 178. Intrări jurnal KF (Fișier inel de chei). Fișier descriere câmp QASYKFJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. C Operație certificat K Operație fișier inel de chei P Parolă incorectă T Operație rădăcină de încredere
	225	611	Operație certificat	Char(3)	Tip acțiune ⁴ . ADK Certificat cu cheie privată adăugată ADD Certificat adăugat REQ Certificat cerut SGN Certificat semnat

Tabela 178. Intrări jurnal KF (Fișier inel de chei) (continuare). Fișier descriere câmp QASYKFJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	228	614	Operație inel de chei	Char(3)	Tip acțiune 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 fișier PWD Modifică parola fișier inel de chei RMV Pereche inele chei înlăturată INF Extragere informații pereche inel de chei 2DB Fișier inel de chei convertit la un format bază de date de chei 2YR fișier bază de date de chei convertit la fișier inel de chei
	231	617	Operație root de încredere	Char(3)	Tip acțiune 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 fișier inel de chei
	254	640	CCSID nume obiect	Binary(5)	CCSID nume fișier inel de chei
	258	644	ID regiune sau țară nume obiect	Char(2)	ID țară sau regiune nume fișier inel de chei
	260	646	ID limbă nume obiect	Char(3)	ID limbă nume fișier inel de chei
	263	649	Rezervat	Char(3)	
	266	652	ID fișier părinte	Char(16)	OD fișier director părinte inel de chei
	282	668	ID fișier obiect	Char(16)	Nume fișier director inel de chei
	298	684	Nume obiect	Char(512)	Nume fișier inel de chei
	810	1196	Rezervat	Char(18)	
	828	1214	Lungime nume obiect	Binary(4)	Lungime nume fișier destinație sau sursă
	830	1216	CCSID nume obiect	Binary(5)	CCSID nume fișier destinație sau sursă
	834	1220	ID regiune sau țară nume obiect	Char(2)	ID regiune sau țară nume fișier destinație sau sursă
	836	1222	ID limbă nume obiect	Char(3)	ID limbă nume fișier destinație sau sursă.
	839	1225	Rezervat	Char(3)	
	842	1228	ID fișier părinte	Char(16)	ID fișier director părinte destinație sau sursă.
	858	1244	ID fișier obiect	Char(16)	ID fișier director destinație sau sursă
	874	1260	Nume obiect	Char(512)	Nume fișier destinație sau sursă.

Disponere intrări jurnal de auditare

Tabela 178. Intrări jurnal KF (Fișier inel de chei) (continuare). Fișier descriere câmp QASYKFJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1386	1772	Lungime etichetă certificat	Binary(4)	Lungime etichetă certificat.
	1388	1774	Etichetă certificat ¹	Char(1026)	Etichetă certificat.
	2414	2800	ID fișier obiect	Char(16)	ID fișier 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 țară nume cale	Char(2)	ID-ul regiune sau țară pentru numele cale absolută.
	2451	2837	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	2454	2840	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	2456	2842	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru fișierul inel de chei. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	2457	2843	ID fișier înrudit ²	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	2473	2859	Nume cale absolută ¹	Char(5002)	Numele cale absolută al fișierului inel de chei.
	7475	7861	ID fișier obiect	Char(16)	ID-ul fișier al fișierului destinație sau sursă.
	7491	7877	Nume ASP	Char(10)	Nume ASP fișier destinație sau sursă
	7501	7887	Număr ASP	Char(5)	Număr ASP fișier destinație sau sursă
	7506	7892	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii.
	7510	7896	ID regiune sau țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	7512	7898	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	7515	7901	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.

Tabela 178. Intrări jurnal KF (Fișier inel de chei) (continuare). Fișier descriere câmp QASYKFJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	7517	7903	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru fișierul destinație sau sursă. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	7518	7904	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	7534	7920	Nume cale absolută ¹	Char(5002)	Numele cale absolută al fișierului destinație sau sursă.
¹	Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.				
²	Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				
³	Când indicatorul de nume cale (offset 7517) este "N", acest câmp va conține ID-ul de fișier relativ al numelui căii absolute la offset-ul 7534. Când indicatorul de nume cale este "Y", acest câmp va conține 16 octeți de zerouri hexa.				
⁴	Câmpul va conține spații goale când nu este o operație de certificat.				
⁵	Câmpul va conține spații goale când nu este o operație de fișier inel de chei.				
⁶	Câmpul va conține spații goale când nu este o operație de root de încredere.				

Tabela 179. Intrări jurnal LD (director de căutare, legare, dezlegare). Fișier descriere câmp QASYLDJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. L Legare director U Dezlegare director K Căutare director
157	225	611	(Zonă rezervată)	Char(20)	
	243	629	Lungime nume obiect ¹	Binary (4)	Lungimea numelui obiectului.
177	245	631	CCSID nume obiect ¹	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
181	249	635	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.

Disponere intrări jurnal de auditare

Tabela 179. Intrări jurnal LD (director de căutare, legare, dezlegare) (continuare). Fișier descriere câmp QASYLDJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
183	251	637	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
186	254	640	(Zonă rezervată)	Char(3)	
189	257	643	ID fișier părinte ^{1,2}	Char(16)	ID-ul fișierului directorului părinte.
205	273	659	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
221	289	675	Nume obiect ¹	Char(512)	Numele obiectului.
	801	1187	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	838	1224	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	841	1227	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	843	1229	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	844	1230	ID fișier înrudit ₁	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	860	1246	Nume cale ²	Char(5002)	Numele căii obiectului.

¹ Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

² Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

Tabela 180. Intrări jurnal ML (Acțiuni mail). Fișier descriere câmp QASYMLJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
157	225	611	Profil utilizator	Char(10)	O Istoric de poștă deschis Nume profil utilizator.

Tabela 180. Intrări jurnal ML (Acțiuni mail) (continuare). Fișier descriere câmp QASYMLJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
167	235	621	ID utilizator	Char(8)	Identificator utilizator
175	243	629	Adresă	Char(8)	Adresă utilizator

Tabela 181. Intrări jurnal NA (Modificare atribut). Fișier descriere câmp QASYNAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificare la atributul rețea. 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.

Tabela 182. Intrări de jurnal ND (Filtru de căutare director APPN). Fișier descriere câmp QASYNDJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 locație CP filtrat	Char(8)	Nume locație CP filtrat.
181	249	635	NETID locație CP filtrat	Char(8)	NETID locație CP filtrat.
189	257	643	Nume locație partener	Char(8)	Nume locație partener.
197	265	651	NETID locație partener	Char(8)	NETID locație partener.
205	273	659	Sesiune intrare	Char(1)	Sesiune intrare. Y Aceasta este o sesiune intrare N Aceasta nu este o sesiune intrare

Disponere intrări jurnal de auditare

Tabela 182. Intrări de jurnal ND (Filtru de căutare director APPN) (continuare). Fișier descriere câmp QASYNDJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
206	274	660	Sesiune ieșire	Char(1)	Sesiune ieșire. Y Aceasta este o sesiune ieșire N Aceasta nu este o sesiune ieșire

Pentru informații suplimentare despre Filtrul de căutare director și Punctul final APPN, vedeți Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Tabela 183. Intrări de jurnal NE (Filtru punct final APPN). Fișier descriere câmp QASYNEJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Violare filtru punct final.
157	225	611	Nume locație locală	Char(8)	Nume locație locală.
165	233	619	Nume locație la distanță	Char(8)	Nume locație la distanță.
173	241	627	NETID la distanță	Char(8)	NETID la distanță.
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 ieșire	Char(1)	Sesiune ieșire. Y Aceasta este o sesiune ieșire N Aceasta nu este o sesiune ieșire

Pentru informații suplimentare despre Filtrul de căutare director și Punctul final APPN, vedeți Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii).

Tabela 184. Intrări jurnal OM (Modificare gestiune obiect). Fișier descriere câmp QASYOMJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. M Obiect mutat la o bibliotecă diferită. R Obiect redenumit.

Tabela 184. Intrări jurnal OM (Modificare gestiune obiect) (continuare). Fișier descriere câmp QASYOMJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
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)	
	497	883	Lungime nume cale	Binary(4)	Lungimea câmpului nume obiect vechi.
431	499	885	CCSID nume obiect ¹	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
435	503	889	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.
437	505	891	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
440	508	894	(Zonă rezervată)	Char(3)	
443	511	897	Fișier părinte vechi ^{1,2}	Char(16)	ID-ul fișier al directorului părinte vechi.
459	527	913	ID fișier obiect vechi ^{1,2}	Char(16)	ID-ul fișier al obiectului vechi.
475	543	929	Nume obiect vechi ¹	Char(512)	Numele obiectului vechi.
987	1055	1441	ID fișier părinte nou ^{1,2}	Char(16)	ID fișier al directorului părinte nou.
1003	1071	1457	Nume obiect nou ^{1, 2, 6}	Char(512)	Numele nou al obiectului.
	1583	1969	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier 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.

Disponere intrări jurnal de auditare

Tabela 184. Intrări jurnal OM (Modificare gestiune obiect) (continuare). Fișier descriere câmp QASYOMJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1618	2004	ID regiune sau țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	1620	2006	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1623	2009	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1625	2011	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1626	2012	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1642	2028	Nume cale absolută ⁵	Char(5002)	Numele cale absolută vechi al obiectului.
	6644	7030	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	6681	7067	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	6684	7070	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	6686	7072	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	6687	7073	ID fișier înrudit ⁴	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	6703	7089	Nume cale absolută ⁵	Char(5002)	Numele cale absolută nou al obiectului.

Tabela 184. Intrări jurnal OM (Modificare gestiune obiect) (continuare). Fișier descriere câmp QASYOMJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1					Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.
2					Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.
3					Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.
4					Când indicatorul de nume cale (offset 6686) este "N", acest câmp va conține ID-ul de fișier relativ al numelui căii absolute la offset-ul 6703. Când indicatorul de nume cale este "Y", acest câmp va conține 16 octeți de zerouri hexa.
5					Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.
6					Nu există nici un câmp lungime asociat pentru această valoare. Șirul este completat cu null dacă nu este de lungime de 512 caractere.
7					Dacă obiectul vechi este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul vechi nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.
8					Dacă obiectul nou este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nou nu este în bibliotecă, acestea sunt informațiile ASP pentru obiect.

Tabela 185. Intrări jurnal OR (restaurare obiect)(. Fișier descriere câmp QASYORJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 moștenire. Y A fost restaurat un program în stare sistem. N A fost restaurat un program în stare utilizator.

Disponere intrări jurnal de auditare

Tabela 185. Intrări jurnal OR (restaurare obiect)((continuare). Fișier descriere câmp QASYORJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
206	274	660	Comanda sistem 2	Char(1)	<p>Y A fost restaurată o comandă sistem.</p> <p>N A fost restaurată o comandă în stare utilizator.</p>
207	275	661	(Zonă rezervată)	Char(18)	Indicatorul mod SETUID.
			Mod SETUID	Char(1)	
	276	662	Mod SETGID	Char(1)	Indicatorul mod SETGID.
					<p>Y Bitul mod SETGID pentru obiectul restaurat este activ.</p> <p>N Bitul mod SETGID pentru obiectul restaurat nu este activ.</p>
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 potrivește cu conținutul obiectului	
				I Semnătură ignorată	
				N Obiect de nesemnat	
				S Semnătura este validă	
				T Semnătură fără încredere	
				U Obiect nesemnat	
				278	664
	279	(Zonă rezervată)	Char(14)	Atributul obiectului.	
		Atribut obiect	Char(10)		
		(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)	Folderul în care a fost restaurat DLO.
255	323	709	Cale folder restaurare	Char(63)	
318	386	772	Nume DLO salvare	Char(12)	Numele DLO al obiectului salvat.
330	398	784	(Zonă rezervată)	Char(8)	

Tabela 185. Intrări jurnal OR (restaurare obiect)((continuare). Fișier descriere câmp QASYORJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
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	479	865	(Zonă rezervată)	Char(20)	
	497	883	(Zonă rezervată)	Char(18)	
			Lungime nume cale	Binary (4)	Lungimea câmpului Nume obiect vechi.
431	499	885	CCSID nume obiect ³	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
435	503	889	ID regiune sau țară nume obiect ³	Char(2)	ID-ul regiunii sau țării 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 fișier părinte ^{3,4}	Char(16)	ID-ul fișierului directorului părinte.
459	527	913	ID fișier obiect ^{3,4}	Char(16)	ID-ul fișier al obiectului.
475	543	929	Nume obiect ³	Char(512)	Numele obiectului.
	1055	1441	ID fișier vechi	Char(16)	ID-ul fișier al obiectului vechi.
	1071	1457	ID fișier mediu	Char(16)	ID-ul fișier (FID) care a fost restaurat în fișierul de mediu.
					Notă: FID-ul memorat pe mediu este FID-ul pe care l-a avut obiectul în sistemul sursă.
	1087	1473	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	1124	1510	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1127	1513	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1129	1515	Indicator nume cale	Char(1)	Indicator nume cale:
				Y	Câmpul Nume cale conține numele căii absolute complete pentru obiect.
				N	Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1130	1516	ID fișier înrudit ⁵	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1146	1532	Nume cale ⁶	Char(5002)	Numele căii obiectului.

Disponere intrări jurnal de auditare

Tabela 185. Intrări jurnal OR (restaurare obiect)((continuare). Fișier descriere câmp QASYORJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1					Acest câmp are o intrare doar dacă obiectul care a fost restaurat este un program.
2					Acest câmp are o intrare doar dacă obiectul care a fost restaurat este o comandă.
3					Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină".
4					Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.
5					Dacă câmpul indicator nume de cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.
6					Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.
7					Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 186. Intrări jurnal OW (modificare drept de proprietate). Fișier descriere câmp QASYOWJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vezi Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
157	225	611	Nume obiect	Char(10)	A Modificare proprietar obiect 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	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 setului de caractere codate pentru numele obiect.
352	420	806	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiunii sau țării pentru numele obiectului.
354	422	808	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
357	425	811	(Zonă rezervată)	Char(3)	
360	428	814	ID fișier părinte ^{1,2}	Char(16)	ID-ul fișierului directorului părinte.

Tabela 186. Intrări jurnal OW (modificare drept de proprietate) (continuare). Fișier descriere câmp QASYOWJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
376	444	830	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
392	460	846	Nume obiect ¹	Char(512)	Numele obiectului.
	972	1358	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	1009	1395	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1012	1398	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1014	1400	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele căii absolute complet pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1015	1401	ID fișier înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
1031	1417	Nume cale ⁴	Char(5002)	Numele căii obiectului.	

¹ Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină".

² Un ID care are bitul cel mai din stânga setat și restul biților 0 indică faptul că ID -ul NU este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este un câmp de lungime variabilă. Primii 2 octeți conțin lungimea numelui căii.

⁵ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP despre obiect.

Tabela 187. Intrări jurnal O1 (Acces optic). fișier descriere câmp QASY01JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Disponere intrări jurnal de auditare

Tabela 187. Intrări jurnal O1 (Acces optic) (continuare). fișier descriere câmp QASY01JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
156	224	610	Tip intrare.	Char(1)	R-Citire U-Actualizare D-Ștergere C-Creare director X-Eliberare fișier reținut
157	225	611	Tip obiect	Char(1)	F-Fișier D-Sfârșit director S-Spațiu de stocare
158	226	612	Tip acces	Char(1)	D-Date fișier A-Atribute director fișier R-Restaurare operație S-Salvare operație
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 fișier/director optic
		929	Nume ASP	Char(10)	Nume ASP pentru bibliotecă CSI
		939	Număr ASP	Char(5)	Număr ASP pentru bibliotecă CSI

Notă: Această intrare este folosită pentru auditarea următoarelor funcții:

- Deschidere fișier sau director
- Creare director
- Ștergere director fișiere
- Modificare sau extragere atribute
- Eliberare fișier optic reținut

Tabela 188. Intrări jurnal O2 (Acces optic). Fișier descriere câmp QASY02JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare.	Char(1)	C-Copiere R-Redenumire B-Copie de rezervă a directorului sau fișierului S-Salvare fișier reținut M-Mutare fișier
157	225	611	Tip obiect	Char(1)	F-Fișier D-Director

Tabela 188. Intrări jurnal O2 (Acces optic) (continuare). Fișier descriere câmp QASY02JE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
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 fișier/director optic sursă
474	542	928	Nume dispozitiv tgt	Char(10)	Numele LUD bibliotecă destinație
484	552	938	Nume CSI tgt	Char(8)	Numele obiect parte destinație
492	560	946	Bibliotecă CSI tgt	Char(10)	Bibliotecă obiect parte destinație
502	570	956	Nume volum tgt	Char(32)	Nume volum optic destinație
534	602	988	Nume obj tgt	Char(256)	Nume fișier/director optic destinație
		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 destinație	Char(10)	Numele ASP pentru biblioteca CSI destinație
		1269	Numărul ASP pentru biblioteca CSI destinație	Char(5)	Numărul ASP pentru biblioteca CSI destinație

Tabela 189. Intrări jurnal O3 (Acces optic). fișier descriere câmp QASY03JE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru listarea câmpului.
156	224	610	Tip intrare.	Char(1)	<p>A Modificare attribute volum</p> <p>B Volum copie de rezervă</p> <p>C Conversie volum copie de rezervă la volum primar</p> <p>E Exportare</p> <p>I Inițializare</p> <p>K Verificare Volum</p> <p>L Modificare listă autorizări</p> <p>M Importare</p> <p>N Redenumire</p> <p>R Citire absolută</p>
157	225	611	Nume dispozitiv	Char(10)	Nume LUD bibliotecă
167	235	621	Nume CSI	Char(8)	Nume obiect parte

Disponere intrări jurnal de auditare

Tabela 189. Intrări jurnal O3 (Acces optic) (continuare). fișier descriere câmp QASY03JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
175	243	629	Biblioteca CSI	Char(10)	Biblioteca 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 autorizație veche
259	327	713	Listă auth nouă ³	Char(10)	Listă de autorizație 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 conține numele volumului nou pentru funcțiile Inițializare, Redenumire și Conversie; el conține numele volumului copie de rezervă pentru funcțiile Copiere de rezervă. El conține numele volum pentru Importare, Exportare, Modificare listă autorizație, Modificare attribute volum și Citire sector.				
²	Folosit doar pentru Importare, Exportare și Modificare listă autorizație.				
³	Folosit doar pentru Modificare listă autorizație.				
⁴	Folosit doar pentru Citire sector.				

Tabela 190. Intrări jurnal PA (Adoptare program). Fișier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificați programul pentru a adopta autorizarea proprietarului. J Programul Java adoptă autorizarea proprietarului. M Modificați valorile SETUID, SETGID ale obiectului sau Redenumirea restricționată și indicatorul mod dezlegare.
157	225	611	Nume program ³	Char(10)	Numele programului.
167	235	621	Biblioteca 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 restricționată și 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.

Tabela 190. Intrări jurnal PA (Adoptare program) (continuare). Fișier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	263	649	Rezervat	Char(17)	
	281	667	Lungime nume obiect ¹	Binary (4)	Lungimea numelui obiectului.
	283	669	CCSID nume obiect ¹	Binary(5)	identificator de set de caractere codate pentru numele obiect.
	287	673	ID regiune sau țară nume obiect	Char(2)	ID-ul de regiune sau țară pentru numele obiect.
	289	675	ID limbă nume obiect ¹	Char(3)	ID-ul limbă pentru numele obiectului.
	292	678	Rezervat	Char(3)	
	295	681	ID părinte ^{1, 2, 3}	Char(16)	ID fișier părinte
	311	697	ID fișier obiect ³	Char(16)	ID-ul fișier pentru obiect
	327	713	Nume obiect ¹	Char(512)	Numele obiect pentru obiect.
	839	1225	Mod SETUID	Char(1)	Indicatorul de mod ID utilizator efectiv set (SETUID). Y Bitul de mod SETUID este activ pentru obiect. N Bitul de mod SETUID nu este activ pentru obiect.
	840	1226	Mod SETGID	Char(1)	Indicatorul de mod ID grup efectiv set (SETGID). Y Bitul de mod SETGID este activ pentru obiect. N Bitul de mod SETGID nu este activ pentru obiect.
	841	1227	Proprietar grup primar	Char(10)	Numele proprietarului grup primar.
	851	1237	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	888	1274	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	891	1277	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolut.
	893	1279	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține numele complet pentru calea obiectului, în schimb conține un nume de cale înrudit. Câmpul ID fișier înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale înrudit.
	894	1280	ID fișier director înrudit ⁴	Char(16)	Când câmpul Indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	910	1296	Nume cale ⁵	Char(5002)	Numele căii obiectului.

Disponere intrări jurnal de auditare

Tabela 190. Intrări jurnal PA (Adoptare program) (continuare). Fișier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1					Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină" (/).
2					Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.
3					Când tipul de intrare este "J", câmpurile nume program și nume bibliotecă vor conține "*N". În plus, ID-ul de fișier părinte și ID-ul de fișier obiect vor conține zerouri binare.
4					Dacă câmpul Indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.
5					Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.
6					Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.

Tabela 191. Intrări jurnal PG (Modificare grup primar). Fișier descriere câmp QASYPGJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificați 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	Existență obiect	Char(1)	Y *OBJEXIST
206	274	660	Gestionare obiect	Char(1)	Y *OBJMGT
207	275	661	Operațional obiect	Char(1)	Y *OBJOPR
208	276	662	Modificare obiect	Char(1)	Y *OBJALTER
209	277	663	Referință obiect	Char(1)	Y *OBJREF
210	278	664	(Zonă rezervată)	Char(10)	
220	288	674	Gestionare listă autorizații	Char(1)	Y *AUTLMGT
221	289	675	Autorizare citire	Char(1)	Y *READ
222	290	676	Adăugare autorizare	Char(1)	Y *ADD
223	291	677	Actualizare autorizare	Char(1)	Y *UPD
224	292	678	Ștergere autorizare	Char(1)	Y *DLT
225	293	679	Execuție autorizare	Char(1)	Y *EXECUTE

Tabela 191. Intrări jurnal PG (Modificare grup primar) (continuare). Fișier descriere câmp QASYPGJE/J4/J5

Offset			Câmp	Format	Descriere	
JE	J4	J5				
226	294	680	(Zonă rezervată)	Char(10)		
236	304	690	Excludere autorizare	Char(1)	Y	*EXCLUDE
237	305	691	Revocare grup primar vechi	Char(1)	Y	Revocare autorizare pentru grupul primar anterior.
					' '	Nu revocați autorizarea pentru grupul primar anterior.
238	306	692	(Zonă rezervată)	Char (20)		
258	326	712	Utilizator office	Char(10)		Numele utilizatorului de tip office.
268	336	722	Nume DLO	Char(12)		Numele obiectului bibliotecă documente sau al directorului.
280	348	734	(Zonă rezervată)	Char(8)		
288	356	742	Cale director	Char(63)		Calea directorului.
351	419	805	Office în numele Utilizatorului	Char(10)		Utilizatorul care lucrează în numele altui utilizator.
361			(Zonă rezervată)	Char(20)		
	429	815	(Zonă rezervată)	Char(18)		
	447	833	Lungime nume obiect ¹	Binary (4)		Lungimea numelui obiectului.
381	449	835	CCSID nume obiect ¹	Binary(5)		identificator de set de caractere codate pentru numele obiect.
385	453	839	ID regiune sau țară nume obiect ¹	Char(2)		ID-ul regiune sau țară pentru numele obiect.
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 fișier părinte ^{1,2}	Char(16)		ID-ul fișier al directorului părinte.
409	477	863	ID fișier obiect ^{1,2}	Char(16)		ID-ul fișier al obiectului.
425	493	879	Nume obiect ¹	Char(512)		Numele obiectului.
	1005	1391	ID fișier obiect	Char(16)		ID-ul fișier 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 țară nume cale	Char(2)		ID-ul de regiune sau țară pentru numele de cale absolută.
	1042	1428	ID limbă nume cale	Char(3)		ID limbă pentru numele de cale absolută.
	1045	1431	Lungime nume cale	Binary(4)		Lungimea numelui de cale absolută.
	1047	1433	Indicator nume cale	Char(1)		Indicator nume cale:
					Y	Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect.
					N	Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.

Disponere intrări jurnal de auditare

Tabela 191. Intrări jurnal PG (Modificare grup primar) (continuare). Fișier descriere câmp QASYPGJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1048	1434	ID fișier director înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1064	1450	Nume cale ⁴	Char(5002)	Numele căii obiectului.
¹	Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină" (/).				
²	Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.				
³	Dacă câmpul indicator nume de cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				
⁴	Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.				
⁵	O valoare de *N înseamnă că valoarea Grup primar vechi nu a fost disponibilă.				
⁶	Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.				

Tabela 192. Intrări jurnal PO (Ieșire imprimantă). Fișier descriere câmp QASYPOJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip ieșire	Char(1)	Tipul ieșirii. D Tipărire directă R Trimitere către sistemul la distanță pentru tipărire S Fișier din spool tipărit
157	225	611	Stare după tipărire	Char(1)	D Șters după tipărire H Reținere după tipărire S Salvat după tipărire ' ' Tipărire directă
158	226	612	Nume job	Char(10)	Prima parte a numelui de job calificat.
168	236	622	Nume utilizator job	Char(10)	A doua parte a numelui de job calificat.
178	246	632	Număr job	Zoned(6,0)	A treia parte a numelui de job calificat.
184	252	638	Profil utilizator	Char(10)	Profilul utilizator care a creat ieșirea.
194	262	648	Coadă ieșire	Char(10)	Coadă ieșire care conține fișierul spool. ¹
204	272	658	Numele bibliotecă coadă ieșire	Char(10)	Numele bibliotecii care conține coada de ieșire. ¹
214	282	668	Nume dispozitiv	Char(10)	Dispozitivul unde ieșirea a fost tipărită ² .
224	292	678	Tip dispozitiv	Char(4)	Tipul dispozitivului imprimantă ² .
228	296	682	Model dispozitiv	Char(4)	Modelul dispozitivului imprimantă ² .
232	300	686	Numele fișier dispozitiv	Char(10)	Numele fișierului dispozitiv folosit pentru a accesa imprimanta.

Tabela 192. Intrări jurnal PO (Ieșire imprimantă) (continuare). Fișier descriere câmp QASYPOJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
242	310	696	Biblioteca fișier dispozitiv	Char(10)	Numele bibliotecii pentru fișierul dispozitiv.
252	320	706	Nume fișier spool	Char(10)	Numele fișierului spool ¹
262	330	716	Număr fișier spool scurt	Char(4)	Numărul fișierului spool ¹ . Setări la spații dacă este prea lung.
266	334	720	Tip formular	Char(10)	Tipul de formular al fișierului spool.
276	344	730	Date utilizator	Char(10)	Datele utilizator asociate cu fișierul spool ¹ .
286			(Zonă rezervată)	Char(20)	
	354	740	Număr fișier spool	Char(6)	Numărul fișierului spool.
	360	746	Zonă rezervată	Char(14)	
306	374	760	Sistem la distanță	Char(255)	Numele sistemului la distanță la care este trimisă tipărirea.
561	629	1015	Coadă tipărire sistem la distanță	Char(128)	Numele cozii de ieșire de pe sistemul la distanță.
	757	1143	Numele sistem job fișier spool	Char (8)	Numele sistemului pe care există fișierul spool.
	765	1151	Data de creare fișier spool	Char (7)	Data de creare fișier spool (CYYMMDD)
	772	1158	Timp de creare fișier spool	Char(6)	Timp de creare fișier spool (HHMMSS).
		1164	Nume ASP	Char(10)	Nume ASP pentru biblioteca dispozitiv
		1174	Număr ASP	Char(5)	Numărul ASP pentru biblioteca fișier dispozitiv
		1179	Numele ASP coadă ieșire	Char(10)	Nume ASP pentru bibliotecă coadă ieșire.
		1189	Numărul ASP coadă de ieșire	Char(5)	Numărul ASP pentru bibliotecă coadă de ieșire.
¹	Acest câmp este gol dacă tipul ieșirii este direct tipărit.				
²	Acest câmp este gol dacă tipul ieșirii este tipărit la distanță.				

Tabela 193. Intrări jurnal PS (Interschimbare profil). Fișier descriere câmp QASYPSJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Disponere intrări jurnal de auditare

Tabela 193. Intrări jurnal PS (Interschimbare profil) (continuare). Fișier descriere câmp QASYPSJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Interschimbare profil în timpul passthrough. E Terminare lucru în numele relației. H Tratare profil generată de API-ul QSYGETPH. I Toate jetoanele profil au fost respinse M Numărul maxim de jetoane profil care au fost generate. P Jeton profil general pentru utilizator. R Toate jetoanele profil pentru un utilizator au fost îndepărtate. S Pornire lucru în numele relației V Profil utilizator autentificat
157	225	611	Profil utilizator	Char(10)	Nume profil utilizator.
167	235	621	Locație sursă	Char(8)	Locație sursă pass-through.
175	243	629	Profil utilizator destinație original	Char(10)	Profilul original utilizator destinație pass-through.
185	253	639	Profil nou utilizator destinație	Char(10)	Profil nou utilizator destinație pass-through.
195	263	649	Utilizator office	Char(10)	Pornirea și oprirea utilizatorului office în numele relației.
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.

Tabela 194. Intrări jurnal PW (Parolă). Fișier descriere câmp QASYPWJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 194. Intrări jurnal PW (Parolă) (continuare). Fișier descriere câmp QASYPWJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare violare	Char(1)	Tipul violării A Eșuare legătură APPC. C Autentificare utilizator când comanda CHKPWD a eșuat. 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 eșuat deoarece este dezactivat profilul utilizator. R Încercarea de autentificare utilizator a eșuat 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 comunicații pe care a fost introdusă parola sau ID-ul utilizator. Dacă tipul intrării este X, Y sau Z, acest câmp va conține numele uneltei service care este accesată.
207	275	661	Numele locației la distanță	Char(8)	Numele locației la distanță pentru legătura APPC.
215	283	669	Nume locație locală	Char(8)	Numele locației locale pentru legătura APPC.
223	291	677	ID rețea	Char(8)	ID-ul rețea pentru legătura APPC.
		685 ²	Nume obiect	Char(10)	Numele obiectului care este decriptat.
		695	Bibliotecă obiect	Char(10)	Biblioteca pentru obiectul care este decriptat.
		705	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 informațiile ASP pentru biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP pentru obiect.					
² Dacă numele obiectului este *N și tipul violării este S, utilizatorul a încercat să decripteze date într-o variabilă gazdă.					

Disponere intrări jurnal de auditare

Tabela 195. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat). Fișier descriere câmp QASYRAJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 îndepărtată.
197	265	651	AUTL îndepărtată	Char(1)	Y Lista de autorizații îndepărtat 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 director	Char(63)	Directorul care conține obiectul bibliotecă de documente.
301			(Zonă rezervată)	Char(20)	
	369	755	(Zonă rezervată)	Char(18)	
	387	773	Lungime nume obiect	Binary(4)	Lungimea numelui obiectului.
321	389	775	CCSID nume obiect ¹	Binary(5)	identificator de set de caractere codate pentru numele obiect.
325	393	779	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiune sau țară pentru numele obiect.
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 fișier părinte ^{1,2}	Char(16)	ID-ul fișier al directorului părinte.
349	417	803	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
365	433	819	Nume obiect ¹	Char(512)	Numele obiectului.
	945	1331	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	982	1368	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	985	1371	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.

Tabela 195. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat) (continuare). Fișier descriere câmp QASYRAJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	987	1373	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	988	1374	ID fișier director înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1004	1390	Nume cale ⁴	Char(5002)	Numele căii obiectului.
¹	Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină" (/).				
²	Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.				
³	Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				
⁴	Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.				
⁵	Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.				

Tabela 196. Intrări jurnal RJ (Restaurare descriere job). Fișier descriere câmp QASYRJJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A restaurarea unei descrieri job care a avut specificat un profil utilizator în parametrul USER.
157	225	611	Nume descriere job	Char(10)	Numele descrierii de job restaurate.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care a fost restaurată descrierea de job.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume utilizator	Char(10)	Numele profilului utilizator specificat în descrierea de job.
		649	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOB
		659	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOB

Disponere intrări jurnal de auditare

Tabela 197. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat). Fișier descriere câmp QASYROJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 director	Char(63)	Directorul în care a fost restaurat obiectul.
308			(Zonă rezervată)	Char(20)	
	376	762	(Zonă rezervată)	Char(18)	
	394	780	Lungime nume obiect ¹	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect ¹	Binary(5)	identificator de set de caractere codate pentru numele obiect.
332	400	786	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiune sau țară pentru numele obiect.
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 fișier părinte ^{1,2}	Char(16)	ID-ul fișier al directorului părinte.
356	424	810	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
372	440	826	Nume obiect ¹	Char(512)	Numele obiectului.
	952	1338	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.

Tabela 197. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat) (continuare). Fișier descriere câmp QASYROJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fișier director înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1011	1397	Nume cale ⁴	Char(5002)	Numele căii obiectului.
¹	Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină" (/).				
²	Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.				
³	Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.				
⁴	Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.				
⁵	Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.				

Tabela 198. Intrări RP (Restaurare programe care adoptă autorizare). Fișierul descriere câmp QASYRPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Restaurare programe care adoptă autorizarea proprietarului
157	225	611	Nume program	Char(10)	Numele programului
167	235	621	Bibliotecă program	Char(10)	Numele bibliotecii 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 țară nume obiect ¹	Char (2)	ID-ul regiune sau țară pentru numele obiect.
	289	675	ID limbă nume obiect ¹	Char (3)	ID-ul limbă pentru numele obiectului.
	292	678	(Zonă rezervată)	Char (3)	

Disponere intrări jurnal de auditare

Tabela 198. Intrări RP (Restaurare programe care adoptă autorizare) (continuare). Fișierul descriere câmp QASYRPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	295	681	ID fișier părinte ^{1,2}	Char (16)	ID-ul fișier al directorului părinte.
	311	697	ID fișier obiect ^{1,2}	Char (16)	ID-ul fișier al obiectului.
	327	713	Nume obiect ¹	Char (512)	Numele obiectului.
	839	1225	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	876	1262	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	879	1265	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	881	1267	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	882	1268	ID fișier director înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	898	1284	Nume cale ⁴	Char(5002)	Numele căii obiectului.

¹ Aceste câmpuri sunt folosite doar pentru obiectele din QOpenSys și sistemul de fișiere "root" (/).

² Dacă un ID care are cel mai din stânga bit setat și restul de biți zero, ID-ul **nu** este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.

⁵ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.

Tabela 199. Intrări jurnal RQ (Restaurare obiect descriptor de modificare cerere). Fișier descriere câmp QASYRQJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Restaurați obiectul *CRQD care adoptă autorizare.
157	225	611	Nume obiect	Char(10)	Numele descriptorului de modificare cerere.

Tabela 199. Intrări jurnal RQ (Restaurare obiect descriptor de modificare cerere) (continuare). Fișier descriere câmp QASYRQJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
167	235	621	Biblioteca obiect	Char(10)	Numele bibliotecii unde este găsit descriptorul de modificare cerere.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
		639	Nume ASP	Char(10)	Nume ASP pentru biblioteca CRQD
		649	Număr ASP	Char(5)	Număr ASP pentru biblioteca CRQD

Tabela 200. Intrări jurnal RU (Restaurare autorizare pentru profil utilizator). Fișier de descriere câmp QASYRUJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Restaurare autorizare pentru profilurile utilizator
157	225	611	Nume utilizator	Char(10)	Numele profilului utilizator a cărui autorizare a fost restaurată.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
	253	639	Autorizare restaurată	Char(1)	Indică dacă toate autorizările au fost restaurate pentru utilizator. A Toate autorizaările au fost restaurate S Unele autorizări nu au fost restaurate

Tabela 201. Intrări jurnal RZ (Modificare grup primar pentru obiectul restaurat). Fișier descriere câmp QASYRZJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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	Biblioteca obiect	Char(10)	Numele bibliotecii unde este găsit obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Grup primar vechi	Char(10)	Grupul primar anterior pentru obiect.
195	263	649	Grup primar nou	Char(10)	Grupul primar nou pentru obiect.
205	273	659	(Zonă rezervată)	Char(20)	
225	293	679	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
237	305	691	(Zonă rezervată)	Char(8)	
245	313	699	Cale director	Char(63)	Directorul în care a fost restaurat obiectul.
308			(Zonă rezervată)	Char(20)	

Disponere intrări jurnal de auditare

Tabela 201. Intrări jurnal RZ (Modificare grup primar pentru obiectul restaurat) (continuare). Fișier descriere câmp QASYRZJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	376	762	(Zonă rezervată)	Char(18)	
	394	780	Lungime nume obiect ¹	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect ¹	Binary(5)	identificator de set de caractere codate pentru numele obiect.
332	400	786	ID regiune sau țară nume obiect ¹	Char(2)	ID-ul regiune sau țară pentru numele obiect.
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 fișier părinte ^{1,2}	Char(16)	ID-ul fișier al directorului părinte.
356	424	810	ID fișier obiect ^{1,2}	Char(16)	ID-ul fișier al obiectului.
372	440	826	Nume obiect ¹	Char(512)	Numele obiectului.
	952	1338	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fișier director înrudit ³	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	1011	1397	Nume cale ⁴	Char(5002)	Numele căii obiectului.

¹ Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys și "rădăcină"(/).

² Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.

³ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁴ Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.

Tabela 202. Intrări jurnal SD (Modificare director de distribuție sistem). Fișier de descriere câmp QASYS DJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 Afișare intrare director OUT Cerere fișier ieșire PRT Tipărire intrare director RMV Îndepărtare intrare director RNM Redenumire intrare director RTV Extragere detalii SUP Intrare furnizor
160	228	614	Tip înregistrare	Char(4)	DIRE Director DPTD Detalii departament SHDW Umbră director SRCH Căutare director
164	232	618	Sistem origine	Char(8)	Sistemul origine a modificării
172	240	626	Profil utilizator	Char(10)	Profilul utilizator care face modificarea
182	250	636	Cerere sistem	Char(8)	Sistemul care cere modificarea
190	258	644	Cerere funcție	Char(6)	INIT Inițializare OFFLIN Inițializare offline REINIT Reinițializare 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 rețea	Char(47)	ID-ul utilizator rețea care este modificat

Disponere intrări jurnal de auditare

Tabela 203. Intrări jurnal SE (Modificare intrare rutare subsistem). Fișier descriere câmp QASYSEJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
157	225	611	Nume subsistem	Char(10)	A Intrare rutare subsistem modificată 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 secvență	Char(4)	Numărul de secvență
209	277	663	Numele comandă	Char(3)	Tipul comenzii folosite
					ADD ADDRTGE
					CHG CHGRTGE
					RMV RMVRTGE
		666	Nume ASP pentru biblioteca SBSD	Char(10)	Nume ASP pentru biblioteca SBSD
		676	Număr ASP pentru biblioteca SBSD	Char(5)	Număr ASP pentru biblioteca SBSD
		681	Nume ASP pentru biblioteca program	Char(10)	Nume ASP pentru biblioteca program
		691	Număr ASP pentru biblioteca program	Char(5)	Număr ASP pentru biblioteca program

Tabela 204. Intrări jurnal SF (Acțiune către fișierul spool). Fișier descriere câmp QASYSFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 204. Intrări jurnal SF (Acțiune către fișierul spool) (continuare). Fișier descriere câmp QASYSFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip acces	Char(1)	Tipul intrării A Fișier din spool citit C Fișier din spool creat D Fișier din spool șters H Fișier din spool reținut I Creați un fișier inline R Fișier din spool eliberat S Fișier spool salvat. T Fișier spool restaurat. U Modificare attribute cu relevanță pentru securitate fișier spool. V Modificare doar attribute fără relevanță pentru securitate fișier spool.
157	225	611	Nume fișier bază de date	Char(10)	Numele fișierul bază de date care conține fișierul spool
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii pentru fișierul bază de date
177	245	631	Tip obiect	Char(8)	Tipul obiectului fișierului bază de date
185	253	639	Zonă rezervată	Char(10)	
195	263	649	Nume membru	Char(10)	Numele membrului de fișier.
205	273	659	Nume fișier spool	Char(10)	Numele fișierului spool ¹ .
215	283	669	Număr fișier spool scurt	Char(4)	Numărul fișierului spool ¹ . Dacă numărul fișierului spool este mai mare de 4 octeți, acest câmp va fi gol și va fi folosit câmpul Număr fișier spool (J5 offset 693).
219	287	673	Nume coadă ieșire	Char(10)	Numele cozii de ieșire care conține fișierul spool.
229	297	683	bibliotecă coadă ieșire	Char(10)	Numele bibliotecii pentru coada de ieșire.
239			Zonă rezervată	Char(20)	
	307	693	Număr fișier spool	Char(6)	Numărul fișierului spool.
	313	699	Zonă rezervată	Char(14)	
259	327	713	Copii vechi	Char(3)	Numărul copiilor vechi din fișierul spool
262	330	716	Copii noi	Char(3)	Numărul copiilor noi din fișierul spool
265	333	719	Imprimantă veche	Char(10)	Imprimanta veche pentru fișierul spool
275	343	729	Imprimantă nouă	Char(10)	Imprimanta nouă pentru fișierul spool
285	353	739	Coadă de ieșire nouă	Char(10)	Coadă de ieșire nouă pentru fișierul spool
295	363	749	Bibliotecă coadă ieșire nouă	Char(10)	Biblioteca pentru noua coadă de ieșire
305	373	759	Tip formular vechi	Char(10)	Tipul formularului vechi al fișierului spool
315	383	769	Tip formular nou	Char(10)	Tipul formularului nou al fișierului spool
325	393	779	Pagină de repornire veche	Char(8)	Pagina de repornire veche pentru fișierul spool
333	401	787	Pagina de repornire nouă	Char(8)	Pagina de repornire nouă pentru fișierul spool

Disponere intrări jurnal de auditare

Tabela 204. Intrări jurnal SF (Acțiune către fișierul spool) (continuare). Fișier descriere câmp QASYSFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
341	409	795	Început interval pagină veche	Char(8)	Început interval pagină veche al fișierului spool
349	417	803	Pornire interval pagină nouă	Char(8)	Început interval pagină nouă al fișierului spool
357	425	811	Sfârșit interval pagină veche	Char(8)	Sfârșit interval pagină veche al fișierului spool
365	433	819	Sfârșit interval pagină nouă	Char(8)	Sfârșit interval pagină nouă al fișierului spool
	441	827	Nume job fișier spool	Char(10)	Numele jobului fișier spool.
	451	837	Utilizator job fișier spool	Char(10)	Utilizatorul pentru jobul fișier spool.
	461	847	Numărul job fișier spool	Char(6)	Numărul pentru jobul fișier spool.
	467	853	Desenator vechi	Char(8)	Desenator sursă vechi.
	475	861	Desenator nou	Char(8)	Desenator sursă nou.
	483	869	Nume definiție pagină veche	Char(10)	Nume definiție pagină veche.
	493	879	Bibliotecă definiție pagină veche	Char(10)	Nume bibliotecă definiție pagină veche
	503	889	Nume definiție pagină nouă	Char(10)	Nume definiție pagină nouă.
	513	899	Bibliotecă definiție pagină nouă	Char(10)	Bibliotecă definiție pagină nouă.
	523	909	Nume definiție formular vechi	Char(10)	Nume definiție formular vechi.
	533	919	Bibliotecă definiție formular vechi	Char(10)	Nume bibliotecă definiție formular vechi.
	543	929	Numele definiției noi de formular	Char(10)	Numele definiției noi de formular
	553	939	Bibliotecă definiție formular nouă	Char(10)	Nume bibliotecă definiție formular nou.
	563	949	Opțiunea 1 veche definită de utilizator	Char(10)	Opțiunea 1 veche definită de utilizator.
	573	959	Opțiunea 2 veche definită de utilizator	Char(10)	Opțiunea 2 veche definită de utilizator.
	583	969	Opțiunea 3 veche definită de utilizator	Char(10)	Opțiunea 3 veche definită de utilizator.
	593	979	Opțiunea 4 veche definită de utilizator	Char(10)	Opțiunea 4 veche definită de utilizator.
	603	989	Opțiunea 1 nouă definită de utilizator	Char(10)	Opțiunea 1 nouă definită de utilizator.

Tabela 204. Intrări jurnal SF (Acțiune către fișierul spool) (continuare). Fișier descriere câmp QASYSFJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	613	999	Opțiunea 2 nouă definită de utilizator	Char(10)	Opțiunea 2 nouă definită de utilizator.
	623	1009	Opțiunea 3 nouă definită de utilizator	Char(10)	Opțiunea 3 nouă definită de utilizator.
	633	1019	Opțiunea 4 nouă definită de utilizator	Char(10)	Opțiunea 4 nouă definită de utilizator.
	643	1029	Obiect vechi definit de utilizator	Char(10)	Nume obiect vechi definit de utilizator.
	653	1039	Biblioteca obiecte vechi 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	Biblioteca 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 fișier spool	Char(8)	Numele sistemului pe care există fișierul spool.
	711	1097	Data de creare fișier spool	Char(7)	Data de creare fișier spool (CYYMMDD).
	718	1104	Timp de creare fișier spool	Char(6)	Timp de creare fișier spool (HHMMSS).
		1110	Numele datelor vechi definite de utilizator	Char(255)	Numele datelor vechi definite de utilizator
		1365	Numele datelor noi definite de utilizator	Char(255)	Numele datelor noi definite de utilizator
		1620	Nume fișier ASP	Char(10)	Nume ASP pentru biblioteca de fișier bază de date.
		1630	Număr fișier ASP	Char(5)	Număr ASP pentru biblioteca fișierului bază de date.
		1635	Nume ASP coadă de ieșire	Char(10)	Nume ASP pentru bibliotecă coadă ieșire.
		1645	Numărul ASP coadă de ieșire	Char(5)	Numărul ASP pentru bibliotecă coadă de ieșire.
		1650	Nume ASP nou coadă de ieșire	Char(10)	Nume ASP pentru bibliotecă coadă de ieșire nouă.
		1660	Număr ASP nou pentru coada de ieșire	Char(5)	Număr ASP pentru bibliotecă coadă de ieșire nouă.

Disponere intrări jurnal de auditare

Tabela 204. Intrări jurnal SF (Acțiune către fișierul spool) (continuare). Fișier descriere câmp QASYSFJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
		1665	Stare fișier spool vechi	Char(3)	Stare fișier spool vechi
		1668	Stare nouă fișier spool	Char(3)	Stare nouă fișier spool
		1671	Data originală de creație	Char(7)	Data originală de creație.
		1678	Timpul original de creație	Char(6)	Timpul original de creație.
		1684	Data de expirare fișier spool vechi	Char(7)	Data de expirare fișier spool vechi
		1687	Data de expirare fișier spool nou	Char(7)	Data de expirare fișier spool nou

¹ Acest câmp este gol când tipul intrării este I (tipărire inline).

Tabela 205. Intrări jurnal SG (Semnale asincrone). Fișier descriere câmp QASYSJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. A Semnal asincron iSeries procesat P Semnal asincron de mediu de spațiu de adrese private (PASE) procesat
	225	611	Număr semnal	Char(4)	Număr semnalului care a fost procesat.
	229	615	Acțiune de tratare	Char(1)	Acțiunea luată pentru acest semnal. C Continuați procesul E Excepție semnal H Tratare prin invocarea funcției de prindere semnal S Opriți procesul T Terminați procesul U Terminați cererea
	230	616	Sursă semnal	Char(1)	Sursa semnalului. M Sursa mașină P Sursă proces Notă: Când valoarea sursei de semnal este mașină, 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.

Tabela 205. Intrări jurnal SG (Semnale asincrone) (continuare). Fișier descriere câmp QASYSJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	257	643	Utilizator curent job sursă	Char(10)	Profil 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.

Tabela 206. Intrări jurnal SK (Conexiuni socket securizate). Fișier de descriere câmp QASYSKJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	A Acceptare C Conectare D Adresă DHCP asignată F Mail filtrat P Port indisponibil R Refuzare poștă 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 distanță. ³	Char(15)	Adresa IP la distanță.
	260	646	Port la distanță	Char(5)	Portul la distanță.
	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 distanță ²	Char(46)	Adresa IP la distanță
	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 câmpul lungime variabilă. Primii 2 octeți conțin lungimea câmpului.

² Când tipul intrării este D, acest câmp conține adresa IP asignată de serverul DHCP clientului care a făcut cererea.

³ Aceste câmpuri suportă doar adrese IPv4.

Disponere intrări jurnal de auditare

Tabela 207. Intrări jurnal SM (Modificare gestiune sisteme). Fișier de descriere câmp QASYSMJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	<p>Funcție accesată</p> <p>B Listă copie de rezervă modificată</p> <p>C Opțiuni de curățare automată</p> <p>D DRDA</p> <p>F Sistem de fișiere HFS</p> <p>N Operație fișier rețea</p> <p>O Opțiuni copie de rezervă modificate</p> <p>P Planificare de pornire/oprire alimentare</p> <p>S Listă de răspunsuri sistem</p> <p>T Timpi de recuperare cale de acces modificați</p>
157	225	611	Tip acces	Char(1)	<p>A Adăugare</p> <p>C Modificare</p> <p>D Ștergere</p> <p>R Îndepărtare</p> <p>S Afișare</p> <p>T Extragere sau primire</p>
158	226	612	Număr secvență	Char(4)	Numărul secvență al acțiunii
162	230	616	ID mesaj	Char(7)	ID mesaj asociat cu acțiunea
169	237	623	Nume bază de date relațională	Char(18)	Numele pentru baza de date relațională
187	255	641	Nume sistem de fișiere	Char(10)	Numele pentru sistemul de fișiere
197	265	651	Opțiune copie de rezervă modificată	Char(10)	Opțiunea 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 fișier rețea	Char(10)	Numele fișierului rețea care a fost folosit
227	295	681	Membru fișier rețea	Char(10)	Numele membrului fișierului rețea
237	305	691	Numărul fișierului rețea	Zoned(6,0)	Numărul fișierului rețea
243	311	697	Proprietar fișier rețea	Char(10)	Numele profilului utilizator care deține fișierul rețea
253	321	707	Utilizatorul care a generat fișierul rețea	Char(8)	Numele profilului utilizator care a generat fișierul rețea
261	329	715	Adresa care a generat fișierul rețea	Char(8)	Adresa care a generat fișierul rețea

Tabela 208. Intrări jurnal SO (Acțiuni informații utilizator de securitate server). Fișier descriere câmp QASYSOJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării A Adăugare intrare C Modificare intrare R Îndepărtare intrare T Extragere intrare
157	225	611	Profil utilizator	Char(10)	Numele profilului utilizator.
	235	621	Tip intrare informații utilizator	Char(1)	N Tip intrare nespecificată. U Intrarea este o intrare de informații aplicație utilizator. Y Intrarea este o intrare de autentificare server.
	236	622	Parolă memorată	Char(1)	N Parolă nememorată S Nici o modificare Y Parola este memorată.
	237	623	Nume server	Char(200)	Numele serverului.
	437	823	(Zonă rezervată)	Char(3)	
	440	826	Lungime ID utilizator	Binary (4)	Lungimea ID-ului utilizator.
	442	828	(Zonă rezervată)	Char(20)	
	462	848	ID utilizator	Char(1002) ¹	ID-ul pentru utilizator.

¹ Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea câmpului.

Tabela 209. Intrări jurnal ST (Acțiune unelte service). Fișier descriere câmp QASYSTJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării A Înregistrare service

Disponere intrări jurnal de auditare

Tabela 209. Intrări jurnal ST (Acțiune unelte service) (continuare). Fișier descriere câmp QASYSTJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
157	225	611	Unealtă service	Char(2)	Tipul intrării.
					AN ANZJVM
					CS STRCPYSCN
					CD QTACTLDV, QTADMPDV
					CE QWTCTLTR
					CT DMPCLUTRC
					DC DLTCMNTRC
					DD DMPDLO
					DJ DMPJVM, QPYRTJVM
					DM DMPMEMINF
					DO DMPOBJ
					DS DMPSYSOBJ, QTADMPTS, QTADMPDV
					EC ENDCMNTRC
					ER ENDRMTSPT
					HD QYHCHCOP (DASD)
					HL QYHCHCOP (LPAR)
					JW QPYRTJWA
					MC QWMMMAINT (change)
					MD QWMMMAINT (dump)
					OP Consola de operații
					PC PRTC MNTRC
					PE PRTERLOG, QTADMPDV
					PI PRTINTDTA, QTADMPDV
					PS QP0FPTOS
					SC STRCMNTRC
					SE QWTSETTR
					SF QWCCDSIC, QWVRCSTK (afișare intrare stivă internă)
					SJ STRSRVJOB
					SR STRRMTSPT
					ST STRSST
					TA TRCTCPAPP

Tabela 209. Intrări jurnal ST (Acțiune unelte service) (continuare). Fișier descriere câmp QASYSTJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
					TC TRCCNN (specificat *FORMAT)
					TE ENDTRC, ENDPEX, TRCJOB(specificat *OFF sau *END)
					TI TRCINT sau TRCCNN (*ON, *OFF sau *END specificat)
					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 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 director	Char(63)	Directorul care conține obiectul bibliotecă de documente
	432	818	Câmp JUID	Char(10)	JUID a jobului destinație.
	442	828	Acțiune de urmărire din timp ¹	Char(10)	Acțiunea cerută pentru căutarea de job din timp *ON Căutarea din timp activată *OFF Urmărire din timp dezactivată *RESET Urmărire din timp dezactivată și informațiile de urmărire șterse.
	452	838	Opțiune de urmărire aplicație ²	Char(1)	Opțiunea de urmărire specificată în TRCTCPAPP. Y Colecția de informații de urmărire pornită N Colecția de informații de urmărire oprită și informațiile de urmărire scrise în fișierul spool E Colecția de informații de urmărire terminată și toate informațiile de urmărire șterse (nici o ieșire creată)
	453	839	Aplicație urmărită ²	Char(10)	Numele aplicației care este urmărită.

Disponere intrări jurnal de auditare

Tabela 209. Intrări jurnal ST (Acțiune unelte service) (continuare). Fișier descriere câmp QASYSTJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	463	849	Profil unelte service ³	Char(10)	Numele profilului unelte service folosite pentru STRSST.
		859	ID nod sursă	Char(8)	ID nod sursă
		867	Utilizator sursă	Char(10)	Utilizator sursă
		877	Numele ASP pentru biblioteca de obiecte	Char(10)	Numele ASP pentru biblioteca de obiecte
		887	Număr ASP pentru biblioteca de obiecte	Char(5)	Număr ASP pentru biblioteca de obiecte
		892	Numele ASP pentru biblioteca de obiecte DMPSYSOBJ	Char(10)	Numele ASP pentru biblioteca de obiecte DMPSYSOBJ
		902	Număr ASP pentru biblioteca de obiecte DMPSYSOBJ	Char(5)	Număr ASP pentru biblioteca de obiecte DMPSYSOBJ
		907	Tip de consolă ⁴	Char(10)	Tipul consolei. Valorile posibile sunt: <ul style="list-style-type: none"> • *DIRECT • *LAN • *HMC
		917	Acțiune consolă ⁴	Char(10)	Acțiune consolă. Valorile posibile sunt: <ul style="list-style-type: none"> • *RECOVERY • *TAKEOVER
		927	Familia de adrese ⁴	Char(10)	Familia de adrese. <ul style="list-style-type: none"> • *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 uneltă 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 uneltă de service ale dispozitivului consolă precedent pentru *LAN.
		1049	Urmărește sesiune ⁵	Char(10)	ID urmărire sesiune.

¹ Acest câmp este folosit doar când tipul intrării (offset 225) este CE.

² Acest câmp este folosit doar când tipul intrării (offset 225) este TA.

³ Acest câmp este folosit doar când tipul intrării (offset 611) este ST sau OP.

| ⁴ Acest câmp este folosit doar când tipul intrării (offset 611) este OP.

| ⁵ Acest câmp este folosit doar când tipul intrării (offset 611) este WS sau WE.

Tabela 210. Intrări jurnal SV (Acțiune pentru valoarea sistem). Fișier descriere câmp QASYSVJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. A Modificare pentru valorile sistem B Modificare pentru atributele service C Modificare pentru ceasul sistem
157	225	611	Valoare sistem sau atribut service	Char(10)	Numele valorii sistem sau atributului service
167	235	621	Valoare nouă	Char(250)	Valoarea la care valoarea sistem sau atributul sistem a fost modificată
417	485	871	Valoare veche	Char(250)	Valoarea valorii sistem sau atributului sistem înainte sa fie modificată
667	735	1121	Continuarea valorii noi	Char(250)	Continuarea valorii la care valoarea sistem sau atributul sistem au fost modificate.
917	985	1371	Continuarea valorii vechi	Char(250)	A fost modificată continuarea valorii sistem sau atributului sistem.

Tabela 211. Intrări jurnal VA (Modificarea listei de control acces). Fișier descriere câmp QASYVAJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Stare	Char(1)	Starea cererii. S Cu succes F Eșuare
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
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	Acțiune executată	Char(1)	Acțiunea executată în profilul de control acces: A Adăugare C Modificare D Ștergere
198	266	652	Nume resursă	Char(260)	Numele resursei de modificat.

Disponere intrări jurnal de auditare

Tabela 212. Intrări jurnal VC (Terminare și oprire conexiune). Fișier descriere câmp QASYVCJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Acțiune de conectare.	Char(1)	Acțiunea de conectare care a apărut. S Pornire E Terminare R Refuzare
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
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 îndepărtată sau lipsă de permisiuni administrative E Eroare, deconectare sesiune sau parolă incorectă N Deconectare normală sau limită de nume utilizator P Nici o permisiune de acces la resursa partajată
203	271	657	Nume rețea	Char(12)	Numele rețea asociat cu conexiunea.

Tabela 213. Intrări jurnal VF (Închiderea fișierelor server). Fișier descriere câmp QASYVFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Motiv închidere	Char(1)	Motivul pentru care fișierul a fost închis. A Deconectare administrativă N Deconectare client normală S Deconectare sesiune
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.

Tabela 213. Intrări jurnal VF (Închiderea fișierelor server) (continuare). Fișier descriere câmp QASYVFJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
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 fișier	Char(5)	ID-ul fișierului care a fost închis.
202	270	656	Durată	Char(6)	Numărul de secunde în care fișierul a fost deschis.
208	276	662	Nume resursă	Char(260)	Numele resursei care deține fișierul accesat.

Tabela 214. Intrări jurnal VL (Limită cont depășită). fișier descriere câmp QASYVLJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Motiv	Char(1)	Motivul pentru care limita a fost depășită. A Cont expirat D Cont dezactivat L Orele de logare depășite U Necunoscut sau indisponibil W Stație de lucru nevalidă
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului cu violare limită cont.
187	255	641	Utilizator	Char(10)	Numele utilizatorului cu violare limită cont.
197	265	651	Nume resursă	Char(260)	Numele resursei care este folosită.

Tabela 215. Intrări jurnal VN (Logare și delogare rețea). Fișier descriere câmp QASYVNJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip logare	Char(1)	Tipul evenimentului care a apărut: F Cerere delogare O Cerere logare R Logare refuzată

Disponere intrări jurnal de auditare

Tabela 215. Intrări jurnal VN (Logare și delogare rețea) (continuare). Fișier descriere câmp QASYVNJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului pentru eveniment.
187	255	641	Utilizator	Char(10)	Utilizatorul care s-a logat sau s-a delogat.
197	265	651	Privilegiu utilizator	Char(1)	Privilegiul utilizatorului care se loghează: A Administrator G Musafir U Utilizator
198	266	652	Motiv refuzare	Char(1)	Motivul refuzării încercării de logare: A Access refuzat F Dezactivare forțată datorită limitei de logare P Parolă incorectă
199	267	653	Motiv adițional	Char(1)	Detalii despre refuzul accesului: A Cont expirat D Cont dezactivat L Ore de logare nevalide R ID solicitant nevalid U Necunoscut sau indisponibil

Tabela 216. Intrări jurnal VO (Listă de validare). Fișier descriere câmp QASYVOJ4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507 și Tabela 151 la pagina 509 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. A Adăugare intrare în lista de validare C Modificare intrare în lista de validare F Căutare intrare în lista de validare R Îndepărtare intrare în lista de validare U Verificare fără succes a unei intrări în lista de validare V Verificare cu succes a unei intrări în lista de validare

Tabela 216. Intrări jurnal VO (Listă de validare) (continuare). Fișier descriere câmp QASYVOJ4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	225	611	Tip fără succes	Char(1)	Tipul unei verificări fără succes. E Datele criptate sunt incorecte I ID-ul intrării nu a fost găsit V Lista de validare nu a fost găsită
	226	612	Lista de validare	Char(10)	Numele listei de validare.
	236	622	Nume bibliotecă	Char(10)	Numele bibliotecii în care este lista de validare.
	246	632	Date criptate	Char(1)	Valoare date de criptat. Y Datele de criptat au fost specificate în cerere. N Datele de criptat nu au fost specificate în cerere.
	247	633	Date intrare	Char(1)	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 situația implicită. 1 Datele de criptat pot fi folosite pentru a verifica o intrare și datele pot fi întoarse într-o operație de căutare.
	253	639	Atribut de certificat X.509	Char (1)	Certificat X.509
	254	640	(Zonă rezervată)	Char (28)	
	282	668	ID intrare	Byte(100)	ID-ul intrare
	382	768	Date intrare	Byte(1000)	Datele de intrare.
		1768	Numele ASP pentru biblioteca listei de validare	Char(10)	Numele ASP pentru biblioteca listei de validare
		1778	Numărul ASP pentru biblioteca listei de validare	Char(5)	Numărul ASP pentru biblioteca listei de validare

Tabela 217. Intrări jurnal VP (Eroare parolă rețea). Fișier descriere câmp QASYVPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Disponere intrări jurnal de auditare

Tabela 217. Intrări jurnal VP (Eroare parolă rețea) (continuare). Fișier descriere câmp QASYVPJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
156	224	610	Tip eroare	Char(1)	Tipul erorii care a apărut. P Eroare parolă
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care a inițiat cererea.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care a încercat să se logheze.

Tabela 218. Intrări jurnal VR (Acces resursă rețea). Fișier descriere câmp QASYVRJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Stare	Char(1)	Starea de acces. F Accesul la resursă a eșuat S Accesul la resursă a reușit
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere resursa.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere resursa.
197	265	651	Tip operație	Char(1)	Tipul operației care este executată: A Atributele de resursă modificate C Instanța resursei create D Resursă ștersă P Permișiuni resursă modificate R Citire de date sau rulare de la o resursă W Date scrise într-o resursă X Resursa nu funcționa
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 fișier	Char(5)	ID-ul fișierului care este accesat.
211	279	665	Nume resursă	Char(260)	Numele resursei folosite.

Tabela 219. Intrări jurnal VS (Sesiune server). Fișier descriere câmp QASYVSJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Acțiune sesiune	Char(1)	Acțiunea sesiune care a apărut. E Terminare sesiune S Pornire sesiune
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care evenimentul a fost logat pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere sesiune.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere sesiunea.
197	265	651	Privilegiu utilizator	Char(1)	Nivelul de privilegiu al utilizatorului pentru pornirea de sesiune: A Administrator G Musafir U Utilizator
198	266	652	Cod motiv	Char(1)	codul motiv pentru terminarea sesiunii. A Deconectare administrator D Deconectarea automată (timeout), partajare îndepărtată sau lipsă de permisiuni administrative E Eroare, deconectare sesiune sau parolă incorectă N Deconectare normală sau limită de nume utilizator R Restricție cont

Tabela 220. Intrări jurnal VU (Modificare profil rețea). Fișier descriere câmp QASYVUJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip	Char(1)	Tipul înregistrării care a fost modificată. G Înregistrare grup U Înregistrare utilizator M Informații globale profil utilizator
157	225	611	Nume server	Char(10)	Numele descrierii server rețea care a înregistrat evenimentul.

Disponere intrări jurnal de auditare

Tabela 220. Intrări jurnal VU (Modificare profil rețea) (continuare). Fișier descriere câmp QASYVUJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere modificarea profilului utilizator.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere modificarea profilului utilizator.
197	265	651	Acțiune	Char(1)	Acțiune cerută: A Adăugare C Modificare D Ștergere P Parolă incorectă
198	266	652	Nume resursă	Char(260)	Numele resursei.

Tabela 221. Intrări jurnal VV (modificare stare service). Fișier descriere câmp QASYVVJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea 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 rețea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reținut în istoric evenimentul pe serverul rețea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere modificarea.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere modificarea.

Tabela 221. Intrări jurnal VV (modificare stare service) (continuare). Fișier descriere câmp QASYVVJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
197	265	651	Stare	Char(1)	Starea cererii serviciului: A Serviciu activ B Pornirea serviciului în așteptare C Continuare serviciu în așteptare E Oprirea așteptării 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 operația de modificare.
290	358	744	Serviciu	Char(20)	Serviciul care fost modificat.

Tabela 222. Intrări jurnal X0 (Autentificare rețea). Fișier descriere câmp QASYX0JE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Disponere intrări jurnal de auditare

Tabela 222. Intrări jurnal X0 (Autentificare rețea) (continuare). Fișier descriere câmp QASYX0JE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
156	224	610	Tip intrare	Char(1)	Tipul intrării:
					1 Tichet serviciu valid
					2 Principalele serviciu nu se potrivesc
					3 Principalele client nu se potrivesc
					4 Nepotrivire adresă IP tichet
					5 Eșuare decriptare tichet
					6 Eșuare decriptare autentificator
					7 Regiunea nu este în regiunile locale client
					8 Tichetul este o încercare de repetiție
					9 Tichetul nu este încă valid
					A Decriptare eroare sumă de control KRB_AP_PRIV sau KRB_AP_SAFE
					B Nepotrivire adresă IP la distanță
					C Nepotrivire adresă IP locală
					D Eroare amprentă de timp KRB_AP_PRIV sau KRB_AP_SAFE
					E eroare repetiție KRB_AP_PRIV sau KRB_AP_SAFE
					F eroare ordine secvență 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 desfășurare GSS sau verificare GSS
					O Decriptare/decodificare desfășurare GSS sau verificare GSS
					P Eroare sumă de control desfășurare GSS sau verificare GSS
					Q Eroare secvențială desfășurare 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 distanță	Char(21)	Adresă IP la distanță
	262	648	Adresă IP locală	Char(21)	Adresa IP locală
	283	669	Adrese criptate	Char(256)	Adrese IP criptate
	539	925	Indicator adrese criptate	Char(1)	Indicator adrese IP criptate
					Y toate adresele incluse
					N nu toate adresele incluse
					X nefurnizat

Tabela 222. Intrări jurnal X0 (Autentificare rețea) (continuare). Fișier descriere câmp QASYX0JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	540	926	Stegulețe tichet	Char(8)	Stegulețe 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 reinnoire tichet	Char(8)	Reinnoire 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 acreditate 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 autenticator)
	1638	2024	Lungime Principal client	Binary(4)	Lungime Principal client (din autenticator)
	1640	2026	Indicator Principal client	Char(1)	Indicator Principal client (din autenticator) Y Principal client complet N Principal client incomplet X nefurnizat
	1641	2027	Principal client	Char(512)	Principal client din autenticator
	2153	2539	CCSID Principal client	Binary(5)	CCSID Principal client (din tichet)
	2157	2543	Lungime Principal client	Binary(4)	Lungime Principal client (din tichet)

Disponere intrări jurnal de auditare

Tabela 222. Intrări jurnal X0 (Autentificare rețea) (continuare). Fișier descriere câmp QASYX0JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	2159	2545	Indicator Principal client	Char(1)	Indicator Principal client (din tichet) Y Principal client complet N Principal client incomplet X nefurnizat
	2160	2546	Principal client	Char(512)	Principal client din tichet
	2672	3058	CCSID principal server GSS	Binary(5)	CCSID principal server (din acreditare GSS)
	2676	3062	Lungime principal server GSS	Binary(4)	Lungime principal server (din acreditare GSS)
	2678	3064	Indicator principal 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 distanță GSS	Binary(5)	CCSID nume principal la distanță GSS
	3714	4100	Lungime principal la distanță GSS	Binary(4)	Lungime nume principal la distanță GSS
	3716	4102	Indicator principal la distanță GSS	Char(1)	Indicator nume principal la distanță GSS Y Principal la distanță complet N Principal la distanță incomplet X nefurnizat
	3717	4103	Principal la distanță GSS	Char(512)	Principal la distanță GSS

Tabela 223. Intrări jurnal X1 (Jeton identitate). Fișier descriere câmp QASYX1JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
		1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.

Tabela 223. Intrări jurnal X1 (Jeton identitate) (continuare). Fișier descriere câmp QASYX1JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
		610	Tip intrare	Char(1)	Tipul intrării: D Delegare jeton identitate cu succes F Delegare jeton identitate eșuată G Obținere cu succes a utilizatorului din jetonul identitate U Obținerea utilizatorului din jetonul identitate a eșuat
		611	Cod motiv	Binary(5)	cod motiv pentru cererea eșuată: 9 Nepotrivire lungime jeton 10 Nepotrivire identificator EIM 11 Nepotrivire ID instanță aplicație 12 Semnătură jeton nevalidă 13 Jeton identitate nevalid 14 Utilizator destinație nevalid 16 Tratare cheie nevalidă 17 Versiune jeton nesuportată 18 Cheie publică negăsită Notă: La o eșuare, doar informațiile care au fost validate până la punctul eșuării for fi completate în câmpurile text.
		615	Rezervat	Char(7)	Rezervat
		622	CCSID date	Binary(5)	CCSID-ul datelor din câmpurile text
		626	Lungime receptor	Binary(5)	Lungimea datelor din câmpul receptorului.
		630	Receptor	Char(508)	Receptorul jetonului identitate care fie a eșuat cererea fie a avut succes. Datele din acest câmp vor fi în formatul: <EIMID>eimID_receptor </EIMID> <APPID>RECEIVER_appID </APPID> <TIMESTAMP>amprentă_timp_receiver </TIMESTAMP>. Amprenta de timp va fi inclusă doar în cererile de delegare.
		1138	Lungime expeditor	Binary(5)	Lungimea datelor din câmpul expeditorului.
		1142		Char(508)	Expeditorul jetonului identitate care fie a eșuat cererea fie a avut succes. Datele din acest câmp vor fi în formatul: <EIMID>eimID_expeditor</EIMID> <APPID>appID_expeditor</APPID> <TIMESTAMP>amprentă_timp_expeditor</TIMESTAMP>
		1650	Lungime inițiator	Binary(5)	Lungimea datelor din câmpul inițiatorului.
		1654	Inițiator	Char(508)	Inițiatorul cererii jeton identitate. Dacă expeditorul și inițiatorul sunt aceiași, câmpul cu lungimea inițiator va fi 0. Datele din acest câmp vor fi în formatul: <EIMID>eimID_inițiator</EIMID> <APPID>appID_inițiator</APPID> <TIMESTAMP>amprentă_timp_inițiator</TIMESTAMP>
		2162	Lungime lanț	Binary(5)	Lungimea datelor din câmpul lanț.

Disponere intrări jurnal de auditare

Tabela 223. Intrări jurnal X1 (Jeton identitate) (continuare). Fișier descriere câmp QASYX1JE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
		2166	Lanț	Char(2036)	Lanțul expeditorilor între inițiator și ultimul expeditor. Lanțul va fi în ordinea de la cel din urmă la cel dintâi. Dacă nu există alți expeditori, atunci câmpul lungime lanț va fi 0. Acest câmp va fi trunchiat dacă lanțul este mai lung decât lungimea acestui câmp. Datele din acest câmp vor fi în formatul: <SNDRz><EIMID>sndrz_eimID</EIMID> <APPID>sndrz_appID</APPID> <TIMESTAMP>sndrz_timestamp</TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Intrări lanț	Binary(5)	Numărul de intrări din câmpul lanț.
		4206	Intrări lanț disponibile	Binary(5)	Numărul intrărilor disponibile pentru lanțul expeditorilor. Acest număr poate fi mai mare decât numărul de intrări din câmp în cazul în care câmpul este trunchiat.
		4210	Lungime registru sursă	Binary(5)	Lungimea datelor din câmpul registru sursă.
		4214	Registru sursă	Char(508)	Registru 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 destinație	Binary(5)	Lungimea datelor din câmpul registru destinație.
		5238	Registru destinație	Char(508)	Registru destinație specificat.
		5746	Lungime utilizator registru destinație	Binary(5)	Lungimea datelor din câmpul utilizator registru destinație.
		5750	Utilizator registru destinație	Char(508)	Utilizatorul registru destinație spre care indică jetonul identitate.

Tabela 224. Intrări jurnal YC (Modificarea obiectului DLO). Fișier descriere câmp QASYCJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect
					C Modificarea unui obiect DLO
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Utilizator office	Char(10)	Profilul utilizator al utilizatorului office
195	263	649	Nume document sau director	Char(12)	Numele documentului sau directorului
207	275	661	(Zonă rezervată)	Char(8)	

Tabela 224. Intrări jurnal YC (Modificarea obiectului DLO) (continuare). Fișier descriere câmp QASYCJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
215	283	669	Cale director	Char(63)	Directorul care conține 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 Vedeți Tabela 228 la pagina 616 pentru o listă de coduri pentru tipurile de acces.

Tabela 225. Intrări jurnal YR (Citirea obiectului DLO). Fișier descriere câmp QASYRJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect R Citirea unui obiect DLO
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Utilizator office	Char(10)	Profilul utilizator al utilizatorului office
195	263	649	Nume document sau director	Char(12)	Numele obiectului bibliotecă de documente
207	275	661	(Zonă rezervată)	Char(8)	
215	283	669	Cale director	Char(63)	Directorul care conține 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 Vedeți Tabela 228 la pagina 616 pentru o listă de coduri pentru tipurile de acces.

Tabela 226. Intrări jurnal ZC (Modificare obiect). Fișier descriere câmp QASYZCJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect C Modificarea unui obiect U Modernizarea accesului deschis către un obiect
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este localizat obiectul
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Tip acces	Packed(5,0)	Tipul de acces ¹

Disponere intrări jurnal de auditare

Tabela 226. Intrări jurnal ZC (Modificare obiect) (continuare). Fișier descriere câmp QASYZCJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
188	256	642	Date specifice de acces	Char(50)	<p>Date specifice despre acces</p> <p>Când tipul obiect este *IMGCLG, acest câmp conține următorul format:</p> <p>Char 3 Numărul index al intrării catalog de imagini.</p> <p>Blank Indică faptul că operația a fost pentru un catalog de imagini.</p> <p>Char 32 ID-ul volum al intrării catalog de imagini.</p> <p>Blank Indică faptul că operația a fost pentru un catalog de imagini.</p> <p>Char 1 Tipul de acces pentru intrare. Valorile posibile sunt menționate mai jos.</p> <p>Blank Indică faptul că operația a fost pentru un catalog de imagini.</p> <p>R Fișierul care conține catalogul de imagini este numai-scriere.</p> <p>W Fișierul care conține intrarea catalog de imagini poate fi citit/scriș.</p> <p>Char 1 Protecția la scriere pentru intrare.</p> <p>Blank Indică faptul că operația a fost pentru un catalog de imagini.</p> <p>Y Fișierul care conține intrarea catalog de imagini este protejat la scriere.</p> <p>N Fișierul care conține intrarea catalog de imagini nu este protejat la scriere.</p> <p>Char 10 Numele dispozitivului virtual.</p> <p>Blank Indică faptul că operația a fost pentru un catalog de imagini sau că respectivul catalog de imagini nu este în stare Pregătit.</p> <p>Char 3 Nefolosit.</p>
238			(Zonă rezervată)	Char(20)	
	306	692	(Zonă rezervată)	Char(18)	
	324	710	Lungime nume obiect ²	Binary (4)	Lungimea numelui obiectului.
258	326	712	CCSID nume obiect ²	Binary(5)	identificator de set de caractere codate pentru numele obiect.
262	330	716	ID regiune sau țară nume obiect ²	Char(2)	ID-ul regiune sau țară pentru numele obiect.
264	332	718	ID limbă nume obiect ²	Char(3)	ID-ul limbă pentru numele obiectului.

Tabela 226. Intrări jurnal ZC (Modificare obiect) (continuare). Fișier descriere câmp QASYZCJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
267	335	721	(Zonă rezervată)	Char(3)	
270	338	724	ID fișier părinte ² ³	Char(16)	ID-ul fișier al directorului părinte.
286	354	740	ID fișier obiect ² ³	Char(16)	ID-ul fișier al obiectului.
302	370	756	Nume obiect ²	Char(512)	Numele obiectului.
	882	1268	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	919	1305	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	924	1310	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	925	1311	ID fișier director înrudit ⁴	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
941	1327	Nume cale ⁵	Char(5002)	Numele căii obiectului.	

¹ Vedeți Tabela 228 la pagina 616 pentru o listă de coduri pentru tipurile de acces.

² Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.

³ Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.

⁴ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁵ Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.

⁶ Dacă obiectul este într-o bibliotecă, acestea sunt informațiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informațiile ASP ale obiectului.

Disponere intrări jurnal de auditare

Tabela 227. Intrări jurnal ZR (Citire obiect). Fișier descriere câmp QASYZRJE/J4/J5

Offset			Câmp	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeți Tabela 150 la pagina 507, Tabela 151 la pagina 509 și Tabela 152 la pagina 510 pentru menționarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect
157	225	611	Nume obiect	Char(10)	R Citirea unui obiect 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
188	256	642	Date specifice de acces	Char(50)	Date specifice despre acces. Când tipul obiect este *IMGCLG, acest câmp conține următorul format: Char 3 Numărul index al intrării catalog de imagini. Blank Indică faptul că operația a fost pentru un catalog de imagini. Char 32 ID-ul volum al intrării catalog de imagini. Blank Indică faptul că operația a fost pentru un catalog de imagini. Char 1 Tipul de acces pentru intrare. Valorile posibile sunt menționate mai jos. Blank Indică faptul că operația a fost pentru un catalog de imagini. R Fișierul care conține catalogul de imagini este numai-scriere. W Fișierul care conține intrarea catalog de imagini poate fi citit/scriș. Char 1 Protecția la scriere pentru intrare. Blank Indică faptul că operația a fost pentru un catalog de imagini. Y Fișierul care conține intrarea catalog de imagini este protejat la scriere. N Fișierul care conține intrarea catalog de imagini nu este protejat la scriere. Char 10 Numele dispozitivului virtual. Blank Indică faptul că operația 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)	

Tabela 227. Intrări jurnal ZR (Citire obiect) (continuare). Fișier descriere câmp QASYZRJE/J4/J5

Offset					
JE	J4	J5	Câmp	Format	Descriere
	324	710	Lungime nume obiect ²	Binary(4)	Lungimea numelui obiectului.
258	326	712	CCSID nume obiect ²	Binary(5)	identificator de set de caractere codate pentru numele obiect.
262	330	716	ID regiune sau țară nume obiect ²	Char(2)	ID-ul regiune sau țară pentru numele obiect.
264	332	718	ID limbă nume obiect ²	Char(3)	ID-ul limbă pentru numele obiectului.
267	335	721	(Zonă rezervată)	Char(3)	
270	338	724	ID fișier părinte ^{2,3}	Char(16)	ID-ul fișier al directorului părinte.
286	354	740	ID fișier obiect ^{2,3}	Char(16)	ID-ul fișier al obiectului.
302	370	756	Nume obiect ²	Char(512)	Numele obiectului.
	882	1268	ID fișier obiect	Char(16)	ID-ul fișier 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 țară nume cale	Char(2)	ID-ul de regiune sau țară pentru numele de cale absolută.
	919	1305	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	924	1310	Indicator nume cale	Char(1)	Indicator nume cale: Y Câmpul Nume cale absolută conține numele complet pentru cale absolută pentru obiect. N Câmpul Nume cale nu conține un nume de cale absolut pentru obiect, în schimb conține un nume de cale relativ. Câmpul ID fișier director înrudit este valid și poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	925	1311	ID fișier înrudit ⁴	Char(16)	Când câmpul indicator nume cale este "N", acest câmp va conține ID-ul de fișier al directorului care conține obiectul identificat în câmpul Nume cale. Altfel conține zerouri în format hexazecimal. ³
	941	1327	Nume cale ⁵	Char(5002)	Numele căii obiectului.

¹ Vedeți Tabela 228 la pagina 616 pentru o listă de coduri pentru tipurile de acces.

² Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fișiere QOpenSys, "rădăcină" și sistemele de fișiere definite de utilizator.

³ Un ID care are bitul cel mai din stânga setat și restul zero indică faptul că ID-ul NU este setat.

⁴ Dacă câmpul indicator nume cale este N, dar ID-ul fișier director înrudit conține doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informațiilor despre numele căii.

⁵ Acesta este câmpul lungime variabilă. Primii 2 octeți conțin lungimea numelui cale.

Tabela 228 listează codurile de acces folosite pentru intrările jurnal auditare obiecte din fișierele QASYJCJE/J4/J5, QASYRJE/J4/J5, QASYZCJE/J4/J5 și QASYZRJE/J4/J5.

Disponere intrări jurnal de auditare

Tabela 228. Codurile numerice pentru tipurile de acces

Cod	Tip acces	Cod	Tip acces	Cod	Tip acces
1	Adăugare	26	Încărcare	51	Trimitere
2	Activare program	27	Listare	52	Pornire
3	Analiză	28	Mutare	53	Transfer
4	Aplicare	29	Combinare	54	Urmărire
5	Apel sau TFRCTL	30	Deschidere	55	Verificare
6	Configurare	31	Tipărire	56	Alimentare
7	Modificare	32	Cerere	57	Lucru
8	Verificare	33	Revendicare	58	Atribut DLO citire/modificare
9	Închidere	34	Recepție	59	Securitate DLO citire/modificare
10	Curățare	35	Citire	60	Conținut DLO citire/modificare
11	Comparație	36	Reorganizare	61	Toate părțile DLO citire/modificare
12	Anulare	37	Eliberare	62	Adăugare constrângere
13	Copiere	38	Îndepărtare	63	Modificare constrângere
14	Creare	39	Redenumire	64	Înlăturare constrângere
15	Conversie	40	Înlocuire	65	Pornire procedură
16	Depanare	41	Continuare	66	Obținere acces la **OOPOOL
17	Ștergere	42	Restaurare	67	Semnare obiect
18	Abandon	43	Extragere	68	Înlăturarea tuturor semnăturilor
19	Afișare	44	Rulare	69	Curățare obiect semnat
20	Editare	45	Revocare	70	MOUNT
21	Oprire	46	Salvare	71	Descărcare
22	Fișier	47	Salvare cu eliberare spațiu de stocare	72	Oprire derulare înapoi
23	Acordare	48	Salvare și ștergere		
24	Reținere	49	Lansare		
25	Inițializare	50	Setare		

Anexa G. Comenzile și meniurile pentru comenzi de securitate

Această anexă descrie comenzile și meniurile pentru uneltele de securitate. Exemple despre folosirea comenzilor sunt incluse în acest manual.

Două meniuri sunt disponibile pentru uneltele de securitate:

- Meniul SECTOOLS (Unelte securitate) pentru a rula comenzile în mod interactiv.
- Meniul SECBATCH (Lansare sau Planificare rapoarte de securitate pentru batch) pentru a rula comenzile de rapoarte în batch. Meniul SECBATCH are două părți. Prima parte a meniului folosește comanda Lansare Job (SBMJOB) pentru a lansa rapoarte pentru procesarea imediată în batch.

A doua parte a meniului folosește comanda Adăugare intrare planificată a jobului (ADDJOBSCDE). O folosiți pentru a planifica rapoartele de securitate care să fie rulate regulat la un anumit moment de timp speciificat.

Opțiunile din meniul cu unelte de securitate

Următoarea ilustrație arată partea despre meniul SECTOOLS care se referă la profilurile utilizator. Pentru a accesa acest meniu, tastați GO SECTOOLS.

```
SECTOOLS                               Unelte de securitate

Selectați unul din următoarele:

  Gestionare profiluri
    1. Analizare parolelor implicite

    2. Afișarea listei de profiluri active
    3. Modificarea listei de profiluri active
    4. Analizarea activității profilului

    5. Afișarea planificatorului de activare
    6. Modificarea intrării planificatorului de activare

    7. Afișarea planificatorului de expirare
    8. Modificarea expirării intrării de planificare
    9. Tipărire internele profilului
```

Tabela 229 descrie aceste opțiuni de meniuri și comenzile asociate:

Tabela 229. Comenzi unelte pentru Profiluri utilizatori

Meniul ¹ Opțiune	Nume comandă	Descriere	Fișier bază de date folosit
1	ANZDFTPWD	Folosiți comanda Analizare parole implicite pentru a raporta și a lua acțiuni pe profilurile utilizatori care au o parolă egală cu cea a numelui profilului utilizator.	QASECPWD ²
2	DSPACTPRFL	Folosiți comanda Afișare listă de profiluri active pentru a afișa sau tipări lista de profiluri utilizatori care sunt exceptați de la procesarea ANZPRFACT.	QASECIDL ²

Tabela 229. Comenzi unelte pentru Profiluri utilizatori (continuare)

Meniul ¹ Opțiune	Nume comandă	Descriere	Fișier bază de date folosit
3	CHGACTPRFL	Folosiți comanda Modificare listă de profiluri activă pentru a adăuga sau înlătura profiluri de utilizatori din lista de excepții pentru comanda ANZPRFACT. Un profil utilizator care este în lista de profiluri active este permanent activ (doar dacă înlăturați 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	Folosiți comanda Analizare activitate profil pentru a dezactiva profilurile utilizator care nu au fost folosite un anumit număr de zile specificat. După ce folosiți comanda ANZPRFACT pentru a specifica numărul de zile, sistemul rulează jobul ANZPRFACT în fiecare noapte. Puteți folosi comanda CHGACTPRFL pentru a exclude profilurile utilizator de a fi dezactivate.	QASECIDL ²
5	DSPACTSCD	Folosiți comanda Afișare planificator activare profiluri pentru a afișa sau a tipări informații despre planificator pentru activarea sau dezactivarea profilurilor de utilizatori specifice. Creați planificatorul cu ajutorul comenzii CHGACTSCDE.	QASECACT ²
6	CHGACTSCDE	Folosiți 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 faceți planificarea, sistemul creează intrări de planificare a jobului pentru orele de activare și dezactivare.	QASECACT ²
7	DSPEXPSCDE	Folosiți comanda Afișare planificare expirare pentru a afișa sau tipări lista de profiluri de utilizatori care sunt planificați pentru a fi dezactivați sau înlăturați din sistem în viitor. Folosiți comanda CHGEXPSCDE pentru a seta profilurile de utilizatori care vor expira.	QASECEXP ²
8	CHGEXPSCDE	Folosiți comanda Modificare intrări de expirare pentru a planifica un profil utilizator pentru înlăturare. Puteți înlătura profilul temporar (prin dezactivarea lui) sau îl puteți șterge din sistem. Această comandă folosește o intrare de planificator de joburi care rulează în fiecare zi la 00:01 (1 minut după miezul nopții). Jobul privește în fișierul QASECEXP pentru a determina dacă orice profiluri utilizator sunt setate pentru a expira în acea zi. Folosiți comanda DSPEXPSCD pentru a afișa profilurile utilizatori care sunt planificate pentru expirare.	QASECEXP ²
9	PRTPRFINT	Folosiți comanda Tipărire profiluri interne pentru a tipări un report cu informațiile interne despre numărul de intrări într-un obiect profil utilizator (*USRPRF).	

Tabela 229. Comenzi unelte pentru Profiluri utilizatori (continuare)

Meniul ¹ Opțiune	Nume comandă	Descriere	Fișier bază de date folosit
<p>Note:</p> <p>1. Opțiuni sunt din meniul SECTOOLS.</p> <p>2. Acest fișier este în biblioteca QUSRSYS.</p>			

Puteți apăsa pe pagină jos în meniu pentru a vedea opțiunile suplimentare. Tabela 230 descrie opțiunile meniu și comenzile asociate pentru auditarea securității:

Tabela 230. Comenzi unelte pentru auditarea de securitate

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
10	CHGSECAUD	<p>Folosiți comanda Modificare auditare securitate pentru a seta auditarea securității și pentru a modifica valorile de sistem care controlează auditarea de securitate. Când rulați comanda CHGSECAUD, sistemul creează jurnalul de auditare de securitate (QAUDJRN) dacă nu există deja.</p> <p>Comanda CHGSECAUD furnizează opțiuni care simplifică setarea QAUDLVL (nivel de auditare) și pentru valorile de sistem QAUDLVL2 (extensie de nivel de auditare). Puteți specifica *ALL pentru a activa toate setările de nivel de auditare. Sau, puteți specifica *DFTSET pentru a activa cele mai comune setări folosite (*AUTFAIL, *CREATE, *DELETE, *SECURITY, și *SAVRST).</p> <p>Notă: Dacă folosiți uneltele de securitate pentru a seta auditarea, fiți siguri că planificați pentru gestiunea primitorilor jurnalului de auditare. Altfel, se poate să întâlniți imediat probleme la utilizarea disc-ului.</p>	
11	DSPSECAUD	Folosiți comanda Afișare auditare securitate pentru a afișa informații despre jurnalul de auditare securitate și valorile de sistem care controlează auditarea de securitate.	
12	CPYAUDJRNE	Folosiți comanda copiere intrări jurnal auditat pentru a copia intrările jurnalului de auditare de securitate în fișiere de ieșire.	QASYxxJ5 ²
<p>¹ Opțiuni sunt din meniul SECTOOLS.</p> <p>² xx este un tip de intrare de două caractere. De exemplu, fișierul de ieșire model pentru intrările de jurnal AE este QSYS/QASYAEJ5. Fișierele de ieșire model sunt descrise în Anexa F din această carte.</p>			

Cum se folosește meniul batch securitate

Următoarea este prima parte a meniului SECBATCH:

```
SECBATCH          Submit or Schedule Security Reports To Batch          Sistem:
Select one of the following:

Submit Reports to Batch
 1. Adopting objects
 2. Audit journal entries
 3. Authorization list authorities
 4. Command authority
 5. Command private authorities
 6. Communications security
 7. Directory authority
 8. Directory private authority
 9. Document authority
10. Document private authority
11. File authority
12. File private authority
13. Folder authority
```

Atunci când selectați o opțiune din acest meniu, vedeți ecranul Lansare job (SBMJOB), după cum urmează:

```
Lansare job (SBMJOB)
Introduceți opțiunile și apăsați Enter.
Comandă pentru rulare . . . . . > PRTADPOBJ USRPRF(*ALL)
-----
Nume job . . . . . *JOBBD      Nume, *JOBBD
Descriere job. . . . . *USRPRF  Nume, *USRPRF
  Bibliotecă. . . . .          Nume, *LIBL, *CURLIB
Coadă job . . . . . *JOBBD      Nume, *JOBBD
  Bibliotecă. . . . .          Nume, *LIBL, *CURLIB
Prioritate job (în JOBQ) . . . *JOBBD      1-9, *JOBBD
Prioritate ieșire (în OUTQ) . . *JOBBD      1-9, *JOBBD
Dispozitiv tipărire . . . . . *CURRENT    Nume, *CURRENT, *USRPRF...
```

Dacă vreți să modificați opțiunea implicită pentru comandă, puteți apăsa F4 (Prompt) din linia *Comanda de rulare*.

Pentru a vedea Planificarea rapoartelor batch, mergeți o pagină în jos la meniul SECBATCH. Prin folosirea opțiunilor din această parte a meniului, puteți de exemplu să configurați sistemul să ruleze versiuni modificate ale rapoartelor regulat.

```
SECBATCH          Submit or Schedule Security Reports To Batch          Sistem:
Select one of the following:

 28. User objects
 29. User profile information
 30. User profile internals
 31. Check object integrity

Schedule Batch Reports
 40. Adopting objects
 41. Audit journal entries
 42. Authorization list authorities
 43. Command authority
 44. Command private authority
 45. Communications security
 46. Directory authority
```

Puteți apăsa page down pentru opțiuni suplimentare ale meniului. Atunci când selectați o opțiune din această parte a meniului, vedeți ecranul Adăugare intrare planificator de joburi:

```

                                Adăugare intrare planif. job (ADDJOBSCDE)

Introduceți opțiunile și apăsați Enter.

Nume job . . . . . _____ Nume, *JOBID
Comandă de rulat . . . . . > PRTADPOBJ USRPRF(*ALL)

_____  

_____  

_____  

_____  

_____  

Frecvență . . . . . _____ *ONCE, *WEEKLY, *MONTHLY
Dată planificare, sau. . . . . *CURRENT Date, *CURRENT, *MONTHST
Zi planificare . . . . . *NONE *NONE, *ALL, *MON, *TUE.
+ pentru mai multe valori
Oră planificare . . . . . *CURRENT Oră, *CURRENT

```

Puteți să poziționați cursorul pe linia *Comandă de rulat* și apăsați F4 (Prompt) pentru a alege diferite setări pentru raport. Ar trebui să asociați un nume de job cu sens astfel încât să recunoașteți intrarea atunci când afișați intrările din planificarea de joburi.

Opțiunile din meniul batch securitate

Tabela 231 descrie opțiunile meniu și comenzile asociate pentru rapoartele de securitate.

Atunci când rulați rapoarte de securitate, sistemul afișează doar informații care îndeplinesc ambele criterii de selecție pe care le specificați și criteriul de selecție pentru unealtă. De exemplu, descrierea de job care specifică numele profil utilizator și securitate relevantă. De aceea, raportul descriere de job (PRTJOBDAUT) tipărește descrieri de job din biblioteca specificată numai dacă autorizația publică pentru descrierea de job nu este *EXCLUDE și dacă descrierea de job specifică un nume profil utilizator în parametrul USER.

În mod similar, atunci când tipăriți informații subsistem (comanda PRTSBSDAU), sistemul tipărește informații despre subsistem numai când descrierea subsistem are o intrare de comunicații care specifice un profil utilizator.

Dacă un anumit raport tipărește mai puține informații decât vă așteptați, consultați informațiile de ajutor online pentru a vedea criteriile de selecție pentru raport.

Tabela 231. Comenzi pentru rapoarte securitate

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
1, 40	PRTADPOBJ	Folosiți comanda Tipărire obiecte adoptare pentru a tipări o listă de obiecte ca adoptă autorizarea pentru profilul de utilizator specificat. Puteți 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 selecție. Raportul modificat listează diferențele între obiectele adoptate care sunt curent pe sistem și obiectele adoptate care au fost pe sistem ultima oară când rulează raportul.	QSECADPOLD ²
2, 41	DSPAUDJRNE ⁶	Folosiți comanda Afișare intrări jurnal de auditare pentru a afișa sau tipări informații despre intrările din jurnalul de auditare de securitate. Puteți selecta tipuri de intrări specifice, utilizatori specifice, și o perioadă de timp.	QASYxxJ5 ³

Tabela 231. Comenzi pentru rapoarte securitate (continuare)

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
3, 42	PRTPVTAUT *AUTL	<p>Când folosiți comanda Tipărire autorizări private pentru obiectele *AUTL, primiți o listă a tuturor listelor de autorizări pe sistem. Raportul include utilizatorii care sunt autorizați pentru fiecare listă și ce autorizări au utilizatorii pentru liste. Folosiți această informație pentru a vă ajuta să analizați sursele de autorizări de obiecte pe sistemul dumneavoastră.</p> <p>Acest raport are trei versiuni. Reportul complet listează toate listele de autorizate pe sistem. Raportul modificat listează adăugările și modificările pentru autorizări de când ați rulat ultima oară raportul. Raportul șters listează utilizatorii ale căror autorizări pentru listele de autorizare au fost șterse de la ultima rulare a raportului.</p> <p>Când tipăriți raportul complet, aveți opțiunea de a tipări o listă de obiecte pentru fiecare listă de autorizare securizată. Sistemul va crea un raport separat pentru fiecare listă de autorizare.</p>	QSECATLOLD ²
6, 45	PRTCMNSEC	<p>Folosiți comanda Tipărire securitate comunicație pentru a tipări setările relevante pentru securitate pentru obiectele care afectează comunicația pe sistemul dumneavoastră. Setările afectează cum utilizatorii și joburile pot intra pe sistemul dumneavoastră.</p> <p>Această comandă produce două rapoarte: un raport care afișează setările pentru listele de configurare pe sistem și un raport care listează parametrii relevanți pentru securitate pentru descriptorii de linie, pentru controlere și pentru descrierile dispozitivelor. Fiecare din aceste rapoarte au o versiune completă și o versiune modificată.</p>	QSECCMNOLD ²
15, 54	PRTJOBDAUT	<p>Folosiți comandă Tipărire autorizare descriere job pentru a tipări o listă a descriptorilor de joburi care specifică un profil de utilizator și au autorizările publice care nu sunt *EXCLUDE. Raportul arată autorizările speciale pentru profilul utilizatorului care este specificat în descrierea de job.</p> <p>Acest raport are două versiuni. Raportul complet listează toate obiectele de descriere de joburi care îndeplinesc criteriile de selecție. Raportul modificat listează diferențele între obiectele de descriere a jobului care sunt curent pe sistem și obiectele de descriere de job care au fost pe sistem ultima dată când s-a rulat raportul.</p>	QSECJBDOLD ²

Tabela 231. Comenzi pentru rapoarte securitate (continuare)

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
Vedeți nota 4	PRTPUBAUT	<p>Folosiți comanda Tipărire obiecte autorizate pentru publicare pentru a tipări o listă de obiecte ale cărei autorizare publică nu este *EXCLUDE. Când rulați comanda, specificați tipul obiectului și biblioteca sau bibliotecile pentru raport. Folosiți comanda PRTPUBAUT pentru a tipări informații despre obiecte pe care fiecare utilizator de pe sistem le poate accesa.</p> <p>Acest raport are două versiuni. Raportul complet listează toate obiectele care îndeplinesc criteriile de selecție. Raportul modificat listează diferențele între obiectele specificate care sunt curent pe sistem și obiectele (de același tip în aceeași bibliotecă) care au fost pe sistem ultima oară când ați rulat raportul.</p>	QPBxxxxxx ⁵
Vedeți nota 4.	PRTPVTAUT	<p>Folosiți comanda Tipărire autorizări private pentru a tipări o listă de autorizări private pentru obiecte pentru tipurile specificate în biblioteca specificată. Folosiți acest raport pentru a vă ajuta să determinați sursele de autorizări pentru obiecte.</p> <p>Acest raport are trei versiuni. Raportul complet listează toate obiectele care îndeplinesc criteriile de selecție. Raportul modificat listează diferențele între obiectele specificate care sunt curent pe sistem și obiectele (de același tip în aceeași bibliotecă) care au fost pe sistem ultima dată când s-a rulat raportul. Raportul șters listează utilizatorii ale căror autorizări pentru un obiect au fost șterse de când ați tipărit ultima dată raportul.</p>	QPVxxxxxx ⁵
24, 63	PRTQAUT	<p>Folosiți Tipărire raport coadă pentru a tipări setările de securitate pentru cozile de ieșire și cozile de joburi pe sistemul dumneavoastră. Aceste setări controlează cine poate vizualiza și modifica intrări în coada de ieșire sau coada de job.</p> <p>Acest raport are două versiuni. Raportul complet listează toate cozile de ieșire și obiectele cozii de job care îndeplinesc criteriul de selecție. Raportul modificat listează diferențele între obiectele cozii de ieșire și cozii de job care sunt curent pe sistem și între obiectele cozii de ieșire și cozii de job care au fost pe sistem ultima dată când ați rulat raportul.</p>	QSECQOLD ²
25, 64	PRTSBSDAUT	<p>Folosiți comanda Tipărire descriere subsistem pentru a tipări intrările de comunicație relevante de securitate pentru descrierile de subsistem pe sistemul dumneavoastră. Aceste setări controlează cum poate porni lucrul pe sistemul dumneavoastră și cum pot porni joburile. Raportul tipărește o descriere de subsistem doar are intrări de comunicații care specifică un nume de profil de utilizator.</p> <p>Acest raport are două versiuni. Raportul complet listează toate obiectele de descriere de subsistem care întrunesc criteriile de selecție. Raportul modificat listează diferențele între descrierea subsistemului care sunt curent pe sistem și obiectele descrierii subsistemului care au fost pe sistem ultima oară când ați rulat raportul.</p>	QSECSBDOLD ²

Tabela 231. Comenzi pentru rapoarte securitate (continuare)

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
26, 65	PRTSYSSECA	Folosiți comanda Tipărire atribute de securitate sistem pentru a tipări o listă de valori de sistem relevante de securitate și atribute de rețea. Raportul arată valoarea curentă și valoarea recomandată.	
27, 66	PRTRGPGM	Folosiți comanda Tipărire programe declanșare pentru a tipări o listă de programe declanșare care sunt asociate cu fișierele bazei de date pe sistemul dumneavoastră. Acest raport are două versiuni. Raportul complet listează toate programele declanșate care sunt asigurate și întrunesc criteriul dumneavoastră de selecție. Raportul modificat listează programele declanșate care au asigurate de la ultima oară când ați rulat raportul.	QSECTRGOLD ²
28, 67	PRTUSROBJ	Folosiți 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. Puteți folosi acest raport pentru a tipări o listă de obiecte utilizator care sunt într-o bibliotecă (ca de exemplu QSYS) care este în porțiunea de sistem în lista bibliotecii. Acest raport are două versiuni. Raportul complet listează toate obiectele utilizator care îndeplinesc criteriul de selecție. Raportul modificat listează diferențele între obiectele utilizator care sunt curent pe sistem și obiectele utilizator care sunt pe sistem ultima oară când ați rulat raportul.	QSECPUOLD ²
29, 68	PRTUSRPRF	Folosiți comanda Tipărire profil utilizator pentru a analiza profilurile utilizator care îndeplinesc criteriile specificate. Puteți selecta profilurile utilizator bazate pe autorizările specificate, clasele de utilizator, sau o nepotrivire între autorizările speciale și clasa de utilizator. Puteți tipări informațiile de autorizare, informațiile despre mediu, sau informațiile despre parolă.	
30, 69	PRTPRFINT	Folosiți comanda Tipărire profil intern pentru a tipări un raport cu informațiile interne a numărului intrărilor conținute într-un obiect profil utilizator (*USRPRF).	
31, 70	CHKOBJITG	Folosiți 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 detectați încercările de a introduce un program virus în sistemul dumneavoastră sau pentru a modifica un program pentru a realiza instrucțiuni neautorizate.	

Tabela 231. Comenzi pentru rapoarte securitate (continuare)

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
1		Opțiunile sunt din meniul SECBATCH.	
2		Acest fișier este în biblioteca QUSRSYS.	
3		xx este un tip de intrare de două caractere. De exemplu, fișierul de ieșire model pentru intrările de jurnal AE este QSYS/QASYAEJ5. Fișierele de ieșire model sunt descrise în Anexa F din această carte.	
4		Meniul SECTOOLS conține opțiuni pentru tipurile de obiect care sunt obișnuit scopul administratorilor de securitate. De exemplu, folosiți opțiunile 11 sau 50 pentru a rula comanda PRTPUBAUT pe obiectele *FILE. Folosiți opțiunile generale (18 și 57) pentru a specifica tipul de obiect. Folosiți opțiunile 12 și 15 pentru a rula comanda PRTPVTAUT pentru obiectele *FILE. Folosiți opțiunile generale (19 și 58) pentru a specifica tipul de obiect.	
5		xxxxxx din numele fișierului este tipul obiectului. De exemplu, fișierul pentru obiectele program este numit QPBPGM pentru autorizațiile publice și QVPVGM pentru autorizațiile private. Fișierele sunt în biblioteca QUSRSYS. Fișierul conține un membru pentru fiecare bibliotecă pentru care ați tipărit un raport. Numele membru este același ca și numele bibliotecă.	
6		Comanda DSPAUDJRNE este depășită. Comanda nu suportă toate tipurile de înregistrări de auditare a securității și nu listează toate câmpurile pentru înregistrările pe care ea le suportă.	

Comenzile pentru personalizarea securității

Puteți utiliza vrăjitorul de securitate pentru a personaliza securitatea sistemului. Pentru mai multe informații, vedeți subiectul "Complete the Security Wizard" în centrul de informare iSeries.

Tabela 232 descrie comenzile pe care le puteți folosi pentru a personaliza securitatea pe sistemul dumneavoastră. Aceste comenzi sunt în meniul SECTOOLS.

Tabela 232. Comenzi pentru Personalizarea sistemului dumneavoastră

Meniu ¹ Option	Nume comandă	Descriere	Fișier bază de date folosit
60	CFGSYSSEC	Folosiți 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 setate de comanda Configurare securitate sistem" descrie ce face comanda.	
61	RVKPUBAUT	Folosiți comanda Revocare autorizație publică pentru a seta autorizația publică la *EXCLUDE pentru un set de comenzi sensibile la securitate pe sistemul dumneavoastră. "Ce face comanda Revocare autorizare publică" la pagina 627 listează acțiunile pe care le realizează comanda RVKPUBAUT.	
1		Opțiuni sunt din meniul SECTOOLS.	

Valorile setate de comanda Configurare securitate sistem

Tabela 233 listează valorile sistem care sunt setate când rulați comanda CFGSYSSEC. Comanda CFGSYSSEC rulează un program care este numit QSYS/QSECCFGS.

Tabela 233. Valori setate de comanda CFGSYSSEC

Nume valoare sistem	Setare	Descriere valoare sistem
QAUTOCFG	0 (Nu)	Configurare automată a noilor dispozitive

Tabela 233. Valori setate de comanda CFGSYSSEC (continuare)

Nume valoare sistem	Setare	Descriere valoare sistem
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 și programele care adoptă autorizație pot fi restaurare
QDEVRCYACN	*DSCMSG (Deconectare cu mesaj)	Acțiunea sistem atunci când comunicațiile sunt restabilite
QDSCJOBITV	120	Perioada de timp înainte ca sistemul să acționeze la un job deconectat
QDSPSGNINF	1 (Da)	Dacă utilizatorii văd ecranul cu informații de semnare
QINACTITV	60	Perioada de timp înainte ca sistemul să acționeze la un job interactiv inactiv
QINACTMSGQ	*ENDJOB	Acțiunile realizate de sistem pentru un job inactiv
QLMTDEVSSN	1 (Da)	Dacă utilizatorii sunt limitați la semnarea pe un singur dispozitiv la un moment dat
QLMTSECOFR	1 (Da)	Dacă utilizatorii *ALLOBJ și *SERVICE sunt limitați la anumite dispozitive
QMAXSIGN	3	Câte încercări consecutive, fără succes de semnare sunt permise
QMAXSGNACN	3 (Ambele)	Dacă sistemul dezactivează dezactivează stația de lucru sau profilul utilizator atunci când limita QMAXSIGN este atinsă.
QPWDEXPITV	60	Cât de des trebuie să-și modifice utilizatorii parolele
QPWDMINLEN	6 (Vedeți nota 3)	Lungime minimă pentru parole
QPWDMAXLEN	8 (Vedeți nota 4)	Lungime maximă pentru parole
QPWDPOSDIF	1 (Da)	Dacă fiecare poziție dintr-o parolă trebuie să difere de aceeași poziție din vechea parolă
QPWDLMTCHR	Vedeți nota 2	Caractere care nu sunt permise în parolă
QPWDLMTAJC	1 (Da)	Dacă numere adiacente sunt interzise în parole
QPWDLMTREP	2 (Nu pot fi repetate consecutiv)	Dacă sunt interzise caractere repetate în parole
QPWDRQDDGT	1 (Da)	Dacă parolele trebuie să aibă cel puțin un număr
QPWDRQDDIF	1 (32 parole unice)	Câte parole unice sunt necesare înainte ca o parolă să poată fi repetată
QPWDVLDPGM	*NONE	Programul ieșire utilizator pe care sistem îl apelează pentru a valida parolele
QRMTSIGN	*FRCSIGNON	Cum manipulează sistemul o încercare de semnare la distanță (passthrough sau TELNET).
QRMTSVRATR	0 (Off)	Permite ca sistemul să fie analizat la distanță.
QSECURITY	50	Nivelul de securitate care este impus
QVFYOBJRST	3	Verificare obiect la restaurare
Note:		
1. Dacă rulați curent cu QSECURITY de 30 sau mai puțin, revedeți informațiile din Capitolul 2 din această carte înainte de a modifica la un nivel de securitate mai înalt.		
2. Caracterele restricționate sunt stocate în ID CPXB302 în fișierul de mesaje QSYS/QCPFMSG. Sunt livrate ca AEIOU@\$. Puteți folosi comanda Modificare descriere mesaj (CHGMSGD) ca să modificați caracterele restricționate.		
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.		

Comanda CFGSYSSEC setează de asemenea parola la *NONE pentru următoarele profiluri utilizator furnizate de IBM:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

În sfârșit, comanda CFGSYSSEC configurează auditarea de securitate conform valorilor pe care le-ați specificat folosind comanda Modificare auditare securitate (CHGSECAUD).

Modificarea programului

Dacă unele dintre aceste setări nu sunt corespunzătoare cu instalarea dumneavoastră, puteți crea propria versiune de program care procesează comanda. Faceți următoarele acțiuni:

- ___ Pasul 1. Folosiți comanda Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care rulează atunci când folosiți comanda CFGSYSSEC. Programul pentru extragere este QSYS/QSECCFGS. Atunci când extrageți, dați-i un *nume diferit*.
- ___ Pasul 2. Editați programul pentru a realiza modificările. Apoi compilați-l. Atunci când îl compilați, asigurați-vă că *nu* înlocuiți programul QSYS/QSECCFGS furnizat de IBM. Programul dumneavoastră ar trebuie să aibă un nume diferit.
- ___ Pasul 3. Folosiți comanda Modificare comandă (CHGCMD) pentru a modifica parametrul de comandă (PGM) pentru comanda CFGSYSSEC. Setări valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creați un program în biblioteca QGPL care se numește MYSECCFG, veți introduce următoarea comandă:

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

Note:

- a. Dacă modificați programul QSYS/QSECCFGS, IBM nu poate garanta sau sugera fiabilitatea, capacitatea de service, performanța sau funcția programului. Se declină în mod expres răspunderea pentru garanțiile implicite de vandabilitate și de potrivire cu un anumit scop.
- b. Dacă modificați comanda CFGSYSSEC pentru a utiliza un program diferit de procesare a comenzilor, semnătura digitală a acestei comenzi nu va mai fi validă.

Ce face comanda Revocare autorizare publică

Puteți folosi comanda Revocare autorizație publică (RVKPUBAUT) pentru a seta autorizația publică *EXCLUDE pentru un set de comenzi și programe. Comanda RVKPUBAUT rulează un program care este numit QSYS/QSECRVKP. La livrare, QSECRVKP revocă autorizația publică (prin setarea la *EXCLUDE) pentru comenzile care sunt listate în Tabela 234 la pagina 628 și interfețele programabile pentru aplicații (API) care sunt listate în Tabela 235 la pagina 628. Atunci când sosește sistemul dumneavoastră, aceste comenzi și API-uri au autorizația publică setată la *USE.

Comenzile care sunt listate în Tabela 234 la pagina 628 și API-urile care sunt listate în Tabela 235 la pagina 628 realizează pe sistemul dumneavoastră funcții care pot oferi posibilitatea de a face rău. Ca administrator de securitate, ar trebui să autorizați explicit utilizatorii să ruleze aceste comenzi și programe decât să le faceți disponibile tuturor utilizatorilor de pe sistem.

Atunci când rulați comanda RVKPUBAUT, specificați biblioteca în care se află aceste comenzi. Biblioteca implicită este QSYS. Dacă aveți mai multe limbi naționale pe sistem, trebuie să rulați comanda pentru fiecare bibliotecă QSYSxxx.

Tabela 234. Comenzi ale căror autorizații publice sunt setate de comanda RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

API-urile din Tabela 235 sunt toate în biblioteca QSYS:

Tabela 235. Programe ale căror autorizații publice sunt setate de comanda RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Pe V3R7, când rulați comanda RVKPUBAUT, sistemul setează autorizația publică pentru directorul rădăcină la *USE (numai dacă nu este deja *USE sau mai puțin).

Modificarea programului

Dacă unele dintre aceste setări nu sunt corespunzătoare pentru instalarea dumneavoastră, puteți crea propria versiune de program care procesează comanda. Faceți următoarele acțiuni:

- ___ Pasul 1. Folosiți comanda Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care rulează atunci când folosiți comanda RVKPUBAUT. Programul pentru a fi extras este QSYS/QSECRVKP. Atunci când îl extrageți, dați-i un nume diferit.
- ___ Pasul 2. Editați programul pentru a realiza modificările. Apoi compilați-l. Atunci când îl compilați, asigurați-vă că nu înlocuiți programul furnizat de IBM QSYS/QSECRVKP. Programul dumneavoastră ar trebui să aibă un nume diferit.
- ___ Pasul 3. Folosiți comanda Modificare comandă (CHGCMD) pentru a modifica programul să proceseze parametrul de comandă (PGM) pentru comanda RVKPUBAUT. Setări valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creați un program în biblioteca QGPL care se numește MYRVKPGM, veți introduce următoarea comandă:
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)

Note:

- a. Dacă modificați programul QSYS/QSECRVKP, IBM nu poate garanta sau implica încredere, servibilitate, performanțe sau funcționabilitate pentru program. Garanțiile implicate pentru fabricare sau potrivirea cu un anumit scop nu sunt acordate explicit.
- b. Dacă modificați comanda RVKPUBAUT pentru a utiliza un program de procesare comenzi diferit atunci semnătura digitală a acestei comenzi nu va mai fi validă.

Anexa H. Informații înrudite pentru iSeriesSecurity Reference

Mai jos sunt prezentate manuale de produs și cărți Redbooks de la IBM (în format PDF), situri Web și subiecte din centrul de informare care sunt legate de subiectul referință la securitate. Puteți vizualiza sau tipări oricare dintre PDF-uri.

Securitatea avansată

- *Tips and Tools for Securing Your iSeries*, SC41-5300-07 furnizează un set de sugestii practice pentru utilizarea caracteristicilor de securitate ale iSeries și pentru stabilirea procedurilor de operare legate de securitate. Această carte descrie de asemenea cum se face setarea și utilizarea uneltelor de securitate care fac parte din i5/OS. Vedeți iSeries: CD-ROM-ul manuale suplimentare Centrul de informare.
- *Implementing iSeries 400 Security, 3rd Edition* de Wayne Madden și Carol Woodbury. Loveland, Colorado: 29th Street Press, o divizie a Duke Communication International, 1998. Furnizează îndrumări și sugestii practice pentru planificarea, setarea și gestionarea securității iSeries.

Număr de comandă ISBN
1-882419-78-2

Salvarea de rezervă și recuperarea

- *Backup and Recovery*, SC41-5304-08 furnizează informații despre planificarea unei strategii de salvare de rezervă și de recuperare, despre salvarea informațiilor din sistemul dumneavoastră și despre recuperarea sistemului, a pool-urilor de memorie auxiliară și a opțiunilor de protejare a discului. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Informații suplimentare de salvare de rezervă și de recuperare pot fi găsite în Centrul de informare. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru informații suplimentare.

Informații privind securitatea de bază și securitatea fizică

- Subiectul Securitatea de bază a sistemului și planificarea din Centrul de informare explică de ce este necesară securitatea, definește conceptele importante și furnizează informații despre planificarea, implementarea și monitorizarea securității de bază în sistem. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Programul licențiat iSeries Access pentru Windows

- Subiectul iSeries Access pentru Windows din Centrul de informare furnizează informații tehnice despre programele iSeries Access pentru Windows pentru toate versiunile de iSeries Access pentru Windows. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Comunicațiile și lucrul în rețea

- *SNA Distribution Services*, SC41-5410-01 furnizează informații despre configurarea unei rețele pentru SNADS (Systems Network Architecture distribution services) și configurarea unei punți VM/MVS (Virtual Machine/Multiple Virtual Storage). În plus, sunt discutate funcțiile de distribuire a obiectelor, serviciile pentru biblioteca de documente și serviciile pentru directorul de distribuție sistem.
- *Remote Work Station Support*, SC41-5402-00 furnizează informații despre cum se face setarea și utilizarea suportului pentru stație de lucru la distanță, cum ar fi passthrough stație de afișare, facilitate de comandă gazdă distribuită și atașament la distanță 3270. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.

- Centrul de informare furnizează informații despre procesarea de fișiere la distanță. El descrie cum se face definirea unui fișier la distanță în i5/OS DDM (distributed data management), cum se creează un fișier DDM, ce utilitare de fișiere sunt suportate prin DDM și cerințele DDM i5/OS în raport cu alte sisteme. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.
- Centrul de informare furnizează informații care descriu cum se face utilizarea și configurarea TCP/IP și a mai multor aplicații TCP/IP, cum ar fi FTP, SMTP și TELNET. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Criptografia

- *Cryptographic Support/400*, SC41-3342-00 descrie capabilitățile de securitate de date ale produsului program cu licență Cryptographic Facility. El explică cum se face utilizarea facilității și furnizează informații de referință pentru programatori. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.

Operațiile de sistem generale

- “Operațiile de sistem de bază” din Centrul de informare furnizează informații privind modul în care se face pornirea și oprirea sistemului și cum se face tratarea problemelor de sistem. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii suplimentare.

Instalarea programelor livrate de IBM și configurarea sistemului

- *Local Device Configuration*, SC41-5121-00 furnizează informații despre cum se face o configurare inițială și cum se face modificarea acelei configurații. Conține de asemenea informații conceptuale despre configurarea dispozitivelor. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.
- *Instalarea, modernizarea sau ștergerea i5/OS și software-ului înrudit*, SC41-5120-09 furnizează proceduri pas-cu-pas pentru instalarea inițială, pentru instalarea programelor cu licență, pentru PTF-uri și pentru limbi secundare de la IBM. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.

Sistemul de fișiere integrat

- Subiectul Sistemul de fișiere integrat din Centrul de informare iSeries furnizează o privire generală asupra Sistemul de fișiere integrat, inclusiv ce este, cum poate fi folosit și ce interfețe sunt disponibile. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Internetul

- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* SG24-4929 discută problemele legate de securitate și riscurile conectării serverului iSeries la Internet. Vi se oferă exemple, recomandări, sugestii și tehnici pentru aplicații.
- *iSeries and the Internet*, G325-6321, vă ajută să vă rezolvați problemele potențiale de securitate pe care le puteți avea la conectarea iSeries la Internet. Pentru informații suplimentare, vizitați următoarea pagină de bază IBM I/T (Information Technology) Security :
<http://www.ibm.com/security>
- *Cool Title About the AS/400 and Internet*, SG24-4815, vă poate ajuta să înțelegeți și apoi să utilizați Internetul (sau rețeaua dumneavoastră internă) de pe iSeries. Vă ajută să înțelegeți cum se folosesc funcțiile și caracteristicile. Această carte vă inițiază pentru a folosi e-mail-ul, transferul de fișiere, emularea de terminal, gopher, HTTP și 5250 pentru gateway HTML.

IBM Lotus Domino

- URL-ul <http://www.lotus.com/ldd/doc> furnizează informații despre Lotus Notes, Domino și IBM Domino pentru iSeries. De pe acest sit Web puteți descărca informații în formatul de bază de date Domino (.NSF) și în formatul Adobe Acrobat (.PDF), puteți căuta în baza de date și puteți afla cum puteți obține manuale tipărite.

Suportul optic

- *Optical Support*, SC41-5310-04 furnizează informații despre funcții care sunt unice pentru *Optical Support*. Conține de asemenea informații folositoare pentru utilizarea și înțelegerea dispozitivelor CD, a dispozitivelor de bibliotecă de mediu optic atașate direct și a dispozitivelor de bibliotecă de mediu optic atașate la LAN. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.

Tipărirea

- Centrul de informare furnizează informații despre elementele și conceptele de tipărire ale sistemului, despre suportul de fișier imprimantă și de spool de tipărire pentru operațiile de tipărire și despre conectarea imprimantei. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Programarea

- *CL Programming*, SC41-5721-06, furnizează o discuție amplă a subiectelor de programare, incluzând o discuție generală asupra obiectelor și a bibliotecilor, asupra programării CL, asupra controlului de flux și a comunicației între programe, asupra gestionării obiectelor din programele CL și asupra creării de programe CL. Alte subiecte includ mesajele predefinite și improvizate și tratarea mesajelor, definirea și crearea de comenzi și meniuri definite de utilizator, testarea aplicațiilor, incluzând modul de depanare, puncte de întrerupere, urmăriri și funcții de afișare. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Subiectul CL din Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii) furnizează o descriere completă a limbajului CL (control language - limbaj de control) iSeries și a comenzilor lui din i5/OS. Comenzile i5/OS sunt utilizate pentru a accesa funcții ale programului licențiat i5/OS (5722-SS1). Toate comenzile CL non-i5/OS — cele asociate cu celelalte programe cu licență, incluzând toate limbile și diversele utilitare — sunt descrise în alte cărți care suportă acele programe cu licență.
- Subiectul Programare din Centrul de informare furnizează informații despre multe dintre limbajele și utilitarele disponibile în iSeries. El conține rezumate ale:
 - Tuturor comenzilor CL iSeries (din programele i5/OS și din toate celelalte programe cu licență), sub diferite forme.
 - Informațiilor înrudite cu comenzile CL, cum ar fi mesajele de eroare care pot fi monitorizate de fiecare comandă și fișierele livrate de IBM care sunt utilizate de unele comenzi.
 - Obiectelor livrate de IBM, incluzând biblioteci.
 - Valorilor sistem livrate de IBM.
 - Cuvintelor cheie DDS pentru fișiere fizice, logice, de afișare, de imprimantă și ICF.
 - Instrucțiunilor REXX și ale funcțiilor încorporate.
 - Altor limbaje (cum ar fi RPG) și altor utilitare (cum ar fi SEU și SDA).
- Centrul de informare conține mai multe subiecte privind Administrarea sistemelor și Controlul funcționării din iSeries. Unele din aceste subiecte includ colecții de date de performanță, administrare de valori sistem și administrare de spațiu de stocare. Pentru detalii despre accesarea Centrului de informare, vedeți “Cerințe preliminare și informații înrudite” la pagina xvi.
- Subiectul gestiunea muncii din centrul de informații furnizează informații despre cum se face crearea și modificarea o gestiune a muncii.
- Subiectul API din Centrul de informare (vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii) furnizează informații despre cum se face crearea, utilizarea și ștergerea obiectelor care ajută la gestionarea performanței de sistem, utilizarea eficientă a spool-ului și întreținerea eficientă a fișierelor bază de date. Această carte include de asemenea informații despre crearea și întreținerea de programe pentru obiectele sistem și despre extragerea informațiilor i5/OS prin operații cu obiecte, fișiere bază de date, joburi și fișiere spool.

Utilitare

- *ADTS for AS/400: Source Entry Utility*, SC09-2605-00 furnizează informații despre folosirea utilitarului SEU (source entry utility) din ADT (Application Development Tools) pentru a crea și edita membrii sursă. Cartea explică cum se face pornirea și terminarea unei sesiuni SEU și cum se face utilizarea numeroaselor caracteristici ale acestui editor de text. Cartea conține exemple pentru a ajuta atât utilizatorii noi, cât și pe cei experimentați să realizeze diverse operații de editare, de la cele mai simple comenzi de linie până la utilizarea prompturilor predefinite pentru limbajele de nivel înalt și pentru formate de date. Vedeți iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Subiectul Bază de date DB2 Universal pentru iSeries din centrul de informații furnizează o privire generală despre cum să proiectați, scrie, rula și testa instrucțiunile din DB2 UDB pentru iSeries Query Manger și SQL Development Kit. Descrie de asemenea SQL interactiv (Structured Query Language) și furnizează exemple despre cum se scriu instrucțiunile SQL în programe COBOL, RPG, C, FORTRAN și PL/I. Vedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.
- Subiectul Bază de date DB2 Universal pentru iSeries din Centrul de informare furnizează informații despre cum se face:
 - Construirea, întreținerea și rularea de interogări SQL
 - Crearea de rapoarte de la cele mai simple la cele complexe
 - Construirea, actualizarea, gestionarea, interogarea și raportarea în tabelele bazei de date, utilizând o interfață bazată pe formulare
 - Definirea și modelarea interogărilor SQL și a rapoartelor pentru includerea în programe de aplicațieVedeți “Cerințe preliminare și informații înrudite” la pagina xvi pentru detalii.

Anexa I. Observații

Aceste informații au fost elaborate pentru produsele și serviciile oferite în S.U.A. Este posibil ca

IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Luați legătura cu reprezentantul IBM local pentru informații despre produsele și serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Însă este responsabilitatea utilizatorului să evalueze și să verifice funcționarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licență cu privire la aceste patente. Puteți trimite solicitări de licență, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pentru cererile de licență privind informații (DBCS) pe doi octeți, contactați Departamentul de proprietate intelectuală IBM din țara dumneavoastră sau trimiteți cereri, în scris, la:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor țări unde asemenea prevederi nu sunt în concordanță cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANȚIE, EXPRESĂ SAU IMPLICITĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilității pentru garanțiile exprese sau implicite în anumite tranzacții și de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informații pot include inexactități tehnice sau erori tipografice. Periodic, informațiile incluse aici sunt modificate; aceste modificări vor fi încorporate în noile ediții ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment, fără notificare.

Referirile din aceste informații la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezența 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 folosi sau distribui informațiile pe care le furnizați în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație pentru dumneavoastră.

Posesorii de licențe pentru acest program care doresc să obțină informații despre el în scopul de a permite: (I) schimbul de informații între programe create independent și alte programe (inclusiv acesta) și (II) utilizarea mutuală a informațiilor 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 informații pot fi disponibile cu condiția respectării termenilor și condițiilor, iar în unele cazuri cu plata unor taxe.

Programul licențiat descris în această publicație și toate materialele licențiate disponibile pentru el sunt furnizate de IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice acord echivalent între noi.

Toate datele de performanță din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obținute în alte medii de funcționare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare și nu există nici o garanție că aceste măsurători vor fi identice pe sistemele disponibile pe piață. Mai mult decât atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informațiile privind produsele non-IBM au fost obținute de la furnizorii acestor produse, din anunțurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse și nu poate confirma acuratețea performanțelor, compatibilitatea sau oricare alte pretenții legate de produsele non-IBM. Întrebările legate de capacitățile produselor non-IBM le veți adresa furnizorilor acestor produse.

Toate declarațiile privind direcțiile de viitor și intențiile IBM-ului pot fi schimbate sau se poate renunța la ele, fără notificare prealabilă și reprezintă doar scopuri și obiective.

Aceste informații conțin exemple de date și rapoarte folosite în operațiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci și de produse. Toate aceste nume sunt fictive și orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidență.

LICENȚĂ COPYRIGHT:

Aceste informații conțin exemple de programe de aplicații în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteți copia, modifica și distribui aceste exemple de programe sub orice formă fără ca IBM să pretindă vreo plată, când o faceți în scopul dezvoltării, folosirii, promovării și distribuirii programelor de aplicații conform cu interfața de programare aplicații pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunțit în toate condițiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcționarea acestor programe.

Fiecare copie sau porțiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunț de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Părți din acest cod sunt derivate din IBM Corp. Sample Programs. © Copyright IBM Corp. _introduceți anul sau anii_. Toate drepturile rezervate.

Dacă vizualizați aceste informații folosind o copie electronică, fotografiile și ilustrațiile color s-ar putea să nu apară.

Informații privind interfața de programare

Această publicație, iSeries Referințe privind securitatea, conține informații despre interfețele de programare menite să permită beneficiarului obținerea serviciilor i5/OS.

Mărci comerciale

Următorii termeni sunt mărci comerciale deținute de International Business Machines Corporation în Statele Unite, în alte țări sau ambele:

AIX
AS/400
COBOL/400
DB2
DB2 Universal Database
Domino
DRDA
e(logo)server
eServer
i5/OS
IBM
iSeries
Lotus
MQSeries
NetServer
Notes
OfficeVision
OS/2
Print Services Facility
PrintManager
Redbooks
RPG/400
SAA
SecureWay
System/36
System/38
SystemView
WebSphere
zSeries

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci comerciale deținute de Microsoft Corporation în Statele Unite, în alte țări sau ambele.

Java și toate mărcile comerciale bazate pe Java sunt mărci comerciale deținute de Sun Microsystems, Inc. în Statele Unite, în alte țări sau ambele.

Linux este o marcă comercială deținută de Linus Torvalds în Statele Unite, în alte țări sau ambele.

Alte nume de companii, de produse sau de servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

Utilizare personală: Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza lucrări derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

Utilizare comercială: Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit al IBM.

Cu excepția a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licențe sau drepturi, explicit sau implicit, pentru Publicații sau alte informații, date, software sau altă proprietate intelectuală conținută în acestea.

IBM își rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicațiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât în deplină conformitate cu legile și regulamentele aplicabile, inclusiv toate legile și regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANȚIE PRIVIND CONȚINUTUL ACESTOR PUBLICAȚII. ACESTE PUBLICAȚII SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Index

Caractere speciale

(*Mgt) Management authority 112
(*Ref) Reference authority 112
(numărul de identificare utilizator) parametru
 profil utilizator 90
(valoarea sistem QPWDLMTAJC (caracterele
 alăturate ale parolei interzise)
 valoarea setată de comanda
 CFGSYSSEC 625
*ADD (add) authority 112
*ALLOBJ
 autorizare de clasă utilizator 8
*ASSIST program de tratare tastă Attn 86
*CRQD
 restaurare
 intrare jurnal auditare
 (QAUDJRN) 244
*DISABLED (dezactivare) stare profil
 utilizator
 descriere 62
 profil utilizator QSECOFR (responsabil cu
 securitatea) 62
*DLT (delete) authority 112
*ENABLED (activare) stare profil
 utilizator 62
*EXECUTE (execute) authority 112
*Mgt (Management) authority 112
*NOSTSMSG (nici un mesaj de stare) opțiune
 utilizator 90
*R (read - citire) 301
*R (read) 113
*Ref (Reference) authority 112
*ROLLKEY (tastă de rotire) opțiune
 utilizator 90
*RW (read, write) 113, 301
*RWX (read - citire, write - scriere, execute -
 execuție) 301
*RWX (read, write, execute) 113
*RX (read - citire, execute - execuție) 301
*RX (read, execute) 113
*SAVSYS (save system) special authority
 *OBJEXIST authority 112
*STSMSG (mesaj de stare) opțiune
 utilizator 90
*UPD (update) authority 112
*W (write - scriere) 301
*W (write) 113
*WX (write - scriere, execute - execuție) 301
*WX (write, execute) 113
*X (execute - execuție) 301
*X (execute) 113

A

acces
 împiedicare
 interfață nesuportată 13
 prevenire
 neautorizat 233

acces (*continuare*)
 restricționare
 consolă 230
 stații de lucru 230
acordare
 autorizare folosind un obiect referit 144
 autorizare obiect 272
 efectul asupra autorizării
 anterioare 141
 obiecte multiple 141
 autorizare utilizator
 descriere comandă 274
 permisiune utilizator 275
activare
 funcția de auditare a securității 256
 profil utilizator 617
 automat 617
 program eșantion 104
 profil utilizator QSECOFR (responsabil cu
 securitatea) 62
activare (*ENABLED) stare profil
 utilizator 62
Acumulare autorizări speciale 214
adăugare
 autorizare obiect de bibliotecă de
 documente (DLO) 275
 autorizare utilizator 140
 intrare de autentificare server 276
 intrare director 276
 intrare lista de biblioteci 183, 186
 listă de autorizare
 intrări 145
 obiecte 146
 utilizatori 145
 listă de autorizații
 intrări 271
 utilizatori 271
 profiluri utilizator 98
add (*ADD) authority 112, 300
ADDFTNTBLE (Add DBCS Font Table Entry
 - Adăugare intrare tabelă fonturi DBCS)
 autorizație obiect cerută pentru
 comenzi 311
ADDTCPHTE (Adăugare intrare tabel gazdă
 TCP/IP)
 obiect autorizare cerută 438
ADDTRCFTR
 profiluri utilizator livrat de IBM
 autorizate 288
adoptare autorizare proprietar
 Vedeți autorizare adoptată
adoptată
 autorizare
 afișare 134
afișare
 adoptare program 130
 auditare de securitate 277
 auditare obiect 254
 auditare securitate 619
 autorizare 133, 272

afișare (*continuare*)
 autorizare adoptată
 descriere comandă 275
 fișiere critice 209
 parametrul USRPRF 130
 programe care adoptă un profil 130
 autorizare obiect 268, 272
 autorizare obiect de bibliotecă de
 documente 275
 descriere de job 232
 descriere obiect 272
 deținători de autorizare 131
 descriere comandă 271
 domeniu obiect 13
 fișier spool 186
 informații de semnare
 valoarea de sistem QDPSGNINF 22
 informații semnare
 parametru profil utilizator
 DPSGNINF 73
 recomandări 74
 intrări jurnal de auditare 277
 intrări jurnal de auditare
 (QAUDJRN) 234, 260
 jurnal
 auditare activitate fișier 209, 266
 listă de autorizații
 obiecte de bibliotecă de documente
 (DLO) 275
 utilizatori 271
 nume cale 143
 obiect
 originator 123
 obiecte din lista de autorizare 146
 obiecte listă de autorizații 271
 parametru CRTAUT (create authority -
 creare autorizare) 137
 profil utilizator
 descriere comandă 274
 individual 104
 listă de profiluri activă 617
 listă rezumat 104
 planificare activare 617
 planificator de expirare 617
 programe care adoptă 130, 268
 starea program 13
 Comanda DSPPGM (Display Program
 - Afișare program) 13
 toate profilurile utilizator 104
 utilizatori autorizați 267, 274
 valoare sistem QAUDCTL (auditare
 control) 619
 valoarea sistem QAUDLVL (nivel
 auditare) 619
 valoarea de sistem QAUDCTL (control
 auditare) 277
 valoarea de sistem QAUDLVL (nivel de
 auditare) 277
afișare DSPAUTUSR (Display Authorized
 Users - Afișare utilizatori autorizați) 267

afișare funcții de service
 autorizare specială *SERVICE
 (service) 70

AFP (Advanced Function Printing - Funcție
 avansată de tipărire)
 autorizație obiect cerută pentru
 comenzi 311

ajustare performanță
 securitate 192

alertă
 necesități ale autorizării obiect pentru
 comenzi 312

analizare
 autorizare obiect 268
 eșuare de program 268
 intrări jurnal audit, metode 260
 profil utilizator
 de autorizările speciale 621
 de către clasa de utilizatori 621
 profiluri de utilizator 267

analiză problemă
 valoare de sistem atribut service la distanță
 (QRMTSRVATR) 33

anulare
 funcție de auditare 260

ANZBESTMDL
 profiluri utilizator livrat de IBM
 autorizate 288

ANZDBF
 profiluri utilizator livrat de IBM
 autorizate 288

ANZDBFKEY
 profiluri utilizator livrat de IBM
 autorizate 288

ANZJVM
 profiluri utilizator livrat de IBM
 autorizate 288

ANZPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 288

ANZPRFACT
 profiluri utilizator livrat de IBM
 autorizate 288

apelare
 program
 transferare autorizare adoptată 128

API (application programming interface -
 interfață de programare aplicație)
 nivel de securitate 40 13

API-ul de extragere informații receptor jurnal
 auditare obiect 477

API-ul QjoAddRemoteJournal (Adăugare
 jurnal la distanță)
 auditare obiect 476

API-ul QjoChangeJournal State (Modificare
 stare jurnal)
 auditare obiect 476

API-ul QjoEndJournal (terminare jurnalizare)
 auditare obiect 448

API-ul QjoEndJournal (Terminare jurnalizare)
 auditare obiect 476

API-ul QjoRemoveRemoteJournal (Înlăturare
 jurnal la distanță)
 auditare obiect 476

API-ul QjoRetrieveJournalEntries (Extragere
 intrări jurnal)
 auditare obiect 476

API-ul QjoRetrieveJournalInformation
 (Extragere informații jurnal)
 auditare obiect 477

API-ul QJORJIDI (Extragere informații
 identificator jurnal (JID))
 auditare obiect 476

API-ul QjoSJRNE (Trimitere intrare jurnal)
 auditare obiect 477

API-ul QjoStartJournal (Pornire jurnalizare)
 auditare obiect 448, 477

API-ul QSPRJOBQ (Extragere informații
 coadă joburi)
 auditare obiect 475

API-ul QWCLSCDE (Listare intrare
 planificare job)
 auditare obiect 476

Arhitectură rețea de sisteme (SNA)
 profil utilizator servicii distribuție
 (QSNADS) 281

atribut de rețea
 acces de gestiune a datelor distribuite
 (DDMACC) 233
 acțiune job (JOBACN) 233
 autorizare specială *SECADM
 (administrator de securitate) 69
 autorizație obiect cerută pentru
 comenzi 395
 comandă pentru setare 278
 DDMACC (distributed data management
 access - acces de gestiune a datelor
 distribuite) 233
 JOBACN (job action - acțiune job) 233
 modificare
 intrare jurnal auditare
 (QAUDJRN) 248
 PCSACC (acces suport PC) 233
 Suport PC (PCSACC) 233

atribut de rețea DDMACC (distributed data
 management access - acces de gestiune a
 datelor distribuite) 233

atribut de rețea JOBACN (acțiune job) 233

atribut de rețea JOBACN acțiune job 233

atribut de rețea PCSACC (PC Support access -
 acces de suport PC) 233

atribut domeniu, obiect
 afișare 13
 descriere 13

atribut rețea
 acțiune job (JOBACN) 189
 Cerere client acces (PCSACC) 189
 comandă pentru setare 625
 JOBACN (acțiune job) 189
 PCSACC (Cerere client acces) 189
 tipărire securitate relevantă 621

atribut rețea acțiune job (JOBACN) 189

atribut rețea JOBACN (acțiune job) 189

atribut rețea
 cerere DDM acces (DDMACC) 190
 DDMACC (cerere DDM acces) 190

atribut stare
 obiect 13

atribut stare, program
 afișare 13

atribute de securitate
 autorizație obiect cerută pentru
 comenzi 423

atribute jurnal
 lucru cu 267

atribute rețea
 modificare
 comanda 189
 tipărire comunicații de securitate 278
 tipărire important pentru securitate 278

auditare
Vedeți și auditare obiect
Vedeți și jurnal auditare (QAUDJRN)
Vedeți și variabilă de sistem nivel auditare
 (QAUDLVL)
 acces neautorizat 233
 activare 256
 acțiuni 234
 atribute de rețea 233
 autorizare 232
 profiluri de utilizator 232
 autorizare adoptată 232
 autorizare obiect 268
 autorizare specială *ALLOBJ (toate
 obiectele) 231
 autorizare specială *AUDIT (auditare) 71
 autorizări programator 231
 capabilități limită 231
 comunicații 233
 condiții de eroare 50
 controale parolă 231
 controlare 50
 criptare a datelor sensibile 233
 date sensibile
 autorizare 232
 criptare 233
 descrieri de joburi 232
 Directory Server 461
 eșuare de program 268
 fișiere spool 496
 gestionare utilizator 106
 integritate obiect 269
 interfețe nesuportate 233
 listă de verificare 229
 liste de bibliotecă 232
 logare de la distanță 233
 logare fără ID-ul și parola utilizator 232
 lucru în numele 479
 metode 265
 modificare
 descriere comandă 272, 275

obiect
 implicită 254
 planificare 252
 obiecte QTEMP 255
 oprire 50, 260
 pași pentru pornire 256
 planificare
 privire generală 234
 variabile de sistem 254

pornire 256
 privire generală 229

profil de grup
 apartenență 231
 autorizare specială *ALLOBJ (toate
 obiectele) 231
 parolă 231

profil utilizator
 administrare 231

- auditare (*continuare*)
 - profil utilizator (*continuare*)
 - autorizare specială *ALLOBJ (toate obiectele) 231
 - profiluri de utilizator furnizate de IBM 230
 - programe neautorizate 233
 - recuperare cale de acces 450
 - responsabil cu securitatea 270
 - salvare operații 228
 - securitate fizică 230
 - servicii mail 479
 - servicii office 479
 - setare 256
 - terminare 50
 - terminare anormală 50
 - utilizare
 - coadă de mesaje QSYSMSG 233
 - istoric QHST (history-istoric sistem) 265
 - jurnale 265
 - utilizatori inactivi 232
 - valori de sistem 49, 230
 - variabile de sistem 254
- auditare *NODGRP (grup de noduri) 483
- auditare acțiune
 - definiție 234
 - Directory Server 461
 - fișiere spool 496
 - lista de răspuns 492
 - planificare 234
 - recuperare cale de acces 450
 - servicii mail 479
 - servicii office 479
- auditare bibliotecă (*LIB) 477
- auditare cerere query manager (*QMQRV) 490
- auditare clasă (*CLS) 454
- auditare coada de mesaje (*MSGQ) 482
- auditare coadă de ieșire (*OUTQ) 485
- auditare coadă joburi (*JOBQ) 474
- auditare coadă utilizator (*USRQ) 504
- auditare comandă (*CMD) 454
- auditare de securitate
 - afișare 277
 - instalare 277
- auditare definiție cerere (*QRYDFN) 490
- auditare definiție de pagină (*PAGDFN) 486
- auditare definiție produs (*PRDDFN) 489
- auditare descriere C locale (*CLD) 453
- auditare descriere clasă de serviciu (*COSD) 455
- auditare descriere controler (*CTLD) 457
- auditare descriere de linie (*LIND) 478
- auditare descriere dispozitiv (*DEVD) 457
- auditare descriere mașină S/36 (*S36) 502
- auditare descriere mod (*MODD) 480
- auditare descriere NetBIOS (*NTBD) 483
- auditare descriere server de rețea (*NWS) 484
- auditare descriere sesiune (*SSND) 498
- auditare descriere subsistem (*SBSD) 492
- auditare director (*DIR) 458
- auditare disponibilitate produs (*PRDAVL) 489
- auditare fișier de mesaje (*MSGF) 481
- auditare fișier flux (*STMF) 498
- auditare fișiere speciale (*CHRSF) 452
- auditare format diagramă (*CHTFMT) 452
- auditare formular query manager (*QMFORM) 489
- auditare grup de descriptori tipărire (*PDG) 487
- auditare grup de noduri (*NODGRP) 483
- auditare grup panouri (*PNLGRP) 488
- auditare hartă de produse sistem încrucișate (*CSPMAP) 456
- auditare index de căutare (*SCHIDX) 493
- auditare indexul utilizator (*USRIDX) 503
- auditare informații parte comunicații (*CSI) 456
- auditare interfață de rețea (*NWID) 484
- auditare încărcare de produse (*PRDLOD) 489
- auditare jurnal (*JRN) 476
- auditare legătură simbolică (*SYMLNK) 501
- auditare listă de conexiuni (*CNL) 455
- auditare listă de noduri (*NODL) 483
- auditare listă de validare (*VLDL) 504
- auditare meniu (*MENU) 480
- auditare modul (*MODULE) 480
- auditare obiect
 - afișare 254
 - definiție 252
 - lista de răspuns 492
 - modificare
 - descriere comandă 272, 275
 - obiect *ALRTBL (tabelă alertă) 450
 - obiect *CHTFMT (format diagramă) 452
 - obiect *CMD (Comandă) 454
 - obiect *CRQD (modificare descriere cerere) 453
 - obiect *CSPMAP (hartă de produse sistem încrucișate) 456
 - obiect *CSPTBL (tabelă de produse sistem încrucișate) 456
 - obiect *CTLD (descriere controler) 457
 - obiect *DEVD (descriere dispozitiv) 457
 - obiect *DIR (director) 458
 - obiect *DOC (document) 462
 - obiect *DTAARA (zona de date) 466
 - obiect *DTAQ (coadă de date) 466
 - obiect *EDTD (descriere editare) 467
 - obiect *EXITRG (înregistrare ieșire) 467
 - obiect *FCT (tabelă de control formulare) 468
 - obiect *FILE (fișier) 468
 - obiect *FLR (folder) 462
 - obiect *FNTRSC (resursă font) 471
 - obiect *FORMDF (definiție de formular) 472
 - obiect *FTR (filtru) 472
 - obiect *GSS (set simboluri grafice) 473
 - obiect *IGCDCT (dicționar set de caractere pe doi octeți) 473
 - obiect *IGCSRT (sortare set de caractere pe doi octeți) 473
 - obiect *IGCTBL (tabelă set de caractere pe doi octeți) 474
 - obiect *JOBQ (descriere job) 474
 - obiect *JOBQ (coadă joburi) 474
 - obiect *JOBSCD (planificator job) 475
 - obiect *JRN (jurnal) 476
 - obiect *MENU (meniu) 480
- auditare obiect (*continuare*)
 - obiect *NTBD (descriere NetBIOS) 483
 - obiect *NWS (descriere server de rețea) 484
 - obiect *OVL (suprapunere) 486
 - obiect *PGM (program) 487
 - obiect *QMQRV (cerere query manager) 490
 - obiect *QRYDFN (definiție cerere) 490
 - obiect *S36 (descriere mașină S/36) 502
 - obiect *SPADCT (scriere dicționar ajutor) 496
 - obiect *SQLPKG (pachet SQL) 497
 - obiect *SSND (descriere sesiune) 498
 - obiect *STMF (fișier flux) 498
 - obiect *SVRSTG (spațiu de stocare server) 498
 - obiect *SYMLNK (legătură simbolică) 501
 - obiect *TBL (tabelă) 502
 - obiect *USRPRF (profil utilizator) 503
 - obiect *USRQ (coada utilizator) 504
 - obiect *USRSPC (spațiu utilizator) 504
 - obiect cerere query manager (*QMQRV) 490
 - obiect coadă de date (*DTAQ) 466
 - obiect coadă joburi (*JOBQ) 474
 - obiect definiție cerere (*QRYDFN) 490
 - obiect definiție de formular (*FORMDF) 472
 - obiect descriere clasă de serviciu (*COSD) 455
 - obiect descriere controler (*CTLD) 457
 - obiect descriere dispozitiv (*DEVD) 457
 - obiect descriere editare (*EDTD) 467
 - obiect descriere job (*JOBQ) 474
 - obiect descriere mașină S/36 (*S36) 502
 - obiect descriere NetBIOS (*NTBD) 483
 - obiect descriere server de rețea (*NWS) 484
 - obiect descriere sesiune (*SSND) 498
 - obiect dicționar de date (*DTADCT) 466
 - obiect dicționar set de caractere pe doi octeți (*IGCDCT) 473
 - obiect director (*DIR) 458
 - obiect document (*DOC) 462
 - obiect filtru (*FTR) 472
 - obiect fișier (*FILE) 468
 - obiect flux (*STMF) 498
 - obiect folder (*FLR) 462
 - obiect format diagramă (*CHTFMT) 452
 - obiect formular query manager (*QMFORM) 489
 - obiect interfață de rețea (*NWID) 484
 - obiect înregistrare ieșire (*EXITRG) 467
 - obiect jurnal (*JRN) 476
 - obiect legătură simbolică (*SYMLNK) 501
 - obiect meniu (*MENU) 480
 - obiect modificare descriere cerere (*CRQD) 453
 - obiect pachet SQL (*SQLPCK) 497
 - obiect planificator job (*JOBSCD) 475
 - obiect profil utilizator (*USRPRF) 503
 - obiect program service (*SRVPGM) 498
 - obiect resursă font (*FNTRSC) 471
 - obiect set simboluri grafice (*GSS) 473

auditare obiect (*continuare*)

- obiect sortare set de caractere pe doi octeți (*IGCSRT) 473
- obiect spațiu de stocare server (*SVRSTG) 498
- obiect spațiu utilizator (*USRSPC) 504
- obiect suprapunere (*OVL) 486
- obiect tabela set de caractere pe doi octeți (*IGCTBL) 474
- obiect tabelă (*TBL) 502
- obiect tabelă alertă (*ALRTBL) 450
- obiect tabelă de control formulare (*FCT) 468
- obiect tabelă de produse sistem încrucișate (*CSPTBL) 456
- obiect zona de date (*DTAARA) 466
- obiectul *AUTHLR (deținător de autorizare) 451
- obiectul *AUTL (listă de autorizații) 451
- obiectul *BNDDIR (directorul de legături) 451
- obiectul *CFGL (listă de configurație) 452
- obiectul *CLD (descriere C locale) 453
- obiectul *CLS (Clasă) 454
- obiectul *CNL (lista de conexiuni) 455
- obiectul *COSD (descriere clasă de serviciu) 455
- obiectul *CSI (informații parte comunicații) 456
- obiectul *DTADCT (dicționar de date) 466
- obiectul *JRNRCV (receptor jurnal) 477
- obiectul *LIB (bibliotecă) 477
- obiectul *LIND (descriere de linie) 478
- obiectul *MODD (descriere mod) 480
- obiectul *MODULE (modul) 480
- obiectul *MSGF (fișier de mesaje) 481
- obiectul *MSGQ (coadă de mesaje) 482
- obiectul *NODGRP (grup de noduri) 483
- obiectul *NODL (listă de noduri) 483
- obiectul *NWID (interfață de rețea) 484
- obiectul *OUTQ (coadă de ieșire) 485
- obiectul *PAGDFN (definiție de pagină) 486
- obiectul *PAGSEG (segment de pagină) 486
- obiectul *PDG (grup de descriptori tipărire) 487
- obiectul *PRDAVL (disponibilitatea produsului) 489
- obiectul *PRDDFN (definiție produs) 489
- obiectul *PRDLOD (încărcarea de produse) 489
- obiectul *QMFORM (formular query manager) 489
- obiectul *RCT (tabelă cod referință) 491
- obiectul *SBSD (descriere subsistem) 492
- obiectul *SCHIDX (index de căutare) 493
- obiectul *SOCKET (socket-ul local) 494
- obiectul *SRVPGM (program service) 498
- obiectul *USRIDX (indexul utilizator) 503

auditare obiect (*continuare*)

- obiectul *VLDL (listă de valide) 504
- obiectul bibliotecă (*LIB) 477
- obiectul clasă (*CLS) 454
- obiectul coadă de mesaje (*MSGQ) 482
- obiectul coadă de ieșire (*OUTQ) 485
- obiectul coadă utilizator (*USRQ) 504
- obiectul comandă (*CMD) 454
- obiectul definiție de pagină (*PAGDFN) 486
- obiectul definiție produs (*PRDDFN) 489
- obiectul descriere C locale (*CLD) 453
- obiectul descriere de linie (*LIND) 478
- obiectul descriere mod (*MODD) 480
- obiectul descriere subsistem (*SBSD) 492
- obiectul deținător de autorizare (*AUTHLR) 451
- obiectul director de legături (*BNDDIR) 451
- obiectul disponibilitatea produsului (*PRDAVL) 489
- obiectul fișier de mesaje (*MSGF) 481
- obiectul grup de descriptori tipărire (*PDG) 487
- obiectul grup de noduri (*NODGRP) 483
- obiectul hartă de produse sistem încrucișate (*CSPMAP) 456
- obiectul index de căutare (*SCHIDX) 493
- obiectul indexul utilizator (*USRIDX) 503
- obiectul informații parte comunicații (*CSI) 456
- obiectul încărcare de produse (*PRDLOD) 489
- obiectul lista de conexiuni (*CNL) 455
- obiectul listă de autorizații (*AUTL) 451
- obiectul listă de configurație (*CFGL) 452
- obiectul listă de noduri (*NODL) 483
- obiectul listă de validare (*VLDL) 504
- obiectul modul (*MODULE) 480
- obiectul receptor jurnal (*JRNRCV) 477
- obiectul scriere dicționar ajutor (*SPADCT) 496
- obiectul segment de pagină (*PAGSEG) 486
- obiectul socket local (*SOCKET) 494
- obiectul tabelă cod referință (*RCT) 491
- obiectul program (*PGM) 487
- operații comune 447
- planificare 252
- auditare obiect *ALRTBL (tabelă alertă) 450
- auditare obiect *AUTHLR (deținător de autorizare) 451
- auditare obiect *BNDDIR (director de legături) 451
- auditare obiect *CFGL (listă de configurație) 452
- auditare obiect *CHRSF (Fișiere speciale) 452
- auditare obiect *CHTFMT (format diagramă) 452
- auditare obiect *CLD (descriere C locale) 453

auditare obiect *CLS (Clasă) 454

auditare obiect *CMD (Comandă) 454

auditare obiect *COSD (descriere clasă de serviciu) 455

auditare obiect *CRQD (modificare descriere cerere) 453

auditare obiect *CSI (informații parte comunicații) 456

auditare obiect *CSPMAP (hartă de produse sistem încrucișate) 456

auditare obiect *CSPTBL (tabelă de produse sistem încrucișate) 456

auditare obiect *CTLD (descriere controler) 457

auditare obiect *DEVD (descriere dispozitiv) 457

auditare obiect *DIR (director) 458

auditare obiect *DOC (document) 462

auditare obiect *DTAARA (zona de date) 466

auditare obiect *DTADCT (dicționar de date) 466

auditare obiect *DTAQ (coadă de date) 466

auditare obiect *EDTD (descriere editare) 467

auditare obiect *EXITRG (înregistrare ieșire) 467

auditare obiect *FCT (tabelă de control formulare) 468

auditare obiect *FNTRSC (resursă font) 471

auditare obiect *FORMDF (definiție de formular) 472

auditare obiect *FTR (filtru) 472

auditare obiect *GSS (set simboluri grafice) 473

auditare obiect *IGCSRT (sortare set de caractere pe doi octeți) 473

auditare obiect *IGCTBL (tabela set de caractere pe doi octeți) 474

auditare obiect *JOB (descriere job) 474

auditare obiect *JOBSCD (planificator job) 475

auditare obiect *JRN (jurnal) 476

auditare obiect *JRNRCV (receptor jurnal) 477

auditare obiect *LIB (bibliotecă) 477

auditare obiect *LIND (descriere de linie) 478

auditare obiect *MENU (meniu) 480

auditare obiect *MODD (descriere mod) 480

auditare obiect *MODULE (modul) 480

auditare obiect *MSGF (fișier de mesaje) 481

auditare obiect *MSGQ (coadă de mesaje) 482

auditare obiect *NODL (listă de noduri) 483

auditare obiect *NTBD (descriere NetBIOS) 483

auditare obiect *NWID (interfață de rețea) 484

auditare obiect *NWS (descriere server de rețea) 484

auditare obiect *OUTQ (coadă de ieșire) 485

auditare obiect *OVL (suprapunere) 486

auditare obiect *PAGDFN (definiție de pagină) 486

auditare obiect *PAGSEG (segment de pagină) 486

auditare obiect *PDG (grup de descriptori tipărire) 487

auditare obiect *PNLGRP (grup panouri) 488

auditare obiect *PRDAVL (disponibilitate produs) 489

auditare obiect *PRDDFN (definiție produs) 489

auditare obiect *PRDLOD (încărcarea de produse) 489

auditare obiect *QMFORM (formular query manager) 489

auditare obiect *QMQRV (cerere query manager) 490

auditare obiect *QRYDFN (definiție cerere) 490

auditare obiect *S36 (descriere mașină S/36) 502

auditare obiect *SBSD (descriere subsistem) 492

auditare obiect *SCHIDX (index de căutare) 493

auditare obiect *SOCKET (socket local) 494

auditare obiect *SPADCT (scriere dicționar ajutor) 496

auditare obiect *SQLPKG (pachet SQL) 497

auditare obiect *SRVPGM (program service) 498

auditare obiect *SSND (descriere sesiune) 498

auditare obiect *STMF (fișier flux) 498

auditare obiect *SYNLNK (legătură simbolică) 501

auditare obiect *TBL (tabelă) 502

auditare obiect *USRIDX (indexul utilizator) 503

auditare obiect *USRPRF (profil utilizator) 503

auditare obiect *USRQ (coadă utilizator) 504

auditare obiect *USRSPC (spațiu utilizator) 504

auditare obiect *VLDL (listă de validare) 504

auditare obiect cu modificare descriere cerere (*CRQD) 453

auditare obiect de bibliotecă de documente modificare descriere comandă 275

auditare obiect definiție de formular (*FORMDF) 472

auditare obiect descriere job (*JOB) 474

auditare obiect dicționar set de caractere pe doi octeți (*IGCDCT) 473

auditare obiect director de legături 451

auditare obiect fișier (*FILE) 468

auditare obiect listă de configurație 452

auditare obiect resursă font (*FNTRSC) 471

auditare obiect set simboluri grafice (*GSS) 473

auditare obiect sortare set de caractere pe doi octeți (*IGCSRT) 473

auditare obiect tabelă alertă (*ALRTBL) 450

auditare obiect tabelă set de caractere pe doi octeți (*IGCTBL) 474

auditare obiect utilitar interactive data definiție (IDDU) 466

auditare obiect obiect *PNLGRP (grup panouri) 488

auditare obiect grup panouri (*PNLGRP) 488

auditare pachet SQL (*SQLPKG) 497

auditare planificator job (*JOBSCD) 475

auditare profil utilizator (*USRPRF) 503

auditare program (*PGM) 487

auditare program service (*SRVPGM) 498

auditare receptor jurnal creare 256

auditare receptor jurnal numire 257

auditare receptor jurnal salvare 260

auditare receptor jurnal ștergere 260

auditare receptor jurnal (*JRNRCV) 477

auditare scriere dicționar ajutor (*SPADCT) 496

auditare securitate afișare 619

auditare securitate autorizație obiect cerută pentru comenzi 423

auditare securitate configurare 619

auditare segment de pagină (*PAGSEG) 486

auditare socket local (*SOCKET) 494

auditare spațiu utilizator (*USRSPC) 504

auditare suprapunere (*OVL) 486

auditare tabelă (*TBL) 502

auditare tabelă cod referință (*RCT) 491

auditare tabelă de produse sistem încrucișate (*CSPTBL) 456

auditare utilizator modificare descriere comandă 275

auditare utilizator descrieri comenzi 274

auditarea de obiect *CNL (lista de conexiuni) 455

auditarea obiect *AUTL (listă de autorizații) 451

audob *JOBQ (coadă joburi) 474

audop *IGCDCT (dicționar set de caractere pe doi octeți) 473

audpb *FILE (fișier) 468

audpb filtru (*FTR) 472

autentificare ID digital 96

autentificare server autorizație obiect cerută pentru comenzi 424

authority cache autorizări private 173

authorization list - listă de autorizare asigurarea obiectelor furnizate de IBM 118

autorizare management (*AUTLMGT) 112, 118

descriere 117

autorizare *Vedeți și verificare autorizare*

*ADD (add - adăugare) 112, 300

*ALL (all - toate) 113, 300

*AUTLMGT (authorization list management - management listă de autorizare) 112, 118

*AUTLMGT (gestionare listă autorizare) 300

autorizare (continuare)

*CHANGE (change - modificare) 113, 300

*DLT (delete - ștergere) 300

*DLT (delete) 112

*EXCLUDE (exclude - excludere) 113

*EXECUTE (executare) 300

*EXECUTE (execute) 112

*Mgt 112

*OBJALTER (object alter) 112

*OBJALTER (transformare obiect) 299

*OBJEXIST (existență obiect) 112, 299

*OBJMGT (gestionare obiect) 299

*OBJMGT (gestiune obiect) 112

*OBJOPR (operațional obiect) 112, 299

*OBJREF (object reference - referință obiect) 112

*OBJREF (obiect referință) 300

*R (read - citire) 301

*R (read) 113

*READ (read - citire) 112, 300

*Ref (Reference) 112

*RW (read, write) 113, 301

*RWX (read - citire, write - scriere, execute - execuție) 301

*RWX (read, write, execute) 113

*RX (read - citire, execute - execuție) 301

*RX (read, execute) 113

*UPD (update - actualizare) 300

*UPD (update) 112

*USE (use - utilizare) 300

*USE (use) 113

*W (write - scriere) 301

*W (write) 113

*WX (write - scriere, execute - execuție) 301

*WX (write, execute) 113

*X (execute - execuție) 301

*X (execute) 113

adăugarea de utilizatori 140

adoptată afișare 134, 209

auditare 268

exemplu verificare autorizare 166, 168

ignorare 205

intrare jurnal auditare (QAUDJRN) 244

proiectare aplicație 203, 205, 206

scop 128

adopted 519

afișare descriere comandă 272

afișare în detaliu (*EXPERT opțiune utilizator) 88, 89, 90

asignarea noilor obiecte 124

auditare 232

authorization list - listă de autorizare management (*AUTLMGT) 112

autorizare specială *ALLOBJ (toate obiectele) 68

autorizare specială *AUDIT (auditare) 71

autorizare specială *IOSYSCFG (configurare sistem) 71

autorizare specială *JOBCTL (control de job) 69

- autorizare (*continuare*)
 - autorizare specială *SAVSYS (salvare sistem) 70
 - autorizare specială *SECADM (administrator de securitate) 69
 - autorizare specială *SERVICE (service) 70
 - autorizare specială *SPLCTL (control de spool) 69
 - autorizarea pentru schimbarea bibliotecă 138
 - bibliotecă 5
 - câmp
 - definiție 112
 - copiere
 - descriere comandă 274
 - exemplu 101
 - recomandări 144
 - redenumire profil 106
 - date
 - definiție 112
 - definiță de utilizator 139
 - definiție 112
 - detaliu, afișare (*EXPERT opțiune utilizator) 88, 89, 90
 - deținere la ștergerea unui fișier 131
 - director 5
 - ecrane 133
 - eliminarea utilizator 140
 - folosirea generic pentru grup 141
 - grup
 - afișare 134
 - exemplu 163, 167
 - grup primar 111, 123
 - exemplu 164
 - gestionare 103
 - ignorare adoptată 131
 - introducere 4
 - listă de autorizare
 - format pe mediu de stocare 221
 - management (*AUTLMGT) 300
 - stocare 220
 - stocate pe mediu de stocare 221
 - lucru cu
 - descriere comandă 272
 - Management authority
 - *Mgt(*) 112
 - modificare 520
 - descriere comandă 272
 - intrare jurnal auditare (QAUDJRN) 247
 - obiect
 - *ADD (add - adăugare) 112, 300
 - *DLT (delete - ștergere) 300
 - *DLT (delete) 112
 - *EXECUTE (executare) 300
 - *EXECUTE (execute) 112
 - *OBJEXIST (existență obiect) 112, 299
 - *OBJMGT (gestionare obiect) 299
 - *OBJMGT (gestiune obiect) 112
 - *OBJOPR (operațional obiect) 112, 299
 - *READ (read - citire) 112, 300
 - *Ref (Reference) 112
 - *UPD (update - actualizare) 300
 - *UPD (update) 112
 - definiție 112
- autorizare (*continuare*)
 - obiect (*continuare*)
 - exclude (*EXCLUDE) 113
 - format pe mediu de stocare 220
 - stocare 220
 - stocate pe mediu de stocare 220
 - obiect nou
 - exemplu 124
 - parametru CRTAUT (create authority - creare autorizare) 118, 136
 - parametru GRPAUT (autorizare de grup) 80
 - parametru GRPAUT (autorizare grup) 122
 - parametru GRPAUTTYP (tip autorizare de grup) 81
 - valoare de sistem QUSEADPAUT (utilizare autorizare adoptată) 30
 - Valoarea de sistem QCRTAUT (create authority - creare autorizare) 22
 - obiect referit
 - folosire 144
 - obiecte multiple 141
 - object alter - alterare obiect (*OBJALTER) 112
 - object reference - referință obiect (*OBJREF) 112
 - parametru autorizare specială (SPCAUT) 68
 - privat
 - definiție 111
 - privată
 - restaurarea 219, 223
 - salvarea 219
 - profilului utilizator
 - format pe mediu de stocare 221
 - stocare 220
 - stocate pe mediu de stocare 221
 - public
 - definiție 111
 - exemplu 165, 167
 - restaurarea 219
 - salvarea 219
 - publică
 - restaurarea 223
 - referință obiect (*OBJREF) 300
 - restaurare
 - descriere comandă 275
 - intrare jurnal auditare (QAUDJRN) 245
 - restaurarea
 - descrierea procesului 224
 - privire generală asupra 219
 - procedură 223
 - schimbare
 - proceduri 138
 - stocare
 - cu obiect 220
 - cu profilul utilizatorului 220
 - listă de autorizare 220
 - subseturi definite de sistem 113
 - subseturi folosite în mod obișnuit 113
 - ștergere utilizator 140
 - transformare obiect (*OBJALTER) 299
 - verificare 147
 - inițiere job batch 176
 - inițiere job interactiv 175
- autorizare (*continuare*)
 - verificare (*continuare*)
 - proces de semnare 175
 - autorizare *ADD (add - adăugare) 300
 - autorizare *ALL (tot) 300
 - autorizare *AUTLMGT (authorization list management - management listă de autorizare) 112
 - autorizare *AUTLMGT (gestionare listă autorizare) 300
 - autorizare *CHANGE (modificare) 300
 - autorizare *DLT (delete - ștergere) 300
 - autorizare *EXCLUDE (exclude) 113
 - autorizare *EXECUTE (executare) 300
 - autorizare *OBJALTER (transformare obiect) 299
 - autorizare *OBJEXIST (existență obiect) 112, 299
 - autorizare *OBJMGT (gestionare obiect) 299
 - autorizare *OBJMGT (gestiune obiect) 112
 - autorizare *OBJOPR (operațional obiect) 112, 299
 - autorizare *OBJREF (obiect referință) 300
 - autorizare *READ (read - citire) 300
 - autorizare *READ (read) 112
 - autorizare *UPD (update - actualizare) 300
 - autorizare *USE (utilizare) 300
 - autorizare actualizare (*UPD) 300
 - autorizare adoptata
 - dispunere fișier AP (autorizare adoptată) 519
 - intrare jurnal auditare (QAUDJRN) 519
 - autorizare adoptată
 - afișare
 - descriere comandă 275
 - fișiere critice 209
 - parametrul USRPRF 130
 - programe care adoptă un profil 130
 - auditare 232
 - autorizare de grup 128
 - creare program 130
 - definiție 128
 - diagramă de flux (flowchart) 159
 - drept de proprietate obiect 130
 - exemplu 203, 205, 206
 - exemplu verificare autorizare 166, 168
 - funcție cerere sistem 129
 - funcții de depanare 129
 - ignorare 131, 205
 - inițiere job 176
 - intrare jurnal auditare (QAUDJRN) 244
 - modificare
 - intrare jurnal auditare (QAUDJRN) 248
 - nivel de auditare *PGMADP (adoptare program) 244
 - program de tratare a mesajului de întrerupere 129
 - programe legate 130
 - programe service 130
 - proiectare aplicație 203, 205, 206
 - recomandări 131
 - restaurare de programe
 - modificări ale dreptului de proprietate și ale autorizării 225
 - riscuri 131

- autorizare adoptată (*continuare*)
 schimbare
 autorizare cerută 130
 job 130
 scop 128
 securitate bibliotecă 115
 special authority 128
 tasta Atenție (ATTN) 129
 tip de intrare jurnal AP (autorizare adoptată) 244
 transferare la job grup 129
- autorizare câmp
 definiție 112
- autorizare citire (*READ) 300
- autorizare de grup
 autorizare adoptată 128
 descriere 111
 exemplu verificare autorizare 163, 167
 parametru profil utilizator GRPAUT 80, 122, 124
 parametru profil utilizator GRPAUTTYPE 81
 parametrul profil utilizator GRPAUTTYPE 124
- autorizare de utilizator
 copiere
 exemplu 101
 redenumire profil 106
- autorizare definită de sistem 113
- autorizare definită de utilizator (USER DEF - user-defined) 139
- autorizare exclude (*EXCLUDE) 113
- autorizare executare (*EXECUTE) 300
- autorizare existență (*OBJEXIST) 112, 299
- autorizare gestionare (*OBJMGT)
 obiect 299
- autorizare gestiune (*OBJMGT)
 obiect 112
- autorizare grup primar
 exemplu verificare autorizare 164
- autorizare modificare (*CHANGE) 300
- autorizare obiect
 acordare 272
 efectul asupra autorizării anterioare 141
 obiecte multiple 141
 afișare 268, 272
 afișare în detaliu (*EXPERT opțiune utilizator) 88, 89, 90
 analizare 268
 autentificare server 424
 autorizare specială *ALLOBJ (toate obiectele) 68
 autorizare specială *SAVSYS (salvare sistem) 70
 comenzi 272
 comenzi alertă 312
 Comenzi asistent operațional 400
 comenzi atribut rețea 395
 comenzi atribute de securitate 423
 comenzi auditare securitate 423
 comenzi bibliotecă 382
 comenzi cadru de lucru server de poștă 389
 comenzi cititor 418
 comenzi clasă 316
 Comenzi coadă de date 326
- autorizare obiect (*continuare*)
 comenzi coadă de ieșire 404
 comenzi coadă de joburi 371
 comenzi coadă de mesaje 393
 comenzi cod acces 400
 comenzi configurație LAN extinsă cu comunicație fără fir 336
 comenzi configurație server de rețea 399
 comenzi control comitere 320
 Comenzi corecție temporară program (PTF) 424
 comenzi criptografie 324
 comenzi CSI 320
 comenzi curățare 400
 comenzi de configurare 321
 comenzi de descriere alertă 312
 comenzi descriere cerere de modificare 315
 comenzi descriere clasă-de-serviciu 316
 comenzi descriere controler 323
 comenzi descriere de editare 336
 comenzi descriere de linie 387
 comenzi descriere dispozitiv 326
 comenzi descriere interfață de rețea 397
 comenzi descriere job 370
 comenzi descriere mesaj 392
 comenzi descriere mod 394
 comenzi descriere NetBIOS 395
 comenzi descriere server de rețea 399
 comenzi deținător de autorizare 314
 comenzi dicționar ajutător pentru corectare ortografică 428
 comenzi director 329
 comenzi director baze de date relaționale 419
 comenzi distribuție 330
 comenzi document 331
 comenzi educație online 400
 comenzi emulare 328
 comenzi filtrare 344
 comenzi financiare 344
 comenzi fișier 337
 comenzi fișier mesaj 392
 comenzi fișier spool 429
 comenzi format diagramă 315
 comenzi grup de panouri 390
 comenzi hardware 419
 comenzi ieșire imprimantă 429
 comenzi imprimantă 443
 comenzi index căutare 366
 comenzi index căutare informații 366
 comenzi index text 400
 comenzi index, coadă și spațiu utilizator 439
 comenzi întrebări și răspunsuri 417
 comenzi job 367
 comenzi jurnal 372
 comenzi limbaj 376
 comenzi limbaj de programare 376
 comenzi listă autorizare 314
 comenzi listă de conexiuni 322
 comenzi listă de configurare 322
 comenzi listă de distribuție 331
 comenzi listă de noduri 399
 comenzi listă replici 433
 comenzi listă replici sistem 433
 comenzi locale 389
- autorizare obiect (*continuare*)
 Comenzi Management/400 416
 comenzi mediu de stocare 389
 Comenzi mediu System/36 434
 comenzi meniu 390
 comenzi mesaj 391
 comenzi migrare 393
 comenzi modernizare informații ordine 438
 comenzi obiect bibliotecă document (DLO) 331
 comenzi obiect de personalizare stație de lucru 443
 comenzi obișnuite pentru obiect 303
 comenzi optice 401
 comenzi pachet 405
 comenzi passthrough stație de afișare 330
 Comenzi pentru funcția avansată de tipărire 311
 comenzi performanță 406
 comenzi permisiune utilizator 400
 comenzi planificare job 372
 comenzi problemă 411
 comenzi profil utilizator 439, 440
 comenzi program cu licență 387
 Comenzi PTF (corecție temporară program) 424
 comenzi receptor jurnal 376
 comenzi salvare de rezervă 400
 comenzi scriitor imprimantă 443
 Comenzi server de rețea 397
 comenzi service 424
 comenzi sesiune 419
 comenzi set de caractere pe doi octeți 335
 comenzi set de simboluri grafice 345
 comenzi sistem 433
 comenzi subsistem 431
 comenzi tabel de control formulare 419
 comenzi tabelă 436
 comenzi tabelă alertă 312
 Comenzi TCP/IP (Transmission Control Protocol/Internet Protocol) 436
 comenzi token-ring 389
 comenzi valori sistem 433
 comenzi zonă de date 325
 comenzilor programului 412
 definiție 112
 definiție interactivă de date 366
 detaliu, afișare (*EXPERT opțiune utilizator) 88, 89, 90
 director de legare 314
 editare 138, 272
 format pe mediu de stocare 220
 listă de validare 443
 modificare
 intrare jurnal auditare (QAUDJRN) 247
 necesar pentru comenzi *CMD 319
 operații grafice 345
 recuperare cale de acces 310
 resurse comenzi 419
 revocare 272
 RJE (intrare job la distanță) 419
 schimbare
 proceduri 138
 server gazdă 346
 sferă de comenzi control 429

- autorizare obiect (*continuare*)
 - Socket-uri AF_INET peste SNA 312
 - stocare 220
 - autorizare operațional (*OBJOPR) 112, 299
 - autorizare pentru date
 - definiție 112
 - autorizare privată
 - definiție 111
 - diagramă de flux (flowchart) 151
 - drept de proprietate obiect 111
 - planificare aplicații 200
 - restaurarea 219, 223
 - salvarea 219
 - autorizare proprietar
 - diagramă de flux (flowchart) 152
 - autorizare publică
 - biblioteca 136
 - definiție 111
 - diagramă de flux (flowchart) 158
 - exemplu verificare autorizare 165, 167
 - obiecte noi
 - descriere 118
 - specificare 136
 - profil utilizator
 - recomandare 93
 - restaurarea 219, 223
 - revocare 278
 - salvarea 219
 - autorizare read (*READ) 112
 - autorizare referință obiect (*OBJREF) 300
 - autorizare specială
 - *ALLOBJ (toate obiectele)
 - adăugat automat 11
 - auditare 231
 - funcții permise 68
 - înlăturat automat 10
 - riscuri 68
 - *ALLOBJt (toate obiectele)
 - eșuare semnare 177
 - *AUDIT (auditare)
 - funcții permise 71
 - riscuri 71
 - *IOSYSCFG (configurare sistem)
 - funcții permise 71
 - riscuri 71
 - *JOBCTL (control de job)
 - funcții permise 69
 - parametru limită de prioritate (PTYLMT) 77
 - riscuri 69
 - *JOBCTL (control job)
 - parametrii cozii de ieșire 187
 - *SAVSYS (salvare sistem)
 - autorizare *OBJEXIST 300
 - descriere 227
 - funcții permise 70
 - înlăturat automat 10
 - riscuri 70
 - *SECADM (administrator de securitate)
 - funcții permise 69
 - *SERVICE (service)
 - eșuare semnare 177
 - funcții permise 70
 - riscuri 70
 - *SPLCTL (control de spool)
 - funcții permise 69
 - riscuri 69
 - autorizare specială (*continuare*)
 - *SPLCTL (control spool)
 - parametrii cozii de ieșire 187
 - adăugat de sistem
 - modificare nivel de securitate 10
 - definiție 68
 - înlăturat de sistem
 - modificare nivel de securitate 10
 - înlăturată de sistem
 - înlăturată automat 222
 - listare utilizatori 267
 - modificare nivel de securitate 10
 - profil utilizator 68
 - recomandări 71
 - autorizare specială (*ALLOBJ) toate obiectele
 - auditare 231
 - înlăturată de sistem
 - restaurare profil 222
 - autorizare specială *ALLOBJ (toate obiectele)
 - auditare 231
 - funcții permise 68
 - înlăturată de sistem
 - restaurare profil 222
 - riscuri 68
 - autorizare specială *AUDIT (auditare)
 - funcții permise 71
 - riscuri 71
 - autorizare specială *IOSYSCFG (configurare sistem)
 - funcții permise 71
 - riscuri 71
 - autorizare specială *JOBCTL (control de job)
 - funcții permise 69
 - limită de prioritate (PTYLMT) 77
 - riscuri 69
 - autorizare specială *SAVSYS (salvare sistem)
 - autorizare *OBJEXIST 300
 - descriere 227
 - funcții permise 70
 - riscuri 70
 - autorizare specială *SECADM (administrator de securitate)
 - funcții permise 69
 - autorizare specială *SERVICE (service)
 - funcții permise 70
 - riscuri 70
 - autorizare specială *SPLCTL (control de spool)
 - funcții permise 69
 - riscuri 69
 - autorizare specială administrator de securitate (*SECADM)
 - funcții permise 69
 - autorizare specială configurare sistem (*IOSYSCFG)
 - funcții permise 71
 - riscuri 71
 - autorizare specială control de job (*JOBCTL)
 - funcții permise 69
 - limită de prioritate (PTYLMT) 77
 - riscuri 69
 - autorizare specială control de spool (*SPLCTL)
 - funcții permise 69
 - riscuri 69
 - autorizare specială de auditare (*AUDIT)
 - funcții permise 71
- autorizare specială de auditare (*AUDIT) (*continuare*)
 - riscuri 71
- autorizare specială de service (*SERVICE) (*continuare*)
 - riscuri 70
- autorizare specială de salvare sistem (*SAVSYS)
 - autorizare *OBJEXIST 300
 - funcții permise 70
 - riscuri 70
- autorizare specială salvare sistem(*SAVSYS)
 - descriere 227
- autorizare specială toate obiectele (*ALLOBJ)
 - funcții permise 68
 - riscuri 68
- autorizare ștergere (*DLT) 300
- autorizare tot (*ALL) 300
- autorizare transformare obiect (*OBJALTER) 299
- autorizare utilizare (*USE) 300
- autorizare utilizator
 - adăugare 140
 - copiere
 - descriere comandă 274
 - recomandări 144
- autorizare, obiect
 - Vedeți* autorizare obiect
- Autorizarea *ADOPTED (adopted) 134
- autorizarea *ALL (all) 113
- autorizarea *CHANGE (change) 113
- Autorizarea *GROUP (group) 134
- autorizarea *OBJALTER (object alter) 112
- autorizarea *OBJREF (object reference) 112
- autorizarea *USE (use) 113
- Autorizarea adopted (*ADOPTED) 134
- autorizarea all (*ALL) 113
- autorizarea change (*CHANGE) 113
- Autorizarea group (*GROUP) 134
- autorizarea object alter (*OBJALTER) 112
- autorizarea object reference (*OBJREF) 112
- autorizarea specială
 - asignarea analizării 621
- autorizarea specială *ALLOBJ (toate obiectele)
 - adăugat de sistem
 - modificare niveluri de securitate 11
 - eșuare semnare 177
 - înlăturat de sistem
 - modificare niveluri de securitate 10
- autorizarea specială *JOBCTL (control job)
 - parametrii cozii de ieșire 187
- autorizarea specială *SAVSYS (salvare sistem)
 - înlăturat de sistem
 - modificare niveluri de securitate 10
- autorizarea specială *SERVICE (service)
 - eșuare semnare 177
- autorizarea specială *SPLCTL (control spool)
 - parametrii cozii de ieșire 187
- autorizarea specială control job (*JOBCTL)
 - parametrii cozii de ieșire 187
- autorizarea specială control spool (*SPLCTL)
 - parametrii cozii de ieșire 187
- autorizarea specială salvare sistem (*SAVSYS)
 - înlăturat de sistem
 - modificare niveluri de securitate 10
- autorizarea specială service (*SERVICE)
 - eșuare semnare 177

autorizarea specială toate obiectele
 (*ALLOBJ)
 adăugat de sistem
 modificare niveluri de securitate 11
 eșuare semnare 177
 înlăturat de sistem
 modificare niveluri de securitate 10
 autorizarea use (*USE) 113
 Autorizarea USER DEF (user-defined) 139
 autorizație adoptată
 tipărire listă de obiecte 621
 autorizație publică
 revocare 625
 Revocare folosind comanda
 RVKPUBAUT 627
 tipărire 623
 autorizări de câmp 115
 autorizări private
 authority cache 173
 Autorizări speciale
 autorizări, speciale 214
 Autorizări speciale, acumulare 214
 Autorizări, acumulare speciale 214
 autorizări, câmp 115
 avantaje
 listă de autorizații 212

B

bandă
 necesități ale autorizării obiect pentru
 comenzi 389
 protejare 230
 batch
 restricționare joburi 193
 biblioteca curentă
 lista de biblioteci 183, 185
 modificare
 metode 183
 recomandări 185
 recomandări 185
 biblioteca produs
 lista de biblioteci
 descriere 183
 biblioteca QSYS (sistem)
 liste de autorizare 118
 biblioteca sistem (QSYS)
 liste de autorizare 118
 bibliotecă
 autorizare
 definiție 5
 descriere 115
 obiecte noi 118
 autorizare publică
 specificare 136
 creare 136
 curentă 64
 drept de proprietate asupra obiectului 216
 listare
 conținut 268
 toate bibliotecile 268
 necesități ale autorizării obiect pentru
 comenzi 382
 parametru CRTAUT (create authority -
 creare autorizare)
 descriere 118
 exemplu 124

bibliotecă (*continuate*)
 parametru CRTAUT (create authority -
 creare autorizare) (*continuate*)
 riscuri 119
 specificare 136
 parametrul create authority (CRTAUT)
 descriere 118
 exemplu 124
 riscuri 119
 specificare 136
 planificare 199
 proiectare 199
 QTEMP (temporară)
 nivel de securitate 50 17
 restaurarea 219
 salvarea 219
 securitate
 autorizare adoptată 115
 descriere 115
 exemplu 200
 linii de ghidare 200
 proiectare 199
 riscuri 114
 tipărire listă de descrieri de
 subsistem 277
 valoare creare auditare obiect
 (CRTOBJAUD) 54
 valoare CRTOBJAUD (creare auditare
 obiect) 54
 valoarea AUTOCFG (configurare automată
 dispozitiv) 31
 valoarea configurare automată dispozitiv
 (AUTOCFG) 31
 valoarea QRETSVRSEC (retain server
 security - reținere securitate server) 27
 bibliotecă curentă
 definiție 64
 limitare capabilități 65
 modificare
 limitare capabilități 65
 profil utilizator 64
 bibliotecă pretindere spațiu de stocare (QRCL)
 setare valoare de sistem QALWUSRDMN
 (permitere obiecte utilizator) 22
 bibliotecă produs
 lista de biblioteci 185
 recomandări 185
 bibliotecă QRCL (pretindere spațiu de stocare)
 setare valoare de sistem QALWUSRDMN
 (permitere obiecte utilizator) 22
 bibliotecă QTEMP (temporară)
 nivel de securitate 50 17
 Bibliotecă QUSER38 117
 bibliotecă temporară (QTEMP)
 nivel de securitate 50 17
 bloc de control intern
 împiedicarea modificării 17

C

cadru de lucru server de poștă
 autorizație obiect cerută pentru
 comenzi 389
 caracter numeric necesar în parolă 44
 caractere
 parolă 40
 caractere parolă 40

cartuș
 autorizație obiect cerută pentru
 comenzi 389
 cartuș bandă
 autorizație obiect cerută pentru
 comenzi 389
 catalog SQL 212
 Cerere client atributul rețea acces
 (PCSACC) 189
 cerere DDM atribut rețea acces
 (DDMACC) 190
 CFGTCPSMTP Comanda (Configurare
 TCP/IP SMTP)
 autorizări obiect necesare 438
 CHGACTSCDE
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGASPA
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCDEFNT (Change Coded Font -
 Modificare font codificat)
 autorizație obiect cerută pentru
 comenzi 311
 CHGCLUCFG
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCLUNODE
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCLURCY
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCLUVER
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCRG
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCRGDEVE
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGCRGPRI
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGFCNARA
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGFNTTBLE (Change DBCS Font Table
 Entry - Modificare intrare tabelă fonturi
 DBCS)
 necesități ale autorizării obiect pentru
 comenzi 311
 CHGGPHFMT
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGIMGCLG
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGIMGCLGE
 profiluri utilizator livrat de IBM
 autorizate 288
 CHGJOBTRC
 profiluri utilizator livrat de IBM
 autorizate 289

CHGSECAUD (Change Security Auditing - Modificare auditare securitate) funcția de auditare a securității 256

CHKASPBAL
 profiluri utilizator livrat de IBM autorizate 289

cititor
 necesități ale autorizării obiect pentru comenzi 418

clasa
 relația cu securitatea 192

clasă
 necesități ale autorizării obiect pentru comenzi 316

clasă utilizatori
 asignare analizare 621

clasă, utilizator
Vedeți parametru clasă utilizator (USRCLS)

cluster
 necesități ale autorizării obiect pentru comenzi 316

coadă de ieșire
 creare 188
 parametru afișare date (DSPDTA) 186
 parametru AUTCHK (autorizare pentru verificare) 187
 parametru autorizare pentru verificare (AUTCHK) 187
 parametru control operator (OPRCTL) 187
 parametru DSPDTA (afișare date) 186
 parametru OPRCTL (control operator) 187
 securizare 188

coadă de mesaje
 restrângere 182

coadă de date
 autorizatie obiect cerută pentru comenzi 326

coadă de ieșire
 autorizare specială *JOBCTL (control de job) 69
 autorizare specială *SPLCTL (control de spool) 69
 creare 186
 gestiune descriere 186
 modificare 186
 parametru *OPRCTL (control de operator) 69
 profil utilizator 85
 securizare 186
 tipărire parametri importanți pentru securitate 277
 tipărire parametrului relevanți de securitate 623

coadă de joburi
 autorizare specială *JOBCTL (control de job) 69
 autorizare specială *SPLCTL (control de spool) 69
 autorizatie obiect cerută pentru comenzi 371
 parametru *OPRCTL (control de operator) 69

coadă de mesaje
 autorizatie obiect cerută pentru comenzi 393
 creare automată 83
 mod de livrare *BREAK (întrerupere) 84
 mod de livrare *DFT (implicit) 84
 mod de livrare *HOLD (reținere) 84
 mod de livrare *NOTIFY (notificare) 84
 parametru de gravitate (SEV) 84
 profil utilizator
 parametru de gravitate (SEV) 84
 parametru de livrare (DLVRY) 84
 recomandări 84
 ștergere 101

QSYSMSG 265
 Valoarea de sistem QMAXSGNACN (acționează când încercările sunt atinse) 26
 valoarea de sistem QMAXSIGN (maximum sign-on attempts - număr maxim de încercări de semnare) 25

răspunsuri implicite 84

recomandare
 parametru profil utilizator MSGQ 84

valoarea de sistem job inactiv (QINACTMSGQ) 24

coadă de mesaje QSYSMSG
 auditare 233, 265

Coadă de mesaje QSYSMSG
 Valoarea de sistem QMAXSGNACN (acționează când încercările sunt atinse) 26
 valoarea de sistem QMAXSIGN (maximum sign-on attempts - număr maxim de încercări de semnare) 25

coadă ieșire
 autorizatie obiect cerută pentru comenzi 404

coadă job
 tipărire parametri importanți pentru securitate 277
 tipărire parametrului relevanți de securitate 623

coamanda WRKPEXDFN
 profiluri utilizator livrat de IBM autorizate 297

cod acces
 autorizatie obiect cerută pentru comenzi 400

cod referință sistem (SRC)
 B900 3D10 (auditare eroare) 51

Comand SAV (Save - Salvare)
 autorizarea obiect necesară 360

Comand ENDWTR (End Writer - Oprește scriitor)
 autorizarea obiect necesară 443

Comand RVKPUBAUT (Revocare autorizare publică)
 descriere 278

comanda
 creare
 parametru ALWLMTUSR (permitere utilizator limitat) 67
 parametru PRDLIB (biblioteca produs) 185
 riscuri de securitate 185

comanda (*continuare*)
 modificare
 parametru ALWLMTUSR (permitere utilizator limitat) 67
 parametru PRDLIB (biblioteca produs) 185
 riscuri de securitate 185
 revocare autorizatie publică 625

Comanda (Afișare puncte de întrerupere)
 autorizarea obiect necesară 413

comanda access (Determinare accesibilitate fișier)
 auditare obiect 458

comanda accessx (Determinare accesibilitate fișier)
 auditare obiect 458

comanda Acordare autorizare de utilizator (GRTUSRAUT)
 copiere autorizare 101
 redenumire profil 106

Comanda Acordare autorizare obiect (GRTOBJAUT) 272

Comanda Acordare autorizare utilizator (GRTUSRAUT)
 descriere 274

Comanda Acordare permisiune utilizator (GRTUSRAUT) 275

Comanda Adăugare autorizare obiect de bibliotecă de documente (ADDLLOAUT) 275

Comanda Adăugare intrare director (ADDLDIR) 276

Comanda Adăugare intrare listă de autorizații (ADDAUTLE) 271

Comanda Adăugare intrare planificator de joburi (ADDJOBSCDE)
 meniu SECBATCH 621

Comanda Add Authorization List Entry (ADDAUTLE) 145

comanda ADDACC (Adăugare cod acces)
 auditare obiect 465

comanda ADDACC (Add Access Code - Adăugare cod acces)
 autorizarea obiect necesară 400

comanda ADDAJE (Adăugare intrare job autostart)
 auditare obiect 492

Comanda ADDAJE (Add Autostart Job Entry - Adăugare intrare pornire automată job)
 autorizarea obiect necesară 431

comanda ADDALRACNE (Adăugare intrare acțiune alertă)
 auditare obiect 472

Comanda ADDALRACNE (Add Alert Action Entry - Adăugare intrare acțiune alertă)
 autorizarea obiect necesară 344

comanda ADDALRD (Adăugare descriere alertă)
 auditare obiect 450

Comanda ADDALRD (Add Alert Description - adăugare descriere alertă)
 autorizarea obiect necesară 312

comanda ADDALRSLTE (Adăugare intrare selecție alertă)
 auditare obiect 472

Comanda ADDALRSLTE (Add Alert Selection Entry - Adăugare intrare selecție alertă)
autorizarea obiect necesară 344

comanda ADDAUTLE (Adăugare intrare listă de autorizații)
auditare obiect 451

Comanda ADDAUTLE (Adăugare intrare listă de autorizații)
descriere 271

Comanda ADDAUTLE (Add Authorization List Entry - Adăugare intrare în lista de autorizare)
autorizarea obiect necesară 314
folosire 145

Comanda AADBKP (Adăugare punct de întrerupere)
autorizarea obiect necesară 412

comanda AADBNDIRE (Adăugare intrare director de legături)
auditare obiect 452

Comanda AADBNDIRE (Add Binding Directory Entry - Adăugare intrare director de legare)
autorizarea obiect necesară 314

comanda ADDBSCDEVE (Adăugare intrare dispozitiv BSC)
auditare obiect 469

comanda ADDCFGLE (Adăugare intrări listă de configurație)
auditare obiect 452

Comanda ADDCFGLE (Add Configuration List Entries - Adăugare intrări în lista de configurare)
autorizarea obiect necesară 322

comanda ADDCLUNODE (Add - Adăugare) profiluri utilizator livrat de IBM
autorizate 287

comanda ADDCMDCRQA (Adăugare activitate cerere de modificare comandă)
auditare obiect 453

comanda ADDCMDCRQA (Add Command Change Request Activity - Adăugare activitate cerere modificare comandă)
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDCMDCRQA (Add Command Change Request Activity - Adăugare activitate cerere modificare comandă)
autorizări obiect necesare 315

comanda ADDCMNDEVE (Adăugare intrare dispozitiv de comunicații)
auditare obiect 469

comanda ADDCMNE (Adăugare intrare comunicații)
auditare obiect 492

Comanda ADDCMNE (Add Communications Entry - Adăugare intrare comunicații)
autorizarea obiect necesară 431

comanda ADDCNNLE (Adăugare intrare listă de conexiuni)
auditare obiect 455

Comanda ADDCOMSNMP (Adăugare comunitate pentru SNMP)
autorizarea obiect necesară 438

comanda ADDCRGDEVE
autorizarea obiect necesară 317

comanda ADDCRGDEVE (*continua*)
profiluri utilizator livrat de IBM
autorizate 287

comanda ADDCRGNODE
autorizarea obiect necesară 317
profiluri utilizator livrat de IBM
autorizate 287

comanda ADDCRSDMNK (Add Cross Domain Key - Adăugare cheie traversare domeniu)
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDCRSDMNK (Add Cross Domain Key - Adăugare cheie traversare domeniu)
autorizări obiect necesare 324

comanda ADDDEVDMNE
autorizarea obiect necesară 317
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDDIRE (Adăugare intrare director)
descriere 276

Comanda ADDDIRE (Add Directory Entry - Adăugare intrare director)
autorizarea obiect necesară 329

Comanda ADDDIRSHD (Add Directory Shadow System - Adăugare sistem umbră director)
autorizarea obiect necesară 329

Comanda ADDDLOAUT (Adăugare autorizare obiect de bibliotecă de documente)
descriere 275

comanda ADDDLOAUT (Adăugare autorizare obiect de bibliotecă documente)
auditare obiect 463

Comanda ADDDLOAUT (Add Document Library Object Authority - Adăugare autorizare obiect bibliotecă document)
autorizări obiect necesare 331

comanda ADDDSPDEVE (Adăugare intrare dispozitiv)
auditare obiect 469

Comanda ADDDSTLE (Add Distribution List Entry - Adăugare intrare în lista de distribuție)
autorizarea obiect necesară 331

comanda ADDDSTQ (Add Distribution Queue - Adăugare coadă de distribuție)
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDDSTQ (Add Distribution Queue - Adăugare coadă de distribuție)
autorizarea obiect necesară 330

comanda ADDDSTRTE (Adăugare rută de distribuție)
profiluri utilizator autorizate livrat de IBM
287

Comanda ADDDSTRTE (Add Distribution Route - Adăugare rută de distribuție)
autorizarea obiect necesară 330

comanda ADDDSTSYSN (Adăugare nume sistem secundar de distribuție)
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDDSTSYSN (Add Distribution Secondary System Name - Adăugare nume sistem secundar de distribuție)
autorizări obiect necesare 330

Comanda ADDDTADFN (Add Data Definition - Adăugare definiție de date)
autorizarea obiect necesară 366

Comanda ADDEMLCFGE (Add Emulation Configuration Entry - Adăugare intrare configurație de emulare)
autorizarea obiect necesară 328

Comanda ADDENVVAR (Add Environment Variable - Adăugare variabilă de mediu)
autorizarea obiect necesară 336

Comanda ADDEWCBCDE (Add Extended Wireless Controller Bar Code Entry - Adăugare intrare cod de bare controler de comunicație fără fir extinsă)
autorizarea obiect necesară 336

Comanda ADDEWCM (Add Extended Wireless Controller Member - Adăugare membru controler de comunicație fără fir extinsă)
autorizări obiect necesare 336

Comanda ADDEWCPTCE (Add Extended Wireless Controller PTC Code Entry - Adăugare intrare PTC controler de comunicație fără fir extinsă)
autorizări obiect necesare 336

Comanda ADDEWLM (Add Extended Wireless Line Member - Adăugare membru linie de comunicație fără fir extinsă)
autorizarea obiect necesară 336

comanda ADDEXITPGM (Adăugare program ieșire)
auditare obiect 467

Comanda ADDEXITPGM (Add Exit Program - Adăugare program de ieșire)
autorizarea obiect necesară 418

comanda ADDEXITPGM (Add Exit Program - Adăugare program ieșire)
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDDFCTE (Adăugare intrare tabel de control formulare)
autorizări obiect necesare 419

comanda ADDICFDEVE (Adăugare intrare dispozitiv program funcție de comunicații intersisteme)
auditare obiect 469

Comanda ADDICFDEVE (Add Intersystem Communications Function Program Device Entry - Adăugare intrare dispozitiv program de funcționare a comunicațiilor intersistem)
autorizarea obiect necesară 337

Comanda ADDIMGCLGE
autorizarea obiect necesară 346
profiluri utilizator livrat de IBM
autorizate 287

Comanda ADDIPSIFC (Add IP over SNA Interface - Adăugare IP pe interfață SNA)
autorizarea obiect necesară 312

Comanda ADDIPSLC (Add IP over SNA Location - Adăugare IP pe locație SNA)
autorizarea obiect necesară 312

- Comanda ADDIPSRTE (Add IP over SNA Route - Adăugare IP pe rută SNA) autorizarea obiect necesară 312
- comanda ADDJOBQE (Adăugare intrare coadă joburi) auditare obiect 475, 492
- Comanda ADDJOBQE (Add Job Queue Entry - Adăugare intrare în coadă de joburi) autorizarea obiect necesară 431
- comanda ADDJOBSCDE (Adăugare intrare planificare job) auditare obiect 475
- Comanda ADDJOBSCDE (Adăugare intrare planificator de joburi) autorizări obiect necesare 372
menui SECBATCH 621
- Comanda ADDLANADPI (Adăugare informații adaptor LAN) autorizarea obiect necesară 389
- comanda ADDLFM (Adăugare membru fișier logic) auditare obiect 469
- Comanda ADDLFM (Add Logical File Member - Adăugare membru fișier logic) autorizarea obiect necesară 337
- Comanda ADDLIBLE (Add Library List Entry - Adăugare intrare în lista de biblioteci) autorizarea obiect necesară 382
- comanda ADDLIBLE (Add Library List Entry - Adăugare intrare listă de biblioteci) 183
- comanda ADDLIBLE (Add Library List Entry - Adăugare intrare listă de biblioteci) 186
- Comanda ADDLICENSE (Add License Key - Adăugare cheie de licență) autorizarea obiect necesară 386
- comanda ADDLNK (Adăugare legătură) auditare obiect 494, 499
- Comanda ADDLNK (Add Link - Adăugare legătură) autorizarea obiect necesară 347
- comanda ADDMFS (Add Mounted File System - Adăugare sistem de fișiere montat) autorizarea obiect necesară 439
profiluri utilizator livrat de IBM autorizate 287
- Comanda ADDMFS (Add Mounted File System - Adăugare sistem de fișiere montat) autorizări obiect necesare 396
- Comanda ADDMSGD (Adăugare descriere mesaj) auditare obiect 481
- Comanda ADDMSGD (Add Message Description - Adăugare descriere mesaj) autorizarea obiect necesară 392
- Comanda ADDNETJOB (Add Network Job Entry - Adăugare intrare job rețea) autorizarea obiect necesară 395
profiluri utilizator autorizate livrat de IBM 287
- Comanda ADDNETTBLE (Adăugare intrare tabel rețea) autorizări obiect necesare 438
- comanda ADDNODLE (Adăugare intrare listă de noduri) auditare obiect 483
- Comanda ADDNODLE (Add Node List Entry - Adăugare intrare în lista de noduri) autorizarea obiect necesară 399
- Comanda ADDNWSSTGL (Add Network Server Storage Link - Adăugare legătură spațiu de stocare server de rețea) autorizarea obiect necesară 397
- comanda ADDOBJCRQA (Adăugare activitate cerere modificare obiect) auditare obiect 453
- Comanda ADDOBJCRQA (Add Object Change Request Activity - Adăugare activitate de cerere modificare obiect) profiluri utilizator livrat de IBM autorizate 287
- Comanda ADDOBJCRQA (Add Object Change Request Activity - Adăugare activitate de cerere de modificare obiect) autorizări obiect necesare 315
- comanda ADDOFENR (Adăugare înrolare birou) auditare obiect 463
- Comanda ADDOPTCTG (Add Optical Cartridge - Adăugare cartuș optic) autorizarea obiect necesară 401
profiluri utilizator livrat de IBM autorizate 287
- comanda ADDOPTSVR (Add Optical Server - Adăugare server optic) profiluri utilizator livrat de IBM autorizate 287
- Comanda ADDOPTSVR (Add Optical Server - Adăugare server optic) autorizarea obiect necesară 401
- Comanda ADDPCST (Add Physical File Constraint - Adăugare constrângere fișier fizic) autorizarea obiect necesară 337
- comanda ADDPEXDFN () profiluri utilizator livrat de IBM autorizate 287
- Comanda ADDPEXDFN (Add Performance Explorer Definition - Adăugare definiție explorare performanță) autorizarea obiect necesară 406
- comanda ADDPEXFR () profiluri utilizator livrat de IBM autorizate 287
- comanda ADDPFCST (Adăugare constrângere fișier fizic) auditare obiect 469
- comanda ADDPFM (Adăugare membru fișier fizic) auditare obiect 469
- Comanda ADDPFM (Add Physical File Member - Adăugare membru fișier fizic) autorizarea obiect necesară 337
- comanda ADDPFTRG (Adăugare declanșator fișier fizic) auditare obiect 469
autorizarea obiect necesară 337
- comanda ADDPFVLM (Adăugare membru de lungime variabilă fișier fizic) auditare obiect 469
- Comanda ADDPGM (Adăugare program) autorizarea obiect necesară 412
- comanda ADDPJE (Adăugare intrare job prestart) auditare obiect 492
- Comanda ADDPJE (Add Prestart Job Entry - Adăugare intrare job prestart) autorizarea obiect necesară 432
- comanda ADDPRBACNE (Adăugare intrare acțiune problemă) auditare obiect 472
- Comanda ADDPRBACNE (Add Problem Action Entry - Adăugare intrare acțiune problemă) autorizarea obiect necesară 344, 411
- comanda ADDPRBSLTE (Adăugare intrare selecție problemă) auditare obiect 472
- Comanda ADDPRBSLTE (Add Problem Selection Entry - Adăugare intrare selecție problemă) autorizarea obiect necesară 344, 412
- comanda ADDPRDCRQA (Adăugare activitate cerere de modificare produs) auditare obiect 453
- comanda ADDPRDCRQA (Add Product Change Request Activity - Adăugare activitate cerere modificare produs) profiluri utilizator livrat de IBM autorizate 287
- Comanda ADDPRDCRQA (Add Product Change Request Activity - Adăugare activitate cerere modificare produs) autorizări obiect necesare 315
- comanda ADDPRDLICI (Adăugare informații de licență produs) auditare obiect 489
- comanda ADDPTFCRQA (Adăugare activitate cerere modificare PTF) auditare obiect 453
- comanda ADDPTFCRQA (Add PTF Change Request Activity - Adăugare activitate cerere modificare PTF) profiluri utilizator autorizate livrat de IBM 287
- Comanda ADDPTFCRQA (Add PTF Change Request Activity - Adăugare activitate cerere modificare PTF) autorizarea obiect necesară 315
- Comanda ADDRBDIRE (Adăugare intrare director baze de date relaționale) autorizarea obiect necesară 419
- Comanda ADDRJECMNE (Adăugare intrare comunicații RJE) autorizări obiect necesare 419
- Comanda ADDRJERDRE (Adăugare intrare cititor) autorizări obiect necesare 420
- Comanda ADDRJEWTRE (Adăugare intrare scriitor RJE) autorizări obiect necesare 420
- comanda ADDRMTJRN (Adăugare jurnal la distanță) auditare obiect 476
- Comanda ADDRMTSVR (Add Remote Server - Adăugare server la distanță) autorizarea obiect necesară 398

comanda ADDRPLYE (Adăugare intrare listă răspuns)
 auditare obiect 492
 profiluri utilizator livrat de IBM autorizate 287

Comanda ADDRPLYE (Add Reply List Entry - Adăugare intrare listă replică)
 autorizarea obiect necesară 433

comanda ADDRSCCRQA (Adăugare activitate cerere de modificare resursă)
 auditare obiect 453

Comanda ADDRSCCRQA (Add Resource Change Request Activity - Adăugare activitate de cerere de modificare resursă)
 autorizări obiect necesare 315
 profiluri utilizator livrat de IBM autorizate 288

comanda ADDRTGE (Adăugare intrare rutare)
 auditare obiect 492

Comanda ADDRTGE (Add Routing Entry - Adăugare intrare rutare)
 autorizarea obiect necesară 432

comanda ADDSCHIDX (Adăugare intrare index de căutare)
 auditare obiect 488, 493

Comanda ADDSCHIDX (Add Search Index Entry - Adăugare intrare index de căutare)
 autorizări obiect necesare 366

Comanda ADDSOCE (Adăugare intrare sferă de control)
 autorizarea obiect necesară 429

Comanda ADDSRVTBLE (Adăugare intrare tabel service)
 autorizarea obiect necesară 438
 autorizări obiect necesare 438

Comanda ADDSVRAUTE (Adăugare intrare autentificare server)
 autorizarea obiect necesară 424

Comanda ADDTAPCTG (Add Tape Cartridge - Adăugare cartuş bandă)
 autorizarea obiect necesară 389

Comanda ADDTCPIFC (Adăugare interfaţă TCP/IP)
 autorizarea obiect necesară 438

Comanda ADDTCPPORT (Adăugare intrare port TCP/IP)
 autorizarea obiect necesară 438

Comanda ADDTCPRSI (Adăugare informaţii sistem la distanţă TCP/IP)
 autorizarea obiect necesară 438

Comanda ADDTCPRTE (Adăugare rută TCP/IP)
 autorizarea obiect necesară 438

Comanda ADDTRC (Adăugare urmă)
 autorizarea obiect necesară 412

comanda ADDWSE (Add Workstation Entry - Adăugare intrare staţie de lucru)
 auditare obiect 492
 autorizarea obiect necesară 432

Comanda Afişare auditare de securitate (Valori DSPSECAUD)
 descriere 277

Comanda Afişare auditare obiect de bibliotecă de documente (DSPDLOAUD) 275

Comanda Afişare auditare securitate (DSPSECAUD)
 descriere 619

Comanda Afişare autorizare (DSPAUT) 272

Comanda Afişare autorizare obiect (DSPOBJAUT) 272

Comanda Afişare autorizare obiect de bibliotecă de documente (DSPDLOAUD) 275

Comanda Afişare descriere obiect (DSPOBJD) 272
 creat de 123

Comanda Afişare deţinător de autorizare (DSPAUTHLR) 271

Comanda Afişare intrări jurnal de auditare (DSPAUDJRNE)
 descriere 277, 621

Comanda Afişare listă de autorizaţii (DSPAUTL) 271

Comanda Afişare obiecte de bibliotecă de documente pentru listă de autorizaţii (DSPAUTLDLO) 275

Comanda Afişare obiecte listă de autorizaţii (DSPAUTOBJ) 271

Comanda Afişare planificare activare (DSPACTSCD)
 descriere 617

Comanda Afişare Planificator de expirare (DSPEXPSCD)
 descriere 617

comanda Afişare profil utilizator (DSPUSRPRF)
 folosind 104

Comanda Afişare profil utilizator (DSPUSRPRF)
 descriere 274

Comanda Afişare program (DSPPGM)
 autorizare adoptată 130

Comanda Afişare program service (DSPSRVPGM)
 autorizare adoptată 130

Comanda Afişare programe care adoptă (DSPPGMADP)
 descriere 275
 folosirea 130

comanda Afişare utilizatori autorizaţi (DSPAUTUSR)
 exemplu 104

Comanda Afişare utilizatori autorizaţi (DSPAUTUSR)
 descriere 274

comanda ALCOBJ (Allocate Object - Alocare obiect)
 autorizarea obiect necesară 303

comanda ALCOBJ (Alocare obiect)
 auditare obiect 449

Comanda Analizare activitate profil (ANZPRFACT)
 creare utilizator exempt 617
 descriere 617

Comanda Analizare parole implicite (ANZDFTPWD)
 descriere 617

comanda ANSLIN (Linie răspuns)
 auditare obiect 478

comanda ANSQST (Answer Questions - Răspuns întrebări)
 profiluri utilizator livrat de IBM autorizate 288

Comanda ANSQST (Answer Questions - Răspuns la întrebări)
 autorizarea obiect necesară 417

Comanda ANZBESTMDL (Analyze BEST/1 Model - Analizare model BEST/1)
 autorizarea obiect necesară 406

Comanda ANZDBF (Analyze Database File - Analiză fişier bază de date)
 autorizări obiect necesare 406

Comanda ANZDBFKEY (Analyze Database File Keys - Analiză chei fişier bază de date)
 autorizarea obiect necesară 406

Comanda ANZDFTPWD (Analizare parolă implicită)
 autorizarea obiect necesară 440

Comanda ANZDFTPWD (Analizare parole implicite)
 descriere 617

comanda ANZDFTPWD (Analyze Default Passwords - Analizare parole implicite)
 profiluri utilizator livrat de IBM autorizate 288

comanda ANZJVM
 autorizarea obiect necesară 367

Comanda ANZPFRDT2 (Analyze Performance Data - Analiză date de performanţă)
 autorizarea obiect necesară 406

Comanda ANZPFRDTA (Analyze Performance Data - Analiză date de performanţă)
 autorizarea obiect necesară 406

comanda ANZPGM (Analiză program)
 auditare obiect 488

Comanda ANZPGM (Analyze Program - Analiză program)
 autorizarea obiect necesară 406

comanda ANZPRB (Analyze Problem - Analizare problemă)
 profiluri utilizator livrat de IBM autorizate 288

Comanda ANZPRB (Analyze Problem - Analiză problemă)
 autorizarea obiect necesară 412

Comanda ANZPRFACT (Analizare activitate profil)
 creare utilizator exempt 617
 descriere 617

Comanda ANZPRFACT (Analyze Profile Activity - Analiză activitate profil)
 autorizarea obiect necesară 440

comanda ANZQRY (Analiză cerere)
 auditare obiect 490

Comanda ANZQRY (Analiză interogare)
 autorizarea obiect necesară 416

Comanda ANZS34OCL (Analyze System/34 OCL - Analiză OCL System/34)
 autorizarea obiect necesară 393

comanda ANZS34OCL (Analyze System/34 OCL - Analiză sistem/34 OCL)
 profiluri utilizator livrat de IBM autorizate 288

Comanda ANZS34OCL (Analyze System/36 OCL - Analiză OCL System/36)
 autorizări obiect necesare 393

comanda ANZS36OCL (Analiză System/36 OCL)
 profiluri utilizator livrat de IBM autorizate 288

Comanda Apelare program (CALL)
 transferare autorizare adoptată 128

comanda APYJRNCHG (Aplicare modificări jurnalizate)
 auditare obiect 448, 476

comanda APYJRNCHG (Apply Journalized Changes - Aplicare modificări jurnalizate)
 profiluri utilizator livrat de IBM autorizate 288

Comanda APYJRNCHG (Apply Journalized Changes - Aplicare modificări jurnalizate)
 autorizarea obiect necesară 373

comanda APYJRNCHGX (Aplicare extindere modificări jurnal)
 auditare obiect 469, 476

Comanda APYPTF (Apply Program Temporary Fix - Aplicare corecție temporară pentru program)
 autorizarea obiect necesară 424

comanda APYPTF (Apply Program Temporary Fix - Aplicare corecție temporară program)
 profiluri utilizator livrat de IBM autorizate 288

comanda APYRMTPTF (Apply Remote Program Temporary Fix - Aplicare corecție temporară program la distanță)
 profiluri utilizator livrat de IBM autorizate 288

Comanda ASKQST (Răspuns întrebare)
 autorizarea obiect necesară 417

Comanda Autorizare tipărire descriere job (PRTJOBDAUT)
 descriere 621

Comanda BCHJOB (Batch Job - Job batch)
 autorizarea obiect necesară 367

Comanda CALL (Apel program)
 autorizarea obiect necesară 412

comanda CALL (Apelare program)
 transferare autorizare adoptată 128

Comanda CFGDSTSRV (Configure Distribution Services - Configurare servicii de distribuție)
 autorizarea obiect necesară 330

comanda CFGDSTSRV (Configure Distribution Services - Configurare servicii distribuție)
 profiluri utilizator autorizate livrat de IBM 288

Comanda CFGIPS (Configure IP over SNA Interface - Configurare IP pe interfață SNA)
 autorizarea obiect necesară 312

comanda CFGRPDS (Configurare punte VM/MVS)
 profiluri utilizator livrat de IBM autorizate 288

Comanda CFGRPDS (Configure VM/MVS Bridge - Configurare punte VM/MVS)
 autorizarea obiect necesară 330

Comanda CFGSYSSEC (Configurare securitate sistem)
 autorizarea obiect necesară 423
 descriere 278, 625

Comanda CFGSYSSEC (Configurare securitate sistem) (continuare)
 profiluri utilizator autorizate livrat de IBM 288

Comanda CFGTCP (Configurare TCP/IP)
 obiect autorizare cerută 438

Comanda CFGTCPAPP (Configurare aplicații TCP/IP)
 autorizarea obiect necesară 438

Comanda CFGTCPLPD (Configurare TCP/IP LPD)
 autorizarea obiect necesară 438

Comanda CFGTCPTELN (Modifiare TCP/IP TELNET)
 autorizarea obiect necesară 438

Comanda Change Authority (CHGAUT) 138

Comanda Change Authorization List Entry (CHGAUTLE)
 folosire 145

Comanda Change Journal - Modificare jurnal (CHGJRN) 258, 260

comanda Change Object Owner (CHGOBJOWN) 142

Comanda Change Object Primary Group (CHGOBJPGP) 123, 143

Comanda Change Owner (CHGOWN) 142

Comanda Change Primary Group (CHGPGP) 143

comanda Change Program (CHGPGM)
 specificarea parametrului USEADPAUT 131

comanda Change Service Program (CHGSRVPGM)
 specificarea parametrului USEADPAUT 131

Comanda CHGACGCDE (Change Accounting Code - Modificare cod de contabilizare)
 autorizarea obiect necesară 367

Comanda CHGACGCDE (Modificare cod de contabilizare)
 relație la profil utilizator 82

Comanda CHGACTPRFL (Modificare listă de profiluri activă)
 autorizarea obiect necesară 440
 descriere 617

Comanda CHGACTSCDE (Modificare intrare planificator activare)
 descriere 617

Comanda CHGACTSCDE (Modificare intrare planificator de activități)
 autorizarea obiect necesară 440

Comanda CHGAJE (Change Autostart Job Entry - Modificare intrare job autostart)
 autorizări obiect necesare 432

comanda CHGAJE (Modificare intrare job autostart)
 auditare obiect 492

Comanda CHGALRACNE (Change Alert Action Entry - Modificare intrare acțiune alertă)
 autorizarea obiect necesară 344

comanda CHGALRACNE (Modificare intrare acțiune alertă)
 auditare obiect 472

Comanda CHGALRD (Change Alert Description - Modificare descriere alertă)
 autorizarea obiect necesară 312

comanda CHGALRD (Modificare descriere alertă)
 auditare obiect 450

Comanda CHGALRSLTE (Change Alert Selection Entry - Modificare intrare selecție alertă)
 autorizarea obiect necesară 344

comanda CHGALRSLTE (Modificare intrare selecție alertă)
 auditare obiect 472

Comanda CHGALRTBL (Change Alert Table - Modificare tabel alertă)
 autorizarea obiect necesară 312

comanda CHGALRTBL (Modificare tabelă alertă)
 auditare obiect 450

Comanda CHGASPA 326

comanda CHGATR (Modificare atribut)
 auditare obiect 458

comanda CHGATR (Modificare atribut)
 auditare obiect 459

comanda CHGAUD (Auditare modificare)
 auditare obiect 494, 499

Comanda CHGAUD (Change Auditing - Modificare auditare)
 autorizarea obiect necesară 348

comanda CHGAUD (Modificare auditare)
 auditare obiect 459
 folosind 106

Comanda CHGAUD (Modificare auditare)
 descriere 272, 275

Comanda CHGAUT (Change Authority - Modificare autorizare)
 autorizări obiect necesare 348

Comanda CHGAUT (Change Authority - Schimbare autorizare) 138

comanda CHGAUT (Modificare autorizare)
 auditare obiect 459, 494, 499

Comanda CHGAUT (Modificare autorizare)
 descriere 272

Comanda CHGAUTLE (Change Authorization List Entry - Modificare intrare listă de autorizații)
 autorizarea obiect necesară 314

Comanda CHGAUTLE (Change Authorization List Entry - Schimbare intrare din lista de autorizare)
 folosire 145

comanda CHGAUTLE (Modificare intrare listă de autorizații)
 auditare obiect 451

Comanda CHGAUTLE (Modificare intrare listă de autorizații)
 descriere 271

Comanda CHGBCKUP (Change Backup Options - Modificare opțiuni salvare de rezervă)
 autorizarea obiect necesară 400

Comanda CHGCFGL (Change Configuration List - Modificare listă de configurare)
 autorizarea obiect necesară 322

comanda CHGCFGL (Modificare listă de configurație)
 auditare obiect 452

Comanda CHGCFGLE (Change Configuration List Entry - Modificare intrare listă de configurare)
 autorizarea obiect necesară 322

comanda CHGCFGLE (Modificare intrare listă de configurație)
 auditare obiect 452

Comanda CHGCLNUP (Change Cleanup - Modificare curățare)
 autorizarea obiect necesară 400

Comanda CHGCLS (Change Class - Modificare clasă)
 autorizarea obiect necesară 316

comanda CHGCLS (modificare clasă)
 auditare obiect 454

comanda CHGCLUCFG
 autorizarea obiect necesară 317

comanda CHGCLUNODE
 autorizarea obiect necesară 317

comanda CHGCLUVER
 autorizarea obiect necesară 317

comanda CHGCMD (Change Command - Modificare comandă)
 parametrul PRDLIB (biblioteca produs) 185
 parametrul PRDLIB (biblioteca produs) 185
 riscuri de securitate 185

Comanda CHGCMD (Change Command - Modificare comandă)
 autorizarea obiect necesară 319

comanda CHGCMD (Modificare comandă)
 auditare obiect 454
 parametru ALWLMTUSR (permitere utilizator limitat) 67

comanda CHGCMDCRQA (Change Command Change Request Activity - Modificare activitate cerere modificare comandă)
 profiluri utilizator livrat de IBM autorizate 288

Comanda CHGCMDDCRQA (Change Command Change Request Activity - Modificare activitate cerere modificare comandă)
 autorizări obiect necesare 315

comanda CHGCMDDCRQA (Modificare activitate cerere de modificare comandă)
 auditare obiect 453

Comanda CHGCMDDFT (Change Command Default - Modificare comandă implicită)
 autorizarea obiect necesară 319

Comanda CHGCMDDFT (Change Command Default - Modificare valoare implicită a comenzii) 209
 using 209

comanda CHGCMDDFT (Modificare valoare implicită comandă)
 auditare obiect 454

Comanda CHGCMNE (Change Communications Entry - Modificare intrare comunicații)
 autorizări obiect necesare 432

comanda CHGCMNE (Modificare intrare comunicații)
 auditare obiect 492

comanda CHGCNNL (Modificare listă de conexiuni)
 auditare obiect 455

comanda CHGCNNLE (Modificare intrare listă de conexiuni)
 auditare obiect 455

Comanda CHGCOMSNMP (Modificare comunitate pentru SNMP)
 obiect autorizare cerută 438

Comanda CHGCOSD (Change Class-of-Service Description - Modificare descriere clasă-de-serviciu)
 autorizarea obiect necesară 316

comanda CHGCOSD (Modificare descriere clasă de serviciu)
 auditare obiect 456

comanda CHGCRG
 autorizarea obiect necesară 317

comanda CHGCRGDEVE
 autorizarea obiect necesară 317

comanda CHGCRGPRI
 autorizarea obiect necesară 317

comanda CHGCRQD (Modificare descriere cerere)
 auditare obiect 453
 autorizarea obiect necesară 315

comanda CHGCRSDMNK (Change Cross Domain Key - Modificare cheie traversare domeniu)
 profiluri utilizator livrat de IBM autorizate 288

Comanda CHGCRSDMNK (Change Cross Domain Key - Modificare cheie traversare domeniu)
 autorizări obiect necesare 325

Comanda CHGCSI (Change Communications Side Information - Modificare CSI)
 autorizarea obiect necesară 320

comanda CHGCSI (Modificare CSI)
 auditare obiect 456

comanda CHGCSPPGM (Modificare program CSP/AE)
 auditare obiect 487

Comanda CHGCTLAPPC (Change Controller Description (APPC) - Modificare descriere controler)
 autorizarea obiect necesară 323

Comanda CHGCTLASC (Change Controller Description (Async) - Modificare descriere controler)
 autorizarea obiect necesară 323

Comanda CHGCTLBSC (Change Controller Description (BSC) - Modificare descriere controler (BSC))
 autorizarea obiect necesară 323

Comanda CHGCTLFNC (Change Controller Description (Finance) - Modificare descriere controler (Financiar))
 autorizarea obiect necesară 323

Comanda CHGCTLHOST (Change Controller Description (SNA Host) - Modificare descriere controler (Gazdă SNA))
 autorizarea obiect necesară 323

Comanda CHGCTLLWS (Change Controller Description (Local Workstation Station) - Modificare descriere controler (Stație de lucru locală))
 autorizarea obiect necesară 323

Comanda CHGCTLNET (Change Controller Description (Network) - Modificare descriere controler (Rețea))
 autorizări obiect necesare 323

Comanda CHGCTLRRTL (Change Controller Description (Retail) - Modificare descriere controler (Retail))
 autorizarea obiect necesară 323

Comanda CHGCTLRWS (Change Controller Description (Remote Workstation Station) - Modificare descriere controler (Statie de lucru la distanță))
 autorizarea obiect necesară 323

Comanda CHGCTLTAP (Change Controller Description (TAPE) - Modificare descriere controler (TAPE))
 autorizări obiect necesare 323

Comanda CHGCTLVWS (Change Controller Description (Virtual Workstation Station) - Modificare descriere controler (Stație de lucru virtuală))
 autorizarea obiect necesară 323

comanda CHGCURDIR (Modificare director curent)
 auditare obiect 460

comanda CHGCURLIB (Change Current Library - Modificare bibliotecă curentă)
 restricționare 185

Comanda CHGCURLIB (Change Current Library - Modificare bibliotecă curentă)
 autorizarea obiect necesară 382

Comanda CHGDBG (Modificare depanare)
 autorizarea obiect necesară 412

Comanda CHGD DMF (Change Distributed Data Management File - Modificare fișier de gestiune date distribuite)
 autorizarea obiect necesară 337

comanda CHGD DMF (Modificare fișier gestiune date distribuite)
 auditare obiect 469

Comanda CHGDEVAPPC (Change Device Description (APPC) - Modificare descriere dispozitiv (APPC))
 autorizarea obiect necesară 326

Comanda CHGDEVASC (Change Device Description (Async) - Modificare descriere dispozitiv (Async))
 autorizarea obiect necesară 326

Comanda CHGDEVASP (Change Device Description for Auxiliary Storage Pool - Modificare descriere dispozitiv pentru pool de memorie auxiliară)
 autorizări obiect necesare 326

Comanda CHGDEVBSC (Change Device Description (BSC) - Modificare descriere dispozitiv (BSC))
 autorizarea obiect necesară 326

Comanda CHGDEVCRP
 autorizarea obiect necesară 326

- Comanda CHGDEVDKT (Change Device Description (Diskette) - Modificare descriere dispozitiv (Dischetă))
autorizarea obiect necesară 326
- Comanda CHGDEVDSP (Change Device Description (Display) - Modificare descriere dispozitiv (Ecran))
autorizarea obiect necesară 326
- Comanda CHGDEVFNC (Change Device Description (Finance) - Modificare descriere dispozitiv (Financiar))
autorizarea obiect necesară 326
- Comanda CHGDEVHOST (Change Device Description (SNA Host) - Modificare descriere dispozitiv (Gazdă SNA))
autorizarea obiect necesară 326
- Comanda CHGDEVINTR (Change Device Description (Intrasytem) - Modificare descriere dispozitiv (Intrasistem))
autorizarea obiect necesară 326
- Comanda CHGDEVMLB
autorizarea obiect necesară 326
- Comanda CHGDEVNET (Change Device Description (Network) - Modificare descriere dispozitiv (Rețea))
autorizarea obiect necesară 327
- Comanda CHGDEVNWSH
autorizarea obiect necesară 327
- Comanda CHGDEVOPT (Change Device Description (Optical) - Modificare descriere dispozitiv (Optic))
autorizarea obiect necesară 327, 401
- Comanda CHGDEVPRT (Change Device Description (Printer) - Modificare descriere dispozitiv (Imprimantă))
autorizarea obiect necesară 327
- Comanda CHGDEVRTL (Change Device Description (Retail) - Modificare descriere dispozitiv (Retail))
autorizarea obiect necesară 327
- Comanda CHGDEVSNPT (Change Device Description (SNPT) - Modificare descriere dispozitiv (SNPT))
autorizarea obiect necesară 327
- Comanda CHGDEVSNUF (Change Device Description (SNUF) - Modificare descriere dispozitiv (SNUF))
autorizarea obiect necesară 327
- Comanda CHGDEVTAP (Change Device Description (Tape) - Modificare descriere dispozitiv (Bandă))
autorizarea obiect necesară 327
- Comanda CHGDIRE (Change Directory Entry - Modificare intrare director)
autorizarea obiect necesară 329
- Comanda CHGDIRE (Modificare intrare director)
descriere 276
- Comanda CHGDIRSHD (Change Directory Shadow System - Modificare sistem umbră director)
autorizarea obiect necesară 329
- Comanda CHGDKTF (Change Diskette File - Modificare fișier dischetă)
autorizarea obiect necesară 337
- Comanda CHGDKTF (Modificare fișier deschetă)
auditare obiect 469
- comanda CHGDLOAUD (Modificare auditare obiect bibliotecă document)
autorizare specială *AUDIT (auditare) 71
- Comanda CHGDLOAUD (Modificare auditare obiect bibliotecă document)
Valoarea de sistem QAUDCTL (Control auditare) 50
- comanda CHGDLOAUD (Modificare auditare obiect bibliotecă documente)
auditare obiect 463
- Comanda CHGDLOAUD (Modificare auditare obiect de bibliotecă de documente)
descriere 275
- Comanda CHGDLOAUT (Change Document Library Object Auditing - Modificare auditare obiect bibliotecă document)
autorizarea obiect necesară 331
- Comanda CHGDLOAUT (Change Document Library Object Authority - Modificare autorizare obiect bibliotecă de documente)
autorizarea obiect necesară 331
- Comanda CHGDLOAUT (Modificare autorizare obiect de bibliotecă de documente)
descriere 275
- comanda CHGDLOAUT (Modificare autorizare obiect de bibliotecă documente)
auditare obiect 463
- Comanda CHGDLOOWN (Change Document Library Object Owner - Modificare proprietar obiect bibliotecă de documente)
autorizarea obiect necesară 332
- comanda CHGDLOOWN (Modificare proprietar obiect bibliotecă documente)
auditare obiect 463
- Comanda CHGDLOOWN (Modificare proprietar obiect de bibliotecă de documente)
descriere 275
- Comanda CHGDLOPGP (Change Document Library Object Primary Group - Modificare grup primar obiect bibliotecă de documente)
autorizarea obiect necesară 332
- Comanda CHGDLOPGP (Modificare grup primar obiect de bibliotecă de documente)
descriere 275
- comanda CHGDLOPGP (Modificare grup primar obiect de bibliotecă documente)
auditare obiect 463
- Comanda CHGDLOUAD (Modificare auditare obiect de bibliotecă de documente)
descriere 275
- Comanda CHGDOCD (Change Document Description - Modificare descriere document)
autorizarea obiect necesară 332
- comanda CHGDOCD (Modificare descriere document)
auditare obiect 463
- Comanda CHGDSPF (Change Display File - Modificare fișier de afișare)
autorizarea obiect necesară 337
- comanda CHGDSPF (Modificare fișier de afișare)
auditare obiect 469
- Comanda CHGDSTD (Change Distribution Description - Modificare descriere distribuție)
autorizarea obiect necesară 331
- comanda CHGDSTD (Modificare descriere distribuție)
auditare obiect 463
- Comanda CHGDSTL (Change Distribution List - Modificare listă de distribuție)
autorizarea obiect necesară 331
- Comanda CHGDSTPWD (Change Dedicated Service Tools Password - Modificare parolă instrumente service dedicate)
autorizări obiect necesare 440
- Comanda CHGDSTPWD (Modificare parolă Unelte de service dedicate)
profiluri utilizator livrat de IBM autorizate 288
- Comanda CHGDSTPWD (Modificare parolă Unelte de service dedicate)
descriere 273
- comanda CHGDSTQ (Change Distribution Queue - Modificare coadă de distribuție)
profiluri utilizator autorizate livrat de IBM 288
- Comanda CHGDSTQ (Change Distribution Queue - Modificare coadă de distribuție)
autorizarea obiect necesară 331
- Comanda CHGDSTRTE (Change Distribution Route - Modificare rută distribuție)
autorizarea obiect necesară 331
- comanda CHGDSTRTE (Modificare rută de distribuție)
profiluri utilizator autorizate livrat de IBM 288
- Comanda CHGDSTA (Change Data - Modificare date)
autorizarea obiect necesară 338
- Comanda CHGDTAARA (Change Data Area - Modificare zonă de date)
autorizarea obiect necesară 325
- comanda CHGDTAARA (Modificare zonă de date)
auditare obiect 466
- Comanda CHGEMLCFGE (Change Emulation Configuration Entry - Modificare intrare configurație de emulare)
autorizări obiect necesare 328
- Comanda CHGENVVAR (Change Environment Variable - Modificare variabilă de mediu)
autorizarea obiect necesară 336
- Comanda CHGEWCBCDE (Change Extended Wireless Controller Bar Code Entry - Modificare intrare cod de bare controler de comunicație fără fir extinsă)
autorizarea obiect necesară 336
- Comanda CHGEWCM (Change Extended Wireless Controller Member - Modificare membru controler de comunicație fără fir extinsă)
autorizări obiect necesare 336
- Comanda CHGEWCPTCE (Change Extended Wireless Controller PTC Code Entry - Modificare intrare PTC controler de comunicație fără fir extinsă)
autorizarea obiect necesară 336

- Comanda CHGEWLM (Change Extended Wireless Line Member - Modificare membru linie de comunicație fără fir extinsă) autorizarea obiect necesară 336
- Comanda CHGEXPSCDE (Change Expiration Schedule Entry - Modificare intrare planificator de expirare) autorizarea obiect necesară 440
- comanda CHGEXPSCDE (Modificare intrare planificare expirare) profiluri utilizator livrat de IBM autorizate 288
- Comanda CHGEXPSCDE (Modificare intrare planificator de expirare) descriere 617
- Comanda CHGFCT (Modificare tabel de control formulare) autorizarea obiect necesară 420
- Comanda CHGFCTE (Modificare intrare tabel de control formulare) autorizarea obiect necesară 420
- Comanda CHGFTR (Change Filter - Modificare filtrare) autorizarea obiect necesară 344
- comanda CHGFTR (Modificare filtru) auditare obiect 472
- Comanda CHGGPHFMT (Change Graph Format - Modificare format diagramă) autorizarea obiect necesară 406
- Comanda CHGGPHPKG (Change Graph Package - Modificare pachet diagramă) autorizarea obiect necesară 406
- comanda CHGGPHPKG (Change Graph Package - Modificare pachet grafic) profiluri utilizator livrat de IBM autorizate 288
- Comanda CHGGRPA (Change Group Attributes - Modificare atribute grup) autorizarea obiect necesară 368
- Comanda CHGHLLPTR (Modificare nivel superior a pointerului limbajului) autorizări obiect necesare 412
- Comanda CHGICFDEVE (Change Intersystem Communications Function Program Device Entry - Modificare intrare dispozitiv program de funcționare a comunicațiilor intersistem) autorizarea obiect necesară 338
- Comanda CHGICFF (Change Intersystem Communications Function File - Modificare fișier de funcții de comunicații intersistem) autorizarea obiect necesară 338
- Comanda CHGIPLA 367
- Comanda CHGIPSIFC (Change IP over SNA Interface - Modificare IP pe interfață SNA) autorizarea obiect necesară 312
- Comanda CHGIPSLOC (Change IP over SNA Location - Modificare IP pe locație SNA) autorizarea obiect necesară 312
- Comanda CHGIPSTOS (Change IP over SNA Type of Service - Modificare IP pe tipul de serviciu SNA) autorizarea obiect necesară 312
- Comanda CHGJOB (Change Job - Modificare job) autorizarea obiect necesară 368
- comanda CHGJOB (Modificare job) auditare obiect 475
- comanda CHGJOB (Schimbare job) autorizare adoptată 130
- Comanda CHGJOB (Change Job Description - Modificare descriere job) autorizarea obiect necesară 371
- comanda CHGJOB (Modificare descriere job) auditare obiect 474
- Comanda CHGJOBQE (Change Job Queue Entry - Modificare intrare în coadă de joburi) autorizarea obiect necesară 432
- comanda CHGJOBQE (Modificare intrare coadă joburi) auditare obiect 475, 492
- Comanda CHGJOBSCDE (Change Job Schedule Entry - Modificare intrare planificare job) autorizări obiect necesare 372
- comanda CHGJOBSCDE (Modificare intrare planificare job) auditare obiect 475
- comanda CHGJOBTYP (Change Job Type - Modificare tip job) profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGJOBTYP (Change Job Type - Modificare tip job) autorizarea obiect necesară 406
- comanda CHGJRN (Change Journal - Modificare jurnal) profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGJRN (Change Journal - Modificare jurnal) autorizarea obiect necesară 373
- detășare receptor 258, 260
- comanda CHGJRN (Modificare jurnal) auditare obiect 476, 477
- comanda CHGJRNOBJ (Modificare obiect jurnalizat) auditare obiect 448
- Comanda CHGLANADPI (Modificare informații adaptor LAN) autorizarea obiect necesară 389
- Comanda CHGLF (Change Logical File - Modificare fișier logic) autorizarea obiect necesară 338
- comanda CHGLF (Modificare fișier logic) auditare obiect 470
- Comanda CHGLFM (Change Logical File Member - Modificare membru fișier logic) autorizarea obiect necesară 338
- comanda CHGLFM (Modificare membru fișier logic) auditare obiect 470
- Comanda CHGLIB (Change Library - Modificare bibliotecă) autorizarea obiect necesară 382
- comanda CHGLIB (Modificare bibliotecă) auditare obiect 478
- comanda CHLIBL (Change Library List - Modificare lista de biblioteci) 183
- folosire 183
- Comanda CHLIBL (Change Library List - Modificare listă de biblioteci) autorizarea obiect necesară 382
- Comanda CHGLICINF (Change License Information - Modificare informații licență) autorizarea obiect necesară 387
- profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGLINASC (Change Line Description (Async) - Modificare descriere de linie (Async)) autorizări obiect necesare 387
- Comanda CHGLINBSC (Change Line Description (BSC) - Modificare descriere de linie (BSC)) autorizări obiect necesare 387
- Comanda CHGLINETH (Change Line Description (Ethernet) - Modificare descriere de linie (Ethernet)) autorizarea obiect necesară 387
- Comanda CHGLINFAX (Change Line Description (FAX) - Modificare descriere de linie (FAX)) autorizarea obiect necesară 387
- Comanda CHGLINFR (Change Line Description (Frame Relay Network) - Modificare descriere de linie (Rețea frame relay)) autorizări obiect necesare 387
- Comanda CHGLINIDD (Change Line Description (DDI Network) - Modificare descriere de linie (Rețea DDI)) autorizarea obiect necesară 387
- Comanda CHGLINSDLC (Change Line Description (SDLC) - Modificare descriere de linie (SDLC)) autorizarea obiect necesară 387
- Comanda CHGLINTDLC (Change Line Description (TDLC) - Modificare descriere de linie (TDLC)) autorizarea obiect necesară 387
- Comanda CHGLINTRN (Change Line Description (Token-Ring Network) - Modificare descriere de linie (Rețea token ring)) autorizări obiect necesare 387
- Comanda CHGLINWLS (Change Line Description (Wireless) - Modificare descriere de linie (Comunicație fără fir)) autorizarea obiect necesară 387
- Comanda CHGLINX25 (Change Line Description (X.25) - Modificare descriere de linie (X.25)) autorizări obiect necesare 387
- Comanda CHGLPDA (Modificare atribute LPD) autorizarea obiect necesară 438
- comanda CHGMGDSYSA (Change Managed System Attributes - Modificare atribute sistem gestionat) profiluri utilizator autorizate livrat de IBM 289
- comanda CHGMGRSRVA (Change Manager Service Attributes - Modificare atribute servicii manager) profiluri utilizator autorizate livrat de IBM 289

comanda CHGMNU (Change Menu - Modificare meniu)
parametrul PRDLIB (biblioteca produs) 185
riscuri de securitate 185

Comanda CHGMNU (Change Menu - Modificare meniu)
autorizarea obiect necesară 390

comanda CHGMNU (Modificare meniu)
auditare obiect 480

Comanda CHGMOD (Change Module - Modificare modul)
autorizarea obiect necesară 394

comanda CHGMOD (Modificare modul)
auditare obiect 481

Comanda CHGMODD (Change Mode Description - Modificare descriere mod)
autorizarea obiect necesară 394

comanda CHGMODD (Modificare descriere mod)
auditare obiect 480

Comanda CHGMSGD (Change Message Description - Modificare descriere mesaj)
autorizarea obiect necesară 392

comanda CHGMSGD (Modificare descriere mesaj)
auditare obiect 481

Comanda CHGMSGF (Change Message File - Modificare fișier mesaj)
autorizarea obiect necesară 392

comanda CHGMSGF (Modificare fișier mesaje)
auditare obiect 481

Comanda CHGMSGQ (Change Message Queue - Modificare coadă de mesaje)
autorizarea obiect necesară 393

comanda CHGMSGQ (Modificare coadă de mesaje)
auditare obiect 482

Comanda CHGMSTK (Change Master Key - Modificare cheie master)
autorizarea obiect necesară 325

comanda CHGMSTK (Change Master Key - Modificare cheie primară)
profiluri utilizator livrat de IBM autorizate 289

comanda CHGNETA (Change Network Attributes - Modificare atribute rețea) 189
folosire 189
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGNETA (Change Network Attributes - Modificare atribute rețea)
autorizarea obiect necesară 395

comanda CHGNETJOBE (Change Network Job Entry - Modificare intrare job rețea)
profiluri utilizator autorizate livrat de IBM 289

Comanda CHGNETJOBE (Change Network Job Entry - Modificare intrare job rețea)
autorizarea obiect necesară 395

comanda CHGNFSEXP (Change Network File System Export - Modificare exportare sistem de fișiere rețea)
autorizarea obiect necesară 396
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGNFSEXP (Change Network File System Export - Modificare exportare sistem de fișiere rețea)
autorizarea obiect necesară 396

Comanda CHGNTBD (Change NetBIOS Description - Modificare descriere NetBIOS)
autorizarea obiect necesară 395

comanda CHGNTBD (Modificare descriere NetBIOS)
auditare obiect 483

Comanda CHGNWIFR (Change Network Interface Description (Frame Relay Network) - Modificare descriere interfață de rețea (Rețea frame relay))
autorizarea obiect necesară 397

comanda CHGNWISDN (Modificare descriere interfață de rețea pentru ISDN)
auditare obiect 484

Comanda CHGNWSA (Change Network Server Attribute - Modificare atribut server de rețea)
autorizări obiect necesare 398

comanda CHGNWSA (Change Network Server Attributes - Modificare atribute server de rețea)
profiluri utilizator autorizate livrat de IBM 289

Comanda CHGNWSALS (Change Network Server Alias - Modificare alias server de rețea)
autorizarea obiect necesară 398

Comanda CHGNWSCFG
autorizarea obiect necesară 399
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGNWSD (Change Network Server Description - Modificare descriere server de rețea)
autorizarea obiect necesară 399

comanda CHGNWSD (Modificare descriere server de rețea)
auditare obiect 484

Comanda CHGNWSSTG (Change Network Server Storage Space - Ștergere spațiu de stocare server de rețea)
autorizarea obiect necesară 397

Comanda CHGNWSVRA (Create Network Server Attribute - Creare atribut server de rețea)
autorizarea obiect necesară 397

Comanda CHGOBJAUD (Change Object Audit - Modificare auditare obiect)
autorizarea obiect necesară 303

comanda CHGOBJAUD (Modificare auditare obiect)
autorizare specială *AUDIT (auditare) 71

Comanda CHGOBJAUD (Modificare auditare obiect)
descriere 272
Valoarea de sistem QAUDCTL (Control auditare) 50

Comanda CHGOBJCRQA (Change Object Change Request Activity - Modificare activitate cerere modificare obiect)
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGOBJCRQA (Change Object Change Request Activity - Modificare activitate de cerere de modificare obiect)
autorizări obiect necesare 315

comanda CHGOBJCRQA (Modificare activitate cerere de modificare obiect)
auditare obiect 454

Comanda CHGOBJD (Change Object Description - Modificare descriere obiect)
autorizări obiect necesare 303

comanda CHGOBJD (Modificare descriere obiect)
auditare obiect 448

comanda CHGOBJOWN (Change Object Owner - Schimbă proprietar obiect)
folosire 142

Comanda CHGOBJOWN (Change Object Owner - Schimbă proprietar obiect)
autorizarea obiect necesară 304

comanda CHGOBJOWN (Modificare proprietar obiect)
auditare obiect 448

Comanda CHGOBJOWN (Modificare proprietar obiect)
descriere 272

Comanda CHGOBJPGP (Change Object Primary - Modificare obiect primar)
autorizarea obiect necesară 304

Comanda CHGOBJPGP (Change Object Primary Group - Schimbă grup primar obiect) 123, 143

Comanda CHGOBJPGP (Modificare grup primar de obiecte)
descriere 272

Comanda CHGOBJUAD (Modificare auditare obiect)
descriere 275

comanda CHGOPTA (Change Optical Attributes - Modificare atribute optice)
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGOPTA (Change Optical Attributes - Modificare atribute optice)
autorizarea obiect necesară 401

Comanda CHGOPTVOL (Change Optical Volume - Modificare volum optic)
autorizarea obiect necesară 402

comanda CHGOUTQ (Change Output Queue - Modificare coadă de ieșire) 186
folosire 186

Comanda CHGOUTQ (Change Output Queue - Modificare coadă de ieșire)
autorizarea obiect necesară 404

comanda CHGOUTQ (Modificare coadă de ieșire)
auditare obiect 485

Comanda CHGOWN (Change Owner - Modificare proprietar)
autorizarea obiect necesară 349

Comanda CHGOWN (Change Owner) 142

comanda CHGOWN (Modificare proprietar)
auditare obiect 459, 494, 499, 501

Comanda CHGOWN (Schimbare proprietar)
descriere 272

- Comanda CHGPCST (Change Physical File Constraint - Modificare constrângere fișier fizic)
 autorizarea obiect necesară 338
- comanda CHGPDGPRF (Modificare profil grup de descriptori tipărire)
 auditare obiect 487
- Comanda CHGPDGPRF (Modificare profil grup descriptor de tipărire)
 autorizarea obiect necesară 411
- Comanda CHGPEXDFN (Change Performance Explorer Definition - Modificare definiție explorare performanță)
 autorizări obiect necesare 407
- comanda CHGPEXDFN (Change Performance Explorer Definition - Modificare definiție Performance Explorer)
 profiluri utilizator autorizate livrat de IBM 289
- Comanda CHGPF (Change Physical File - Modificare fișier fizic)
 autorizarea obiect necesară 338
- comanda CHGPF (Modificare fișier fizic)
 auditare obiect 470
- Comanda CHGPFCNARA (Change Functional Area - Modificare zonă funcțională)
 autorizări obiect necesare 406
- comanda CHGPFCST (Modificare constrângere fișier fizic)
 auditare obiect 470
- Comanda CHGPFM (Change Physical File Member - Modificare membru fișier fizic)
 autorizarea obiect necesară 338
- comanda CHGPFM (Modificare membru fișier fizic)
 auditare obiect 470
- Comanda CHGPFTRG (Change Physical File Trigger - Modificare declanșator fișier fizic)
 autorizarea obiect necesară 338
- comanda CHGPGM (Change Program - Schimbare program)
 specificarea parametrului USEADPAUT 131
- comanda CHGPGM (Modificare program)
 auditare obiect 487
- Comanda CHGPGM (Modificare program)
 autorizarea obiect necesară 413
- Comanda CHGPGMVAR (Modificare variabilă program)
 autorizarea obiect necesară 413
- Comanda CHGPGP (Change Primary Group - Modificare grup primar)
 autorizarea obiect necesară 349
- Comanda CHGPGP (Change Primary Group - Schimbă grup primar) 143
- comanda CHGPGP (Modificare grup primar)
 auditare obiect 459, 494, 499, 501
- Comanda CHGPGP (Modificare grup primar)
 descriere 272
- Comanda CHGPJ (Change Prestart Job - Modificare job prestart)
 autorizarea obiect necesară 368
- Comanda CHGPJE (Change Prestart Job Entry - Modificare intrare job prestart)
 autorizări obiect necesare 432
- comanda CHGPJE (Modificare intrare job prestart)
 auditare obiect 493
- comanda CHGPRB (Change Problem - Modificare problemă)
 profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGPRB (Change Problem - Modificare problemă)
 autorizarea obiect necesară 412
- Comanda CHGPRBACNE (Change Problem Action Entry - Modificare intrare acțiune problemă)
 autorizarea obiect necesară 344, 412
- comanda CHGPRBACNE (Modificare intrare acțiune problemă)
 auditare obiect 472
- Comanda CHGPRBSLTE (Change Problem Selection Entry - Modificare intrare selecție problemă)
 autorizarea obiect necesară 344, 412
- comanda CHGPRBSLTE (Modificare intrare selecție problemă)
 auditare obiect 472
- comanda CHGPRDCRQA (Change Product Change Request Activity - Modificare activitate cerere modificare produs)
 profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGPRDCRQA (Change Product Change Request Activity - Modificare activitate de cerere de modificare produs)
 autorizări obiect necesare 315
- comanda CHGPRDCRQA (Modificare activitate cerere de modificare produs)
 auditare obiect 454
- Comanda CHGPRF (Change Profile - Modificare profil)
 autorizarea obiect necesară 440
- comanda CHGPRF (Modificare profil)
 folosind 101
- Comanda CHGPRF (Modificare profil)
 descriere 274
- Comanda CHGPRTF (Change Printer File - Modificare fișier imprimantă)
 autorizarea obiect necesară 338
- comanda CHGPRTF (Modificare fișier imprimantă)
 auditare obiect 470
- Comanda CHGPSFCFG (Modificare configurare facilitate servicii de tipărire)
 autorizări obiect necesare 411
- comanda CHGPTFCRQA (Change PTF Change Request Activity - Modificare activitate cerere modificare PTF)
 profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGPTFCRQA (Change PTF Change Request Activity - Modificare activitate de cerere de modificare PTF)
 autorizări obiect necesare 315
- comanda CHGPTFCRQA (Modificare activitate cerere de modificare PTF)
 auditare obiect 454
- comanda CHGPTR (Change Pointer - Modificare pointer)
 profiluri utilizator livrat de IBM autorizate 289
- Comanda CHGPTR (Modificare pointer)
 autorizarea obiect necesară 413
- comanda CHGPWD (Change Password - Modificare parolă)
 valori de sistem de parole de impunere 39
- Comanda CHGPWD (Change Password - Modificare parolă)
 auditare 231
 autorizarea obiect necesară 440
- Comanda CHGPWD (Change Recovery for Access Paths - Modificare recuperare pentru căi de acces)
 autorizarea obiect necesară 310
- Comanda CHGPWD (Edit Recovery for Access Paths - Editare recuperare pentru căi de acces)
 autorizarea obiect necesară 310
- comanda CHGPWD (Modificare parolă)
 auditare obiect 503
 setare parolă egală cu nume profil 60
- Comanda CHGPWD (Modificare parolă)
 descriere 273
- Comanda CHGPWRSCD (Change Power On/Off Schedule - Modificare planificare alimentare On/Off)
 autorizarea obiect necesară 400
- Comanda CHGPWRSCDE (Change Power On/Off Schedule Entry - Modificare intrare planificare alimentare On/Off)
 autorizarea obiect necesară 400
- Comanda CHGQRYA (Modificare atribut interogare)
 autorizarea obiect necesară 416
- comanda CHGQSTDB (Change Question-and-Answer Database - Modificare bază de date întrebare-răspuns)
 profiluri utilizator autorizate livrat de IBM 289
- Comanda CHGQSTDB (Change Question-and-Answer Database - Modificare bază de date întrebare-și-răspuns)
 autorizarea obiect necesară 417
- comanda CHGRCYAP (Change Recovery for Access Paths - Modificare recuperare pentru căile de acces)
 profiluri utilizator autorizate livrat de IBM 289
- comanda CHGRCYAP (Recuperare modificări pentru căile de acces)
 auditare obiect 450
- Comanda CHGRDBDIRE (Modificare intrare director baze de date relaționale)
 autorizarea obiect necesară 419
- Comanda CHGRJECMNE (Modificare intrare comunicații RJE)
 autorizări obiect necesare 420
- Comanda CHGRJERDRE (Modificare intrare cititor RJE)
 autorizări obiect necesare 420
- Comanda CHGRJEWTR (Modificare intrare scriitor RJE)
 autorizări obiect necesare 420

comanda CHGRMTJRN (Modificare jurnal la distanță)
auditare obiect 476

Comanda CHGRPYLE (Change Reply List Entry - Modificare intrare listă de replici)
autorizarea obiect necesară 433

comanda CHGRPYLE (Modificare intrare listă răspuns)
auditare obiect 492
profiluri utilizator autorizate livrat de IBM 289

comanda CHGRSCCRQA (Change Resource Change Request Activity - Modificare activitate cerere modificare resursă)
autorizări obiect necesare 315
profiluri utilizator livrat de IBM autorizate 289

comanda CHGRSCCRQA (Modificare activitate cerere de modificare resursă)
auditare obiect 454

Comanda CHGRTGE (Change Routing Entry - Modificare intrare rutare)
autorizarea obiect necesară 432

comanda CHGRTGE (Modificare intrare rutare)
auditare obiect 493

Comanda CHGS34LIBM (Change System/34 Library Members - Modificare membri bibliotecă System/34)
profiluri utilizator livrat de IBM autorizate 289

comanda CHGS34LIBM (Modificare membrii bibliotecă System/34)
autorizarea obiect necesară 393

Comanda CHGS36 (Change System/36 - Modificare System/36)
autorizarea obiect necesară 434

comanda CHGS36 (Modificare System/36)
auditare obiect 502

Comanda CHGS36A (Change System/36 Attributes - Modificare atribute System/36)
autorizarea obiect necesară 434

Comanda CHGS36PGMA (Change System/36 Program Attributes - Modificare atribute program System/36)
autorizări obiect necesare 434

comanda CHGS36PGMA (Modificare atribute program System/36)
auditare obiect 487

Comanda CHGS36PRCA (Change System/36 Procedure Attributes - Modificare atribute procedură System/36)
autorizări obiect necesare 434

comanda CHGS36PRCA (Modificare atribute procedură System/36)
auditare obiect 470

Comanda CHGS36SRCA (Modificare atribute sursă System/36)
autorizări obiect necesare 434

Comanda CHGSAVF (Change Save File - Modificare fișier de salvare)
autorizarea obiect necesară 338

comanda CHGSAVF (Modificare fișier salvare)
auditare obiect 470

Comanda CHGSBSD (Change Subsystem Description - Modificare descriere subsistem)
autorizări obiect necesare 432

comanda CHGSBSD (Modificare descriere subsistem)
auditare obiect 493

Comanda CHGSCHIDX (Change Search Index - Modificare index de căutare)
autorizarea obiect necesară 366

comanda CHGSCHIDX (Modificare index de căutare)
auditare obiect 494

Comanda CHGSECA (Modificare atribute de securitate)
autorizarea obiect necesară 423

Comanda CHGSECAUD (Modificare auditare de securitate)
descriere 277

Comanda CHGSECAUD (Modificare auditare securitate)
autorizarea obiect necesară 423
descriere 619

Comanda CHGSHRPOOL (Modificare spațiu de stocare partajat)
autorizarea obiect necesară 433

Comanda CHGSNMPA (Modificare atribute SNMP)
autorizarea obiect necesară 438

comanda CHGSPLFA (Change Spooled File Attributes - Modificare atribute fișier spool) 186
parametrul DSPDTA la cozii de ieșire 186

Comanda CHGSPLFA (Change Spooled File Attributes - Modificare atribute fișier spool)
autorizări obiect necesare 429

comanda CHGSPLFA (Modificare atribute fișier spool)
auditare acțiune 496
auditare obiect 485

Comanda CHGSRCPF (Change Source Physical File - Modificare fișier fizic sursă)
autorizarea obiect necesară 338

Comanda CHGSRVA (Modificare atribute service)
autorizarea obiect necesară 424

comanda CHGSRVPGM (Change Service Program - Schimbare program de serviciu)
specificarea parametrului USEADPAUT 131

comanda CHGSRVPGM (Modificare program service)
auditare obiect 498

Comanda CHGSRVPGM (Modificare program service)
autorizarea obiect necesară 413

Comanda CHGSSND (Modificare descriere sesiune)
autorizări obiect necesare 420

Comanda CHGSSNMAX (Change Session Maximum - Modificare maxim sesiune)
autorizarea obiect necesară 394

comanda CHGSSNMAX (Modificare maxim sesiuni)
auditare obiect 480

Comanda CHGSVRAUTE (Modificare intrare autentificare server)
autorizarea obiect necesară 424

Comanda CHGSYSDIRA (Change System Directory Attributes - Modificare atribute director sistem)
autorizarea obiect necesară 329

comanda CHGSYSDIRA (Modificare atribute director sistem)
auditare obiect 462

Comanda CHGSYSJOB (Change System Job - Modificare job sistem)
autorizarea obiect necesară 368

comanda CHGSYSLIBL (Change System Library List - Modificare lista de biblioteci sistem) 183
folosire 183

comanda CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem)
profiluri utilizator autorizate livrat de IBM 289

Comanda CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem) 202
autorizarea obiect necesară 382
exemplu de programare 202

comanda CHGSYSVAL (Change System Value - Modificare valoare sistem)
profiluri utilizator livrat de IBM autorizate 289

Comanda CHGSYSVAL (Change System Value - Modificare valoare sistem)
autorizarea obiect necesară 433

Comanda CHGTAPCTG (Change Tape Cartridge - Modificare cartuș bandă)
autorizarea obiect necesară 389

Comanda CHGTAPF (Change Tape File - Modificare fișier bandă)
autorizarea obiect necesară 338

comanda CHGTAPF (Modificare fișier bandă)
auditare obiect 470

Comanda CHGTCPA (Modificare atribute TCP/IP)
autorizări obiect necesare 438

Comanda CHGTCPHTE (Modificare intrare tabel gazdă TCP/IP)
autorizarea obiect necesară 438

Comanda CHGTCPIFC (Modificare intrare TCP/IP)
autorizarea obiect necesară 438

Comanda CHGTCPRTE (Modificare intrare rută TCP/IP)
autorizări obiect necesare 438

Comanda CHGTELNA (Modificare atribute TELNET)
autorizarea obiect necesară 438

Comanda CHGTIMZON 438

comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator)
Valoarea de sistem QAUDCTL (Control auditare) 50

Comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator)
autorizarea obiect necesară 440
Valoarea de sistem QAUDCTL (Control auditare) 50

comanda CHGUSRAUD (Modificare auditare utilizator)
autorizare specială *AUDIT (auditare) 71
folosind 106

Comanda CHGUSRAUD (Modificare auditare utilizator)
descriere 274, 275

comanda CHGUSRPRF (Change User Profile - Modificare profil utilizator)
valori de sistem de compunere parolă 39

Comanda CHGUSRPRF (Change User Profile - Modificare profil utilizator)
autorizarea obiect necesară 441

comanda CHGUSRPRF (Modificare profil utilizator)
auditare obiect 503
folosind 101
setare parolă egală cu nume profil 60

Comanda CHGUSRPRF (Modificare profil utilizator)
descriere 273, 274

Comanda CHGUSRTRC (Change User Trace - Modificare urmă utilizator)
autorizarea obiect necesară 368

Comanda CHGVTMAP (Modificare hartă tastatură VT100)
autorizarea obiect necesară 438

comanda CHGWSE (Change Workstation Entry - Modificare intrare stație de lucru)
auditare obiect 493
autorizări obiect necesare 432

Comanda CHKCMNTRC (Check Communications Trace - Verificare urmă comunicații)
autorizarea obiect necesară 424

comanda CHKCMNTRC (Check Communications Trace - Verificare urmărire comunicații)
profiluri utilizator autorizate livrat de IBM 289

Comanda CHKDKT (Check Diskette - Verificare dischetă)
autorizarea obiect necesară 389

Comanda CHKDLO (Check Document Library Object - Verificare obiect bibliotecă document)
autorizarea obiect necesară 332

Comanda CHKDOC (Check Document - Verificare document)
autorizarea obiect necesară 332

comanda CHKDOC (Verificare document)
auditare obiect 462

comanda CHKIGCTBL (Verificare tabelă fonturi DBCS)
auditare obiect 474

Comanda CHKIN (Check In - Înregistrare)
autorizarea obiect necesară 350

comanda CHKIN (Înregistrare)
auditare obiect 494, 499

Comanda CHKOBJ (Check Object - Verificare obiect)
autorizarea obiect necesară 304

comanda CHKOBJ (Verificare obiect)
auditare obiect 449

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului)
auditare folosire 233

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului) (*continuare*)
descriere 269

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate obiect) 3
autorizarea obiect necesară 304

Comanda CHKOBJITG (Verificare integritate obiect)
descriere 274, 621

Comanda CHKOUT (Check Out - Anulare înregistrare)
autorizarea obiect necesară 350

comanda CHKOUT (Debifare)
auditare obiect 494, 499

comanda CHKPRDOPT (Check Product Option - Verificare opțiune produs)
profiluri utilizator livrat de IBM autorizate 289

Comanda CHKPRDOPT (Check Product Option - Verificare opțiune produs)
autorizarea obiect necesară 424

Comanda CHKPWD (Check Password - Verificare parolă)
autorizarea obiect necesară 441

comanda CHKPWD (Verificare parolă)
auditare obiect 503
folosind 107

Comanda CHKPWD (Verificare parolă)
descriere 273

Comanda CHKTAP (Check Tape - Verificare bandă)
autorizarea obiect necesară 390

Comanda CLRDKT (Clear Diskette - Curățare dischetă)
autorizarea obiect necesară 390

Comanda CLRJOBQ (Clear Job Queue - Curățare coadă joburi)
autorizarea obiect necesară 371

comanda CLRJOBQ (Curățare coadă joburi)
auditare obiect 474

Comanda CLRRLIB (Clear Library - Curățare bibliotecă)
autorizarea obiect necesară 382

comanda CLRRLIB (Curățare bibliotecă)
auditare obiect 478

Comanda CLRMSGQ (Clear Message Queue - Curățare coadă de mesaje)
autorizarea obiect necesară 393

comanda CLRMSGQ (Curățare coadă de mesaje)
auditare obiect 482

Comanda CLRROUTQ (Clear Output Queue - Curățare coadă de ieșire)
autorizarea obiect necesară 404

comanda CLRROUTQ (Curățare coadă de ieșire)
auditare acțiune 497
auditare obiect 485

Comanda CLRPFM (Clear Physical File Member - Curățare membru fișier fizic)
autorizarea obiect necesară 338

comanda CLRPFM (Curățare membru fișier fizic)
auditare obiect 470

Comanda CLRSVAVF (Clear Save File - Curățare fișier de salvare)
autorizarea obiect necesară 338

Comanda CLRTRCDTA (Ștergere date urmărite)
autorizarea obiect necesară 413

comanda CMPJRNIMG (Comparație imagini jurnal)
auditare obiect 476

Comanda CMPJRNIMG (Compare Journal Images - Comparare imagini jurnal)
autorizarea obiect necesară 373

Comanda CNLJRERDR (Anulare cititor RJE)
autorizarea obiect necesară 421

Comanda CNLJREWTR (Anulare scriitor RJE)
autorizarea obiect necesară 421

Comanda COMMIT (Comitere)
autorizarea obiect necesară 320

Comanda Configurare securitate sistem (CFGSYSSEC)
descriere 278, 625

comanda CPHDTA (Cipher Data - Cifrare date)
profiluri utilizator livrat de IBM autorizate 289

Comanda CPHDTA (Cipher Data - Cifrare date)
autorizarea obiect necesară 325

Comanda CPROBJ (Compress Object - Comprimare obiect)
autorizarea obiect necesară 304

comanda CPROBJ (Comprimare obiect)
auditare obiect 449

comanda CPY (Copiere)
auditare obiect 459

Comanda CPY (Copy - Copiere)
autorizarea obiect necesară 350

Comanda CPYAUDJRNE
autorizarea obiect necesară 373

comanda CPYCFGL (Copiere listă de configurație)
auditare obiect 452

Comanda CPYCFGL (Copy Configuration List - Copiere listă de configurare)
autorizarea obiect necesară 322

Comanda CPYCNARA (Copy Functional Area - Copiere zonă funcțională)
autorizarea obiect necesară 407

comanda CPYDOC (Copiere document)
auditare obiect 462, 463

Comanda CPYDOC (Copy Document - Copiere document)
autorizarea obiect necesară 332

comanda CPYF (Copiere fișier)
auditare obiect 468, 470

Comanda CPYF (Copy File - Copiere fișier)
autorizarea obiect necesară 338

Comanda CPYFRMDIR (Copy from Directory - Copiere din director)
autorizarea obiect necesară 329

Comanda CPYFRMDKT (Copy from Diskette - Copiere de pe dischetă)
autorizarea obiect necesară 338

Comanda CPYFRMIMP (Copy form Import File - Copiere din fișier de importare)
autorizarea obiect necesară 338

- Comanda CPYFRMQRYF (Copy form Query File - Copiere din fișier de interogare) autorizarea obiect necesară 339
- Comanda CPYFRMSTMF (Copy form Stream File - Copiere din fișier flux) autorizări obiect necesare 339
- Comanda CPYFRMTAP (Copy from Tape - Copiere de pe bandă) autorizarea obiect necesară 339
- Comanda CPYGPFFMT (Copy Graph Format - Copiere format diagramă) autorizarea obiect necesară 407
- Comanda CPYGPFFPKG (Copy Graph Package - Copiere pachet grafic) autorizarea obiect necesară 407
- comanda CPYIGCTBL (Copiere tabelă fonturi DBCS) auditare obiect 474
- Comanda CPYIGCTBL (Copy DBCS Font Table - Copiere tabel font DBCS) autorizarea obiect necesară 335
- Comanda CPYLIB (Copy Library - Copiere bibliotecă) autorizarea obiect necesară 383
- Comanda CPYOPT (Copy Optical - Copiere optic) autorizarea obiect necesară 402
- Comanda CPYPRDTA (Copy Performance Data - Copiere date de performanță) autorizarea obiect necesară 407
- Comanda CPYPTF (Copie corecție temporară program) autorizarea obiect necesară 424
profiluri utilizator livrat de IBM autorizate 289
- Comanda CPYPTFGRP (Copiere grup PTF) autorizarea obiect necesară 424
- comanda CPYSPLF (Copiere fișier spool) auditare acțiune 496
auditare obiect 485
- comanda CPYSPLF (Copy Spooled File - Copiere fișier spool) 186
- comanda CPYSPLF (Copy Spooled File - Copierea unui fișier spool) parametrul DSPDTA al cozii de ieșire 186
- Comanda CPYSPLF (Copy Spooled File - Copierea unui fișier spool) autorizarea obiect necesară 430
- Comanda CPYSRCF (Copy Source File - Copiere fișier sursă) autorizarea obiect necesară 339
- Comanda CPYTODIR (Copy to Directory - Copiere în director) autorizări obiect necesare 329
- Comanda CPYTODKT (Copy to Diskette - Copiere pe dischetă) autorizarea obiect necesară 339
- Comanda CPYTOIMP (Copy form Import File - Copiere în fișier de importare) autorizarea obiect necesară 339
- Comanda CPYTOSTMF (Copy form Stream File - Copiere în fișier flux) autorizarea obiect necesară 339
- Comanda CPYTOTAP (Copy to Tape - Copiere pe bandă) autorizarea obiect necesară 339
- comanda Creare comandă (CRTCMD) parametru ALWLMTUSR (permitere utilizator limitat) 67
- Comanda Creare deținător de autorizare (CRTAUTHLR) 271, 276
- Comanda Creare listă de autorizații (CRTAUTL) 271
- comanda Creare profil utilizator (CRTUSRPRF) folosind 98
- Comanda Creare profil utilizator (CRTUSRPRF) descriere 273, 274
- Comanda Creare receptor jurnal - Create Journal Receiver (CRTJRNRCV) 256
- comanda Create Authority Holder (CRTAUTHLR) 131
- Comanda Create Authorization List (CRTAUTL) 144
- comanda Create Library (CRTLIB) 136
- Comanda CRTADMDMN profiluri utilizator livrat de IBM autorizate 289
- Comanda CRTALRTBL (Create Alert Table - Creare tabel alertă) autorizarea obiect necesară 312
- Comanda CRTAUTHLR (Creare deținător de autorizare) descriere 271, 276
- comanda CRTAUTHLR (Create Authority Holder - Creare deținător de autorizare) considerente 131
profiluri utilizator autorizate livrat de IBM 289
- Comanda CRTAUTHLR (Create Authority Holder - Creare deținător de autorizare) autorizarea obiect necesară 314
- Comanda CRTAUTL (Creare listă de autorizații) descriere 271
- Comanda CRTAUTL (Create Authorization List - Creare listă de autorizare) autorizarea obiect necesară 314
folosire 144
- comanda CRTBESTMDL (Create BEST/1 Model - Creare model BEST/1) profiluri utilizator livrat de IBM autorizate 289
- Comanda CRTBESTMDL (Create Best/1-400 RPG - Creare RPG Best/1-400) autorizarea obiect necesară 407
- Comanda CRTBNDC (Create Bound C Program - Creare program C legat) autorizarea obiect necesară 376
- Comanda CRTBNDCBL (Create Bound COBOL Program - Creare program COBOL legat) autorizări obiect necesare 377
- Comanda CRTBNDCPP (Create Bound CPP Program - Creare program CPP legat) autorizarea obiect necesară 377
- Comanda CRTBNDDIR (Create Binding Directory - Creare director de legare) autorizarea obiect necesară 314
- Comanda CRTBNDRPG (Create Bound RPG Program - Creare program RPG legat) autorizări obiect necesare 377
- comanda CRTBSCF (Creare fișier bisync) auditare obiect 468
- Comanda CRTCBMOD (Create COBOL Module - Creare modul COBOL) autorizarea obiect necesară 377
- Comanda CRTCLBLPGM (Create COBOL Program - Creare program COBOL) autorizarea obiect necesară 378
- Comanda CRTCFGL (Create Configuration List - Creare listă de configurare) autorizarea obiect necesară 322
- Comanda CRTCLD (Create C Locale Description - Creare descriere C locală) autorizări obiect necesare 377
- Comanda CRTCLPGM (Create Control Language Program - Creare program limbaj control) autorizări obiect necesare 378
- comanda CRTCLS (Create Class - Creare clasă) autorizarea obiect necesară 316
profiluri utilizator livrat de IBM autorizate 289
- comanda CRTCLU autorizarea obiect necesară 318
- comanda CRTCMD (Creare comandă) parametru ALWLMTUSR (permitere utilizator limitat) 67
- comanda CRTCMD (Create Command - Creare comandă) parametrul PRDLIB (bibliotecă produs) 185
parametrul PRDLIB (bibliotecă produs) 185
riscuri de securitate 185
- Comanda CRTCMD (Create Command - Creare comandă) autorizarea obiect necesară 319
- comanda CRTCMNF (Creare fișier comunicații) auditare obiect 468
- Comanda CRTCMOD (Create C Module - Creare modul C) autorizări obiect necesare 378
- Comanda CRTCOSD (Create Class-of-Service Description - Creare descriere clasă-de-serviciu) autorizarea obiect necesară 316
- Comanda CRTCPMOD (Create Bound CPP Module - Creare modul CPP legat) autorizarea obiect necesară 378
- Comanda CRTCRQD (Create Change Request Description - Creare descriere cerere de modificare) autorizarea obiect necesară 315
- Comanda CRTCSI (Create Communications Side Information - Creare CSI) autorizarea obiect necesară 320
- Comanda CRTCTLAPPC (Create Controller Description (APPC) - Creare descriere controler (APPC)) autorizarea obiect necesară 323
- Comanda CRTCTLASC (Create Controller Description (Async) - Creare descriere controler (Async)) autorizarea obiect necesară 323

- Comanda CRTCTLBSC (Create Controller Description (BSC) - Creare descriere controler (BSC))
autorizarea obiect necesară 323
- Comanda CRTCTLFNC (Create Controller Description (Finance) - Creare descriere controler (Financiar))
autorizarea obiect necesară 323
- Comanda CRTCTLHOST (Create Controller Description (SNA Host) - Creare descriere controler (Gazdă SNA))
autorizarea obiect necesară 324
- Comanda CRTCTLLWS (Create Controller Description (Local Workstation Station) - Creare descriere controler (Stație de lucru locală))
autorizarea obiect necesară 324
- Comanda CRTCTLNET (Create Controller Description (Network) - Creare descriere controler (Rețea))
autorizarea obiect necesară 324
- Comanda CRTCTLRTL (Create Controller Description (Retail) - Creare descriere controler (Retail))
autorizarea obiect necesară 324
- Comanda CRTCTLRWS (Create Controller Description (Remote Workstation Station) - Creare descriere controler (Statie de lucru la distanță))
autorizarea obiect necesară 324
- Comanda CRTCTLTAP (Create Controller Description (Tape) - Creare descriere controler (Bandă))
autorizarea obiect necesară 324
- Comanda CRTCTLVWS (Create Controller Description (Virtual Workstation Station) - Creare descriere controler (Stație de lucru virtuală))
autorizarea obiect necesară 324
- Comanda CRTDDMF (Create Distributed Data Management File - Creare fișier de gestiune date distribuite)
autorizarea obiect necesară 340
- Comanda CRTDEVAPPC (Create Device Description (APPC) - Creare descriere dispozitiv (APPC))
autorizarea obiect necesară 327
- Comanda CRTDEVASC (Create Device Description (Async) - Creare descriere dispozitiv (Async))
autorizarea obiect necesară 327
- Comanda CRTDEVASP (Create Device Description for Auxiliary Storage Pool - Creare descriere dispozitiv pentru pool de memorie auxiliară)
autorizări obiect necesare 327
- Comanda CRTDEVBSC (Create Device Description (BSC) - Creare descriere dispozitiv (BSC))
autorizări obiect necesare 327
- Comanda CRTDEVDKT (Create Device Description (Diskette) - Creare descriere dispozitiv (Dischetă))
autorizarea obiect necesară 327
- Comanda CRTDEVDSP (Create Device Description (Display) - Creare descriere dispozitiv (Ecran))
autorizarea obiect necesară 327
- Comanda CRTDEVFNC (Create Device Description (Finance) - Creare descriere dispozitiv (Financiar))
autorizarea obiect necesară 327
- Comanda CRTDEVHOST (Create Device Description (SNA Host) - Creare descriere dispozitiv (Gazdă SNA))
autorizarea obiect necesară 327
- Comanda CRTDEVINTR (Create Device Description (Intrasystem) - Creare descriere dispozitiv (Intrasistem))
autorizarea obiect necesară 327
- Comanda CRTDEVMLB (Create Device Description (Magnetic Library) - Creare descriere dispozitiv (Magazin magnetic))
autorizarea obiect necesară 327
- Comanda CRTDEVNET (Create Device Description (Network) - Creare descriere dispozitiv (Rețea))
autorizarea obiect necesară 327
- Comanda CRTDEVNWSH (Create Device Description (Network Workstation) - Creare descriere dispozitiv (Stație de lucru rețea))
autorizarea obiect necesară 327
- Comanda CRTDEVOPT (Create Device Description (Optical) - Creare descriere dispozitiv (Optic))
autorizarea obiect necesară 327, 403
- Comanda CRTDEVPRPT (Create Device Description (Printer) - Creare descriere dispozitiv (Imprimantă))
autorizarea obiect necesară 327
- Comanda CRTDEVRTL (Create Device Description (Retail) - Creare descriere dispozitiv (Retail))
autorizarea obiect necesară 327
- Comanda CRTDEVSNPT (Create Device Description (SNPT) - Creare descriere dispozitiv (SNPT))
autorizarea obiect necesară 327
- Comanda CRTDEVSNUF (Create Device Description (SNUF) - Creare descriere dispozitiv (SNUF))
autorizarea obiect necesară 328
- Comanda CRTDEVTAP (Create Device Description (Tape) - Creare descriere dispozitiv (Bandă))
autorizarea obiect necesară 328
- comanda CRTDIR (Creare director)
auditare obiect 459
- Comanda CRTDKTF (Create Diskette File - Creare fișier dischetă)
autorizarea obiect necesară 340
- Comanda CRTDOC (Create Document - Creare document)
autorizarea obiect necesară 332
- comanda CRTDSPF (Creare fișier de afișare)
auditare obiect 468
- Comanda CRTDSPF (Create Display File - Creare fișier de afișare)
autorizarea obiect necesară 340
- Comanda CRTDSTL (Create Distribution List - Creare listă de distribuție)
autorizarea obiect necesară 331
- Comanda CRTDTAARA (Create Data Area - Creare zonă de date)
autorizarea obiect necesară 325
- Comanda CRTDTADCT (Create a Data Dictionary - Creare dicționar de date)
autorizarea obiect necesară 366
- Comanda CRTDTAQ (Create Data Queue - Creare coadă de date)
autorizarea obiect necesară 326
- comanda CRTDUPOBJ (Creare obiect duplicat)
auditare obiect 447
- Comanda CRTDUPOBJ (Create Duplicate Object - Creare obiect duplicat)
autorizări obiect necesare 304
- Comanda CRTEDTD (Create Edit Description - Creare descriere de editare)
autorizarea obiect necesară 336
- Comanda CRTFCNARA (Create Functional Area - Creare zonă funcțională)
autorizări obiect necesare 407
- Comanda CRTFACT (Create Control Form - Creare tabel de control formulare)
autorizarea obiect necesară 421
- comanda CRTFLR (Creare folder)
auditare obiect 464
- Comanda CRTFLR (Create Folder - Creare folder)
autorizarea obiect necesară 332
- Comanda CRTFNTRSC (Create Font Resources - Creare font resurse)
autorizarea obiect necesară 311
- Comanda CRTFORMDF (Create Form Definition - Creare definiție formular)
autorizarea obiect necesară 311
- Comanda CRTFTR (Create Filter - Creare filtru)
autorizarea obiect necesară 344
- comanda CRTGDF (Creare fișier de date grafice)
auditare obiect 453
- Comanda CRTGPHPKG (Create Graph Package - Creare pachet grafic)
autorizări obiect necesare 408
- Comanda CRTGSS (Create Graphics Symbol Set - Creare set de simboluri grafice)
autorizări obiect necesare 345
- Comanda CRTHSTDTA (Create Historical Data - Creare date istorice)
autorizarea obiect necesară 408
- comanda CRTICFF (Creare fișier ICF)
auditare obiect 468
- Comanda CRTICFF (Create Intersystem Communications Function File - Creare fișier de funcții de comunicații intersistem)
autorizarea obiect necesară 340
- Comanda CRTIGCDCT (Create DBCS Conversion Dictionary - Creare dicționar de conversie DBCS)
autorizarea obiect necesară 335
- comanda CRTIMGCLG
autorizarea obiect necesară 346
- comanda CRTJOB (Create Job Description - Creare descriere job)
profiluri utilizator livrat de IBM autorizate 290
- Comanda CRTJOB (Create Job Description - Creare descriere job)
autorizarea obiect necesară 371

- Comanda CRTJOBQ (Create Job Queue - Creare coadă de joburi)
autorizarea obiect necesară 371
- Comanda CRTJRN (Create Journal - Creare jurnal) 257
autorizarea obiect necesară 373
creare jurnal auditare (QAUDJRN) 257
- Comanda CRTJRNRCV (Create Journal - Creare jurnal)
receptor jurnal creare auditare (QAUDJRN) 256
- Comanda CRTJRNRCV (Create Journal Receiver - Creare receptor jurnal)
autorizarea obiect necesară 376
- comanda CRTLASREP (Create Local Abstract Syntax - Creare sitaxă abstractă locală)
profiluri utilizator autorizate livrat de IBM 290
- comanda CRTLF (Creare fișier logic)
auditare obiect 468, 502
- Comanda CRTLF (Create Logical File - Creare fișier logic)
autorizarea obiect necesară 340
- comanda CRTLIB (Create Library - Creare bibliotecă) 136
- Comanda CRTLIB (Create Library - Creare bibliotecă)
autorizarea obiect necesară 383
- Comanda CRTLINASC (Create Line Description (Async) - Creare descriere de linie (Async))
autorizări obiect necesare 388
- Comanda CRTLINBSC (Create Line Description (BSC) - Creare descriere de linie (BSC))
autorizări obiect necesare 388
- Comanda CRTLINDDI (Create Line Description (DDI Network) - Creare descriere de linie (Rețea DDI))
autorizarea obiect necesară 388
- Comanda CRTLINETH (Create Line Description (Async) - Creare descriere de linie (Ethernet))
autorizarea obiect necesară 388
- Comanda CRTLINFAX (Create Line Description (FAX) - Creare descriere de linie (FAX))
autorizări obiect necesare 388
- Comanda CRTLINFR (Create Line Description (Frame Relay Network) - Creare descriere de linie (Rețea frame relay))
autorizarea obiect necesară 388
- Comanda CRTLINS DLC (Create Line Description (SDLC) - Creare descriere de linie (SDLC))
autorizări obiect necesare 388
- Comanda CRTLINTDLC (Create Line Description (TDL) - Creare descriere de linie (TDL))
autorizări obiect necesare 388
- Comanda CRTLINTRN (Create Line Description (Token-Ring Network) - Creare descriere de linie (Rețea token ring))
autorizarea obiect necesară 388
- Comanda CRTLINWLS (Create Line Description (Wireless) - Creare descriere de linie (Comunicație fără fir))
autorizarea obiect necesară 388
- Comanda CRTLINX25 (Create Line Description (X.25) - Creare descriere de linie (X.25))
autorizări obiect necesare 388
- Comanda CRTLOCALE (Creare locale)
autorizarea obiect necesară 389
- comanda CRTMENU (Creare meniu)
parametrul PRDLIB (biblioteca produs) 185
riscuri de securitate 185
- comanda CRTMNU (Create Menu - Creare meniu)
parametrul PRDLIB (biblioteca produs) 185
riscuri de securitate 185
- Comanda CRTMNU (Create Menu - Creare meniu)
autorizarea obiect necesară 390
- Comanda CRTMODD (Create Mode Description - Creare descriere mod)
autorizarea obiect necesară 394
- comanda CRTMSDF (Creare fișier dispozitiv mixt)
auditare obiect 468
- Comanda CRTMSGF (Create Message File - Creare fișier mesaj)
autorizarea obiect necesară 392
- Comanda CRTMSGFMNU (Creare meniu fișier de mesaje)
autorizări obiect necesare 434
- Comanda CRTMSGQ (Create Message Queue - Creare coadă de mesaje)
autorizarea obiect necesară 393
- Comanda CRTNODL (Create Node List - Creare listă de noduri)
autorizarea obiect necesară 399
- Comanda CRTNTBD (Create NetBIOS Description - Creare descriere NetBIOS)
autorizarea obiect necesară 395
- Comanda CRTNWIFR (Create Network Interface Description (Frame Relay Network) - Creare descriere interfață de rețea (Rețea frame relay))
autorizarea obiect necesară 397
- Comanda CRTNWSALS (Create Network Server Alias - Creare alias server de rețea)
autorizări obiect necesare 398
- Comanda CRTNWS CFG (Create Network Server Alias - Creare alias server de rețea)
autorizarea obiect necesară 399
profiluri utilizator livrat de IBM autorizate 290
- Comanda CRTNWS D (Create Network Server Description - Creare descriere server de rețea)
autorizarea obiect necesară 399
- Comanda CRTNWSSTG (Create Network Server Storage Space - Creare spațiu de stocare server de rețea)
autorizarea obiect necesară 397
- Comanda CRTOUTQ (Creare coadă ieșire)
autorizarea obiect necesară 405
- comanda CRTOUTQ (Create Output Queue - Creare coada de ieșire) 188
- comanda CRTOUTQ (Create Output Queue - Creare coadă de ieșire) 186
exemple 188
folosire 186
- Comanda CRTOVL (Create Overlay - Creare suprapunere)
autorizarea obiect necesară 311
- Comanda CRTPAGDFN (Create Page Definition - Creare definiție pagină)
autorizarea obiect necesară 311
- Comanda CRTPAGSEG (Create Page Segment - Creare segment de pagină)
autorizarea obiect necesară 311
- Comanda CRTPDG (Creare grup descriptor de tipărire)
autorizarea obiect necesară 411
- comanda CRTPEXDTA (Create Performance Explorer Data - Creare fapte Performance Explorer)
profiluri utilizator autorizate livrat de IBM 290
- comanda CRTPF (Creare fișier fizic)
auditare obiect 468
- Comanda CRTPF (Create Physical File - Creare fișier fizic)
autorizarea obiect necesară 340
- comanda CRTPFRDTA (Create Performance Data - Creare date de performanță)
autorizarea obiect necesară 408
- comanda CRTPGM (Creare program)
auditare obiect 451
- comanda CRTPGM (Creare Program)
auditare obiect 481, 487, 498
- Comanda CRTPNLGRP (Create Panel Group - Creare grup de panouri)
autorizarea obiect necesară 391
- comanda CRTPRTF (Creare fișier imprimantă)
auditare obiect 468
- Comanda CRTPRTF (Create Printer File - Creare fișier imprimantă)
autorizarea obiect necesară 341
- Comanda CRTPSFCFG (Creare configurare facilități servicii de tipărire)
autorizări obiect necesare 411
- comanda CRTQMFORM (Creare formular Query Management)
auditare obiect 489
- Comanda CRTQMFORM (Creare formular Query Management)
autorizări obiect necesare 416
- comanda CRTQMQR (Creare cerere Query Management)
auditare obiect 490
- Comanda CRTQSTDB (Creare bază de date Întrebări și răspunsuri)
autorizarea obiect necesară 417
profiluri utilizator livrat de IBM autorizate 290
- comanda CRTQSTL (Create Question-and-Answer Load - Creare încărcare întrebare-răspuns)
profiluri utilizator autorizate livrat de IBM 290
- Comanda CRTRJEBS CF (Creare fișier RJE BSC)
autorizarea obiect necesară 421

- Comanda CRTRJECFG (Creare configurație)
autorizarea obiect necesară 421
- Comanda CRTRJECMNF (Creare fișier de
comunicații RJE)
autorizări obiect necesare 421
- Comanda CRTRPGMOD (Creare RPG
Module - Creare modul RPG)
autorizarea obiect necesară 378
- Comanda CRTRPGPGM (Creare RPG/400
Program - Creare program RPG/400)
autorizarea obiect necesară 379
- Comanda CRTRPTPGM (Creare Auto Report
Program - Creare program raport auto)
autorizări obiect necesare 379
- Comanda CRTS36CBL (Create System/36
COBOL - Creare COBOL System/36)
autorizarea obiect necesară 379
- Comanda CRTS36DSPF (Creare fișier de
afișare System/36)
autorizări obiect necesare 341, 434
- Comanda CRTS36MNU (Creare meniu
System/36)
autorizarea obiect necesară 391, 434
- Comanda CRTS36MSGF (Creare fișier de
mesaje System/36)
autorizări obiect necesare 435
- Comanda CRTS36RPG (Create System/36
RPG - Creare RPG System/36)
autorizarea obiect necesară 379
- Comanda CRTS36RPGR (Create System/36
RPG - Creare RPGR System/36)
autorizarea obiect necesară 379
- Comanda CRTS36RPT (Create System/36
Auto Report - Creare raport auto System/36)
autorizări obiect necesare 379
- Comanda CRTSAVF (Create Save File -
Creare fișier de salvare)
autorizarea obiect necesară 341
- comanda CRTSBSD (Creare descriere
subsistem)
profiluri utilizator livrat de IBM
autorizate 290
- Comanda CRTSBSD (Create Subsystem
Description - Creare descriere subsistem)
autorizări obiect necesare 432
- Comanda CRTSCHIDX (Create Search Index
- Creare index de căutare)
autorizarea obiect necesară 366
- comanda CRTSPADCT (Creare dicționar de
adăugare silabisire)
auditare obiect 496
- Comanda CRTSPADCT (Create Spelling Aid
Dictionary - Creare dicționar ajutător pentru
corectare ortografică)
autorizări obiect necesare 428
- Comanda CRTSQLCBL (Create Structured
Query Language COBOL - Creare COBOL
limbaj interogare structurat)
autorizarea obiect necesară 380
- Comanda CRTSQLCBLI (Create Structured
Query Language ILE COBOL Object -
Creare obiect COBOL ILE limbaj interogare
structurat)
autorizarea obiect necesară 380
- Comanda CRTSQLCI (Create Structured
Query Language ILE C Object - Creare
obiect C ILE limbaj interogare structurat)
autorizarea obiect necesară 379
- Comanda CRTSQLCPPI (Create SQL ILE
C++ Object - Creare obiect C++ ILE SQL)
autorizări obiect necesare 380
- Comanda CRTSQLFTN (Create Structured
Query Language FORTRAN - Creare
interogare structurată limbaj FORTRAN)
autorizarea obiect necesară 380
- Comanda CRTSQLPKG (Create Structured
Query Language Package - Creare pachet în
limbaj de interogare structurat)
autorizarea obiect necesară 405
- Comanda CRTSQLPLI (Create Structured
Query Language PL/I - Creare PL/I limbaj
interogare structurat)
autorizarea obiect necesară 381
- Comanda CRTSQLRPG (Create Structured
Query Language RPG - Creare RPG
interogare structurată limbaj)
autorizarea obiect necesară 381
- Comanda CRTSQLRPGI (Create Structured
Query Language ILE RPG Object - Creare
obiect RPG ILE limbaj interogare structurat)
autorizarea obiect necesară 381
- Comanda CRTSRCPF (Create Source Physical
File - Creare fișier fizic sursă)
autorizarea obiect necesară 341
- comanda CRTSRVPGM (Creare program
service)
auditare obiect 451, 481, 498
- Comanda CRTSRVPGM (Creare program
service)
autorizarea obiect necesară 413
- Comanda CRTSSND (Creare descriere
sesiune)
autorizări obiect necesare 421
- Comanda CRTTAPF (Create Tape File -
Creare fișier bandă)
autorizarea obiect necesară 341
- Comanda CRTTBL (Creare tabelă)
autorizarea obiect necesară 436
- Comanda CRTTIMZON 438
- comanda CRTUDFS (Create User-Defined
File System - Creare sistem de fișiere definit
de utilizator)
profiluri utilizator autorizate livrat de
IBM 290
- Comanda CRTUDFS (Create User-Defined
File System - Creare sistem de fișiere definit
de utilizator)
autorizarea obiect necesară 439
- comanda CRTUSRPRF (Creare profil
utilizator)
folosind 98
- Comanda CRTUSRPRF (Creare profil
utilizator)
descriere 273, 274
- Comanda CRTUSRPRF (Create User Profile -
Creare profil utilizator)
autorizarea obiect necesară 441
- comanda CRTVLDL (Create Validation List -
Creare listă de validare)
profiluri utilizator livrat de IBM
autorizate 290
- Comanda CRTVLDL (Create Validation List -
Creare listă de validare)
autorizarea obiect necesară 443
- Comanda CRTWSCST (Create Workstation
Customizing Object - Creare obiect
personalizare stație de lucru)
autorizarea obiect necesară 443
- comanda CVTBASSTR (Convert BASIC
Stream Files - Convertire fișiere flux
BASIC)
profiluri utilizator autorizate livrat de
IBM 290
- Comanda CVTBASSTR (Convert BASIC
Stream Files - Convertire fișiere flux
BASIC)
autorizări obiect necesare 393
- comanda CVTBASUNF (Convert BASIC
Unformatted Files - Convertire fișiere
neformatate BASIC)
autorizarea obiect necesară 393
- Comanda CVTBASUNF (Convert BASIC
Unformatted Files - Convertire fișiere
neformatate BASIC)
profiluri utilizator autorizate livrat de
IBM 290
- comanda CVTBGUDTA (Convert BGU Data -
Convertire date BGU)
profiluri utilizator livrat de IBM
autorizate 290
- Comanda CVTBGUDTA (Convert BGU Data
- Convertire date BGU)
autorizări obiect necesare 393
- Comanda CVTCLSRC (Convertire sursă CL)
autorizarea obiect necesară 413
- Comanda CVTDIR (Convert Directory -
Convertire director)
autorizarea obiect necesară 351
- Comanda CVTEDU (Convert Education -
Convertire educație)
autorizarea obiect necesară 400
- Comanda CVTIPSIFC (Convert IP over SNA
Interface - Convertire IP pe interfață SNA)
autorizarea obiect necesară 312
- Comanda CVTIPSLOC (Convert IP over SNA
Location - Convertire IP pe locație SNA)
autorizarea obiect necesară 312
- Comanda CVTOPTBKU (Convert Optical
Backup - Convertire salvare de rezervă
optică)
autorizarea obiect necesară 403
- Comanda CVTPFRDTA (Convert
Performance Data - Convertire date de
performanță)
autorizări obiect necesare 408
- Comanda CVTPFRTHD (Convert
Performance Thread Data - Convertire date
fir de execuție de performanță)
autorizări obiect necesare 408
- Comanda CVTRJEDTA (Convertire date RJE)
autorizarea obiect necesară 422
- Comanda CVTRPGSRC (Convert RPG Source
- Convertire sursă RPG)
autorizarea obiect necesară 381

Comanda DLTDADCT (Delete Data Dictionary - Ștergere dicționar de date) autorizarea obiect necesară 366

Comanda DLTDATAQ (Delete Data Queue - Ștergere coadă de date) autorizarea obiect necesară 326

Comanda DLTEDTD (Delete Edit Description - Ștergere descriere de editare) autorizarea obiect necesară 336

Comanda DLTF (Delete File - Ștergere fișier) autorizarea obiect necesară 341

Comanda DLTFCNARA (Delete Functional Area - Ștergere zonă funcțională) autorizarea obiect necesară 408

Comanda DLTFCT (Ștergere tabel de control formulare) autorizarea obiect necesară 422

Comanda DLTFNTRSC (Delete Font Resources - Ștergere font resurse) autorizarea obiect necesară 311

Comanda DLTFORMDF (Delete Form Definition - Ștergere definiție formular) autorizarea obiect necesară 311

Comanda DLTFTR (Delete Filter - Ștergere filtru) autorizarea obiect necesară 344

Comanda DLTGPHFMT (Delete Graph Format - Ștergere format grafic) autorizarea obiect necesară 408

Comanda DLTGPHPKG (Delete Graph Package - Ștergere pachet grafic) autorizarea obiect necesară 408

Comanda DLTGSS (Delete Graphics Symbol Set - Ștergere set de simboluri grafice) autorizarea obiect necesară 345

Comanda DLTHSTDTA (Delete Historical Data - Ștergere date istorice) autorizarea obiect necesară 408

Comanda DLTIGCDCT (Delete DBCS Conversion Dictionary - Ștergere dicționar de conversie DBCS) autorizarea obiect necesară 335

Comanda DLTIGCSRT (Delete IGC Sort - Ștergere sortare IGC) autorizarea obiect necesară 335

Comanda DLTIGCTBL (Delete DBCS Font Table - Ștergere tabel font DBCS) autorizarea obiect necesară 335

comanda DLTIMGCLG autorizarea obiect necesară 346

Comanda DLTI PXD 366

Comanda DLTIJOB (Delete Job Description - Ștergere descriere de job) autorizarea obiect necesară 371

Comanda DLTIJOBQ (Delete Job Queue - Ștergere coadă de joburi) autorizarea obiect necesară 371

Comanda DLTIJRN (Delete Journal - Ștergere jurnal) autorizarea obiect necesară 373

Comanda DLTIJRNRCV (Delete Journal Receiver - Ștergere receptor jurnal) 260 autorizări obiect necesare 376 oprire funcție auditare 260

Comanda DLTLIB (Delete Library - Ștergere bibliotecă) autorizarea obiect necesară 383

comanda DLTLICPGM (Delete Licensed Program - Ștergere program cu licență) profiluri utilizator livrat de IBM autorizate 291

Comanda DLTLICPGM (Delete Licensed Program - Ștergere program cu licență) autorizarea obiect necesară 387

Comanda DLTLIND (Delete Line Description - Ștergere descriere de linie) autorizarea obiect necesară 388

Comanda DLTLOCALE (Creare locală) autorizarea obiect necesară 389

Comanda DLTMNU (Delete Menu - Ștergere meniu) autorizarea obiect necesară 391

Comanda DLTMOD (Delete Module - Ștergere modul) autorizarea obiect necesară 394

Comanda DLTMODD (Delete Mode Description - Ștergere descriere mod) autorizarea obiect necesară 394

Comanda DLTMSGF (Delete Message File - Ștergere fișier mesaj) autorizarea obiect necesară 392

Comanda DLTMSGQ (Delete Message Queue - Ștergere coadă de mesaje) autorizarea obiect necesară 393

Comanda DLTNETF (Delete Network File - Ștergere fișier rețea) autorizarea obiect necesară 395

Comanda DLTNODL (Delete Node List - Ștergere listă de noduri) autorizarea obiect necesară 399

Comanda DLTNTBD (Delete NetBIOS Description - Ștergere descriere NetBIOS) autorizarea obiect necesară 395

Comanda DLTNWID (Delete Network Interface Description - Ștergere descriere interfață de rețea) autorizarea obiect necesară 397

Comanda DLTNWSALS (Delete Network Server Alias - Ștergere alias server de rețea) autorizarea obiect necesară 398

Comanda DLTNWSCFG autorizarea obiect necesară 399 profiluri utilizator livrat de IBM autorizate 291

Comanda DLTNWSD (Delete Network Server Description - Ștergere descriere server de rețea) autorizarea obiect necesară 399

Comanda DLTNWSSTG (Delete Network Server Storage Space - Ștergere spațiu de stocare server de rețea) autorizarea obiect necesară 397

Comanda DLTOUQ (Delete Output Queue - Ștergere coadă de ieșire) autorizarea obiect necesară 405

Comanda DLTOVL (Delete Overlay - Ștergere suprapunere) autorizarea obiect necesară 311

Comanda DLTPAGDFN (Delete Page Definition - Ștergere definiție pagină) autorizarea obiect necesară 311

Comanda DLTPAGSEG (Delete Page Segment - Ștergere segment de pagină) autorizarea obiect necesară 311

Comanda DLTPDG (Ștergere grup descriptor tipărire) autorizarea obiect necesară 411

Comanda DLTPXD (Delete Performance Explorer Data - Ștergere date explorare performanță) autorizarea obiect necesară 408

Comanda DLTPFRDTA (Delete Performance Data - Ștergere date de performanță) autorizarea obiect necesară 408

Comanda DLTPGM (Ștergere program) autorizarea obiect necesară 413

Comanda DLTPNLGRP (Delete Panel Group - Ștergere grup de panouri) autorizarea obiect necesară 391

comanda DLTPRB (Delete Problem - Ștergere problemă) profiluri utilizator livrat de IBM autorizate 291

Comanda DLTPRB (Delete Problem - Ștergere problemă) autorizarea obiect necesară 412

Comanda DLTPSFCFG (Ștergere configurație facilități servicii de tipărire) autorizări obiect necesare 411

comanda DLTPTF (Delete PTF - Ștergere PTF) profiluri utilizator livrat de IBM autorizate 291

Comanda DLTPTF (Delete PTF - Ștergere PTF) autorizarea obiect necesară 424

Comanda DLTMFORM (Ștergere formular Query Management) autorizarea obiect necesară 416

comanda DLTQRY (Ștergere cerere) auditare obiect 491

Comanda DLTQRY (Ștergere interogare) autorizarea obiect necesară 416

comanda DLTQST (Delete Question - Ștergere întrebare) profiluri utilizator livrat de IBM autorizate 291

comanda DLTQSTDB (Delete Question-and-Answer Database - Ștergere bază de date întrebare-răspuns) profiluri utilizator autorizate livrat de IBM 291

Comanda DLTRJECFG (Ștergere configurare RJE) autorizări obiect necesare 422

comanda DLTRMTPTF (Delete Remote PTF - Ștergere PTF la distanță) profiluri utilizator livrat de IBM autorizate 291

Comanda DLTSBSD (Ștergere descriere subsistem) autorizarea obiect necesară 432

Comanda DLTSCHIDX (Delete Search Index - Ștergere index de căutare) autorizarea obiect necesară 366

comanda DLTSHF (Ștergere raft de cărți) auditare obiect 464

comanda DLTSMGOBJ (Delete Systems Management Object - Ștergere obiect gestiune sisteme)
 profiluri utilizator autorizate livrat de IBM 291

Comanda DLTSPADCT (Ștergere dicționar ajutător pentru corectare ortografică)
 autorizarea obiect necesară 428

Comanda DLTSPLF (Delete Spooled File - Ștergere fișier spool)
 autorizarea obiect necesară 430

comanda DLTSPLF (Ștergere fișier spool)
 auditare acțiune 497
 auditare obiect 485

Comanda DLTSQPKG (Delete Structured Query Language Package - Ștergere pachet în limbaj de interogare structurat)
 autorizări obiect necesare 405

Comanda DLTSRVPGM (Ștergere program service)
 autorizarea obiect necesară 413

Comanda DLTSND (Ștergere descriere sesiune)
 autorizarea obiect necesară 422

Comanda DLTTBL (Ștergere tabelă)
 autorizarea obiect necesară 436

Comanda DLTTIMZON 438

Comanda DLTTTRC (Ștergere urmă)
 autorizarea obiect necesară 425

comanda DLTUDFS (Delete User-Defined File System - Ștergere sistem de fișiere definit de utilizator)
 profiluri utilizator autorizate livrat de IBM 291

Comanda DLTUDFS (Delete User-Defined File System - Ștergere sistem de fișiere definit de utilizator)
 autorizări obiect necesare 439

Comanda DLTUSRIDX (Ștergere index utilizator)
 autorizarea obiect necesară 439

Comanda DLTUSRPRF (Delete User Profile - Ștergere profil utilizator)
 autorizarea obiect necesară 441

comanda DLTUSRPRF (Ștergere profil utilizator)
 auditare obiect 503
 exemplu 102

Comanda DLTUSRPRF (Ștergere profil utilizator)
 descriere 274
 drept de proprietate obiect 122

Comanda DLTUSRQ (Ștergere coadă utilizator)
 autorizarea obiect necesară 439

Comanda DLTUSRSPC (Ștergere spațiu utilizator)
 autorizarea obiect necesară 439

Comanda DLTUSRTRC (Delete User Trace - Ștergere urmă utilizator)
 autorizarea obiect necesară 368

comanda DLTVLDL (Delete Validation List - Ștergere listă de validare)
 profiluri utilizator livrat de IBM autorizate 291

Comanda DLTVLDL (Delete Validation List - Ștergere listă de validare)
 autorizarea obiect necesară 443

Comanda DLTWNTSVR
 profiluri utilizator livrat de IBM autorizate 291

Comanda DLTWSCST (Delete Workstation Customizing Object - Ștergere obiect personalizare stație de lucru)
 autorizări obiect necesare 443

Comanda DLYJOB (Delay Job - Întârziere job)
 autorizarea obiect necesară 368

comanda DMPCLPGM (Abandon program CL)
 auditare obiect 488

Comanda DMPCLPGM (Dump program CL)
 autorizarea obiect necesară 413

comanda DMPDLO (Abandon obiect bibliotecă documente)
 auditare obiect 462

comanda DMPDLO (Dump Document Library Object - Abandonare obiect de bibliotecă de documente)
 profiluri utilizator autorizate livrat de IBM 291

Comanda DMPDLO (Dump Document Library Object - Abandonare obiect de bibliotecă de documente)
 autorizarea obiect necesară 332

comanda DMPJOB (Abandonare job)
 profiluri utilizator livrat de IBM autorizate 291

comanda DMPJOB (Dump Job - Abandonare job)
 autorizarea obiect necesară 425

comanda DMPJOBINT (Abandonare job intern)
 profiluri utilizator livrat de IBM autorizate 291

comanda DMPJOBINT (Dump Job Internal - Abandonare job intern)
 autorizarea obiect necesară 425

comanda DMPOBJ (Abandon obiect)
 auditare obiect 447

Comanda DMPOBJ (Dump Object - Abandon obiect)
 autorizarea obiect necesară 304
 profiluri utilizator livrat de IBM autorizate 291

comanda DMPYSOJB (Abandon obiect sistem)
 auditare obiect 447

comanda DMPYSOJB (Dump System Object - Abandonare obiect sistem)
 profiluri utilizator livrat de IBM autorizate 291

Comanda DMPYSOJB (Dump System Object - Abandonare obiect sistem)
 autorizarea obiect necesară 304

Comanda DMPPTAP (Dump Tape - Dump bandă)
 autorizarea obiect necesară 390

comanda DMPTRC (Dump Trace - Abandonare urmărire)
 autorizarea obiect necesară 408

Comanda DMPTRC (Dump Trace - Dump urmă)
 profiluri utilizator livrat de IBM autorizate 291

Comanda DMPUSRTRC (Dump User Trace - Dump urmă utilizator)
 autorizarea obiect necesară 368

Comanda DSCJOB (Disconnect Job - Deconectare job)
 autorizarea obiect necesară 368

comanda DSPACC (Afișare cod acces)
 auditare obiect 465

Comanda DSPACC (Display Access Code - Afișare cod acces)
 autorizări obiect necesare 400

Comanda DSPACCAUT (Display Access Code Authority - Afișare autorizare cod acces)
 autorizarea obiect necesară 400

Comanda DSPACTPJ (Display Active Prestart Jobs - Afișare joburi prerestart active)
 autorizarea obiect necesară 368

Comanda DSPACTPREF (Afișare listă de profiluri active)
 descriere 617

Comanda DSPACTPREF (Afișare listă profiluri active)
 autorizarea obiect necesară 441

Comanda DSPACTSCD (Afișare planificator de activare)
 autorizarea obiect necesară 441
 descriere 617

Comanda DSPASPSTS
 autorizarea obiect necesară 328

Comanda DSPAUDJRNE (Afișare intrări jurnal de auditare)
 descriere 277, 621

Comanda DSPAUDJRNE (Display Audit Journal Entries - Afișare intrări jurnal de auditare)
 autorizarea obiect necesară 373

comanda DSPAUT (Afișare autorizare)
 auditare obiect 460, 495, 500

Comanda DSPAUT (Afișare autorizare)
 descriere 272

Comanda DSPAUT (Display Authority - Afișare autorizare)
 autorizarea obiect necesară 351

comanda DSPAUTHLR (Afișare deținător de autorizare)
 auditare obiect 451

Comanda DSPAUTHLR (Afișare deținător de autorizare)
 descriere 271

comanda DSPAUTHLR (Display Authority Holder - Afișare deținător de autorizare)
 folosirea 131

Comanda DSPAUTHLR (Display Authority Holder - Afișare deținător de autorizare)
 autorizarea obiect necesară 314

comanda DSPAUTL (Afișare listă de autorizații)
 auditare obiect 451

Comanda DSPAUTL (Afișare listă de autorizații)
 descriere 271

Comanda DSPAUTL (Display Authorization List - Afișare listă de autorizații)
 autorizări obiect necesare 314

comanda DSPAUTLDLO (Afișare obiecte bibliotecă de documente listă de autorizații)
 auditare obiect 451

Comanda DSPAUTLDLO (Afișare obiecte de bibliotecă de documente pentru listă de autorizații)
 autorizarea obiect necesară 332
 descriere 275

Comanda DSPAUTLDLO (Display Authorization List Document Library Objects - Afișare obiecte de bibliotecă de documente pentru listă de autorizații)
 autorizarea obiect necesară 314

comanda DSPAUTLOBJ (Afișare obiecte din lista de autorizații)
 auditare obiect 451

Comanda DSPAUTLOBJ (Afișare obiecte listă de autorizații)
 descriere 271

Comanda DSPAUTLOBJ (Display Authorization List Objects - Afișare obiecte din lista de autorizare)
 autorizarea obiect necesară 314
 folosire 146

comanda DSPAUTUSR (Afișare utilizatori autorizați)
 exemplu 104

Comanda DSPAUTUSR (Afișare utilizatori autorizați)
 descriere 274

comanda DSPAUTUSR (Display Authorized Users - Afișare utilizatori autorizați)
 auditare 267

Comanda DSPAUTUSR (Display Authorized Users - Afișare utilizatori autorizați)
 auditare 267
 autorizarea obiect necesară 441

Comanda DSPBCKSTS (Display Backup Status - Afișare stare salvare de rezervă)
 autorizarea obiect necesară 400

Comanda DSPBCKUP (Display Backup Options - Afișare opțiuni salvare de rezervă)
 autorizarea obiect necesară 401

Comanda DSPBCKUPL (Display Backup List - Afișare listă salvare de rezervă)
 autorizarea obiect necesară 401

Comanda DSPBNDDIR (Display Binding Directory - Afișare director de legare)
 autorizarea obiect necesară 315

comanda DSPBNDDIRE (Afișare director legături)
 auditare obiect 452

comanda DSPCFGL (Afișare listă de configurație)
 auditare obiect 452

Comanda DSPCFGL (Display Configuration List - Afișare listă de configurare)
 autorizarea obiect necesară 322

comanda DSPCHT (Afișare diagramă)
 auditare obiect 452

Comanda DSPCHT (Display Chart - Afișare diagramă)
 autorizarea obiect necesară 315

comanda DSPCLS (Afișare clasă)
 auditare obiect 454

Comanda DSPCLS (Display Class - Afișare clasă)
 autorizarea obiect necesară 316

comanda DSPCMD (Afișare comandă)
 auditare obiect 454

Comanda DSPCMD (Display Command - Afișare comandă)
 autorizarea obiect necesară 319

comanda DSPCNL (Afișare listă de conexiuni)
 auditare obiect 455

Comanda DSPCNL (Display Connection List - Afișare listă de conexiuni)
 autorizarea obiect necesară 322

Comanda DSPCNNSTS (Display Connection Status - Afișare stare conexiune)
 autorizarea obiect necesară 328

comanda DSPCOSD (Afișare descriere clasă de serviciu)
 auditare obiect 456

Comanda DSPCOSD (Display Class-of-Service Description - Afișare descriere clasă-de-serviciu)
 autorizarea obiect necesară 316

comanda DSPPCST (Afișare constrângeri de verificare în așteptare)
 auditare obiect 471

Comanda DSPPCST (Display Check Pending Constraint - Afișare constrângere de verificare în așteptare)
 autorizarea obiect necesară 341

comanda DSPCSI (Afișare informații parte comunicații)
 auditare obiect 456

Comanda DSPCSI (Display Communications Side Information - Afișare CSI)
 autorizări obiect necesare 321

comanda DSPCSPOBJ (Afișare obiect CSP/AE)
 auditare obiect 456, 488

comanda DSPCTLD (Afișare descriere controler)
 auditare obiect 457

Comanda DSPCTLD (Display Controller Description - Afișare descriere controler)
 autorizarea obiect necesară 324

comanda DSPCURDIR (Afișare director curent)
 auditare obiect 458

Comanda DSPCURDIR (Display Current Directory - Afișare director curent)
 autorizări obiect necesare 352

Comanda DSPDBG (Afișare depanare)
 autorizarea obiect necesară 413

Comanda DSPDBGWCH (Afișare ferestre depanare)
 autorizarea obiect necesară 413

comanda DSPDBR (Afișare relații bază de date)
 auditare obiect 471

Comanda DSPDBR (Display Database Relations - Afișare relații bază de date)
 autorizări obiect necesare 341

Comanda DSPDDMF (Display Distributed Data Management File - Afișare fișier de gestiune date distribuite)
 autorizări obiect necesare 341

comanda DSPDEVD (Afișare descriere dispozitiv)
 auditare obiect 458

Comanda DSPDEVD (Display Device Description - Afișare descriere dispozitiv)
 autorizarea obiect necesară 328

Comanda DSPDIRE (Display Directory Entry - Afișare intrare director)
 autorizarea obiect necesară 329

Comanda DSPDKT (Display Diskette - Afișare dischetă)
 autorizarea obiect necesară 390

comanda DSPDLOAD (Afișare auditare obiect bibliotecă documente)
 auditare obiect 462

Comanda DSPDLOAD (Afișare auditare obiect de bibliotecă de documente)
 descriere 275

Comanda DSPDLOAD (Display Document Library Object Auditing - Afișare auditare obiect bibliotecă de documente)
 autorizări obiect necesare 332

Comanda DSPDLOAD (Display Document Library Object Auditing - Afișare auditare obiect bibliotecă document)
 utilizare 254

Comanda DSPDLOAD (Afișare autorizare obiect de bibliotecă de documente)
 descriere 275

comanda DSPDLOAD (Afișare autorizare obiect de bibliotecă documente)
 auditare obiect 462

Comanda DSPDLOAD (Display Document Library Object Authority - Afișare autorizare obiect bibliotecă de documente)
 autorizări obiect necesare 332

Comanda DSPDLONAM (Display Document Library Object Name - Afișare nume obiect bibliotecă document)
 autorizări obiect necesare 332

comanda DSPDOC (Afișare document)
 auditare obiect 462

Comanda DSPDOC (Display Document - Afișare document)
 autorizarea obiect necesară 332

Comanda DSPDSTL (Display Distribution List - Afișare listă de distribuție)
 autorizarea obiect necesară 331

comanda DSPDSTLOG (Display Distribution Log - Afișare istoric de distribuție)
 profiluri utilizator livrat de IBM
 autorizate 291

Comanda DSPDSTLOG (Display Distribution Log - Afișare istoric distribuție)
 autorizări obiect necesare 331

Comanda DSPDSTSRV (Display Distribution Services - Afișare servicii de distribuție)
 autorizarea obiect necesară 331

Comanda DSPDTA (Display Data - Afișare date)
 autorizarea obiect necesară 341

comanda DSPDTAARA (Afișare zonă de date)
 auditare obiect 466

Comanda DSPDTAARA (Display Data Area - Afişare zonă de date)
 autorizarea obiect necesară 325

Comanda DSPDTADCT (Display Data Dictionary - Afişare dicţionar de date)
 autorizarea obiect necesară 366

comanda DSPEDTD (Afişare descriere editare)
 auditare obiect 467

Comanda DSPEDTD (Display Edit Description - Afişare descriere de editare)
 autorizarea obiect necesară 336

Comanda DSPEWCBCDE (Display Extended Wireless Controller Bar Code Entry - Afişare intrare cod de bare controler de comunicaţie fără fir extinsă)
 autorizarea obiect necesară 336

Comanda DSPEWCM (Display Extended Wireless Controller Member - Afişare membru controler de comunicaţie fără fir extinsă)
 autorizări obiect necesare 336

Comanda DSPEWCPTCE (Display Extended Wireless Controller PTC Code Entry - Afişare intrare PTC controler de comunicaţie fără fir extinsă)
 autorizarea obiect necesară 336

Comanda DSPEWLM (Display Extended Wireless Line Member - Afişare membru linie de comunicaţie fără fir extinsă)
 autorizarea obiect necesară 336

Comanda DSPEXPSCD (Afişare planificator de expirare)
 autorizarea obiect necesară 441
 descriere 617

Comanda DSPF (Display File - Afişare fişier) 352

comanda DSPFD (Afişare descriere fişier)
 auditare obiect 471

Comanda DSPFD (Display File Description - Afişare descriere fişier)
 autorizări obiect necesare 341

comanda DSPFFD (Afişare descriere câmp fişier)
 auditare obiect 471

Comanda DSPFFD (Display File Field Description - Afişare descriere câmp fişier)
 autorizări obiect necesare 341

Comanda DSPFLR (Display Folder - Afişare folder)
 autorizarea obiect necesară 332

Comanda DSPFNTRSCA (Display Font Resource - Afişare font resurse)
 autorizarea obiect necesară 311

Comanda DSPGDF (Display Graphics Data File - Afişare fişier de date grafică)
 autorizarea obiect necesară 315

Comanda DSPHDWRSC (Afişare resurse hardware)
 autorizarea obiect necesară 419

comanda DSPHLPDOC (Afişare document ajutor)
 auditare obiect 462

Comanda DSPHSTGPH (Display Historical Graph - Afişare grup istoric)
 autorizarea obiect necesară 409

comanda DSPIGCDCT (Afişare dicţionar conversie DBCS)
 auditare obiect 473

Comanda DSPIGCDCT (Display DBCS Conversion Dictionary - Afişare dicţionar de conversie DBCS)
 autorizarea obiect necesară 335

Comanda DSPIPXD 366

Comanda DSPJOB (Display Job - Afişare job)
 autorizarea obiect necesară 368

comanda DSPJOB (Afişare descriere job)
 auditare obiect 474

Comanda DSPJOB (Display Job Description - Afişare descriere de job) 232
 utilizare 232

Comanda DSPJOB (Display Job Description - Afişare descriere job)
 autorizarea obiect necesară 371

Comanda DSPJOB (Display Object Description - Afişare descriere obiect)
 folosire fişier de ieşire 268
 utilizare 254

Comanda DSPJOBLOG (Display Job Log - Afişare istoric job)
 autorizarea obiect necesară 368

comanda DSPJRN (Afişare jurnal)
 auditare obiect 476, 477

comanda DSPJRN (Display Journal - Afişare jurnal)
 afişare jurnal QAUDJRN (audit) 234
 auditare activitate fişier 266
 creare fişier de ieşire 262
 exemplu de jurnal de auditare (QAUDJRN) 260, 261

Comanda DSPJRN (Display Journal - Afişare jurnal)
 auditare activitate fişier 209
 autorizări obiect necesare 374

Comanda DSPJRN (Display Jurnal - Afişare jurnal)
 afişare jurnal QAUDJRN (audit) 234
 auditare activitate fişier 266
 creare fişier de ieşire 262
 exemplu de jurnal de auditare (QAUDJRN) 260, 261

comanda DSPJRNRCVA (Afişare atribute receptor jurnal)
 auditare obiect 477

Comanda DSPJRNRCVA (Display Journal Receiver Attributes - Afişare atribute receptor jurnal)
 autorizarea obiect necesară 376

Comanda DSPLANADPP (Afişare profil adaptor LAN)
 autorizarea obiect necesară 389

Comanda DSPLANSTS (Afişare stare LAN)
 autorizarea obiect necesară 389

comanda DSPLIB (Afişare bibliotecă)
 auditare obiect 477

Comanda DSPLIB (Display Library - Afişare bibliotecă) 268
 autorizarea obiect necesară 383
 utilizare 268

Comanda DSPLIB (Display Library Description - Afişare descriere bibliotecă)
 autorizarea obiect necesară 383
 Parametrul CRTAUT 137

Comanda DSPLICENSE (Display License Key - Afişare cheie de licenţă)
 autorizarea obiect necesară 386

comanda DSPLIND (Afişare descriere de linie)
 auditare obiect 479

Comanda DSPLIND (Display Line Description - Afişare descriere de linie)
 autorizarea obiect necesară 388

comanda DSPLNK (Afişare legături)
 auditare obiect 458, 494, 499, 501

comanda DSPLOG (Afişare istoric)
 auditare obiect 482

Comanda DSPLOG (Display Log - Afişare istoric)
 autorizarea obiect necesară 393

comanda DSPMFSINF (Display Mounted File System Information - Afişare informaţii sistem de fişiere montat)
 profiluri utilizator livrat de IBM autorizate 291

Comanda DSPMFSINF (Display Mounted File System Information - Afişare informaţii sistem de fişiere montat)
 autorizarea obiect necesară 396

comanda DSPMGDSYSA (Display Managed System Attributes - Afişare atribute de sistem gestionate)
 profiluri utilizator livrat de IBM autorizate 291

comanda DSPMNUA (Afişare atribute meniu)
 auditare obiect 480

Comanda DSPMNUA (Display Menu Attributes - Afişare atribute meniu)
 autorizarea obiect necesară 391

comanda DSPMOD (Afişare modul)
 auditare obiect 481

Comanda DSPMOD (Display Module - Afişare modul)
 autorizarea obiect necesară 394

comanda DSPMODD (Afişare descriere mod)
 auditare obiect 480

Comanda DSPMODD (Display Mode Description - Afişare descriere mod)
 autorizarea obiect necesară 394

Comanda DSPMODSRC (Afişare sursă modul)
 autorizarea obiect necesară 414

comanda DSPMODSRC (Afişare sursă modul)
 auditare obiect 469

comanda DSPMODSTS (Afişare stare mod)
 auditare obiect 458

Comanda DSPMODSTS (Display Mode Status - Afişare stare mod)
 autorizarea obiect necesară 394

comanda DSPMSG (Afişare mesaje)
 auditare obiect 482

Comanda DSPMSG (Display Messages - Afişare mesaje)
 autorizări obiect necesare 391

comanda DSPMSGD (Afişare descrieri mesaje)
 auditare obiect 481

Comanda DSPMSGD (Display Message Descriptions - Afişare descrieri mesaj)
 autorizarea obiect necesară 392

Comanda DSPNETA (Display Network Attributes - Afișare atribute rețea) autorizarea obiect necesară 395

comanda DSPNTBD (Afișare descriere NetBIOS) auditare obiect 483

Comanda DSPNTBD (Display NetBIOS Description - Afișare descriere NetBIOS) autorizarea obiect necesară 395

comanda DSPNWID (Afișare descriere interfață de rețea) auditare obiect 484

Comanda DSPNWID (Display Network Interface Description - Afișare descriere interfață de rețea) autorizarea obiect necesară 397

Comanda DSPNWSA (Display Network Server Attribute - Afișare atribut server de rețea) autorizarea obiect necesară 398

Comanda DSPNWSALS (Display Network Server Alias - Afișare alias server de rețea) autorizarea obiect necesară 398

Comanda DSPNWSCFG autorizarea obiect necesară 399
profiluri utilizator livrat de IBM autorizate 291

comanda DSPNWSA (Afișare descriere server de rețea) auditare obiect 484

Comanda DSPNWSA (Display Network Server Description - Afișare descriere server de rețea) autorizarea obiect necesară 399

Comanda DSPNWSASN (Display Network Server Session - Afișare sesiune server de rețea) autorizarea obiect necesară 398

Comanda DSPNWSSTC (Display Network Server Statistics - Afișare statistici server de rețea) autorizarea obiect necesară 398

Comanda DSPNWSSTG (Display Network Server Storage Space - Afișare spațiu de stocare server de rețea) autorizarea obiect necesară 398

Comanda DSPNWSUSR (Display Network Server User - Afișare utilizator server de rețea) autorizări obiect necesare 398

Comanda DSPNWSUSRA (Display Network Server User Attribute - Afișare atribut utilizator server de rețea) autorizarea obiect necesară 398

comanda DSPOBJAUT (Afișare autorizare obiect) auditare obiect 449

Comanda DSPOBJAUT (Afișare autorizare obiect) descriere 272

Comanda DSPOBJAUT (Display Object Authority - Afișare autorizare obiect) 268
autorizarea obiect necesară 304
utilizare 268

comanda DSPOBJD (Afișare descriere obiect) auditare obiect 449

Comanda DSPOBJD (Afișare descriere obiect) creat de 123
descriere 272

Comanda DSPOBJD (Display Object Description - Afișare descriere obiect) autorizări obiect necesare 304
domeniul obiect 13
folosire fișier de ieșire 268
starea program 13
utilizare 254

Comanda DSPOPT (Display Optical - Afișare optic) autorizarea obiect necesară 403

Comanda DSPOPTLCK (Display Optical Lock - Afișare blocare optică) autorizarea obiect necesară 403

Comanda DSPOPTSVR (Display Optical Server - Afișare server optic) autorizarea obiect necesară 403

comanda DSPPDGPRF (Afișare profil grup descriptor tipărire) autorizarea obiect necesară 411

comanda DSPPFM (Afișare membru fișier fizic) auditare obiect 468

Comanda DSPPFM (Display Physical File Member - Afișare membru fișier fizic) autorizarea obiect necesară 341

Comanda DSPPFRTA (Display Performance Data - Afișare date de performanță) autorizarea obiect necesară 409

Comanda DSPPFGRPH (Display Performance Graph - Afișare grafic de performanță) autorizarea obiect necesară 409

comanda DSPPGM (Afișare program) auditare obiect 488

Comanda DSPPGM (Afișare program) autorizare adoptată 130
autorizarea obiect necesară 414

Comanda DSPPGM (Display Program - Afișare program) starea program 13

Comanda DSPPGMADP (Afișare adoptare program) autorizarea obiect necesară 441

comanda DSPPGMADP (Afișare programe care adoptă) auditare obiect 503
folosirea 130

Comanda DSPPGMADP (Afișare programe care adoptă) descriere 275

Comanda DSPPGMADP (Display Programs That Adopt - Afișare programe care adoptă) auditare 268
using 209

comanda DSPPGMREF (Afișare referințe program) auditare obiect 471

Comanda DSPPGMREF (Afișare referințe program) autorizări obiect necesare 414

Comanda DSPPGMVAR (Afișare variabilă program) autorizarea obiect necesară 414

Comanda DSPPRB (Display Problem - Afișare problemă) autorizarea obiect necesară 412

comanda DSPPTF (Display Program Temporary Fix - Afișare corecție temporară program) profiluri utilizator livrat de IBM autorizate 291

Comanda DSPPTF (Display Program Temporary Fix - Afișare corecție temporară program) autorizarea obiect necesară 425

Comanda DSPPWSCD (Display Power On/Off Schedule - Afișare planificare alimentare On/Off) autorizarea obiect necesară 401

comanda DSPRCYAP (Afișare modificări pentru căile de acces) auditare obiect 450
autorizarea obiect necesară 310

Comanda DSPRDBDIRE (Afișare intrare director baze de date relaționale) autorizări obiect necesare 419

Comanda DSPRJECFG (Afișare configurație RJE) autorizarea obiect necesară 422

comanda DSPS36 (Afișare System/36) auditare obiect 502

Comanda DSPS36 (Display System/36 - Afișare System/36) autorizarea obiect necesară 435

Comanda DSPSAVF (Display Save File - Afișare fișier de salvare) autorizarea obiect necesară 341

comanda DSPSBSB (Afișare descriere subsistem) auditare obiect 493

Comanda DSPSBSB (Display Subsystem Description - Afișare descriere subsistem) autorizarea obiect necesară 432

Comanda DSPSECA (Afișare atribute de securitate) autorizarea obiect necesară 423

Comanda DSPSECAUD (Afișare auditare securitate) descriere 619

Comanda DSPSECAUD (Afișare valori de auditare de securitate) descriere 277

Comanda DSPSECAUD (Display Security Auditing Values - Afișare valori de auditare securitate) autorizarea obiect necesară 423

Comanda DSPSFWRSC (Afișare resurse hardware) autorizarea obiect necesară 419

Comanda DSPSOCSTS (Afișare stare sferă de control) autorizarea obiect necesară 429

comanda DSPSPLF (Afișare fișier spool) auditare acțiune 496
auditare obiect 485

comanda DSPSPLF (Display Spooled File - Afișare fișier spool) 186
parametrul DSPDATA al cozii de ieșire 186

- Comanda DSPSPLF (Display Spooled File - Afișare fișier spool)
autorizarea obiect necesară 430
- Comanda DSPSRVA (Afișare atribute service)
autorizarea obiect necesară 425
- comanda DSPSRVPGM (Afișare program service)
auditare obiect 498
autorizarea obiect necesară 414
- Comanda DSPSRVPGM (Afișare program service)
autorizare adoptată 130
- comanda DSPSRVSTS (Display Service Status - Afișare stare serviciu)
profiluri utilizator livrat de IBM autorizate 291
- Comanda DSPSRVSTS (Display Service Status - Afișare stare serviciu)
autorizarea obiect necesară 425
- Comanda DSPSYSVAL (Afișare valoare sistem)
autorizarea obiect necesară 433
- Comanda DSPTAP (Display Tape - Afișare bandă)
autorizarea obiect necesară 390
- Comanda DSPTAPCTG (Display Tape Cartridge - Afișare cartuș bandă)
autorizarea obiect necesară 390
- Comanda DSPTRC (Afișare urmă)
autorizarea obiect necesară 414
- Comanda DSPTRCDTA (Afișare date urmărite)
autorizarea obiect necesară 414
- comanda DSPUDFS (Display User-Defined File System - Afișare sistem de fișiere definit de utilizator)
profiluri utilizator autorizate livrat de IBM 291
- Comanda DSPUDFS (Display User-Defined File System - Afișare sistem de fișiere definit de utilizator)
autorizarea obiect necesară 439
- Comanda DSPUSRPF (Afișare profil utilizator - (Display User Profile)
folosire fișier de ieșire 267
- comanda DSPUSRPMN (Afișare permisiune utilizator)
auditare obiect 465
- Comanda DSPUSRPMN (Display User Permission - Afișare permisiune utilizator)
autorizări obiect necesare 400
- comanda DSPUSRPRF (Afișare profil utilizator)
auditare obiect 504
folosind 104
- Comanda DSPUSRPRF (Afișare profil utilizator)
descriere 274
- Comanda DSPUSRPRF (Display User Profile - Afișare profil utilizator)
autorizarea obiect necesară 441
folosire fișier de ieșire 267
- Comanda DSPVTMAP (Afișare hartă tastatură VT100)
autorizări obiect necesare 438
- Comanda DUPDKT (Duplicate Diskette - Duplicare dischetă)
autorizarea obiect necesară 390
- Comanda DUPOPT (Duplicate Optical - Duplicare optic)
autorizarea obiect necesară 403
- Comanda DUPTAP (Duplicate Tape - Duplicare bandă)
autorizarea obiect necesară 390
- Comanda Edit Authorization List (EDTAUTL) 145
- Comanda Edit Object Authority (EDTOBJAUT) 138
- Comanda Editare autorizare obiect (EDTOBJAUT) 272
- Comanda Editare autorizare obiect de bibliotecă de documente (EDTDLOAUT) 275
- Comanda Editare listă de autorizații (EDTAUTL) 271
- Comanda EDTAUTL (Edit Authorization List - Editare listă de autorizare)
autorizarea obiect necesară 314
folosire 145
- comanda EDTAUTL (Editare listă de autorizații)
auditare obiect 451
- Comanda EDTAUTL (Editare listă de autorizații)
descriere 271
- Comanda EDTBCKUPL (Edit Backup List - Editare listă de salvări de rezervă)
autorizarea obiect necesară 401
- Comanda EDTCPCST (Edit Check Pending Constraints - Editare constrângere de verificare în așteptare)
autorizarea obiect necesară 342
- comanda EDTCPCST (Edit Check Pending Constraints - Editare verificare constrângeri în curs)
profiluri utilizator autorizate livrat de IBM 291
- comanda EDTCPCST (Editare constrângeri de verificare în așteptare)
auditare obiect 471
- Comanda EDTDEVRSC (Editare resurse dispozitiv)
autorizarea obiect necesară 419
- Comanda EDTDLOAUT (Edit Document Library Object Authority - Editare autorizare obiect bibliotecă de documente)
autorizări obiect necesare 332
- comanda EDTDLOAUT (Editare autorizare obiect bibliotecă de documente)
auditare obiect 462, 464
- Comanda EDTDLOAUT (Editare autorizare obiect de bibliotecă de documente)
descriere 275
- Comanda EDTDOC (Edit Document - Editare document)
autorizarea obiect necesară 332
- comanda EDTDOC (Editare document)
auditare obiect 464
- Comanda EDTF (Edit file - Editare document) 355
- Comanda EDTIGCDCT (Edit DBCS Conversion Dictionary - Editare dicționar de conversie DBCS)
autorizarea obiect necesară 335
- comanda EDTIGCDCT (Editare dicționar conversie DBCS)
auditare obiect 473
- comanda EDTLIBL (Edit Library List - Editare lista de biblioteci) 183
folosire 183
- Comanda EDTLIBL (Edit Library List - Editare listă de biblioteci)
autorizarea obiect necesară 383
- Comanda EDTOBJAUT (Edit Object Authority - Editare autorizare obiect)
autorizarea obiect necesară 305
folosire 138
- comanda EDTOBJAUT (Editare autorizare obiect)
auditare obiect 449
- Comanda EDTOBJAUT (Editare autorizare obiect)
descriere 272
- comanda EDTQST (Edit Questions and Answers - Editare întrebări și răspunsuri)
profiluri utilizator livrat de IBM autorizate 291
- Comanda EDTQST (Edit Questions and Answers - Editare întrebări și răspunsuri)
autorizarea obiect necesară 417
- comanda EDTRBDAP (Edit Rebuild Of Access Paths - Editare reconstruire căi de acces)
profiluri utilizator autorizate livrat de IBM 291
- comanda EDTRCYAP (Edit Recovery for Access Paths - Editare recuperare căi de acces)
profiluri utilizator autorizate livrat de IBM 291
- comanda EDTRCYAP (Editare modificări pentru căile de acces)
auditare obiect 450
- Comanda EDTS36PGMA (Edit System/36 Program Attributes - Editare atribute program System/36)
autorizarea obiect necesară 435
- comanda EDTS36PGMA (Editare atribute program System/36)
auditare obiect 488
- Comanda EDTS36PRCA (Edit System/36 Procedure Attributes - Editare atribute procedură System/36)
autorizarea obiect necesară 435
- comanda EDTS36PRCA (Editare atribute procedură System/36)
auditare obiect 470
- Comanda EDTS36SRCA (Edit System/36 Source Attributes - Editare atribute sursă System/36)
autorizarea obiect necesară 435
- comanda EDTS36SRCA (Editare atribute sursă System/36)
auditare obiect 470

Comanda EDTWSOAUT (Edit Workstation Object Authority - Editare autorizare obiect stație de lucru)
autorizări obiect necesare 345

Comanda EJTEMLOUT (Eject Emulation Output - Ejectare ieșire emulare)
autorizări obiect necesare 328

Comanda EML3270 (Emulate 3270 Display - Emulare ecran 3270)
autorizarea obiect necesară 329

Comanda EMLPRTKEY (Emulate Printer Key - Emulare cheie imprimantă)
autorizarea obiect necesară 329

Comanda ENCCPHK (Encipher Cipher Key - Cifrare cheie cifru)
autorizarea obiect necesară 325

comanda ENCCPHK (Encipher Cipher Key - Descifrare cifre cheie)
profiluri utilizator livrat de IBM autorizate 291

comanda ENCFRMMSTK (Descifrare din cheia primară)
profiluri utilizator livrat de IBM autorizate 291

Comanda ENCFRMMSTK (Encipher from Master Key - Cifrare din cheie master)
autorizarea obiect necesară 325

comanda ENCTOMSTK (Descifrare în cheia primară)
profiluri utilizator livrat de IBM autorizate 291

Comanda ENCTOMSTK (Encipher to Master Key - Cifrare în cheie master)
autorizarea obiect necesară 325

Comanda ENDASPBAL 328

Comanda ENDCBLDBG (Terminare depanare COBOL)
autorizarea obiect necesară 381, 414

Comanda ENDCLNUP (End Cleanup - Terminare curățare)
autorizarea obiect necesară 401

comanda ENDCLUNOD
autorizarea obiect necesară 318

Comanda ENDCMNTRC (Terminare urmă comunicații)
autorizarea obiect necesară 425

Comanda ENDCMTCTL (End Commitment Control - Oprește control comitere)
autorizarea obiect necesară 320

Comanda ENDCPYSCN (Terminare copiere ecran)
autorizarea obiect necesară 425

Comanda ENDCTRLRCY (End Controller Recovery - Oprește recuperare controler)
autorizarea obiect necesară 324

comanda ENDCTRLRCY (Terminare recuperare controler)
auditare obiect 457

Comanda ENDDDBG (Terminare depanare)
autorizarea obiect necesară 414

comanda ENDDBGSVR (End Debug Server - Terminare depanare server)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDDBMON (End Database Monitor - Terminare monitorizare bază de date)
autorizarea obiect necesară 410

Comanda ENDDEVRCY (End Device Recovery - Oprește recuperare dispozitiv)
autorizarea obiect necesară 328

comanda ENDDEVRCY (Terminare recuperare dispozitiv)
auditare obiect 458

Comanda ENDDIRSHD (End Directory Shadow System - Oprește sistem umbră director)
autorizarea obiect necesară 329

comanda ENDDIRSHD (Terminare umbrire director)
auditare obiect 462

Comanda ENDDSKRGZ (End Disk Reorganization - Oprește reorganizare disc)
autorizarea obiect necesară 330

Comanda ENDGRPJOB (End Group Job - Terminare job de grup)
autorizarea obiect necesară 368

Comanda ENDHOSTSVR (End Host Server - Oprește server gazdă)
autorizarea obiect necesară 346

comanda ENDIDXMN (Terminare monitorizare index)
profiluri utilizator livrat de IBM autorizate 292

comanda ENDIPSIFC (End IP over SNA Interface - Terminare IP prin interfața SNA)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDIPSIFC (End IP over SNA Interface - Terminare IP prin interfața SNA)
autorizarea obiect necesară 312

Comanda ENDJOB (End Job - Terminare job)
autorizarea obiect necesară 368

Valoarea de sistem QINACTMSGQ 24

comanda ENDJOB (Terminare job)
auditare acțiune 497

comanda ENDJOBABN (End Job Abnormal - Terminare anormală job)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDJOBABN (End Job Abnormal - Terminare anormală job)
autorizarea obiect necesară 368

Comanda ENDJOBTRC (End Job Trace - Terminare urmărire job)
autorizarea obiect necesară 409

Comanda ENDJRN (End Journal - Terminare jurnal)
autorizarea obiect necesară 355, 374

comanda ENDJRN (Terminare jurnalizare)
auditare obiect 448

Comanda ENDJRNAP (End Journal Access Path - Terminare cale acces jurnal)
autorizarea obiect necesară 374

Comanda ENDJRNP (End Journal Physical File Changes - Terminare modificări fișier fizic jurnal)
autorizarea obiect necesară 374

comanda ENDJRNxxx (Terminare jurnalizare)
auditare obiect 476

Comanda ENDLINRCY (End Line Recovery - Oprește recuperare linie)
autorizarea obiect necesară 388

comanda ENDLINRCY (Terminare recuperare linie)
auditare obiect 479

Comanda ENDLOGSVR (End Job - Terminare job)
autorizarea obiect necesară 368

comanda ENDMGDSYS (End Managed System - Terminare sistem gestionat)
profiluri utilizator livrat de IBM autorizate 292

comanda ENDMGRSRV (End Manager Services - Terminare servicii manager)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDMOD (End Mode - Terminare mod)
autorizarea obiect necesară 394

comanda ENDMOD (Terminare mod)
auditare obiect 480

comanda ENDMSF (End Mail Server Framework - Terminare cadru de lucru server de mail)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDMSF (End Mail Server Framework - Terminare cadru de lucru server de poștă)
autorizări obiect necesare 389

comanda ENDNFSSVR (End Network File System Server - Terminare server sistem de fișiere rețea)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDNFSSVR (End Network File System Server - Terminare server sistem de fișiere rețea)
autorizarea obiect necesară 396

comanda ENDNWIRCY (Terminare recuperare interfață de rețea)
auditare obiect 484

Comanda ENDPASTHR (End Pass-Through - Terminare passthrough)
autorizarea obiect necesară 330

Comanda ENDPPEX (End Performance Explorer - Terminare explorare performanță)
autorizarea obiect necesară 409

comanda ENDPPEX (End Performance Explorer - Terminare Performance Explorer)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDPFRMON (End Performance Monitor - Terminare monitorizare performanță)
autorizarea obiect necesară 410

comanda ENDPFRTRC (Terminare urmărire performanță)
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDPJ (End Prestart Jobs - Terminare joburi prestart)
autorizarea obiect necesară 368

comanda ENDPJ (Terminare joburi prestart)
auditare acțiune 497

Comanda ENDRTEML (End Printer Emulation - Oprire emulare imprimantă) autorizări obiect necesare 329

Comanda ENDRDR (End Reader - Terminare cititor) autorizarea obiect necesară 418

Comanda ENDRJESSN (Terminare sesiune RJE) autorizarea obiect necesară 422

Comanda ENDRQS (Terminare cerere) autorizarea obiect necesară 414

comanda ENDS36 (Terminare System/36) auditare obiect 502

Comanda ENDSBS (End Subsystem - Oprire subsistem) autorizarea obiect necesară 432

comanda ENDSBS (Terminare subsistem) auditare obiect 492

Comanda ENDSRVJOB (Terminare job service) autorizarea obiect necesară 425
profiluri utilizator livrat de IBM autorizate 292

Comanda ENDSYS (Terminare sistem) autorizarea obiect necesară 433

comanda ENDSYSMGR (Terminare manager sistem) profiluri utilizator livrat de IBM autorizate 292

Comanda ENDTCP (End TCP/IP - Terminare TCP/IP) autorizarea obiect necesară 436

comanda ENDTCP (Terminare TCP/IP) profiluri utilizator livrat de IBM autorizate 292

comanda ENDTCPCNN (End TCP/IP Connection - Terminare conexiune TCP/IP) autorizarea obiect necesară 438

Comanda ENDTCPCNN (Terminare conexiune TCP/IP) profiluri utilizator livrat de IBM autorizate 292

Comanda ENDTCPICF (Oprire interfață TCP/IP) autorizări obiect necesare 437

Comanda ENDTCPPTP (Terminare TCP/IP punct-la-punct) autorizări obiect necesare 437

Comanda ENDTCPSPRV (Terminare serviciu TCP/IP) autorizarea obiect necesară 437

comanda ENDTCPSVR (End TCP/IP Server - Terminare server TCP/IP) profiluri utilizator livrat de IBM autorizate 292

Comanda ENDTRC (Terminare urmărire) autorizarea obiect necesară 425

Comanda ENDWCH autorizarea obiect necesară 425

Comanda ENDWCH (End Watch - Terminare supraveghere) profiluri utilizator livrat de IBM autorizate 292

Comanda ENTCBLDBG (Terminare depanare COBOL) autorizarea obiect necesară 382, 414

Comanda EXTPGMINF (Extragere informații program) autorizări obiect necesare 414

Comanda Extragere intrare listă de autorizații (RTVAUTLE) 271

comanda Extragere profil utilizator (RTVUSRPRF) 107

Comanda Extragere profil utilizator (RTVUSRPRF) 274

comanda faccessx (Determinare accesibilitate fișier pentru o clasă de utilizatori după descriptor) auditare obiect 459

comanda FILDOC (Document fișier) auditare obiect 464

Comanda FILDOC (File Document - Clasare document) autorizarea obiect necesară 332

Comanda FNDSTRPDM (Find String Using PDM - Găsire șir folosind PMD) autorizarea obiect necesară 312

Comanda FTP (Protocol transfer fișiere) autorizarea obiect necesară 437

Comanda GENCAT (Merge Message Catalog - Combinare catalog de mesaje) autorizarea obiect necesară 342

Comanda GENCMDDOC (Generate Command Documentation - Generare documentație comandă) autorizarea obiect necesară 320

Comanda GENCPHK (Generate Cipher Key - Generare cheie cifru) autorizarea obiect necesară 325

comanda GENCPHK (Generate Cipher Key - Generare cheie de cifrare) profiluri utilizator livrat de IBM autorizate 292

comanda GENCRSDMNK (Generare cheie de traversare domeniu) profiluri utilizator livrat de IBM autorizate 292

Comanda GENCRSDMNK (Generate Cross Domain Key - Generare cheie de-a lungul domeniului) autorizări obiect necesare 325

Comanda GENMAC (Generate Message Authentication Code - Generare cod de autentificare mesaj) autorizarea obiect necesară 325
profiluri utilizator autorizate livrat de IBM 292

Comanda GENPIN (Generate Personal Identification Number - Generare număr de identificare personal) autorizarea obiect necesară 325
profiluri utilizator autorizate livrat de IBM 292

comanda GENS36RPT (Generate System/36 Report - Generare raport System/36) profiluri utilizator autorizate livrat de IBM 292

Comanda GENS36RPT (Generate System/36 Report - Generare raport System/36) autorizări obiect necesare 393

comanda GENS38RPT (Generate System/38 Report - Generare raport System/36) profiluri utilizator autorizate livrat de IBM 292

Comanda GENS38RPT (Generate System/38 Report - Generare raport System/38) autorizarea obiect necesară 393

comanda Gestionare atribute jurnal (Work with Journal Attributes - WRKJRNA) 260, 267

comanda Gestionare jurnal (Work with Journal - WRKJRN) 260, 267

comanda Gestionare profiluri utilizator (WRKUSRPRF) 97

comanda Gestionare valori de sistem (Work with System Values - WRKSYSVAL) 230

Comanda GO (Go to Menu - Deplasare la meniu) autorizarea obiect necesară 391

Comanda Grant Object Authority (GRTOBJAUT) 138
efectul asupra autorizării anterioare 141
obiecte multiple 141

Comanda Grant User Authority (GRTUSRAUT) recomandări 144

comanda GRTACCAUT (Acordare autorizare cod acces) auditare obiect 464

Comanda GRTACCAUT (Grant Access Code Authority - Acordare autorizare cod acces) autorizarea obiect necesară 400

comanda GRTACCAUT (Grant Access Code Authority - Acordare autorizare cod de acces) profiluri utilizator autorizate livrat de IBM 292

comanda GRTOBJAUT (Acordare autorizare obiect) auditare obiect 448

Comanda GRTOBJAUT (Acordare autorizare obiect) descriere 272

Comanda GRTOBJAUT (Grant Object Authority - Acordare autorizare obiect) 138
autorizarea obiect necesară 305
efectul asupra autorizării anterioare 141
obiecte multiple 141

comanda GRTUSRAUT (Acordare autorizare de utilizator) copie autorizare 101
redenumire profil 106

comanda GRTUSRAUT (Acordare autorizare utilizator) auditare obiect 503, 504

Comanda GRTUSRAUT (Acordare autorizare utilizator) descriere 274

Comanda GRTUSRAUT (Grant User Authority - Acordare autorizare utilizator) autorizarea obiect necesară 441
recomandări 144

comanda GRTUSRPMN (Acordare permisiune utilizator) auditare obiect 464

Comanda GRTUSRPMN (Acordare permisiuni utilizator) descriere 275

- Comanda GRTUSRPMN (Grant User Permission - Acordare permisiune utilizator) autorizări obiect necesare 400
- Comanda GRTWSOAUT (Grant Workstation Object Authority - Acordare autorizare obiect stație de lucru) autorizări obiect necesare 345
- Comanda HLDCMNDEV (Hold Communications Device - Reținere dispozitive de comunicație) autorizarea obiect necesară 328
- comanda HLDCMNDEV (Reținere dispozitiv comunicații) auditare obiect 458
- comanda HLDCMNDEV (Reținere dispozitiv de comunicații) profiluri utilizator autorizate livrat de IBM 292
- Comanda HLDDSTQ (Hold Distribution Queue - Reținere coadă de distribuție) autorizarea obiect necesară 331
profiluri utilizator livrat de IBM autorizate 292
- Comanda HLDJOB (Hold Job - Reținere job) autorizarea obiect necesară 368
- comanda HLDJOBQ (Blocare coadă joburi) auditare obiect 475
- Comanda HLDJOBQ (Hold Job Queue - Reținere coadă joburi) autorizarea obiect necesară 371
- comanda HLDJOBSCDE (Blocare intrare planificare job) auditare obiect 475
- Comanda HLDJOBSCDE (Hold Job Schedule Entry - Reținere intrare planificare job) autorizarea obiect necesară 372
- Comanda HLDOUTQ (Hold Output Queue - Reținere coadă de ieșire) autorizarea obiect necesară 405
- comanda HLDOUTQ (Reținere coadă de ieșire) auditare obiect 485
- Comanda HLDRDR (Hold Reader - Reținere cititor) autorizarea obiect necesară 418
- Comanda HLDSPFL (Reținere fișier spool) auditare acțiune 497
auditare obiect 485
autorizarea obiect necesară 430
- comanda INSPTF (Install Program Temporary Fix - Instalare corecție temporară program) profiluri utilizator livrat de IBM autorizate 292
- Comanda INSPTF (Install Program Temporary Fix - Instalare corecție temporară program) autorizarea obiect necesară 425
- comanda INSRMTPRD (Install Remote Product - Instalare produs la distanță) profiluri utilizator livrat de IBM autorizate 292
- Comanda INSWNTSVR profiluri utilizator livrat de IBM autorizate 292
- Comanda INZDKT (Initialize Diskette - Inițializare dischetă) autorizarea obiect necesară 390
- comanda INZDSTQ (Initialize Distribution Queue - Inițializare coadă de distribuție) profiluri utilizator autorizate livrat de IBM 292
- Comanda INZDSTQ (Initialize Distribution Queue - Inițializare coadă de distribuție) autorizarea obiect necesară 331
- Comanda INZNWSCFG autorizarea obiect necesară 399
profiluri utilizator livrat de IBM autorizate 292
- Comanda INZOPT (Initialize Optical - Inițializare optic) autorizarea obiect necesară 403
- Comanda INZPFM (Initialize Physical File Member - Inițializare membru fișier fizic) autorizări obiect necesare 342
- comanda INZPFM (Inițializare membru fișier fizic) auditare obiect 470
- comanda INZSYS (Initialize System - Inițializare sistem) autorizarea obiect necesară 387
profiluri utilizator livrat de IBM autorizate 292
- Comanda INZTAP (Initialize Tape - Inițializare bandă) autorizarea obiect necesară 390
- Comanda Înlăturare autorizare obiect de bibliotecă de documente (RMVDLOAUT) 275
- Comanda Înlăturare intrare director (RMVDIRE) 276
- Comanda Înlăturare intrare listă de autorizații (RMVAUTLE) 271
- Comanda JRNAP (Journal Access Path - Cale de acces jurnal) autorizarea obiect necesară 374
- comanda JRNAP (Pornire cale acces jurnal) auditare obiect 476
- Comanda JRNPF (Journal Physical File - Fișier fizic jurnal) autorizarea obiect necesară 374
- comanda JRNPF (Pornire fișier fizic jurnal) auditare obiect 476
- Comanda Lansare job (SBMJOB) meniu SECBATCH 620
- comanda LNKDTADFN (Legare definiții de date) auditare obiect 466
- Comanda LNKDTADFN (Link Data Definition - Legătură definiție de date) autorizarea obiect necesară 366
- comanda LODIMGCLG autorizarea obiect necesară 346
- Comanda LODIMGCLGE autorizarea obiect necesară 346
- Comanda LODOPTFMW autorizarea obiect necesară 403
- comanda LODPTF (Load Program Temporary Fix - Încărcare corecție temporară program) profiluri utilizator livrat de IBM autorizate 293
- Comanda LODPTF (Load Program Temporary Fix - Încărcare corecție temporară program) autorizarea obiect necesară 425
- comanda LODQSTDB (Load Question-and-Answer Database - Încărcare bază de date întrebare-răspuns) profiluri utilizator autorizate livrat de IBM 293
- Comanda LPR (Solicitant linie imprimantă) autorizarea obiect necesară 437
- Comanda LTQMQR (Ștergere interogare Query Management) autorizarea obiect necesară 416
- Comanda Lucru cu autorizare (WRKAUT) 272
- Comanda Lucru cu directoare (WRKDIRE) 276
- Comanda Lucru cu liste de autorizație (WRKAUTL) 271
- Comanda Lucru cu obiecte (WRKOBJ) 272
- Comanda Lucru cu obiecte după grup primar (WRKOBJPGP) descriere 272
- Comanda Lucru cu obiecte după proprietar (WRKOBJOWN) descriere 272
- Comanda Lucru cu profiluri utilizator (WRKUSRPRF) 274
- Comanda Merge Source (Merge Source - Combinare sursă) autorizarea obiect necesară 342
- comanda MGRS36 (Migrate System/36 - Migrare System/36) profiluri utilizator livrat de IBM autorizate 293
- comanda MGRS36ITM (Migrate System/36 Item - Migrare element System/36) profiluri utilizator autorizate livrat de IBM 293
- Comanda MGRS36ITM (Migrate System/36 Item - Migrare element System/36) autorizarea obiect necesară 393
- Comanda MGRS38OBJ (Migrate System/38 Objects - Migrare obiecte System/38) autorizări obiect necesare 393
profiluri utilizator autorizate livrat de IBM 293
- Comanda MGRTCPHT (Combinare tabel gazdă TCP/IP) autorizarea obiect necesară 438
- comanda Modificare atribute grup de noduri (Modificare atribute grup de noduri) auditare obiect 483
- comanda Modificare auditare (CHGAUD) folosind 106
- Comanda Modificare auditare (CHGAUD) descriere 272, 275
- Comanda Modificare auditare de securitate (CHGSECAUD) descriere 277
- comanda Modificare auditare obiect (CHGOBJAUD) autorizare specială *AUDIT (auditare) 71
- Comanda Modificare auditare obiect (CHGOBJAUD) descriere 272, 275
Valoarea de sistem QAUDCTL (Control auditare) 50

comanda Modificare auditare obiect bibliotecă document (CHGDLOAUD)
autorizare specială *AUDIT (auditare) 71

Comanda Modificare auditare obiect bibliotecă document (CHGDLOAUD)
Valoarea de sistem QAUDCTL (Control auditare) 50

Comanda Modificare auditare obiect de bibliotecă de documente (CHGDLOAUD)
descriere 275

Comanda Modificare auditare securitate (CHGSECAUD)
descriere 619

comanda Modificare auditare utilizator (CHGUSRAUD)
autorizare specială *AUDIT (auditare) 71
folosind 106

Comanda Modificare auditare utilizator (CHGUSRAUD) 274
descriere 275

Comanda Modificare autorizare (CHGAUT) 272

Comanda Modificare autorizare obiect de bibliotecă de documente (CHGDLOAUD) 275

comanda Modificare cod de contabilizare (CHGACGCDE) 82

comanda Modificare comandă (CHGCMD)
parametru ALWLMTUSR (permitere utilizator limitat) 67

Comanda Modificare grup primar (CHGPGP) 272

Comanda Modificare grup primar de obiecte (CHGOBJPGP) 272

Comanda Modificare grup primar obiect de bibliotecă de documente (CHGDLOPGP)
descriere 275

Comanda Modificare intrare director (CHGDIRE) 276

Comanda Modificare intrare listă de autorizații (CHGAUTLE)
descriere 271

Comanda Modificare Intrare planificator de activare (CHGACTSCDE)
descriere 617

Comanda Modificare intrare planificator de expirare (CHGEXPSCDE)
descriere 617

Comanda Modificare listă de profiluri activă (CHGACTPRFL)
descriere 617

Comanda Modificare parolă (Change Password - CHGPWD)
auditare 231

comanda Modificare parolă (CHGPWD)
setare parolă egală cu nume profil 60
valori de sistem de parole de impunere 39

Comanda Modificare parolă (CHGPWD)
descriere 273

Comanda Modificare parolă Unelte de service dedicate (CHGDSTPWD) 273

comanda Modificare profil (CHGPRF) 101

Comanda Modificare profil (CHGPRF) 274

comanda Modificare profil utilizator (CHGUSRPRF)
folosind 101
setare parolă egală cu nume profil 60

Comanda Modificare profil utilizator (CHGUSRPRF) 274
descriere 273

Comanda Modificare proprietar obiect (CHGOBJOWN) 272

Comanda Modificare proprietar obiect de bibliotecă de documente (CHGDLOOWN) 275

Comanda MOUNT (Adăugare sistem de fișiere)
autorizarea obiect necesară 439

Comanda MOUNT (Add Mounted File System - Adăugare sistem de fișiere montat)
autorizări obiect necesare 396

comanda MOV (Mutare)
auditare obiect 460, 499, 501

Comanda MOVD (Move Document - Mutare document)
autorizarea obiect necesară 332

Comanda Move - Mutare
autorizarea obiect necesară 356

Comanda MOVOBJ (Move Object - Mutare obiect)
autorizarea obiect necesară 305

comanda MOVOBJ (Mutare obiect)
auditare obiect 448, 478

comanda MRGDOC (Combinare document)
auditare obiect 462, 464

Comanda MRGDOC (Merge Document - Combinare document)
autorizarea obiect necesară 332

Comanda MRGFORMD (Merge Form Description - Combinare descriere formular)
autorizarea obiect necesară 312

comanda MRGMSGF (Combinare fișier mesaj)
auditare obiect 481

Comanda MRGMSGF (Merge Message File - Combinare fișier mesaj)
autorizarea obiect necesară 393

Comanda NETSTAT (Stare rețea)
autorizarea obiect necesară 438

Comanda OPNDBF (Open Database File - Deschidere fișier bază de date)
autorizarea obiect necesară 342

Comanda OPNQRYF (Open Query File - Deschidere fișier de interogare)
autorizarea obiect necesară 342

comanda OVRMSGF (Înlocuire cu fișier de mesaje)
auditare obiect 482

comanda PAGDOC (Paginare document)
auditare obiect 464

Comanda PAGDOC (Paginate Document - Paginare document)
autorizarea obiect necesară 333

Comanda PING (Verificare conexiune TCP/IP)
autorizarea obiect necesară 438

comanda PKGPRDDST (Package Product Distribution - Pachet de distribuție produse)
profiluri utilizator livrat de IBM autorizate 293

comanda Pornire System/36 (STRS36)
profil utilizator mediu special 72

Comanda pretindere spațiu de stocare (RCLSTG) 17

Comanda pretindere spațiu de stocare (RCLSTG) (*continuare*)
setare valoare de sistem QALWUSRDMN (permitere obiecte utilizator) 22

Comanda Pretindere spațiu de stocare (RCLSTG) 124

Comanda PRTACTRPT (Print Activity Report - Tipărire raport activitate)
autorizarea obiect necesară 409

Comanda PRTADPOBJ (Tipărire obiect adoptat)
autorizarea obiect necesară 305

Comanda PRTADPOBJ (Tipărire obiecte care adoptă)
descriere 621

comanda PRTCMDUSG (Tipărire folosire comandă)
auditare obiect 454, 488

Comanda PRTCMDUSG (Tipărire folosire comandă)
autorizarea obiect necesară 414

Comanda PRTCMNSEC (Print Communication Security - Tipărire securitate comunicație)
autorizarea obiect necesară 324

Comanda PRTCMNSEC (Tipărire securitate comunicații)
autorizarea obiect necesară 328, 388
descriere 278, 621

comanda PRTCMNTRC (Print Communications Trace - Tipărire urmărire comunicații)
profiluri utilizator autorizate livrat de IBM 293

Comanda PRTCMNTRC (Print Communications Trace - Tipărire urmărire comunicații)
autorizări obiect necesare 425

Comanda PRTCPTRPT (Print Component Report - Tipărire raport componentă)
autorizarea obiect necesară 409

comanda PRTCSPAPP (Tipărire aplicație CSP/AE)
auditare obiect 488

Comanda PRTDEVADR (Print Device Addresses - Adrese dispozitiv de tipărire)
autorizări obiect necesare 321

comanda PRTDEVADR (Tipărire adrese dispozitiv)
auditare obiect 457

comanda PRTDOC (Tipărire document)
auditare obiect 463

comanda PRTDSKINF (Print Disk Activity Information - Tipărire informații de activitate disc)
autorizarea obiect necesară 401

Comanda PRTERRLOG (Print Error Log - Tipărire istoric eroare)
autorizarea obiect necesară 425

Comanda PRTINTDTA (Print Internal Data - Tipărire date interne)
autorizarea obiect necesară 425

Comanda PRTIPSCFG (Print IP over SNA Configuration - Tipărire IP pe configurație SNA)
autorizarea obiect necesară 312

- Comanda PRTJOBDAUT (Tipărire autorizare descriere de job)
 autorizarea obiect necesară 371
 descriere 277
- Comanda PRTJOBDAUT (Tipărire autorizare descriere job)
 descriere 621
- Comanda PRTJOBTRPT (Print Job Report - Tipărire raport job)
 autorizarea obiect necesară 409
- Comanda PRTJOBTRC (Print Job Trace - Tipărire urmă job)
 autorizarea obiect necesară 409
- Comanda PRTLCKRPT (Print Lock Report - Tipărire raport blocare)
 autorizarea obiect necesară 409
- Comanda PRTPXRPT (Print Performance Explorer Report - Tipărire raport explorare performanțe)
 autorizarea obiect necesară 409
- Comanda PRTPOLRPT (Print Pool Report - Tipărire raport pool)
 autorizarea obiect necesară 409
- comanda PRTPRFINT (Print Profile Internals - Tipărire interne profil)
 profiluri utilizator livrat de IBM autorizate 293
- Comanda PRTPUBAUT (Print Public Authorities - Tipărire autorizări publice)
 autorizarea obiect necesară 305
- Comanda PRTPUBAUT (Tipărire obiecte autorizate pentru publicare)
 descriere 621
- Comanda PRTPUBAUT (Tipărire obiecte autorizate public)
 descriere 277
- Comanda PRTPVTAUT (Print Private Authorities - Tipărire autorizări private)
 autorizarea obiect necesară 305
- Comanda PRTPVTAUT (Tipărire autorizații private)
 descriere 623
 listă de autorizații 621
- Comanda PRTPVTAUT (Tipărire autorizări private)
 descriere 277
- Comanda PRTQAUT (Print Queue Authorities - Tipărire autorizări coadă)
 autorizarea obiect necesară 371, 405
- Comanda PRTQAUT (Tipărire autorizare coadă)
 descriere 277, 623
- Comanda PRTRSCRPT (Print Resource Report - Tipărire raport resursă)
 autorizarea obiect necesară 409
- Comanda PRTSBSDAUT (Print Subsystem Description Authority - Tipărire autorizare descriere subsistem)
 autorizări obiect necesare 432
- Comanda PRTSBSDAUT (Tipărire autorizare descriere subsistem)
 descriere 277
- Comanda PRTSBSDAUT (Tipărire descriere subsistem)
 descriere 621
- Comanda PRSQLINF (Print Structured Query Language Information - Tipărire informații limbaj de interogare structurat)
 autorizarea obiect necesară 405
- comanda PRSQLINF (Tipărire informații SQL)
 auditare obiect 488, 497, 498
- Comanda PRSYSRPT (Print System Report - Tipărire raport sistem)
 autorizarea obiect necesară 410
- Comanda PRSYSSECA (Atribut Tipărire securitate sistem)
 autorizarea obiect necesară 423
- Comanda PRSYSSECA (Tipărire atribute de securitate sistem)
 descriere 278
- Comanda PRSYSSECA (Tipărire atribute securitate sistem)
 descriere 621
- Comanda PRTTNSRPT (Print Transaction Report - Tipărire raport tranzacție)
 autorizarea obiect necesară 410
- Comanda PRTRC (Tipărire urmărire)
 autorizarea obiect necesară 425
- Comanda PRTRGPGM (Print Trigger Program - Program declanșator de tipărire)
 autorizarea obiect necesară 342
- Comanda PRTRGPGM (Tipărire programe de declanșare)
 descriere 277
- Comanda PRTRGPGM (Tipărire programe declanșatoare)
 descriere 621
- Comanda PRTUSROBJ (Print User Object - Tipărire obiect utilizator)
 autorizarea obiect necesară 305
- Comanda PRTUSROBJ (Tipărire obiecte utilizator)
 descriere 277
- Comanda PRTUSROBJ (Tipărire obiecte utilizatori)
 descriere 621
- Comanda PRTUSRPRF (Print User Profile - Tipărire profil utilizator)
 autorizarea obiect necesară 441
- Comanda PRTUSRPRF (Tipărire profil utilizator)
 descriere 621
- comanda PWRDWN SYS (Power Down System - Oprire sistem)
 profiluri utilizator livrat de IBM autorizate 293
- Comanda PWRDWN SYS (Power Down System - Oprire sistem)
 autorizarea obiect necesară 433
- comanda QlgAccess (Determinare accesibilitate fișier)
 auditare obiect 458
- comanda QlgAccessx (Determinare accesibilitate fișier)
 auditare obiect 458
- Comanda QPWLDMTCHR 61
- comanda QRYDOCLIB (Cerere bibliotecă documente)
 auditare obiect 464
- Comanda QRYDOCLIB (Query Document Library - Interogare bibliotecă de documente)
 autorizări obiect necesare 333
- Comanda QRYDST (Query Distribution - Interogare distribuție)
 autorizarea obiect necesară 331
- Comanda QRYPRBSTS (Query Problem Status - Interogare stare problemă)
 autorizarea obiect necesară 412
- Comanda QSH (Pornire QSH)
 alias pentru STRQSH 416
- Comanda RCLACTGRP (Reclamare grup activare)
 autorizarea obiect necesară 433
- Comanda RCLDBXREF
 autorizarea obiect necesară 305
- Comanda RCLDLO (Reclaim Document Library Object - Recuperare obiect bibliotecă de documente)
 autorizări obiect necesare 333
- comanda RCLDLO (Revendicare obiect bibliotecă documente)
 auditare obiect 465
- Comanda RCLLNK (Reclaim Object Links - Revocare legături obiect)
 autorizarea obiect necesară 357
- Comanda RCLOBJOWN (Reclaim Objects by Owner - Revendicare obiecte de către proprietar)
 autorizarea obiect necesară 305
 profiluri utilizator livrat de IBM autorizate 293
- Comanda RCLOPT (Reclaim Optical - Reclamare optic)
 autorizarea obiect necesară 403
- comanda RCLOPT (Reclaim Optical - Revendicare mediu optic)
 profiluri utilizator livrat de IBM autorizate 293
- Comanda RCLRSC (Reclamare resurse)
 obiect autorizare cerută 433
- comanda RCLSPLSTG (Reclaim Spool Storage - Revendicare spațiu de stocare spool)
 profiluri utilizator livrat de IBM autorizate 293
- Comanda RCLSPLSTG (Reclaim Spool Storage - Revendicare spațiu de stocare spool)
 autorizarea obiect necesară 430
- comanda RCLSTG (Pretindere spațiu de stocare)
 autorizarea obiect necesară 305
 Profil QDFTOWN (proprietar implicit) 124
 profiluri utilizator livrat de IBM autorizate 293
- Comanda RCLSTG (pretindere spațiu de stocare)
 nivel de securitate 50 17
 setare valoare de sistem QALWUSRDMN (permitere obiecte utilizator) 22
- comanda RCLSTG (Reclaim Storage)
 listă de autorizare deteriorată 227

comanda RCLSTG (Revendicare spațiu de stocare)
auditare obiect 448

Comanda RCLTMPSTG (Reclaim Temporary Storage - Prindere spațiu de stocare temporar)
autorizarea obiect necesară 305

comanda RCLTMPSTG (Reclaim Temporary Storage - Revendicare spațiu de stocare temporar)
profiluri utilizator autorizate livrat de IBM 293

comanda RCLTMPSTG (Revendicare spațiu de stocare temporar)
auditare obiect 450

comanda RCV DST (Primire distribuție)
auditare obiect 464

Comanda RCV DST (Receive Distribution - Recepționare distribuție)
autorizarea obiect necesară 331

comanda RCVJRNE (Primire intrare jurnal)
auditare obiect 476

Comanda RCVJRNE (Receive Journal Entry - Primire intrare jurnal)
autorizarea obiect necesară 374

Comanda RCV MGR DTA (Receive Migration Data - Primire date de migrare)
autorizarea obiect necesară 393

comanda RCVMSG (Primire mesaj)
auditare obiect 482

Comanda RCVMSG (Receive Message - Primire mesaj)
autorizarea obiect necesară 391

Comanda RCVNETF (Receive Network File - Primire fișier rețea)
autorizarea obiect necesară 396

comanda Reclaim Storage (RCLSTG) 227

Comanda Remove Authorization List Entry (RMVAUTLE) 145

comanda RESMGRNAM (Resolve Duplicate and Incorrect Office Object Names - Rezolvare duplicat și nume incorecte de obiect office)
autorizarea obiect necesară 393

Comanda RESMGRNAM (Resolve Duplicate and Incorrect Office Object Names - Rezolvare nume obiecte de tip office incorecte sau duplicate)
profiluri utilizator livrat de IBM autorizate 294

Comanda Restaurare autorizare (RSTAUT)
descriere 275

Comanda Restaurare profiluri utilizator (RSTUSRPRF) 275

comanda Restore Authority (RSTAUT)
folosind 223
procedură 224
rol în restaurarea securității 219

comanda Restore Document Library Object (RSTDLO) 219

comanda Restore Licensed Program (RSTLICPGM)
recomandări 225
riscuri de securitate 225

comanda Restore Object (RSTOBJ)
folosind 219

comanda Restore User Profiles (RSTUSRPRF) 219

Comanda RETURN (Întoarcere)
autorizarea obiect necesară 433

Comanda Revocare autorizare obiect (RVKOBJAUT) 272

Comanda Revocare autorizare publică (RVKPUBAUT)
descriere 278

Comanda Revocare autorizație publică (RVKPUBAUT)
descriere 625

Comanda Revocare permisiune utilizator (RVKUSRPMN) 275

Comanda Revoke Object Authority (RVKOBJAUT) 138, 146

comanda RGZDLO (Reorganizare obiect bibliotecă documente)
auditare obiect 464

Comanda RGZDLO (Reorganize Document Library Object - Reorganizare obiect bibliotecă de documente)
autorizări obiect necesare 333

comanda RGZPFM (Reorganizare membru fișier fizic)
auditare obiect 470

Comanda RGZPFM (Reorganize Physical File Member - Reorganizare membru fișier fizic)
autorizarea obiect necesară 342

comanda RLSCMNDEV (Eliberare dispozitiv comunicații)
auditare obiect 458, 479

comanda RLSCMNDEV (Release Communications Device - Eliberare dispozitiv comunicații)
profiluri utilizator autorizate livrat de IBM 294

Comanda RLSCMNDEV (Release Communications Device - Eliberare dispozitive de comunicații)
autorizarea obiect necesară 328

comanda RLSDSTQ (Release Distribution Queue - Eliberare coadă de distribuție)
profiluri utilizator autorizate livrat de IBM 294

Comanda RLSDSTQ (Release Distribution Queue - Eliberare coadă de distribuție)
autorizarea obiect necesară 331

comanda RLSIFSLCK (Release IFS Lock - Eliberare blocare IFS)
profiluri utilizator livrat de IBM autorizate 294

Comanda RLSIFSLCK (Release IFS Lock - Eliberare blocare IFS)
autorizări obiect necesare 396

Comanda RLSJOB (Release Job - Eliberare job)
autorizarea obiect necesară 368

comanda RLSJOBQ (Eliberare coadă joburi)
auditare obiect 475

Comanda RLSJOBQ (Release Job Queue - Eliberare coadă de joburi)
autorizarea obiect necesară 371

comanda RLSJOBSCDE (Eliberare intrare planificare job)
auditare obiect 475

Comanda RLSJOBSCDE (Release Job Schedule Entry - Eliberare intrare planificare job)
autorizarea obiect necesară 372

comanda RLSOUTQ (Eliberare coadă de ieșire)
auditare obiect 485

Comanda RLSOUTQ (Release Output Queue - Eliberare coadă de ieșire)
autorizarea obiect necesară 405

Comanda RLSRDR (Release Reader - Eliberare cititor)
autorizarea obiect necesară 418

comanda RLSRMTPHS (Release Remote Phase - Eliberare fază la distanță)
profiluri utilizator livrat de IBM autorizate 294

comanda RLSSPLF (Eliberare fișier spool)
auditare obiect 486

Comanda RLSSPLF (Release Spooled File - Eliberare fișier spool)
autorizarea obiect necesară 430

Comanda RLSWTR (Eliberare scriitor)
autorizarea obiect necesară 444

comanda RMVACC (Înlăturare cod acces)
auditare obiect 465

comanda RMVACC (Remove Access Code - Înlăturare cod acces)
profiluri utilizator livrat de IBM autorizate 294

Comanda RMVACC (Remove Access Code - Înlăturare cod acces)
autorizarea obiect necesară 400

comanda RMVAJE (Înlăturare intrare job autostart)
auditare obiect 493

Comanda RMVAJE (Remove Autostart Job Entry - Înlăturare intrare job autostart)
autorizarea obiect necesară 432

comanda RMVALRD (Înlăturare descriere alertă)
auditare obiect 450

Comanda RMVALRD (Remove Alert Description - Înlăturare descriere alertă)
autorizarea obiect necesară 312

comanda RMVAUTLE (Înlăturare intrare listă de autorizații)
auditare obiect 451

Comanda RMVAUTLE (Înlăturare intrare listă de autorizații)
descriere 271

Comanda RMVAUTLE (Remove Authorization List Entry - Ștergere intrare din lista de autorizare)
autorizarea obiect necesară 314
folosire 145

Comanda RMVBKP (Înlăturare punct de întrerupere)
autorizarea obiect necesară 414

comanda RMVBNDIRE (Înlăturare intrare director de legături)
auditare obiect 452

Comanda RMVBNDIRE (Remove Binding Directory Entry - Înlăturare intrare director de legare)
autorizarea obiect necesară 315

- comanda RMVCFGLE (Înlăturare intrare listă de configurație)
auditare obiect 452
- Comanda RMVCFGLE (Remove Configuration List Entries - Înlăturare intrări în lista de configurare)
autorizarea obiect necesară 322
- comanda RMVCLUNODE
autorizarea obiect necesară 318
- comanda RMVCMNE (Înlăturare intrare comunicații)
auditare obiect 493
- Comanda RMVCMNE (Remove Communications Entry - Înlăturare intrare comunicații)
autorizarea obiect necesară 432
- comanda RMVCNNLE (Înlăturare intrare listă de conexiuni)
auditare obiect 455
- Comanda RMVCOMSNMP (Înlăturare comunitate pentru SNMP)
autorizarea obiect necesară 438
- comanda RMVCRQD (Înlăturare activitate de modificare descriere cerere)
auditare obiect 454
- Comanda RMVCRQDA (Remove Change Request Description - Înlăturare descriere cerere de modificare)
autorizări obiect necesare 315
- comanda RMVCRSDMNK (Remove Cross Domain Key - Înlăturare cheie de traversare domeniu)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVCRSDMNK (Remove Cross Domain Key - Înlăturare cheie de traversare domeniu)
autorizări obiect necesare 325
- comanda RMVDEVDMNE
autorizarea obiect necesară 319
- comanda RMVDIR (Înlăturare director)
auditare obiect 460
- Comanda RMVDIR (Remove Directory - Înlăturare director)
autorizarea obiect necesară 357
- Comanda RMVDIRE (Înlăturare intrare director)
descriere 276
- Comanda RMVDIRE (Remove Directory Entry - Înlăturare intrare director)
autorizarea obiect necesară 329
- Comanda RMVDIRSHD (Remove Directory Shadow System - Înlăturare sistem umbră director)
autorizarea obiect necesară 329
- Comanda RMVDLOAUT (Înlăturare autorizare obiect de bibliotecă de documente)
descriere 275
- comanda RMVDLOAUT (Înlăturare autorizare obiect de bibliotecă de documente)
auditare obiect 465
autorizări obiect necesare 333
- Comanda RMVDSTLE (Remove Distribution List Entry - Înlăturare intrare din lista de distribuție)
autorizarea obiect necesară 331
- comanda RMVDSTQ (Remove Distribution Queue - Înlăturare coadă de distribuție)
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVDSTQ (Remove Distribution Queue - Înlăturare coadă de distribuție)
autorizarea obiect necesară 331
- Comanda RMVDSTRTE (Remove Distribution Route - Înlăturare rută distribuție)
autorizarea obiect necesară 331
profiluri utilizator autorizate livrat de IBM 294
- comanda RMVDSTSYSN (Remove Distribution Secondary System Name - Înlăturare nume sistem secundar de distribuție)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVDSTSYSN (Remove Distribution Secondary System Name - Înlăturare nume sistem secundar de distribuție)
autorizări obiect necesare 331
- Comanda RMVEMLCFGE (Remove Emulation Configuration Entry - Înlăturare intrare configurație de emulare)
autorizări obiect necesare 329
- Comanda RMVENVVAR (Remove Environment Variable - Înlăturare variabilă de mediu)
autorizarea obiect necesară 336
- Comanda RMVEWCBCE (Remove Extended Wireless Controller Bar Code Entry - Înlăturare intrare cod de bare controler de comunicație fără fir extinsă)
autorizarea obiect necesară 336
- Comanda RMVEWCPTCE (Remove Extended Wireless Controller PTC Code Entry - Înlăturare intrare PTC controler de comunicație fără fir extinsă)
autorizarea obiect necesară 337
- comanda RMVEXITPGM (Adăugare program ieșire)
auditare obiect 468
- Comanda RMVEXITPGM (Remove Exit Program - Înlăturare program de ieșire)
autorizarea obiect necesară 418
- comanda RMVEXITPGM (Remove Exit Program - Înlăturare program ieșire)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVFCTE (Înlăturare intrare table de control formulare)
autorizarea obiect necesară 422
- comanda RMVFTRACNE (Înlăturare intrare acțiune filtru)
auditare obiect 472
- Comanda RMVFTRACNE (Remove Filter Action Entry - Înlăturare intrare acțiune filtru)
autorizarea obiect necesară 344
- comanda RMVFTRSLTE (Înlăturare intrare selecție filtru)
auditare obiect 472
- Comanda RMVFTRSLTE (Remove Filter Selection Entry - Înlăturare intrare selecție filtru)
autorizarea obiect necesară 344
- Comanda RMVICFDEVE (Remove Intersystem Communications Function Program Device Entry - Înlăturare intrare dispozitiv program de funcționare a comunicațiilor intersistem)
autorizarea obiect necesară 342
- comanda RMVIMGCLGE
autorizarea obiect necesară 347
- Comanda RMVIPSIFC (Remove IP over SNA Interface - Înlăturare IP pe interfață SNA)
autorizarea obiect necesară 312
- Comanda RMVIPSLOC (Remove IP over SNA Location - Înlăturare IP pe locație SNA)
autorizarea obiect necesară 312
- Comanda RMVIPS RTE (Remove IP over SNA Route - Înlăturare IP pe rută SNA)
autorizarea obiect necesară 312
- comanda RMVJOBQE (Înlăturare intrare coadă joburi)
auditare obiect 475, 493
- Comanda RMVJOBQE (Remove Job Queue Entry - Înlăturare intrare coadă de joburi)
autorizarea obiect necesară 432
- comanda RMVJOBSCDE (Înlăturare intrare planificare job)
auditare obiect 475
- Comanda RMVJOBSCDE (Remove Job Schedule Entry - Înlăturare intrare planificare job)
autorizarea obiect necesară 372
- comanda RMVJRNCHG (Înlăturare schimbări jurnalizate)
auditare obiect 448, 477
- comanda RMVJRNCHG (Remove Journalized Changes - Înlăturare modificări jurnalizate)
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVJRNCHG (Remove Journalized Changes - Înlăturare modificări jurnalizate)
autorizarea obiect necesară 374
- comanda RMVLANADP (Remove LAN Adapter - Înlăturare adaptor LAN)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVLANADPI (Înlăturare informații adaptor LAN)
autorizarea obiect necesară 389
- Comanda RMVLANADPT (Înlăturare adaptor LAN)
autorizarea obiect necesară 389
- comanda RMVLIBLE (Remove Library List Entry - Înlăturare intrare lista de bibliotecii)
folosire 183
- comanda RMVLIBLE (Remove Library List Entry - Înlăturare intrare lista de bibliotecii)
183
- Comanda RMVLICKEY (Remove License Key - Înlăturare cheie de licență)
autorizarea obiect necesară 386
- comanda RMVLNK (Înlăturare legătură)
auditare obiect 495, 500, 501

- Comanda RMVLNK (Remove Link - Înlăturare legătură)
autorizarea obiect necesară 358
- comanda RMVM (Înlăturare membru)
auditare obiect 471
- Comanda RMVM (Remove Member - Înlăturare membru)
autorizarea obiect necesară 342
- comanda RMVMFS (Remove Mounted File System - Înlăturare sistem de fișiere montat)
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVMFS (Remove Mounted File System - Înlăturare sistem de fișiere montat)
autorizarea obiect necesară 396
- comanda RMVMSG (Înlăturare mesaj)
auditare obiect 482
- Comanda RMVMSG (Remove Message - Înlăturare mesaj)
autorizarea obiect necesară 391
- comanda RMVMSGD (Înlăturare descriere mesaj)
auditare obiect 481
- Comanda RMVMSGD (Remove Message Description - Înlăturare descriere mesaj)
autorizarea obiect necesară 392
- comanda RMVNETJOB (Remove Network Job Entry - Înlăturare intrare job rețea)
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVNETJOB (Remove Network Job Entry - Înlăturare intrare job rețea)
autorizarea obiect necesară 396
- Comanda RMVNETTBL (Înlăturare intrare tabel rețea)
autorizarea obiect necesară 438
- comanda RMVNODLE (Înlăturare intrare listă de noduri)
auditare obiect 483
- Comanda RMVNODLE (Remove Node List Entry - Înlăturare intrare din lista de noduri)
autorizarea obiect necesară 399
- Comanda RMVNSSTGL (Remove Network Server Storage Link - Înlăturare legătură spațiu de stocare server de rețea)
autorizarea obiect necesară 398
- comanda RMVOPTCTG (Remove Optical Cartridge - Înlăturare cartuș optic)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVOPTCTG (Remove Optical Cartridge - Înlăturare cartuș optic)
autorizarea obiect necesară 403
- comanda RMVOPTSVR (Înlăturare server optic)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVOPTSVR (Remove Optical Server - Înlăturare server optic)
autorizarea obiect necesară 403
- comanda RMVPEXDFN (Înlăturare definiție Performance Explorer)
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVPEXDFN (Remove Performance Explorer Definition - Înlăturare definiție explorare performanță)
autorizări obiect necesare 410
- comanda RMVPEXFTR
profiluri utilizator livrat de IBM autorizate 294
- comanda RMVPFCST (Înlăturare constrângere fișier fizic)
auditare obiect 471
- Comanda RMVPFCST (Remove Physical File Constraint - Înlăturare constrângere fișier fizic)
autorizarea obiect necesară 342
- comanda RMVPFTGR (Înlăturare declanșator fișier fizic)
auditare obiect 471
- Comanda RMVPFTGR (Remove Physical File Trigger - Înlăturare declanșator fișier fizic)
autorizarea obiect necesară 342
- Comanda RMVPGM (Înlăturare program)
autorizarea obiect necesară 414
- comanda RMVPJE (Înlăturare intrare job prestart)
auditare obiect 493
- Comanda RMVPJE (Remove Prestart Job Entry - Înlăturare intrare job prestart)
autorizarea obiect necesară 432
- comanda RMVPTF (Remove Program Temporary Fix - Înlăturare corecție temporară program)
profiluri utilizator livrat de IBM autorizate 294
- Comanda RMVPTF (Remove Program Temporary Fix - Înlăturare corecție temporară program)
autorizarea obiect necesară 425
- Comanda RMVRDBDIRE (Înlăturare intrare director baze de date relaționale)
autorizarea obiect necesară 419
- Comanda RMVRJECMNE (Înlăturare intrare comunicații RJE)
autorizarea obiect necesară 422
- Comanda RMVRJERDRE (Înlăturare intrare cititor RJE)
autorizarea obiect necesară 422
- Comanda RMVRJEWTR (Înlăturare intrare scriitor RJE)
autorizarea obiect necesară 422
- comanda RMVRMTJRN (Înlăturare jurnal la distanță)
auditare obiect 477
- comanda RMVRMTPTF (Înlăturare corecție temporară program la distanță)
profiluri utilizator livrat de IBM autorizate 294
- comanda RMVRPYLE (Înlăturare intrare listă răspuns)
auditare obiect 492
profiluri utilizator autorizate livrat de IBM 294
- Comanda RMVRPYLE (Remove Reply List Entry - Înlăturare intrare listă de replici)
autorizarea obiect necesară 433
- comanda RMVRTGE (Înlăturare intrare rutare)
auditare obiect 493
- Comanda RMVRTGE (Remove Routing Entry - Înlăturare intrare rutare)
autorizarea obiect necesară 433
- comanda RMVSCIDX (Înlăturare intrare index de căutare)
auditare obiect 494
- Comanda RMVSCIDX (Remove Search Index Entry - Înlăturare intrare index de căutare)
autorizarea obiect necesară 367
- Comanda RMVSOCE (Înlăturare intrare sferă de control)
autorizarea obiect necesară 429
- Comanda RMVSVRAUTE (Înlăturare intrare autentificare server)
autorizarea obiect necesară 424
- Comanda RMVTAPCTG (Remove Tape Cartridge - Înlăturare cartuș bandă)
autorizarea obiect necesară 390
- Comanda RMVTCPHTE (Înlăturare intrare tabel gazdă)
autorizarea obiect necesară 438
- Comanda RMVTCPIFC (Înlăturare interfață TCP/IP)
autorizarea obiect necesară 438
- Comanda RMVTCPPORT (Înlăturare intrare port TCP/IP)
autorizări obiect necesare 438
- Comanda RMVTCPRSI (Înlăturare informații sistem la distanță TCP/IP)
autorizarea obiect necesară 438
obiect autorizare cerută 438
- Comanda RMVTCPRTE (Înlăturare rută TCP/IP)
autorizarea obiect necesară 438
- Comanda RMVTRC (Înlăturare urmă)
autorizarea obiect necesară 414
- comanda RMVWSE (Remove Workstation Entry - Înlăturare intrare stație de lucru)
auditare obiect 493
autorizarea obiect necesară 433
- comanda RNM (Redenumire)
auditare obiect 460, 495, 500, 501
- Comanda RNM (Rename - Redenumire)
autorizarea obiect necesară 358
- comanda RNMCNLE (Redenumire intrare listă de conexiuni)
auditare obiect 455
- Comanda RNMDIRE (Rename Directory Entry - Redenumire intrare director)
autorizarea obiect necesară 329
- Comanda RNMDKT (Rename Diskette - Redenumire dischetă)
autorizarea obiect necesară 390
- comanda RNMDLO (Înlăturare obiect bibliotecă documente)
auditare obiect 465
- Comanda RNMDLO (Rename Document Library Object - Redenumire obiect bibliotecă de documente)
autorizări obiect necesare 333
- Comanda RNMDSTL (Rename Distribution List - Redenumire listă de distribuție)
autorizarea obiect necesară 331
- comanda RNMM (Redenumire membru)
auditare obiect 471

Comanda RNMM (Rename Member - Redenumire membru)
 autorizarea obiect necesară 342

comanda RNMOBJ (Redenumire obiect)
 auditare obiect 449, 478, 502

Comanda RNMOBJ (Rename Object - Redenumire obiect)
 autorizarea obiect necesară 305

Comanda RNMTCPHTE (Redenumire intrare tabel gazdă TCP/IP)
 autorizarea obiect necesară 438

Comanda ROLLBACK (Rollback - Derulare înapoi)
 autorizarea obiect necesară 320

comanda RPLDOC (Înlocuire document)
 auditare obiect 465

Comanda RPLDOC (Replace Document - Înlocuire document)
 autorizarea obiect necesară 333

Comanda RRTJOB (Reroute Job - Rerutare job)
 autorizarea obiect necesară 368

Comanda RSMBKP (Continuare punct de întrerupere)
 autorizarea obiect necesară 414

comanda RSMCTLCY (Continuare recuperare controler)
 auditare obiect 457

Comanda RSMCTLCY (Resume Controller Recovery - Continuare recuperare controler)
 autorizarea obiect necesară 324

comanda RSMDEVRCY (Reluare recuperare dispozitiv)
 auditare obiect 458

Comanda RSMDEVRCY (Resume Device Recovery - Continuare recuperare dispozitiv)
 autorizarea obiect necesară 328

comanda RSMLINRCY (Reluare recuperare linie)
 auditare obiect 479

Comanda RSMLINRCY (Resume Line Recovery - Continuare recuperare linie)
 autorizarea obiect necesară 389

comanda RSMNWIRCY (Reluare recuperare interfață de rețea)
 auditare obiect 484

comanda RST (Restaurare)
 auditare obiect 449, 460, 495, 500, 501
 profiluri utilizator livrat de IBM autorizate 294

Comanda RST (Restore - Restaurare)
 autorizarea obiect necesară 359

Comanda RSTAUT (Restaurare autorizare)
 descriere 275

Comanda RSTAUT (Restore Authority - Restaurare autorizare)
 folosind 223
 intrare jurnal auditare (QAUDJRN) 245
 procedură 224
 rol în restaurarea securității 219

comanda RSTAUT (Restore Authority)
 autorizarea obiect necesară 441
 profiluri utilizator livrat de IBM autorizate 294

comanda RSTCFG (Restaurare configurație)
 auditare obiect 449

comanda RSTCFG (Restore Configuration - Restaurare configurație)
 profiluri utilizator livrat de IBM autorizate 294

Comanda RSTCFG (Restore Configuration - Restaurare configurație)
 autorizarea obiect necesară 321

comanda RSTDLO (Restaurare obiect bibliotecă documente)
 auditare obiect 465

comanda RSTDLO (Restore Document Library Object - Restaurare obiect bibliotecă de documente)
 autorizarea obiect necesară 333
 profiluri utilizator autorizate livrat de IBM 294

Comanda RSTDLO (Restore Document Library Object - Salvare obiect bibliotecă document) 219

comanda RSTLIB (Restaurare bibliotecă)
 auditare obiect 449

comanda RSTLIB (Restore Library - Restaurare bibliotecă)
 profiluri utilizator livrat de IBM autorizate 294

Comanda RSTLIB (Restore Library - Restaurare bibliotecă) 219
 autorizări obiect necesare 384

Comanda RSTLIB (Restore Library - Salvare bibliotecă) 219

comanda RSTLICPGM (Restaurare program cu licență)
 auditare obiect 449

comanda RSTLICPGM (Restore Licensed Program - Restaurare program cu licență)
 profiluri utilizator autorizate livrat de IBM 294

Comanda RSTLICPGM (Restore Licensed Program - Restaurare program cu licență)
 autorizarea obiect necesară 387

comanda RSTLICPGM (Restore Licensed Program - Restaurare program licențiat)
 recomandări 225
 riscuri de securitate 225

comanda RSTOBJ (Restaurare obiect)
 auditare obiect 449

comanda RSTOBJ (Restore Object - Restaurare obiect)
 profiluri utilizator livrat de IBM autorizate 294

Comanda RSTOBJ (Restore Object - Restaurare obiect)
 autorizarea obiect necesară 306
 folosind 219

comanda RSTS36F (Restore System/36 File - Restaurare fișier System/36)
 profiluri utilizator livrat de IBM autorizate 294

Comanda RSTS36F (Restore System/36 File - Restaurare fișier System/36)
 autorizarea obiect necesară 342, 435

comanda RSTS36FLR (Restore System/36 Folder - Restaurare folder System/36)
 profiluri utilizator autorizate livrat de IBM 294

Comanda RSTS36FLR (Restore System/36 Folder - Restaurare folder System/36)
 autorizări obiect necesare 333, 435

comanda RSTS36LIBM (Restore System/36 Library Members - Restaurare membrii bibliotecă System/36)
 profiluri utilizator livrat de IBM autorizate 294

Comanda RSTS36LIBM (Restore System/36 Library Members - Restaurare membrii bibliotecă System/36)
 autorizarea obiect necesară 384, 435

comanda RSTS38AUT (Restore System/38 Authority - Restaurare autorizare System/38)
 profiluri utilizator autorizate livrat de IBM 294

Comanda RSTS38AUT (Restore System/38 Authority - Restaurare autorizare System/38)
 autorizări obiect necesare 393

comanda RSTSHF (Restaurare raft de cărți)
 auditare obiect 465

comanda RSTUSFCNR (Restore USF Container - Restaurare container USF)
 profiluri utilizator livrat de IBM autorizate 294

comanda RSTUSRPRF (Restaurare profiluri utilizator)
 auditare obiect 503

Comanda RSTUSRPRF (Restaurare profiluri utilizator)
 autorizarea obiect necesară 442
 descriere 275
 profiluri utilizator livrat de IBM autorizate 295

comanda RSTUSRPRF (Restore User Profiles)
 descriere 219

comanda RTVAUTLE (Extragere intrare listă de autorizații)
 auditare obiect 451

Comanda RTVAUTLE (Extragere intrare listă de autorizații)
 descriere 271

Comanda RTVAUTLE (Retrieve Authorization List Entry - Extragere intrare din lista de autorizații)
 autorizarea obiect necesară 314

Comanda RTVBCKUP (Retrieve Backup Options - Extragere opțiuni salvare de rezervă)
 autorizarea obiect necesară 401

comanda RTVBNDSRC (Extragere sursă binder)
 auditare obiect 452

comanda RTVBNDSRC (Extragere sursă legătură)
 auditare obiect 481, 498

Comanda RTVBNDSRC (Retrieve Binder Source - Extragere sursă binder)
 *SRVPGM, extrăgând exporturi din 394
 autorizarea obiect necesară 394

comanda RTVCFGSRC (Extragere sursă configurație)
 auditare obiect 455, 456, 457, 458, 479, 484, 485

- Comanda RTVCFGSRG (Retrieve Configuration Source - Extragere sursă configurație)
 autorizări obiect necesare 321
- comanda RTVCFGSTS (Extragere stare configurație)
 auditare obiect 457, 458, 479, 484, 485
- Comanda RTVCFGSTS (Retrieve Configuration Status - Extragere stare configurație)
 autorizarea obiect necesară 321
- comanda RTVCLDSRC (Extragere sursă C Locale)
 auditare obiect 453
- Comanda RTVCLNUP (Retrieve Cleanup - Extragere curățare)
 autorizarea obiect necesară 401
- comanda RTVCLSRC (Extragere sursă CL)
 auditare obiect 487
- Comanda RTVCLSRC (Extragere sursă CL)
 autorizarea obiect necesară 414
- comanda RTVCURDIR (Extragere director curent)
 auditare obiect 459
- Comanda RTVCURDIR (Retrieve Current Directory - Extragere director curent)
 autorizări obiect necesare 360
- Comanda RTVDLONAM (Retrieve Document Library Object Name - Extragere nume obiect bibliotecă document)
 autorizări obiect necesare 333
- comanda RTVDOC (Extragere document)
 auditare obiect 463, 465
- Comanda RTVDOC (Retrieve Document - Extragere document)
 autorizarea obiect necesară 333
- Comanda RTVDSKINF (Retrieve Disk Activity Information - Extragere informații activitate disc)
 autorizarea obiect necesară 401
 profiluri utilizator autorizate livrat de IBM 295
- comanda RTVDTAARA (Extragere zonă de date)
 auditare obiect 466
- Comanda RTVDTAARA (Retrieve Data Area - Extragere zonă de date)
 autorizarea obiect necesară 325
- Comanda RTVGRPA (Extragere atribute grup)
 autorizarea obiect necesară 433
- Comanda RTVIMGLG
 autorizarea obiect necesară 347
 profiluri utilizator livrat de IBM autorizate 295
- Comanda RTVJOBA (Retrieve Job Attributes - Extragere atribute job)
 autorizarea obiect necesară 368
- comanda RTVJRNE (Extragere intrare jurnal)
 auditare obiect 476
- Comanda RTVJRNE (Retrieve Journal Entry - Extragere intrare jurnal)
 autorizarea obiect necesară 375
- Comanda RTVLIBD (Retrieve Library Description - Extragere descriere bibliotecă)
 autorizarea obiect necesară 384
- comanda RTVMBRD (Extragere descriere membru)
 auditare obiect 471
- Comanda RTVMBRD (Retrieve Member Description - Extragere descriere membru)
 autorizarea obiect necesară 342
- comanda RTVMSG (Extragere mesaj)
 auditare obiect 481
- Comanda RTVNETA (Retrieve Network Attributes - Extragere atribute rețea)
 autorizarea obiect necesară 396
- comanda RTVOBJD (Extragere descriere obiect)
 auditare obiect 450
- Comanda RTVOBJD (Retrieve Object Description - Extragere descriere obiect)
 autorizarea obiect necesară 306
- Comanda RTVPDGPFR (Extragere profil grup descriptor tipărire)
 autorizarea obiect necesară 411
- comanda RTVPRD (Retrieve Product - Extragere produs)
 profiluri utilizator livrat de IBM autorizate 295
- comanda RTVPPTF (Retrieve PTF - Extragere PTF)
 profiluri utilizator livrat de IBM autorizate 295
- Comanda RTVPWRSCDE (Retrieve Power On/Off Schedule Entry - Extragere intrare planificare alimentare On/Off)
 autorizarea obiect necesară 401
- comanda RTVQMFOM (Extragere formular Query Management)
 auditare obiect 491
- Comanda RTVQMFOM (Retragere formular Query Management)
 autorizări obiect necesare 416
- comanda RTVQMQR (Extragere cerere Query Management)
 auditare obiect 490, 491
- Comanda RTVQMQR (Retrieve Query Management Query) command
 autorizări obiect necesare 416
- comanda RTVS36A (Extragere atribute System/36)
 auditare obiect 502
- Comanda RTVS36A (Retrieve System/36 Attributes - Extragere atribute System/36)
 autorizarea obiect necesară 435
- comanda RTVSMGOBJ (Retrieve Systems Management Object - Extragere obiect gestiune sisteme)
 profiluri utilizator livrat de IBM autorizate 295
- Comanda RTVSYSVAL (Extragere valoare sistem)
 autorizarea obiect necesară 433
- comanda RTVUSRPRF (Extragere profil utilizator)
 auditare obiect 504
 folosind 107
- Comanda RTVUSRPRF (Extragere profil utilizator)
 descriere 274
- Comanda RTVUSRPRF (Retrieve User Profile - Extragere profil utilizator)
 autorizarea obiect necesară 442
- comanda RTVWSCST (Retrieve Workstation Customizing Object - Extragere obiect de personalizare stație de lucru)
 auditare obiect 505
 autorizarea obiect necesară 443
- Comanda RUNBACKUP (Run Backup - Rulare salvare de rezervă)
 autorizarea obiect necesară 401
- comanda RUNLPDA (Rulare LPDA-2)
 auditare obiect 478
- comanda RUNLPDA (Run LPDA-2 - Rulare LPDA-2)
 profiluri utilizator livrat de IBM autorizate 295
- Comanda RUNLPDA (Run LPDA-2 - Rulare LPDA-2)
 autorizarea obiect necesară 425
- comanda RUNQRY (Rulare cerere)
 auditare obiect 491
- Comanda RUNQRY (Run Query - Rulare interogare)
 autorizarea obiect necesară 416
- comanda RUNSMGCMD (Run Systems Management Command - Rulare comandă gestiune sisteme)
 profiluri utilizator autorizate livrat de IBM 295
- comanda RUNSMGOBJ (Run Systems Management Object - Rulare obiect gestiune sisteme)
 profiluri utilizator autorizate livrat de IBM 295
- Comanda RUNSQLSTM (Run Structured Query Language Statement - Rulare instrucțiune limbaj de interogare structurat)
 autorizări obiect necesare 382
- comanda RVKACCAUT (Revocare autorizare cod acces)
 auditare obiect 465
- Comanda RVKACCAUT (Revoke Access Code Authority - Revocare autorizare cod acces)
 autorizarea obiect necesară 400
- comanda RVKOBJAUT (Revocare autorizare obiect)
 auditare obiect 449
- Comanda RVKOBJAUT (Revocare autorizare obiect)
 descriere 272
- Comanda RVKOBJAUT (Revoke Object Authority - Revocare autorizare obiect) 138
 autorizarea obiect necesară 307
 folosire 146
- Comanda RVKPUBAUT
 detalii 627
- Comanda RVKPUBAUT (Revocare autorizare publică)
 profiluri utilizator livrat de IBM autorizate 295
- Comanda RVKPUBAUT (Revocare autorizare publică)
 descriere 625

Comanda RVPUBAUT (Revoke Public Authority - Revocare autorizare publică) autorizarea obiect necesară 306

comanda RVKUSRPMN (Revocare permisiune utilizator) auditare obiect 465 autorizarea obiect necesară 400

Comanda RVKUSRPMN (Revocare permisiune utilizator) descriere 275

Comanda RVKWSOAUT (Revoke Workstation Object Authority - Revocare autorizare obiect pentru stație de lucru) autorizări obiect necesare 345

Comanda Salvare date de securitate (SAVSECDTA) 275

Comanda Salvare obiect (SAVOBJ) 219, 260

Comanda Salvare sistem (SAVSYS) 275

comanda SAV (Salvare) auditare obiect 447, 459, 499, 501

comanda SAVAPARDTA (Save APAR Data - Salvare date APAR) profiluri utilizator livrat de IBM autorizate 295

Comanda SAVAPARDTA (Save APAR Data - Salvare date APAR) autorizarea obiect necesară 425

comanda SAVCFG (Salvare configurație) auditare obiect 457, 478, 483, 484

Comanda SAVCFG (Save Configuration - Salvare configurație) autorizarea obiect necesară 321

comanda SAVCHGOBJ (Salvare obiect modificat) auditare obiect 447

Comanda SAVCHGOBJ (Save Changed Object - Salvare obiect modificat) autorizarea obiect necesară 307

comanda SAVDLO (Salvare obiect bibliotecă documente) auditare obiect 447, 463 folosind 219

Comanda SAVDLO (Save Document Library Object - Salvare obiect bibliotecă de documente) autorizarea obiect necesară 334

comanda Save Document Library Object (SAVDLO) 219

comanda Save System (SAVSYS) 219

Comanda SAVLB (Save Library - Salvare bibliotecă) 219

comanda SAVLIB (Salvare bibliotecă) auditare obiect 447

Comanda SAVLIB (Save Library - Salvare bibliotecă) autorizări obiect necesare 385 folosind 219

comanda SAVLICPGM (Salvare program licențiat) auditare obiect 447

comanda SAVLICPGM (Save Licensed Program - Salvare program cu licență) profiluri utilizator livrat de IBM autorizate 295

Comanda SAVLICPGM (Save Licensed Program - Salvare program cu licență) autorizarea obiect necesară 387

comanda SAVOBJ (Salvare obiect) auditare obiect 447

Comanda SAVOBJ (Save Object - Salvare obiect) autorizări obiect necesare 307 folosind 219 salvare receptor jurnal audit 260

Comanda SAVRSOBJ (Save Restore Object - Salvare restaurare obiect) autorizarea obiect necesară 308

Comanda SAVRSTCFG (Save Restore Configuration - Salvare restaurare configurație) autorizări obiect necesare 321

Comanda SAVRSTCHG (Save Restore Change - Salvare modificare restaurată) autorizarea obiect necesară 308

Comanda SAVRSTDLO (Save Restore Document Library Object - Salvare obiect bibliotecă de documente) autorizarea obiect necesară 334

Comanda SAVRSTLIB (Save Restore Library - Salvare restaurare bibliotecă) autorizarea obiect necesară 385

Comanda SAVS36F (Salvare fișier System/36) autorizarea obiect necesară 343, 435

Comanda SAVS36LIBM (Save System/36 Library Members - Salvare membri bibliotecă System/36) autorizarea obiect necesară 343, 385

comanda SAVSAVFDTA (Salvare date fișier de salvare) auditare obiect 447 autorizarea obiect necesară 343

Comanda SAVSECDTA (Salvare date de securitate) descriere 275

Comanda SAVSECDTA (Save Security Data - Salvare date de securitate) autorizarea obiect necesară 442 folosind 219

Comanda SAVSEDTA (Save Security Data - Salvare date de securitate) 219

comanda SAVSHF (Salvare raft de cărți) auditare obiect 447, 463

comanda SAVSTG (Salvare spațiu de stocare) auditare obiect 450

Comanda SAVSTG (Save Storage - Salvare spațiu de stocare) autorizarea obiect necesară 308

Comanda SAVSYS (Salvare sistem) descriere 275

Comanda SAVSYS (Save System - Salvare sistem) autorizarea obiect necesară 308 folosind 219

comanda SBMCRQ (Lansare modificare cerere) auditare obiect 453

Comanda SBMDBJOB (Submit Database Jobs - Lansare joburi bază de date) autorizarea obiect necesară 368

Comanda SBMDKTJOB (Submit Diskette Jobs - Lansare joburi dischetă) autorizarea obiect necesară 369

comanda SBMFNCJOB (Lansare job Finanțe) profiluri utilizator livrat de IBM autorizate 295

Comanda SBMFNCJOB (Submit Finance Job - Lansare job financiar) autorizarea obiect necesară 344

comanda SBMJOB (Submit Job - Lansare job) 176 verificare autorizare 176

Comanda SBMJOB (Submit Job - Lansare job) autorizarea obiect necesară 369 meniu SECBATCH 620

Comanda SBMNETJOB (Submit Network Job - Lansare job rețea) autorizarea obiect necesară 369

Comanda SBMNWSCMD (Submit Network Server Command - Lansare comandă server de rețea) autorizări obiect necesare 398

comanda SBMNWSCMD (Submit Network Server Command - Lansare comandă server rețea) profiluri utilizator autorizate livrat de IBM 295

Comanda SBMRJEJOB (Lansare Job RJE) autorizarea obiect necesară 422

Comanda SBMRMTCMD (Submit Remote Command - Lansare comandă la distanță) autorizarea obiect necesară 320

Comanda Schimbare job (CHGJOB) autorizare adoptată 130

Comanda Schimbare proprietar (CHGOWN) 272

comanda Setare program Attn (SETATNPGM) 86

Comanda SETATNPGM (Setare program Attention) autorizarea obiect necesară 414

comanda SETATNPGM (Setare program Attn) inițializare job 86

Comanda SETCSTDTA (Set Customization Data - Setare personalizare date) autorizări obiect necesare 345

Comanda SETMSTK (Set Master Key - Setare cheie master) autorizarea obiect necesară 325

comanda SETMSTK (Set Master Key - Setare cheie primară) profiluri utilizator livrat de IBM autorizate 295

Comanda SETOBJACC (Set Object Access - Setare acces obiect) autorizarea obiect necesară 308

Comanda SETPGMINF (Setare informații program) autorizări obiect necesare 414

Comanda SETTAPCGY (Set Tape Category - Setare categorie bandă) autorizarea obiect necesară 390

Comanda SETVTTBL (Setare tabele de traducere VT) autorizarea obiect necesară 437

Comanda SIGNOFF (Anulare semnare) autorizarea obiect necesară 433

Comanda SLTCMD (Select Command - Selectare comandă) autorizarea obiect necesară 320

- Comanda SNDBRKMMSG (Send Break Message - Trimitere mesaj cu întrerupere) autorizarea obiect necesară 392
- comanda SNDDOC (Trimitere document) auditare obiect 463
- Comanda SNDDST (Send Distribution - Trimitere distribuție) autorizarea obiect necesară 331
- comanda SNDDST (Trimitere distribuție) auditare obiect 463
- Comanda SNDDSTQ (Send Distribution Queue - Trimitere coadă de distribuție) autorizarea obiect necesară 331
- comanda SNDDSTQ (Send Distribution Queue - Trimitere coadă distribuție) profiluri utilizator livrat de IBM autorizate 295
- comanda SNDDTAARA (Trimitere zonă de date) auditare obiect 466
- Comanda SNDEMLIGC (Send DBCS 3270PC Emulation Code - Trimitere cod de emulare DBCS 3270PC) autorizarea obiect necesară 329
- Comanda SNDFNCIMG (Send Finance Diskette Image - Trimitere imagine dischetă financiar) autorizarea obiect necesară 344
- Comanda SNDJRNE (Send Journal Entry - Trimitere intrare jurnal) 258 autorizarea obiect necesară 375
- comanda SNDJRNE (Trimitere intrare jurnal) auditare obiect 477
- Comanda SNDMGRDTA (Send Migration Data - Trimitere date de migrare) autorizarea obiect necesară 393
- Comanda SNDMSG (Send Message - Trimitere mesaj) autorizarea obiect necesară 392
- Comanda SNDNETF (Send Network File - Trimitere fișier rețea) autorizarea obiect necesară 396
- Comanda SNDNETMSG (Send Network Message - Trimitere mesaj rețea) autorizarea obiect necesară 396
- comanda SNDNETSPLF (Send Network Spooled File - Trimitere fișier spool de rețea) 186 parametrii coadă de ieșire 186
- Comanda SNDNETSPLF (Send Network Spooled File - Trimitere fișier spool de rețea) autorizarea obiect necesară 430
- comanda SNDNETSPLF (Trimitere pe rețea a fișierului spool) auditare acțiune 496 auditare obiect 486
- Comanda SNDNWSMSG (Send Network Server Message - Trimitere mesaj server de rețea) autorizarea obiect necesară 398
- Comanda SNDPGMMSG (Send Program Message - Trimitere mesaj program) autorizarea obiect necesară 392
- comanda SNDPRD (Send Product - Trimitere produs) profiluri utilizator livrat de IBM autorizate 295
- comanda SNDPTF (Send PTF - Trimitere PTF) profiluri utilizator livrat de IBM autorizate 295
- comanda SNDPTFORD (Send Program Temporary Fix Order - Trimitere ordin de corecție temporară program) profiluri utilizator autorizate livrat de IBM 295
- Comanda SNDPTFORD (Send Program Temporary Fix Order - Trimitere ordin de corecție temporară program) autorizarea obiect necesară 425
- Comanda SNDRJECMD (Trimiere comandă RJE) autorizarea obiect necesară 422
- Comanda SNDRJECMD (Trimitere RJE) autorizarea obiect necesară 422
- Comanda SNDRPY (Send Reply - Trimitere replică) autorizarea obiect necesară 392
- comanda SNDRPY (Trimitere răspuns) auditare obiect 483
- comanda SNDSMGOBJ (Send Systems Management Object - Trimitere obiect gestiune sisteme) profiluri utilizator autorizate livrat de IBM 295
- comanda SNDSRVRQS (Send Service Request - Trimitere cerere service) profiluri utilizator livrat de IBM autorizate 295
- Comanda SNDSRVRQS (Send Service Request - Trimitere cerere service) autorizarea obiect necesară 425
- Comanda SNDTCPSPLF (Send TCP Spooled File - Trimitere fișier spool TCP) autorizarea obiect necesară 431
- Comanda SNDTCPSPLF (Send TCP/IP Spooled File - Trimitere fișier spool TCP/IP) autorizarea obiect necesară 437
- comanda SNDTCPSPLF (Trimitere prin TCP/IP a fișierului spool) auditare acțiune 496 auditare obiect 505
- Comanda SNDUSRMSG (Send User Message - Trimitere mesaj utilizator) autorizarea obiect necesară 392
- Comanda STATFS (Display Mounted File System Information - Afișare informații sistem de fișiere montat) autorizarea obiect necesară 396
- Comanda STRAPF (Start Advanced Printer Function - Pornire funcție avansată de printare) autorizări obiect necesare 312, 343
- Comanda STRASPBAL 328
- comanda STRBEST (Start BEST/1 - Pornire BEST/1) profiluri utilizator livrat de IBM autorizate 295
- Comanda STRBEST (Start Best/1-400 Capacity Planner - Pornire planificator capacitate Best/1-400) autorizări obiect necesare 410
- Comanda STRBGU (Start Business Graphics Utility - Pornire utilitar grafice de afaceri) autorizarea obiect necesară 312
- Comanda STRCBLDBG (Pornire depanare COBOL) autorizarea obiect necesară 382, 414
- Comanda STRCGU (Start CGU - Pornire GCU) autorizarea obiect necesară 335
- Comanda STRCLNUP (Start Cleanup - Pornire curățare) autorizarea obiect necesară 401
- comanda STRCLUNOD autorizarea obiect necesară 319
- comanda STRCMNTRC (Start Communications Trace - Pornire urmărire comunicații) profiluri utilizator autorizate livrat de IBM 295
- Comanda STRCMNTRC (Start Communications Trace - Pornire urmărire comunicații) autorizări obiect necesare 426
- Comanda STRCMTCTL (Start Commitment Control - Pornire control comitere) autorizări obiect necesare 320
- Comanda STRCPYSCN (Pornire copiere ecran) autorizarea obiect necesară 426
- comanda STRCSP (Pornire utilitare CSP/AE) auditare obiect 488
- comanda STRDBG (Pornire depanare) auditare obiect 469, 487
- comanda STRDBG (Start Debug - Pornire depanare) profiluri utilizator livrat de IBM autorizate 295
- Comanda STRDBG (Start Debug - Pornire depanare) autorizarea obiect necesară 415
- comanda STRDBGSVR (Start Debug Server - Pornire depanare server) profiluri utilizator livrat de IBM autorizate 295
- Comanda STRDBMON (Start Database Monitor - Pornire monitorizare bază de date) autorizarea obiect necesară 410
- Comanda STRDBRDR (Start Database Reader - Pornire cititor bază de date) autorizarea obiect necesară 418
- Comanda STRDFU (Start DFU - Pornire DFU) autorizarea obiect necesară 313, 343
- comanda STRDIRSHD (Pornire umbrire director) auditare obiect 462
- Comanda STRDIRSHD (Start Directory Shadow System - Pornire sistem umbră director) autorizarea obiect necesară 329
- Comanda STRDKTRDR (Start Diskette Reader - Pornire cititor dischetă) autorizarea obiect necesară 418
- Comanda STRDKTWTR (Pornire scriitor dischetă) autorizarea obiect necesară 444

Comanda STRDSKRGZ (Start Disk Reorganization - Pornire reorganizare disc) autorizarea obiect necesară 330

Comanda STREDU (Start Education - Pornire educație) autorizarea obiect necesară 400

Comanda STREML3270 (Start 3270 Display Emulation - Pornire emulare ecran 3270) autorizări obiect necesare 329

comanda STRFMA (Pornire ajutor gestiune fonturi) auditare obiect 474

Comanda STRFMA (Start Font Management Aid - Pornire ajutor gestionare font) autorizarea obiect necesară 336

Comanda STRHOSTSVR (Start Host Server - Pornire server gazdă) autorizarea obiect necesară 346

Comanda STRIDD (Start Interactive Data Definition Utility - Pornire utilitate definiție interactivă de date) autorizări obiect necesare 366

comanda STRIDXMON (Start Index Monitor - Pornire monitorizare index) profiluri utilizator livrat de IBM autorizate 295

comanda STRIPSIFC (Start IP over SNA Interface - Pornire IP prin interfața SNA) profiluri utilizator autorizate livrat de IBM 295

Comanda STRIPSIFC (Start IP over SNA Interface - Pornire IP prin interfața SNA) autorizarea obiect necesară 312

comanda STRJOBTRC (Start Job Trace - Pornire urmărire job) profiluri utilizator livrat de IBM autorizate 295

Comanda STRJOBTRC (Start Job Trace - Pornire urmărire job) autorizarea obiect necesară 410

comanda STRJRN (Pornire jurnalizare) auditare obiect 449

Comanda STRJRN (Start Journal - Pornire jurnal) autorizarea obiect necesară 361, 375

Comanda STRJRNAP (Start Journal Access Path - Pornire cale acces jurnal) autorizarea obiect necesară 375

Comanda STRJRNOBJ (Start Journal Object - Pornire obiect jurnal) autorizarea obiect necesară 375

Comanda STRJRNPf (Start Journal Physical File - Pornire fișier fizic jurnal) autorizarea obiect necesară 375

comanda STRJRNxxx (Pornire jurnalizare) auditare obiect 477

Comanda STRLOGSVR (Start Job Log Server - Afișare istoric job server) autorizarea obiect necesară 369

comanda STRMGDSYS (Start Managed System - Pornire sistem gestionat) profiluri utilizator livrat de IBM autorizate 295

comanda STRMGRSRV (Start Manager Services - Pornire servicii manager) profiluri utilizator livrat de IBM autorizate 295

comanda STRMOD (Pornire mod) auditare obiect 480

Comanda STRMOD (Start Mode - Pornire mod) autorizarea obiect necesară 394

comanda STRMSF (Start Mail Server Framework - Pornire cadru de lucru server de mail) profiluri utilizator livrat de IBM autorizate 295

Comanda STRMSF (Start Mail Server Framework - Pornire cadru de lucru server de poștă) autorizarea obiect necesară 389

comanda STRNFSSVR (Start Network File System Server - Pornire server sistem de fișiere rețea) profiluri utilizator livrat de IBM autorizate 295

Comanda STRNFSSVR (Start Network File System Server - Pornire server sistem de fișiere rețea) autorizări obiect necesare 397

Comanda STROBJCVN 308

comanda STRPASTHR (Pornire Pass-Through) auditare obiect 457

Comanda STRPASTHR (Start Pass-Through - Pornire passthrough) autorizarea obiect necesară 330

Comanda STRPDM (Start Programming Development Manager - Pornire manager dezvoltare programare) autorizarea obiect necesară 313

Comanda STRPEX (Start Performance Explorer - Pornire explorare performanță) autorizarea obiect necesară 410

comanda STRPEX (Start Performance Explorer - Pornire Performance Explorer) profiluri utilizator livrat de IBM autorizate 296

Comanda STRPFRG (Start Performance Graphics - Pornire grafice de performanță) autorizarea obiect necesară 410

Comanda STRPFRT (Start Performance Tools - Pornire unelte de performanță) autorizarea obiect necesară 410

comanda STRPFTRC (Start Performance Trace - Pornire urmărire performanță) profiluri utilizator livrat de IBM autorizate 296

Comanda STRPFTRC (Start Performance Trace - Pornire urmărire performanță) autorizarea obiect necesară 410

Comanda STRPJ (Start Prestart Jobs - Pornire joburi prestart) autorizarea obiect necesară 369

Comanda STRPRTEML (Start Printer Emulation - Pornire emulare imprimantă) autorizări obiect necesare 329

comanda STRPRTWTR (Pornire scriitor imprimantă) auditare obiect 485, 505

Comanda STRPRTWTR (Start Printer Writer - Pornire scriitor imprimantă) autorizarea obiect necesară 444

comanda STRQMQRy (Pornire cerere Query Management) auditare obiect 489, 490, 491

Comanda STRQMQRy (Start Query Management Query - Început interogare Query Management) autorizări obiect necesare 417

Comanda STRQRy (Pornire interogare) autorizarea obiect necesară 417

Comanda STRQSH (Pornire QSH) autorizarea obiect necesară alias, QSH 415

Comanda STRQST (Start Question and Answer - Pornire întrebări și răspunsuri) autorizarea obiect necesară 418

Comanda STRREXPRC (Start REXX Procedure - Pornire procedură REXX) autorizarea obiect necesară 382

comanda STRRGZIDX (Start Reorganization of Index - Pornire reorganizare index) profiluri utilizator autorizate livrat de IBM 296

Comanda STRRJECSL (Pornire consolă RJE) autorizarea obiect necesară 422

Comanda STRRJERDR (Pornire cititor RJE) autorizarea obiect necesară 422

Comanda STRRJESSN (Pornire sesiune RJE) autorizarea obiect necesară 423

Comanda STRRJEWTR (Pornire scriitor RJE) autorizarea obiect necesară 423

Comanda STRRLU (Start Report Layout Utility - Pornire utilitar machetă raport) autorizarea obiect necesară 313

comanda STRRMTWTR (Pornire scriitor la distanță) auditare acțiune 496, 505
auditare obiect 485

Comanda STRRMTWTR (Start Remote Writer - Pornire scriitor la distanță) autorizarea obiect necesară 444

comanda STRS36 (Pornire System/36) auditare obiect 502
profil utilizator mediu special 72

comanda STRS36MGR (Start System/36 Migration - Pornire migrare System/36) profiluri utilizator livrat de IBM autorizate 296

Comanda STRS36MGR (Start System/36 Migration - Pornire migrare System/36) autorizarea obiect necesară 393

comanda STRS38MGR (Start System/38 Migration - Pornire migrare System/38) profiluri utilizator livrat de IBM autorizate 296

Comanda STRS38MGR (Start System/38 Migration - Pornire migrare System/38) autorizări obiect necesare 393

comanda STRSBS (Pornire subsistem) auditare obiect 492

Comanda STRSBS (Start Subsystem - Pornire subsistem) autorizarea obiect necesară 433

comanda STRSCHIDX (Pornire index de căutare) auditare obiect 493

- Comanda STRSCHIDX (Start Search Index - Pornire index de căutare)
 autorizarea obiect necesară 367
- Comanda STRSDA (Start SDA - Pornire SDA)
 autorizarea obiect necesară 313
- Comanda STRSEU (Start SEU - Pornire SEU)
 autorizarea obiect necesară 313
- Comanda STRSQL (Start Structured Query Language - Pornire limbaj de interogare structurat)
 autorizarea obiect necesară 382, 406
- comanda STRSRVJOB (Start Service Job - Pornire job service)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda STRSRVJOB (Start Service Job - Pornire job service)
 autorizarea obiect necesară 426
- comanda STRSST (Start System Service Tools - Pornire unelte service sistem)
 profiluri utilizator autorizate livrat de IBM 296
- Comanda STRSST (Start System Service Tools - Pornire unelte service sistem)
 autorizarea obiect necesară 426
- comanda STRSSYSMGR (Start System Manager - Pornire manager sistem)
 profiluri utilizator livrat de IBM autorizate 296
- comanda STRTCP (Start TCP/IP - Pornire TCP/IP)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda STRTCP (Start TCP/IP - Pornire TCP/IP)
 autorizarea obiect necesară 437
- Comanda STRTCPFTP (Pornire protocol transfer fișier TCP/IP)
 autorizarea obiect necesară 437
- comanda STRTCPIFC (Start TCP/IP Interface - Pornire interfață TCP/IP)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda STRTCPIFC (Start TCP/IP Interface - Pornire interfață TCP/IP)
 autorizări obiect necesare 437
- Comanda STRTCPPTP (Pornire TCP/IP punct-la-punct)
 autorizări obiect necesare 437
- comanda STRTCPSVR (Start TCP/IP Server - Pornire server TCP/IP)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda STRTCPSVR (Start TCP/IP Server - Pornire server TCP/IP)
 autorizarea obiect necesară 437
- Comanda STRTCPTELN (Pornire TCP/IP TELNET)
 autorizarea obiect necesară 437
- Comanda STRTRC (Pornire urmărire)
 autorizarea obiect necesară 426
- comanda STRUPDIDX (Start Update of Index - Pornire actualizare index)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda STRWCH (Start Watch - Pornire observare)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda Ștergere deținător de autorizare (DLTAUTHLR) 271, 276
- Comanda Ștergere listă de autorizații (DLTAUTL) 271
- comanda Ștergere profil utilizator (DLTUSRPRF)
 exemplu 102
- Comanda Ștergere profil utilizator (DLTUSRPRF)
 descriere 274
 drept de proprietate obiect 122
- Comanda TELNET (Pornire TCP/IP TELNET)
 autorizarea obiect necesară 437
- Comanda Terminare job (ENDJOB)
 Valoarea de sistem QINACTMSGQ 24
- Comanda TFRBCHJOB (Transfer Batch Job - Transferare job batch)
 autorizarea obiect necesară 369
- comanda TFRBCHJOB (Transfer job batch)
 auditare obiect 475
- Comanda TFRCTL (Control transfer)
 autorizarea obiect necesară 415
- Comanda TFRCTL (Transferare control)
 transferare autorizare adoptată 129
- Comanda TFRGRPJOB (Transfer la job grup)
 autorizare adoptată 129
- Comanda TFRGRPJOB (Transfer to Group Job - Transferare în job de grup)
 autorizarea obiect necesară 369
- Comanda TFRJOB (Transfer Job - Transferare job)
 autorizarea obiect necesară 369
- Comanda TFRPASTHR (Transfer Pass-Through - Transferare passthrough)
 autorizarea obiect necesară 330
- Comanda TFRSECJOB (Transfer Secondary Job - Transferare job secundar)
 autorizarea obiect necesară 369
- Comanda Tipărire atribute de securitate sistem (PRTSYSSECA)
 descriere 278
- Comanda Tipărire atribute securitate sistem (PRTSYSSECA)
 descriere 621
- Comanda tipărire autorizare coadă (PRTQAUT)
 descriere 623
- Comanda Tipărire autorizare coadă (PRTQAUT)
 descriere 277
- Comanda Tipărire autorizare descriere de job (PRTJOBDAUT) 277
- Comanda Tipărire autorizare descriere subsistem (PRTSBSDAUT)
 descriere 277
- Comanda Tipărire autorizări private (PRTPVTAUT) 277
 descriere 623
 listă de autorizații 621
- Comanda Tipărire descriere subsistem (PRTSBSDAUT)
 descriere 621
- Comanda Tipărire obiecte autorizate pentru publicare (PRTPUBAUT)
 descriere 623
- Comanda Tipărire obiecte autorizate public (PRTPUBAUT) 277
- Comanda Tipărire obiecte care adoptă (PRTADPOBJ)
 descriere 621
- Comanda Tipărire obiecte utilizator (PRTUSROBJ)
 descriere 277
- Comanda Tipărire obiecte utilizatori (PRTUSROBJ)
 descriere 621
- Comanda Tipărire profil utilizator (PRTUSRPRF)
 descriere 621
- Comanda Tipărire programe de declanșare (PRTRGPGM)
 descriere 277
- Comanda Tipărire securitate comunicație (PRTCMNSEC)
 descriere 621
- Comanda Tipărire securitate comunicații (PRTCMNSEC)
 descriere 278
- Comanda Transferare control (TFRCTL)
 transferare autorizare adoptată 129
- Comanda Transferare la job grup (TFRGRPJOB)
 autorizare adoptată 129
- Comanda TRCASPBAL 328
- Comanda TRCCNN (Urmărire conexiune)
 autorizarea obiect necesară 426
- comanda TRCCPIC (Trace CPI Communications - Urmărire comunicații CPI)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda TRCCPIC (Trace CPI Communications - Urmărire comunicații CPI)
 autorizarea obiect necesară 426
- comanda TRCCSP (Urmărire aplicație CSP/AE)
 auditare obiect 488
- comanda TRCICF (Trace ICF - Urmărire ICF)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda TRCICF (Trace ICF - Urmărire ICF)
 autorizarea obiect necesară 426
- comanda TRCINT (Trace Internal - Pornire internal)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda TRCINT (Trace Internal - Pornire internal)
 autorizarea obiect necesară 426
- comanda TRCJOB (Trace Job - Urmărire job)
 profiluri utilizator livrat de IBM autorizate 296
- Comanda TRCJOB (Trace Job - Urmărire job)
 autorizarea obiect necesară 426
- Comanda TRCTCPAPP
 autorizarea obiect necesară 426

Comanda TRMPRTEML (Terminate Printer Emulation - Terminare emulare imprimantă) autorizarea obiect necesară 329

Comanda TRNPIN (Translate Personal Identification Number - Traducere număr de identificare personal) autorizarea obiect necesară 325

comanda TRNPIN (Translate Personal Identification Number - Traducere număr identificare personală) profiluri utilizator autorizate livrat de IBM 296

Comanda UNMOUNT (Remove Mounted File System - Înlăturare sistem de fișiere montat) autorizarea obiect necesară 397

Comanda UPDDTA (Update Data - Actualizare date) autorizarea obiect necesară 343

Comanda UPDPGM (Actualizare program) autorizarea obiect necesară 415

comanda UPDPGM (Creare program) auditare obiect 452, 481, 487

Comanda UPDPTFINF (Update PTF Information - Actualizare informații FTP) profiluri utilizator livrat de IBM autorizate 296

comanda UPDSRVPGM (Actualizare program service) auditare obiect 452, 498

Comanda UPDSRVPGM (Actualizare program service) autorizarea obiect necesară 415

comanda UPDSRVPGM (Creare program service) auditare obiect 481

Comanda Verificare integritate obiect (CHKOBJITG) descriere 274, 621

comanda Verificare parolă (CHKPWD) 107

Comanda Verificare parolă (CHKPWD) 273

comanda VFYCMN (Verificare comunicații) auditare obiect 457, 478

Comanda VFYCMN (Verificare comunicații) autorizarea obiect necesară 412

comanda VFYCMN (Verify Communications - Verificare comunicații) profiluri utilizator livrat de IBM autorizate 296

Comanda VFYCMN (Verify Communications - Verificare comunicații) autorizarea obiect necesară 426

comanda VFYIMGCLG autorizarea obiect necesară 347

comanda VFYLNKLPDA (Verificare legătură care suportă LPDA-2) auditare obiect 478

Comanda VFYLNKLPDA (Verificare suport legătură LPDA-2) autorizarea obiect necesară 426

profiluri utilizator autorizate livrat de IBM 296

Comanda VFYMSTK (Verify Master Key - Verificare cheie master) autorizarea obiect necesară 325

comanda VFYMSTK (Verify Master Key - Verificare cheie primară) profiluri utilizator livrat de IBM autorizate 296

Comanda VFYPIN (Verify Personal Identification Number - Verificare număr de identificare personal) autorizarea obiect necesară 325

comanda VFYPIN (Verify Personal Identification Number - Verificare număr de identificare personală) profiluri utilizator autorizate livrat de IBM 296

Comanda VFYPRT (Verificare imprimantă) autorizarea obiect necesară 412

comanda VFYPRT (Verify Printer - Verificare imprimantă) profiluri utilizator livrat de IBM autorizate 296

Comanda VFYPRT (Verify Printer - Verificare imprimantă) autorizarea obiect necesară 427

Comanda VFYTAP (Verificare bandă) autorizarea obiect necesară 412

comanda VFYTAP (Verify Tape - Verificare bandă) profiluri utilizator livrat de IBM autorizate 296

Comanda VFYTAP (Verify Tape - Verificare bandă) autorizarea obiect necesară 427

Comanda VFYTCPCNN (Verificare conexiune TCP/IP) autorizarea obiect necesară 438

comanda VRYCFG (Modificare configurație) auditare obiect 457, 458, 478, 484

Comanda VRYCFG (Vary Configuration - Variere configurație) autorizarea obiect necesară 321

Comanda Work with Authority (WRKAUT) 138

comanda Work with Objects by Owner (WRKOBJOWN) folosire 142

Comanda Work with Objects by Primary Group (WRKOBJPGP) 123, 143

Comanda WRKACTJOB (Work with Active Jobs - Gestionare joburi active) autorizarea obiect necesară 369

Comanda WRKALR (Work with Alerts - Lucru cu alerte) autorizarea obiect necesară 312

comanda WRKALRD (Gestionare descriere alertă) auditare obiect 450

comanda WRKALRD (Work with Alert Descriptions - Lucru cu descrieri de alerte) autorizarea obiect necesară 312

comanda WRKALRTBL (Gestionare tabelă alertă) auditare obiect 451

Comanda WRKALRTBL (Work with Alert Tables - Lucru cu tabele de alerte) autorizarea obiect necesară 312

Comanda WRKASJOB autorizarea obiect necesară 369

comanda WRKAUT (Gestionare autorizare) auditare obiect 460, 495, 500

Comanda WRKAUT (Lucru cu autorizare) descriere 272

Comanda WRKAUT (Work with Authority - Gestionare autorizări) 138

Comanda WRKAUT (Work with Authority Directory - Gestionare director autorizare) autorizări obiect necesare 361

comanda WRKAUTL (Gestionare listă de autorizații) auditare obiect 451

Comanda WRKAUTL (Lucru cu liste de autorizație) descriere 271

Comanda WRKAUTL (Work with Authorization Lists - Lucru listele autorizare) autorizarea obiect necesară 314

comanda WRKBNDDIR (Gestionare director de legături) auditare obiect 452

Comanda WRKBNDDIR (Work with Binding Directory - Gestionare director de legare) autorizarea obiect necesară 315

comanda WRKBNDDIR (Gestionare intrare director de legături) auditare obiect 452

Comanda WRKBNDDIR (Work with Binding Directory Entry - Gestionare intrare director de legare) autorizarea obiect necesară 315

comanda WRKCFGL (Gestionare listă de configurație) auditare obiect 452

Comanda WRKCFGL (Work with Configuration Lists - Gestionare liste de configurație) autorizarea obiect necesară 322

comanda WRKCFGSTS (Gestionare stare configurație) auditare obiect 458, 479, 484

Comanda WRKCFGSTS (Work with Configuration Status - Gestionare stare configurație) autorizarea obiect necesară 321

Comanda WRKCHTFMT (Work with Chart Formats - Gestionare formate de diagrame) autorizarea obiect necesară 315

comanda WRKCLS (Gestionare clasă) auditare obiect 454

Comanda WRKCLS (Work with Classes - Gestionare clase) autorizarea obiect necesară 316

comanda WRKCMD (Gestionare comandă) auditare obiect 455

Comanda WRKCMD (Work with Commands - Gestionare comenzi) autorizarea obiect necesară 320

Comanda WRKCMTDFN (Work with Commitment Definition - Gestionare definiție comitere) autorizarea obiect necesară 320

Comanda WRKCNL (Work with Connection Lists - Gestionare liste de conexiuni) autorizarea obiect necesară 322

- comanda WRKCNNLE (Gestionare intrări listă de conexiuni)
auditare obiect 455
- comanda WRKCNTINF (Work with Contact Information - Gestionare informații contact)
profiluri utilizator autorizate livrat de IBM 296
- Comanda WRKCNTINF (Work with Contact Information - Gestionare informații contact)
autorizarea obiect necesară 418, 427
- comanda WRKCOSD (Gestionare descriere clasă-de-serviciu)
auditare obiect 456
- Comanda WRKCOSD (Work with Class-of-Service Descriptions - Gestionare descrieri ale clasei-de-serviciu)
autorizarea obiect necesară 316
- comanda WRKCRQD (Gestionare descrieri cerere modificare)
auditare obiect 454
- Comanda WRKCRQD (Work with Change Request Description - Gestionare descriere cerere de modificare)
autorizarea obiect necesară 315
- comanda WRKCSI (Gestionare CSI)
auditare obiect 456
- Comanda WRKCSI (Work with Communications Side Information - Gestionare CSI)
autorizări obiect necesare 321
- comanda WRKCTLD (Gestionare descrieri controler)
auditare obiect 457
- Comanda WRKCTLD (Work with Controller Descriptions - Gestionare descrieri controler)
autorizarea obiect necesară 324
- Comanda WRKDBFIDD (Work with Database Files Using IDDU - Gestionare fișiere bază de date folosind IDDU)
autorizarea obiect necesară 366
- Comanda WRKDDMF (Work Distributed Data Management Files - Gestionare fișiere de gestiune date distribuite)
autorizări obiect necesare 343
- comanda WRKDEVD (Gestionare descrieri dispozitiv)
auditare obiect 458
- Comanda WRKDEVD (Work with Device Descriptions - Gestionare descrieri dispozitiv)
autorizarea obiect necesară 328
- comanda WRKDEVTBL (Work with Device Tables - Gestionare tabele de dispozitive)
profiluri utilizator autorizate livrat de IBM 296
- Comanda WRKDEVTBL (Work with Device Tables - Gestionare tabele dispozitiv)
autorizarea obiect necesară 345
- Comanda WRKDIRE (Lucru cu directoare)
descriere 276
- Comanda WRKDIRE (Work with Directory Entry - Gestionare intrare director)
autorizarea obiect necesară 329
- Comanda WRKDIRLOC (Work with Directory Locations - Gestionare locații director)
autorizarea obiect necesară 329
- Comanda WRKDIRSHD (Work with Directory Shadow Systems - Gestionare sisteme umbră director)
autorizarea obiect necesară 329
- comanda WRKDOC (Gestionare documente)
auditare obiect 463
- Comanda WRKDOC (Work with Documents - Gestionare documente)
autorizarea obiect necesară 334
- comanda WRKDOCLIB (Gestionare biblioteci de documente)
auditare obiect 465
- Comanda WRKDOCLIB (Work with Document Libraries - Gestionare biblioteci de documente)
autorizări obiect necesare 400
- comanda WRKDOCPRQ (Gestionare coadă de tipărire documente)
auditare obiect 465
- Comanda WRKDOCPRQ (Work with Document Print Queue - Gestionare coadă de tipărire documente)
autorizarea obiect necesară 400
- comanda WRKDPCQ (Work with DSNX/PC Distribution Queues - Gestionare cozi de distribuție DSNX/PC)
profiluri utilizator autorizate livrat de IBM 296
- Comanda WRKDPCQ (Work with DSNX/PC Queues - Gestionare cozi DSNX/PC de date)
autorizarea obiect necesară 331
- Comanda WRKDSKSTS (Work with Disk Status - Gestionare stare disc)
autorizarea obiect necesară 330
- Comanda WRKDSLTL (Work with Distribution Lists - Gestionare liste de distribuție)
autorizarea obiect necesară 331
- Comanda WRKDSTQ (Work Distribution Queue - Gestionare coadă de distribuție)
autorizarea obiect necesară 331
- profiluri utilizator autorizate livrat de IBM 296
- comanda WRKDTAARA (Gestionare zone de date)
auditare obiect 466
- Comanda WRKDTAARA (Work with Data Areas - Gestionare zone de date)
autorizarea obiect necesară 325
- Comanda WRKDTADCT (Work with Data Dictionaries - Gestionare dicționare de date)
autorizarea obiect necesară 366
- Comanda WRKDTADFN (Work with Data Definitions - Gestionare definiții de date)
autorizarea obiect necesară 366
- comanda WRKDTAQ (Gestionare cozi de date)
auditare obiect 467
- Comanda WRKDTAQ (Work with Data Queues - Gestionare cozi de date)
autorizarea obiect necesară 326
- comanda WRKEDTD (Gestionare descrieri editare)
auditare obiect 467
- Comanda WRKEDTD (Work with Edit Descriptions - Gestionare descriere de editare)
autorizarea obiect necesară 336
- Comanda WRKENVVAR (Work Environment Variable - Gestionare variabile de mediu)
autorizarea obiect necesară 336
- comanda WRKF (Gestionare fișiere)
auditare obiect 471
- Comanda WRKF (Work with Files - Gestionare fișiere)
autorizarea obiect necesară 343
- Comanda WRKFNCARA (Work with Functional Areas - Gestionare zone funcționale)
autorizarea obiect necesară 410
- Comanda WRKFCT (Gestionare tabel de control formulare)
autorizarea obiect necesară 423
- Comanda WRKFLLR (Work with Folders - Gestionare foldere)
autorizarea obiect necesară 334
- comanda WRKFNTRSC (Gestionare resurse font)
auditare obiect 472
- Comanda WRKFNTRSC (Work with Font Resources - Lucru cu resurse font)
autorizarea obiect necesară 311
- comanda WRKFORMDF (Gestionare definiții de formular)
auditare obiect 472
- Comanda WRKFORMDF (Work with Form Definitions - Gestionare definiții de formular)
autorizarea obiect necesară 311
- Comanda WRKFSTAF (Gestionare opțiune alertă FFST)
autorizarea obiect necesară 427
- Comanda WRKFSTPCT (Gestionare tabel de control probă FFST)
autorizarea obiect necesară 427
- comanda WRKFTR (Gestionare filtre)
auditare obiect 473
- Comanda WRKFTR (Work with Filters - Gestionare filtre)
autorizarea obiect necesară 344
- comanda WRKFTRACNE (Gestionare intrări acțiune filtru)
auditare obiect 473
- Comanda WRKFTRACNE (Work with Filter Action Entries - Gestionare intrări acțiune filtre)
autorizarea obiect necesară 344
- comanda WRKFTRSLTE (Gestionare intrări selecție filtru)
auditare obiect 473
- Comanda WRKFTRSLTE (Work with Filter Selection Entries - Gestionare intrări selecție filtre)
autorizări obiect necesare 344
- comanda WRKGGSS (Gestionare seturi de simboluri grafice)
auditare obiect 473
- Comanda WRKGGSS (Work with Graphics Symbol Sets - Gestionare seturi de simboluri grafice)
autorizarea obiect necesară 345
- Comanda WRKHDWRSC (Gestionare resurse hardware)
autorizarea obiect necesară 419

- Comanda WRKHLDOPTF (Work with Help Optical Files - Gestionare fișiere optice de ajutor)
 autorizarea obiect necesară 403
- Comanda WRKIMGCLG
 autorizarea obiect necesară 347
- comanda WRKIMGCLGE
 autorizarea obiect necesară 347
- Comanda WRKIPXD 366
- Comanda WRKJOB (Work with Job - Gestionare job)
 autorizarea obiect necesară 369
- comanda WRKJOB (Gestionare descrieri de job)
 auditare obiect 474
- Comanda WRKJOB (Work with Job Descriptions - Gestionare descrieri de job)
 autorizarea obiect necesară 371
- Comanda WRKJOBLOG (Work with Job Logs - Gestionare jurnale de job)
 autorizarea obiect necesară 369
- comanda WRKJOBQ (Gestionare coadă joburi)
 auditare obiect 475
- Comanda WRKJOBQ (Work Job Queue - Gestionare coadă joburi)
 autorizarea obiect necesară 371
- comanda WRKJOBSCDE (Gestionare intrări planificare job)
 auditare obiect 475
- Comanda WRKJOBSCDE (Work with Job Schedule Entries - Gestionare intrări planificare job)
 autorizarea obiect necesară 372
- comanda WRKJRN (Gestionare jurnal)
 auditare obiect 477
- comanda WRKJRN (Work with Journal - Gestionare jurnal)
 profiluri utilizator livrat de IBM autorizate 296
 utilizare 260, 267
- Comanda WRKJRN (Work with Journal - Gestionare jurnal)
 autorizarea obiect necesară 375
- comanda WRKJRNA (Gestionare attribute jurnal)
 auditare obiect 477
- comanda WRKJRNA (Work with Journal Attributes - Gestionare attribute jurnal)
 utilizare 260, 267
- Comanda WRKJRNA (Work with Journal Attributes - Gestionare attribute jurnal)
 autorizări obiect necesare 375
- comanda WRKJRNCV (Gestionare receptori jurnal)
 auditare obiect 477
- Comanda WRKJRNCV (Work with Journal Receivers - Gestionare receptori jurnal)
 autorizarea obiect necesară 376
- Comanda WRKLANADPT (Gestionare adaptoare LAN)
 autorizarea obiect necesară 389
- Comanda WRKLIB (Work with Libraries - Gestionare biblioteci)
 autorizarea obiect necesară 385
- Comanda WRKLIBPDM (Work with Libraries Using PDM- Lucru cu biblioteci folosind PDM)
 autorizarea obiect necesară 313
- comanda WRKLICINF (Work with License Information - Gestionare informații licență)
 profiluri utilizator autorizate livrat de IBM 297
- comanda WRKLIND (Gestionare descrieri de linie)
 auditare obiect 479
- Comanda WRKLIND (Work with Line Descriptions - Gestionare descrieri de linie)
 autorizarea obiect necesară 389
- comanda WRKLNK (Gestionare legături)
 auditare obiect 459, 460, 494, 495
- comanda WRKLNK (Lucrare cu legături)
 auditare obiect 499, 500, 501, 502
- Comanda WRKLNK (Work with Links - Gestionare legături)
 autorizarea obiect necesară 362
- Comanda WRKMBRPDM (Work with Members Using PDM- Lucru cu membrii folosind PDM)
 autorizarea obiect necesară 313
- comanda WRKMNU (Gestionare meniuri)
 auditare obiect 480
- Comanda WRKMNU (Work with Menus - Gestionare meniuri)
 autorizarea obiect necesară 391
- comanda WRKMOD (Gestionare module)
 auditare obiect 481
- Comanda WRKMOD (Work with Module - Gestionare modul)
 autorizarea obiect necesară 394
- comanda WRKMODD (Gestionare descrieri mod)
 auditare obiect 480
- Comanda WRKMODD (Work with Mode Descriptions - Gestionare descrieri mod)
 autorizarea obiect necesară 394
- comanda WRKMSG (Gestionare mesaje)
 auditare obiect 483
- Comanda WRKMSG (Work with Messages - Gestionare mesaje)
 autorizarea obiect necesară 392
- comanda WRKMSGD (Gestionare descrieri de mesaj)
 auditare obiect 481
- Comanda WRKMSGD (Work with Message Descriptions - Gestionare descrieri mesaj)
 autorizarea obiect necesară 392
- comanda WRKMSGF (Gestionare fișiere de mesaje)
 auditare obiect 482
- Comanda WRKMSGF (Work with Message Files - Gestionare fișiere mesaj)
 autorizarea obiect necesară 393
- comanda WRKMSGQ (Gestionare cozi de mesaje)
 auditare obiect 483
- Comanda WRKMSGQ (Work with Message Queues - Gestionare cozi de mesaje)
 autorizarea obiect necesară 393
- Comanda WRKNAMSMTP (Gestionare nume pentru SMTP)
 obiect autorizare cerută 438
- Comanda WRKNETF (Work with Network Files - Gestionare fișiere rețea)
 autorizarea obiect necesară 396
- Comanda WRKNETJOB (Work with Network Job Entries - Gestionare intrări job rețea)
 autorizarea obiect necesară 396
- Comanda WRKNETTBLE (Gestionare intrări tabel rețea)
 autorizarea obiect necesară 438
- comanda WRKNODL (Gestionare listă de noduri)
 auditare obiect 483
- Comanda WRKNODL (Work with Node List - Gestionare listă de noduri)
 autorizarea obiect necesară 399
- comanda WRKNODLE (Gestionare intrări listă de noduri)
 auditare obiect 483
- Comanda WRKNODLE (Work with Node List Entries - Gestionare intrări în lista de noduri)
 autorizarea obiect necesară 399
- comanda WRKNBTBD (Gestionare descriere NetBIOS)
 auditare obiect 484
- Comanda WRKNBTBD (Work with NetBIOS Description - Gestionare descriere NetBIOS)
 autorizarea obiect necesară 395
- comanda WRKNWID (Gestionare descriere interfață de rețea)
 auditare obiect 484
- Comanda WRKNWID (Work with Network Interface Description Command - Gestionare comandă descriere interfață de rețea)
 autorizări obiect necesare 397
- Comanda WRKNWSALS (Work with Network Server Alias - Gestionare aliasuri server de rețea)
 autorizarea obiect necesară 398
- Comanda WRKNWSCFG
 autorizarea obiect necesară 399
- profiluri utilizator livrat de IBM autorizate 297
- comanda WRKNWSD (Gestionare descrierea server de rețea)
 auditare obiect 485
- Comanda WRKNWSD (Work with Network Server Description - Gestionare descriere server de rețea)
 autorizarea obiect necesară 399
- Comanda WRKNWSEN (Work with Network Server User Enrollment - Gestionare înrolare utilizator server de rețea)
 autorizarea obiect necesară 398
- Comanda WRKNWSSN (Work with Network Server Session - Gestionare sesiune server de rețea)
 autorizarea obiect necesară 398
- Comanda WRKNWSSTG (Work with Network Server Storage Space - Gestionare spațiu de stocare server de rețea)
 autorizarea obiect necesară 398
- Comanda WRKNWSSTS (Work with Network Server Status - Gestionare stare server de rețea)
 autorizarea obiect necesară 398

- Comanda WRKOBJ (Lucru cu obiecte)
descriere 272
- Comanda WRKOBJ (Work with Objects -
Lucru cu obiecte)
autorizarea obiect necesară 308
- comanda WRKOBJCSP (Gestionare obiecte
pentru CSP/AE)
auditare obiect 456, 457, 488
- comanda WRKOBJLCK (Gestionare blocare
obiect)
auditare obiect 450
- comanda WRKOBJLCK (Work with Object
Locks - Gestionare blocări de obiecte)
autorizări obiect necesare 308
- comanda WRKOBJOWN (Gestionare obiecte
după proprietar)
auditare obiect 450, 504
- Comanda WRKOBJOWN (Lucru cu obiecte
după proprietar)
descriere 272
- comanda WRKOBJOWN (Work with Objects
by Owner - Gestionare obiecte după
proprietar)
folosire 142
- Comanda WRKOBJOWN (Work with Objects
by Owner - Gestionare obiecte după
proprietar)
auditare 232
autorizarea obiect necesară 309
- Comanda WRKOBJPDM (Work with Objects
Using PDM- Lucru cu obiecte folosind
PDM)
autorizarea obiect necesară 313
- Comanda WRKOBJPGP (Lucru cu obiecte
după grup primar)
descriere 272
- Comanda WRKOBJPGP (Work with Objects
by Primary Group - Gestionare obiecte după
grupul primar) 123, 143
autorizări obiect necesare 309
- Comanda WRKOPTDIR (Work with Optical
Directories - Gestionare directoare optice)
autorizarea obiect necesară 403
- Comanda WRKOPTF (Work with Optical
Files - Gestionare fișiere optice)
autorizarea obiect necesară 403
- Comanda WRKOPTVOL (Work with Optical
Volumes - Gestionare volume optice)
autorizarea obiect necesară 403
- comanda WRKORDINF (Work with Order
Information - Gestionare informații
comandă)
profiluri utilizator livrat de IBM
autorizate 297
- Comanda WRKORDINF (Work with Order
Information - Gestionare informații
comandă)
autorizarea obiect necesară 439
- comanda WRKOUTQ (Gestionare coadă de
ieșire)
auditare obiect 486
- Comanda WRKOUTQ (Work with Output
Queue - Gestionare coadă de ieșire)
autorizarea obiect necesară 405
- comanda WRKOUTQD (Gestionare descriere
coadă de ieșire)
auditare obiect 486
- comanda WRKOUTQD (Work with Output
Queue Description - Gestionare descriere
coadă de ieșire) 186
parametrii de securitate 186
- Comanda WRKOUTQD (Work with Output
Queue Description - Gestionare descriere
coadă de ieșire)
autorizarea obiect necesară 405
- comanda WRKOVL (Gestionare suprapuneri)
auditare obiect 486
- Comanda WRKOVL (Work with Overlays -
Lucru cu suprapuneri)
autorizarea obiect necesară 311
- comanda WRKPAGDFN (Gestionare definiții
de pagină)
auditare obiect 486
- Comanda WRKPAGDFN (Work with Page
Definitions - Gestionare definiții de pagină)
autorizarea obiect necesară 311
- comanda WRKPAGSEG (Gestionare segmente
de pagină)
auditare obiect 486
- Comanda WRKPAGSEG (Work with Page
Segments - Gestionare segmente de pagină)
autorizarea obiect necesară 311
- Comanda WRKPCLTBLE (Gestionare intrări
tabel protocol)
autorizarea obiect necesară 438
- comanda WRKPDG (Gestionare grup de
descriptori tipărire)
auditare obiect 487
- comanda WRKPEXFTR
profiluri utilizator livrat de IBM
autorizate 297
- comanda WRKPF CST (Gestionare
constrângeri fișier fizic)
auditare obiect 471
- Comanda WRKPF CST (Work with Physical
File Constraints - Gestionare constrângeri
fișier fizic)
autorizări obiect necesare 343
- comanda WRKPGM (Gestionare programe)
auditare obiect 488
- Comanda WRKPGM (Gestionare programe)
autorizarea obiect necesară 415
- comanda WRKPGMTBL (Work with Program
Tables - Gestionare tabele program)
profiluri utilizator autorizate livrat de
IBM 297
- Comanda WRKPGMTBL (Work with Program
Tables - Gestionare tabele program)
autorizarea obiect necesară 345
- comanda WRKPNLGRP (Gestionare grupuri
de panouri)
auditare obiect 489
- Comanda WRKPNLGRP (Work Panel Groups
- Gestionare grupuri de panouri)
autorizarea obiect necesară 391
- Comanda WRKPRB (Gestionare probleme)
autorizarea obiect necesară 412
- comanda WRKPRB (Work with Problem -
Gestionare probleme)
profiluri utilizator livrat de IBM
autorizate 297
- Comanda WRKPRB (Work with Problem -
Gestionare probleme)
autorizarea obiect necesară 427
- Comanda WRKPTFGRP (Gestionare grup
PTF)
autorizarea obiect necesară 427
- comanda WRKQMF FORM (Gestionare
formular Query Management)
auditare obiect 490
- Comanda WRKQMF FORM (Work with Query
Management Form - Gestionare formular
Query Management)
autorizarea obiect necesară 417
- Comanda WRKQMORY (Gestionare
interogări Query Management)
autorizarea obiect necesară 417
- Comanda WRKQRY (Gestionare interogare)
autorizarea obiect necesară 417
- Comanda WRKQST (Work with Questions -
Gestionare întrebări)
autorizarea obiect necesară 418
- Comanda WRKRDBDIRE (Gestionare intrări
director baze de date relaționale)
autorizarea obiect necesară 419
- comanda WRKREGINF (Gestionare informații
de înregistrare)
auditare obiect 468
- Comanda WRKREGINF (Work with
Registration - Gestionare înregistrare)
autorizarea obiect necesară 418
- Comanda WRKRJESSN (Gestionare sesiuni
RJE)
autorizarea obiect necesară 423
- comanda WRKRYPYLE (Gestionare intrări listă
răspuns sistem)
auditare obiect 492
- Comanda WRKRYPYLE (Work with System
Reply List Entries - Lucrul cu intrări listă
de replici sistem)
autorizarea obiect necesară 433
- comanda WRKS36PGMA (Gestionare atribute
program System/36)
auditare obiect 488
- Comanda WRKS36PGMA (Work with
System/36 Program Attributes - Gestionare
atribute program System/36)
autorizarea obiect necesară 436
- comanda WRKS36PRCA (Gestionare atribute
procedură System/36)
auditare obiect 471
- Comanda WRKS36PRCA (Work with
System/36 Procedure Attributes - Gestionare
atribute procedură System/36)
autorizarea obiect necesară 436
- comanda WRKS36SRCA (Gestionare atribute
sursă System/36)
auditare obiect 471
- Comanda WRKS36SRCA (Work with
System/36 Source Attributes - Gestionare
atribute sursă System/36)
autorizarea obiect necesară 436
- Comanda WRKSBJMJOB (Work with
Submitted Jobs - Gestionare joburi lansate)
autorizarea obiect necesară 369
- comanda WRKSBS (Gestionare subsisteme)
auditare obiect 493
- Comanda WRKSBS (Work with Subsystems -
Gestionare subsisteme)
autorizarea obiect necesară 433

comanda WRKSBSD (Gestionare descrieri subsistem)
 auditare obiect 493

Comanda WRKSBSD (Work with Subsystem Descriptions - Gestionare descrieri de subsisteme)
 autorizarea obiect necesară 433

comanda WRKSBSJOB (Gestionare joburi subsistem)
 auditare obiect 493

Comanda WRKSBSJOB (Work with Subsystem Jobs - Gestionare joburi subsistem)
 autorizarea obiect necesară 369

comanda WRKSCHIDX (Gestionare indecși de căutare)
 auditare obiect 494

Comanda WRKSCHIDX (Work with Search Indexes - Gestionare indecși de căutare)
 autorizarea obiect necesară 367

comanda WRKSCHIDX (Gestionare intrări index de căutare)
 auditare obiect 493

Comanda WRKSCHIDX (Work with Search Index Entries - Gestionare intrări indecși de căutare)
 autorizarea obiect necesară 367

Comanda WRKSHRPOOL (Gestionare spații de stocare partajate)
 autorizarea obiect necesară 433

Comanda WRKSOC (Gestionare sferă de control)
 autorizarea obiect necesară 429

Comanda WRKSPADCT (Gestionare dicționare ajutoare pentru corectare ortografică)
 autorizări obiect necesare 428

comanda WRKSPLF (Gestionare fișiere spool)
 auditare obiect 486

comanda WRKSPLF (Work with Spooled Files - Gestionare fișiere spool)
 autorizarea obiect necesară 431

comanda WRKSPLFA (Gestionare atribute fișier spool)
 auditare obiect 486

comanda WRKSPTPRD (Gestionare produse suportate)
 auditare obiect 489

comanda WRKSRVPGM (Gestionare programe serviciu)
 auditare obiect 498

Comanda WRKSRVPGM (Gestionare programe serviciu)
 autorizarea obiect necesară 415

comanda WRKSRVPVD (Work with Service Providers - Gestionare furnizorii de servicii)
 profiluri utilizator autorizate livrat de IBM 297

Comanda WRKSRVPVD (Work with Service Providers - Gestionare furnizorii de servicii)
 autorizarea obiect necesară 427

Comanda WRKSSND (Gestionare descriere sesiune)
 autorizarea obiect necesară 423

Comanda WRKSYSACT (Work with System Activity - Gestionare activitate sistem)
 autorizarea obiect necesară 410

comanda WRKSYSSTS (Work with System Status - Gestionare stare sistem) 192

Comanda WRKSYSSTS (Work with System Status - Gestionare stare sistem)
 autorizarea obiect necesară 433

comanda WRKSYSVAL (Work with System Values - Gestionare valori de sistem)
 utilizare 230

Comanda WRKSYSVAL (Work with System Values - Gestionare valori de sistem)
 autorizarea obiect necesară 433

Comanda WRKTAPCTG (Work with Tape Cartridge - Gestionare cartuș bandă)
 autorizarea obiect necesară 390

comanda WRKTBL (Gestionare tabele)
 auditare obiect 503

Comanda WRKTBL (Work with Tables - Gestionare tabele)
 autorizarea obiect necesară 436

Comanda WRKTCPSTS (Gestionare stare rețea TCP/IP)
 autorizarea obiect necesară 438

Comanda WRKTIMZON 438

Comanda WRKTRC
 profiluri utilizator livrat de IBM autorizate 297

comanda WRKTXIDX (Work with Text Index - Gestionare index text)
 profiluri utilizator livrat de IBM autorizate 297

Comanda WRKUSRJOB (Work with User Jobs - Gestionare joburi utilizator)
 autorizarea obiect necesară 369

comanda WRKUSRPRF (Gestionare profiluri utilizator)
 auditare obiect 504
 folosind 97

Comanda WRKUSRPRF (Lucru cu profiluri utilizator)
 descriere 274

Comanda WRKUSRPRF (Work with User Profiles - Gestionare profiluri utilizator)
 autorizarea obiect necesară 442

comanda WRKUSRTBL (Work with User Tables - Gestionare tabele utilizator)
 profiluri utilizator livrat de IBM autorizate 297

Comanda WRKUSRTBL (Work with User Tables - Gestionare tabele utilizator)
 autorizarea obiect necesară 345

Comanda WRKWCH
 profiluri utilizator livrat de IBM autorizate 297

Comanda WRKWTR (Gestionare scriitori)
 autorizarea obiect necesară 444

comanda, CL

Acordare autorizare de utilizator (GRTUSRAUT)
 copii autorizare 101
 redenumire profil 106

ADDJOBSCDE (Adăugare intrare planificator de joburi)
 meniu SECBATCH 621

ADDLIB (Add Library List Entry - Adăugare intrare lista de bibliotecă) 183, 186

comanda, CL (*continuare*)

ADDLIB (Add Library List Entry - Adăugare intrare lista de bibliotecă) 183

afișare cuvinte cheie (*CLKWD opțiune utilizator) 88, 89, 90

Afișare profil utilizator (DSPUSRPRF)
 folosind 104

Afișare utilizatori autorizați (DSPAUTUSR)
 exemplu 104

ANZDFTPWD (Analizarea parolelor implicite)
 descriere 617

ANZPRFACT (Analizare activitate profil)
 creare utilizator exempt 617
 descriere 617

CFGSYSSEC (Configurare securitate sistem)
 descriere 625

Change User Audit (CHGUSRAUD)
 folosind 106

CHGACGCDE (Modificare cod de contabilizare) 82

CHGACTPRFL (Modificarea listei de profiluri activă)
 descriere 617

CHGACTSCDE (Modificare intrare planificator activare)
 descriere 617

CHGCMD (Change Command - Modificare comandă)
 parametrul PRDLIB (biblioteca produs) 185
 riscuri de securitate 185

CHGCMD (Modificare comandă)
 parametrul ALWLMTUSR (permitere utilizator limitat) 67

CHGCURLIB (Change Current Library - Modificare biblioteca curentă)
 restricționare 185

CHGDLOAUD (Modificare auditare obiect bibliotecă document)
 autorizare specială *AUDIT (auditare) 71

CHGEXPSCDE (Modificare Intrare planificator expirare)
 descriere 617

CHGLIBL (Change Library List - Modificare lista de bibliotecă) 183

CHGMNU (Change Menu - Meniu modificare)
 parametrul PRDLIB (biblioteca produs) 185
 riscuri de securitate 185

CHGMNU (Change Menu - Modificare meniu)
 parametrul PRDLIB (biblioteca produs) 185
 riscuri de securitate 185

CHGNETA (Change Network Attributes - Modificare atribute rețea) 189

CHGOBJAUD (Modificare auditare obiect)
 autorizare specială *AUDIT (auditare) 71

CHGOUTQ (Change Output Queue - Modificare coadă de ieșire) 186

comanda, CL (<i>continua</i>)	comanda, CL (<i>continua</i>)	comanda, CL (<i>continua</i>)
CHGPRF (Modificare profil) 101	cuvinte cheie, afișare (*CLKWD opțiune utilizator) 88, 89, 90	permisă pentru limitare capabilități utilizator 67
CHGPWD (Modificare parolă) setare parolă egală cu nume profil 60	denumiri parametru, afișare (*CLKWD opțiune utilizator) 88, 89, 90	planificare activare 617
CHGSECAUD (Modificare auditare securitate) descriere 619	DLTUSRPRF (Ștergere profil utilizator) exemplu 102	Pornire System/36 (STRS36) profil utilizator, mediu special 72
CHGSPLFA (Change Spooled File Attributes - Modificare atribute fișier spool) 186	DSPACTPRFL (Afișare listă de profiluri active) descriere 617	PRTADPOBJ (Tipărire obiecte care adoptă) descriere 621
CHGSYSLIBL (Change System Library List - Modificare lista de biblioteci sistem) 183	DSPACTSCD (Afișare planificator activare) descriere 617	PRTCMNSEC (Tipărire securitate comunicație) descriere 621
CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem) 202	DSPAUDJRNE (Afișare intrări jurnal de auditare) descriere 621	PRTJOBDAUT (Autorizarea tipărire descriere job) descriere 621
CHGUSRAUD (Modificare auditare utilizator) autorizare specială *AUDIT (auditare) 71	DSPAUTUSR (Afișare utilizatori autorizați) exemplu 104	PRTPUBAUT (Tipărire obiect autorizate de publicare) descriere 621
folosind 106	DSPEXPSCD (Afișare planificator de expirare) descriere 617	PRTPVTAUT (Tipărire autorizări private) descriere 623
CHGUSRPRF (Modificare profil utilizator) folosind 101	DSPJRN (Display Journal - Afișare jurnal) auditare activitate fișier 209	listă de autorizații 621
setare parolă egală cu nume profil 60	DSPSECAUD (Afișare auditare securitate) descriere 619	PRTQAUT (Tipărire coadă autorizare) descriere 623
CHKOBJITG (Verificare integritate obiect) descriere 621	DSPSPLF (Display Spooled File - Afișare fișier spool) 186	PRTSBSDAUT (Tipărire descriere subsistem) descriere 621
CHKPWD (Verificare parolă) 107	DSPUSRPRF (Afișare profil utilizator) folosind 104	PRTSYSSECA (Tipărire atribute securitate sistem) descriere 621
Comanda CHGCMDDF (Change Command Default - Modificare valoare implicită a comenzii) 209	EDTLIBL (Edit Library List - Editare lista de biblioteci) 183	PRTTRGPGM (Tipărire programe declanșatoare) descriere 621
Comanda CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem) 202	Extragere profil utilizator (RTVUSRPRF) 107	PRTUSROBJ (Tipărire obiecte utilizatori) descriere 621
Comanda DSPJRN (Display Journal - Afișare jurnal) auditare activitate fișier 209	Gestionare profiluri utilizator (WRKUSRPRF) 97	PRTUSRPRF (Tipărire profil utilizator) descriere 621
Comanda DSPPGMADP (Display Programs That Adopt - Afișare programe care adoptă) using 209	GRTUSRAUT (Acordare autorizare de utilizator) copiere autorizare 101	RMVLIBL (Remove Library List Entry - Înlăturare intrare lista de biblioteci) 183
CPYSPLF (Copy Spooled File - Copiere fișier spool) 186	redenumire profil 106	RTVUSRPRF (Extragere profil utilizator) 107
Creare comandă (CRTCMD) parametru ALWLMTUSR (permite utilizator limitat) 67	Modificare auditare obiect (CHGOBJAUD) autorizare specială *AUDIT (auditare) 71	RVKPUBAUT (Revocare autorizație publică) descriere 625
Creare profil utilizator (CRTUSRPRF) descriere 98	Modificare auditare obiect bibliotecă document (CHGDLOAUD) autorizare specială *AUDIT (auditare) 71	detalii 627
CRTCMD (Creare comandă) parametru ALWLMTUSR (permite utilizator limitat) 67	Modificare cod de contabilizare (CHGACGCDE) 82	SBMJOB (Lansare job) meniu SECBATCH 620
CRTCMD (Create Command - Creare comandă) parametrul PRDLIB (biblioteca produs) 185	Modificare comandă (CHGCMD) parametru ALWLMTUSR (permite utilizator limitat) 67	SBMJOB (Submit Job - Lansare job) 176
riscuri de securitate 185	Modificare parolă (CHGPWD) setare parolă egală cu nume profil 60	Setare program Attn (SETATNPGM) 86
CRTMNU (Create Menu - Creare meniu) parametrul PRDLIB (biblioteca produs) 185	Modificare profil (CHGPRF) 101	SETATNPGM (Setare program Attn) 86
riscuri de securitate 185	Modificare profil utilizator (CHGUSRPRF) folosind 101	SNDNETSPLF (Send Network Spooled File - Trimitere fișier spool de rețea) 186
CRTOUTQ (Create Output Queue - Creare coadă de ieșire) 188	setare parolă egală cu nume profil 60	STRS36 (Pornire System/36) profil utilizator, mediu special 72
CRTOUTQ (Create Output Queue - Creare coadă de ieșire) 186	parametru ALWLMTUSR (permite utilizator limitat) 67	Ștergere profil utilizator (DLTUSRPRF) exemplu 102
CRTUSRPRF (Creare profil utilizator) descriere 98		Verificare parolă (CHKPWD) 107

comanda, Sistemul de fișiere integrat
 CHGAUD (Modificare auditare)
 folosind 106
 Modificare auditare (CHGAUD)
 folosind 106

comandă
 auditare
 intrare jurnal auditare
 (QAUDJRN) 241
 modificare
 valori implicite 209
 NLV (versiune limbă națională)
 securitate 209
 planificare securitate 208
 revocare autorizare publică 278
 System/38
 securitate 209

comandă (tip obiect *CMD)
 autorizație obiect cerută pentru
 comenzi 319

comandă ADDCLUNODE
 autorizarea obiect necesară 316

comandă capabilitate
 listare utilizatori 267

comandă CHGPRF (Modificare profil
 utilizator)
 auditare obiect 503

comandă CHGS36A (Modificare atribute
 System/36)
 auditare obiect 502

comandă CHGWTR (Modificare scriitor)
 autorizări obiect necesare 443

comandă CPY (Copiere obiect)
 auditare obiect 458

comandă CPY (Copiere)
 auditare obiect 498, 499, 501

comandă CPYIGCSRT (Copiere tabelă sortare
 DBCS)
 auditare obiect 473

comandă HLDWTR (Reținere scriitor)
 autorizarea obiect necesară 443

comandă MOVDOC (Mutare document)
 auditare obiect 464

comandă securitate
 listă 271

comandă TFRJOB (Transfer job)
 auditare obiect 475

comandă WRKCNL (Gestionare liste de
 conexiuni)
 auditare obiect 455

comandă, CL
 Acordare autorizare obiect
 (GRTOBJAUT) 272
 Acordare autorizare utilizator
 (GRTUSRAUT)
 descriere 274
 Acordare permisiune utilizator
 (GRTUSRAUT) 275
 Adăugare autorizare obiect de bibliotecă de
 documente (ADDLOAUT) 275
 Adăugare intrare de autentificare server
 (ADDSVRAUTE) 276
 Adăugare intrare director
 (ADDIRE) 276
 Adăugare intrare listă de autorizații
 (ADDAUTLE) 271

comandă, CL (continuare)
 Add Authorization List Entry
 (ADDAUTLE) 145
 ADDAUTLE (Adăugare intrare listă de
 autorizații) 271
 ADDAUTLE (Add Authorization List
 Entry - Adăugare intrare în lista de
 autorizare) 145
 ADDIRE (Adăugare intrare
 director) 276
 ADDLOAUT (Adăugare autorizare
 obiect de bibliotecă de documente) 275
 ADDSVRAUTE (Adăugare intrare de
 autentificare server) 276
 Afișare auditare de securitate (Valori
 DSPSECAUD)
 descriere 277
 Afișare auditare obiect de bibliotecă de
 documente (DSPDLOAUD) 275
 Afișare autorizare obiect
 (DSPOBJAUT) 272
 Afișare autorizare obiect de bibliotecă de
 documente (DSPDLOAUT) 275
 Afișare descriere obiect (DSPOBJD) 272
 creat de 123
 domeniu obiect 13
 starea program 13
 Afișare deținător de autorizare
 (DSPAUTHLR) 271
 Afișare intrări jurnal de auditare
 (DSPAUDJRNE)
 descriere 277
 Afișare jurnal (DSPJRN)
 afișare jurnal QAUDJRN (audit) 234
 auditare activitate fișier 266
 creare fișier de ieșire 262
 exemplu de jurnal de auditare
 (QAUDJRN) 260, 261
 Afișare listă de autorizații
 (DSPAUTL) 271
 Afișare obiecte de bibliotecă de documente
 pentru listă de autorizații
 (DSPAUTLDLO) 275
 Afișare obiecte listă de autorizații
 (DSPAUTLOBJ) 271
 Afișare profil utilizator (Display User
 Profile) (DSPUSRPRF)
 folosire fișier de ieșire 267
 Afișare profil utilizator (DSPUSRPRF)
 descriere 274
 Afișare program (DSPPGM)
 autorizare adoptată 130
 starea program 13
 Afișare program service (DSPSRVPGM)
 autorizare adoptată 130
 Afișare programe care adoptă
 (DSPPGMADP)
 descriere 275
 folosirea 130
 Afișare utilizatori autorizați
 (DSPAUTUSR)
 descriere 274
 Apelare program (CALL)
 transferare autorizare adoptată 128
 auditare obiect de bibliotecă de documente
 (CHGDLOAUD) 275
 descriere 275

comandă, CL (continuare)
 autorizare obiect, tabelă 272
 CALL (Apelare program)
 transferare autorizare adoptată 128
 CFGSYSSEC (Configurare securitate
 sistem)
 descriere 278
 Change Authorization List Entry
 (CHGAUTLE)
 folosire 145
 Change Journal - Modificare jurnal
 (CHGJRN) 258, 260
 Change Object Auditing (CHGOBJAUD)
 Valoarea de sistem QAUDCTL
 (Control auditare) 50
 Change Object Owner
 (CHGOBJOWN) 142
 Change Object Primary Group
 (CHGOBJPGP) 123, 143
 Change Program (CHGPGM)
 specificarea parametrului
 USEADPAUT 131
 Change Service Program (CHGSRVPGM)
 specificarea parametrului
 USEADPAUT 131
 CHGAUTLE (Change Authorization List
 Entry - Schimbare intrare din lista de
 autorizare)
 folosire 145
 CHGAUTLE (Modificare intrare listă de
 autorizații)
 descriere 271
 CHGDIRE (Modificare intrare
 director) 276
 CHGDLOAUD (Modificare auditare
 obiect bibliotecă document)
 Valoarea de sistem QAUDCTL
 (Control auditare) 50
 CHGDLOAUD (Modificare auditare
 obiect de bibliotecă de documente) 275
 CHGDLOAUT (Modificare autorizare
 obiect de bibliotecă de documente) 275
 CHGDLOOWN (Modificare proprietar
 obiect de bibliotecă de documente) 275
 CHGDLOPGP (Modificare grup primar
 obiect de bibliotecă de documente) 275
 CHGDLOUAD (Modificare auditare
 obiect de bibliotecă de documente)
 descriere 275
 CHGDSTPWD (Modificare parolă Unelte
 de service dedicate) 273
 CHGJOB (Schimbare job)
 autorizare adoptată 130
 CHGJRN (Change Journal - Modificare
 jurnal) 258, 260
 CHGOBJAUD (Modificare auditare
 obiect) 272
 descriere 275
 Valoarea de sistem QAUDCTL
 (Control auditare) 50
 CHGOBJOWN (Change Object Owner -
 Schimbare proprietar obiect) 142
 CHGOBJOWN (Modificare proprietar
 obiect) 272
 CHGOBJPGP (Change Object Primary
 Group - Schimbare grup primar
 obiect) 123, 143

comandă, CL (*continuare*)

CHGOBJPGP (Modificare grup primar de obiecte) 272
 CHGPGM (Change Program - Schimbă program)
 specificarea parametrului
 USEADPAUT 131
 CHGPRF (Modificare profil) 274
 CHGPWD (Change Password - Modificare parolă)
 auditare 231
 CHGPWD (Modificare parolă)
 descriere 273
 valori de sistem de parole de impunere 39
 CHGSECAUD (Modificare auditare de securitate)
 descriere 277
 CHGSRVPGM (Change Service Program - Schimbare program de serviciu)
 specificarea parametrului
 USEADPAUT 131
 CHGSVRAUTE (Modificare intrare de autentificare server) 276
 CHGUSRAUD (Change User Audit - Modificare auditare utilizator)
 Valoarea de sistem QAUDCTL (Control auditare) 50
 CHGUSRAUD (Modificare auditare utilizator) 274
 descriere 275
 CHGUSRPRF (Modificare profil utilizator) 274
 descriere 273
 valori de sistem de compunere parolă 39
 CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului)
 auditare folosire 233
 descriere 269
 CHKOBJITG (Check Object Integrity - Verificare integritate obiect)
 auditare folosire 233
 descriere 269
 CHKOBJITG (Verificare integritate obiect)
 descriere 274
 CHKPWD (Verificare parolă) 273
 Comanda CRTJRNRCV (Create Journal Receiver - Creare receptor jurnal) 256
 comanda DSPAUTUSR (Display Authorized Users - Afișare utilizatori autorizați)
 auditare 267
 Comanda DSPAUTUSR (Display Authorized Users - Afișare utilizatori autorizați)
 auditare 267
 Comanda DSPJOB (Display Object Description - Afișare descriere obiect) 254
 folosire fișier de ieșire 268
 Comanda DSPOBJD (Display Object Description - Afișare descriere obiect) 254
 folosire fișier de ieșire 268
 comanda Save Document Library Object (SAVDLO) 219

comandă, CL (*continuare*)

Configurare securitate sistem (CFGSYSSEC)
 descriere 278
 Creare deținător de autorizare (CRTAUTHLR) 271, 276
 Creare jurnal - Create Journal (CRTJRN) 257
 Creare listă de autorizații (CRTAUTL) 271
 Creare profil utilizator (CRTUSRPRF)
 descriere 273, 274
 Creare receptor jurnal - Create Journal Receiver (CRTJRNRCV) 256
 Create Authority Holder (CRTAUTHLR) 131
 Create Authorization List (CRTAUTL) 144
 Create Library (CRTLIB) 136
 CRTAUTHLR (Creare deținător de autorizare) 271, 276
 CRTAUTHLR (Create Authority Holder - Creare deținător de autorizare) 131
 CRTAUTL (Creare listă de autorizații) 271
 CRTAUTL (Create Authorization List - Creare listă de autorizare) 144
 CRTJRN (Create Journal - Afișare jurnal) 257
 CRTLIB (Create Library) 136
 CRTUSRPRF (Creare profil utilizator)
 descriere 273, 274
 Delete Authority Holder (DLTAUTHLR) 132
 Delete Authorization List (DLTAUTL) 146
 deținător de autorizare, tabelă 271, 276
 director distribuție sistem, tabelă 276
 Display Authority Holder (DSPAUTHLR) 131
 Display Authorization List Objects (DSPAUTOBJ) 146
 Display Document Library Object Auditing - Afișare auditare obiect bibliotecă document (DSPDLOAUD) 254
 Display Job Description - Afișare descriere de job (DSPJOB) 232
 Display Library - Afișare bibliotecă (DSPLIB) 268
 Display Library Description (DSPLIBD)
 Parametrul CRTAUT 137
 DLTAUTHLR (Delete Authority Holder) 132
 DLTAUTHLR (Ștergere deținător de autorizare) 271
 DLTAUTL (Delete Authorization List - Ștergere listă de autorizare) 146
 DLTAUTL (Ștergere listă de autorizații) 271
 DLTJRNRCV (Delete Journal Receiver - Ștergere receptor jurnal) 260
 DLTUSRPRF (Ștergere profil utilizator)
 descriere 274
 drept de proprietate obiect 122
 DSPAUDJRNE (Afișare intrări jurnal de auditare)
 descriere 277

comandă, CL (*continuare*)

DSPAUTHLR (Afișare deținător de autorizare) 271
 DSPAUTHLR (Display Authority Holder - Afișare deținător de autorizare) 131
 DSPAUTL (Afișare listă de autorizații) 271
 DSPAUTLDLO (Afișare obiecte de bibliotecă de documente pentru listă de autorizații) 275
 DSPAUTLOBJ (Afișare obiecte listă de autorizații) 271
 DSPAUTLOBJ (Display Authorization List Objects - Afișare obiecte din lista de autorizare) 146
 DSPAUTUSR (Afișare utilizatori autorizați)
 descriere 274
 DSPDLOAUD (Afișare auditare obiect de bibliotecă de documente) 275
 DSPDLOAUD (Display Document Library Object Auditing - Afișare auditare obiect bibliotecă document) 254
 DSPDLOAUD (Afișare autorizare obiect de bibliotecă de documente) 275
 DSPJOB (Display Job Description - Afișare descriere de job) 232
 DSPJRN (Afișare jurnal)
 afișare jurnal QAUDJRN (audit) 234
 auditare activitate fișier 266
 creare fișier de ieșire 262
 exemplu de jurnal de auditare (QAUDJRN) 260, 261
 DSPLIB (Display Library - Afișare bibliotecă) 268
 DSPLIBD (Display Library Description)
 Parametrul CRTAUT 137
 DSPOBJAUT (Afișare autorizare obiect) 272
 DSPOBJAUT (Display Object Authority - Afișare autorizare obiect) 268
 DSPOBJD (Afișare descriere obiect) 272
 creat de 123
 DSPOBJD (Display Object Description - Afișare descriere obiect)
 domeniu obiect 13
 starea program 13
 DSPPGM (Afișare program)
 autorizare adoptată 130
 DSPPGM (Display Program - Afișare program)
 starea program 13
 DSPPGMADP (Afișare programe care adoptă)
 descriere 275
 folosirea 130
 DSPPGMADP (Display Programs That Adopt - Afișare programe care adoptă) auditare 268
 DSPSECAUD (Afișare valori de auditare de securitate)
 descriere 277
 DSPSRVPGM (Afișare program service)
 autorizare adoptată 130
 DSPUSRPRF (Afișare profil utilizator)
 descriere 274

comandă, CL (<i>continuare</i>)	comandă, CL (<i>continuare</i>)	comandă, CL (<i>continuare</i>)
DSPUSRPRF (Display User Profile - Afișare profil utilizator) folosire fișier de ieșire 267	Lucru cu liste de autorizație (WRKAUTL) 271	PRTCMNSEC (Tipărire securitate comunicații) descriere 278
Edit Authorization List (EDTAUTL) 145	Lucru cu obiecte (WRKOBJ) 272	PRTJOBDAUT (Tipărire autorizare descriere de job) 277
Edit Object Authority (EDTOBJAUT) 138	Lucru cu obiecte după grup primar (WRKOBJPGP) descriere 272	PRTPUBAUT (Tipărire obiecte autorizate public) 277
Editare autorizare obiect (EDTOBJAUT) 272	Lucru cu obiecte după proprietar (WRKOBJOWN) descriere 272	PRTPVTAUT (Tipărire autorizări private) 277
Editare autorizare obiect de bibliotecă de documente (EDTDLOAUT) 275	Lucru cu profiluri utilizator (WRKUSRPRF) 274	PRTQAUT (Tipărire autorizare coadă) descriere 277
Editare listă de autorizații (EDTAUTL) 271	Modificare auditare de securitate (CHGSECAUD) descriere 277	PRTSBSDAUT (Tipărire autorizare descriere subsistem) descriere 277
EDTAUTL (Edit Authorization List - Editare listă de autorizare) 145	Modificare auditare obiect (CHGOBJAUD) 272	PRTSYSSECA (Tipărire atribute de securitate sistem) descriere 278
EDTAUTL (Editare listă de autorizații) 271	Modificare auditare obiect bibliotecă document (CHGDLOAUD) Valoarea de sistem QAUDCTL (Control auditare) 50	PRTTRGPGM (Tipărire programe de declanșare) descriere 277
EDTDLOAUT (Editare autorizare obiect de bibliotecă de documente) 275	Modificare auditare utilizator (CHGUSRAUD) 274	PRTUSROBJ (Tipărire obiecte utilizator) descriere 277
EDTOBJAUT (Edit Object Authority) 138	descriere 275	RCLSTG (pretindere spațiu de stocare) 17, 22, 124
EDTOBJAUT (Editare autorizare obiect) 272	Modificare autorizare obiect de bibliotecă de documente (CHGDLOAUT) 275	RCLSTG (Reclaim Storage) 227
ENDJOB (End Job - Terminare job) Valoarea de sistem QINACTMSGQ 24	Modificare grup primar de obiecte (CHGOBJPGP) 272	Reclaim Storage (RCLSTG) 227
Extragere intrare listă de autorizații (RTVAUTLE) 271	Modificare grup primar obiect de bibliotecă de documente (CHGDLOPGP) 275	Remove Authorization List Entry (RMVAUTLE) 145
Extragere profil utilizator (RTVUSRPRF) 274	Modificare intrare de autentificare server (CHGSVRAUTE) 276	Restaurare autorizare (RSTAUT) descriere 275 folosind 223 procedură 224
Gestionare atribute jurnal (Work with Journal Attributes - WRKJRNA) 260, 267	Modificare intrare director (CHGDIRE) 276	Restaurare profiluri utilizator (RSTUSRPRF) 219, 275
Gestionare jurnal (Work with Journal - WRKJRN) 260, 267	Modificare intrare listă de autorizații (CHGAUTLE) descriere 271	Restore Authority (RSTAUT) rol în restaurarea securității 219
Gestionare valori de sistem (Work with System Values - WRKSYSVAL) 230	Modificare parolă (Change Password - CHGPWD) auditare 231	Restore Authority - Restaurare autorizare (RSTAUT) intrare jurnal auditare (QAUDJRN) 245
Grant Object Authority (GRTOBJAUT) efectul asupra autorizării anterioare 141 obiecte multiple 141	Modificare parolă (CHGPWD) descriere 273 valori de sistem de parole de impunere 39	Restore Document Library Object (RSTDLO) 219
Grant User Authority (GRTUSRAUT) recomandări 144	Modificare parolă Unelte de service dedicate (CHGDSTPWD) 273	Restore Library (RSTLIB) 219
GRTOBJAUT (Acordare autorizare obiect) 272	Modificare profil (CHGPRF) 274	Restore Licensed Program (RSTLICPGM) recomandări 225 riscuri de securitate 225
GRTOBJAUT (Grant Object Authority) efectul asupra autorizării anterioare 141 obiecte multiple 141	Modificare profil utilizator (CHGUSRPRF) 274 descriere 273 valori de sistem de compunere parolă 39	Restore Object (RSTOBJ) folosind 219
Grant User Authority (GRTUSRAUT) Acordare autorizare utilizator) descriere 274	Modificare proprietar obiect (CHGOBJOWN) 272	Revocare autorizare obiect (RVKOBJAUT) 272
GRTOBJAUT (Grant Object Authority - Acordare autorizare utilizator) recomandări 144	Modificare proprietar obiect de bibliotecă de documente (CHGDLOOWN) 275	Revocare autorizare publică (RVKPUBAUT) descriere 278
GRTUSRAUT (Acordare autorizare utilizator) descriere 274	obiect de bibliotecă de documente (DLO) tabelă 275 parole, tabelă 273	Revocare permisiune utilizator (RVKUSRPMN) 275
GRTUSRAUT (Grant User Authority - Acordare autorizare utilizator) recomandări 144	Pretindere spațiu de stocare (RCLSTG) 17, 22, 124	Revoke Object Authority (RVKOBJAUT) 146
GRTUSRPMN (Acordare permisiuni utilizator) 275	profiluri utilizator (înruit), tabelă 275	RMVAUTLE (Înlăturare intrare listă de autorizații) 271
Înlăturare autorizare obiect de bibliotecă de documente (RMVDLOAUT) 275	profiluri utilizator(lucru cu), tabelă 274	RMVAUTLE (Remove Authorization List Entry - Ștergere intrare din lista de autorizare) 145
Înlăturare intrare de autentificare server (RMVSVRAUTE) 276		RMVDIRE (Înlăturare intrare director) 276
Înlăturare intrare director (RMVDIRE) 276		RMVDLOAUT (Înlăturare autorizare obiect de bibliotecă de documente) 275
Înlăturare intrare listă de autorizații (RMVAUTLE) 271		
liste de autorizații 271		
Lucru cu directoare (WRKDIRE) 276		

comandă, CL (*continuare*)
 RMVSVRAUTE (Înlăturare intrare de autentificare server) 276
 RSTAUT (Restaurare autorizare) descriere 275
 RSTAUT (Restore Authority - Restaurare autorizare) folosind 223
 intrare jurnal auditare (QAUDJRN) 245
 procedură 224
 RSTAUT (Restore Authority) rol în restaurarea securității 219
 RSTDLO (Restore Document Library Object) 219
 RSTLIB (Restore Library) 219
 RSTLICPGM (Restore Licensed Program - Restaurare program licențiat) recomandări 225
 riscuri de securitate 225
 RSTOBJ (Restore Object) folosind 219
 RSTUSRPRF (Restaurare profiluri utilizator) 275
 RSTUSRPRF (Restore User Profiles) 219
 RTVAUTLE (Extragere intrare listă de autorizații) 271
 RTVUSRPRF (Extragere profil utilizator) 274
 RVKOBJAUT (Revocare autorizare obiect) 272
 RVKOBJAUT (Revoke Object Authority) 146
 RVKPUBAUT (Revocare autorizare publică) descriere 278
 RVKUSRPMN (Revocare permisiune utilizator) 275
 Salvare date de securitate (SAVSECDTA) 275
 Salvare obiect (SAVOBJ) 260
 Salvare sistem (SAVSYS) 275
 SAVDLO (Save Document Library Object) 219
 Save Library (SAVLIB) 219
 Save Object (SAVOBJ) 219
 Save Security Data (SAVSECDTA) 219
 Save System (SAVSYS) 219
 SAVLIB (Save Library) 219
 SAVOBJ (Save Object - Salvare obiect) 260
 SAVOBJ (Save Object) 219
 SAVSECDTA (Salvare date de securitate) 275
 SAVSECDTA (Save Security Data) 219
 SAVSYS (Salvare sistem) 275
 SAVSYS (Save System) 219
 Schimbare job (CHGJOB) autorizare adoptată 130
 securitate, listă 271
 Send Journal Entry - Trimitere intrare jurnal (SNDJRNE) 258
 setare valoare de sistem QALWUSRDMN (permitere obiecte utilizator) 22
 SNDJRNE (Send Journal Entry - Trimitere intrare jurnal) 258

comandă, CL (*continuare*)
 Ștergere deținător de autorizare (DLTAUTHLR) 271
 Ștergere listă de autorizații (DLTAUTL) 271
 Ștergere profil utilizator (DLTUSRPRF) descriere 274
 drept de proprietate obiect 122
 Ștergere receptor jurnal (DLTJRNRVCV) 260
 Terminare job (ENDJOB) Valoarea de sistem QINACTMSGQ 24
 TFRCTL (Control transfer) transferare autorizare adoptată 129
 TFRGRPJOB (Transfer la job grup) autorizare adoptată 129
 Tipărire atribute de securitate comunicații (PRTCMNSEC) descriere 278
 Tipărire atribute de securitate sistem (PRTSYSSECA) descriere 278
 Tipărire autorizare coadă (PRTQAUT) descriere 277
 Tipărire autorizare descriere de job (PRTJOBDAUT) 277
 Tipărire autorizare descriere subsistem (PRTSBSDAUT) descriere 277
 Tipărire autorizări private (PRTPVTAUT) 277
 Tipărire obiecte autorizate public (PRTPUBAUT) 277
 Tipărire obiecte utilizator (PRTUSROBJ) descriere 277
 Tipărire programe de declanșare (PRTTRGPGM) descriere 277
 Transferare control (TFRCTL) transferare autorizare adoptată 129
 Transferare la job grup (TFRGRPJOB) autorizare adoptată 129
 unelte de securitate 277, 617
 Verificare integritate obiect (CHKOBJITG) descriere 274
 Verificare parolă (CHKPWD) 273
 Work with Objects by Owner (WRKOBJOWN) folosire 142
 Work with Objects by Primary Group (WRKOBJJPGP) 123, 143
 WRKAUTL (Lucru cu liste de autorizație) 271
 WRKDIRE (Lucru cu directoare) 276
 WRKJRN (Work with Journal - Gestionare jurnal) 260, 267
 WRKJRNA (Work with Journal Attributes - Gestionare atribute jurnal) 260, 267
 WRKOBJ (Lucru cu obiecte) 272
 WRKOBJOWN (Lucru cu obiecte după proprietar) descriere 272
 WRKOBJOWN (Work with Objects by Owner - Gestionare obiecte după proprietar) auditare 232

comandă, CL (*continuare*)
 WRKOBJOWN (Work with Objects by Owner - Gestionare obiecte după proprietar) (*continuare*) folosire 142
 WRKOBJJPGP (Lucru cu obiecte după grup primar) descriere 272
 WRKOBJJPGP (Work with Objects by Primary Group - Gestionare obiecte după grupul primar) 123, 143
 WRKSYSVAL (Work with System Values - Gestionare valori de sistem) 230
 WRKUSRPRF (Lucru cu profiluri utilizator) 274
 comandă, generică
 Change Authority (CHGAUT) 138
 Change Owner (CHGOWN) 142
 Change Primary Group (CHGPGP) 143
 CHGAUT (Change Authority) 138
 CHGOWN (Change Owner - Schimbă proprietar) 142
 CHGPGP (Change Primary Group - Schimbare grup primar) 143
 Grant Object Authority (GRTOBJAUT) 138
 GRTOBJAUT (Grant Object Authority) 138
 Revoke Object Authority (RVKOBJAUT) 138
 RVKOBJAUT (Revoke Object Authority) 138
 Work with Authority (WRKAUT) 138
 WRKAUT (Work with Authority) 138
 comandă, obiect generic
 Afișare autorizare (DSPAUT) 272
 CHGAUD (Modificare auditare) 272 descriere 275
 CHGAUT (Modificare autorizare) 272
 CHGOWN (Schimbare proprietar) 272
 CHGPGP (Modificare grup primar) 272
 DSPAUT (Afișare autorizare) 272
 Lucru cu autorizare (WRKAUT) 272
 Modificare auditare (CHGAUD) 272 descriere 275
 Modificare autorizare (CHGAUT) 272
 Modificare grup primar (CHGPGP) 272
 Schimbare proprietar (CHGOWN) 272
 WRKAUT (Lucru cu autorizare) 272
 Comands CRTQSTLOD (Create Question-and-Answer Load - Creare încărcare Întrebare-și-Răspuns) autorizarea obiect necesară 417
 Comands DLTQST (Delete Question - Ștergere întrebare) autorizarea obiect necesară 417
 Comands DLTQSTDB (Delete Question-and-Answer Database - Ștergere bază de date Întrebare-și-Răspuns) autorizarea obiect necesară 417
 Comands LODQSTDB (Load Question-and-Answer Database - Încărcare bază de date Întrebare-și-Răspuns) autorizarea obiect necesară 418
 combinare metode de autorizare exemplu 171

comenzi
 Dezvoltare de aplicații 312
 Comenzi asistent operațional
 autorizare obiect cerută pentru
 comenzi 400
 comenzi CHGIMGCLG
 autorizarea obiect necesară 346
 comenzi CHGIMGCLGE
 autorizarea obiect necesară 346
 comenzi descriere cerere de modificare
 autorizare obiect cerută pentru
 comenzi 315
 comenzi descriere fus orar 438
 comenzi dezvoltare
 Aplicații 312
 Comenzi dezvoltare aplicație 312
 Comenzi înlocuire 212
 Compania de jucării JKL
 diagramă a aplicațiilor 195
 comparație
 profil de grup și listă de autorizații 215
 complex
 autorizare
 exemplu 171
 comunicații
 monitorizare 233
 comunicații interproces
 incorect
 intrare jurnal auditare
 (QAUDJRN) 240
 comutator cheie
 auditare 230
 conexiune
 oprire
 intrare jurnal auditare
 (QAUDJRN) 242
 pornire
 intrare jurnal auditare
 (QAUDJRN) 242
 confidențialitate 1
 configurare
 auditare securitate 619
 configurare sistem
 autorizare specială *IOSYSCFG
 (configurare sistem) 71
 configurație
 automată
 dispozitive virtuale (valoare de sistem
 QAUTOVRT) 32
 autorizare obiect cerută pentru
 comenzi 321
 configurație LAN de comunicație fără fir
 autorizare obiect cerută pentru
 comenzi 336
 configurație LAN de comunicație fără fir
 extinsă
 autorizare obiect cerută pentru
 comenzi 336
 configurație server de rețea
 autorizare obiect cerută pentru
 comenzi 399
 consolă
 autorizare necesară pentru semnare 179
 QSECOFR (responsabil cu securitatea)
 profil utilizator 179
 QSRV (service) profil utilizator 179
 consolă (continuare)
 QSRVBAS (service de bază) profil
 utilizator 179
 restricționare acces 230
 valoare de sistem QCONSOLE 179
 consolă sistem
Vedeți și consolă
 valoare de sistem QCONSOLE 179
 contabilizare job
 profil utilizator 82
 control comitere
 autorizare obiect cerută pentru
 comenzi 320
 controlare
 acces
 cerere DDM (DDM) 190
 iSeries Access 189
 obiecte 13
 programe sistem 13
 auditare 50
 la distanță
 prezentare job 189
 semnare (valoarea de sistem
 QRMTSIGN) 27
 listă de bibliotecă utilizator 201
 operații de restaurare 191
 operații de salvare 191
 conținut
 unelte de securitate 277, 617
 copiere
 autorizare de utilizator
 exemplu 101
 redenumire profil 106
 autorizare utilizator
 descriere comandă 274
 recomandări 144
 fișier spool 186
 profil utilizator 99
 copierea de rezervă a
 informațiilor de securitate 219
 corecție temporară obiect (PTF)
 autorizare obiect cerută pentru
 comenzi 424
 CPYFCNARA
 profiluri utilizator livrat de IBM
 autorizate 289
 CPYGPFFMT
 profiluri utilizator livrat de IBM
 autorizate 289
 CPYGPFFPKG
 profiluri utilizator livrat de IBM
 autorizate 289
 CPYPPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 289
 CPYPTFGRP (Copy Program Temporary Fix
 Group - Copiere grup corecții temporare
 program) 289
 creare
 auditare receptor jurnal 256
 bibliotecă 136
 coada de ieșire 188
 coadă de ieșire 186
 comanda
 parametru ALWLMTUSR (permitere
 utilizator limitat) 67
 creare (continuare)
 comanda (continuare)
 parametrul PRDLIB (biblioteca
 produs) 185
 riscuri de securitate 185
 deținător de autorizare 131, 271, 276
 jurnal audit 257
 listă de autorizare 144
 listă de autorizații 271
 meniu
 parametrul PRDLIB (biblioteca
 produs) 185
 riscuri de securitate 185
 obiect
 intrare jurnal auditare
 (QAUDJRN) 123, 241
 profil utilizator
 descrieri comenzi 273, 274
 exemplu 98
 intrare jurnal auditare
 (QAUDJRN) 245
 metode 96
 program
 autorizare adoptată 130
 creare automată
 profil utilizator 57
 Creare liste de validare (CRTVLDL) 216
 creare obiect
 auditare obiect 448
 criptare
 parolă 60
 criptografie
 autorizare obiect cerută pentru
 comenzi 324
 CRTBNDCL
 autorizarea obiect necesară 377
 CRTCLMOD
 autorizarea obiect necesară 378
 CRTCLU
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTCRG
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTFCNARA
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTFNNTBL (Create DBCS Font Table -
 Creare tabelă fonturi DBCS)
 necesități ale autorizării obiect pentru
 comenzi 311
 CRTGPHFMT
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTGPHPKG
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTHSTDTA
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTIMGCLG
 profiluri utilizator livrat de IBM
 autorizate 290
 CRTPPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 290

CRTUDFS
 profiluri utilizator livrat de IBM
 autorizate 290
 curățare
 necesități ale autorizării obiect pentru
 comenzi 400
 CVTDIR
 profiluri utilizator livrat de IBM
 autorizate 290
 CVTPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 290
 CVTPFRTHD
 profiluri utilizator livrat de IBM
 autorizate 290

D

date confidențiale
 protejare 232
 date de securitate
 salvare 275
 salvarea 219
 date sensibile
 criptare 233
 protejare 232
 DDM (gestiune date distribuite)
 securitate 190
 DDMACC (cerere DDM acces) atribut
 rețea 190
 definiție interactivă de date
 autorizatie obiect cerută pentru
 comenzi 366
 delete (*DLT) authority 112
 delogare
 rețea
 intrare jurnal auditare
 (QAUDJRN) 242
 depășire
 limită cont
 intrare jurnal auditare
 (QAUDJRN) 251
 derulare
 întoarcere (*ROLLKEY opțiune
 utilizator) 90
 descriere
 cerințe securitate bibliotecă 202
 securitate meniu 207
 descriere alertă
 autorizatie obiect cerută pentru
 comenzi 312
 descriere clasă-de-serviciu
 autorizatie obiect cerută pentru
 comenzi 316
 descriere controler
 autorizatie obiect cerută pentru
 comenzi 323
 tipărire parametrului relevanți de
 securitate 621
 descriere de job
 afișare 232
 implicită (QDFTJOB) 78
 intrare de comunicații 181
 intrare stație de lucru 181
 modificare
 intrare jurnal auditare
 (QAUDJRN) 248

descriere de job (*continuare*)
 monitorizare 232
 nivel de securitate 40 13
 parametru USER 181
 probleme de securitate 182
 profil utilizator 78
 protecție 13
 protejare resurse sistem 192
 QDFTJOB (implicită) 78
 recomandări 79
 restaurare
 intrare jurnal auditare
 (QAUDJRN) 244
 descriere de job QDFTJOB (implicită) 78
 descriere de linie
 autorizatie obiect cerută pentru
 comenzi 387
 descriere de subsistem
 intrare de comunicații 181
 modificare intrare rutare
 intrare jurnal auditare
 (QAUDJRN) 249
 performanța 192
 descriere dispozitiv
Vedeți și dispozitiv
 autorizare de folosire 177
 autorizatie obiect cerută pentru
 comenzi 326
 creare
 autorizare publică 119
 valoarea de sistem QCRTAUT (creare
 autorizare) 119
 definiție 177
 drept de proprietate
 deținut de QPGMR (programator)
 profil 179
 deținut de QSECOFR (responsabil cu
 securitatea) profil utilizator 179
 modificare 179
 proprietar implicit 179
 securizare 177
 tipărire parametrului relevanți de
 securitate 621
 descriere editare
 autorizatie obiect cerută pentru
 comenzi 336
 descriere interfață de rețea
 autorizatie obiect cerută pentru
 comenzi 397
 descriere job
 tipărire parametrului relevanți de
 securitate 621
 descriere mesaj
 autorizatie obiect cerută pentru
 comenzi 392
 descriere mod
 autorizatie obiect cerută pentru
 comenzi 394
 Descriere NetBIOS
 autorizatie obiect cerută pentru
 comenzi 395
 descriere obiect
 afișare 272
 descriere server de rețea
 autorizatie obiect cerută pentru
 comenzi 399

descriere subsistem
 autorizare 277
 intrare 277
 tipărire listă de descrieri 277
 tipărire parametrului relevanți de
 securitate 621
 utilizator implicit 277
 descrierea de subsistem
 securitate 181
 descriptor
 înaintare
 intrare jurnal auditare
 (QAUDJRN) 248
 descrierea de job
 autorizatie obiect cerută pentru
 comenzi 370
 detașare
 auditare receptor jurnal 259, 260
 receptor jurnal 258
 deținător de autorizare
 afișare 131, 271
 auditare obiect 451
 autorizatie obiect cerută pentru
 comenzi 314
 comenzi pentru lucrul cu 271, 276
 creare 131, 271, 276
 creat automat 132
 descriere 131
 limita de stocare maximă depășită 124
 migrarea la System/36 132
 restaurarea 219
 riscuri 133
 salvarea 219
 ștergere 132, 271
 tipărire 277
 dezactivare
 funcție de auditare 260
 nivel de securitate 40 16
 nivel de securitate 50 18
 profil utilizator 62
 automat 617
 dezactivare (*DISABLED) stare profil
 utilizator
 descriere 62
 profil utilizator QSECOFR (responsabil cu
 securitatea) 62
 diagramă de flux
 verificare autorizare 147
 dicționar ajutător pentru corectare ortografică
 autorizatie obiect cerută pentru
 comenzi 428
 director
 autorizare 5
 obiecte noi 119
 autorizatie obiect cerută pentru
 comenzi 316, 329, 346, 347
 lucru cu 276
 securitate 117
 director baze de date relaționale
 autorizatie obiect cerută pentru
 comenzi 419
 director de distribuție sistem
 autorizare specială *SECADM
 (administrator de securitate) 69
 ștergere profil utilizator 101

director de legare
autorizație obiect cerută pentru
comenzi 314

director distribuție
modificare
intrare jurnal auditare
(QAUDJRN) 243

director distribuție sistem
comenzi pentru lucrul cu 276

director distribuție, sistem
comenzi pentru lucrul cu 276

director sistem
modificare
intrare jurnal auditare
(QAUDJRN) 243

director, sistem, distribuție
comenzi pentru lucrul cu 276

disc
parametru limitare de folosire
(MAXSTG) 76

dischetă
autorizație obiect cerută pentru
comenzi 389

disponibilitate 1

dispozitiv
Vedeți și descriere dispozitiv
autorizare de semnare 177
securizare 177
virtual
configurația automată (valoarea de
sistem QAUTOVRT) 32
definiție 32

dispozitiv virtual
configurația automată (valoarea de sistem
QAUTOVRT) 32
definiție 32

Disponere de fișier înregistrare generică 539

dispunere fișier 512

dispunere fișier (PG) modificare grup
primar 572

dispunere fișier acordare descriptor (GS) 544

dispunere fișier acțiuni comunicații între
procese (IP) 545

dispunere fișier acțiuni mail (ML) 558

dispunere fișier acțiuni reguli IP (IR) 547

dispunere fișier AD (auditare
modificare) 512

dispunere fișier adoptare program (PA) 570

dispunere fișier AF (eșuare autorizare) 514

dispunere fișier AP (autorizare adoptată) 519

dispunere fișier AU (modificare atribut) 519

dispunere fișier auditare modificare
(AD) 512

dispunere fișier CA (modificare
autorizare) 520

dispunere fișier CD (șir comenzi) 522

dispunere fișier CO (creare obiect) 523

dispunere fișier configurație criptografică
(CY) 530

dispunere fișier CP (modificare profil
utilizator) 525

dispunere fișier CQ (modificare
*CRQD) 527

dispunere fișier creare obiect (CO) 523

dispunere fișier CU (Operații cluster) 527

dispunere fișier cu acces resursă rețea
(VR) 602

dispunere fișier cu acțiune către fișierul spool
(SF) 586

dispunere fișier cu acțiune pentru valoarea
sistem (SV) 597

dispunere fișier cu acțiune unelte service
(ST) 593

dispunere fișier cu acțiuni informații utilizator
de securitate server (SO) 593

dispunere fișier cu autentificare kerberos
(X0) 605

dispunere fișier cu citire obiect (ZR) 614

dispunere fișier cu citirea obiectului DLO
(YR) 611

dispunere fișier cu eroare parolă rețea
(VP) 601

dispunere fișier cu închiderea fișierelor server
(VF) 598

dispunere fișier cu limită cont depășită
(VL) 599

dispunere fișier cu listă de validare (VO) 600

dispunere fișier cu logare și delogare rețea
(VN) 599

dispunere fișier cu modificare autorizare
pentru obiectul restaurat (RA) 578

dispunere fișier cu modificare de grup primar
pentru obiectul restaurat (RZ) 583

dispunere fișier cu modificare director de
distribuție sistem (SD) 585

dispunere fișier cu modificare drept de
proprietate pentru obiectul restaurat
(RO) 580

dispunere fișier cu modificare gestiune sisteme
(SM) 592

dispunere fișier cu modificare intrare rutare
subsistem (SE) 586

dispunere fișier cu modificare obiect
(ZC) 611

dispunere fișier cu modificare profil rețea
(VU) 603

dispunere fișier cu modificare stare service
(VV) 604

dispunere fișier cu modificarea listei de control
acces (VA) 597

dispunere fișier cu modificarea obiectului DLO
(YC) 610

dispunere fișier cu restaurare *CRQD
(RQ) 583

dispunere fișier cu restaurare autorizare pentru
profil utilizator (RU) 583

dispunere fișier cu restaurare descriere job
(RJ) 579

dispunere fișier cu restaurare programe care
adoptă autorizare (RP) 581

dispunere fișier cu sesiune server (VS) 603

dispunere fișier cu terminare și oprire
conexiune (VC) 598

dispunere fișier CV (verificare
conexiune) 528

dispunere fișier CY (configurație
criptografică) 530

dispunere fișier DI (Directory Server) 532

dispunere fișier director APPN (ND) 559

dispunere fișier DO (operație ștergere) 536

dispunere fișier DS (Resetare ID utilizator
unelte service furnizate de IBM) 538

dispunere fișier eșuare autorizare (AF) 514

dispunere fișier EV (variabilă mediu) 539

dispunere fișier gestiune securitate internet
(GS) 548

dispunere fișier GR (înregistrare
generică) 539

dispunere fișier GS (acordare descriptor) 544

dispunere fișier ieșire imprimantă (PO) 574

dispunere fișier interschimbare profil
(PS) 575

dispunere fișier IP (acțiuni comunicații între
procese) 545

dispunere fișier IR (acțiuni reguli IP) 547

dispunere fișier IS (gestiune securitate
internet) 548

dispunere fișier JD (modificare descriere
job) 550

dispunere fișier JS (modificare job) 550

dispunere fișier KF (fișier inel de chei) 554

dispunere fișier LD (director de căutare, legare,
dezlegare) 557

dispunere fișier ML (acțiuni mail) 558

dispunere fișier modificare *CRQD
(CQ) 527

dispunere fișier modificare atribut (AU) 519

dispunere fișier modificare atribut rețea
(NA) 559

dispunere fișier modificare autorizare
(CA) 520

dispunere fișier modificare descriere job
(JD) 550

dispunere fișier modificare drept de proprietate
(OW) 566

dispunere fișier modificare job (JS) 550

dispunere fișier modificare profil utilizator
(CP) 525

dispunere fișier NA (modificare atribut
rețea) 559

dispunere fișier ND (director APPN) 559

dispunere fișier NE (punct final APPN) 560

dispunere fișier operație ștergere (DO) 536

dispunere fișier Operații cluster (CU) 527

dispunere fișier OW (modificare drept de
proprietate) 566

dispunere fișier PA (adoptare program) 570

dispunere fișier PG (modificare grup
primar) 572

dispunere fișier PO (ieșire imprimantă) 574

dispunere fișier PS (interschimbare
profil) 575

dispunere fișier punct final APPN (NE) 560

dispunere fișier QASYADJE (auditare
modificare) 512

dispunere fișier QASYAFJE (eșuare
autorizare) 514

dispunere fișier QASYAPJE (autorizare
adoptată) 519

dispunere fișier QASYAUJ5 (modificare
atribut) 519

dispunere fișier QASYCAJE (modificare
autorizare) 520

dispunere fișier QASYCDJE (șir
comenzi) 522

dispunere fișier QASYCOJE (creare
obiect) 523

dispunere fișier QASYCPJE (modificare profil
utilizator) 525

dispunere fișier QASYCQJE (modificare
*CRQD) 527

dispunere fișier QASYCUJ4 (Operații cluster) 527

dispunere fișier QASYCVJ4 (verificare conexiune) 528

dispunere fișier QASYCYJ4 (configurație criptografică) 530

dispunere fișier QASYCYJ4 (Directory Server) 532

dispunere fișier QASYDOJE (operație ștergere) 536

dispunere fișier QASYDSJE (Resetare ID utilizator unelte service furnizate de IBM) 538

dispunere fișier QASYEVJE (EV) 539

dispunere fișier QASYGRJ4 (înregistrare generică) 539

dispunere fișier QASYGSJE (acordare descriptor) 544

dispunere fișier QASYGSJE (acțiuni comunicații între procese) 545

dispunere fișier QASYGSJE (gestiune securitate internet) 548

dispunere fișier QASYIRJ4 (acțiuni reguli IP) 547

dispunere fișier QASYJDJE (modificare descriere job) 550

dispunere fișier QASYJSJE (modificare job) 550

dispunere fișier QASYKFJ4 (fișier inel de chei) 554

dispunere fișier QASYLDJE (director de căutare, legare, dezlegare) 557

dispunere fișier QASYMLJE (acțiuni mail) 558

dispunere fișier QASYNAJE (modificare atribut rețea) 559

dispunere fișier QASYNDJE (director APPN) 559

dispunere fișier QASYNEJE (punct final APPN) 560

dispunere fișier QASYO1JE (acces optic) 567, 568

dispunere fișier QASYO3JE (acces optic) 569

dispunere fișier QASYOMJE (gestiune obiect) 560

dispunere fișier QASYORJE (restaurare obiect) 563

dispunere fișier QASYOWJE (modificare drept de proprietate) 566

dispunere fișier QASYPAJE (adoptare program) 570

dispunere fișier QASYPGJE (modificare grup primar) 572

dispunere fișier QASYPSJE (interschimbare profil) 575

dispunere fișier QASYPWJE (parolă) 576

dispunere fișier QASYRAJE (modificare de autorizare pentru obiectul restaurat) 578

dispunere fișier QASYRJJE (restaurare descriere job) 579

dispunere fișier QASYROJE (modificare drept de proprietate pentru programul obiect) 580

dispunere fișier QASYRPJE (restaurare programe care adoptă autorizare) 581

dispunere fișier QASYRQJE (restaurare *CRQD care adoptă autorizare) 582

dispunere fișier QASYRUJE (restaurare autorizare pentru profil utilizator) 583

dispunere fișier QASYRZJE (modificare grup primar pentru obiectele restaurate) 583

dispunere fișier QASYSDJE (modificare director de distribuție sistem) 585

dispunere fișier QASYSEJE (modificare intrare rutare subsistem) 586

dispunere fișier QASYSFJE (acțiune către fișierul spool) 586

dispunere fișier QASYSGJ4() 590, 591

dispunere fișier QASYSMJE (modificare gestiune sisteme) 592

dispunere fișier QASYSOJ4 (acțiuni informații utilizator de securitate server) 593

dispunere fișier QASYSTJE (acțiune unelte service) 593

dispunere fișier QASYSVJE (acțiune pentru valoarea sistem) 597

dispunere fișier QASYVAJE (modificarea listei de control acces) 597

dispunere fișier QASYVCJE (terminare și oprire conexiune) 598

dispunere fișier QASYVFJE (închiderea fișierelor server) 598

dispunere fișier QASYVLJE (limită cont depășită) 599

dispunere fișier QASYVNJE (logare și delogare rețea) 599

dispunere fișier QASYVOJ4 (listă de validare) 600

dispunere fișier QASYVPJE (eroare parolă rețea) 601

dispunere fișier QASYVRJE (acces resursă rețea) 602

dispunere fișier QASYVSJE (sesiune server) 603

dispunere fișier QASYVUJE (modificare profil rețea) 603

dispunere fișier QASYVVJE (modificare stare service) 604

dispunere fișier QASYX0JE (autentificare kerberos) 605

dispunere fișier QASYXCJE (modificarea obiectului DLO) 610

dispunere fișier QASYXRJE (citirea obiectului DLO) 611

dispunere fișier QASYZCJE (modificare obiect) 611

dispunere fișier QASYZRJE (citire obiect) 614

dispunere fișier SD (modificare director de distribuție sistem) 585

dispunere fișier SE (modificare intrare rutare subsistem) 586

dispunere fișier server director (DI) 532

dispunere fișier SF (acțiune către fișierul spool) 586

dispunere fișier SM (modificare gestiune sisteme) 592

dispunere fișier SO (acțiuni informații utilizator de securitate server) 593

dispunere fișier ST (acțiune unelte service) 593

dispunere fișier SV (acțiune pentru valoarea sistem) 597

dispunere fișier șir comenzi (CD) 522

dispunere fișier VA (modificarea listei de control acces) 597

dispunere fișier VC (terminare și oprire conexiune) 598

dispunere fișier verificare conexiune (CV) 528

dispunere fișier VF (închiderea fișierelor server) 598

dispunere fișier VL (limită cont depășită) 599

dispunere fișier VN (logare și delogare rețea) 599

dispunere fișier VO (listă de validare) 600

dispunere fișier VP (eroare parolă rețea) 601

dispunere fișier VR (acces resursă rețea) 602

dispunere fișier VS (sesiune server) 603

dispunere fișier VU (modificare profil rețea) 603

dispunere fișier VV (modificare stare service) 604

dispunere fișier X0 (autentificare kerberos) 605

dispunere fișier YC (modificarea obiectului DLO) 610

dispunere fișier YR (citirea obiectului DLO) 611

dispunere fișier ZC (modificare obiect) 611

dispunere fișier ZR (citire obiect) 614

distribuție

- autorizație obiect cerută pentru comenzi 330

DLO (obiect de bibliotecă de documente) autorizare descrieri comenzi 275

DLTCLU

- profiluri utilizator livrat de IBM autorizate 290

DLTCRGCLU

- profiluri utilizator livrat de IBM autorizate 290

DLTEXPSPLF

- profiluri utilizator livrat de IBM autorizate 290

DLTFCNARA

- profiluri utilizator livrat de IBM autorizate 290

DLTFNTTBL (Delete DBCS Font Table - Ștergere tabelă fonturi DBCS) autorizație obiect cerută pentru comenzi 311

DLTGPHFMT
 profiluri utilizator livrat de IBM
 autorizate 290

DLTGPHPKG
 profiluri utilizator livrat de IBM
 autorizate 290

DLTHSTDTA
 profiluri utilizator livrat de IBM
 autorizate 291

DLTIMGCLG
 profiluri utilizator livrat de IBM
 autorizate 291

DLTPEXDTA
 profiluri utilizator livrat de IBM
 autorizate 291

DLTPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 291

DMPJVM
 profiluri utilizator livrat de IBM
 autorizate 291

DMPMEMINF
 profiluri utilizator livrat de IBM
 autorizate 291

document
 autorizație obiect cerută pentru
 comenzi 331
 obiect bibliotecă (DLO) 219
 parolă
 modificare la restaurare a
 profilului 221
 parolă (DOCPWD parametru profil
 utilizator) 83
 profil QDOC 281
 restaurarea 219
 salvarea 219

domeniu *SYSTEM (sistem) 13
 domeniu *USER (utilizator) 13
 domeniu obiect
 afișare 13
 definiție 13
 domeniu sistem (*SYSTEM) 13
 domeniu utilizator (*USER) 13

drept de proprietate
Vedeți și drept de proprietate obiect
 asignarea noilor obiecte 124
 autorizare adoptată 130
 descriere 122
 descriere dispozitiv 179
 diagramă de flux (flowchart) 152
 fișier spool 186
 gestionare
 dimensiune profil proprietar 122
 ieșire imprimantă 186
 introducere 5
 lucrul cu 142
 modificare
 intrare jurnal auditare
 (QAUDJRN) 248
 modificare la restaurare 222
 intrare jurnal auditare
 (QAUDJRN) 244
 obiect
 autorizare privată 111
 gestionare 216
 obiect nou 124

drept de proprietate (*continuare*)
 parametru profil utilizator OWNER
 descriere 79
 parametrul ALWOBJDIF (allow object
 differences - permisiune a diferențelor
 dintre obiecte) 222
 profil de grup 122
 profil utilizator (QDFTOWN)
 implicit 124
 restaurarea 219, 222
 salvarea 219
 schimbare
 autorizare cerută 122
 metode 142
 stație de lucru 179
 ștergere
 profil deținut 101
 profil proprietar 122

drept de proprietate asupra obiectului
 diagramă de flux (flowchart) 152
 lucrul cu 142
 modificare
 mutare aplicație la producție 216
 schimbare
 metode 142

drept de proprietate obiect
 autorizare adoptată 130
 autorizare privată 111
 descriere 122
 gestionare
 dimensiune profil proprietar 122
 lucru cu 272
 modificare
 descriere comandă 272
 intrare jurnal auditare
 (QAUDJRN) 248
 modificare la restaurare 222
 parametrul ALWOBJDIF (allow object
 differences - permisiune a diferențelor
 dintre obiecte) 222
 profil de grup 122
 responsabilități 232
 restaurarea 219, 222
 salvarea 219
 schimbare
 autorizare cerută 122
 ștergere
 profil deținut 101
 profil proprietar 122

drept de proprietate, obiect
 responsabilități 232

DSPCDEFNT (Display Coded Font - Afișare
 font codificat)
 autorizație obiect cerută pentru
 comenzi 311

DSPFNNTBL (Display DBCS Font Table -
 Afișare tabelă fonturi DBCS)
 autorizație obiect cerută pentru
 comenzi 311

DSPHSTGPH
 profiluri utilizator livrat de IBM
 autorizate 291

DSPJRNA (S/38E) Gestionare atribute jurnal
 auditare obiect 477

DSPJRNMNU (S/38E) Gestionare jurnal
 auditare obiect 477

DSPLNK
 autorizări obiect necesare 352

DSPPPFRDTA
 profiluri utilizator livrat de IBM
 autorizate 291

DSPPPFRGPH
 profiluri utilizator livrat de IBM
 autorizate 291

DSPSYSSTS Comanda DSPMODSTS
 (Display System Status - Afișare stare
 sistem)
 autorizări obiect necesare 433

DST (dedicated service tools - unelte dedicate
 de service)
 auditare parole 230
 resetare parolă
 intrare jurnal auditare
 (QAUDJRN) 245

DST (unelte de service dedicate)
 modificare ID utilizator 109
 modificare parole 109
 resetare parolă
 descriere comandă 273

E

Ecran de semnare
 afișare sursă pentru 180
 modificare 180

Ecran informații de semnare
 mesaj parolă expirată 39

ecran Informații semnare
 mesaj de expirare parolă 61
 parametru profil utilizator
 DSPSGNINF 74

Ecran Ștergere profil utilizator 102

ecranul Adăugare utilizator
 eșantion 98

Ecranul Afișare autorizare obiect
 afișare în detaliu (*EXPERT opțiune
 utilizator) 88, 89, 90
 exemplu 136, 137

Ecranul Afișare listă de autorizații
 afișare în detaliu (*EXPERT opțiune
 utilizator) 88, 89, 90

ecranul Afișare utilizatori autorizați
 (DSPAUTUSR) 104

Ecranul Copiere utilizator 100

ecranul Creare profil utilizator 97

Ecranul Editare autorizare obiect
 afișare în detaliu (*EXPERT opțiune
 utilizator) 88, 89, 90

Ecranul Editare listă de autorizații
 afișare în detaliu (*EXPERT opțiune
 utilizator) 88, 89, 90

ecranul Gestionare înrolare utilizator 98

ecranul Gestionare obiecte după
 proprietar 102

ecranul Gestionare profiluri utilizator 97

ecranul Informații semnare
 exemplu 22

ecranul Înlăturare utilizator 102, 103

ecranul Modificare auditare utilizator 106

Ecranul Work with Objects by Owner -
 Gestionare obiecte după proprietar 142

editare
 autorizare obiect 138, 272

- editare (*continuare*)
 - lista de biblioteci 183
 - listă de autorizare 145
 - listă de autorizații 271
 - obiect de bibliotecă de documente (DLO)
 - autorizare 275
- educație online
 - autorizație obiect cerută pentru comenzi 400
- eliminare
 - autorizare utilizator
 - listă de autorizare 145
 - obiect 140
 - autorizarea pentru un utilizator 140
 - listă de autorizare
 - autorizare utilizator 145
 - obiect 146
- emulare
 - autorizație obiect cerută pentru comenzi 328
- ENDASPBAL
 - profiluri utilizator livrat de IBM autorizate 292
- ENDCHTSVR
 - profiluri utilizator livrat de IBM autorizate 292
- ENDCLUNOD
 - profiluri utilizator livrat de IBM autorizate 292
- ENDCMNTRC
 - profiluri utilizator livrat de IBM autorizate 292
- ENDCRG
 - profiluri utilizator livrat de IBM autorizate 292
- ENDHOSTSVR
 - profiluri utilizator livrat de IBM autorizate 292
- ENDJOBTRC
 - profiluri utilizator livrat de IBM autorizate 292
- ENDTCPIFC
 - profiluri utilizator livrat de IBM autorizate 292
- eșuare
 - semnare
 - autorizarea specială *ALLOBJ (toate obiectele) 177
 - autorizarea specială *SERVICE (service) 177
 - profilul utilizator QSECOFR (responsabil cu securitatea) 177
- eșuare autorizare
 - descriere dispozitiv 177
 - inițiere job 175
 - instrucțiune restricționată 15
 - interfață nesuportată 13, 15
 - proces de semnare 175
 - validare program 15
 - violare descriere de job 14
 - violare protecție hardware 14
 - violare semnare implicită 14
- eșuare de autorizare
 - intrare jurnal auditare (QAUDJRN) 244
- eșuare de program
 - auditare 268
- eșuare de program (*continuare*)
 - restaurare de programe
 - intrare jurnal auditare (QAUDJRN) 244
- execuție (*EXECUTE) authority 112
- exemplu
 - activare profil utilizator 104
 - autorizare adoptată
 - procesul de verificare autorizare 166, 168
 - proiectare aplicație 203, 206
 - autorizare publică
 - crearea de noi obiecte 118
 - comanda RSTLICPGM (Restore Licensed Program - Restaurare program licențiat) 225
 - comenzi restricționare salvare și restaurare 191
 - Compania de jucării JKL aplicații 195
 - controlare
 - listă de biblioteci utilizator 201
 - descriere
 - securitate bibliotecă 202
 - securitate meniu 206, 207
 - ignorare autorizare adoptată 205
 - lista de biblioteci
 - risc de securitate 183
 - listă de biblioteci
 - controlare porțiune utilizator 201
 - modicare porțiune sistem 202
 - program 201
 - modificare
 - niveluri de ajutorare 64
 - porțiune sistem a listei de biblioteci 202
 - nivel de ajutorare
 - modificare 64
 - program de validare ieșire parolă 46
 - program validare parolă 46
 - securitate bibliotecă
 - descriere 202
 - planificare 200
 - securitate meniu
 - descriere 206, 207
 - securizare cozi de ieșire 188
 - verificare autorizare
 - autorizare adoptată 166, 168
 - autorizare de grup 163
 - autorizare publică 165, 167
 - grup primar 164
 - ignorarea autorizării de grup 167
 - listă de autorizare 169
- expirare
 - parolă (valoare de sistem QPWDEXPITV) 39
 - profil utilizator
 - planificator afișare 617
 - setări planificare 617
- extragere
 - intrare listă de autorizații 271
 - profil utilizator 107, 274
- F**
 - felia de timp 192
- filtrare
 - necesități ale autorizării obiect pentru comenzi 344
- financiar
 - necesități ale autorizării obiect pentru comenzi 344
- fișier
 - descriș prin program
 - deținere autorizare la ștergere 131
 - jurnalizare
 - unealtă de securitate 209
 - necesități ale autorizării obiect pentru comenzi 337
 - planificare securitate 209
 - securizare
 - câmpuri 209
 - critic 209
 - înregistrări 209
 - sursă
 - securizare 216
- Fișier de afișare ecran de semnare 180
- fișier descriș prin program
 - deținere autorizare la ștergere 131
- fișier logic
 - securizare
 - câmpuri 209
 - înregistrări 209
- fișier mesaj
 - autorizație obiect cerută pentru comenzi 392
- fișier spool
 - afișare 186
 - auditare acțiune 496
 - autorizare specială *JOBCTL (control de job) 69
 - autorizare specială *SPLCTL (control de spool) 69
 - autorizație obiect cerută pentru comenzi 429
 - copiere 186
 - gestiune 186
 - mutare 186
 - proprietar 186
 - securizare 186
 - ștergere profil utilizator 103
- fișier spool de rețea
 - trimitere 186
- fișiere class
 - fișiere jar 216
- fișiere jar
 - fișiere class 216
- fișiere sursă
 - securizare 216
- fișierul spool
 - modificare
 - intrare jurnal auditare (QAUDJRN) 250
- folder
 - securitate partajată 190
- folder partajat
 - securizare 190
- format diagramă
 - autorizație obiect cerută pentru comenzi 315
- format înregistrare QJORDJE2 507

forțare conversie la restaurare (QFRCCVNRST)
 valoare de sistem 36

funcția de auditare a securității
 activare 256
 CHGSECAUD 256
 oprire 260

Funcția PCTA (PC text-assist - Asistent text PC)
 deconectare (valoarea de sistem QINACTMSGQ) 24

funcție avansată de tipărire (AFP)
 autorizație obiect cerută pentru comenzi 311

funcție cerere sistem
 autorizare adoptată 129

funcție de adoptare a programului
Vedeți autorizare adoptată

funcție de auditare
 activare 256
 oprire 260
 pornire 256

funcție dump
 autorizare specială *SERVICE (service) 70

funcție mesaj (iSeries Access)
 securizare 190

funcție permisă
 limitare capabilități (LMTCPB) 67

funcții de depanare
 autorizare adoptată 129

G

gestionare
 auditare utilizator 106
 jurnal audit 258
 profiluri utilizator 97

gestiune
 descriere coadă de ieșire 186
 fișiere spool 186
 stare sistem 192

gestiune sisteme
 modificare
 intrare jurnal auditare (QAUDJRN) 250

gid (group identification number - număr de identificare utilizator)
 restaurarea 222

grup
 autorizare
 afișare 134
 primar
Vedeți și grup primar
 introducere 5

grup de panouri
 autorizație obiect cerută pentru comenzi 390

grup multiplu
 exemplu 170
 planificare 214

grup primar
 definiție 111
 descriere 123
 gestionare 103
 introducere 5
 lucru cu obiecte 272

grup primar (*continuare*)
 lucru cu 143
 modificare
 descriere comandă 272
 intrare jurnal auditare (QAUDJRN) 248
 modificare în timpul restaurării
 intrare jurnal auditare (QAUDJRN) 245
 modificare la restaurare 222

obiect nou 124
 planificare 213
 restaurarea 219, 222
 salvarea 219
 schimbare 123
 ștergere
 profil 101

grup suplimentar
 planificare 214

grupuri suplimentare
 parametru profil utilizator SUPGRPPRF 81

H

hardware
 autorizație obiect cerută pentru comenzi 419
 protecție îmbunătățită a spațiului de stocare 14

I

ID digital
 dacă nu este găsită autorizare privată. 96

ID utilizator
 DST (unelte de service dedicate)
 modificare 109
 incorect
 intrare jurnal auditare (QAUDJRN) 240

ID-uri utilizator cifre 59

identificator de limbă
 parametru profil utilizator LANGID 87
 parametru profil utilizator SRTSEQ 87
 valoare de sistem QLANGID 87

identificator de regiune sau țară
 parametru profil utilizator CNTRYID 88
 valoare de sistem QCNTYID 88

identificator set de caractere codate
 parametru profil utilizator CCSID 88
 valoare de sistem QCCSID 88

ieșire 46
 necesități ale autorizării obiect pentru comenzi 429

ieșire imprimantă
 autorizare specială *JOBCTL (control de job) 69
 autorizare specială *SPLCTL (control de spool) 69
 autorizație obiect cerută pentru comenzi 429
 proprietar 186
 securizare 186

ignorare
 autorizare adoptată 131

imagine
 necesități ale autorizării obiect pentru comenzi 346

implicit 281
 mod de livrare *DFT
Vedeți și coadă de mesaje
 profil utilizator 84
 profil utilizator cu proprietar (QDFTOWN)
 valori implicite 281
 profil utilizator proprietar (QDFTOWN)
 descriere 124
 intrare jurnal auditare (QAUDJRN) 244
 restaurare de programe 225

semnare
 nivel de securitate 40 14

valoare
 profil utilizator 279
 profil utilizator furnizat de IBM 279

implicită
 descriere de job (QDFTJOB) 78
 obiect
 auditare 254

imprimantă
 profil utilizator 85
 virtuală
 securizare 190

imprimantă virtuală
 securizare 190

inactiv
 job
 valoare de sistem coadă de mesaje (QINACTMSGQ) 24
 valoarea de sistem interval timeout (QINACTITV) 23

utilizator
 listare 268

incorect ID utilizator
 intrare jurnal auditare (QAUDJRN) 240

index căutare informații
 autorizarea obiect necesară 366

index de căutare
 autorizări obiect necesare 366

index test
 autorizație obiect cerută pentru comenzi 400

informații de ajutor
 afișare ecran întreg (*HLPFULL opțiune utilizator) 90

informații de ajutor online
 afișare ecran întreg (*HLPFULL opțiune utilizator) 90

informații de securitate
 format pe mediu de stocare 220
 format pe sistem 220
 stocat pe sistem 220
 stocate pe mediu de stocare 220

informații de semnare
 afișare
 valoarea de sistem QDPSGNINF 22

informații parte comunicații
 autorizație obiect cerută pentru comenzi 320

informații semnare
 afișare
 parametru profil utilizator DSPSGNINF 73

- informațiilor de securitate
 - recuperarea 219
 - restaurarea 219
 - salvare de rezervă 219
 - salvarea 219
- inițiere job
 - autorizare adoptată 176
 - Programul tratare-tastă-atenție 176
- instalare
 - auditare de securitate 277
- instalarea
 - sistem de operare 227
- instrucțiune restricționată
 - intrare jurnal auditare (QAUDJRN) 244
- integritate 1
 - verificare
 - auditare folosire 233
 - descriere 269, 274
- integritate obiect
 - auditare 269
- interfață de nivel de apelare
 - nivel de securitate 40 13
- interfață de programare aplicație (API)
 - nivel de securitate 40 13
- interfață nesuportată
 - intrare jurnal auditare (QAUDJRN) 13, 244
- interogare
 - analizare intrări jurnal audit 262
- interval de expirare parolă (PWDEXPITV)
 - recomandări 74
- interval timeout
 - valoare de sistem coadă de mesaje (QINACTMSGQ) 24
 - valoarea de sistem joburi inactice (QINACTITV) 23
- intrare de autentificare server
 - adăugare 276
 - înlăturare 276
 - modificare 276
- intrare de comunicații
 - descriere de job 181
- intrare de rutare
 - autorizare program 176
 - performanța 192
- intrare director
 - adăugare 276
 - înlăturare 276
 - modificare 276
 - ștergere profil utilizator 101
- intrare job la distanță (RJE)
 - autorizație obiect cerută pentru comenzi 419
- intrare jurnal
 - trimitere 258
- intrare rutare
 - modificare
 - intrare jurnal auditare (QAUDJRN) 249
- intrare stație de lucru
 - descriere de job 181
 - semnare fără ID utilizator și fără parolă 14
- Intrări
 - intrări jurnal
 - auditare 239
 - securitate 239

- Intrări jurnal
 - auditare de securitate 239
- Intrări jurnal auditare securitate 239
- IPL (Initial Program Load)
 - autorizare specială *JOBCTL (control de job) 69
- iSeries Access
 - controlare semnare 27
 - securitate folder partajat 190
 - securitate funcție mesaj 190
 - securitate imprimantă virtuală 190
 - securitate transfer fișier 190
- istoric QHST (history-istoric sistem)
 - folosire pentru monitorizare a securității 265

Î

- împiedicare
 - abuzuri performanță 192
- acces
 - cerere DDM (DDM) 190
 - iSeries Access 189
 - modificare a blocurilor de control interne 17
 - parole triviale 38
 - prezentare job la distanță 189
- împiedicare profiluri mari
 - planificare aplicații 200
- în numele
 - auditare 479
- înaintare
 - descriptor
 - intrare jurnal auditare (QAUDJRN) 248
 - socket
 - intrare jurnal auditare (QAUDJRN) 248
- înlăturare
 - angajați care nu mai au nevoie de acces 232
 - autorizare obiect de bibliotecă de documente 275
 - intrare de autentificare server 276
 - intrare director 276
 - intrare lista de biblioteci 183
 - listă de autorizații
 - autorizare utilizator 271
 - nivel de securitate 40 16
 - nivel de securitate 50 18
 - profil utilizator
 - automat 617
 - coadă de mesaje 101
 - grup primar 101
 - intrare director 101
 - liste de distribuție 101
 - obiecte deținute 101
- înregistrare în istoricul sistem (QHST)
 - folosire pentru monitorizare a securității 265
- înregistrare în istoric
 - rețea
 - intrare jurnal auditare (QAUDJRN) 242
- înrolare
 - utilizatori 98

- întoarcere
 - pagină în jos (*ROLLKEY opțiune utilizator) 90
 - Pagină în sus (*ROLLKEY opțiune utilizator) 90
- întrebare și răspuns
 - autorizație obiect cerută pentru comenzi 417

J

- Java
 - necesități ale autorizării obiect pentru comenzi 367
- job
 - anularea automată 33, 34
 - autorizare specială *JOBCTL (control de job) 69
 - inactiv
 - valoarea de sistem interval timeout (QINACTITV) 23
 - modificare
 - intrare jurnal auditare (QAUDJRN) 241
 - necesități ale autorizării obiect pentru comenzi 367
 - planificare 192
 - restricționare la batch 193
 - schimbare
 - autorizare adoptată 130
 - securitate când pornește 175
 - valoare de sistem interval job deconectat (QDSCJOBITV) 33
 - valoare de sistem verificare obiect la restaurare (QVFYOBJRST) 34
 - job batch
 - autorizare specială *SPLCTL (control de spool) 69
 - prioritate 77
 - securitate când pornește 175, 176
 - job grup
 - autorizare adoptată 129
 - job inactiv
 - mesaj (CPII126) 24
 - job interactiv
 - rutare
 - parametru SPENV (mediu special) 72
 - securitate când pornește 175
 - jurnal
 - afișare
 - auditare activitate fișier 209, 266
 - auditare (QAUDJRN)
 - introducere 233
 - folosire pentru monitorizare a securității 265
 - gestionare 258
 - lucru cu 267
 - necesități ale autorizării obiect pentru comenzi 372
 - jurnal audit
 - lucru cu 260
 - jurnal auditare
 - tipărire intrări 621
 - jurnal auditare (QAUDJRN)
 - Vedeți și auditare obiect
 - disponere fișier O1 (acces optic) 567, 568

jurnal auditare (QAUDJRN) *(continuare)*
 dispunere fișier O3 (acces optic) 569
 dispunere fișier PG (modificare grup primar) 572
 dispunere fișier PO (ieșire imprimantă) 574
 dispunere fișier PS (interschimbare profil) 575
 dispunere fișier PW (parolă) 576
 dispunere fișier RA (modificare de autorizare pentru obiectul restaurat) 578
 dispunere fișier RJ (restaurare descriere job) 579
 dispunere fișier RO (modificare drept de proprietate pentru obiectul restaurat) 580
 dispunere fișier RP (restaurare programe care adoptă autorizare) 581
 dispunere fișier RQ (restaurare obiect *CRQD care adoptă autorizare) 582
 dispunere fișier RU (restaurare autorizare pentru profil utilizator) 583
 dispunere fișier RZ (modificare grup primar pentru obiectul restaurat) 583
 dispunere fișier SD (modificare director de distribuție sistem) 585
 dispunere fișier SE (modificare intrare rutare subsistem) 586
 dispunere fișier SF (acțiune către fișierul spool) 586
 dispunere fișier SG 590, 591
 dispunere fișier SM (modificare gestiune sisteme) 592
 dispunere fișier SO (acțiuni informații utilizator de securitate server) 593
 dispunere fișier ST (acțiune unelte service) 593
 dispunere fișier SV (acțiune pentru valoarea sistem) 597
 dispunere fișier VA (modificarea listei de control acces) 597
 dispunere fișier VC (terminare și oprire conexiune) 598
 dispunere fișier VF (închiderea fișierelor server) 598
 dispunere fișier VL (limită cont depășită) 599
 dispunere fișier VN (logare și delogare rețea) 599
 dispunere fișier VO (listă de validare) 600
 dispunere fișier VP (eroare parolă rețea) 601
 dispunere fișier VR (acces resursă rețea) 602
 dispunere fișier VS (sesiune server) 603
 dispunere fișier VU (modificare profil rețea) 603
 dispunere fișier VV (modificare stare service) 604
 dispunere fișier X0 (autentificare kerberos) 605
 dispunere fișier YC (modificarea obiectului DLO) 610
 dispunere fișier YR (citirea obiectului DLO) 611

jurnal auditare (QAUDJRN) *(continuare)*
 dispunere fișier ZC (modificare obiect) 611
 dispunere fișier ZR (citire obiect) 614
 tip de intrare AD (auditare modificare) 247
 tip de intrare AF (eșuare autorizare) 244
 descriere 240
 tip de intrare AP (autorizare adoptată) 244
 tip de intrare CA (modificare autorizare) 247
 tip de intrare CO (creare obiect) 241
 tip de intrare CP (modificare profil utilizator) 245
 tip de intrare CQ (modificare obiect *CRQD) 245
 tip de intrare DS (resetare parolă DST) 245
 tip de intrare GS (înainte descriptor) 248
 tip de intrare IP (comunicații interproces) 240
 tip de intrare IP (modificare drept de proprietate) 248
 tip de intrare JD (modificare descriere de job) 248
 tip de intrare JS (modificare job) 241
 tip de intrare NA (modificare atribut de rețea) 248
 tip de intrare OM (gestionare obiect) 243
 tip de intrare OR (restaurare obiect) 244
 tip de intrare OW (modificare drept de proprietate) 248
 tip de intrare PA (adoptare program) 248
 tip de intrare PG (modificare grup primar) 248
 tip de intrare PO (ieșire tipărită) 244
 tip de intrare PS (profil swap) 248
 tip de intrare PW (parolă) 240
 tip de intrare RA (modificare autorizare pentru obiect restaurat) 244
 tip de intrare RJ (restaurare descriere de job) 244
 tip de intrare RO (modificare drept de proprietate pentru obiect restaurat) 244
 tip de intrare RP (restaurare de programe care adoptă autorizarea) 244
 tip de intrare RQ (restaurare obiect *CRQD) 244
 tip de intrare RU (restaurare autorizare pentru profil utilizator) 245
 tip de intrare RZ (modificare grup primar pentru obiect restaurat) 245
 tip de intrare SD (modificare director de distribuție a sistemului) 243
 tip de intrare SE (modificare a intrării de rutare subsistem) 249
 tip de intrare SF (modificare la fișierul spool) 250
 tip de intrare SM (modificare gestiune sisteme) 250
 tip de intrare ST (acțiune unelte service) 250
 tip de intrare SV (acțiune pentru variabila de sistem) 249

jurnal auditare (QAUDJRN) *(continuare)*
 tip de intrare VA (modificare a listei de acces control) 249
 tip de intrare VL (cont limită depășit) 251
 tip de intrare VN (logare sau delogare la rețea) 242
 tip de intrare VP (eroare parolă rețea) 241
 tip de intrare VU (modificare profil de rețea) 249
 tip de intrare VV (modificare stare serviciu) 250
 tip intrare CD (șir comandă) 241
 tip intrare CO (creare obiect) 123
 tip intrare DO (ștergere operație) 241
 tip intrare ML (acțiuni poștă) 243
 tip intrare VC (pornire sau oprire conexiune) 242
 tip intrare VS (sesiune server) 242
 Jurnal auditare (QAUDJRN) 570
 jurnal auditare deteriorat 258
 jurnal auditare QAUDJRN
Vedeți și variabila de sistem QAUDLVL (audit level - nivel audit)
 afișare intrări 234, 260
 analizare
 cu interogare 262
 creare 257
 curățare automată 258
 detașare receptor 258, 260
 deteriorat 258
 gestionare 258
 intrări de sistem 258
 introducere 233
 metode de analizare 260
 modificare receiver 260
 oprire 260
 prag de stocare receptor 258
 jurnal auditare securitate
 tipărire intrări 621
 jurnal de auditare
 afișare intrări 277
 jurnal de auditare (QAUDJRN)
 afișare intrări 234, 260
 analizare
 cu interogare 262
 condiții de eroare 50
 creare 257
 curățare automată 258
 detașare receptor 258, 260
 deteriorat 258
 dispunere fișier AD (auditare modificare) 512
 dispunere fișier AF (eșuare autorizare) 514
 dispunere fișier AP (autorizare adoptată) 519
 dispunere fișier AU (modificare atribut) 519
 dispunere fișier CA (modificare autorizare) 520
 dispunere fișier CD (șir comenzi) 522
 dispunere fișier CO (creare obiect) 523
 dispunere fișier CP (modificare profil utilizator) 525
 dispunere fișier CQ (modificare *CRQD) 527
 dispunere fișier CU (Operații cluster) 527

- jurnal de auditare (QAUDJRN) (*continuare*)
- dispunere fișier CV (verificare conexiune) 528
 - dispunere fișier CY (configurație criptografică) 530
 - dispunere fișier DI (Directory Server) 532
 - dispunere fișier DO (operație ștergere) 536
 - dispunere fișier DS (Resetare ID utilizator unelte service furnizate de IBM) 538
 - dispunere fișier EV (variabilă mediu) 539
 - dispunere fișier GR (înregistrare generică) 539
 - dispunere fișier GS (acordare descriptor) 544
 - dispunere fișier IP (acțiuni comunicații între procese) 545
 - dispunere fișier IR (acțiuni reguli IP) 547
 - dispunere fișier IS (gestiune securitate internet) 548
 - dispunere fișier JD (modificare descriere job) 550
 - dispunere fișier JS (modificare job) 550
 - dispunere fișier KF (fișier inel de chei) 554
 - dispunere fișier LD (director de căutare, legare, dezlegare) 557
 - dispunere fișier ML (acțiuni mail) 558
 - dispunere fișier NA (modificare atribut rețea) 559
 - dispunere fișier ND (director APPN) 559
 - dispunere fișier NE (punct final APPN) 560
 - dispunere fișier OM (gestiune obiect) 560
 - dispunere fișier OR (restaurare obiect) 563
 - dispunere fișier OW (modificare drept de proprietate) 566
 - gestionare 258
 - intrări de sistem 258
 - introducere 233
 - metode de analizare 260
 - modificare receiver 260
 - nivel forțare 51
 - oprire 260
 - prag de stocare receptor 258
 - Tip intrare AF (authority failure - eșuare autorizare)
 - interfață nesuportată 13
 - validare program 15
 - violare de instrucțiuni restricționată 15
 - violare de interfață nesuportată 15
 - violare descriere de job 14
 - violare protecție hardware 14
 - violare semnare implicită 14
 - valoare de sistem extensie nivel auditare (QAUDLVL2) 53
 - valoare de sistem nivel auditare (QAUDLVL) 51
- jurnal de auditare de securitate
- afișare intrări 277
- jurnal QAUDJRN (auditare) 248, 251
- Vedeți și* auditare obiect condiții de eroare 50
- dispunere fișier AD (auditare modificare) 512
- jurnal QAUDJRN (auditare) (*continuare*)
- dispunere fișier AF (eșuare autorizare) 514
 - dispunere fișier AP (autorizare adoptată) 519
 - dispunere fișier AU (modificare atribut) 519
 - dispunere fișier CA (modificare autorizare) 520
 - dispunere fișier CD (șir comenzi) 522
 - dispunere fișier CO (creare obiect) 523
 - dispunere fișier CP (modificare profil utilizator) 525
 - dispunere fișier CQ (modificare *CRQD) 527
 - dispunere fișier CU (Operații cluster) 527
 - dispunere fișier CV (verificare conexiune) 528
 - dispunere fișier CY (configurație criptografică) 530
 - dispunere fișier DI (Directory Server) 532
 - dispunere fișier DO (operație ștergere) 536
 - dispunere fișier DS (Resetare ID utilizator unelte service furnizate de IBM) 538
 - dispunere fișier EV (variabilă mediu) 539
 - dispunere fișier GR (înregistrare generică) 539
 - dispunere fișier GS (acordare descriptor) 544
 - dispunere fișier IP (acțiuni comunicații între procese) 545
 - dispunere fișier IR (acțiuni reguli IP) 547
 - dispunere fișier IS (gestiune securitate internet) 548
 - dispunere fișier JD (modificare descriere job) 550
 - dispunere fișier JS (modificare job) 550
 - dispunere fișier KF (fișier inel de chei) 554
 - dispunere fișier LD (director de căutare, legare, dezlegare) 557
 - dispunere fișier ML (acțiuni mail) 558
 - dispunere fișier NA (modificare atribut rețea) 559
 - dispunere fișier ND (director APPN) 559
 - dispunere fișier NE (punct final APPN) 560
 - dispunere fișier O1 (acces optic) 567, 568
 - dispunere fișier O3 (acces optic) 569
 - dispunere fișier OM (gestiune obiect) 560
 - dispunere fișier OR (restaurare obiect) 563
 - dispunere fișier OW (modificare drept de proprietate) 566
 - dispunere fișier PG (modificare grup primar) 572
 - dispunere fișier PO (ieșire imprimantă) 574
 - dispunere fișier PS (interschimbare profil) 575
 - dispunere fișier PW (parolă) 576
 - dispunere fișier RA (modificare de autorizare pentru obiectul restaurat) 578
 - dispunere fișier RJ (restaurare descriere job) 579
- jurnal QAUDJRN (auditare) (*continuare*)
- dispunere fișier RO (modificare drept de proprietate pentru obiectul restaurat) 580
 - dispunere fișier RP (restaurare programe care adoptă autorizare) 581
 - dispunere fișier RQ (restaurare obiect *CRQD care adoptă autorizare) 582
 - dispunere fișier RU (restaurare autorizare pentru profil utilizator) 583
 - dispunere fișier RZ (modificare grup primar pentru obiectul restaurat) 583
 - dispunere fișier SD (modificare director de distribuție sistem) 585
 - dispunere fișier SE (modificare intrare rutare subsistem) 586
 - dispunere fișier SF (acțiune către fișierul spool) 586
 - dispunere fișier SG 590, 591
 - dispunere fișier SM (modificare gestiune sisteme) 592
 - dispunere fișier SO (acțiuni informații utilizator de securitate server) 593
 - dispunere fișier ST (acțiune unelte service) 593
 - dispunere fișier SV (acțiune pentru valoarea sistem) 597
 - dispunere fișier VA (modificarea listei de control acces) 597
 - dispunere fișier VC (terminare și oprire conexiune) 598
 - dispunere fișier VF (închiderea fișierelor server) 598
 - dispunere fișier VL (limită cont depășită) 599
 - dispunere fișier VN (logare și delogare rețea) 599
 - dispunere fișier VO (listă de validare) 600
 - dispunere fișier VP (eroare parolă rețea) 601
 - dispunere fișier VR (acces resursă rețea) 602
 - dispunere fișier VS (sesiune server) 603
 - dispunere fișier VU (modificare profil rețea) 603
 - dispunere fișier VV (modificare stare service) 604
 - dispunere fișier X0 (autentificare kerberos) 605
 - dispunere fișier YC (modificarea obiectului DLO) 610
 - dispunere fișier YR (citirea obiectului DLO) 611
 - dispunere fișier ZC (modificare obiect) 611
 - dispunere fișier ZR (citire obiect) 614
 - nivel forțare 51
 - PA (adoptare program) 570
 - tip de intrare AD (auditare modificare) 247
 - tip de intrare AF (eșuare autorizare) 244
 - descriere 240
 - tip de intrare AP (autorizare adoptată) 244
 - tip de intrare CA (modificare autorizare) 247

jurnal QAUDJRN (auditare) *(continuare)*
 tip de intrare CO (creare obiect) 241
 tip de intrare CP (modificare profil utilizator) 245
 tip de intrare CQ (modificare obiect *CRQD) 245
 tip de intrare DS (resetare parolă DST) 245
 tip de intrare IP (comunicații interproces) 240
 tip de intrare JD (modificare descriere de job) 248
 tip de intrare JS (modificare job) 241
 tip de intrare NA (modificare atribut de rețea) 248
 tip de intrare OM (gestionare obiect) 243
 tip de intrare OR (restaurare obiect) 244
 tip de intrare OW (modificare drept de proprietate) 248
 tip de intrare PA (adoptare program) 248
 tip de intrare PG (modificare grup primar) 248
 tip de intrare PO (ieșire imprimantă) 244
 tip de intrare PS (profil swap) 248
 tip de intrare PW (parolă) 240
 tip de intrare RA (modificare autorizare pentru obiect restaurat) 244
 tip de intrare RJ (restaurare descriere de job) 244
 tip de intrare RO (modificare drept de proprietate pentru obiect restaurat) 244
 tip de intrare RP (restaurare de programe care adoptată autorizarea) 244
 tip de intrare RQ (restaurare obiect *CRQD) 244
 tip de intrare RU (restaurare autorizare pentru profil utilizator) 245
 tip de intrare RZ (modificare grup primar pentru obiect restaurat) 245
 tip de intrare SD (modificare director de distribuire a sistemului) 243
 tip de intrare SE (modificare a intrării de rutare subsistem) 249
 tip de intrare SF (modificare la fișierul spool) 250
 tip de intrare SM (modificare gestiune sisteme) 250
 tip de intrare ST (acțiune unelte service) 250
 tip de intrare SV (acțiune pentru variabila de sistem) 249
 tip de intrare VA (modificare a listei de acces control) 249
 tip de intrare VN (logare sau delogare la rețea) 242
 tip de intrare VP (eroare parolă rețea) 241
 tip de intrare VU (modificare profil de rețea) 249
 tip de intrare VV (modificare stare serviciu) 250
 Tip intrare AF (authority failure - eșuare autorizare)
 instrucțiune restricționată 15
 interfață nesuportată 13, 15
 validare program 15
 violare descriere de job 14
 violare protecție hardware 14

jurnal QAUDJRN (auditare) *(continuare)*
 Tip intrare AF (authority failure - eșuare autorizare) *(continuare)*
 violare semnare implicită 14
 tip intrare CD (șir comandă) 241
 tip intrare CO (creare obiect) 123
 tip intrare DO (ștergere operație) 241
 tip intrare ML (acțiuni poștă) 243
 tip intrare VC (pornire sau oprire conexiune) 242
 tip intrare VS (sesiune server) 242
 valoare de sistem extensie nivel auditare (QAUDLVL2) 53
 valoare de sistem nivel auditare (QAUDLVL) 51
 jurnal, audit
Vedeți și jurnal auditare (QAUDJRN)
 lucru cu 260
 jurnalizare
 unealtă de securitate 209

L

lansare
 rapoarte de securitate 620

legătură
 necesități ale autorizării obiect pentru comenzi 316, 347

limbaj de programare
 autorizație obiect cerută pentru comenzi 376

limbaj, programare
 autorizație obiect cerută pentru comenzi 376

limitare
 capabilități 66
 comenzi permise 67
 funcții permise 67
 listare utilizatori 267
 modificare bibliotecă curentă 65, 185
 modificare meniu inițial 66
 modificare program de tratare tastă Attn 86
 modificare program inițial 65
 parametru profil utilizator LMTCPB 66
 folosire disc (MAXSTG) 76
 folosire linie de comandă 66
 folosire resurse de sistem
 parametru limită de prioritate (PTYLMT) 77
 încercări de logare
 auditare 230, 233
 responsabil cu securitatea (QLMTSECOFR)
 modificare nivelului de securitate 11
 responsabil cu securitatea (QLMTSECOFR) valoare de sistem autorizare pentru descrierile de dispozitiv 177
 proces de semnare 179
 semnare
 dispozitive multiple 25
 valoare de sistem QMAXSGNACN încercări 26
 valoare de sistem QMAXSIGN încercări 25

limitare *(continuare)*
 sesiuni dispozitiv
 auditare 231
 parametru profil utilizator LMTDEVSSN 75
 recomandări 75
 valoarea de sistem QLMTDEVSSN (device sessions - sesiuni dispozitiv) descriere 25
 valoarea de sistem responsabil cu securitatea (QLMTSECOFR) descriere 25
 variabilă de sistem responsabil cu securitatea (QLMTSECOFR) auditare 230
 limitare capabilități *PARTIAL (parțială) 67
 limitare capabilități parțială (*PARTIAL) 67
 limită cont
 depășită
 intrare jurnal auditare (QAUDJRN) 251
 lista de autorizare QRCLAUTL (reclaim storage) 227
 lista de autorizare reclaim storage (QRCLAUTL) 227
 lista de biblioteci
 adăugare intrări 183, 186
 bibliotecă curentă
 descriere 183
 recomandări 185
 bibliotecă produs
 descriere 183
 recomandări 185
 definiție 183
 editare 183
 înlăturare intrări 183
 modificare 183
 porțiuni sistem
 descriere 183
 recomandări 184
 porțiuni utilizator
 recomandări 185
 recomandări 184
 riscuri de securitate 183
 lista de biblioteci inițială
Vedeți și lista de biblioteci
 recomandări 185
 relația cu lista de biblioteci pentru job 183
 riscuri 185
 lista de biblioteci sistem
 modificare 183
 QSYSLIBL valoare de sistem 183
 lista de răspuns
 auditare acțiune 492
 autorizație obiect cerută pentru comenzi 433
 listare
 conținut bibliotecă 268
 profil utilizator
 individual 104
 listă rezumat 104
 profiluri utilizator selectate 267
 toate bibliotecile 268
 valori de sistem 230

- listă acces control
 - modificare
 - intrare jurnal auditare (QAUDJRN) 249
- listă biblioteci
 - autorizare adoptată 115
- listă de autorizare
 - adăugare
 - intrări 145
 - obiecte 146
 - utilizatori 145
 - afișare
 - obiecte 146
 - autorizare
 - schimbare 145
 - stocare 221
 - autorizație obiect cerută pentru comenzi 314
 - creare 144
 - deteriorat 226
 - editare 145
 - eliminare
 - obiecte 146
 - utilizatori 145
 - gestionare autorizare(*AUTLMGT) 300
 - intrare
 - adăugare 145
 - introducere 4
 - QRCLAUTL (reclaim storage) 227
 - reclaim storage (QRCLAUTL) 227
 - recuperare deteriorat 226
 - restaurarea
 - asociere cu obiectul 223
 - descrierea procesului 226
 - privire generală asupra comenzilor 219
 - salvarea 219
 - securizarea obiectelor 146
 - stocare
 - autorizare 220, 221
 - ștergere 146
 - utilizator
 - adăugare 145
 - verificare autorizare exemplu 169
- listă de autorizare deteriorată
 - recuperarea 226
- listă de autorizații
 - adăugare
 - intrări 271
 - afișare
 - obiecte 271
 - obiecte de bibliotecă de documente (DLO) 275
 - utilizatori 271
 - auditare obiect 451
 - avantaje 212
 - comparație
 - profil de grup 215
 - creare 271
 - editare 271
 - extragere intrări 271
 - informații autorizație de tipărire 621
 - înlăturare
 - intrări 271
 - utilizatori 271
 - lucru cu 271

- listă de autorizații (*continuare*)
 - modificare
 - intrare 271
 - obiect de bibliotecă de documente (DLO)
 - afișare 275
 - profil de grup
 - comparație 215
 - ștergere 271
 - listă de biblioteci
 - bibliotecă curentă
 - profil utilizator 64
 - descriere de job (JOBBD)
 - profil utilizator 78
 - monitorizare 232
 - porțiune sistem
 - modificare 202
 - porțiune utilizator
 - controlare 201
 - listă de biblioteci inițială
 - bibliotecă curentă 64
 - descriere de job (JOBBD)
 - profil utilizator 78
 - listă de biblioteci sistem
 - modificare 202
 - listă de conexiuni
 - autorizație obiect cerută pentru comenzi 322
 - listă de configurare
 - autorizație obiect cerută pentru comenzi 322
 - listă de distribuție
 - autorizație obiect cerută pentru comenzi 331
 - ștergere profil utilizator 101
 - listă de noduri
 - autorizație obiect cerută pentru comenzi 399
 - listă de profiluri activă
 - modificare 617
 - listă de validare
 - autorizație obiect cerută pentru comenzi 443
 - listă de verificare
 - auditare securitate 229
 - planificare securitate 229
 - listă replici sistem
 - autorizație obiect cerută pentru comenzi 433
 - liste de autorizații
 - avantaje 212
 - planificare 212
 - liste de validare
 - utilizator internet 216
 - Liste de validare, creare 216
 - Liste de validare, ștergere 216
 - Liste, creare validare 216
 - Liste, ștergere validare 216
 - listing
 - deținători de autorizare 131
 - locale
 - necesități ale autorizării obiect pentru comenzi 389
- LODIMGCLG
 - profiluri utilizator livrat de IBM autorizate 292

- LODOPTFMW
 - profiluri utilizator livrat de IBM autorizate 293
- logare
 - incorect ID utilizator
 - intrare jurnal auditare (QAUDJRN) 240
 - parolă incorectă
 - intrare jurnal auditare (QAUDJRN) 240
 - preîntâmpinare implicită 232
- lucru cu
 - atribute jurnal 260, 267
 - autorizare 272
 - autorizare obiect 272
 - deținători de autorizare 271, 276
 - director 276
 - director sistem 276
 - jurnal 267
 - liste de autorizații 271
 - obiecte 272
 - obiecte de bibliotecă de documente (DLO) 275
 - obiecte după grup primar 272
 - obiecte după proprietar 272
 - parolă 273
 - profiluri utilizator 274, 275
- lucru în numele
 - auditare 479
- lucrul cu
 - drept de proprietate asupra obiectului 142
 - grup primar 143
 - obiecte de grup primar 123
 - lungimea parolei 41

M

- maxim
 - lungime a parolei (valoare de sistem QPWDMAXLEN). 41
 - parametru spațiu de stocare (MAXSTG)
 - operație de restaurare 76
 - profil utilizator 76
 - receptor jurnal 76
 - parametrul spațiu de stocare (MAXSTG)
 - deținător de autorizare 124
 - drept de proprietate grup al obiectelor 122
 - valoarea de sistem QMAXSIGN (maximum sign-on attempts - număr maxim de încercări de semnare)
 - descriere 25
- maximum
 - auditare 230
 - dimensiune
 - receptor jurnal auditare (QAUDJRN) 258
 - variabilă de sistem (QMAXSIGN)
 - încercări de logare 230
- mărimea parolei 41
- mediu copie de rezervă
 - protejare 230
- mediu de stocare
 - necesități ale autorizării obiect pentru comenzi 389
- mediu special *S36 (System/36) 72

- mediu System/36
 - profil utilizator 72
- Mediu System/36
 - autorizație obiect cerută pentru comenzi 434
- mediu System/38 72
- Mediu System/38 117
- memorie
 - control partajare
 - valoare de sistem QSHRMEMCTL (control memorie de partajare) 29
- meniu
 - Vedeți și* meniu inițial
 - creare
 - parametrul PRDLIB (biblioteca produs) 185
 - riscuri de securitate 185
 - inițial 66
 - modificare
 - parametrul PRDLIB (biblioteca produs) 185
 - riscuri de securitate 185
 - necesități ale autorizării obiect pentru comenzi 390
 - profil utilizator 66
 - proiectare pentru securitate 203
- meniu inițial
 - *SIGNOFF 66
 - ecran de prevenire 66
 - modificare 66
 - profil utilizator 66
 - recomandare 67
- meniu inițial *SIGNOFF 66
- Meniu SECBATCH (Lansare rapoarte batch)
 - lansare rapoarte 620
 - planificare rapoarte 620
- Meniul Cerere sistem
 - opțiuni și comenzi 207
 - using 207
- meniul Cerințe de sistem
 - limitare sesiuni dispozitiv (LMTDEVSSN) 75
- Meniul SECTOOLS (Unelte de securitate) 617
- Meniul Unelte de securitate (SECTOOLS) 617
- meniuri
 - unelte de securitate 617
- mesaj
 - cronometru inactiv (CPI1126) 24
 - necesități ale autorizării obiect pentru comenzi 391
 - notificare tipărire (*PRTMSG opțiune utilizator) 90
 - restricționare conținut 17
 - securitate
 - monitorizare 265
 - stare
 - afișare (*STSMMSG opțiune utilizator) 90
 - neafișare (*NOSTSMMSG opțiune utilizator) 90
 - terminare tipărire (*PRTMSG opțiune utilizator) 90
- mesaj de stare
 - afișare (*STSMMSG opțiune utilizator) 90
- mesaj de stare (*continuare*)
 - neafișare (*NOSTSMMSG opțiune utilizator) 90
- metode de autorizare
 - combinare
 - exemplu 171
- MGRS36APF
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36CBL
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36DFU
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36DSPF
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36LIB
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36MNU
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36MSGF
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36QRY
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36RPG
 - profiluri utilizator livrat de IBM autorizate 293
- MGRS36SEC
 - profiluri utilizator livrat de IBM autorizate 293
- migrare
 - autorizație obiect cerută pentru comenzi 393
 - valoarea de sistem QSECURITY (nivel de securitate)
 - nivelul 10 în nivelul 20 10
 - nivelul 20 în nivelul 30 11
 - nivelul 30 în nivelul 20 10
 - nivelul 40 în nivelul 20 10
 - valoarea de sistem QSECURITY (security level - nivel de securitate)
 - nivelul 20 în nivelul 40 15
 - nivelul 20 în nivelul 50 17
 - nivelul 30 în nivelul 40 15
 - nivelul 30 în nivelul 50 17
- MIGRATE
 - profiluri utilizator livrat de IBM autorizate 293
- mod de acces
 - Vedeți și* autorizare
 - definiție 112
- mod de livrare *BREAK (întrerupere)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare *DFT (implicit)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare *HOLD (reținere)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare *NOTIFY (notificare)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare întrerupere (*BREAK)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare notificare (*NOTIFY)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- mod de livrare reținere (*HOLD)
 - Vedeți și* coadă de mesaje
 - profil utilizator 84
- modernizare informații ordine
 - autorizație obiect cerută pentru comenzi 438
- modificare
 - adoptare program
 - intrare jurnal auditare (QAUDJRN) 248
 - atribut de rețea
 - intrare jurnal auditare (QAUDJRN) 248
 - atribut rețea
 - legat-de-securitate 189
 - auditare
 - descriere comandă 272, 275
 - auditare de securitate 277
 - auditare obiect 71, 272, 275
 - descriere comandă 275
 - auditare obiect de bibliotecă de documente
 - descriere comandă 275
 - auditare receptor jurnal 259, 260
 - auditare securitate 619
 - auditare utilizator 71, 274, 275
 - autorizare
 - descriere comandă 272
 - intrare jurnal auditare (QAUDJRN) 247
 - biblioteca curentă 183, 185
 - coadă de ieșire 186
 - cod de contabilizare 82
 - comanda
 - parametru ALWLMTUSR (permitere utilizator limitat) 67
 - comandă
 - valori implicite 209
 - descriere de job
 - intrare jurnal auditare (QAUDJRN) 248
 - descriere dispozitiv
 - proprietar 179
 - director sistem
 - intrare jurnal auditare (QAUDJRN) 243
 - drept de proprietate
 - descriere dispozitiv 179
 - drept de proprietate asupra obiectului
 - mutare aplicație la producție 216
 - fișierul spool
 - intrare jurnal auditare (QAUDJRN) 250
 - gestiune sisteme
 - intrare jurnal auditare (QAUDJRN) 250
 - grup primar 272
 - intrare jurnal auditare (QAUDJRN) 248

- modificare (*continuare*)
- grup primar în timpul restaurării
 - intrare jurnal auditare (QAUDJRN) 245
 - ID utilizator
 - DST (unelte de service dedicate) 109
 - ID utilizator DST (unelte de service dedicate) 109
 - intrare de autentificare server 276
 - intrare director 276
 - intrare rutare
 - intrare jurnal auditare (QAUDJRN) 249
 - job
 - intrare jurnal auditare (QAUDJRN) 241
 - lista de biblioteci 183
 - lista de biblioteci sistem 183
 - listă acces control
 - intrare jurnal auditare (QAUDJRN) 249
 - listă de autorizații
 - intrare 271
 - listă de biblioteci sistem 202
 - listă de profiluri activă 617
 - menu
 - parametrul PRDLIB (biblioteca produs) 185
 - riscuri de securitate 185
 - modificare
 - intrare jurnal auditare (QAUDJRN) 248
 - obiect de bibliotecă de documente (DLO)
 - autorizare 275
 - grup primar 275
 - proprietar 275
 - obiect IPC
 - intrare jurnal auditare (QAUDJRN) 248
 - parolă
 - descriere 273
 - DST (unelte de service dedicate) 109, 273
 - profiluri utilizator livrate de IBM 108
 - setare parolă egală cu nume profil 60
 - valori de sistem de parole de impunere 39
 - parolă DST (unelte de service dedicate) 109
 - parole profil utilizator livrat de IBM 108
 - profil
 - Vedeți* modificare profil utilizator
 - profil de rețea
 - intrare jurnal auditare (QAUDJRN) 249
 - profil utilizator
 - descrieri comenzi 273, 274
 - intrare jurnal auditare (QAUDJRN) 245
 - metode 101
 - setare parolă egală cu nume profil 60
 - valori de sistem de compunere parolă 39
 - proprietar obiect 272
 - valoarea de sistem QAUDCTL (control auditare) 277
- modificare (*continuare*)
- valoarea de sistem QAUDLVL (nivel de auditare) 277
 - valoarea de sistem QSECURITY (nivel de securitate)
 - nivelul 10 în nivelul 20 10
 - nivelul 20 în nivelul 30 11
 - nivelul 30 în nivelul 20 10
 - nivelul 40 în nivelul 20 10
 - valoarea de sistem QSECURITY (security level - nivel de securitate)
 - nivelul 20 în nivelul 40 15
 - nivelul 20 în nivelul 50 17
 - nivelul 30 în nivelul 40 15
 - nivelul 30 în nivelul 50 17
 - nivelul 40 în nivelul 30 16
 - nivelul 50 la nivelul 30 sau 40 18
 - variabilă de sistem
 - intrare jurnal auditare (QAUDJRN) 249
 - Modificare a auditării securității - Change Security Auditing (CHGSECAUD)
 - Vedeți* și variabilă de sistem nivel auditare (QAUDLVL) auditare
 - un-pas 256
 - modificare CHGCURLIB (Change Current Library - Modificare bibliotecă curentă)
 - restricționare 185
 - modificare completă a parolei 44
 - modificare funcții de service
 - autorizare specială *SERVICE (service) 70
 - modificare sistem-suport gestionare jurnal 258
 - modificare totală a parolei 44
 - modul
 - director de legare 394
 - necesități ale autorizării obiect pentru comenzi 394
 - monitorizare
 - Vedeți* și auditare
 - acces neautorizat 233
 - atribute de rețea 233
 - autorizare 232
 - profiluri de utilizator 232
 - autorizare adoptată 232
 - autorizare obiect 268
 - autorizare specială *ALLOBJ (toate obiectele) 231
 - autorizări programator 231
 - capabilități limită 231
 - comunicații 233
 - controale parolă 231
 - criptare a datelor sensibile 233
 - date sensibile
 - autorizare 232
 - criptare 233
 - descrieri de joburi 232
 - eșare de program 268
 - integritate obiect 269
 - interfețe nesuportate 233
 - listă de verificare pentru 229
 - liste de biblioteci 232
 - logare de la distanță 233
 - logare fără ID-ul și parola utilizator 232
- monitorizare (*continuare*)
- mesaj
 - securitate 265
 - metode 265
 - privire generală 229
 - profil de grup
 - apartenență 231
 - parolă 231
 - profil utilizator
 - administrare 231
 - profiluri de utilizator furnizate de IBM 230
 - programe neautorizate 233
 - responsabil cu securitatea 270
 - securitate fizică 230
 - utilizare
 - coadă de mesaje QSYSMSG 233
 - istoric QHST (history-istoric sistem) 265
 - jurnale 265
 - utilizatori inactivi 232
 - valori de sistem 230
 - MOV
 - autorizarea obiect necesară 356
 - mutare
 - fișier spool 186
 - obiect
 - intrare jurnal auditare (QAUDJRN) 243
- ## N
- neautorizat
 - programe 233
 - nivel de ajutorare
 - avansat 58, 64
 - definiție 58
 - elementar 58, 64
 - exemplu de modificare 64
 - intermediar 58, 64
 - memorat cu profil utilizator 64
 - profil utilizator 63
 - nivel de ajutorare *ADVANCED (avansat) 64
 - nivel de ajutorare *BASIC (elementar) 64
 - nivel de ajutorare *INTERMED (intermediar) 64
 - nivel de ajutorare avansat (*ADVANCED) 58, 64
 - nivel de ajutorare elementar (*BASIC) 58, 64
 - nivel de auditare (*AUTFAIL) eșare autorizare 240
 - nivel de auditare (*PGMFAIL) eșare program 244
 - nivel de auditare *AUTFAIL (eșare autorizare) 240
 - nivel de auditare *CMD (șir comandă) 241
 - nivel de auditare *CREATE (creare) 241
 - nivel de auditare *DELETE (ștergere) 241
 - nivel de auditare *JOBDTA (modificare job) 241
 - nivel de auditare *OBJMGT (gestionare obiect) 243
 - nivel de auditare *OFCSRV (servicii de tip office) 243

nivel de auditare *OFCSRV (servicii office) 461, 479
 nivel de auditare *PGMADP (autorizare adoptată) 244
 nivel de auditare *PGMFAIL (eșuare program) 244
 nivel de auditare *PRTDTA (ieșire imprimantă) 244
 nivel de auditare *SAVRST (salvare/restaurare) 244
 nivel de auditare *SECURITY (securitate) 247
 nivel de auditare *SERVICE (unelte service) 250
 nivel de auditare *SPLFDTA (modificări fișier spool) 250, 496
 nivel de auditare *SYSMGT (gestionare sistem) 250
 nivel de auditare creare (*CREATE) 241
 nivel de auditare gestionare obiect (*OBJMGT) 243
 nivel de auditare gestionare sisteme (*SYSMGT) 250
 nivel de auditare ieșire tipărită (*PRTDTA) 244
 nivel de auditare modificare job (*JOBDTA) 241
 nivel de auditare modificări fișier spool (*SPLFDTA) 250, 496
 nivel de auditare salvare/restaurare (*SAVRST) 244
 nivel de auditare securitate (*SECURITY) 247
 nivel de auditare servicii de tip office (*OFCSRV) 243
 nivel de auditare servicii office (*OFCSRV) 461, 479
 nivel de auditare șir comandă (*CMD) 241
 nivel de auditare ștergere (*DELETE) 241
 nivel de auditare unelte service (*SERVICE) 250
 nivel forțare
 înregistrări auditare 51
 Nivel parolă (QPWDLVL)
 descriere 40
 nivel securitate valoare de sistem (QSECURITY)
 impunere valoare de sistem QLMTSECOFR 179
 nivelul 10
 valoarea de sistem QSECURITY (nivel de securitate) 10
 nivelul 20
 valoarea de sistem QSECURITY (nivel de securitate) 10
 nivelul 30
 valoarea de sistem QSECURITY (nivel de securitate) 11
 nivelul 40
 blocuri de control interne 17
 valoarea de sistem QSECURITY (nivel de securitate) 11
 nivelul 50
 bibliotecă QTEMP (temporară) 17
 blocuri de control interne 17
 tratate mesaj 17
 validarea parametrilor 14

nivelul 50 (continuare)
 valoarea de sistem QSECURITY (security level - nivel de securitate) 16
 Nivelul de asistență intermediar 58, 64
 NLV (versiune limbă națională)
 securitate comandă 209
 notificare, mesaj
 opțiune utilizator nici un mesaj de stare (*NOSTMSG) 90
 parametru DLVRY (livrare coadă de mesaje)
 profil utilizator 84
 număr de identificare grup (group identification number - gid)
 restaurarea 222
 număr necesar în parolă 44
 numărul de identificare utilizator (uid -user identification number)
 restaurarea 222
 numărul de identificare utilizator() parametru
 profil utilizator 90
 nume cale
 afișare 143
 nume generic
 exemplu 142
 numire
 auditare receptor jurnal 257
 profil de grup 59
 profil utilizator 59
 NVL (versiune limbă națională)
 securitate comandă 209

O

obiect
 (*Mgt) authority 112
 (*Ref) authority 112
 add (*ADD) authority 112, 300
 afișare
 originator 123
 asignarea autorizării și dreptului de proprietate 124
 atribut domeniu 13
 atribut stare 13
 auditare
 implicită 254
 modificare 71
 autorizare
 *ALL (all - toate) 113, 300
 *CHANGE (change - modificare) 113, 300
 *USE (use - utilizare) 300
 *USE (use) 113
 folosire referire 144
 nou 119
 obiect nou 118
 schimbare 138
 stocare 220
 subseturi definite de sistem 113
 subseturi folosite în mod obișnuit 113
 autorizare actualizare (*UPD) 300
 autorizare cerută pentru comenzi 303
 autorizare citire (*READ) 300
 autorizare executare (*EXECUTE) 300
 autorizare existență (*OBJEXIST) 112, 299
 autorizare gestionare (*OBJMGT) 299

obiect (continuare)
 autorizare gestiune (*OBJMGT) 112
 autorizare operațional (*OBJOPR) 112, 299
 autorizare read (*READ) 112
 autorizare ștergere (*DLT) 300
 controlarea accesului 13
 delete (*DLT) authority 112
 domeniu utilizator
 expunere de securitate 16
 restricționare 16
 drept de proprietate
 Vedeți și drept de proprietate obiect
 introducere 5
 eșuare interfață nesuportată 13
 execute (*EXECUTE) authority 112
 grup primar 101, 123
 lucru cu 272
 non-IBM
 tipărire listă 277
 profil utilizator proprietar (QDFTOWN)
 implicit 124
 restaurarea 219, 222
 salvarea 219
 securizarea cu o listă de autorizare 146
 stocare
 autorizare 220
 tipărire
 autorizație adoptată 621
 non-IBM 621
 sursă de autorizație 621
 transformat
 verificare 269
 update (*UPD) authority 112
 obiect *PGM (program) 487
 obiect *SVRSTG (spațiu de stocare server) 498
 obiect *USRIDX (index utilizator) 16
 obiect *USRQ (coadă utilizator) 16
 obiect *USRSPC (spațiu utilizator) 16
 obiect bibliotecă document (DLO)
 autorizație obiect cerută pentru comenzi 331
 obiect bibliotecă documente
 auditare obiect 462
 obiect coadă utilizator (*USRQ) 16
 obiect de bibliotecă de documente (DLO)
 adăugare autorizare 275
 afișare autorizare 275
 afișare listă de autorizații 275
 comenzi 275
 editare autorizare 275
 înlăturare autorizare 275
 modificare autorizare 275
 modificare grup primar 275
 modificare proprietar 275
 obiect de domeniu utilizator
 expunere de securitate 16
 restricționare 16
 obiect de personalizare stație de lucru
 autorizație obiect cerută pentru comenzi 443
 obiect index utilizator (*USRIDX) 16
 obiect IPC
 modificare
 intrare jurnal auditare (QAUDJRN) 248

- obiect nou
 - autorizare
 - parametru CRTAUT (create authority - creare autorizare) 118, 136
 - parametru GRPAUT (autorizare de grup) 80
 - parametru GRPAUT (autorizare grup) 122
 - parametru GRPAUTTYP (tip autorizare de grup) 81
 - autorizare (valoare de sistem QCRTAUT) 22
 - autorizare (valoare de sistem QUSEADPAUT) 30
 - exemplu de autorizare 124
 - exemplu de drept de proprietate 124
 - obiect referit 144
 - obiect spațiu de stocare server (*SVRSTG) 498
 - obiect spațiu utilizator (*USRSPC) 16
 - obiecte de grup primar
 - lucrul cu 123
 - obiecte furnizate de IBM
 - securizarea cu o listă de autorizare 118
 - obiectiv
 - confidențialitate 1
 - disponibilitate 1
 - integritate 1
 - obiectul *RCT (tabelă cod referință) 491
 - operație de restaurare
 - spațiu de stocare maxim (MAXSTG) 77
 - spațiu de stocare necesar 77
 - operații de sistem
 - parametru autorizare specială (SPCAUT) 68
 - operații grafice
 - autorizație obiect cerută pentru comenzi 345
 - operație de ștergere tip de intrare jurnal (DO) 241
 - oprire
 - auditare 50
 - conexiune
 - intrare jurnal auditare (QAUDJRN) 242
 - funcție de auditare 260
 - optic
 - necesități ale autorizării obiect pentru comenzi 401
 - opțiune utilizator *CLKWD (cuvânt cheie CL) 88, 89, 90
 - opțiune utilizator *EXPERT (expert) 88, 89, 90, 139
 - opțiune utilizator *HLPFULL (ajutor ecran întreg) 90
 - opțiune utilizator *PRTMSG (mesaj de tipărit) 90
 - opțiune utilizator ajutor ecran întreg (*HLPFULL) 90
 - opțiune utilizator cuvânt cheie CL (*CLKWD) 88, 89, 90
 - opțiune utilizator expert (*EXPERT) 88, 89, 90, 139
 - opțiune utilizator mesaj de tipărit (*PRTMSG) 90
 - opțiune utilizator tastă de rotire (*ROLLKEY) 90
- organigrama
 - autorizarea descriere de dispozitiv 177
 - organigramă
 - determinare mediu special 72
- P**
- pachet
 - necesități ale autorizării obiect pentru comenzi 405
 - parametru
 - validare 14
 - parametru ACGCDE (cod de contabilizare)
 - modificare 82
 - profil utilizator 82
 - parametru acțiune de auditare (AUDLVL)
 - profil utilizator 94
 - parametru ALWLMTUSR (permitere utilizator limitat)
 - comanda Creare comandă (CRTCMD) 67
 - comanda Modificare comandă (CHGCMD) 67
 - limitare capacități 67
 - parametru ASTLVL (nivel de ajutorare)
 - Vedeți și nivel de ajutorare
 - profil utilizator 63
 - parametru ATNPGM (program de tratare tastă Attn)
 - Vedeți și program de tratare tastă Attn
 - profil utilizator 86
 - parametru auditare obiect (OBJAUD)
 - profil utilizator 93
 - parametru AUDLVL (nivel de auditare)
 - profil utilizator 94
 - valoare *CMD (șir comandă) 241
 - parametru AUT (autorizare)
 - profil utilizator 93
 - parametru autorizare specială (SPCAUT)
 - Vedeți și autorizare specială
 - profil utilizator 68
 - recomandări 71
 - parametru bibliotecă curentă (CURLIB)
 - Vedeți și bibliotecă curentă
 - profil utilizator 64
 - parametru CCSID (identificator set de caractere codate)
 - profil utilizator 88
 - parametru CHRIDCTL (opțiuni utilizator)
 - profil utilizator 88
 - parametru clasă utilizator (USRCLS)
 - descriere 62
 - recomandări 63
 - parametru CNTRYID (identificator de regiune sau țară)
 - profil utilizator 88
 - parametru coadă de ieșire (OUTQ)
 - Vedeți și coadă de ieșire
 - profil utilizator 85
 - parametru coadă de mesaje (MSGQ)
 - Vedeți și coadă de mesaje
 - profil utilizator 83
 - parametru cod de contabilizare (ACGCDE)
 - modificare 82
 - profil utilizator 82
 - parametru CRTAUT (create authority - creare autorizare)
 - afișare 137
 - descriere 118
 - riscuri 119
 - parametru CURLIB (bibliotecă curentă)
 - Vedeți și bibliotecă curentă
 - profil utilizator 64
 - parametru de asociere eim (EIMASSOC)
 - profil utilizator 92
 - parametru de autorizare (AUT)
 - profil utilizator 93
 - parametru de gravitate (SEV)
 - Vedeți și coadă de mesaje
 - profil utilizator 84
 - parametru de livrare (DLVRY)
 - Vedeți și coadă de mesaje
 - profil utilizator 84
 - parametru de mediu special (SPCENV)
 - recomandări 72
 - rutare job interactiv 72
 - parametru de setare parolă la expirată (PWDEXP) 61
 - parametru de stare (STATUS)
 - profil utilizator 62
 - parametru descriere (TEXT)
 - profil utilizator 67
 - parametru descriere de job (JOBID)
 - Vedeți și descriere de job
 - profil utilizator 78
 - parametru DEV (dispozitiv de tipărire)
 - profil utilizator 85
 - parametru director de bază (HOMEDIR)
 - profil utilizator 91
 - parametru dispozitiv de tipărire (DEV)
 - profil utilizator 85
 - parametru DLVRY (livrare coadă de mesaje)
 - Vedeți și coadă de mesaje
 - profil utilizator 84
 - parametru DOCPWD (parolă document)
 - profil utilizator 83
 - parametru DSPSGNINF (afișare informații de semnare)
 - profil utilizator 73
 - parametru EIMASSOC (asociere eim)
 - profil utilizator 92
 - parametru GRPAUT (autorizare de grup)
 - profil utilizator 80
 - parametru GRPAUT (autorizare grup)
 - profil utilizator 122, 124
 - parametru GRPAUTTYP (tip autorizare de grup)
 - profil utilizator 81
 - parametru GRPAUTTYP (tip autorizare grup)
 - profil utilizator 124
 - parametru GRPPRF (profil de grup)
 - Vedeți și profil de grup
 - profil utilizator
 - descriere 79
 - parametru HOMEDIR (director de bază)
 - profil utilizator 91
 - parametru INLMNU (meniu inițial)
 - Vedeți și meniu inițial
 - profil utilizator 66
 - parametru INLPGM (program inițial)
 - modificare 65
 - profil utilizator 65

parametru JOBD (descriere de job)
Vedeți și descriere de job
profil utilizator 78

parametru LANGID (identificator de limbă)
parametru profil utilizator SRTSEQ 87
profil utilizator 87

parametru LCLPDMGT (gestiune parolă locală) 75

parametru limitare capabilități (LMTCPB)
Vedeți și capabilități de limitare
profil utilizator 66

parametru limită de prioritate (PTYLMT)
profil utilizator 77
recomandări 78

parametru LMTDEVSSN (limitare sesiuni dispozitiv)
Vedeți și limitare sesiuni dispozitiv
profil utilizator 75

parametru LOCALE (opțiuni utilizator)
profil utilizator 89

parametru MAXSTG (spațiu de stocare maxim)
operație de restaurare 76
profil utilizator 76
receptor jurnal 76

parametru meniu inițial (INLMNU)
Vedeți și meniu inițial
profil utilizator 66

parametru MSGQ (coadă de mesaje)
Vedeți și coadă de mesaje
profil utilizator 83

parametru nivel de auditare (AUDLVL)
modificare 106
valoare *AUTFAIL (eșuare autorizare) 240
valoare *CMD (șir comandă) 241
valoare *CREATE (creare) 241
valoare *DELETE (ștergere) 241
valoare *JOBDDTA (modificare job) 241
valoare *OBJMGT (gestionare obiect) 243
valoare *OFCSRVR (servicii de tip office) 243
valoare *PGMADP (autorizare adoptată) 244
valoare *PGMFAIL (eșuare program) 244
valoare *SAVRST (salvare/restaurare) 244
valoare *SECURITY (securitate) 247
valoare *SERVICE (unelte service) 250
valoare *SPLFDDTA (modificări fișier spool) 250
valoarea *SYSMGT (gestionare sisteme) 250

parametru OBJAUD (auditare obiect)
profil utilizator 93

parametru opțiune utilizator (CHRIDCTL)
profil utilizator 88

parametru opțiune utilizator (LOCALE)
profil utilizator 89

parametru opțiune utilizator (SETJOBATR)
profil utilizator 89

parametru opțiune utilizator (USROPT)
*CLKWD (cuvânt cheie CL) 88, 89, 90
*EXPERT (expert) 88, 89, 90
*HLPFULL (ajutor ecran întreg) 90

parametru opțiune utilizator (USROPT)
(continuare)
*NOSTSMSG (nici un mesaj de stare) 90
*PRMSG (mesaj de tipărit) 90
*ROLLKEY (tastă de rotire) 90
*STSMSG (mesaj de stare) 90
profil utilizator 88, 89, 90

parametru OUTQ (coadă de ieșire)
Vedeți și coadă de ieșire
profil utilizator 85

parametru permite utilizator limitat (ALWLMTUSR)
comanda Creare comandă (CRTCMD) 67
comanda Modificare comandă (CHGCMD) 67
limitare capabilități 67

parametru profil utilizator
număr identificare grup (gid) 91

parametru program inițial (INLPGM)
modificare 65
profil utilizator 65

parametru PTYLMT (limită de prioritate)
profil utilizator 77
recomandări 78

parametru PWDEXP (setare parolă la expirată) 61

parametru PWDEXPITV (interval de expirare parolă) 74

parametru SETJOBATR (opțiuni utilizator)
profil utilizator 89

parametru SEV (gravitate coadă de mesaje)
Vedeți și coadă de mesaje
profil utilizator 84

parametru spațiu de stocare maxim (MAXSTG)
operație de restaurare 76
profil utilizator 76
receptor jurnal 76

parametru SPCAUT (autorizare specială)
Vedeți și autorizare specială
profil utilizator 68
recomandări 71

parametru SPCENV (mediu special)
recomandări 72
rutare job interactiv 72

parametru SRTSEQ (secvență de sortare)
profil utilizator 87

parametru SUPGRPPRF (grupuri suplimentare)
profil utilizator 81

parametru text (TEXT)
profil utilizator 67

parametru USER în descrierea de job 181

parametru USRCLS (clasă utilizator)
descriere 62
recomandări 63

parametru USROPT (opțiune utilizator)
*CLKWD (cuvânt cheie CL) 88, 89, 90
*EXPERT (expert) 88, 89, 90
*HLPFULL (ajutor ecran întreg) 90
*NOSTSMSG (nici un mesaj de stare) 90
*PRMSG (mesaj de tipărit) 90
*ROLLKEY (tastă de rotire) 90
*STSMSG (mesaj de stare) 90

parametru USROPT (opțiuni utilizator)
profil utilizator 88, 89, 90

parametru USRPRF (nume) 59

parametrul (ALWBJDIF - allow object difference) permisiune a diferențelor dintre obiecte) 223

parametrul ALWBJDIF (allow object difference - permisiune a diferențelor dintre obiecte) 223

parametrul AUT (authority)
crearea bibliotecilor 136
crearea obiectelor 137
specificarea listei de autorizare (*AUTL) 145

parametrul AUTCHK (autorizare pentru verificare) 187

parametrul autorizare (AUT)
crearea bibliotecilor 136
crearea obiectelor 137
specificarea listei de autorizare (*AUTL) 145

parametrul create authority (CRTAUT)
afișare 137
descriere 118
riscuri 119

parametrul DSPDDTA (afișare date) 186

parametrul GRPPRF (profil grup)
profil utilizator
exemplu 124

parametrul MAXSTG (spațiu de stocare maxim)
deținător de autorizare
transferat la QDFTOWN (proprietar implicit) 124
drept de proprietate grup al obiectelor 122

parametrul OPRCTL (control operator) 187

parametrul OWNER (proprietar)
profil utilizator 124

parametrul spațiu de stocare maxim (MAXSTG)
deținător de autorizare
transferat la QDFTOWN (proprietar implicit) 124
drept de proprietate grup al obiectelor 122

parametrul use adopted authority (USEADPAUT) 131

parametrul USEADPAUT (use adopted authority - folosire autorizare adoptată) 131

parametrul user option (USROPT)
*EXPERT (expert) 139

parametrul USROPT (user option - opțiune utilizator)
*EXPERT (expert) 139

parolă
auditare
DST (dedicated service tools - unelte dedicate de service) 230
utilizator 231
comenzi pentru lucrul cu 273
comunicații 41
criptare 60
document
parametru profil utilizator
DOCPWD 83
DST (dedicated service tools - unelte dedicate de service)
auditare 230

- parolă (*continuare*)
- DST (unelte de service dedicate)
 - modificare 109
 - egal cu numele profilului utilizatorului 39
 - egală cu nume profil utilizator 60
 - expirare imediată 39
 - gestiune parolă locală
 - parametru profil utilizator LCLPWDMGT 75
 - incorect
 - intrare jurnal auditare (QAUDJRN) 240
 - interval de expirare
 - auditare 231
 - parametru profil utilizator PWDEXPITV 74
 - valoarea de sistem QPWDEXPITV 39
 - împiedicare
 - caractere repetate 43
 - digiiți alăturați (valoarea de sistem QPWDLMTAJC) 43
 - folosirea cuvintelor 42
 - trivială 38
 - lungime
 - valoarea de sistem minimă (QPWDMINLEN) 41
 - valoarea sistem maximă (QPWDMAXLEN) 41
 - lungime maximă (valoarea de sistem QPWDMAXLEN) 41
 - lungime minimă (valoarea de sistem QPWDMINLEN) 41
 - modificare
 - descriere 273
 - DST (unelte de service dedicate) 273
 - setare parolă egală cu nume profil 60
 - valori de sistem de parole de impunere 39
 - modificare la restaurare a profilului 221
 - necesitate
 - caracter numeric character 44
 - diferit (valoarea de sistem QPWDRQDDIF) 42
 - modificare (valoarea de sistem QPWDEXPITV) 39
 - modificare completă 44
 - necesită
 - modificare (parametru PWDEXPITV) 74
 - numai cifre 60
 - parametru de expirare (PWDEXP) 61
 - permisiunea utilizatorilor pentru modificare 231
 - pierdut 60
 - prevenire
 - simplu 231
 - profil de utilizator furnizat de IBM
 - auditare 230
 - profil utilizator 60
 - profil utilizator livrat de IBM
 - modificare 108
 - profil utilizator QPGMR (programator) 627
 - profil utilizator QSRV (service) 627
 - profil utilizator QSRVBAS (serviciu de bază) 627
- parolă (*continuare*)
- profil utilizator QSYSOPR (operator sistem) 627
 - profil utilizator QUSER (utilizator) 627
 - program aprobare
 - cerințe 45
 - exemplu 46
 - risc securitate 45
 - valoarea de sistem QPWDVLDPGM 44
 - program validare
 - cerințe 45
 - exemplu 46
 - risc securitate 45
 - valoarea de sistem QPWDVLDPGM 44
 - programul de validare ieșire
 - exemplu 46
 - PWDEXP (setare parolă la expirată) 61
 - recomandări 61, 62
 - reguli 60
 - resetare
 - DST (dedicated service tools - unelte dedicate de service) 245
 - utilizator 60
 - restricționare
 - caractere 42
 - caractere repetate 43
 - digiiți alăturați (valoarea de sistem QPWDLMTAJC) 43
 - rețea
 - intrare jurnal auditare (QAUDJRN) 241
 - setare la expirată (PWDEXP) 61
 - simplu
 - împiedicare 231
 - sistem 109
 - trivială
 - împiedicare 38
 - valoarea de sistem caractere de poziție (QPWDDIF) 44
 - valoarea sistem (PWDEXPITV) interval expirare
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDLMTCHR)
 - caractere restricționate
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDLMTREP) limită
 - caractere repetate
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDMAXLEN) lungime minimă
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDMINLEN) lungime minimă
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDDIF) necesită diferență de poziție
 - valoarea setată de comanda CFGSYSSEC 625
- parolă (*continuare*)
- valoarea sistem (QPWDRQDDGT) necesită caractere numerice
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWDRQDDIF) diferență cerută
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem (QPWVLDPGM) program de validare
 - valoarea setată de comanda CFGSYSSEC 625
 - valoarea sistem a caracterelor alăturate interzise (QPWDLMTAJC)
 - valoarea setată de comanda CFGSYSSEC 625
 - valori de sistem
 - privire generală 38
 - valori posibile 60
 - verificare 107, 273
 - verificarea pentru valori implicite 617
 - parolă aprobare 44
 - parolă de sistem 109
 - parolă incorectă
 - intrare jurnal auditare (QAUDJRN) 240, 241
 - parolă numai cifre 60
 - parolă numerică 60
 - parolă simplă
 - prevenire 231
 - parolă trivială
 - împiedicare 38
 - parolă validare 44
 - parole
 - niveluri de parolare 268
 - Parole 40
 - parole repetate 42
 - passthrough
 - controlare semnare 27
 - modificare de profil destinație
 - intrare jurnal auditare (QAUDJRN) 248
 - passthrough stație de afișare
 - autorizație obiect cerută pentru comenzi 330
 - modificare de profil destinație
 - intrare jurnal auditare (QAUDJRN) 248
 - PC (calculator personal)
 - împiedicare acces 189
 - PC Organizer
 - deconectare (valoarea de sistem QINACTMSGQ) 24
 - permisă pentru limitare capabilități utilizator 67
 - PCSACC (Cerere client acces) atribut
 - rețea 189
 - performanța
 - clasa 192
 - descriere de job 192
 - descriere de subsistem 192
 - felia de timp 192
 - intrare de rutare 192
 - limită prioritate 192
 - planificare job 192
 - pool 192

performanța (*continuare*)
 prioritate de ieșire 192
 prioritate de rulare 192
 restricționare joburi la batch 193
 spațiu de stocare
 pool 192
 performanță
 autorizație obiect cerută pentru comenzi 406
 permise
 definiție 114
 permisiune
 utilizatori pentru a modifica parolele 231
 permisiune utilizator
 acordare 275
 autorizație obiect cerută pentru comenzi 400
 revocare 275
 permite obiectului să restaureze valori sistem (QALWBJRST)
 valoare setată de comanda CFGSYSSEC 625
 personalizare
 valori securitate 625
 planificare
 audit
 variabile de sistem 254
 auditare
 acțiuni 234
 obiecte 252
 privire generală 234
 controale parolă 231
 grup primar 213
 grupuri multiple 214
 listă de verificare pentru 229
 profil utilizator
 activare 617
 expirare 617
 profiluri de grup 213
 proiectare bibliotecă 199
 rapoarte de securitate 620
 securitate 1
 securitate comandă 208
 securitate fișier 209
 securitate fizică 230
 securitate meniu 203
 securitate programator aplicație 215
 securitate programator sistem 216
 planificare job
 autorizație obiect cerută pentru comenzi 372
 planificare modificării nivel parolă
 creștere nivel parolă 197
 modificare nivel parolă de la 1 la 0 199
 modificare nivel parolă de la 2 la 0 199
 modificare nivel parolă de la 2 la 1 199
 modificare nivel parolă de la 3 la 0 199
 modificare nivel parolă de la 3 la 1 199
 modificare nivel parolă de la 3 la 2 198
 modificare niveluri parolă
 planificare modificării nivel 196, 197
 modificare niveluri parolă (0 la 1) 197
 modificare niveluri parolă (0 la 2) 197
 modificare niveluri parolă (1 la 2) 197
 modificare niveluri parolă (2 la 3) 198
 Modificări QPWLVL 196, 197
 scădere niveluri parolă 198, 199
 planificare prioritate
 limitare 77
 plin
 receptor jurnal auditare (QAUDJRN) 258
 pool 192
 pool de stocare 192
 pornire
 conexiune
 intrare jurnal auditare (QAUDJRN) 242
 funcție de auditare 256
 Pornire comandă QSH (STRQSH)
 autorizarea obiect necesară
 alias, QSH 415
 porțiune sistem
 lista de biblioteci
 descriere 183
 recomandări 184
 listă de biblioteci
 modificare 202
 porțiune utilizator
 lista de biblioteci
 descriere 183
 recomandări 185
 listă de biblioteci
 controlare 201
 poștă
 tratare
 intrare jurnal auditare (QAUDJRN) 243
 pretindere
 spațiu de stocare 17, 124
 setare valoare de sistem
 QALWUSRDMN (permitere obiecte utilizator) 22
 prevenire
 acces neautorizat 233
 logare fără ID-ul și parola utilizator 232
 parole simple 231
 programe neautorizate 233
 prezentare job la distanță
 securizare 189
 prioritate 192
 prioritate de ieșire 192
 prioritate de rulare 192
 privilegiu
 Vedeți și autorizare
 definiție 111
 problemă
 necesități ale autorizării obiect pentru comenzi 411
 procesare parolă 109
 procesor cheie IPL 230
 procesor de comenzi QCMD
 mediu special (SPCENV) 72
 Program de tratare tastă Attn 86
 profil
 acțiuni de auditare (AUDLVL) 94
 analizare cu interogare 267
 auditare
 autorizare de folosit 232
 autorizare specială *ALLOBJ 231
 auditare apartenență 231
 auditare obiect (OBJAUD) 93
 auditare parolă 231
 AUDLVL (acțiune de auditare) 94
 profil (*continuare*)
 furnizat de IBM
 auditare 230
 Cadru de lucru server de mail (QMSF) 281
 cerere test (QTSTRQS) 281
 document (QDOC) 281
 executiv nod sisteme distribuite (QDSNX) 281
 finanțe (QFNC) 281
 instalare automată (QLPAUTO) 281
 instalare programe cu licență (QLPINSTALL) 281
 intrare job la distanță (QRJE) 281
 job spool (QSPLJOB) 281
 operator sistem (QSYSOPR) 281
 partajare bază de date (QDBSHR) 281
 profil de autorizare (QAUTPROF) 281
 profil de autorizare IBM (QAUTPROF) 281
 profil utilizator BRM (QBRMS) 281
 programator (QPGMR) 281
 proprietar (QDFTOWN) implicit 281
 punte VM/MVS (QGATE) 281
 QAUTPROF (profil de autorizare IBM) 281
 QBRMS (profil utilizator BRM) 281
 QDBSHR (partajare bază de date) 281
 QDFTOWN (proprietar implicit) 281
 QDOC (document) 281
 QDSNX (executiv nod sisteme distribuite) 281
 QFNC (finanțe) 281
 QGATE (punte VM/MVS) 281
 QLPAUTO (instalare automată de program cu licență) 281
 QLPINSTALL (instalare program cu licență) 281
 QMSF (cadru de lucru server de mail) 281
 QNFSANON (sistem de fișiere rețea) 281
 QPGMR (programator) 281
 QRJE (intrare job la distanță) 281
 QSECOFR (responsabil cu securitatea) 281
 QSNADS (servicii de distribuție Arhitectură rețea de sisteme) 281
 QSPL (spool) 281
 QSPLJOB (job spool) 281
 QSRV (serviciu) 281
 QSRVBAS (serviciu elementar) 281
 QSYS (sistem) 281
 QSYSOPR (operator sistem) 281
 QTCP (TCP/IP) 281
 QTMLPLD (suport tipărire TCP/IP) 281
 QTSTRQS (cerere test) 281
 QUSER (utilizator stație de lucru) 281
 responsabil cu securitatea (QSECOFR) 281
 servicii de distribuție SNA (QSNADS) 281

- profil (*continuare*)
 furnizat de IBM (*continuare*)
 serviciu (QSRV) 281
 serviciu elementar (QSRVBAS) 281
 sistem (QSYS) 281
 sistem de fișiere rețea (QNFS) 281
 spool (QSPL) 281
 suport tipărire TCP/IP (QTMLPD) 281
 TCP/IP (QTCP) 281
 utilizator stație de lucru (QUSER) 281
- grup 231
Vedeți și profil de grup
 auditare 231
 drept de proprietate obiect 122
 introducere 4, 57
 numire 59
 parolă 60
 planificare 213
 securitate de resurse 4
- livrat de IBM
 comenzi restricționate 287
 modificare 274
 OBJAUD (auditare obiect) 93
 QDFTOWN (default owner - deținător implicit)
 restaurare de programe 225
- swap
 intrare jurnal auditare (QAUDJRN) 248
- tabelă valori implicite 279
- tratare
 intrare jurnal auditare (QAUDJRN) 248
- utilizator 93, 94, 267
 ACGCDE (cod de contabilizare) 82
 afișare informații de semnare (DSPSGNINF) 73
 asociere eim (EIMASSOC) 92
 ASTLVL (nivel de ajutorare) 63
 ATNPGM (program de tratare tastă Attn) 86
 auditare 231
 autorizare (AUT) 93
 autorizare de grup (GRPAUT) 80
 autorizare grup (GRPAUT) 122
 autorizare publică (AUT) 93
 autorizare specială (SPCAUT) 68
 bibliotecă curentă (CURLIB) 64
 capabilități limită 231
 CCSID (identificator set de caractere codate) 88
 CHRIDCTL (opțiuni utilizator) 88
 clasă utilizator (USRCLS) 62
 CNTRYID (identificator de regiune sau țară) 88
 coadă de ieșire (OUTQ) 85
 coadă de mesaje (MSGQ) 83
 cod de contabilizare (ACGCDE) 82
 creare automată 57
 CURLIB (bibliotecă curentă) 64
 descriere (TEXT) 67
 descriere de job (JOB) 78
 DEV (dispozitiv de tipărire) 85
 director de bază (HOMEDIR) 91
 dispozitiv de tipărire (DEV) 85
- profil (*continuare*)
 utilizator (*continuare*)
 DLVRY (livrare coadă de mesaje) 84
 DOCPWD (parolă document) 83
 DSPSGNINF (afișare informații de semnare) 73
 extragere 107
 gestiune parolă locală (LCLPWDMGT) 75
 gravitate (SEV) 84
 gravitate coadă de mesaje (SEV) 84
 GRPAUT (autorizare de grup) 80
 GRPAUT (autorizare grup) 122
 GRPAUTTYP (tip autorizare de grup) 81
 GRPPRF (grup) 79
 grup (GRPPRF) 79
 grupuri suplimentare (SUPGRPPRF) 81
 identificator de limbă (LANGID) 87
 identificator de regiune sau țară (CNTRYID) 88
 identificator set de caractere codate (CCSID) 88
 INLMNU (meniu inițial) 66
 INLPGM (program inițial) 65
 interval de expirare parolă (PWDEXPITV) 74
 introducere 4
 JOB (descriere de job) 78
 KBDBUF (punere în buffer tastatură) 76
 LANGID (identificator de limbă) 87
 LCLPWDMGT (gestiune parolă locală) 75
 limitare capabilități 66
 limitare sesiuni dispozitiv (LMTDEVSSN) 75
 limită de prioritate (PTYLMT) 77
 listare inactivă 268
 listare selectată 267
 listare utilizatori cu autorizare specială 267
 listare utilizatori cu comanda capabilitate 267
 livrare (DLVRY) 84
 livrare coadă de mesaje (DLVRY) 84
 livrat de IBM 108
 LMTCPB (limitare capabilități) 66
 LMTDEVSSN (limitare sesiuni dispozitiv) 75
 LOCALE (opțiuni utilizator) 89
 mare, examinare 268
 MAXSTG (spațiu de stocare maxim) 76
 mediu special (SPCENV) 72
 mediu System/36 72
 meniu inițial (INLMNU) 66
 modificare 101
 MSGQ (coadă de mesaje) 83
 nivel de ajutorare (ASTLVL) 63
 număr identificare grup (gid) 91
 numărul de identificare utilizator() 90
 numire 59
 opțiuni utilizator (CHRIDCTL) 88
 opțiuni utilizator (LOCALE) 89
- profil (*continuare*)
 utilizator (*continuare*)
 opțiuni utilizator (SETJOBATR) 89
 opțiuni utilizator (USROPT) 88, 89, 90
 OUTQ (coadă de ieșire) 85
 parolă 60
 parolă document (DOCPWD) 83
 profil utilizator (USRPRF) 59
 program de tratare tastă Attn (ATNPGM) 86
 program inițial (INLPGM) 65
 proprietar al obiectelor create (OWNER) 79
 proprietarul obiectelor create (OWNER) 122
 PTYLMT (limită de prioritate) 77
 punere în buffer tastatură (KBDBUF) 76
 PWDEXP (setare parolă la expirată) 61
 PWDEXPITV (interval de expirare parolă) 74
 redenumire 106
 roluri 57
 secvență de sortare (SRTSEQ) 87
 setare parolă la expirare (PWDEXP) 61
 SETJOBATR (opțiuni utilizator) 89
 SEV (gravitate coadă de mesaje) 84
 spațiu de stocare maxim (MAXSTG) 76
 SPCAUT (autorizare specială) 68
 SPCENV (mediu special) 72
 SRTSEQ (secvență de sortare) 87
 stare (STATUS) 62
 SUPGRPPRF (grupuri suplimentare) 81
 text (TEXT) 67
 tip autorizare de grup (GRPAUTTYP) 81
 USRCLS (clasă utilizator) 62
 USROPT (opțiuni utilizator) 88, 89, 90
 USRPRF (nume) 59
- profil de grup
 auditare
 apartenență 231
 autorizare specială *ALLOBJ 231
 parolă 231
 comparație
 listă de autorizații 215
 drept de proprietate obiect 122
 introducere 4, 57
 listă de autorizații
 comparație 215
 multiple
 planificare 214
 numire 59
 parametru profil utilizator
 modificare la restaurare a profilului 221
 parametru profil utilizator GRPPRF
 descriere 79
 modificare la restaurare a profilului 221
 parolă 60

- profil de grup (*continuare*)
 - planificare 213
 - primar 123
 - planificare 213
 - profil utilizator
 - descriere 79
 - securitate de resurse 4
 - securitate resursă 111
 - suplimentar
 - parametru SUPGRPPRF (grupuri suplimentare) 81
- profil de rețea
 - modificare
 - intrare jurnal auditare (QAUDJRN) 249
- profil de utilizator furnizat de IBM
 - auditare 230
 - restaurarea 222
- profil mare de utilizator 268
- profil utilizator
 - (gid) număr identificare grup 91
 - (numărul de identificare utilizator) 90
 - ACGCDE (cod de contabilizare) 82
 - activare
 - program eșantion 104
 - acțiune de auditare (AUDLVL) 94
 - afișare
 - descriere comandă 274
 - individual 104
 - informații semnare (DSPSGNINF) 73
 - programe care adoptă 130
 - analizare
 - de autorizările speciale 621
 - de către clasa de utilizatori 621
 - analizare cu interogare 267
 - asociere eim (EIMASSOC) 92
 - ASTLVL (nivel de ajutorare) 63
 - ATNPGM (program de tratare tastă Attn) 86
 - auditare
 - autorizare de folosit 232
 - autorizare specială *ALLOBJ 231
 - utilizatori autorizați 267
 - auditare obiect (OJAUD) 93
 - AUDLVL (acțiune de auditare) 94
 - AUDLVL (nivel de auditare)
 - valoare *CMD (șir comandă) 241
 - AUT (autorizare) 93
 - autorizare (AUT) 93
 - autorizare de grup (GRPAUT) 80
 - autorizare grup (GRPAUT) 122, 124
 - autorizare publică (AUT) 93
 - autorizare specială (SPCAUT) 68
 - autorizare specială *ALLOBJ (toate obiectele) 68
 - autorizare specială *AUDIT (auditare) 71
 - autorizare specială *IOSYSCFG (configurare sistem) 71
 - autorizare specială *JOBCTL (control de job) 69
 - autorizare specială *SAVSYS (salvare sistem) 70
 - autorizare specială *SECADM (administrator de securitate) 69
 - autorizare specială *SERVICE (service) 70
- profil utilizator (*continuare*)
 - autorizare specială *SPLCTL (control de spool) 69
 - autorizare specială administrator de securitate (*SECADM) 69
 - autorizare specială configurare sistem (*IOSYSCFG) 71
 - autorizare specială control de job (*JOBCTL) 69
 - autorizare specială control de spool (*SPLCTL) 69
 - autorizare specială de auditare (*AUDIT) 71
 - autorizare specială de service (*SERVICE) 70
 - autorizare specială salvare sistem (*SAVSYS) 70
 - autorizare specială toate obiectele (*ALLOBJ) 68
 - autorizație obiect cerută pentru comenzi 439, 440
 - autorizări private 95
 - biblioteca curentă (CURLIB) 64
 - capabilități limită
 - auditare 231
 - CCSID (identificator set de caractere codate) 88
 - clasă utilizator (USRCLS) 62
 - CNTRYID (identificator de regiune sau țară) 88
 - coadă de ieșire (OUTQ) 85
 - coadă de mesaje (MSGQ) 83
 - cod de contabilizare (ACGCDE) 82
 - comenzi înrudite pentru lucru cu 275
 - comenzi pentru lucrul cu 274
 - copiere 99
 - creare
 - descriere exemplu 98
 - descrieri comenzi 273, 274
 - intrare jurnal auditare (QAUDJRN) 245
 - metode 96
 - creare automată 57
 - CURLIB (bibliotecă curentă) 64
 - descriere (TEXT) 67
 - descriere de job (JOB) 78
 - DEV (dispozitiv de tipărire) 85
 - director de bază (HOMEDIR) 91
 - dispozitiv de tipărire (DEV) 85
 - DLVRY (livrare coadă de mesaje) 84
 - DOCPWD (parolă document) 83
 - DSPSGNINF (afișare informații de semnare) 73
 - EIMASSOC (asociere eim) 92
 - extragere 107, 274
 - folosit în descrierea de job 13
 - furnizat de IBM
 - auditare 230
 - tabelă valori implicite 279
 - gestionare 97
 - gestiune parolă locală (LCLPWDMGT) 75
 - gravitate (SEV) 84
 - gravitate coadă de mesaje (SEV) 84
 - GRPAUT (autorizare de grup) 80
 - GRPAUT (autorizare grup) 122, 124
 - GRPAUTTYP (tip autorizare de grup) 81
- profil utilizator (*continuare*)
 - GRPAUTTYP (tip autorizare grup) 124
 - GRPPRF (profil de grup)
 - descriere 79
 - GRPPRF (profil grup) 124
 - grup primar 103
 - grupuri suplimentare (SUPGRPPRF) 81
 - HOMEDIR (director de bază) 91
 - ID-uri utilizator doar cifre 59
 - identificator de limbă (LANGID) 87
 - identificator de regiune sau țară (CNTRYID) 88
 - identificator set de caractere codate (CCSID) 88
 - informații obiect deținut 95
 - INLMNU (meniu inițial) 66
 - INLPGM (program inițial) 65
 - interval de expirare parolă (PWDEXPITV) 74
 - introducere 4
 - JOB) (descriere de job) 78
 - KBDBUF (punere în buffer tastatură) 76
 - LANGID (identificator de limbă) 87
 - LCLPWDMGT (gestiune parolă locală) 75
 - limitare capabilități
 - descriere 66
 - lista de biblioteci 185
 - limitare sesiuni dispozitiv (LMTDEVSSN) 75
 - limită de prioritate (PTYLMT) 77
 - listare
 - inactiv 268
 - selectat 267
 - toți utilizatorii 104
 - utilizatori cu autorizare specială 267
 - utilizatori cu comanda capabilitate 267
 - listare toate 104
 - listă de activ permanent
 - modificare 617
 - livrare (DLVRY) 84
 - livrare coadă de mesaje (DLVRY) 84
 - livrat de IBM
 - scop 108
 - LMTCPB (limitare capabilități) 66, 185
 - LMTDEVSSN (limitare sesiuni dispozitiv) 75
 - LOCALE (Locale) 89
 - LOCALE (opțiuni utilizator) 89
 - lucru cu 274
 - mare, examinare 268
 - MAXSTG (spațiu de stocare maxim)
 - descriere 76
 - drept de proprietate grup al obiectelor 122
 - mediu special (SPCENV) 72
 - mediu System/36 72
 - meniu inițial (INLMNU) 66
 - modificare
 - descrieri comenzi 274
 - intrare jurnal auditare (QAUDJRN) 245
 - metode 101
 - parolă 273
 - setare parolă egală cu nume profil 60

- profil utilizator (*continuare*)
- modificare (*continuare*)
 - valori de sistem de componere parolă 39
 - MSGQ (coadă de mesaje) 83
 - nivel de ajutorare (ASTLVL) 63
 - nivel de auditare (AUDLVL)
 - valoare *CMD (șir comandă) 241
 - număr identificare grup (gid) 91
 - numărul de identificare utilizator() 90
 - numire 59
 - OBJAUD (auditare obiect) 93
 - opțiuni utilizator (CHRIDCTL) 88
 - opțiuni utilizator (LOCALE) 89
 - opțiuni utilizator (SETJOBATR) 89
 - opțiuni utilizator (USROPT) 88, 89, 90
 - OUTQ (coadă de ieșire) 85
 - OWNER (proprietar al obiectelor create) 79
 - OWNER (proprietar) 124
 - OWNER (proprietarul obiectelor create) 122
 - parolă 60
 - parolă document (DOCPWD) 83
 - performanță
 - salvare și restaurare 95
 - profil de grup (GRPPRF)
 - descriere 79
 - profil grup (GRPPRF) 124
 - profil utilizator (USRPRF) 59
 - program de tratare tastă Attn (ATNPGM) 86
 - program inițial (INLPGM) 65
 - proprietar (OWNER) 124
 - proprietar al obiectelor create (OWNER) 79
 - proprietar obiect
 - ștergere 122
 - proprietarul obiectelor create (OWNER) 122
 - PTYLMT (limită de prioritate) 77
 - puncte de ieșire 107
 - punere în buffer tastatură (KBDBUF) 76
 - PWDEXP (setare parolă la expirată) 61
 - PWDEXPITV (interval de expirare parolă) 74
 - redenumire 106
 - restaurare
 - descriere comandă 275
 - restaurare autorizare
 - intrare jurnal auditare (QAUDJRN) 245
 - restaurarea
 - comenzi 219
 - intrare jurnal auditare (QAUDJRN) 245
 - roluri 57
 - salvarea 219
 - secvență de sortare (SRTSEQ) 87
 - setare atribuit de job (opțiuni utilizator) 88, 89
 - setare parolă la expirată (PWDEXP) 61
 - SEV (gravitate coadă de mesaje) 84
 - spațiu de stocare maxim (MAXSTG)
 - descriere 76
 - drept de proprietate grup al obiectelor 122
- profil utilizator (*continuare*)
- SPCAUT (autorizare specială) 68
 - SPCENV (mediu special) 72
 - SRTSEQ (secvență de sortare) 87
 - stare (STATUS) 62
 - SUPGRPPRF (grupuri suplimentare) 81
 - ștergere
 - coadă de mesaje 101
 - descriere comandă 274
 - fișiere spool 103
 - intrare director 101
 - liste de distribuție 101
 - tabelă valori implicite 279
 - text (TEXT) 67
 - tip autorizare de grup (GRPAUTTY) 81
 - tip autorizare grup (GRPAUTTY) 124
 - tipărire
 - Vedeți* listare
 - tipuri de ecrane 105
 - tipuri de rapoarte 105
 - USRCLS (clasă utilizator) 62
 - USROPT (opțiuni utilizator) 88, 89, 90
 - USRPRF (nume) 59
 - verificarea pentru parole implicite 617
 - profil utilizator (QLPINSTALL) instalare a programului licențiat
 - restaurarea 222
 - profil utilizator ADSM (QADSM) 281
 - profil utilizator AFDFTUSR (QAFDFTUSR) 281
 - profil utilizator AFOWN (QAFOWN) 281
 - profil utilizator AFUSR (QAFUSR) 281
 - profil utilizator BRM (QBRMS) 281
 - profil utilizator cadru de lucru server de mail (QMSF) 281
 - profil utilizator cerere test (QTSTRQS) 281
 - profil utilizator cu partajare bază de date (QDBSHR) 281
 - profil utilizator cu profil autorizare (QAUTPROF) 281
 - profil utilizator DCEADM (QDCEADM) 281
 - profil utilizator executiv nod sisteme distribuite (QDSNX) 281
 - profil utilizator finanțe (QFNC) 281
 - profil utilizator furnizat de IBM
 - proprietar (QDFTOWN) implicit
 - descriere 124
 - QDFTOWN (proprietar implicit)
 - descriere 124
 - tabelă valori implicite 279
 - profil utilizator instalare automată (QLPAUTO)
 - valori implicite 281
 - profil utilizator instalare program cu licență (QLPINSTALL)
 - valori implicite 281
 - profil utilizator intrare job la distanță (QRJE) 281
 - profil utilizator job spool (QSPLJOB) 281
 - profil utilizator livrat de IBM
 - Vedeți și* profiluri specifice
 - ADSM (QADSM) 281
 - AFDFTUSR (QAFDFTUSR) 281
 - AFOWN (QAFOWN) 281
 - AFUSR (QAFUSR) 281
 - BRM (QBRMS) 281
- profil utilizator livrat de IBM (*continuare*)
- Cadru de lucru server de mail (QMSF) 281
 - cerere test (QTSTRQS) 281
 - comenzi restricționate 287
 - DCEADM (QDCEADM) 281
 - document (QDOC) 281
 - executiv nod sisteme distribuite (QDSNX) 281
 - finanțe (QFNC) 281
 - instalare automată (QLPAUTO) 281
 - instalare programe cu licență (QLPINSTALL) 281
 - intrare job la distanță (QRJE) 281
 - job spool (QSPLJOB) 281
 - modificare parolă 108
 - operator sistem (QSYSOPR) 281
 - partajare bază de date (QDBSHR) 281
 - profil autorizare (QAUTPROF) 281
 - profil de autorizare IBM (QAUTPROF) 281
 - profil utilizator BRM (QBRMS) 281
 - Profil utilizator NFS (QNFSANON) 281
 - programator (QPGMR) 281
 - proprietar (QDFTOWN) implicit
 - valori implicite 281
 - punte VM/MVS (QGATE) 281
 - QADSM (ADSM) 281
 - QAFDFTUSR (AFDFTUSR) 281
 - QAFOWN (AFOWN) 281
 - QAFUSR (AFUSR) 281
 - QAUTPROF (partajare bază de date) 281
 - QAUTPROF (profil de autorizare IBM) 281
 - QBRMS (BRM) 281
 - QBRMS (profil utilizator BRM) 281
 - QDBSHR (partajare bază de date) 281
 - QDCEADM (DCEADM) 281
 - QDFTOWN (proprietar implicit)
 - valori implicite 281
 - QDOC (document) 281
 - QDSNX (executiv nod sisteme distribuite) 281
 - QFNC (finanțe) 281
 - QGATE (punte VM/MVS) 281
 - QLPAUTO (instalare automată de program cu licență) 281
 - QLPINSTALL (instalare program cu licență) 281
 - QMSF (cadru de lucru server de mail) 281
 - QNFSANON (profil utilizator NFS) 281
 - QPGMR (programator) 281
 - QRJE (intrare job la distanță) 281
 - QSECOFR (responsabil cu securitatea) 281
 - QSNADS (servicii de distribuție Arhitectură rețea de sisteme) 281
 - QSPL (spool) 281
 - QSPLJOB (job spool) 281
 - QSRV (serviciu) 281
 - QSRVBAS (serviciu elementar) 281
 - QSYS (sistem) 281
 - QSYSOPR (operator sistem) 281
 - QTCP (TCP/IP) 281
 - QTMLPD (suport tipărire TCP/IP) 281
 - QTSTRQS (cerere test) 281

- profil utilizator livrat de IBM (*continuare*)
 QUSER (utilizator stație de lucru) 281
 responsabil cu securitatea
 (QSECOFR) 281
 scop 108
 servicii de distribuție SNA
 (QSNADS) 281
 serviciu (QSRV) 281
 serviciu elementar (QSRVBAS) 281
 sistem (QSYS) 281
 spool (QSPL) 281
 suport tipărire TCP/IP (QTMLPD) 281
 TCP/IP (QTCP) 281
 utilizator stație de lucru (QUSER) 281
- profil utilizator operator sistem
 (QSYSOPR) 281
- profil utilizator pentru utilizator stație de lucru
 (QUSER) 281
- profil utilizator programator (QPGMR)
 valori implicite 281
- profil utilizator punte VM/MVS
 (QGATE) 281
- profil utilizator QADSM (ADSM) 281
- profil utilizator QAFDFTUSR
 (AFDFTUSR) 281
- profil utilizator QAFOWN (AFOWN) 281
- profil utilizator QAFUSR (AFUSR) 281
- profil utilizator QAUTPROF (profil
 autorizare) 281
- profil utilizator QBRMS (BRM) 281
- profil utilizator QDBSHRDO (partajare bază
 de date) 281
- profil utilizator QDCEADM
 (DCEADM) 281
- Profil utilizator QDFTOWN (default owner -
 deținător implicit)
 restaurare de programe 225
- profil utilizator QDFTOWN (proprietar
 implicit)
 descriere 124
 intrare jurnal auditare (QAUDJRN) 244
 valori implicite 281
- profil utilizator QDOC (document) 281
- profil utilizator QDSNX (executiv nod sisteme
 distribuite) 281
- profil utilizator QFNC (finanțe) 281
- profil utilizator QGATE (punte
 VM/MVS) 281
- profil utilizator QLPAUTO (instalare automată
 a programului licențiat)
 restaurarea 222
- profil utilizator QLPAUTO (instalare automată
 de program cu licență)
 valori implicite 281
- profil utilizator QLPINSTALL (instalare a
 programului licențiat)
 restaurarea 222
- profil utilizator QLPINSTALL (instalare
 program cu licență)
 valori implicite 281
- profil utilizator QMSF (cadru de lucru server
 de mail) 281
- profil utilizator QPGMR (programator)
 parolă setată de comanda
 CFGSYSSEC 627
 valori implicite 281
- profil utilizator QRJE (intrare job la
 distanță) 281
- profil utilizator QSECOFR (responsabil cu
 securitatea)
Vedeți și responsabil cu securitatea
 activare 62
 stare dezactivată 62
 valori implicite 281
- profil utilizator QSECOFR (responsabil de
 securitate)
 restaurarea 222
- profil utilizator QSNADS (servicii de
 distribuție Arhitectură rețea de
 sisteme) 281
- profil utilizator QSPL (spool) 281
- profil utilizator QSPLJOB (job spool) 281
- profil utilizator QSRV (serviciu)
 parolă setată de comanda
 CFGSYSSEC 627
 valori implicite 281
- profil utilizator QSRVBAS (serviciu de bază)
 parolă setată de comanda
 CFGSYSSEC 627
- profil utilizator QSRVBAS (serviciu
 elementar)
 valori implicite 281
- profil utilizator QSYS (sistem)
 restaurarea 222
 valori implicite 281
- profil utilizator QSYSOPR (operator
 sistem) 281
 parolă setată de comanda
 CFGSYSSEC 627
- profil utilizator QTCP (TCP/IP) 281
- profil utilizator QTMLPD (suport tipărire
 TCP/IP) 281
- profil utilizator QTSTRQS (cerere test) 281
- profil utilizator QUSER (utilizator stație de
 lucru) 281
- profil utilizator QUSER (utilizator)
 parolă setată de comanda
 CFGSYSSEC 627
- profil utilizator responsabil cu securitatea
 (QSECOFR)
 activare 62
 restaurarea 222
 stare dezactivată 62
 valori implicite 281
- profil utilizator servicii distribuție SNA
 (QSNADS) 281
- profil utilizator serviciu (QSRV)
 valori implicite 281
- profil utilizator serviciu elementar
 (QSRVBAS) 281
 valori implicite 281
- profil utilizator sistem (QSYS)
 restaurarea 222
 valori implicite 281
- profil utilizator spool (QSPL) 281
- profil utilizator suport tipărire TCP/IP
 (QTMLPD) 281
- profil utilizator TCP/IP (QTCP) 281
- profilului utilizator
 autorizare
 stocare 221
- profilului utilizator (*continuare*)
 GRPPRF (profil grup)
 modificare la restaurare a
 profilului 221
 modificare la restaurare 221
 profil grup (GRPPRF)
 modificare la restaurare a
 profilului 221
 restaurarea
 comenzi 219
 proceduri 221
 stocare
 autorizare 220, 221
- profiluri mari
 planificare aplicații 200
- profiluri utilizator livrat de IBM
 autorizate 289, 297
- program
 afișare
 autorizare adoptată 130
 autorizare adoptată
 afișare 130
 auditare 232
 creare 130
 ignorare 131
 intrare jurnal auditare
 (QAUDJRN) 248
 restaurarea 225
 scop 128
 transferare 128, 129
 creare
 autorizare adoptată 130
 declanșator
 listare totală 277
 eșuare de program
 intrare jurnal auditare
 (QAUDJRN) 248
 funcție de adoptare a autorizării
 auditare 268
 gestionare profiluri utilizator 107
 ieșire validare parolă
 exemplu 46
 ignorare
 autorizare adoptată 131
 legat
 autorizare adoptată 130
 neautorizat 233
 necesități ale autorizării obiect pentru
 comenzi 412
 prevenire
 neautorizat 233
 restaurare
 valoare de validare 15
 restaurarea
 autorizare adoptată 225
 riscuri 225
 schimbare
 specificarea parametrului
 USEADPAUT 131
 service
 autorizare adoptată 130
 transferare
 autorizare adoptată 128, 129
 traducere 15
 validare parolă
 cerințe 45
 exemplu 46

- program (*continuare*)
 - validare parolă (*continuare*)
 - valoarea de sistem QPWDVLDPGM 44
 - program aprobare, parolă 45, 46
 - Program Attn asistent operațional
 - Program de tratare tastă Attn 86
 - program cu licență
 - autorizație obiect cerută pentru comenzi 387
 - program de declanșare
 - listare totală 277
 - program de tratare a mesajului de întrerupere
 - autorizare adoptată 129
 - Program de tratare tastă Attn
 - *ASSIST 86
 - modificare 86
 - procesor de comenzi QCMD 86
 - profil utilizator 86
 - program inițial 86
 - program QEZMAIN 86
 - setare 86
 - valoarea de sistem QATNPGM 86
 - program legat
 - autorizare adoptată 130
 - definiție 130
 - program licențiat
 - profil utilizator instalare (QLPINSTALL)
 - valori implicite 281
 - profil utilizator instalare automată (QLPAUTO)
 - descriere 281
 - Program QCL 117
 - program QEZMAIN 86
 - program service
 - autorizare adoptată 130
 - program sistem
 - apelare directă 13
 - program validare, parolă 45, 46
 - programator
 - aplicație
 - planificare securitate 215
 - auditare acces pentru bibliotecii de producție 231
 - sistem
 - planificare securitate 216
 - programator (QPGMR) profil utilizator
 - proprietar descriere de dispozitiv 179
 - programe care adoptă
 - afișare 268
 - Programe CLP38 117
 - programe declanșatoare
 - listare toate 621
 - programe licențiate
 - restaurarea
 - recomandări 225
 - riscuri de securitate 225
 - Programul tratare-tastă-atenție
 - inițiere job 176
 - proiectare
 - bibliotecii 199
 - securitate 195
 - proiectare aplicație
 - autorizare adoptată 203, 206
 - bibliotecii 199
 - ignorare autorizare adoptată 205
 - liste de bibliotecii 201
 - proiectare aplicație (*continuare*)
 - meniuri 203
 - profiluri 200
 - recomandări generale de securitate 196
 - proprietar
 - Vedeți și* obiect ownership
 - Vedeți și* ownership
 - parametrul profil utilizator OWNER
 - descriere 122
 - protecție
 - hardware îmbunătățită a spațiului de stocare 14
 - protecție hardware îmbunătățită a spațiului de stocare
 - intrare jurnal auditare (QAUDJRN) 244
 - nivel de securitate 40 14
 - protejare
 - mediu copie de rezervă 230
 - PRTACTRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTCPTRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTDSKINF
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTERRLOG
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTINTDTA
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTJOBTRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTJOBTRC
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTLCKRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTPOLRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTRSCRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTSYSRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTTNSRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PRTTRCRPT
 - profiluri utilizator livrat de IBM autorizate 293
 - PTF (corecție temporară program)
 - autorizație obiect cerută pentru comenzi 424
 - puncte de ieșire
 - profil utilizator 107
 - punere în buffer
 - tastatură 76
 - tastă Attn 76
 - punere în buffer *TYPEAHEAD (tastare înainte) 76
 - punere în buffer tastare înainte (*TYPEAHEAD) 76
 - punere în buffer tastatură
 - parametru profil utilizator KBDBUF 76
 - valoarea de sistem QKBDBUF 76
 - punere în buffer tastă Attn (ATTN) 76
- ## Q
- QASYPOJE (ieșire imprimantă) 574
 - QAUTOVRT valoare sistem (configurare dispozitiv-virtual automată)
 - valoarea setată de comanda CFGSYSSEC 625
 - QLMTSECOFR (responsabil cu securitatea limită) valoare de sistem
 - autorizare pentru descrierile de dispozitiv 177
 - QPGMR (programator) profil utilizator
 - proprietar descriere de dispozitiv 179
 - QPWDLVL
 - Niveluri parole (lungime maximă) 41
 - Niveluri parole (lungime minimă) 41
 - Niveluri parole (QPWDLVL) 41, 42
 - parole sensibile la majuscule 44, 60
 - QPWDLVL (sensibil la majuscule)
 - Niveluri parole (sensibil la majuscule) 43
 - parole sensibile la majuscule
 - QPWDLVL sensibil la majuscule 43
 - QPWDLVL (valoarea curentă sau în așteptare) și nume program 44
 - QSECOFR (responsabil cu securitatea) profil utilizator
 - autorizare pentru consolă 179
 - proprietar descriere de dispozitiv 179
 - QsrRestore
 - auditare obiect 448
 - QSRSTO (Restaurare Obiect) API
 - auditare obiect 448
 - QsrSave
 - auditare obiect 447
 - QSRSAVO
 - auditare obiect 447
 - QSRV (service) profil utilizator
 - autorizare pentru consolă 179
 - QSRVBAS (service de bază) profil utilizator
 - autorizare pentru consolă 179
 - QSYSLIBL (lista de bibliotecii sistem) valoare de sistem 183
 - QSYSOPR (operator sistem) coada de mesaje restrângere 182
 - Query Management/400
 - autorizație obiect cerută pentru comenzi 416
 - QVFYOBJRST (Verify Object Restore - Verificare restaurare obiecte)
 - valoarea de sistem 3
- ## R
- receptor
 - detașare 258, 260
 - modificare 260
 - salvare 260
 - ștergere 260

- receptor jurnal
 - autorizație obiect cerută pentru comenzi 376
 - detașare 258, 260
 - gestionare 258
 - modificare 260
 - spațiu de stocare maxim (MAXSTG) 77
 - spațiu de stocare necesar 77
 - ștergere 260
- receptor jurnal, audit
 - creare 256
 - numire 257
 - prag al spațiului de stocare 258
 - salvare 260
- reclamarea
 - spațiu de stocare 227
- recomandare
 - afișare informații de semnare (DSPSGNINF) 74
 - autorizare adoptată 131
 - autorizare publică
 - profiluri utilizator 93
 - autorizare specială (SPCAUT) 71
 - clasă utilizator (USRCLS) 63
 - coadă de mesaje 84
 - comanda RSTLICPGM (Restore Licensed Program - Restaurare program licențiat) 225
 - descrierii de job 79
 - interval de expirare parolă (PWDEXPITV) 74
 - limitare
 - sesiuni dispozitiv 75
 - limitare capabilități (LMTCPB) 67
 - lista de biblioteci
 - biblioteca curentă 185
 - porțiune bibliotecă produs 185
 - porțiune utilizator 185
 - listă de biblioteci inițială 79
 - mediu special (SPCENV) 72
 - menu inițial (INLMNU) 67
 - numire
 - profil de grup 59
 - profiluri utilizator 59
 - parametru limită de prioritate (PTYLMT) 78
 - parole 61
 - program inițial (INLPGM) 67
 - proiectare aplicație 200
 - proiectare bibliotecă 199
 - proiectare securitate 196
 - setare parolă la expirare (PWDEXP) 62
 - sumar 196
 - valoare de sistem QUSRLIBL 79
 - valoarea de sistem QSECURITY (nivel de securitate) 9
- recomandări
 - lista de biblioteci
 - porțiune sistem 184
- recuperare
 - jurnal auditare deteriorat 258
- recuperare cale de acces
 - auditare acțiune 450
 - autorizație obiect cerută pentru comenzi 310
- recuperarea
 - autorizare privată 219
- recuperarea (*continuare*)
 - autorizare publică 219
 - deținător de autorizare 219
 - drept de proprietate obiect 219
 - informații de securitate 219
 - listă de autorizare 219
 - listă de autorizare deteriorată 226
 - profiluri utilizator 219
- redenumire
 - obiect
 - intrare jurnal auditare (QAUDJRN) 243
 - profil utilizator 106
- refuzare
 - acces
 - cerere DDM (DDM) 190
 - acces iSeries Access 189
 - prezentare job la distanță 189
- resetare
 - parolă DST (dedicated service tools - unelte dedicate de service)
 - intrare jurnal auditare (QAUDJRN) 245
- responsabil cu securitatea
 - Vedeți și* profil utilizator QSECOFR (security officer - responsabil cu securitatea)
 - limitare acces stație de lucru 25
 - monitorizare acțiuni 270
 - restricționare la anumite stații de lucru 230
- responsabil cu securitatea (QSECOFR) profil utilizator
 - autorizare pentru consolă 179
 - proprietar descriere de dispozitiv 179
- restaurare
 - autorizare
 - descriere comandă 275
 - intrare jurnal auditare (QAUDJRN) 245
 - autorizare modificată de sistem
 - intrare jurnal auditare (QAUDJRN) 244
 - descriere de job
 - intrare jurnal auditare (QAUDJRN) 244
 - disponere fișier cu obiectul *CRQD care adoptă autorizare (RQ) 582
 - eșuare de program
 - intrare jurnal auditare (QAUDJRN) 244
 - modificare drept de proprietate
 - intrare jurnal auditare (QAUDJRN) 244
 - obiect
 - intrare jurnal auditare (QAUDJRN) 244
 - obiect*CRQD
 - intrare jurnal auditare (QAUDJRN) 244
 - profil utilizator
 - descriere comandă 275
 - intrare jurnal auditare (QAUDJRN) 245
 - proprietar QDFTOWN (implicit)
 - intrare jurnal auditare (QAUDJRN) 244
- restaurare (*continuare*)
 - restricționare 191
 - riscuri de securitate 191
 - spațiu de stocare maxim (MAXSTG) 77
 - spațiu de stocare necesar 77
 - validare program 15
- restaurarea
 - autorizare
 - descrierea procesului 224
 - privire generală asupra comenzilor 219
 - procedură 223
 - autorizare adoptată
 - modificări ale dreptului de proprietate și ale autorizării 225
 - autorizare privată 219, 223
 - autorizare publică 219, 223
 - autorizare specială *ALLOBJ (toate obiectele)
 - autorizare specială (*ALLOBJ) toate obiectele 222
 - bibliotecă 219
 - deținător de autorizare 219
 - gid (group identification number - număr de identificare utilizator) 222
 - grup primar 219, 222
 - informațiilor de securitate 219
 - listă de autorizare
 - asociere cu obiectul 223
 - descrierea procesului 226
 - privire generală asupra comenzilor 219
 - obiect
 - comenzi 219
 - drept de proprietate 219, 222
 - probleme de securitate 222
 - obiect bibliotecă document (DLO) 219
 - parametrul ALWOBJDIF (allow object differences - permisiune a diferențelor dintre obiecte) 222, 223
 - profilului utilizator
 - proceduri 219, 221
 - programe 225
 - programe licențiate
 - recomandări 225
 - riscuri de securitate 225
 - sistem de operare 227
 - uid (user identification number - număr de identificare utilizator) 222
- restrângere
 - QSYSOPR (operator sistem) coada de mesaje 182
- restricționare
 - acces
 - consolă 230
 - stații de lucru 230
 - capabilități 66
 - caractere din parole 42
 - caractere repetate din parole 43
 - comenzi (ALWLTUSR) 67
 - digiți consecutivi în parole (valoare de sistem QPWDLMTAJC) 43
 - digiți alăturați în parole (valoare de sistem QPWDLMTAJC) 43
 - folosire linie de comandă 66
 - mesaje 17
 - operații de restaurare 191

restricționare (*continuate*)
 operații de salvare 191
 variabilă de sistem responsabil cu
 securitatea (QLMTSECOFR) 230
 resursă
 autorizație obiect cerută pentru
 comenzi 419
 resurse de sistem
 limitare folosire
 parametru limită de prioritate
 (PTYLMT) 77
 resurse sistem
 împiedicare abuz 192
 rețea
 delogare
 intrare jurnal auditare
 (QAUDJRN) 242
 înregistrare în istoric
 intrare jurnal auditare
 (QAUDJRN) 242
 parolă
 intrare jurnal auditare
 (QAUDJRN) 241
 revocare
 autorizare obiect 272
 autorizare publică 278
 autorizație publică 625
 permisiune utilizator 275
 risc
 autorizare adoptată 131
 autorizare specială *ALLOBJ (toate
 obiectele) 68
 autorizare specială *AUDIT (auditare) 71
 autorizare specială *IOSYSCFG
 (configurare sistem) 71
 autorizare specială *JOBCTL (control de
 job) 69
 autorizare specială *SAVSYS (salvare
 sistem) 70
 autorizare specială *SERVICE
 (service) 70
 autorizare specială *SPLCTL (control de
 spool) 69
 autorizări speciale 68
 comanda RSTLICPGM (Restore Licensed
 Program - Restaurare program
 licențiat) 225
 comenzi de restaurare 191
 comenzi salvare 191
 deținător de autorizare 133
 lista de biblioteci 183
 parametrul create authority
 (CRTAUT) 119
 program validare parolă 45
 restaurarea programelor care adoptă
 autorizare 225
 restaurarea programelor cu instrucțiuni
 restricționate 225
 RJE (intrare job la distanță)
 autorizație obiect cerută pentru
 comenzi 419
 RMVCLUNODE
 profiluri utilizator livrat de IBM
 autorizate 294
 RMVCRGDEVE
 profiluri utilizator livrat de IBM
 autorizate 294

RMVCRGNODE
 profiluri utilizator livrat de IBM
 autorizate 294
 RMVDEVDMNE
 profiluri utilizator livrat de IBM
 autorizate 294
 RMVFNTTBLE (Remove DBCS Font Table
 Entry - Înlăturare tabelă fonturi DBCS)
 necesități ale autorizării obiect pentru
 comenzi 311
 RMVIMGCLGE
 profiluri utilizator livrat de IBM
 autorizate 294
 RMVMFMS (Înlăturare sistem de fișiere montat)
 autorizarea obiect necesară 439
 RMVTRCFTR
 profiluri utilizator livrat de IBM
 autorizate 294
 RSTSYSINF
 autorizarea obiect necesară 306

S

salvare
 auditare receptor jurnal 260
 date de securitate 275
 restricționare 191
 riscuri de securitate 191
 sistem 275
 salvare de rezervă
 necesități ale autorizării obiect pentru
 comenzi 400
 salvarea
 auditare 228
 autorizare privată 219
 autorizare publică 219
 bibliotecă 219
 date de securitate 219
 deținător de autorizare 219
 drept de proprietate obiect 219
 grup primar 219
 informațiilor de securitate 219
 listă de autorizare 219
 obiect 219
 obiect bibliotecă document (DLO) 219
 profil utilizator
 comenzi 219
 sistem 219
 save system (*SAVSYS) special authority
 *OBJEXIST authority 112
 SAVRSTCHG
 profiluri utilizator livrat de IBM
 autorizate 295
 SAVRSTLIB
 profiluri utilizator livrat de IBM
 autorizate 295
 SAVRSTOBJ
 profiluri utilizator livrat de IBM
 autorizate 295
 SAVSYSINF
 autorizarea obiect necesară 308
 scanare
 alterări obiect 274
 alternări obiect 233, 269
 schimbare
 autorizare
 proceduri 138
 schimbare (*continuate*)
 autorizare adoptată
 autorizare cerută 130
 autorizare utilizator
 listă de autorizare 145
 grup primar 123
 job
 autorizare adoptată 130
 listă de autorizare
 autorizare utilizator 145
 program
 specificarea parametrului
 USEADPAUT 131
 proprietar obiect 142
 scriitor
 autorizare specială *JOBCTL (control de
 job) 69
 necesități ale autorizării obiect pentru
 comenzi 443
 scriitor imprimantă
 autorizație obiect cerută pentru
 comenzi 443
 securitate
 cheie IPL 2
 coadă de ieșire 186
 Common Criteria
 descriere 6
 de ce e necesară 1
 descriere de job 182
 descrierea de subsistem 181
 fișier spool 186
 fișiere critice 209
 fișiere sursă 216
 fizică 2
 ieșire imprimantă 186
 lista de biblioteci 183
 obiectiv
 confidențialitate 1
 disponibilitate 1
 integritate 1
 planificare 1
 pornire
 job batch 176
 job interactiv 175
 joburi 175
 proiectare 195
 recomandări generale 196
 unelte 277
 valori de sistem 3
 securitate cheie IPL 2
 Securitate Common Criterii (Criterii comune)
 descriere 6
 securitate de resurse
 introducere 4
 securitate fișier
 SQL 212
 securitate fizică 2
 auditare 230
 planificare 230
 securitate la nivel de câmp 209
 securitate la nivel de semnare 209
 securitate resursă
 definiție 111
 limitare acces 217
 seconvență de sortare
 pondere partajată 87
 pondere unică 87

- secvență de sortare (*continuare*)
 - profil utilizator 87
 - valoare de sistem QSRTSEQ 87
 - semnare
 - acțiune când este depășit numărul maxim de încercări de semnare (valoarea de sistem QMAXSGNACN) 26
 - autorizare stație de lucru necesară 177
 - autorizări necesare 175
 - consolă 179
 - eșecuri autorizare 175
 - eșuare responsabil cu securitatea 177
 - eșuare utilizator cu autorizarea specială *ALLOBJ 177
 - eșuare utilizator cu autorizarea specială *SERVICE 177
 - eșuare utilizator service 177
 - fără ID utilizator 181
 - fără ID utilizator și fără parolă 14
 - integritate 3
 - la distanță (valoarea de sistem QRMTSIGN) 27
 - limitare încercări 25
 - obiect 3
 - restricționare responsabil cu securitatea 177
 - verificare securitate 175
 - semnare la distanță
 - valoarea de sistem QRMTSIGN 27
 - semnare obiect 3
 - semnare sistem 3
 - server de directoare
 - auditare 461
 - Server de rețea
 - autorizație obiect cerută pentru comenzi 397
 - server gazdă
 - autorizație obiect cerută pentru comenzi 346
 - service
 - necesități ale autorizării obiect pentru comenzi 424
 - service (QSRV) profil utilizator
 - autorizare pentru consolă 179
 - service de bază (QSRVBAS) profil utilizator
 - autorizare pentru consolă 179
 - servicii distribuție arhitectură rețea de sisteme (SNADS)
 - profil utilizator QSNADS 281
 - servicii mail
 - auditare acțiune 479
 - servicii office
 - auditare acțiune 479
 - sesiune
 - necesități ale autorizării obiect pentru comenzi 419
 - sesiune dispozitiv
 - limitare
 - parametru profil utilizator LMTDEVSSN 75
 - valoarea de sistem QLMTDEVSSN 25
 - sesiune server
 - intrare jurnal auditare (QAUDJRN) 242
 - set de caractere pe doi octeți (DBCS)
 - autorizație obiect cerută pentru comenzi 335
 - set de simboluri grafice
 - autorizație obiect cerută pentru comenzi 345
 - setare
 - atribute rețea 278, 625
 - funcție de auditare 256
 - program de tratare tastă Attn (ATNPGM) 86
 - valori securitate 625
 - valori sistem 278, 625
 - SETVTMAP Comanda (Afișare hartă tastatură VT100)
 - autorizări obiect necesare 438
 - sferă de control
 - autorizație obiect cerută pentru comenzi 429
 - sistem
 - necesități ale autorizării obiect pentru comenzi 433
 - salvare 275
 - salvarea 219
 - sistem de fișiere integrat
 - autorizație obiect cerută pentru comenzi 347
 - sistem de operare
 - instalare de securitate 227
 - SNADS (servicii de distribuție Arhitectură rețea de sisteme)
 - profil utilizator QSNADS 281
 - socket
 - înaintare
 - intrare jurnal auditare (QAUDJRN) 248
 - socket-uri
 - necesități ale autorizării obiect pentru comenzi 312
 - Socket-uri AF_INET peste SNA
 - autorizație obiect cerută pentru comenzi 312
 - spațiu de stocare
 - parametru maxim (MAXSTG) 76
 - prag
 - receptor jurnal auditare (QAUDJRN) 258
 - pretindere 17, 124
 - setare valoare de sistem QALWUSRDMN (permitere obiecte utilizator) 22
 - profil utilizator 76
 - protecție hardware îmbunătățită 14
 - reclamarea 227
 - special authority
 - *SAVSYS (save system)
 - *OBJEXIST authority 112
 - autorizare adoptată 128
 - Speciale, autorizări 214
 - SQL
 - securitate fișier 212
 - SRC (cod referință sistem)
 - B900 3D10 (auditare eroare) 51
 - stare
 - program 13
 - stare sistem
 - gestiune 192
 - starea *SYSTEM (sistem) 13
 - starea *USER (utilizator) 13
 - starea program
 - afișare 13
 - definiție 13
 - starea sistem (*SYSTEM) 13
 - starea utilizator (*USER) 13
 - stație de lucru
 - acces responsabil cu securitatea 25
 - autorizare de semnare 177
 - limitare utilizator la una singură la un moment dat 25
 - restricționare acces 230
 - securizare 177
 - STRASPBAL
 - profiluri utilizator livrat de IBM autorizate 295
 - STRCHTSVR (Start Clustered Hash Table Server - Pornire server tabelă hash din cluster)
 - profiluri utilizator livrat de IBM autorizate 295
 - STRCLUNOD
 - profiluri utilizator livrat de IBM autorizate 295
 - STRCRG
 - profiluri utilizator livrat de IBM autorizate 295
 - STRHOSTSVR
 - profiluri utilizator livrat de IBM autorizate 295
 - STROBJCVN
 - profiluri utilizator livrat de IBM autorizate 296
 - STRPFRG
 - profiluri utilizator livrat de IBM autorizate 296
 - STRPFRT
 - profiluri utilizator livrat de IBM autorizate 296
 - subset
 - autorizare 113
 - subsistem
 - Vedeți și descriere subsistem autorizare specială *JOBCTL (control de job) 69*
 - autorizație obiect cerută pentru comenzi 431
 - semnarea fără ID utilizator și fără parolă 14
 - System/36
 - autorizarea pentru fișiere șterse 131
 - migrare
 - deținători de autorizare 132
 - System/38
 - securitate comandă 209
- ## Ș
- șir comenzi
 - disponere fișier jurnal auditare (QAUDJRN) 522
 - ștergere
 - auditare receptor jurnal 260
 - autorizare utilizator 140
 - autorizarea pentru un utilizator 140
 - deținător de autorizare 132, 271
 - listă de autorizare 146
 - listă de autorizații 271

ștergere (*continuare*)
 obiect
 intrare jurnal auditare (QAUDJRN) 241
 profil proprietar obiect 122
 profil utilizator
 coadă de mesaje 101
 descriere comandă 274
 fișiere spool 103
 grup primar 101
 intrare director 101
 liste de distribuție 101
 obiecte deținute 101
 Ștergere liste de validare (DLTVLDDL) 216
 ștergere obiect
 auditare obiect 448

T

tabel de control formulare
 autorizație obiect cerută pentru comenzi 419
 Tabel WRKSRVTBLE (Gestionare intrări tabel servicii)
 autorizarea obiect necesară 438
 tabelă
 necesități ale autorizării obiect pentru comenzi 436
 tabelă alertă
 autorizație obiect cerută pentru comenzi 312
 tabelă autorizare 221
 tasta Atenție (ATTN)
 autorizare adoptată 129
 tastă pagină în jos
 întoarcere (*ROLLKEY opțiune utilizator) 90
 tastă pagină în sus
 întoarcere (*ROLLKEY opțiune utilizator) 90
 TCP/IP (Transmission Control Protocol/Internet Protocol)
 autorizație obiect cerută pentru comenzi 436
 terminare
 auditare 50
 job deconectat 33, 34
 job inactiv 23
 tip autorizare de grup
 parametru profil utilizator GRPAUTYP 81
 tip de intrare CA (modificare autorizare) 247
 tip de intrare jurnal (CQ) modificare obiect *CRQD 245
 tip de intrare jurnal (RQ) resturare obiect *CRQD 244
 tip de intrare jurnal (SE) modificare a intrării de rutare subsistem 249
 tip de intrare jurnal (VA) modificare a listei de acces control 249
 tip de intrare jurnal (VL) cont limită depășit 251
 tip de intrare jurnal acțiuni poștă (ML) 243
 tip de intrare jurnal AD (auditare modificare) 247
 tip de intrare jurnal adoptare program (PA) 248

tip de intrare jurnal AF (eșuare autorizare) descriere 240, 244
 tip de intrare jurnal AP (autorizare adoptată) 244
 tip de intrare jurnal comunicații interproces (IP) 240
 tip de intrare jurnal CP (modificare profil utilizator) 245
 tip de intrare jurnal CQ (modificare obiect *CRQD) 245
 tip de intrare jurnal creare obiect (CO) 241
 tip de intrare jurnal DS (resetare parolă DST) 245
 tip de intrare jurnal eroare parolă rețea (VP) 241
 tip de intrare jurnal eșuare autorizare (AF) 240
 descriere 244
 tip de intrare jurnal gestionare obiect (OM) 243
 tip de intrare jurnal GS (înantare descriptor) 248
 tip de intrare jurnal ieșire imprimantă (PO) 244
 tip de intrare jurnal IP (comunicații interproces) 240
 tip de intrare jurnal IP (modificare drept de proprietate) 248
 tip de intrare jurnal înaintare descriptor (GS) 248
 tip de intrare jurnal JD (modificare descriere de job) 248
 tip de intrare jurnal JS (modificare job) 241
 tip de intrare jurnal logare sau delogare la rețea (VN) 242
 tip de intrare jurnal modificare a variabilei de sistem (SV) 249
 tip de intrare jurnal modificare atribut de rețea (NA) 248
 tip de intrare jurnal modificare auditare (AD) 247
 tip de intrare jurnal modificare autorizare (CA) 247
 tip de intrare jurnal modificare autorizare pentru obiect restaurat (RA) 244
 tip de intrare jurnal modificare autorizare pentru obiect restaurat (RO) 244
 tip de intrare jurnal modificare descriere de job (JD) 248
 tip de intrare jurnal modificare director de distribuire a sistemului (SD) 243
 tip de intrare jurnal modificare drept de proprietate (IP) 248
 tip de intrare jurnal modificare drept de proprietate (OW) 248
 tip de intrare jurnal modificare gestiune sisteme (SM) 250
 tip de intrare jurnal modificare grup primar (PG) 248
 tip de intrare jurnal modificare grup primar pentru obiect restaurat (RZ) 245
 tip de intrare jurnal modificare job (JS) 241
 tip de intrare jurnal modificare profil rețea (VU) 249
 tip de intrare jurnal modificare profil utilizator (CP) 245

tip de intrare jurnal modificare stare serviciu (VV) 250
 tip de intrare jurnal NA (modificare atribut de rețea) 248
 tip de intrare jurnal OM (gestionare obiect) 243
 tip de intrare jurnal OR (restaurare obiect) 244
 tip de intrare jurnal OW (modificare drept de proprietate) 248
 tip de intrare jurnal PA (adoptare program) 248
 tip de intrare jurnal parolă (PW) 240
 tip de intrare jurnal PG (modificare grup primar) 248
 tip de intrare jurnal PO (ieșire imprimantă) 244
 tip de intrare jurnal profil swap (PS) 248
 tip de intrare jurnal PS (profil swap) 248
 tip de intrare jurnal PW (parolă) 240
 tip de intrare jurnal RA (modificare autorizare pentru obiect restaurat) 244
 tip de intrare jurnal resetare parolă DST (DS) 245
 tip de intrare jurnal restaurare autorizare pentru profil utilizator (RU) 245
 tip de intrare jurnal restaurare de programe care adoptată autorizarea (RP) 244
 tip de intrare jurnal restaurare descriere de job (RJ) 244
 tip de intrare jurnal restaurare obiect (OR) 244
 tip de intrare jurnal RJ (restaurare descriere de job) 244
 tip de intrare jurnal RO (modificare drept de proprietate pentru obiect restaurat) 244
 tip de intrare jurnal RP (restaurare de programe care adoptată autorizarea) 244
 tip de intrare jurnal RQ (resturare obiect *CRQD) 244
 tip de intrare jurnal RU (restaurare autorizare pentru profil utilizator) 245
 tip de intrare jurnal RZ (modificare grup primar pentru obiect restaurat) 245
 tip de intrare jurnal SD (modificare director de distribuire a sistemului) 243
 tip de intrare jurnal SE (modificare a intrării de rutare subsistem) 249
 tip de intrare jurnal SF (modificare la fișierul spool) 250
 tip de intrare jurnal SM (modificare gestiune sisteme) 250
 tip de intrare jurnal ST (acțiune unelte service) 250
 tip de intrare jurnal SV (acțiune pentru variabila de sistem) 249
 tip de intrare jurnal șir comandă (CD) 241
 tip de intrare jurnal VA (modificare a listei de acces control) 249
 tip de intrare jurnal VL (cont limită depășit) 251
 tip de intrare jurnal VN (logare sau delogare la rețea) 242
 tip de intrare jurnal VP (eroare parolă rețea) 241
 tip de intrare jurnal VU (modificare profil de rețea) 249

tip de intrare jurnal VV (modificare stare serviciu) 250

Tip intrare jurnal AF (authority failure - eșuare autorizare)

- instrucțiune restricționată 15
- interfață nesuportată 13, 15
- validare program 15
- violare descriere de job 14
- violare protecție hardware 14
- violare semnare implicită 14

tip intrare jurnal CD (șir comandă) 241

tip intrare jurnal CO (creare obiect) 123, 241

tip intrare jurnal creare obiect (CO) 123

tip intrare jurnal DO (ștergere operație) 241

tip intrare jurnal ML (acțiuni poștă) 243

tip intrare jurnal pornire sau oprire conexiune (VC) 242

tip intrare jurnal sesiune server (VS) 242

tip intrare jurnal VC (pornire sau oprire conexiune) 242

tip intrare jurnal VS (sesiune server) 242

tipărire

- Vedeți și* ieșire imprimantă
- atribut rețea 621
- atribute rețea 278
- comunicații 278
- deținător de autorizare 277
- informații listă de autorizații 621
- informații obiecte adoptate 621
- intrare jurnal auditare (QAUDJRN) 244
- intrări jurnal de auditare 621
- listare de obiecte non-IBM 621
- listă de descrieri de subsistem 277
- listă de obiecte non-IBM 277
- notificare (*PRTMSG opțiune utilizator) 90
- obiecte autorizate pentru publicare 623
- parametri coadă de ieșire importanți pentru securitate 277
- parametri coadă de job importanți pentru securitate 277
- parametrii coadă de ieșire relevanți de securitate 623
- parametrii coadă de job relevanți de securitate 623
- programe de declanșare 277
- programe declanșatoare 621
- securitate 186
- setări de comunicație relevante de securitate 621
- trimitere mesaj (*PRTMSG opțiune utilizator) 90
- valori de sistem 230
- valori descriere subsistem relevante de securitate 621
- valori sistem 278, 621

Tipărire programe declaratoare (PRTRGPGM)

- descriere 621

token-ring

- autorizație obiect cerută pentru comenzi 389

transfer fișier

- securizare 190

transferare

- autorizare adoptată 129
- la job grup 129

translatore programe 15

Transmission Control Protocol/Internet Protocol (TCP/IP)

- autorizație obiect cerută pentru comenzi 436

TRCASPBAL

- profiluri utilizator livrat de IBM autorizate 296

TRCTCPAPP

- profiluri utilizator livrat de IBM autorizate 296

trimitere

- fișier spool de rețea 186
- intrare jurnal 258

U

uid (user identification number - număr de identificare utilizator)

- restaurarea 222

Unealta GHGLIBOWN (Change Library Owner - Modificare proprietar bibliotecă) 216

unelte de securitate

- comenzi 277, 617
- conținut 277, 617
- meniuri 617

unelte de service dedicate (DST)

- modificare ID utilizator 109
- modificare parole 109
- resetare parolă
- descriere comandă 273

Unelte de service dedicate (DST) utilizatori 108

unelte dedicate de service (DST)

- auditare parole 230
- resetare parolă
- intrare jurnal auditare (QAUDJRN) 245

UNMOUNT (Înlăturare sistem de fișiere montat)

- autorizarea obiect necesară 439

update (*UPD) authority 112

utilizator

- adăugare 98
- auditare

 - gestionare 106
 - modificare 71

- înrolare 98

utilizator autorizat

- afișare 274

utilizator internet

- liste de validare 216

V

validare

- programe restaurate 15

validare program

- definiție 15

validarea parametrilor 14

valoare creare auditare obiect (CRTOBJAUD) 54

valoare CRTOBJAUD (creare auditare obiect) 54

valoare CRTOBJAUD (create object auditing - creare auditare obiect) 254

valoare de sistem

- acționează când se ating încercările de semnare (QMAXSGNACN)
- stare profil utilizator 62
- acțiune când este depășit numărul maxim de încercări de semnare (QMAXSGNACN)
- descriere 26
- acțiune oprire auditare (QAUDENDACN) 50
- afișare informații de semnare (QDPSGNINF) 22, 74
- atribut service la distanță (QRMTSRVATR) 33
- auditare 230

 - privire generală 49

- comandă pentru setare 278
- configurația automată a dispozitivelor virtuale (QAUTOVRT) 32
- consolă (QCONSOLE) 179
- control auditare (QAUDCTL)

 - privire generală 50

- control de auditare (QAUDCTL)

 - afișare 277
 - modificare 277

- control memorie de partajare (QSHRMEMCTL)

 - descriere 29
 - valori posibile 30

- Control scanare sisteme de fișiere (QSCANFSCCTL) 28
- control sisteme de fișiere

 - scanare (QSCANFCTLS) 28

- control sisteme de fișiere integrat scanare (QSCANFSCCTL) 28
- creare auditare obiect (QCRTOBJAUD) 54
- creare autorizare (QCRTAUT)

 - descriere 22
 - folosirea 118
 - risc de modificare 22

- dispozitiv de tipărire (QPRTEDEV) 85
- extensie nivel auditare (QAUDLVL2)

 - privire generală 53

- folosire autorizare adoptată (QUSEADPAUT)

 - descriere 30
 - risc de modificare 30

- identificator de limbă (QLANGID) 87
- identificator de regiune sau țară (QCNTYID) 88
- identificator set de caractere codate (QCCSID) 88
- interval de expirare parolă (QPWDEXPITV)

 - parametru profil utilizator PWDEXPITV 74

- Interval timeout job deconectat (QDSCJOBITV) 33
- job inactiv

 - coadă de mesaje (QINACTMSGQ) 24
 - interval timeout (QINACTITV) 23

valoare de sistem (<i>continua</i>)	valoare de sistem (<i>continua</i>)	valoare de sistem (<i>continua</i>)
limitare responsabil cu securitatea (QLMTSECOFR)	parolă (<i>continua</i>)	QDSPSGNINF (afișare informații de semnare) 74
modificare niveluri de securitate 11	digiți de parolă necesari (QPWDRQDDGT) 44	QDSPSGNINF (display sign-on information - afișare informații de semnare) 22
limitare sesiuni dispozitiv (QLMTDEVSSN)	duplicare (QPWDRQDDIF) 42	QFRCCVNRST (forțare conversie la restaurare) 36
parametru profil utilizator LMTDEVSSN 75	interval de expirare (QPWDEXPITV) 74	QINACTITV (inactive job time-out interval - interval timeout job inactiv) 23
limită responsabil cu securitatea (QLMTSECOFR)	interval expirare (QPWDEXPITV) 39	QINACTMSGQ (inactive job message queue - coadă de mesaje a jobului inactiv) 24
autorizare pentru descrierea de dispozitiv 177	limită alăturată (QPWDLMTAJC) 43	QKBDBUF (punere în buffer tastatură) 76
lista de biblioteci sistem (QSYSLIBL) 183	lungime maximă (QPWDMAXLEN) 41	QLANGID (identificator de limbă) 87
listare 230	lungime minimă (QPWDMINLEN) 41	QLMTDEVSSN (limit device sessions - limitare sesiuni dispozitiv) descriere 25
listă de biblioteci utilizator (QUSRLIBL) 79	privire generală 38	QLMTDEVSSN (limitare sesiuni dispozitiv) parametru profil utilizator LMTDEVSSN 75
lucru cu 230	program aprobare (QPWVLDPGM) 44	QLMTSECOFR (limit security officer - limitare responsabil cu securitatea) descriere 25
maximum încercări de semnare (QMAXSIGN)	program validare (QPWVLDPGM) 44	QLMTSECOFR (limitare responsabil cu securitatea) modificare niveluri de securitate 11
stare profil utilizator 62	restricție a digiților consecutivi (QPWDLMTAJC) 43	QLMTSECOFR (responsabil cu securitatea limită) autorizare pentru descrierile de dispozitiv 177
mediu special (QSPCENV) 72	permitere obiecte utilizator (QALWUSRDMN) 17, 21	proces de semnare 179
modificare	program de tratare tastă Attn (QATNPGM) 86	QMAXSGNACN (action when sign-on attempts reached - acțiune când este depășit numărul maxim de încercări de semnare) descriere 26
autorizare specială *SECADM (administrator de securitate) 69	punere în buffer tastatură (QKBDBUF) 76	QMAXSGNACN (acțiunează când se ating încercările de semnare) stare profil utilizator 62
nivel auditare (QAUDLVL)	restaurare obiect) 37	QMAXSIGN (maximum încercări de semnare) stare profil utilizator 62
privire generală 51	QALWUSRDMN (permitere obiecte utilizator) 17, 21	QMAXSIGN (maximum sign-on attempts - număr maxim de încercări de semnare) descriere 25
nivel de auditare (QAUDLVL)	QATNPGM (program de tratare tastă Attn) 86	QPRTDEV (dispozitiv de tipărire) 85
afișare 277	QAUDCTL (control auditare) privire generală 50	QPWDEXPITV (interval de expirare parolă) parametru profil utilizator PWDEXPITV 74
modificare 277	QAUDCTL (control de auditare) afișare 277	QPWDEXPITV (interval expirare parolă) descriere 39
profil utilizator 94	modificare 277	QPWDLMTAJC (limită alăturată parolă) 43
nivel de securitate (QSECURITY)	QAUDENDACN (acțiune oprire auditare) 50	QPWDLMTCHR (caractere limită) 42
autorizare specială 9	QAUDFRCLVL (nivel forțare auditare) 51	QPWDLMTREP (caractere repetate limită) 43
clasă utilizator 9	QAUDLVL (nivel auditare) privire generală 51	QPWDMAXLEN (lungime maximă parolă) 41
comparație a nivelurilor 7	QAUDLVL (nivel de auditare) afișare 277	QPWDMINLEN (lungime minimă parolă) 41
creare automată profil utilizator 57	modificare 277	QPDSCJOBITV (Interval timeout job deconectat) 33
dezactivare nivel 40 16	QAUDLVL2 (extensie nivel auditare) privire generală 53	
dezactivare nivel 50 18	QAUTOCFG (automatic device configuration - configurare automată dispozitiv) 31	
introducere 2	QAUTOVRT (configurația automată a dispozitivelor virtuale) 32	
modificare, 20 dintr-un nivel mai înalt 10	QCCSID (identificator set de caractere codate) 88	
modificare, la nivelul 40 15	QCNTRYID (identificator de regiune sau țară) 88	
modificare, la nivelul 50 17	QCONSOLE (consolă) 179	
modificare, nivelul 10 în nivelul 20 10	QCRTAUT (creare autorizare) descriere 22	
modificare, nivelul 20 în 30 11	folosirea 118	
nivelul 10 10	risc de modificare 22	
nivelul 20 10	QCRTOBJAUD (creare auditare obiect) 54	
nivelul 30 11	QDSCJOBITV (Interval timeout job deconectat) 33	
nivelul 40 11		
nivelul 50 16		
privire generală 7		
recomandări 9		
nivel forțare auditare (QAUDFRCLVL) 51		
nivel securitate (QSECURITY)		
impunere valoare de sistem QLMTSECOFR 179		
opțiune permitere restaurare obiect (QALWOBJRST) 37		
parolă		
caractere de poziție (QPWDPOSDIF) 44		
caractere limită (QPWDLMTCHR) 42		
caractere repetate limită (QPWDLMTREP) 43		

- valoare de sistem (*continuare*)
- QPWDRQDDGT (digiți de parolă necesari) 44
 - QPWDRQDDIF (parolă duplicată) 42
 - QPWDVLDPGM (program validare parolă) 44
 - QRETSVRSEC (retain server security - reținere securitate server) 27
 - QRMTSIGN (remote sign-on - semnare la distanță) 27
 - QRMTSRVATR (atribut service la distanță) 33
 - QSCANFS (scan file systems - scanare sisteme de fișiere) 28
 - QSCANFSCCTL (scan file systems control - control scanare sisteme de fișiere) 28
 - QSECURITY (nivel de securitate)
 - autorizare specială 9
 - clasă utilizator 9
 - comparație a nivelurilor 7
 - modificare, 20 dintr-un nivel mai înalt 10
 - modificare, nivelul 10 în nivelul 20 10
 - modificare, nivelul 20 în 30 11
 - nivelul 10 10
 - nivelul 20 10
 - nivelul 30 11
 - nivelul 40 11
 - privire generală 7
 - recomandări 9
 - QSECURITY (nivel securitate)
 - impunere valoare de sistem QLMTSECOFR 179
 - QSECURITY (security level - nivel de securitate)
 - blocuri de control interne 17
 - creare automată profil utilizator 57
 - dezactivare nivel 40 16
 - dezactivare nivel 50 18
 - introducere 2
 - modificare, la nivelul 40 15
 - modificare, la nivelul 50 17
 - nivelul 50 16
 - tratate mesaj 17
 - validarea parametrilor 14
 - QSHRMEMCTL (control memorie de partajare)
 - descriere 29
 - valori posibile 30
 - QSPCENV (mediu special) 72
 - QSRSEQ (secvență de sortare) 87
 - QSYSLIBL (lista de biblioteci sistem) 183
 - QUSEADPAUT (utilizare autorizare adoptată)
 - descriere 30
 - risc de modificare 30
 - QUSRLIBL (listă de biblioteci utilizator) 79
 - QVIFYOJBIRST (verificare obiect la restaurare) 34
 - referitor la securitate
 - privire generală 31
 - responsabil cu securitatea limită (QLMTSECOFR)
 - proces de semnare 179
- valoare de sistem (*continuare*)
- reținere securitate server (QRETSVRSEC) 27
 - Scanare sisteme de fișiere (QSCANFS) 28
 - securitate
 - introducere 3
 - privire generală 20
 - secvență de sortare (QSRSEQ) 87
 - semnare 40
 - acționează când se ating încercările (QMAXSGNACN) 62
 - acțiune când este depășit numărul de încercări de semnare (QMAXSGNACN) 26
 - încercări maxime (QMAXSIGN) 62
 - la distanță (QRMTSIGN) 27
 - număr maxim de încercări (QMAXSIGN) 25
 - semnare la distanță (QRMTSIGN) 27
 - sisteme de fișiere
 - scanare (QSCANFS) 28
 - sisteme de fișiere integrat
 - scanare (QSCANFS) 28
 - tipărire 230
 - tipărire comunicații de securitate 278
 - tipărire important pentru securitate 278
 - verificare obiect la restaurare (QVIFYOJBIRST) 34
 - valoare de sistem atribut service la distanță (QRMTSRVATR) 33
 - valoare de sistem caractere de poziție (QPWDPOSDIF) 44
 - valoare de sistem caractere limită (QPWDLMTCHR) 42
 - valoare de sistem caractere repetate (QPWDLMTREP) 43
 - valoare de sistem caractere repetate limită (QPWDLMTREP) 43
 - valoare de sistem control auditare (QAUDCTL)
 - privire generală 50
 - valoare de sistem creare auditare obiect (QCRTOJBIAUD)
 - privire generală 54
 - valoare de sistem digiți de parolă necesari (QPWDRQDDGT) 44
 - valoare de sistem extensie nivel auditare (QAUDLVL2) 53
 - valoare de sistem folosire autorizare adoptată (QUSEADPAUT)
 - descriere 30
 - risc de modificare 30
 - valoare de sistem lungime minimă a parolei (QPWDMINLEN) 41
 - valoare de sistem mediu special (QSPCENV) 72
 - valoare de sistem nivel auditare (QAUDLVL) 51
 - valoare de sistem nivel de auditare (QAUDLVL)
 - profil utilizator 94
 - valoare de sistem Nivel parolă (QPWDLVL)
 - descriere 40
 - valoare de sistem opțiune permitere restaurare obiect (QALWOBIRST) 37
- valoare de sistem parolă duplicată (QPWDRQDDIF) 42
- valoare de sistem program validare parolă (QPWDVLDPGM) 44
- valoare de sistem QALWOBIRST (opțiune permitere restaurare obiect) 37
- valoare de sistem QATNPGM (program de tratare tastă Attn) 86
- valoare de sistem QAUDCTL (control auditare)
 - privire generală 50
- valoare de sistem QAUDLVL (nivel auditare)
 - privire generală 51
- valoare de sistem QAUDLVL (nivel de auditare)
 - profil utilizator 94
- valoare de sistem QAUDLVL2 (extensie nivel auditare)
 - privire generală 53
- valoare de sistem QAUTOCFG (automatic device configuration - configurae automată dispozitiv) 31
- valoare de sistem QCCSID (identificator set de caractere codate) 88
- valoare de sistem QCNTYID (identificator de regiune sau țară) 88
- valoare de sistem QCONSOLE (consolă) 179
- valoare de sistem QCRTOJBIAUD (creare auditare obiect) 54
- valoare de sistem QDPSGNINF (afișare informații de semnare) 74
 - valoare setată de comanda CFGSYSSEC 625
- valoare de sistem QKBDBUF (punere în buffer tastatură) 76
- valoare de sistem QLANGID (identificator de limbă) 87
- valoare de sistem QLMTDEVSSN (limitare sesiuni dispozitiv)
 - parametru profil utilizator LMTDEVSSN 75
- valoare de sistem QLMTSECOFR (responsabil cu securitatea limită)
 - proces de semnare 179
- valoare de sistem QMAXSGNACN (acționează când se ating încercările de semnare)
 - stare profil utilizator 62
 - valoare setată de comanda CFGSYSSEC 625
- valoare de sistem QMAXSIGN (maximum încercări de semnare)
 - stare profil utilizator 62
 - valoare setată de comanda CFGSYSSEC 625
- valoare de sistem QPRTEDEV (dispozitiv de tipărire) 85
- valoare de sistem QPWDEXPITV (interval de expirare parolă)
 - parametru profil utilizator PWDEXPITV 74
- valoare de sistem QPWDEXPITV (interval expirare parolă)
 - descriere 39
- valoare de sistem QPWDLMTAJC (limită alăturată parolă) 43

valoare de sistem QPWDLMTCHR (caractere limită) 42	valoare sistem (<i>continuare</i>)	valoare sistem (<i>continuare</i>)
valoare de sistem QPWDLMTREP (caractere repetate limită) 43	QAUTOVRT (configurare dispozitiv-virtual automată) valoare setată de comanda CFGSYSSEC 625	QPWDVLDPGM (program de validare parolă) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QPWDMAXLEN (lungime maximă parolă) 41	QDEVRCYACN (acțiune de recuperare dispozitiv) valoare setată de comanda CFGSYSSEC 625	QRMTSIGN (permitere semnare la distanță) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QPWDMINLEN (lungime minimă parolă) 41	QDSCJOBITV (interval timeout job deconectat) valoare setată de comanda CFGSYSSEC 625	QSECURITY (nivel securitate) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QPWDPOSDIF (caractere de poziție) 44	QDSPGNINF (afișare informații de semnare) valoare setată de comanda CFGSYSSEC 625	securitate setare 625
valoare de sistem QPWDRQDDGT (digiți de parolă necesari) 44	QINACTITV (interval timeout job inactiv) valoare setată de comanda CFGSYSSEC 625	tipărire securitate relevantă 621
valoare de sistem QPWDRQDDIF (parolă duplicată) 42	QINACTMSGQ (coadă de mesaje job inactiv) valoare setată de comanda CFGSYSSEC 625	valoare sistem (QDSPGNINF) afișare informații de semnare
valoare de sistem QPWDVLDPGM (program validare parolă) 44	QINACTMSGQ (coadă de mesaje job inactiv) valoare setată de comanda CFGSYSSEC 625	valoare setată de comanda CFGSYSSEC 625
valoare de sistem QRMTSRVATR (atribut service la distanță) 33	QLMTSECOFR (limitare ofițer securitate) valoare setată de comanda CFGSYSSEC 625	valoare sistem (QLMTSECOFR) limitare ofițer securitate valoare setată de comanda CFGSYSSEC 625
valoare de sistem QSECURITY (nivel securitate) impunere valoare de sistem QLMTSECOFR 179	QMAXSGNACN (acționează când se ating încercările de semnare) valoare setată de comanda CFGSYSSEC 625	valoare sistem (QMAXSGNACN) când ating încercările de semnare valoare setată de comanda CFGSYSSEC 625
valoare de sistem QSHRMEMCTL (control memorie de partajare) descriere 29	QMAXSIGN (maximum încercări de semnare) valoare setată de comanda CFGSYSSEC 625	valoare sistem (QSECURITY) nivel securitate valoare setată de comanda CFGSYSSEC 625
valori posibile 30	QPWDEXPITV (interval expirare parolă) valoare setată de comanda CFGSYSSEC 625	valoare sistem acțiune recuperare dispozitiv(QDEVRCYACN) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QSPCENV (mediu special) 72	QPWDLMTCHR (caractere restricționate de parolă) valoare setată de comanda CFGSYSSEC 625	valoare sistem auditare control (QAUDCTL) afișare 619
valoare de sistem QSRTSEQ (secvență de sortare) 87	QPWDLMTTREP (parola necesită diferență de poziție) valoare setată de comanda CFGSYSSEC 625	modificare 619
valoare de sistem QUSEADPAUT (utilizare autorizare adoptată) descriere 30	QPWDMAXLEN (lungime minimă parolă) valoare setată de comanda CFGSYSSEC 625	valoare sistem automat configurată (QAUTOCFG) valoare setată de comanda CFGSYSSEC 625
risc de modificare 30	QPWDMINLEN (lungime minimă parolă) valoare setată de comanda CFGSYSSEC 625	valoare sistem coadă de mesaje job inactiv (QINACTMSGQ) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QUSRLIBL (listă de biblioteci utilizator) 79	QPWDRQDDGT (parola necesită caractere numerice) valoare setată de comanda CFGSYSSEC 625	valoare sistem configurare automată dispozitiv-virtual (QAUTOVRT) valoare setată de comanda CFGSYSSEC 625
valoare de sistem QVFOBJRST (verificare obiect la restaurare) 34	QPWDRQDDIF (diferențe cerute de parolă) valoare setată de comanda CFGSYSSEC 625	valoare sistem interval timeout job inactiv (QINACTITV) valoare setată de comanda CFGSYSSEC 625
valoare de sistem restaurare referitor la securitate privire generală 34		valoare sistem interval timeout job deconectat(QDSCJOBITV) valoare setată de comanda CFGSYSSEC 625
valoare de sistem verificare obiect la restaurare (QVFOBJRST) 34		valoare sistem nivel auditare (QAUDLVL) afișare 619
valoare de validare definiție 15		modificare 619
intrare jurnal auditare (QAUDJRN) 244		
valoare implicită semnare descrierea de subsistem 181		
valoare sistem autorizație obiect cerută pentru comenzi 433		
comandă pentru setare 625		
QALWOBJRST (permite restaurare obiect) valoare setată de comanda CFGSYSSEC 625		
QAUDCTL (control auditare) afișare 619		
modificare 619		
QAUDLVL (nivel auditare) modificare 619		
QAUDLVL (nivel de auditare) afișare 619		
QAUTOCFG (configurare automată) valoare setată de comanda CFGSYSSEC 625		

valoare sistem pentru maximum încercări de semnare (QMAXSIGN)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem permitere semnare distanță (QRMTSIGN)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QALWOBJRST (permite restaurare obiect)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QAUDCTL (auditare control) afișare 619
modificare 619

valoare sistem QAUDLVL (nivel auditare) afișare 619
modificare 619

valoare sistem QAUTOCFG (configurare automată)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QDEVRACYACN (acțiune recuperare dispozitiv)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QDSCJOBITV (interval timeout job deconectat)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QINACTITV (interval timeout job inactiv)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QINACTMSGQ (coadă de mesaje job inactiv)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QLMTSECOFR (limitare ofițer securitate)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDEXPITV (interval expirare parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDLMTAJC (caractere adiacente restricționate de parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDMAXLEN (lungime minimă parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDMINLEN (lungime minimă parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDRQDDIF (parola necesită diferență de poziție)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDRQDDGT (parola necesită caractere numerice)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDRQDDIF (diferențe cerute de parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QPWDVLDPGM (program de validare parolă)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QRMTSIGN (permitere semnare la distanță)
valoare setată de comanda
CFGSYSSEC 625

valoare sistem QSECURITY (nivel de securitate)
valoare setată de comanda
CFGSYSSEC 625

valoarea AUTOCFG (configurare automată dispozitiv) 31

valoarea configurare automată dispozitiv (AUTOCFG) 31

valoarea de sistem acțiune oprire auditare (QAUDENDACN) 50

valoarea de sistem acțiune recuperare dispozitiv (QDEVRACYACN) 32

valoarea de sistem configurația automată a dispozitivelor virtuale (QAUTOVRT) 32

valoarea de sistem control de auditare (QAUDCTL)
afișare 277
modificare 277

valoarea de sistem creare autorizare (QCRTAUT)
descriere 22
folosirea 118
risc de modificare 22

valoarea de sistem interval timeout job deconectat (QDSCJOBITV) 33

valoarea de sistem nivel de auditare (QAUDLVL)
afișare 277
modificare 277

valoarea de sistem nivel forțare auditare (QAUDFRCLVL) 51

valoarea de sistem permitere obiecte utilizator (QALWUSRDMN) 17, 21

Valoarea de sistem QALWUSRDMN (permitere obiecte utilizator) 17, 21

valoarea de sistem QAUDCTL (control auditare)
afișare 277
modificare 277

valoarea de sistem QAUDENDACN (acțiune oprire auditare) 50

valoarea de sistem QAUDFRCLVL (nivel forțare auditare) 51

valoarea de sistem QAUDLVL (nivel de auditare)
afișare 277
modificare 277

valoarea de sistem QAUTOCFG (automatic device configuration - configurare automată dispozitiv)
privire generală 31

valoarea de sistem QAUTOVRT (configurația automată a dispozitivelor virtuale) 32

valoarea de sistem QCRTAUT (creare autorizare)
folosirea 118

Valoarea de sistem QCRTAUT (create authority - creare autorizare)
descriere 22
risc de modificare 22

valoarea de sistem QDEVRACYACN (acțiune recuperare dispozitiv) 32

valoarea de sistem QDSCJOBITV (interval timeout job deconectat) 33

valoarea de sistem QDSPSGNINF (display sign-on information - afișare informații de semnare) 22

valoarea de sistem QINACTITV (inactive job time-out interval - interval timeout job inactiv) 23

valoarea de sistem QINACTMSGQ (inactive job message queue - coadă de mesaje a jobului inactiv) 24

valoarea de sistem QLMTDEVSSN (limit device sessions - limitare sesiuni dispozitiv)
descriere 25

valoarea de sistem QLMTSECOFR (limit security officer - limitare responsabil cu securitatea)
descriere 25
modificare niveluri de securitate 11

valoarea de sistem QMAXSGNACN (action when sign-on attempts reached - acțiune când este depășit numărul maxim de încercări de semnare)
descriere 26

valoarea de sistem QMAXSIGN (maximum sign-on attempts - număr maxim de încercări de semnare)
descriere 25

valoarea de sistem QRETSVRSEC (retain server security - reținere securitate server)
27
privire generală 27

valoarea de sistem QRMTSIGN (remote sign-on - semnare la distanță) 27

Valoarea de sistem QRMTSRVATR (atribut service la distanță) 2

valoarea de sistem QSCANFS (scan file systems - scanare sisteme de fișiere) 28

valoarea de sistem QSCANFS (Scan File Systems - Scanare sisteme de fișiere) 28

valoarea de sistem QSCANFCTL (scan file systems control - control scanare sisteme de fișiere) 28

valoarea de sistem QSECURITY (level of security - nivel de securitate)
nivelul 50 16

valoarea de sistem QSECURITY (nivel de securitate)
autorizare specială 9
clasă utilizator 9
comparație a nivelurilor 7
modificare
nivelul 10 în nivelul 20 10
nivelul 20 în nivelul 30 11
nivelul 30 în nivelul 20 10
nivelul 40 în nivelul 20 10
modificare, 20 dintr-un nivel mai înalt 10
modificare, nivelul 10 în nivelul 20 10

valoarea de sistem QSECURITY (nivel de securitate) (*continuare*)

- modificare, nivelul 20 în 30 11
- nivelul 10 10
- nivelul 20 10
- nivelul 30 11
- nivelul 40 11
- privire generală 7
- recomandări 9

valoarea de sistem QSECURITY (security level - nivel de securitate)

- blocuri de control interne 17
- creare automată profil utilizator 57
- dezactivare nivel 40 16
- dezactivare nivel 50 18
- modificare
 - nivelul 20 în nivelul 40 15
 - nivelul 20 în nivelul 50 17
 - nivelul 30 în nivelul 40 15
 - nivelul 30 în nivelul 50 17
 - nivelul 40 în nivelul 30 16
 - nivelul 50 la nivelul 30 sau 40 18
- modificare, la nivelul 40 15
- modificare, la nivelul 50 17
- nivelul 50 16
 - biblioteca QTEMP (temporară) 17
 - privire generală 16
 - tratare mesaj 17
 - validarea parametrilor 14

Valoarea de sistem QSECURITY (security level - nivel de securitate)

- introducere 2

valoarea QRETSVRSEC (retain server security - reținere securitate server) 27

valoarea sistem

- (caracterele alăturate ale parolei interzise)
- QPWDLMTAJC
 - valoarea setată de comanda CFGSYSSEC 625
- QPWDLMTREP (caractere repetate ale parolei limitate)
 - valoarea setată de comanda CFGSYSSEC 625

valoarea sistem QPWDLMTCHR (caractere ale parolei interzise)

- valoarea setată de comanda CFGSYSSEC 625

valori securitate

- setare 625

variabilă de sistem

- acțiune finală de auditare (QAUDENDACN) 255
- audit
 - planificare 254
- limitare sesiuni dispozitiv (QLMTDEVSSN)
 - auditare 231
- logare
 - la distanță (QRMTSIGN) 233
 - maximum de încercări (QMAXSIGN) 230, 233
 - logare de la distanță (QRMTSIGN) 233
 - maximum de încercări de logare (QMAXSIGN)
 - auditare 230, 233

variabilă de sistem (*continuare*)

- modificare
 - intrare jurnal auditare (QAUDJRN) 249
- nivel de auditare (QAUDLVL)
 - descriere *AUTFAIL (eșuare autorizare) 240
 - modificare 257
 - scop 234
 - valoarea *CREATE (creare) 241
 - valoarea *DELETE (ștergere) 241
 - valoarea *JOBDDTA (modificare job) 241
 - valoarea *OBJMGT (gestionare obiect) 243
 - valoarea *OFCSRV (servicii de tip office) 243
 - valoarea *PGMADP (autorizare adoptată) 244
 - valoarea *PGMFAIL (eșuare program) 244
 - valoarea *PRTDTA (ieșire imprimantă) 244
 - valoarea *SAVRST (salvare/restaurare) 244
 - valoarea *SECURITY (securitate) 247
 - valoarea *SERVICE (unelte service) 250
 - valoarea *SPLFDTA (modificări fișier spool) 250
 - valoarea *SYSMGT (gestionare sisteme) 250
- nivel de securitate (QSECURITY)
 - auditare 230
- nivel forțare auditare (QAUDFRCLVL) 254
- parolă
 - expirare auditare 231
 - prevenire simplă 231
- QAUDENDACN (auditing end action - acțiune finală de auditare) 255
- QAUDFRCLVL (nivel forțare audit) 254
- QAUDLVL (nivel de auditare)
 - descriere *AUTFAIL (eșuare autorizare) 240
 - modificare 257
 - scop 234
 - valoarea *CREATE (creare) 241
 - valoarea *DELETE (ștergere) 241
 - valoarea *JOBDDTA (modificare job) 241
 - valoarea *OBJMGT (gestionare obiect) 243
 - valoarea *OFCSRV (servicii de tip office) 243
 - valoarea *PGMADP (autorizare adoptată) 244
 - valoarea *PGMFAIL (eșuare program) 244
 - valoarea *PRTDTA (ieșire imprimantă) 244
 - valoarea *SAVRST (salvare/restaurare) 244
 - valoarea *SECURITY (securitate) 247
 - valoarea *SERVICE (unelte service) 250

variabilă de sistem (*continuare*)

- QAUDLVL (nivel de auditare) (*continuare*)
 - valoarea *SPLFDTA (modificări fișier spool) 250
 - valoarea *SYSMGT (gestionare sisteme) 250
- QLMTDEVSSN (limit device sessions - limitare sesiuni dispozitiv)
 - auditare 231
- QLMTSECOFR (limit security officer - limitare responsabil cu securitatea)
 - auditare 230
- QMAXSIGN (maximum de încercări de logare)
 - auditare 230, 233
- QPWDEXPITV (password expiration interval - interval de expirare a parolei)
 - auditare 231
- QRMTSIGN (logare de la distanță) 233
- QSECURITY (nivel de securitate)
 - auditare 230

variabilă de sistem (QAUDLVL) nivel de auditare

- Vedeți și jurnal auditare (QAUDJRN)*
- modificare 257
- scop 234
- valoarea *AUTFAIL (eșuare autorizare) 240
- valoarea *CREATE (creare) 241
- valoarea *DELETE (ștergere) 241
- valoarea *JOBDDTA (modificare job) 241
- valoarea *OBJMGT (gestionare obiect) 243
- valoarea *OFCSRV (servicii de tip office) 243
- valoarea *PGMADP (autorizare adoptată) 244
- valoarea *PGMFAIL (eșuare program) 244
- valoarea *PRTDTA (ieșire imprimantă) 244
- valoarea *SAVRST (salvare/restaurare) 244
- valoarea *SECURITY (securitate) 247
- valoarea *SERVICE (unelte service) 250
- valoarea *SPLFDTA (modificări fișier spool) 250
- valoarea *SYSMGT (gestionare sisteme) 250

variabilă de sistem (QSECURITY) nivel de securitate

- auditare 230

variabilă de sistem acțiune finală de auditare (QAUDENDACN) 255

variabilă de sistem logare de la distanță (QRMTSIGN) 233

variabilă de sistem nivel forțare auditare (QAUDFRCLVL) 254

variabilă de sistem QAUDENDACN (auditing end action - acțiune finală de auditare) 255

variabilă de sistem QAUDFRCLVL (nivel forțare audit) 254

variabilă de sistem QAUDLVL (nivel de auditare)

- Vedeți și jurnal QAUDJRN (audit)*
- modificare 257

variabilă de sistem QAUDLVL (nivel de auditare) *(continuare)*
 scop 234
 valoare *AUTFAIL 240
 valoare *CREATE (creare) 241
 valoare *DELETE (ștergere) 241
 valoare *JOBDDTA (modificare job) 241
 valoare *OBJMGT (gestionare obiect) 243
 valoare *OFCSRVR (servicii de tip office) 243
 valoare *PGMADP (autorizare adoptată) 244
 valoare *PGMFAIL (eșuare program) 244
 valoare *PRTDDTA (ieșire imprimantă) 244
 valoare *SAVRST (salvare/restaurare) 244
 valoare *SECURITY (securitate) 247
 valoare *SERVICE (unelte service) 250
 valoare *SPLFDDTA (modificări fișier spool) 250
 valoarea *SYSMGT (gestionare sisteme) 250

variabilă de sistem QLMTDEVSSN (limit device sessions - limitare sesiuni dispozitiv) auditare 231

variabilă de sistem QLMTSECOFR (limit security officer - limitare responsabil cu securitatea) auditare 230

variabilă de sistem QMAXSIGN (maximum de încercări de logare) auditare 230, 233

variabilă de sistem QPWDEXPITV (password expiration interval - interval de expirare a parolei) auditare 231

variabilă de sistem QRMTSIGN (logare de la distanță) 233

variabilă de sistem QSECURITY (nivel de securitate) auditare 230

verificare
Vedeți și verificare autorizare integritate obiect 621
 auditare folosire 233
 descriere 269, 274
 obiecte transformate 269
 parolă 107, 273
 parole implicite 617

verificare autorizare
Vedeți și autorizare autorizare adoptată
 diagramă de flux (flowchart) 159
 exemplu 166, 168
 autorizare de grup
 exemplu 163, 167
 autorizare privată
 diagramă de flux (flowchart) 151
 autorizare proprietar
 diagramă de flux (flowchart) 152
 autorizare publică
 diagramă de flux (flowchart) 158
 exemplu 165, 167

verificare autorizare *(continuare)*
 grup primar
 exemplu 164
 listă de autorizare
 exemplu 169
 secvență 147

VFYIMGCLG
 profiluri utilizator livrat de IBM autorizate 296

violare descriere de job
 intrare jurnal auditare (QAUDJRN) 14

virus
 detectare 233, 269, 274
 scanare 269

vizualizare
 intrări jurnal auditare 260

W

WRKFCNARA
 profiluri utilizator livrat de IBM autorizate 296

WRKIMGCLGE
 profiluri utilizator livrat de IBM autorizate 296

WRKLIB
 profiluri utilizator livrat de IBM autorizate 296

WRKLIBPDM
 profiluri utilizator livrat de IBM autorizate 296

WRKPTFGRP (Work with Program Temporary Fix Groups - Gestionare grupuri de corecții temporare program) 297

WRKSYSACT
 profiluri utilizator livrat de IBM autorizate 297

WRKSYSSTS (Work with System Status - Gestionare stare sistem) 192

Z

zonă de date
 autorizație obiect cerută pentru comenzi 325

Comentarii cititori

IBM Systems - iSeries
Referințe privind securitatea
Versiunea 5 Ediția 4

Publicația nr. SA12-6497-09

Apreciam comentariile dumneavoastră despre această publicație. Nu ezitați să ne trimiteți comentariile despre anumite erori sau lipsuri, despre claritatea, organizarea și conținutul subiectelor din această carte. Comentariile pe care le trimiteți trebuie să se refere la informațiile din acest manual și la modul în care sunt prezentate.

Pentru întrebări cu caracter tehnic și informații despre produse și prețuri vă rugăm să luați legătura cu sucursala IBM din localitatea dumneavoastră, cu partenerul de afaceri IBM sau cu reprezentantul de vânzări autorizat.

Pentru întrebări generale, vă rugăm sunați la "Halo IBM" (număr de telefon 01803/313233).

Când trimiteți comentarii la IBM, acordați IBM-ului dreptul ne-exclusiv de a utiliza sau distribui aceste comentarii în orice mod pe care îl consideră corespunzător, fără ca din aceasta să rezulte vreo obligație față de dumneavoastră.

Comentarii:

Vă mulțumim pentru ajutorul acordat.

Pentru a trimite comentariile:

- Trimiteți comentariile la adresa de pe spatele acestui formular.
- Trimiteți un fax la următorul număr: Alte țări: 1-507-253-5192
- Trimiteți comentariile prin e-mail la: RCHCLERK@us.ibm.com

Dacă doriți un răspuns de la IBM, vă rugăm să completați următoarele informații:

Nume

Adresă

Companie sau organizație

Număr de telefon

Adresă de e-mail

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 HWY 52 N
ROCHESTER MN



Tipărit în S.U.A.

SA12-6497-09

