Deutsch

FUJITSU Software BS2000

SECOS V5.5

Security Control System - Zugangs- und Zugriffskontrolle

Ausgabe März 2018

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Inhalt

1 Einleitung 13

1.1 Zielgruppen des Handbuchs 15
1.2 Lizenzrechtliche Bestimmungen 16
1.3 Konzept des Handbuchs 21
1.4 Readme-Datei 21
1.5 Änderungen gegenüber der vorherigen Ausgabe 22
1.6 Verwendete Metasprache 24

2 Sicherheit in DV-Systemen und im BS2000 25

2.1 Allgemeine Bedrohungen von DV-Systemen 26
2.2 Technische Sicherheitsmaßnahmen im BS2000 29
2.3 Sicherheitskonzeption des BS2000 29
2.4 Grundlegende Aufgabenbereiche im BS2000 30
2.5 Sicherheitsgrundsätze für den Benutzer 32
2.6 Sicherheitskriterien 35

3 SRPM – Privilegien und Betriebsmittel verwalten 39

3.1 Privilegien verwalten 40
3.1.1 Rolle des Sicherheitsbeauftragten 41
3.1.2 Sammelprivilegien 43
3.1.3 Regeln für die Privilegienvergabe 44
3.1.4 Zentralisierte Administration 45
3.1.5 Beschreibung der Privilegien 46
TSOS (TSOS) 46

Sicherheitsbeauftragter (SECURITY-ADMINISTRATION) . . . 46
Alias-Catalog-Service-Verwaltung (ACS-ADMINISTRATION) . . . 49
Vorgenerierte Privilegien (CUSTOMER-PRIVILEGE-1...8) . . . 49
File-Transfer-Verwaltung (FT-ADMINISTRATION) . . . 49
FTAC-Verwaltung (FTAC-ADMINISTRATION) . . . 50
Systemglobale Guard-Administration (GUARD-ADMINISTRATION) . . . 50
Hardware-Online-Wartung (HARDWARE-MAINTENANCE) . . . 51
HSMS-Verwaltung (HSMS-ADMINISTRATION) . . . 52
Netzverwaltung (NET-ADMINISTRATION) . . . 52
Notification-Service-Administration (NOTIFICATION-ADMINISTRATION) . . . 53
Systembedienung (OPERATING) . . . 53
POSIX-Benutzerverwaltung (POSIX-ADMINISTRATION) . . . 54
SPOOL-Verwaltung (PRINT-SERVICE-ADMINISTRATION) . . . 54
Verwaltung des PROP-XT (PROP-ADMINISTRATION) . . . 55
Auswertung der SAT-Dateien (SAT-FILE-EVALUATION) . . . 55
Verwaltung der SAT-Dateien (SAT-FILE-MANAGEMENT) . . . 56
Eingabe von Benutzerkommandos (STD-PROCESSING) . . . 57
Subsystem-Verwaltung (SUBSYSTEM-MANAGEMENT) . . . 58
Software-Monitor-Verwaltung (SW-MONITOR-ADMINISTRATION) . . . 59
Bandverwaltung (TAPE-ADMINISTRATION) . . . 59
Encryption-Key-Verwaltung für Bänder (TAPE-KEY-ADMINISTRATION) . . . 60
Systemglobale Benutzerverwaltung (USER-ADMINISTRATION) . . . 60
Verwaltung einer virtuellen Maschine (VIRTUAL-MACHINE-ADMINISTRATION) . . . 62
Verwaltung von VM2000 (VM2000-ADMINISTRATION) . . . 62

3.1.6 Privilegienverteilung nach First-Start . . . 62
3.1.7 Privilegienverteilung nach Nicht-First-Start . . . 64
3.1.8 Beispiele für die Privilegienvergabe . . . 65

3.2 Benutzer und ihre Betriebsmittel verwalten . . . 66
3.2.1 Berechtigungen zur Benutzerverwaltung . . . 66
3.2.2 Benutzergruppen . . . 68
3.2.3 Aufbau einer Benutzergruppenstruktur . . . 75
3.2.4 Konzept der Verwaltung von Benutzern und Benutzergruppen . . . 78
3.2.5 Beispiele für Benutzergruppen . . . 81
3.2.6 Betriebsmittel der Benutzer begrenzen . . . 88

3.3 Zugangsschutz . . . 91
3.3.1 Kennwortschutz . . . 91
3.3.2 Trennung der Zugangswege . . . 95
3.3.3 Einschränkung des Zugangs über Terminal-Sets . . . 96
3.3.4 Zugangsschutz mit Guards . . . 104
3.3.5 Persönliche Identifizierung . . . 105
3.3.6 Single Sign On mit Kerberos . . . 109

3.3.7 Protokollierung der Zugangsversuche . . . 118
3.3.8 Sperrung von Terminals/Benutzerkennungen nach erfolglosen Zugangsversuchen . . 119
3.3.9 Sperrung von Benutzerkennungen bei Inaktivität . . . 121
3.3.10 Standardschutz für Kennungen . . . 122

3.4 SRPM-Kommandos . . . 124
Funktionelle Übersicht . . . 124
ADD-KEYTAB-ENTRY
Key-Tabellen-Eintrag hinzufügen . . . 129
ADD-USER-GROUP
Benutzergruppe in Benutzerkatalog eintragen . . . 132
CONVERT-KEYTAB
Keytab-Ausgabedatei umsetzen . . . 148
COPY-TERMINAL-SET
Terminal-Set kopieren . . . 151
CREATE-PRIVILEGE-SET
Sammelprivileg erzeugen . . . 154
CREATE-TERMINAL-SET
Terminal-Set anlegen . . . 156
DELETE-PRIVILEGE-SET
Sammelprivileg löschen . . . 159
DELETE-TERMINAL-SET
Terminal-Set löschen . . . 161
MODIFY-KEYTAB-ENTRY
Key-Tabellen-Eintrag ändern . . . 163
MODIFY-LOGON-DEFAULTS
Standardwerte für Schutzattribute ändern . . . 170
MODIFY-LOGON-PROTECTION
Schutzattribute ändern . . . 172
MODIFY-PRIVILEGE-SET
Sammelprivileg ändern . . . 207
MODIFY-TERMINAL-SET
Terminal-Set modifizieren . . . 209
MODIFY-USER-GROUP
Benutzergruppeneintrag ändern . . . 212
REMOVE-KEYTAB-ENTRY
Key-Tabellen-Eintrag löschen . . . 232
REMOVE-USER-GROUP
Benutzergruppe löschen . . . 234
RESET-PRIVILEGE
Systemglobale Privilegien entziehen . . . 236
SET-LOGON-DEFAULTS
Standardwerte für Schutzattribute vereinbaren . . . 239

SET-LOGON-PROTECTION
Schutzattribute vereinbaren . . . 241
SET-PERSONAL-ATTRIBUTES
Persönliche Identifizierung angeben . . . 267
SET-PRIVILEGE
Systemglobale Privilegien vergeben . . . 268
SHOW-KEYTAB-ENTRY
Key-Tabellen-Eintrag anzeigen . . . 270
SHOW-LOGON-DEFAULTS
Standardwerte für Schutzattribute anzeigen . . . 273
SHOW-LOGON-PROTECTION
Schutzattribute anzeigen . . . 277
SHOW-PERSONAL-LOGON-ADMISSION
Persönliche Benutzerkennungen anzeigen . . . 295
SHOW-PRIVILEGE
Systemglobale Privilegien anzeigen . . . 301
SHOW-PRIVILEGE-SET
Sammelprivileg-Definition anzeigen . . . 310
SHOW-TERMINAL-SET
Terminal-Set anzeigen . . . 314
SHOW-USER-GROUP
Benutzergruppeneintrag anzeigen . . . 324
SHOW-USER-SUSPEND
Suspendierungen anzeigen . . . 335
UNLOCK-USER-SUSPEND
Suspendierungen aufheben . . . 338

3.5 SRPM-Makros . . . 339
GETUGR
Gruppenzugehörigkeit einer Benutzerkennung ermitteln . . . 340
SRMKPR
Namen des Principal ausgeben . . . 343
SRMPID
Persönliche Benutzerkennung ermitteln . . . 344
SRMSUG
Gruppeninformation ausgeben . . . 345

3.6 Beispiele zur Benutzerverwaltung . . . 366
3.6.1 Beispiel 1: Gruppenpotential verwalten . . . 367
3.6.2 Beispiel 2: Einrichten neuer Benutzergruppen . . . 383
3.6.3 Beispiel 3: Vergrößern des Gruppenpotentials einer Benutzergruppe . . . 389
3.6.4 Beispiel 4: Verkleinern des Gruppenpotentials einer Benutzergruppe . . . 394
3.6.5 Beispiel 5: Umhängen einer Benutzergruppe . . . 403
3.6.6 Beispiel 6: Löschen einer Benutzergruppe . . . 413

4 Zugriffsschutzmechanismen des BS2000 419

4.1 Übersicht über Zugriffsschutzmechanismen 419

4.2 Zugriffskontrolle des Grundausbaus von BS2000 424
4.2.1 Zugriffsschutz mit ACCESS/USER-ACCESS 424
4.2.2 Einfache Zugriffskontrollliste (BACL) 425

5 GUARDS – Schutz für Objekte 427

5.1 GUARDS-Verwaltung 434

5.2 Rollen der Eigentümer von Objekten 436

5.3 Schutzmechanismen von GUARDS im Überblick 437

5.4 Zugriffs- und Zugangsschutz 438
5.4.1 Zugriffs- und Zugangsschutz einrichten 439
5.4.2 Zugriffsbedingungen definieren 443
5.4.3 Arbeiten mit Objekten, die mit Guards geschützt werden 448

5.5 Standardschutz (Default protection) 449
5.5.1 Anwendungskonzept 451
5.5.2 Festlegung der Schutzattribut-Standardwerte 453
5.5.3 Festlegung der Standardschutzregeln 455
5.5.3.1 Aufbau eines Regelbehälters (Guard Typ DEFAULTP) 457
5.5.3.2 Geltungsbereich der Standardschutzregeln 458
5.5.3.3 Aktivierung eines Regelbehälters 458
5.5.4 Festlegung der Benutzer- und Gruppenkennungen für Pfadnamen (nur für Systemverwaltung) 461
5.5.5 Suchlogik 462
5.5.5.1 Suche nach den aktiven Regelbehältern 462
5.5.5.2 Suche in den aktiven Regelbehältern 463
5.5.5.3 Überlappung von Objektnamen 465
5.5.5.4 Reorganisation aktiver Regelbehälter 466
5.5.6 Allgemeine Hinweise zum Einsatz des Standardschutzes 469

5.6 Miteigentümerschutz (Co-owner protection) 471
5.6.1 Anwendungskonzept 473
5.6.2 Festlegung der Miteigentümerbedingungen 475
5.6.3 Festlegung der Miteigentümerschutzregeln 476
5.6.3.1 Aufbau eines Regelbehälters (Typ COOWNERP) 478
5.6.3.2 Geltungsbereich der Miteigentümerschutzregeln 479
5.6.3.3 Aktivierung eines Regelbehälters 479
5.6.4 Suchlogik 482

5.6.4.1 Suche nach den aktiven Regelbehältern . . . 482
5.6.4.2 Suche in den aktiven Regelbehältern . . . 482
5.6.4.3 Überlappung von Objektnamen . . . 485
5.6.4.4 Reorganisation aktiver Regelbehälter . . . 486

5.7 Einschränkung der TSOS-Miteigentümerschaft . . . 487
5.7.1 Ziel . . . 488
5.7.2 Umfang . . . 488
5.7.3 Systemspezifische Einstellungen . . . 489
5.7.4 Benutzerspezifische Einstellungen . . . 489
5.7.5 Überprüfung . . . 492
5.7.6 Anwendungsbeispiel . . . 494
5.7.7 Sicherung und Restaurierung von Guards mit GUARDS-SAVE . . . 502
5.7.8 Sicherung mit HSMS/ARCHIVE . . . 502
5.7.9 Rechnerverbünde . . . 502

5.8 GUARDS administrieren . . . 503
5.8.1 Guardskatalog . . . 503
5.8.2 Guardskatalog wechseln . . . 503
5.8.3 Guardskatalog wiederherstellen . . . 503
5.8.4 Sicherung mit ARCHIVE . . . 504
5.8.5 GUARDS mit MSCF und SPVS . . . 504
5.8.6 GUARDS und RFA . . . 505
5.8.7 GUARDS und SMS . . . 506

5.9 SSINFO-Datei . . . 507

5.10 GUARDS - Installation und Inbetriebnahme . . . 509

5.11 GUARDS-Kommandos . . . 517
Funktionelle Übersicht . . . 517
ADD-ACCESS-CONDITIONS
Zugriffsbedingungen hinzufügen . . . 519
ADD-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel hinzufügen . . . 530
ADD-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute festlegen . . . 535
ADD-DEFAULT-PROTECTION-RULE
Standardschutzregel hinzufügen . . . 548
ADD-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad hinzufügen . . . 555
CHANGE-GUARD-FILE
Guardskatalog austauschen . . . 558
COPY-GUARD
Guard kopieren . . . 561

CREATE-GUARD
Guard einrichten . . . 563
DELETE-GUARD
Guard löschen . . . 565
MODIFY-ACCESS-CONDITIONS
Zugriffsbedingungen ändern . . . 568
MODIFY-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel ändern . . . 578
MODIFY-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute ändern . . . 584
MODIFY-DEFAULT-PROTECTION-RULE
Standardschutzregel ändern . . . 597
MODIFY-GUARD-ATTRIBUTES
Guard-Attribute ändern . . . 603
REMOVE-ACCESS-CONDITIONS
Zugriffsbedingungen entfernen . . . 606
REMOVE-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel entfernen . . . 609
REMOVE-DEFAULT-PROTECTION-RULE
Standardschutzregel entfernen . . . 612
REMOVE-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad entfernen . . . 615
REPAIR-GUARD-FILE
Guardskatalog wiederherstellen . . . 619
SHOW-ACCESS-ADMISSION
Zugriffserlaubnis anzeigen . . . 622
SHOW-ACCESS-CONDITIONS
Zugriffsbedingungen anzeigen . . . 632
SHOW-COOWNER-ADMISSION-RULE
Miteigentümerberechtigungsregel anzeigen . . . 650
SHOW-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel anzeigen . . . 654
SHOW-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute anzeigen . . . 659
SHOW-DEFAULT-PROTECTION-RULE
Standardschutzregel anzeigen . . . 664
SHOW-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad anzeigen . . . 669
SHOW-EVALUATED-CONDITIONS
Auszuwertende Zugriffsbedingungen anzeigen . . . 673
SHOW-GUARD-ATTRIBUTES
Guard-Attribute anzeigen . . . 676
SHOW-GUARD-MANAGEMENT-STATUS
GUARDS-Systemeinstellungen anzeigen . . . 680

SHOW-OBJECT-PROTECTION-DEFAULT
Standardschutzattribute für Objekt anzeigen . . . 683
5.11.1 Beispiele zu GUARDS-Kommandos . . . 692

5.12 GUARDS-Makros . . . 704
Funktionelle Übersicht . . . 704
ADDATTR
Standardwerte für Schutzattribute festlegen . . . 706
ADDCOO
Miteigentümerschutzregel hinzufügen . . . 719
ADDDEF
Standardschutzregel hinzufügen . . . 726
ADDUID
Kennungen für Objektpfad hinzufügen . . . 734
CHKSAC
Zugriffsbedingungen auswerten . . . 738
COPGUAD
Guard kopieren . . . 744
CREGUAD
Guard einrichten . . . 746
DELGUAD
Guard löschen . . . 748
MODATTR
Standardwerte für Schutzattribute ändern . . . 750
MODCOO
Miteigentümerschutzregel ändern . . . 764
MODDEF
Standardschutzregel ändern . . . 771
MODGUAD
Guard-Attribute ändern . . . 779
MODSAC
Zugriffsbedingungen hinzufügen oder ändern . . . 781
MSGGUAD
Meldungen und Return-Codes ausgeben . . . 791
REMCOO
Miteigentümerschutzregel entfernen . . . 792
REMDEF
Standardschutzregel entfernen . . . 796
REMSAC
Zugriffsbedingungen entfernen . . . 800
REMUID
Kennungen für Objektpfad entfernen . . . 804
SACMGMT
Globale Konstanten definieren . . . 808

SHWACOO
Miteigentümerberechtigungsregel anzeigen . . . 809
SHWATTR
Standardwerte für Schutzattribute anzeigen . . . 813
SHWCOO
Miteigentümerschutzregel anzeigen . . . 816
SHWDEF
Standardschutzregel anzeigen . . . 819
SHWGUAD
Guard-Attribute anzeigen . . . 822
SHWOBJ
Standardschutzattribute für Objekt anzeigen . . . 825
SHWSAC
Zugriffserlaubnis oder Zugriffsbedingungen anzeigen . . . 828
SHWUID
Kennungen für Objektpfad anzeigen . . . 843
5.12.1 Beispiele zu GUARDS-Makros . . . 845
Beispiel 1: Zugriffsbedingungen hinzufügen . . . 845
Beispiel 2: Zugriffsbedingungen ändern . . . 852
Beispiel 3: Zugriffsbedingung löschen . . . 858
Beispiel 4: Zugriffsbedingungen anzeigen . . . 862
5.12.2 Makro-Syntax für GUARDS-Makros . . . 876

5.13 Dienstprogramm GUARDS-SAVE . . . 881
5.13.1 Berechtigungskonzept . . . 882
5.13.2 Auswahl der zu bearbeitenden Guards . . . 883
5.13.3 Bearbeitungsreihenfolge der Guards . . . 886
5.13.4 Umbenennung der Guards beim Restaurieren . . . 887
5.13.4.1 Austausch der Guardpfadnamen . . . 887
5.13.4.2 Austausch der Katalogkennung in Zugriffsbedingungen des Typs PROGRAM . . . 889
5.13.5 Ergebnisprotokoll . . . 890
5.13.6 Zeitstempel und Uhrzeiten . . . 897
5.13.7 Guards sichern . . . 898
5.13.7.1 Die Sicherungsdatei . . . 898
5.13.7.2 Backup-Katalogkennung . . . 899
5.13.8 Guards restaurieren . . . 900
5.13.8.1 Programmgesteuerte Restaurierung . . . 900
5.13.8.2 Prozedurgesteuerte Restaurierung . . . 901
5.13.8.3 Restore-Katalogkennung . . . 905
5.13.9 Gesicherte Guards anzeigen . . . 906
5.13.10 GUARDS-SAVE starten . . . 908
START-GUARDS-SAVE
Starten des Programms GUARDS-SAVE . . . 908

5.13.11 GUARDS-SAVE-Anweisungen . . . 909
BACKUP-GUARDS
Guards in Sicherungsdatei kopieren . . . 910
RESTORE-GUARDS
Guards aus einer Sicherungsdatei restaurieren . . . 915
SHOW-BACKUP-FILE
Inhalt einer Sicherungsdatei anzeigen . . . 922
5.13.12 Beispiele zu GUARDS-SAVE . . . 929
5.13.13 Verhalten von GUARDS-SAVE im Fehlerfall . . . 937
5.13.14 GUARDS-SAVE - Installation und Inbetriebnahme . . . 937

6 Anhang . . . 939

6.1 Wirksamkeit der TSOS-Einschränkung . . . 939

Fachwörter . . . 951

Literatur . . . 967

Stichwörter . . . 971

1 Einleitung

SECOS (SEcurity COntrol System) umfasst eine Produktpalette mit folgenden Bestandteilen: SRPM, GUARDS, GUARDDEF, GUARDCOO, SAT und SECOS-KRB. Diese Bestandteile stellen Verwaltungssysteme und Schnittstellen zur Verfügung, die für jeden einzelnen Benutzer einen individuellen Rahmen an Rechten und Pflichten definieren lassen. Sie spannen einen Bogen vom Einrichten, Verwalten und Löschen von Kennungen über das Arbeiten unter einer Kennung bis zur Überwachung, ob versucht wird, sich illegal Zugriff auf eine Kennung und deren Daten zu verschaffen.

SRPM (System Resources and Privileges Management). SRPM dient der Systemverwaltung (insbesondere dem Sicherheitsbeauftragten und der Benutzerverwaltung), um bereits bei der Einrichtung einer Kennung den Rahmen der Möglichkeiten für diese Kennung abzustecken. Die Kennung kann in ein Gruppenkonzept eingebunden und/oder ihr können besondere Privilegien zugebilligt werden. Auf diese Weise wird eine Benutzerstruktur errichtet, die Sicherheitsverstöße möglichst unwahrscheinlich bzw. die Quellen möglichst schnell lokalisierbar macht. Das Gruppenkonzept erlaubt es weiterhin, bestehende Projekt- und Organisationsformen im BS2000 nachzubilden.

GUARDS (Generally Usable Access contRol aDministration System). GUARDS überwacht den Zugriff der Benutzer auf Dateien, Bibliotheken und weitere Objekte verschiedener Objektverwaltungen. Der Schutz durch GUARDS kann von der jeweiligen Objektverwaltung für alle und von jedem einzelnen Benutzer für seine eigenen Objekte verwendet werden. GUARDS bietet umfangreiche und flexible Möglichkeiten, Daten wirksam gegen unerlaubte Zugriffe zu schützen.

GUARDDEF (Default Protection, Standardschutz). GUARDDEF dient der Vergabe von Standardattributwerten für Dateien und Jobvariablen. Diese Werte können wahlweise für das Anlegen oder Modifizieren dieser Objekte vorgegeben werden. Die Einstellungen können von der Systemverwaltung (TSOS) jeweils pubset-weit und von jedem Benutzer für seine eigenen Objekte unter seiner Benutzerkennung vorgenommen werden.
GUARDDEF nutzt GUARDS zur Ablage der Einstellungen.

GUARDCOO (Co-owner Protection, Miteigentümerschutz). Für Dateien und Jobvariablen kann die standardmäßig feste Eigentümer-Regelung im BS2000 (Eigentümer ist die Kennung, unter der das Objekt katalogisiert ist, TSOS ist Miteigentümer aller Dateien und Jobvariablen) verfeinert definiert werden. Dabei kann die Miteigentümerschaft für unterschiedliche Namensbereiche der Objekte sowohl der Benutzerkennung TSOS entzogen als auch anderen Benutzerkennungen oder den Inhabern bestimmter Privilegien gewährt werden. GUARDCOO nutzt GUARDS zur Ablage der Einstellungen.

SAT (Security Audit Trail). SAT ist die Protokollierungskomponente des BS2000 für sicherheitsrelevante Ereignisse. SAT kann eingesetzt werden, um Eindringversuche zu erkennen und um bei Verstößen gegen die Sicherheitsregelungen den Verursacher zu ermitteln. Dazu protokolliert SAT Ereignisse in SAT-Protokolldateien (SATLOG). In regelmäßigen Abständen müssen diese Dateien von Benutzern mit SAT-Privilegien ausgewertet werden. Hierzu dient das Auswertungsprogramm SATUT.

Besonders sicherheitskritische Ereignisse können ohne Verzögerung mit Hilfe der SAT-Alarmfunktion überwacht werden. Die Alarmmeldung erscheint auf der Operator-Konsole, so dass entschieden werden kann, welche Maßnahmen ergriffen werden sollen.

SECOS-KRB SECOS-KRB ist die Schnittstelle zur Abwicklung der Kerberos-Authentisierung im BS2000.

Dieses Handbuch beschreibt alle SECOS-Komponenten außer der Komponente SAT (Security Audit Trail), die im Handbuch „SECOS - Security Control System - Beweissicherung“ [1] beschrieben ist.

1.1 Zielgruppen des Handbuchs

Das Handbuch wendet sich an alle Benutzer und Betreiber eines sicheren BS2000-Systems. Es beschreibt die Funktionen des Produkts SECOS. Zum Verständnis des Handbuchs sind gute Kenntnisse der Sicherheitsfunktionen im Grundausbau des BS2000 erforderlich.

Für Leser oder Benutzer, die mit Verwaltungsaufgaben betraut sind, sind alle Teile relevant. Kapitel 3 (SRPM) wendet sich vor allem an die mit der Sicherheitsverwaltung oder Benutzerverwaltung betrauten Benutzer.

Für alle Benutzer relevant sind folgende Abschnitte:

– Kapitel 2 zur Sicherheit in DV-Systemen und im BS2000.

– Abschnitt „Protokollierung der Zugangsversuche“ auf Seite 118 und die Beschreibung des zugehörigen Kommandos SHOW-LOGON-PROTECTION ab Seite 277.

– Bei Verwendung der Persönlichen Identifizierung:

  Abschnitt „Persönliche Identifizierung“ auf Seite 105 und die Beschreibungen der entsprechenden Kommandos MODIFY-USER-PROTECTION (siehe Handbuch „Kommandos“ [4]), SET-PERSONAL-ATTRIBUTES (Seite 267) und SHOW-PERSONAL-LOGON-ADMISSION (Seite 295).

– Kapitel 4 und 5 beschreiben die jedem Benutzer zugänglichen Konzepte und Funktionen zum Schutz eigener Daten vor unerwünschtem Zugriff durch andere Benutzer.

1.2 Lizenzrechtliche Bestimmungen

Die folgenden Copyright-Vermerke betreffen ausschließlich das Subsystem SECOSKRB, das Teile der Kerberos-Implementierung Heimdal und der SSL-Bibliothek SSLeay enthält.

```
ThirdpartyLicenseReadme for SECOS-KRB V5.5A              December 2017


Component: src/lib/crypto/builtin/aes
*************************************

License text
************
Copyright (C) 2001, Dr Brian Gladman brg@gladman.uk.net, Worcester, UK.
All rights reserved.
LICENSE TERMS
The free distribution and use of this software in both source and binary
form is allowed (with or without changes) provided that:
1. distributions of this source code include the above copyright notice,
   this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice,
   this list of conditions and the following disclaimer in the
   documentation and/or other associated materials;
3. the copyright holder?s name is not used to endorse products built
   using this software without specific written permission.
DISCLAIMER
This software is provided "as is" with no explicit or implied warranties
in respect of any properties, including, but not limited to, correctness
and fitness for purpose.

--- End of License Text ---
```

```
Component: src/lib/crypto
*************************

License text
************

Copyright (C) 1998 by the FundsXpress, INC.
All rights reserved.

Export of this software from the United States of America may require a
specific license from the United States Government. It is the
responsibility of any person or organization contemplating export to
obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute
this software and its documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice appear in all
copies and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of FundsXpress.
not be used in advertising or publicity pertaining to distribution of
the software without specific, written prior permission. FundsXpress
makes no representations about the suitability of this software for any
purpose. It is provided "as is" without express or implied warranty.
THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

--- End of License Text ---
```

```
Component: src/lib/krb5
***********************

License text
************

Copyright (C) 1994 CyberSAFE Corporation.
Copyright 1990,1991,2007,2008 by the.
Massachusetts Institute of Technologygy.
All Rights Reserved.

Export of this software from the United States of America may require a
specific license from the United States Government. It is the
responsibility of any person or organization contemplating export to
obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute
this software and its documentation for any purpose and without fee is
hereby granted, provided that the above copyright notice appear in all
copies and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of M.I.T. not be
used in advertising or publicity pertaining to distribution of the
software without specific, written prior permission. Furthermore if you
modify this software you must label your software as modified software
and not distribute it in such a fashion that it might be confused with
the original M.I.T. software. Neither M.I.T., the Open Computing
Security Group, nor CyberSAFE Corporation make any representations
about the suitability of this software for any purpose. It is provided
"as is" without express or implied warranty.

--- End of License Text ---
```

```
Component: src/lib/krb5/krb
***************************

License text
************
Copyright (C) 2006 Kungliga Tekniska Hoegskola
(Royal Institute of Technology, Stockholm, Sweden).
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation
   and/or other materials provided with the distribution.
3. Neither the name of KTH nor the names of its contributors may be
   used to endorse or promote products derived from this software
   without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY KTH AND ITS CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL KTH OR ITS CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

--- End of License Text ---
```

```
Component: src/util/support
**************************

License text
************

The OpenLDAP Public License
Version 2.8, 17 August 2003
Redistribution and use of this software and associated documentation
("Software"), with or without modification, are permitted provided that
the following conditions are met:
1. Redistributions in source form must retain copyright statements and
   notices,
2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided with
   the distribution, and
3. Redistributions must contain a verbatim copy of this document.
The OpenLDAP Foundation may revise this license from time to time. Each
revision is distinguished by a version number. You may use this
Software under terms of this license revision or under the terms of any
subsequent revision of the license.
THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING
BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF
THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing in
this Software without specific, written prior permission. Title to
copyright in this Software shall at all times remain with copyright
holders. OpenLDAP is a registered trademark of the OpenLDAP Foundation.
Copyright 1999-2003 The OpenLDAP Foundation,Redwood City,California,USA.
All Rights Reserved. Permission to copy and distribute verbatim copies
of this document is granted.

--- End of License Text ---
```

1.3 Konzept des Handbuchs

Das Handbuch gliedert sich analog zu den Bestandteilen von SECOS in separate Kapitel. Diese Kapitel können unabhängig voneinander zu Rate gezogen werden.

In jedem Kapitel zu einem Bestandteil folgen auf die Einführung die alphabetische Beschreibung von Kommandos und die alphabetische Beschreibung von Makros (sofern Makros zur Verfügung stehen). Jeweils am Ende dieser Kapitel befinden sich Hinweise zur Installation und Inbetriebnahme.

Beispiele folgen den Abschnitten, die sie verdeutlichen sollen.

Für jedes Kommando ist im einführenden Abschnitt der Funktionsbereich und die notwendige Privilegierung vermerkt. Benutzer, die keines der aufgeführten Privilegien besitzen, können das Kommando nicht ausführen.

1.4 Readme-Datei

Ergänzungen gegenüber den Handbüchern sind gegebenenfalls in den Readme-Dateien zu den jeweiligen Produktversionen aufgeführt. Solche Readme-Dateien finden Sie sowohl auf der jeweils aktuellen SoftBooks-DVD als auch unter *http://manuals.ts.fujitsu.com* bei dem jeweiligen Produkt.

Ergänzende Produkt-Informationen

Aktuelle Informationen, Versions-, Hardware-Abhängigkeiten und Hinweise für Installation und Einsatz einer Produktversion enthält die zugehörige Freigabemitteilung. Solche Freigabemitteilungen finden Sie unter *http://manuals.ts.fujitsu.com*.

1.5 Änderungen gegenüber der vorherigen Ausgabe

Die Änderungen zur SECOS-Komponente SAT sind im Handbuch „SECOS - Security Control System - Beweissicherung“ [1] beschrieben.

Änderungen mit SECOS V5.4

– Erweiterung der Kommandos ADD-USER-GROUP / MODIFY-USER-GROUP um die Benutzerattribute HARDWARE-AUDIT, LINKAGE-AUDIT, CRYPTO-SESSION und NET-STORAGE-USAGE. Die Wertebereiche für RESIDENT-PAGES und ADDRESS-SPACE-LIMIT wurden erweitert.
Bei SHOW-USER-GROUP werden entsprechende Ausgabeinformationen und S-Variablen angezeigt.

– Die Beschreibung der Kommandos ADD-USER, MODIFY-USER-ATTRIBUTES, MODIFY-USER-PUBSET-ATTRIBUTES und SHOW-USER-ATTRIBUTES entspricht dem Stand SRPMNUC V20.0.

– Bei dem Makro SRMSUG können mit VERSION=5 bzw. 6 neue Ausgabebereiche generiert werden.

– Die Zugangsklassen RBATCH-ACCESS und POSIX-SERVER-ACCESS wurden in SECOS V5.4 letztmalig unterstützt und entfallen ab SECOS V5.5:

– Die entsprechenden Operanden in den Kommandos MODIFY-LOGON-DEFAULTS, MODIFY-LOGON-PROTECTION, SET-LOGON-DEFAULTS, SET-LOGON-PROTECTION, SHOW-LOGON-PROTECTION entfallen. Die entsprechenden Ausgabefelder und S-Variablen entfallen bei SHOW-LOGON-DEFAULTS und SHOW-LOGON-PROTECTION.

Änderungen mit SECOS V5.5

SECOS V5.5 wird unterstützt in Systemen mit BS2000 OSD/BC ab V10.0. Bestimmte Funktionen sind jedoch nur für Systeme mit BS2000 OSD/BC > V11.0A verfügbar.
Auf solche Abhängigkeiten wird an den entsprechenden Stellen im Handbuch explizit hingewiesen.

– SECOS unterstützt Verbindungen mit folgenden Verschlüsselungsarten:
  – DES-CBC-CRC
  – DES-CBC-MD5
  – ARCFOUR-HMAC
  – AES128-CTS-HMAC-SHA1-96
  – AES256-CTS-HMAC-SHA1-96

– Im Kommando SHOW-LOGON-PROTECTION entfallen die S-Variablen für RBATCH und POSIX-SERVER-ACCESS.

– Im Makro SRMSUG kann mit VERSION=6 ein Ausgabe- bzw. Parameterbereich für SECOS ab Version V5.4A generiert werden.

Bei den folgenden Änderungen ist zu beachten, dass die Änderungen nur für Systeme mit BS2000 OSD/BC > V11.0A gelten!

– In den Kommandos SET- und MODIFY-LOGON-PROTECTION wird die Einschränkung im Operanden PERSONAL-LOGON=*PRIVILEGED aufgehoben.

– Im Kommando SHOW-LOGON-PROTECTION zeigt die Ausgabe mit SCOPE=*ALL neben den explizit festgelegten Attributen auch die aktuellen Standard-Attribute für die Zugangskontrolle an.
Neue S-Variablen (z.B. var(*LIST).DIALOG.ACCESS-DEF) zeigen für das jeweilige Attribut an, ob die Einstellung dem Standard-Attribut entspricht.

Allgemeine Hinweise

Die SRPM-Kommandoübersichten (siehe Abschnitt „SRPM-Kommandos“ auf Seite 124) enthalten auch die Kommandos der Komponente SRPMNUC, die zum BS2000-Grundausbaus gehört. Diese Kommandos werden ausschließlich im Handbuch "Kommandos" [4] der jeweiligen BS2000-Version beschrieben.

Die Bezeichnung des BS2000-Grundausbaus lautet ab Version V10.0: BS2000 OSD/BC. Vorgängerversionen werden mit der bis dahin üblichen Bezeichnung BS2000/OSD-BC zitiert.

1.6 Verwendete Metasprache

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

- Literaturhinweise werden im Text in Kurztiteln angegeben. Der vollständige Titel jeder Druckschrift, auf die durch eine Nummer verwiesen wird, ist im Literaturverzeichnis hinter der entsprechenden Nummer aufgeführt.
- In den Beispielen sind Benutzereingaben und Systemausgaben in `Schreibmaschinenschrift` wiedergegeben.
- Besondere Hinweise auf Metasprache oder verwendete Symbole, die nur für einen Unterbestandteil gelten, finden sich zu Beginn des Kapitels zu diesem Unterbestandteil.
- Die Metasyntax für SDF-Kommandos und -Anweisungen, die Darstellung von Kommando-Returncodes und S-Variablen finden Sie im Handbuch „Kommandos“ [4].
- Die Metasyntax für Makros finden Sie im Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Dieses Symbol steht zusammen mit dem Signalwort **ACHTUNG!** vor Warnhinweisen, die Sie im Interesse der System- und Betriebssicherheit unbedingt beachten müssen.

Dieses Symbol kennzeichnet wichtige Hinweise, die Sie unbedingt beachten sollten.

2 Sicherheit in DV-Systemen und im BS2000

In vielen Firmen und Institutionen werden heute Daten in DV-Systemen gespeichert und verarbeitet, die für den Einzelnen oder für eine ganze Organisation von eminenter Wichtigkeit sind. Neben Funktionalität und Performance ist deshalb ein neuer Aspekt in den Vordergrund getreten: die Sicherheit von DV-Systemen.

Benutzer von DV-Systemen haben das berechtigte Bedürfnis nach Vertraulichkeit und Integrität der gespeicherten Informationen - sei es der langjährig erarbeitete Wissensvorsprung eines Industrieunternehmens gegenüber seinen Konkurrenten, die Daten über eine bestimmte Personengruppe bei einer Finanzbehörde oder der Kontostand eines Sparers bei einer Bank. Die Gründe für die Wichtigkeit des Themas „Sicherheit in DV-Systemen“ sind vielfältig und werden durch die Bemühungen der Hardware- und Software-Hersteller verdeutlicht.

Ziel dieser Bemühungen ist es, die missbräuchliche Verwendung, die Verfälschung bzw. den Verlust von vertraulichen Informationen bei ihrer Verarbeitung und Speicherung in DV-Systemen zu verhindern.

Beeinträchtigungen der Sicherheit können auf vielfältige Weise verursacht werden:

– durch menschliches Fehlverhalten, wie Drücken einer falschen Taste, Start eines falschen Programms, Verlust eines Speichermediums etc.,

– durch spielerischen Forscherdrang des Benutzers,

– durch kriminelle Aktivitäten, angefangen vom jugendlichen Hacker, der auf seine Fähigkeiten durch eine originelle Meldung aufmerksam machen möchte, bis zum professionellen Spionageteam, das wirtschaftliche oder militärische Geheimnisse ausspähen will,

– durch Hardware- oder Software-Fehler, wie Funktionsstörungen der CPU, Übertragungsfehler, Programmfehler etc.,

– durch höhere Gewalt, wie Stromausfall, Feuer, Wassereinbruch, Erdbeben etc.

Der Gesetzgeber hat sich des Themas Datenschutz schon vor längerer Zeit angenommen. Bundes- und Landesdatenschutzgesetze sowie diverse Rechtsvorschriften regeln den Umgang mit personenbezogenen Daten. Sicherheitskriterien legen die Anforderungen an die Sicherheit von DV-Systemen fest. Für die Hardware- und Software-Hersteller stellt sich heute und für die Zukunft die Aufgabe, die technische Basis für die Sicherheit von DV-Systemen und damit für die Realisierung des Datenschutzes zu schaffen und weiterzuentwickeln. Technische Sicherheitseinrichtungen eines Herstellers bleiben jedoch weitgehend nutzlos, wenn sie nicht durch organisatorische Maßnahmen des Benutzers ergänzt werden. Die Verantwortung für den Datenschutz trägt allein der Benutzer eines DV-Systems. Um Datenschutz zu erreichen, muss er zusätzlich und eigenverantwortlich

– die gesetzlichen Vorschriften zum Datenschutz beachten,
– die Grundsätze und Richtlinien seines Unternehmens zum Datenschutz einhalten und
– beim Umgang mit zu schützenden Daten problembewußt handeln.

2.1 Allgemeine Bedrohungen von DV-Systemen

In Abhängigkeit von der Aufgabe und der Einsatzumgebung sowie der Sensibilität der gespeicherten Informationen kann man drei allgemeine Bedrohungen unterscheiden, die die Sicherheit eines DV-Systems gefährden (siehe Bild 1):

– den Verlust der Vertraulichkeit
– den Verlust der Integrität
– den Verlust der Verfügbarkeit

Diese Grundbedrohungen gilt es durch geeignete Maßnahmen in der Einsatzumgebung des DV-Systems sowie im DV-System selbst zu verringern und im Idealfall ganz auszuschalten.

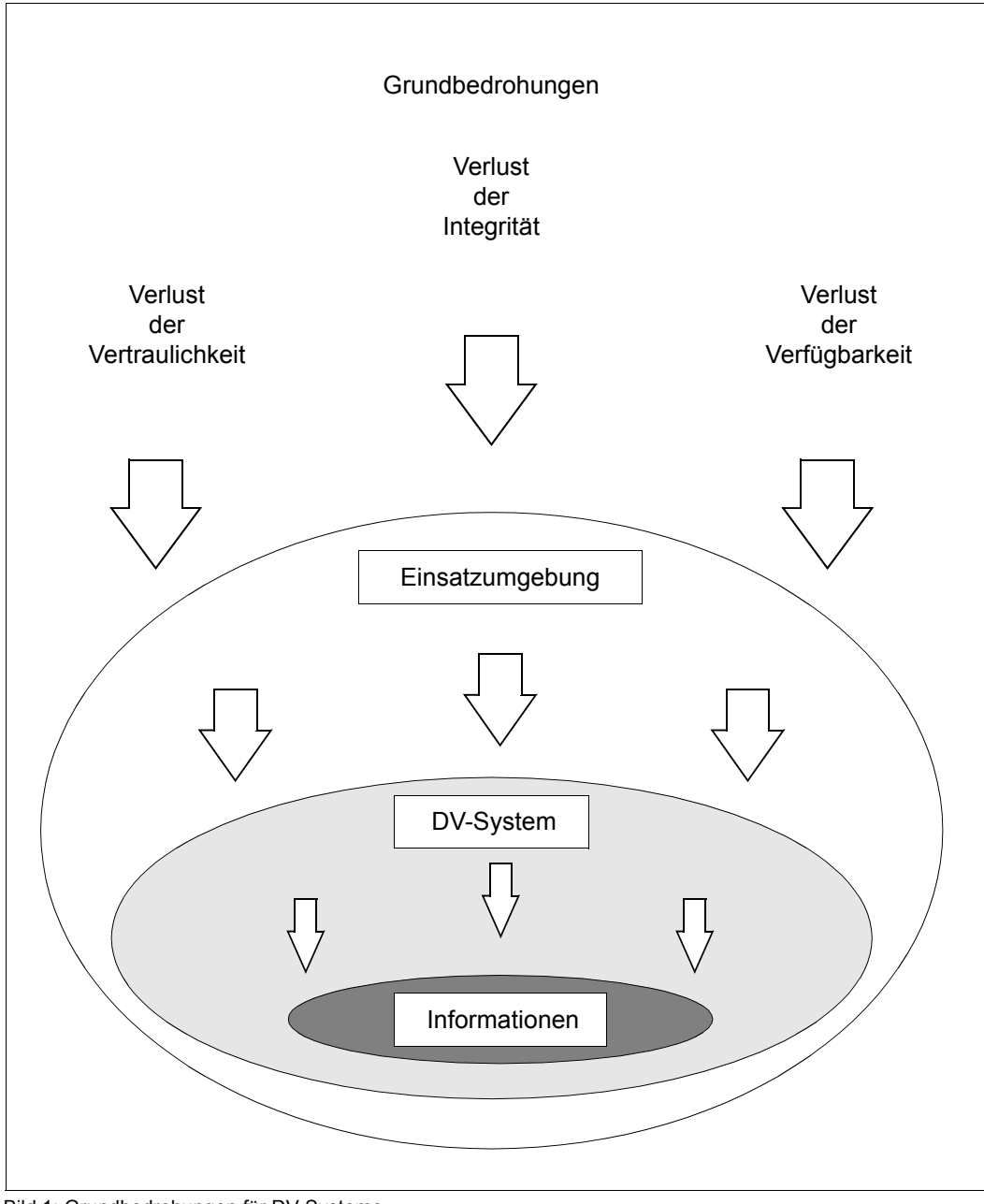


Bild 1: Grundbedrohungen für DV-Systeme

Verlust der Vertraulichkeit

Die Vertraulichkeit der in einem DV-System gespeicherten Informationen ist dann gewährleistet, wenn eine unberechtigte Kenntnisnahme und damit ein Informationsgewinn durch unbefugte Personen ausgeschlossen werden kann. Der Verlust der Vertraulichkeit ist gegeben, wenn die gespeicherten Informationen nicht mit der notwendigen Sorgfalt bezüglich ihrer Geheimhaltung behandelt werden können. Schutzwürdige Informationen dürfen prinzipiell nur denjenigen Personen zugänglich sein, die diese Informationen für die Erfüllung ihrer Aufgaben unbedingt benötigen bzw. für den Zugriff eine besondere Autorisierung besitzen. Die Möglichkeit der unberechtigten Kenntnisnahme von Informationen kann in einem Betriebssystem z.B. durch den Einsatz wirksamer Zugangsschutz- und Zugriffsschutzmechanismen oder durch Verschlüsselung aller Informationen bedeutend verringert werden.

Verlust der Integrität

Die Integrität von gespeicherten Informationen setzt drei Eigenschaften voraus:

– ihre Vollständigkeit

– ihre Unversehrtheit

– ihre Korrektheit

Die Vollständigkeit der Informationen bedeutet hier, dass bei jeder Verarbeitung alle benötigten Informationen vorhanden sein müssen.

Mit der Unversehrtheit der Informationen ist ihre fehlerlose Speicherung gemeint.

Unter der Korrektheit der Informationen versteht man ihre fehlerfreie Abbildung aus der realen Welt.

Der Verlust der Integrität von gespeicherten Informationen kann durch Fehler oder durch unberechtigte Modifikation der Informationen bewirkt werden. Der konsequente Einsatz von Zugangsschutz- und Zugriffsschutzmechanismen trägt dazu bei, die Integrität der gespeicherten Informationen zu sichern.

Verlust der Verfügbarkeit

Die Verfügbarkeit eines DV-Systems ist dann gegeben, wenn sämtliche gespeicherten Informationen und alle Systemfunktionen (Hardware- bzw. Software-Komponenten) zu jedem Zeitpunkt, zu dem sie benötigt werden, in ihrem vollen Umfang benutzt werden können. Der Verlust der Verfügbarkeit kann durch Fehler, aber auch durch unberechtigte Eingriffe in die Hardware- bzw. Software-Konfiguration bewirkt werden. Zur Erhöhung der Verfügbarkeit eines DV-Systems dient daher auch der Einsatz wirkungsvoller Zugangsschutz- und Zugriffsschutzmechanismen.

2.2 Technische Sicherheitsmaßnahmen im BS2000

Zu den wichtigsten technischen Sicherheitsmaßnahmen zählen Maßnahmen für den Zugangsschutz, den Zugriffsschutz und die Protokollierung, wie sie für das BS2000 mit folgenden Funktionseinheiten im Sicherheitspaket SECOS angeboten werden.

SRPM	(System Ressources and Privileges Management),
GUARDS	(Generally Usable Access contRol aDministration System)
GUARDDEF	(GUARDs DEFault protection)
GUARDCOO	(GUARDs COOwner protection)
SAT	(Security Audit Trail)
SECOS-KRB	(Kerberos-Authentisierung)

2.3 Sicherheitskonzeption des BS2000

Das BS2000 ist ein Universal-Betriebssystem, das durch seine Betriebsarten den dialogorientierten Teilnehmer- und Teilhaberbetrieb ebenso wie den Batchbetrieb unterstützt. Seine Sicherheitsfunktionen gewährleisten, dass eine Vielzahl von Benutzern die gebotenen Systemdienstleistungen unabhängig voneinander nutzen kann, ohne sich - sei es zufällig oder absichtlich - gegenseitig zu stören. Alle Sicherheitsfunktionen sind Bestandteile des Betriebssystems und seiner Subsysteme.

Der folgende Abschnitt beschreibt die grundlegenden Aufgabenbereiche, die im Teilnehmerbetrieb des BS2000 unterschieden werden können, und stellt auf diesem Hintergrund die Grundsätze vor, auf denen die Sicherheitskonzeption des Betriebssystems basiert.

2.4 Grundlegende Aufgabenbereiche im BS2000

Das BS2000 unterscheidet im Teilnehmerbetrieb drei verschiedene Arten von Systembenutzern:

– die nicht-privilegierten Benutzer
– die Systemverwaltung
– die Systembedienung

Den verschiedenen Arten von Systembenutzern lassen sich unterschiedliche Aufgabenbereiche zuordnen. Jeder Aufgabenbereich ist mit bestimmten Funktionen und Rechten ausgestattet. Benutzer im Teilnehmerbetrieb sind im Regelfall die überwiegende Mehrzahl der Systembenutzer. Die Systemverwaltung und Systembedienung ist dagegen einer kleinen Anzahl besonders autorisierter Personen vorbehalten.
Im BS2000 können die Aufgaben eines Aufgabenbereichs von mehreren Personen ausgeführt werden; eine Person kann aber ebenso in mehreren Aufgabenbereichen tätig sein. Ein Betreiber des BS2000 hat so die Möglichkeit, die Aufteilung der Benutzerwelt entsprechend seines individuellen Sicherheitsbedarfs vorzunehmen.

Aufgabenbereich des Benutzers im Teilnehmerbetrieb

Der Benutzer im Teilnehmerbetrieb des BS2000 kann Dialog- und Batchverarbeitung nutzen. Ihm stehen als nicht-privilegiertem Systembenutzer über Kommandos, Makros und Dienstprogramme bestimmte Dienstleistungen des Betriebssystems zur Verfügung. Diese umfassen i.A.:

– das Erzeugen, Starten und Steuern von Programmen
– das Erzeugen, Starten und Steuern von Kommandoprozeduren
– das Anfordern von Betriebsmitteln
– den Aufruf spezieller Betriebssystemfunktionen

Für die Ausführung dieser Tätigkeiten bietet das BS2000 eine einheitliche Kommando- und Anweisungsoberfläche sowie eine Programmieroberfläche an.

Aufgabenbereich der Systemverwaltung

Die Systemverwaltung des BS2000 umfasst die Planung und Steuerung des Systembetriebs gemäß strategischer Vorgaben des Betreibers.

Die Systemverwaltung ist zuständig für privilegierte Verwaltungsaufgaben, um einen ordnungsgemäßen Systembetrieb des BS2000 zu gewährleisten und bei Störfällen geeignete Maßnahmen ergreifen zu können. Eine Sonderstellung innerhalb der Systemverwaltung nimmt der Sicherheitsbeauftragte ein. Ihm obliegt die Verwaltung der Systemverwaltungsrechte.

An die Systemverwaltung sind im Allgemeinen folgende Aufgaben geknüpft:

– die Bereitstellung des Systems
– die Auftragsabwicklung und Performance-Überwachung
– die Verwaltung aller Benutzerkennungen und Benutzergruppen
– die SPOOL-Verwaltung
– die Sicherung der Datenbestände der Benutzer
– die Vergabe und der Entzug von Systemverwalter-Privilegien
– die Änderung der Software-Konfiguration
– die Anpassung der Software an geänderte Hardware-Konfigurationen
– die Auswertung von Abrechnungsdaten, Betriebsdaten, Protokollen und Systemfehlerunterlagen
– die Hardware- und Software-Wartung

Zur Ausführung dieser Aufgaben stehen der Systemverwaltung eine ihren Privilegien entsprechende Ausprägung der Kommando- und Anweisungsoberfläche sowie Programmschnittstellen zur Verfügung, mit denen jederzeit in den laufenden Systembetrieb eingegriffen werden kann und die den Zugriff auf alle Dateien, Tabellen und Programme des Systems und aller Benutzer gestatten.

Aus der Menge der Systemverwalter-Privilegien können von der Systemverwaltung bestimmte Privilegien herausgelöst und einzelnen Anwendern im Teilnehmerbetrieb zugeteilt werden (siehe Kapitel „SRPM – Privilegien und Betriebsmittel verwalten“ auf Seite 39 ff). Der Aufgabenbereich der Systemverwaltung kann sich infolgedessen mit dem Aufgabenbereich des Benutzers im Teilnehmerbetrieb überschneiden. Ein typisches Beispiel hierfür ist die Benutzerverwaltung. Sie ist zuständig für die hierarchische Strukturierung der Systembenutzer durch Benutzergruppen und die Verwaltung der Benutzergruppenstruktur.

Aufgabenbereich der Systembedienung

Die Systembedienung des BS2000 ist zuständig für die Steuerung und Überwachung des laufenden Systembetriebs und der Peripherie gemäß den Vorgaben der Systemverwaltung.

Die Systembedienung hat folgende Aufgaben:

– die Inbetriebnahme des Systems
– die Betreuung und Steuerung des laufenden Betriebs
– die manuelle Unterstützung des Betriebs

Der Systembedienung stehen direkt mit der Zentraleinheit verbundene Bedienplätze, die Konsolen, zur Verfügung. Für die Erfüllung ihrer Aufgaben verfügt die Systembedienung über einen speziellen Kommandosatz, mit dem sie privilegierte Funktionen ausführen kann.

2.5 Sicherheitsgrundsätze für den Benutzer

Zugangsschutz (Identifizierung, Authentisierung)

Natürliche Personen benötigen eine Benutzerkennung, um Zugang zum BS2000 zu erhalten und mit dem Betriebssystem arbeiten zu können:

– Eine Person kann mehrere verschiedene Benutzerkennungen besitzen. Sie wird dann vom BS2000 aber so bedient, als würde es sich um getrennte Personen handeln.

– Mehrere Personen können gemeinsam eine Benutzerkennung besitzen. Sie werden dann aber bezüglich der Abwicklung ihrer Tätigkeiten vom BS2000 nicht voneinander unterschieden. Nur im Rahmen der Beweissicherung wird beim Einsatz der persönlichen Identifizierung (siehe Seite 105) oder beim Einsatz von Single Sign On (siehe Seite 109) eine personenbezogene Unterscheidung getroffen.

Die rechtmäßige Verwendung einer Benutzerkennung wird bei jedem Systemzugang durch ein Identifizierungs- und Authentisierungsverfahren überprüft. Dabei wird nach erfolgter Identifizierung eine Verifikation der Identität z.B. durch Kennwortverfahren durchgeführt.

Das BS2000 unterscheidet folgende Zugangsklassen:

– DIALOG
– BATCH
– OPERATOR-ACCESS-TERMINAL
– OPERATOR-ACCESS-PROGRAM
– OPERATOR-ACCESS-CONS
– POSIX-RLOGIN-ACCESS
– POSIX-REMOTE-ACCESS
– NET-DIALOG-ACCESS

Jede Zugangsklasse kann durch ein Kennwortverfahren geschützt werden. Durch getrenntes Sperren einzelner Zugangsklassen kann der Systemzugang für eine Benutzerkennung weiter eingeschränkt werden.

Die Möglichkeiten der Operator-Authentisierung sind detailliert im Handbuch „Einführung in die Systembetreuung“ [2] beschrieben.

Die Möglichkeiten der POSIX-Authentisierung sind detailliert im Handbuch „POSIX“ [25] beschrieben.

Die Kennwörter zur Authentisierung können über den Systemparameter ENCRYPT einwegverschlüsselt im System gespeichert werden.

Fehlversuche bei der Kennworteingabe werden mit Zeitstrafen oder Verbindungsabbau geahndet.

Zugriffsschutz (Rechteverwaltung, Rechteprüfung)

Der Zugriffsschutz für ein Objekt wird durch Eigentümer und Miteigentümer des Objekts bestimmt. Eigentümer ist immer eine Benutzerkennung. Miteigentümer ist standardmäßig die Benutzerkennung TSOS. Für Dateien (auch Bibliotheken) und Jobvariablen können weitere Benutzerkennungen als Miteigentümer festgelegt werden. Außerdem kann für diese Objekte die Miteigentümerschaft der Benutzerkennung TSOS eingeschränkt werden. Nur die unter der Benutzerkennung des Eigentümers oder eines Miteigentümers erzeugten Aufträge können die Zugriffsrechte auf ein Objekt für Benutzerkennungen festlegen und ändern.

Objekte, die der Zugriffskontrolle unterliegen, sind:

- Dateien (gemeinschaftliche Plattendateien, Dateien auf privaten Datenträgern, Dateigenerationen)
- Jobvariable
- Datenträger
  (private Plattenspeicher, Magnetbänder, Magnetbandkassetten)
- Memory-Pools
- FITC-Ports
- Bibliothekselemente
- User Serialization Items
- User Event Items

Zugriffe auf Dateien, Bibliothekselemente und FITC-Ports werden bis auf die Ebene einzelner Benutzer kontrolliert. Zugriffsrechte werden je nach Art des Objekts durch Kennwörter oder andere Zugriffsschutzmechanismen festgelegt. Die Zugriffsrechte werden je nach Art des Objekts beim Zugriff kontrolliert.

Auftragsbeschreibungen für Batch- oder Ausgabeaufträge sowie gestartete Batch- oder Ausgabeaufträge sind einer Benutzerkennung zugeordnet. Sie können von Aufträgen dieser Benutzerkennung und ggf. von der Systembedienung geändert oder beeinflusst werden.

Das Eigentümerrecht einer Benutzerkennung an Objekten, Auftragsbeschreibungen und gestarteten Aufträgen kann additiv von einer Benutzerkennung der Systemverwaltung wahrgenommen werden.

Das Eigentümerrecht an Dateien (auch Bibliotheken) und Jobvariablen kann darüber hinaus auch an weitere Miteigentümer vergeben werden.

Wiederaufbereitung von Speicherobjekten

Speicherobjekte sind Objekte, deren Informationen in einem Speicherbereich abgelegt sind. BS2000 sorgt dafür, dass bei Zuordnung von Objekten zu einem neuen Benutzer kein Zugriff auf den früheren Inhalt möglich ist. Diese Mechanismen zur Wiederaufbereitung verhindern den Informationsfluss zwischen je zwei Nutzungen desselben Speicherobjekts durch unterschiedliche Benutzer. Dies geschieht durch Löschen des früheren Inhalts.

Objekte, die der Wiederaufbereitung des BS2000 unterliegen, sind:

- Dateien
- Jobvariablen
- Speicherseiten des Adressraums
- Memory-Pools
- Magnetbänder und Magnetbandkassetten
- User Serialization Items
- User Event Items

Das Löschen der Inhalte wird je nach Art des Objekts durch ein automatisches, systemgesteuertes, benutzergerechtes oder durch ein organisatorisches Verfahren durchgeführt.

Beweissicherung

Zur Rückverfolgung von Aktionen eines Benutzers können sowohl vom Sicherheitsbeauftragten gesteuerte Systemprotokolle (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1]) als auch vom Benutzer selbst steuerbare auftragsbezogene Ablaufprotokolle erzeugt werden:

- Benutzerprotokolle des Auftragsablaufs im Dialogbetrieb umfassen alle Ein- und Ausgaben an einer Datensichtstation. Benutzerprotokolle des Auftragsablaufs im Batchbetrieb enthalten alle Kommandos und die durch sie bewirkten Ereignisse. In beiden Fällen werden Kennwortangaben durch Pseudozeichen ersetzt.
- Die Protokollierung von Daten zur Benutzer- und Betriebsabrechnung kann vom Benutzer durch eigene Abrechnungssätze ergänzt werden.
- Die Protokollierung sicherheitsrelevanter Ereignisse zu Revisionszwecken wird vom Sicherheitsbeauftragten festgelegt. Der Benutzer kann bei entsprechender Berechtigung die Protokollierung von Zugriffen auf Objekte, deren Eigentümer er ist, selbst steuern.

Benutzer mit besonderen Berechtigungen können angehalten sein, die Protokollierung ihrer Aktionen einzuschalten, um Systemprotokolle zu ergänzen.

2.6 Sicherheitskriterien

Mit dem Grundausbau des BS2000 steht zusammen mit SECOS ein Betriebssystem zur Verfügung, das so entwickelt und produziert wurde, dass es die Funktionsklasse F2 und Qualitätsstufe Q3 der IT-Sicherheitskriterien erfüllt. Definition und Umfeld dieser Sicherheitskriterien sind im Handbuch „IT-Sicherheitskriterien“ [35] beschrieben.

Die Funktionalitätsklasse F2 wird durch folgende fünf Grundfunktionen festgelegt (vereinfachter Auszug):

1. Identifizierung und Authentisierung
   Benutzer müssen vor einer Interaktion mit dem Betriebssystem identifiziert und authentisiert werden. Bei jeder durchgeführten Interaktion muss das System die Identität des Benutzers feststellen können.
2. Rechteverwaltung
   Vom System sind Zugriffsrechte zwischen Benutzern (Subjekten) und Objekten zu verwalten. Die Zugriffsrechte müssen für jeden Benutzer separat festgelegt werden können. Die Weitergabe von Zugriffsrechten muss kontrollierbar sein.
3. Rechteprüfung
   Bei jedem Zugriffsversuch von Benutzern auf Objekte, die der Rechteverwaltung unterliegen, muss das Betriebssystem die Berechtigung hierzu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden.
4. Beweissicherung
   Das System muss eine Protokollierungskomponente enthalten, die in der Lage ist, sicherheitsrelevante Ereignisse zu protokollieren. Dies sind z.B. Benutzung des Identifikations- und Authentisierungsmechanismus, der Zugriff auf Objekte und Aktionen von Benutzern mit besonderen Rechten.
5. Wiederaufbereitung
   Alle Speicherobjekte müssen vor einer Wiederverwendung durch andere Benutzer so aufbereitet werden, dass keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

Die Qualitätsstufe Q3 besteht aus der Sicht des Betreibers in Aspekten der Betriebsqualität und der Abgrenzung zu nicht zu bewertenden Systemteilen (siehe Handbuch „IT-Sicherheitskriterien“ [35]). Dies sind:

1. Nachvollziehbarkeit des Systemstarts.
2. Nachweis von Fehlern beim Einspielen von Software.
3. Verhindern von nichtprotokollierten Eingriffen beim Starten des Systems.
4. Abschottung der nicht zu bewertenden Teile des Systems von denen, die bewertet wurden, um Mißbrauch, Vortäuschen und Umgehen von Sicherheitsfunktionen zu verhindern.

Bedeutung der Sicherheitskriterien für den Benutzer

Ist ein Betriebssystem nach F2/Q3 entwickelt und produziert, so bedeutet das:

1. Die Bestandteile des Betriebssystems wurden nach den Qualitätskriterien Q3 entwickelt; es stehen die Grundfunktionen sicherer Systeme entsprechend F2 bereit.
2. Auf dieser Grundlage ist die Systemverwaltung in der Lage, einen sicheren Rechenbetrieb einzurichten und zu gewährleisten.
3. Der konkrete Umfang an Maßnahmen zur Realisierung von F2/Q3 wird von der Sicherheitspolitik des Benutzers entsprechend des realen Umfelds in seinem Einsatzfall bestimmt.

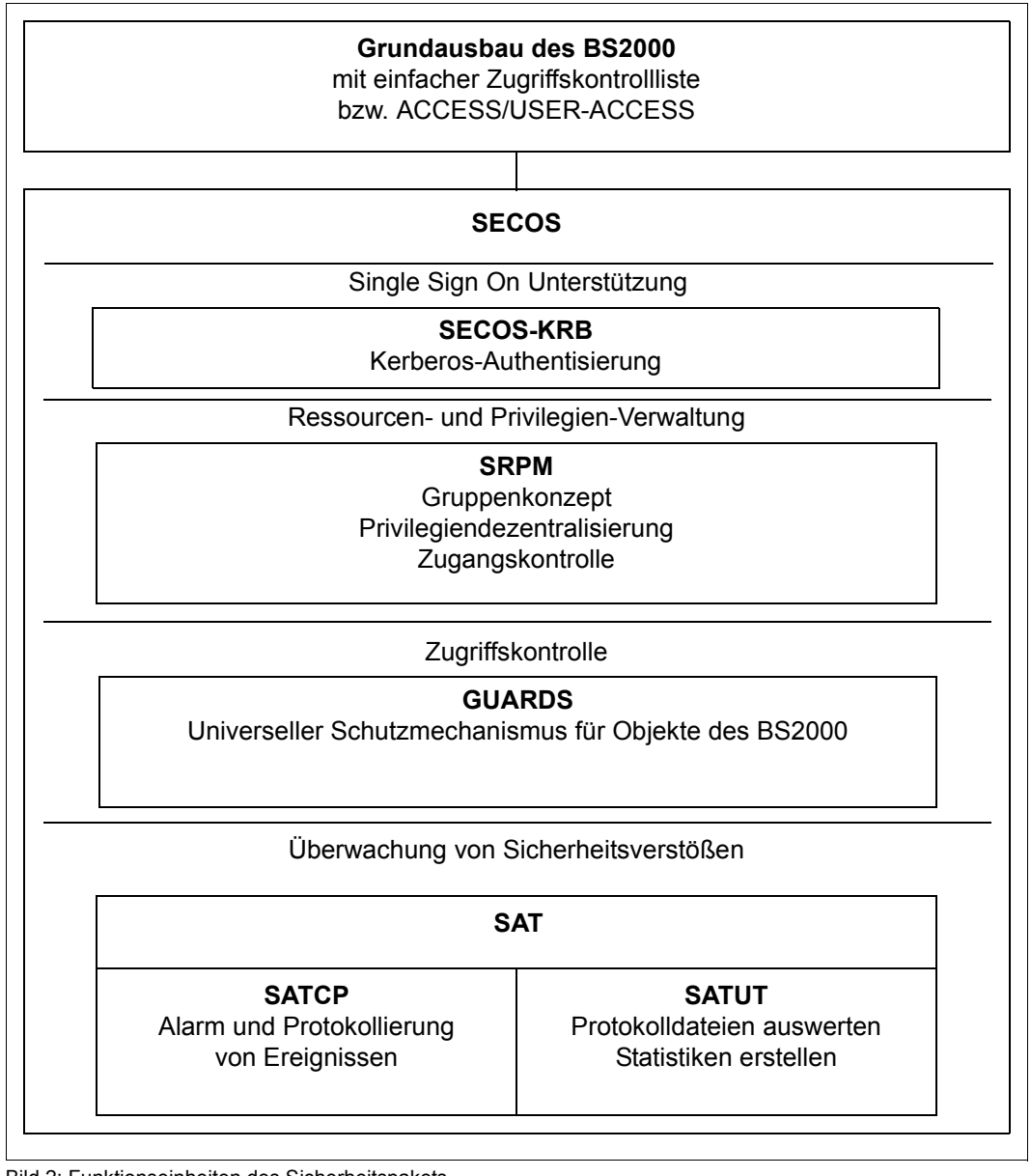


Bild 2: Funktionseinheiten des Sicherheitspakets

3 SRPM – Privilegien und Betriebsmittel verwalten

Betriebsmittel und Privilegien werden im BS2000 gewöhnlich von der Kennung TSOS verwaltet. SRPM erlaubt, diese Aufgaben auch für andere Benutzerkennungen zuzulassen, die Aufgaben also zu verteilen. Die Privilegien, Betriebsmittel zu verwalten, werden im folgenden „systemglobale Privilegien“ genannt. Die Aufteilung der systemglobalen Privilegien bedeutet, dass ein bestimmter Aufgabenbereich der Systembetreuung mit den dazu erforderlichen Systemfunktionen unter der Kennung abgewickelt werden kann, die das entsprechende systemglobale Privileg besitzt. Der volle Privilegienumfang steht damit nicht mehr nur einer einzelnen Kennung zur Verfügung.

Diese Maßnahme bewirkt zum einen eine Entlastung für die Systembetreuung. Zum anderen wird durch die Verteilung der Privilegien die Sicherheit im Rahmen der Systembetreuung erhöht, weil z.B. der Kreis derer kleiner wird, die für anfallende Routinearbeiten das TSOS-Kennwort kennen müssen. Durch gezielte Vergabe oder Entzug von systemglobalen Privilegien für Benutzerkennungen kann für die Abwicklung der Systembetreuung eine auf das jeweilige Rechenzentrum zugeschnittene Aufgabentrennung erreicht werden.

3.1 Privilegien verwalten

Folgende systemglobale Privilegien gibt es:

Bedeutung des Privilegs	Name des Privilegs
Alias-Katalog-Verwaltung	ACS-ADMINISTRATION
Vorgenerierte Privilegien	CUSTOMER-PRIVILEGE-1 . . CUSTOMER-PRIVILEGE-8
File-Transfer-Verwaltung	FT-ADMINISTRATION
FTAC-Verwaltung	FTAC-ADMINISTRATION [1]
Guard-Administration	GUARD-ADMINISTRATION
Hardware-Online-Wartung	HARDWARE-MAINTENANCE
HSMS-Verwaltung	HSMS-ADMINISTRATION
Netzverwaltung	NET-ADMINISTRATION
Notification-Service-Administration	NOTIFICATION-ADMINISTRATION
Systembedienung	OPERATING
POSIX-Benutzerverwaltung	POSIX-ADMINISTRATION
SPOOL-Verwaltung	PRINT-SERVICE-ADMINISTRATION
Verwaltung des PROP-XT	PROP-ADMINISTRATION [2]
SAT-Datei-Auswertung	SAT-FILE-EVALUATION
SAT-Datei-Verwaltung	SAT-FILE-MANAGEMENT
Sicherheitsverwaltung	SECURITY-ADMINISTRATION
Benutzerkommandos ausführen	STD-PROCESSING
Subsystem-Verwaltung	SUBSYSTEM-MANAGEMENT
Software-Monitor-Verwaltung	SW-MONITOR-ADMINISTRATION
Bandverwaltung	TAPE-ADMINISTRATION
Encryption-Key-Verwaltung für Bänder	TAPE-KEY-ADMINISTRATION
TSOS	TSOS
Benutzerverwaltung	USER-ADMINISTRATION
Verwaltung einer virtuellen Maschine	VIRTUAL-MACHINE-ADMINISTRATION
Verwaltung von VM2000	VM2000-ADMINISTRATION

[1] Vor Vergabe des Privilegs FTAC-Verwaltung sollte das Handbuch „Installation und Betrieb“ [11] der im Einsatz befindlichen openFT-Version konsultiert werden (siehe Seite 50).

[2] Mit Einsatz des Produkts PROP-XT wird dieses Privileg ausgewertet.

Wegen der entkoppelten Freigabe beachten Sie bitte die Freigabemitteilungen und Handbücher zu den genannten Produkten.

3.1.1 Rolle des Sicherheitsbeauftragten

Die Rolle des Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) ist für die Sicherheit eines Systems von zentraler Bedeutung. Deshalb unterliegt das Privileg einer besonderen Behandlung. Bei Auslieferung ist das Privileg des Sicherheitsbeauftragten an die Kennung SYSPRIV vergeben.

Die Rolle des Sicherheitsbeauftragten kann keiner anderen Kennung während des laufenden Betriebs zugeordnet werden. Soll eine andere Kennung als SYSPRIV die Rolle des Sicherheitsbeauftragten übernehmen, so ist es mit dem Startup-Parameterservice möglich, die Kennung zu wechseln. Hierzu müssen folgende Voraussetzungen erfüllt sein:

1. Es darf nur eine einzige Kennung Sicherheitsbeauftragter werden. Es darf deshalb in der Startup-Parameterdatei nur eine einzige Kennung angegeben werden.
2. Die Kennung muss bereits existieren.
3. Die Kennung darf auf dem Home-Pubset kein Sammelprivileg und keine Privilegien außer STD-PROCESSING oder (bereits) SECURITY-ADMINISTRATION besitzen.
4. Die Kennungen TSOS oder SYSAUDIT dürfen nicht angegeben werden.
5. Die Kennung darf auf dem Home-Pubset nicht Benutzerverwalter oder Gruppenverwalter sein.

Diese Bedingungen werden beim Startup überprüft. Tritt bei dieser Überprüfung ein Fehler auf oder ist in der Startup-Parameterdatei kein Eintrag für die Kennung des Sicherheitsbeauftragten vorhanden, bleiben die Werte der vorigen Sitzung erhalten, wenn der Startup kein First-Start ist. Wenn der Startup ein First-Start ist, wird die Kennung SYSPRIV zur Kennung des Sicherheitsbeauftragten.

Die Beschränkungen bei der Ernennung des Sicherheitsbeauftragten und SAT-Datei-Verwalters bezüglich der Benutzerkennungen und koexistierender Privilegien und Rechte können bei Bedarf aufgehoben werden (siehe Abschnitt „Zentralisierte Administration“ auf Seite 45).

Wird in der laufenden Sitzung ein Pubset importiert, auf dem die Kennung Verwalter einer Benutzergruppe ist, sorgt die SRPM-Verwaltung dafür, dass der Sicherheitsbeauftragte „illegale“ Kommandos nicht ausführen kann, obwohl diese Kommandos auf Grund seiner Rechte als Gruppenverwalter eigentlich statthaft wären. Das Privileg SECURITY-ADMINISTRATION überlagert diese Berechtigung.

In die Startup-Parameterdatei muss zum Wechsel der Rolle des Sicherheitsbeauftragten Folgendes eingetragen werden:

```
/BEGIN SRPM
SECADM USER-ID=<USERID>
/EOF
```

Für <userid> ist der Name der neuen Kennung einzutragen.

Beim Startup werden folgende Schritte unternommen:

– für die neue Kennung wird das Privileg SECURITY-ADMINISTRATION gesetzt, das Privileg STD-PROCESSING wird entzogen.

– die SAT-Protokollierung wird eingeschaltet; die Kennung gilt für eine Änderung der Protokollierungseinstellung als nicht schaltbar.

– der Kennung, die in der vorigen Sitzung der Sicherheitsbeauftragte war, wird das Privileg SECURITY-ADMINISTRATION entzogen, das Privileg STD-PROCESSING wird gesetzt.

– die SAT-Protokollierung bleibt für diese Kennung eingeschaltet, kann jedoch ausgeschaltet werden.

3.1.2 Sammelprivilegien

Es ist dem Sicherheitsbeauftragten möglich, systemglobale Privilegien zu Sammelprivilegien mit einem frei wählbaren Namen zusammenzufassen.

Mit Hilfe der Sammelprivilegien können Berechtigungsprofile erstellt werden, die genau auf die Bedürfnisse des jeweiligen Anwenders zugeschnitten sind.

Ein Systemprivileg kann in mehreren Sammelprivilegien enthalten sein. Sammelprivilegien werden im Benutzerkatalog hinterlegt. Auf jedem Pubset können also andere Definitionen hinterlegt werden. Für die laufende Sitzung gelten die Definitionen des Home-Pubsets.

Für die **Sicherheitsverwaltung** ergeben sich folgende Vorteile:

– Sammelprivilegien werden zentral im Benutzerkatalog verwaltet. Im Benutzerkatalog ist für die Sammelprivilegien Folgendes hinterlegt:
  – Name und die Definition
  – Bei jedem Benutzer die Namen der zugewiesenen Sammelprivilegien.

  Da die Definitionen der Sammelprivilegien und die Zuweisung der Namen zu einem Benutzer voneinander unabhängig sind, können mit Hilfe einer geänderten Definition großen Gruppen von Kennungen mit nur einem Befehl Privilegien gegeben oder entzogen werden. Es gibt keinen Zeitverzug dadurch, dass jeder Kennung einzeln ein bestimmtes Privileg entzogen oder ein bestimmtes Privileg zugewiesen werden muss.

– der Sicherheitsverwalter bekommt einen schnellen Überblick über Verteilung und Zuordnung von Privilegien (siehe auch Abschnitt „SHOW-PRIVILEGE-SET Sammelprivileg-Definition anzeigen“ auf Seite 310).

Für den **Benutzer** haben Sammelprivilegien folgende Auswirkungen:

– ein Benutzer kann Sammel- und Einzelprivilegien besitzen.

– Ist einem Benutzer ein Sammelprivileg zugeordnet, stehen ihm alle Systemprivilegien des Sammelprivilegs zur Verfügung. Einzel- und Sammelprivilegien sind voneinander unabhängig. Besitzt eine Kennung bereits ein Privileg, welches ihr auch über ein Sammelprivileg zusteht, wird dieses Privileg durch eine Änderung des Sammelprivilegs nicht berührt, es bleibt der Kennung solange erhalten, bis es ihr explizit entzogen wird.

– Wird an einen Benutzer ein Sammelprivileg vergeben, so wird der Name des Sammelprivilegs bei der Benutzerkennung hinterlegt, nicht jedoch die Definition. Die Verbindung zwischen den Privilegien, die der Benutzer über das Sammelprivileg erhält und der Definition des Sammelprivilegs wird über den Namen des Sammelprivilegs hergestellt.

– Sammelprivilegien werden für die Regelung, dass jede Kennung mindestens ein Einzelprivileg besitzen muss, nicht berücksichtigt (siehe folgender Abschnitt „Regeln für die Privilegienvergabe“). Das bedeutet, der Fall „eine Kennung besitzt nur ein Sammelprivileg, aber kein Einzelprivileg“ kann nicht auftreten. Könnte eine Kennung als einziges Privileg nur ein Sammelprivileg besitzen, könnte der Fall eintreten, dass alle Privilegien aus einem Sammelprivileg entfernt werden und dann eine Kennung überhaupt kein Privileg mehr besitzt.

Sollen Privilegien in Gruppen an einzelne Kennungen vergeben werden, empfiehlt es sich wegen der zentralen Wart- und Kontrollierbarkeit, Privilegien als Sammelprivilegien zu vergeben. Selbst wenn ein Sammelprivileg nur ein Privileg enthält, kann durch die zentrale Änderungsmöglichkeit die schnellste Wirkung erzielt werden. So wird sichergestellt, dass bei einer Umorganisation nicht eine Kennung vergessen und so eine potenzielle Sicherheitsgefährdung durch die Hintertür eingeführt wird.

3.1.3 Regeln für die Privilegienvergabe

Eine Benutzerkennung kann mehrere Privilegien besitzen und ein Privileg kann an mehrere Kennungen vergeben sein (Ausnahme: SECURITY-ADMINISTRATION und TSOS). Eine Kennung kann ebenfalls über ein oder mehrere Sammelprivilegien oder Mischungen aus beidem verfügen. Ein Sammelprivileg kann an mehrere Kennungen vergeben sein.

Eine Kennung muss mindestens ein Einzelprivileg besitzen, da unter einer Kennung ohne Privileg keine sinnvolle Arbeit möglich ist. Aus diesem Grund erhält jede Kennung bei der Neueinrichtung (angelegt mit ADD-USER) das Privileg STD-PROCESSING, sofern kein anderes Privileg angegeben wird. Systemkennungen erhalten die für sie vorgesehenen Privilegien. Bis auf die Kennung des Sicherheitsbeauftragten können Kennungen im laufenden Betrieb Privilegien zugewiesen und entzogen werden.

Privilegien können vom Sicherheitsbeauftragten zu Sammelprivilegien zusammengefasst werden (siehe Abschnitt „Sammelprivilegien“ auf Seite 43 und Abschnitt „SRPM-Kommandos“ auf Seite 124f). Einer Kennung können mit dem Kommando SET-PRIVILEGE Einzel- oder Sammelprivilegien zugewiesen werden. Sammelprivilegien bleiben bei der Regelung, dass eine Kennung mindestens ein Einzelprivileg besitzen muss, unberücksichtigt, unabhängig davon wie viele Systemprivilegien in einem Sammelprivileg enthalten sind.

3.1.4 Zentralisierte Administration

Durch die zentralisierte Administration soll einem Systemverwalter, der alleine die 3 Rollen Systemverwalter, Sicherheitsbeauftragter und SAT-Datei-Verwalter wahrnimmt, die Möglichkeit gegeben werden, seine Aufgaben unter **einer** Benutzerkennung zu konzentrieren. Da das Privileg TSOS fest an die Systemkennung TSOS gebunden ist und nicht an eine andere Benutzerkennung vergeben werden kann, kommt pragmatischer Weise nur die Systemkennung TSOS in Frage. Um der Systemverwaltung die Möglichkeit zu geben, eine zentrale Systemverwalterkennung einzurichten, werden die Beschränkungen bei der Ernennung des Sicherheitsbeauftragten und SAT-Datei-Verwalters bezüglich der Benutzerkennungen und koexistierender Privilegien und Rechte aufgehoben.

Die genannten Einschränkungen werden mit der Anweisung SECADM UNITED aufgehoben, die in der Startup-Parameterdatei im Abschnitt “SRPM“ hinterlegt wird. Die Verfahren zur Ernennung der Administratoren ändert sich dadurch nicht.
Der Sicherheitsbeauftragte wird weiterhin mit der Anweisung SECADM USER-ID in der Startup-Parameterdatei ernannt und ernennt seinerseits eine Benutzerkennung seiner Wahl zum SAT-Datei-Verwalter.

Die SRPM-Parameter werden bereits beim Startup im BS2000-Grundausbau ausgewertet. Falls diese Option auch in der Subsysteminfodatei $TSOS.SYSSSI.SRPMOPT.xxx angegeben ist, hat die Angabe in der Startup-Parameterdatei Vorrang vor der Angabe in der Subsysteminfodatei.

Folgende Anweisung in der Startup-Parameterdatei steuert die Nutzung der zentralisierten Administration:

```
/BEGIN SRPM
SECADM UNITED=N[O] / Y[ES]
SECADM USER-ID=TSOS
/EOF
```

3.1.5 Beschreibung der Privilegien

Systemglobale Privilegien werden Benutzerkennungen per Kommando zugeordnet; eine Kennung kann mehrere Einzelprivilegien (und/oder Sammelprivilegien) besitzen und ein Einzelprivileg (und/oder Sammelprivilegien) kann an mehrere Benutzerkennungen vergeben sein. Die Privilegien einer Kennung sind im Benutzerkatalog (Datei SYSSRPM) hinterlegt (siehe Handbuch „Einführung in die Systembetreuung“ [2]). Die Privilegienverteilung im Benutzerkatalog des Home-Pubset ist systemweit wirksam.

Führt man einen First-Start für BS2000 unter Einsatz von SECOS durch, wird die Datei SYSSRPM neu erzeugt; als Standard haben vordefinierte Systemkennungen dann die in Tabelle „Privilegienverteilung nach First Start (Standard-Privilegienverteilung)“ auf Seite 63 beschriebenen Privilegien:

Wird BS2000 unter Einsatz von SECOS nicht mit First-Start sondern mit Kaltstart, Warmstart, etc. hochgefahren (siehe Handbuch „Einführung in die Systembetreuung“ [2]), dann gilt die im Benutzerkatalog des Home-Pubsets festgelegte Priviegienverteilung. Die Beschreibung der Privilegienverteilung nach Nicht-First-Start finden Sie im Abschnitt „Privilegienverteilung nach Nicht-First-Start“ auf Seite 64.

TSOS (TSOS)

Das Privileg TSOS gewährt alle Systemverwalterrechte, die keinem anderen Privileg zugeordnet sind.

Das Privileg TSOS ist fest an die Kennung TSOS geknüpft und kann weder dieser Kennung entzogen, noch an eine andere Kennung vergeben werden.

Das Privileg TSOS wird in Kommandos, Meldungen und Makros mit TSOS angesprochen.

Sicherheitsbeauftragter (SECURITY-ADMINISTRATION)

Der Sicherheitsbeauftragte hat das Recht zur Privilegienverwaltung, der Verwaltung der Operator-Roles und Kerberos-Schlüssel und zum Schalten der Protokollierung (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1]). Für den Inhaber dieses Privilegs ist die Protokollierung mit SAT immer eingeschaltet und kann nicht abgeschaltet werden.

Bei der Auslieferung ist das Privileg SECURITY-ADMINISTRATION an die Kennung SYSPRIV vergeben. Es kann während des laufenden Betriebs keiner anderen Kennung durch das Kommando SET-PRIVILEGE zugewiesen oder durch das Kommando /RESET-PRIVILEGE entzogen werden, und es ist auch nicht möglich, dieses Privileg einem Sammelprivileg zuzuordnen.

Wegen der herausragenden Bedeutung der Sicherheitsverwaltung kann nur mit Hilfe des Startup-Parameterservice festgelegt werden, welche Kennung das Recht des Sicherheitsbeauftragten haben soll (siehe auch Seite 66f).

Einer Kennung, die auf einem bestimmten Pubset das Privileg SECURITY-ADMINISTRATION besitzt, kann auf diesem Pubset kein anderes Privileg oder Sammelprivileg zugewiesen oder entzogen werden. Insbesondere kann der Sicherheitsbeauftragte also seiner eigenen Kennung auf dem Home-Pubset kein Privileg zuweisen, da seine Kennung dort ja das Privileg SECURITY-ADMINISTRATION besitzt. Der Sicherheitsbeauftragte kann jedoch seiner Kennung auf einem anderen Pubset, auf dem er nicht das Privileg SECURITY-ADMINISTRATION besitzt, ein Privileg zuweisen.

Die Beschränkungen bei der Ernennung des Sicherheitsbeauftragten und SAT-Datei-Verwalters bezüglich der Benutzerkennungen und koexistierender Privilegien und Rechte können bei Bedarf aufgehoben werden (siehe Abschnitt „Zentralisierte Administration“ auf Seite 45).

Privilegienverwaltung

Die Privilegienverwaltung darf die einzelnen systemglobalen Privilegien und Sammelprivilegien verwalten, das heißt

- Vergabe von Systemprivilegien und Sammelprivilegien an Benutzerkennungen auf allen Pubsets
- Entzug von Systemprivilegien und Sammelprivilegien für Benutzerkennungen auf allen Pubsets
- Abfrage von Informationen über die aktuelle Verteilung der Systemprivilegien und Sammelprivilegien
- Definition, Modifikation und Löschen von Sammelprivilegien auf allen Pubsets
- Abfrage von Information über die aktuellen Definitionen der Sammelprivilegien

Der Privilegienverwaltung stehen folgende Kommandos zur Verfügung:

CREATE-PRIVILEGE-SET
DELETE-PRIVILEGE-SET
MODIFY-PRIVILEGE-SET
RESET-PRIVILEGE
SET-PRIVILEGE
SHOW-PRIVILEGE
SHOW-PRIVILEGE-SET

Schalten beim Protokollieren

Der Sicherheitsbeauftragte darf

– die Protokollierung mit SAT aktivieren und deaktivieren

– die Protokollierung für Benutzerkennungen und protokollierbare Ereignisse ein- und ausschalten (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1])

Verwaltung der Operator-Roles

Der Sicherheitsbeauftragte darf

– Operator-Roles definieren, modifizieren und löschen

– Operator-Roles an Kennungen vergeben oder entziehen

– Informationen über die aktuelle Definition und Verteilung der Operator-Roles abfragen

Dem Sicherheitsbeauftragten stehen für die Verwaltung der Operator-Roles folgende Kommandos zur Verfügung:

CREATE-OPERATOR-ROLE
DELETE-OPERATOR-ROLE
MODIFY-OPERATOR-ROLE
SHOW-OPERATOR-ROLE
MODIFY-OPERATOR-ATTRIBUTES
SHOW-OPERATOR-ATTRIBUTES

Verwaltung von Kerberos-Schlüsseln

Der Sicherheitsbeauftragte verwaltet die im BS2000 hinterlegten Schlüssel für Kerberos-Authentisierung. Dafür stehen ihm folgende Kommandos zur Verfügung:

ADD-KEYTAB-ENTRY
MODIFY-KEYTAB-ENTRY
REMOVE-KEYTAB-ENTRY
SHOW-KEYTAB-ENTRY

Das Privileg Sicherheitsbeauftragter wird in Kommandos und Meldungen mit SECURITY-ADMINISTRATION, in Makros mit SECADM angesprochen.

Alias-Catalog-Service-Verwaltung (ACS-ADMINISTRATION)

Das Privileg Alias-Catalog-Service-Verwaltung gibt das Recht,

– systemglobale Voreinstellungen und Restriktionen für die Benutzung des ACS (alias catalog service) festzulegen

– die Vereinbarungen von ACS-Systemdateien zu treffen bzw. zu modifizieren

– erweiterte Funktionen einzelner ACS-Kommandos zu nutzen

Weitere Hinweise zum Alias-Catalog-Service finden Sie im Handbuch „Einführung in die Systembetreuung“ [2].

Bei Auslieferung ist das Privileg Alias-Catalog-Service-Verwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg Alias-Catalog-Service-Verwaltung wird in Kommandos und Meldungen mit ACS-ADMINISTRATION, in Makros mit ACSADM angesprochen.

Vorgenerierte Privilegien (CUSTOMER-PRIVILEGE-1...8)

Durch die Vergabe der Systemprivilegien CUSTOMER-PRIVILEGE-1 bis CUSTOMER-PRIVILEGE-8 ist es möglich, den Zugang zu Kommandos und Anweisungen für bestimmte Benutzerkennungen flexibel zu gestalten. Bei der Auslieferung des Systems sind die Privilegien in den Syntaxdateien vorgeneriert enthalten und werden nach der Auslieferung vom Systemadminstrator den Kommandos oder Anweisungen zugeordnet.

Standardmäßig sind diese Privilegien an keine Kennungen vergeben.

File-Transfer-Verwaltung (FT-ADMINISTRATION)

Die File-Transfer-Verwaltung darf das Auftrags- und Netzbeschreibungsbuch des Software-Produkts openFT (BS2000) verwalten, siehe Handbuch „Installation und Betrieb“ [11].

Bei Auslieferung ist das Privileg File-Transfer-Verwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg File-Transfer-Verwaltung wird in Kommandos und Meldungen mit FT-ADMINISTRATION, in Makros mit FTADM angesprochen.

FTAC-Verwaltung (FTAC-ADMINISTRATION)

Die FTAC-Verwaltung darf die Schutzfunktionen des Software-Produkts openFT-AC (BS2000) verwalten (siehe openFT: „Installation und Betrieb“ [11]).

Bei Auslieferung ist das Privileg FTAC-Verwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Vor Vergabe des Privilegs FTAC-Verwaltung sollte das Handbuch der im Einsatz befindlichen openFT-Version konsultiert werden.

Das Privileg FTAC-Verwaltung wird in Kommandos und Meldungen mit FTAC-ADMINISTRATION, in Makros mit FTACADM angesprochen.

Systemglobale Guard-Administration (GUARD-ADMINISTRATION)

Die systemglobale Guard-Administration darf auf allen lokalen Pubsets Aktionen zur Verwaltung von Guards beliebigen Typs durchführen und mit dem Programm GUARDS-SAVE benutzerkennungsübergreifend Guards sichern und restaurieren. Das heißt, eine Benutzerkennung mit diesem Privileg ist Miteigentümer aller Guards im System.

Das Privileg ist standardmäßig der Benutzerkennung TSOS zugeordnet. Es kann ihr aber durch den Sicherheitsbeauftragten entzogen und/oder auf andere Benutzerkennungen übertragen werden.

Das Privileg Guard-Administration wird in Kommandos und Meldungen mit GUARD-ADMINISTRATION, in Makros mit GUAADM angesprochen.

Hardware-Online-Wartung (HARDWARE-MAINTENANCE)

Recht zur Durchführung der Hardware-Online-Wartung. Die Hardware-Online-Wartung umfasst folgende Aufgaben:

– Führen und Auswerten der Hardware-Fehlerstatistik-Datei

– Ablauf von Statistik- und Trace-Programmen unter Steuerung des BS2000 simultan zu den Benutzerprogrammen

Bei Auslieferung ist das Privileg HARDWARE-MAINTENANCE an die Kennung SERVICE vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Sofern das Privileg HARDWARE-MAINTENANCE an eine andere Kennung als SERVICE vergeben wird, ist Folgendes zu beachten:

- Kennungen mit dem Privileg HARDWARE-MAINTENANCE unterliegen bis BS2000 OSD/BC V10.0 aus Sicherheitsgründen besonderen Einschränkungen. Insbesondere das Laden und Ausführen von Programmen ist nicht allgemein gewährleistet.
- Eine Kennung mit dem Privileg HARDWARE-MAINTENANCE ist nur dann zum Zugriff auf Dateien fremder Kennungen (z.B. SERVICE) berechtigt, wenn Folgendes gilt:
  – Falls die Datei mit Guards geschützt ist, müssen im Guard Zugriffsbedingungen festgelegt sein, die der privilegierten Benutzerkennung den Zugriff erlauben.
  – Falls die Datei nicht mit Guards geschützt ist, aber durch eine einfache Zugriffskontrollliste (BACL), muss diese der privilegierten Benutzerkennung den Zugriff erlauben.
  – Wenn die Datei weder mit Guards noch mit einer BACL geschützt ist, muss USER-ACCESS=*SPECIAL gesetzt sein.

  Es muss also dafür gesorgt werden, dass dieser Kennung der Zugriff auf alle für ihre Arbeit benötigten Dateien ermöglicht wird.

Das Privileg Hardware-Online-Wartung wird in Kommandos und Meldungen mit HARDWARE-MAINTENANCE, in Makros mit HWMAINT angesprochen.

HSMS-Verwaltung (HSMS-ADMINISTRATION)

Die HSMS-Verwaltung darf im System Aktionen zur Verwaltung des „Hierarchical Storage Management System“ durchführen (siehe Handbuch „HSMS“ [13]).

Bei Auslieferung ist das Privileg HSMS-Verwaltung an die Benutzerkennungen SYSHSMS und TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg HSMS-Verwaltung umfasst folgende Funktionen:

– Ausführen von HSMS-Verwalter-Anweisungen

– Spezifikation von HSMS-Express-Aufträgen

– Verarbeiten von Objekten anderer Benutzer mit HSMS-Anweisungen

Das Privileg HSMS-Verwaltung wird in Kommandos und Meldungen mit HSMS-ADMINISTRATION, in Makros mit HSMSADM angesprochen.

Netzverwaltung (NET-ADMINISTRATION)

Ein Benutzerauftrag mit dem Privileg Netzverwaltung darf Netzverwaltungsfunktionen ausüben und insbesondere alle BCAM-Kommandos ausführen. Das Privileg ist bei Auslieferung der Kennung TSOS zugeordnet.

Das Privileg Netzverwaltung wird in Kommandos und Meldungen mit NET-ADMINISTRATION, in Makros mit NETADM angesprochen.

Notification-Service-Administration (NOTIFICATION-ADMINISTRATION)

Das Privileg Notification-Service-Administration berechtigt zur Konfiguration des Notification Service , d. h. es erlaubt die Produkte festzulegen, die den Notification Service nutzen dürfen, und welche Methoden zur Benachrichtigung dabei unterstützt werden. Das Privileg ist bei Auslieferung den Kennungen TSOS und SYSSNS zugeordnet.

Notification Service im BS2000 ist ein Produkt, mit dem Benutzer beim Auftreten bestimmter Ereignisse benachrichtigt werden können. Derzeit wird diese Funktionalität von SPOOL genutzt. Ein Benutzer kann per Mail benachrichtigt werden, wenn bei seinen Druckaufträge bestimmte Ereignisse, z.B. Job-Beendigung, eintreten.

Das Privileg Notification-Service-Administration wird in Kommandos und Meldungen mit NOTIFICATION-ADMINISTRATION, in Makros mit NOTIFADM angesprochen.

Systembedienung (OPERATING)

Dieses Privileg gibt das Recht, Aufgaben der BS2000-Systembedienung wahrzunehmen. Dieses Privileg kann an beliebige Benutzerkennungen, außer SYSPRIV, vergeben werden, bei Auslieferung ist es der Kennung SYSOPR zugeordnet. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg Systembedienung wird in Kommandos, Meldungen und Makros mit OPERATING angesprochen.

POSIX-Benutzerverwaltung (POSIX-ADMINISTRATION)

Dieses Privileg gibt das Recht, auf allen lokalen Pubsets die POSIX-Benutzerattribute aller Benutzerkennungen zu verwalten. Es dürfen beliebige Benutzernummern, insbesondere die Nummer 0, vergeben werden. Die Benutzernummern dürfen auch mehrfach vergeben werden. Diese Berechtigung stellt eine Untermenge des Privilegs „systemglobale Benutzerverwaltung“ dar (siehe Seite 60). Weiterhin gibt dieses Privileg das Recht privilegierte POSIX-Funktionen aufzurufen.

Dieses Privileg schützt somit den Zugriff auf POSIX-Attribute, die durch die BS2000-Benutzerverwaltung administriert werden. Weiterhin werden damit Tools zum Installieren des POSIX-Subsystems geschützt. Nähere Informationen siehe Handbuch „POSIX-Grundlagen für Anwender und Systemverwalter“ [25].

Bei Auslieferung ist das Privileg an die Kennung SYSROOT vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg der POSIX-Benutzerverwaltung wird in Kommandos und Meldungen mit POSIX-ADMINISTRATION, in Makros mit POSIXADM angesprochen.

SPOOL-Verwaltung (PRINT-SERVICE-ADMINISTRATION)

Dieses Privileg gibt das Recht folgende SPOOL-Verwaltungsaufgaben durchzuführen:

– Start und Stop von SPOOL-Geräten (Drucker, Bänder)

– SPOOL-Parameter mit dem Dienstprogramm SPSERVE zu modifizieren

– Drucksteuerdateien mit dem Dienstprogramm PRM zu modifizieren

– Druckaufträge aller Benutzer mit folgenden Kommandos zu verwalten:
  CANCEL-PRINT-JOB
  HOLD-PRINT-JOB
  RESUME-PRINT-JOB
  SHOW-PRINT-JOB-ATTRIBUTES
  SHOW-PRINT-JOB-STATUS

Nähere Informationen finden Sie in den Handbüchern SPOOL (BS2000)
„Teil 1, Benutzerhandbuch“ [28] und „Teil 2, Dienstprogramme“ [29].

Bei Auslieferung ist das Privileg an die Kennungen TSOS, SYSSPOOL und SYSSNS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg der SPOOL-Verwaltung wird in Kommandos und Meldungen mit PRINT-SERVICE-ADMINISTRATION, in Makros mit PRSRVADM angesprochen.

Verwaltung des PROP-XT (PROP-ADMINISTRATION)

Dieses Privileg gibt das Recht, PROP-XT-Systemkommandos auszuführen. Kommandos eines PROP dienen der Automatisierung der Systembedienung. Der PROP-XT ist ein eigenes Produkt zur automatisierten Absetzung von Konsol-Kommandos.

Nähere Informationen finden Sie im Handbuch „PROP-XT“ [31].

Bei Auslieferung ist das Privileg zur Verwaltung des PROP-XT an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg zur Verwaltung des PROP-XT wird in Kommandos und Meldungen mit PROP-ADMINISTRATION, in Makros mit PROPADM angesprochen.

Auswertung der SAT-Dateien (SAT-FILE-EVALUATION)

Von SAT erzeugte Protokolldateien und CONSLOG-Dateien können von Kennungen mit dem Privileg SAT-FILE-EVALUATION ausgewertet werden.

Bei Auslieferung ist dieses Privileg an die Kennung SYSAUDIT vergeben. Der Sicherheitsbeauftragte kann dieses Privileg jeder anderen Kennung außer seiner eigenen zuweisen. Dabei sollte jedoch beachtet werden, dass alle SAT-Dateien immer unter der Kennung SYSAUDIT abgelegt werden. Sollen andere Kennungen auf diese Dateien zugreifen, wird aus Sicherheitsgründen empfohlen, diese Dateien mit Guards zu schützen.

Für Kennungen mit diesem Privileg ist die Protokollierung mit SAT zwangsläufig eingeschaltet, kann aber explizit wieder abgeschaltet werden. Es ist hierbei gleichgültig, ob das Privileg als Einzel- oder über ein Sammelprivileg zur Verfügung steht.

Das Privileg SAT-Datei-Auswertung wird in Kommandos und Meldungen mit SAT-FILE-EVALUATION, in Makros mit SATFEVAL angesprochen.

Verwaltung der SAT-Dateien (SAT-FILE-MANAGEMENT)

Die SAT-Datei-Verwaltung darf

- die von SAT (Security Audit Trail) erzeugten Dateien verwalten, insbesondere die SAT-Protokolldatei (SATLOG) mit dem Kommando /CHANGE-SAT-FILE umschalten
- die Protokolldateien und CONSLOG-Dateien auswerten
- mit dem Kommando /SET-REPLOG-READ-MARK den aktuellen Stand der Korrektur-Protokoll-Datei $SYSAUDIT.REPLOG.<date>.<sessnr> anfordern (diese kann dann mit SHOW-FILE angesehen werden), siehe Handbuch „Kommandos“ [4]

Der Inhaber dieses Privilegs heißt SAT-Datei-Verwalter (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1]). Aus Sicherheitsgründen ist für den SAT-Datei-Verwalter die Protokollierung mit SAT immer eingeschaltet.

Bei Auslieferung ist das Privileg SAT-Datei-Verwaltung an die Kennung SYSAUDIT vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst und TSOS) vergeben.

Für Kennungen mit diesem Privileg ist die Protokollierung mit SAT zwangsläufig eingeschaltet und kann solange nicht abgeschaltet werden, wie die Kennung dieses Privileg besitzt. Es ist hierbei gleichgültig, ob das Privileg als Einzel- oder über ein Sammelprivileg zur Verfügung steht.

Die Beschränkungen bei der Ernennung des SAT-Datei-Verwalters bezüglich der Benutzerkennungen und koexistierender Privilegien und Rechte können bei Bedarf aufgehoben werden (siehe Abschnitt „Zentralisierte Administration“ auf Seite 45).

Das Privileg SAT-Datei-Verwaltung wird in Kommandos und Meldungen mit SAT-FILE-MANAGEMENT, in Makros mit SATFMGMT angesprochen.

Eingabe von Benutzerkommandos (STD-PROCESSING)

Das Privileg STD-PROCESSING gibt das Recht Benutzerkommandos einzugeben, d.h. alle Kommandos einzugeben, die dieses Privileg besitzen (siehe Handbuch „Kommandos“ [4]), sowie die nicht-privilegierten Anweisungen von BS2000-Softwareprodukten.

Das Privileg zur Eingabe von Benutzerkommandos ist bei Auslieferung an die beim First-Start erzeugten Kennungen vergeben. Eine Ausnahme bilden die Kennungen SERVICE, SYSAUDIT und SYSPRIV.

Wird eine Kennung mit dem Kommando ADD-USER neu eingerichtet, so wird ihr vom System standardmäßig das Privileg STD-PROCESSING zugewiesen (es gilt die Regelung, dass jede Kennung mindestens ein Privileg besitzen muss).

Eine Benutzerkennung kann nur dann gelöscht werden, wenn sie als einziges Privileg das Privileg STD-PROCESSING besitzt.

Das Privileg zur Eingabe von Benutzerkommandos wird in Kommandos und Meldungen mit STD-PROCESSING, in Makros mit STDPROC angesprochen.

Subsystem-Verwaltung (SUBSYSTEM-MANAGEMENT)

Dieses Privileg beinhaltet das Recht, Aktionen der dynamischen Subsystem-Verwaltung, der Software-Installation und der IMON-Verwaltung durchzuführen. Bei Auslieferung ist das Privileg Subsystem-Verwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Folgende Kommandos sind mit diesem Privileg ausführbar (alphabetische Reihenfolge):

ADD-SUBSYSTEM	SET-DSSM-OPTIONS
HOLD-SUBSYSTEM	SET-INSTALLATION-PATH
LOCK-PRODUCT-VERSION	SHOW-DSSM-INFORMATION
MODIFY-IMON-SCI	SHOW-INSTALLATION-PATH
MODIFY-SUBSYSTEM-PARAMETER	SHOW-POSIX-STATUS
RELEASE-SUBSYSTEM-SPACE	SHOW-SUBSYSTEM-ATTRIBUTES
REMOVE-SUBSYSTEM	SHOW-SUBSYSTEM-INFO
RESUME-SUBSYSTEM	SHOW-SUBSYSTEM-STATUS
RESTORE-SOFTWARE-INVENTORY	START-SUBSYSTEM
SAVE-SOFTWARE-INVENTORY	STOP-SUBSYSTEM
SAVE-SUBSYSTEM-CATALOG	UNLOCK-PRODUCT-VERSION
SELECT-PRODUCT-VERSION	UNLOCK-SUBSYSTEM

Weitere Hinweise zur dynamischen Subsystem-Verwaltung, Software-Installation und der IMON-Verwaltung finden Sie im Handbuch „Einführung in die Systembetreuung“ [2].

Das Privileg Subsystem-Verwaltung wird in Kommandos und Meldungen mit SUBSYSTEM-MANAGEMENT, in Makros mit SUBSMGMT angesprochen.

Software-Monitor-Verwaltung (SW-MONITOR-ADMINISTRATION)

Dieses Privileg gestattet, die Software-Monitore openSM2 und COSMOS zu starten, zu beenden und zu verwalten.

Außerdem dürfen die folgenden Kommandos in vollem Funktionsumfang ausgeführt werden:

SHOW-CACHE-CONFIGURATION	SHOW-ISAM-POOL-ATTRIBUTES
SHOW-DEVICE-CONFIGURATION	SHOW-JOB-CLASS
SHOW-DEVICE-STATUS	SHOW-JOB-STREAM
SHOW-DISK-DEFAULTS	SHOW-MASTER-CATALOG-ENTRY
SHOW-DISK-STATUS	SHOW-TRACE-STATUS
SHOW-GS-STATUS	SHOW-USER-STATUS

Bei Auslieferung ist das Privileg Software-Monitor-Verwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Weitere Informationen zu openSM2 finden Sie im Handbuch „openSM2“ [21].

Das Privileg Software-Monitor-Verwaltung wird in Kommandos und Meldungen mit SW-MONITOR-ADMINISTRATION und in Makros mit SWMONADM angesprochen.

Bandverwaltung (TAPE-ADMINISTRATION)

Die Bandverwaltung darf die Administrationsfunktionen des Bandverwaltungssystems MAREN ausführen. Das heißt, sie darf das MAREN-Verwaltungsprogramm aufrufen, mit dem das MAREN-Archiv verwaltet werden kann (siehe Handbuch „MAREN“ [17]).

Bei Auslieferung ist das Privileg Bandverwaltung an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede Kennung (außer an sich selbst) vergeben.

Das Privileg Bandverwaltung wird in Kommandos und Meldungen mit TAPE-ADMINISTRATION, in Makros mit TAPEADM angesprochen.

Encryption-Key-Verwaltung für Bänder (TAPE-KEY-ADMINISTRATION)

Die Encryption-Key-Verwaltung für Bänder darf die Anweisungen des Programms MARENEKM (MAREN Encryption Key Manager) ausführen. Das heißt, sie darf die Encryption Keys für Bänder verwalten.

Bei Auslieferung ist das Privileg Encryption Key Verwaltung für Bänder an die Kennung SYSMAREN vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede Kennung (außer an sich selbst) vergeben.

Das Privileg Encryption-Key-Verwaltung für Bänder wird in Kommandos und Meldungen mit TAPE-KEY-ADMINISTRATION, in Makros mit TAPEKEYADM angesprochen.

Folgende Anweisungen sind mit diesem Privileg ausführbar (alphabetische Reihenfolge):

ADD-ENCRYPTION-KEY
COPY-ENCRYPTION-KEYS
CREATE-ENCRYPTION-KEY
DELETE-KEY-BOX
EXPORT-KEY-BOX
IMPORT-KEY-BOX
MODIFY-VOLUME-ENCRYPTION-ATTR
REMOVE-ENCRYPTION-KEYS
REPAIR-KEY-BOX
SET-WRITE-ENCRYPTION-KEY
SHOW-ENCRYPTION-KEYS
SHOW-VOLUME-ENCRYPTION-ATTR

Systemglobale Benutzerverwaltung (USER-ADMINISTRATION)

Die systemglobale Benutzerverwaltung darf auf allen lokalen Pubsets Aktionen zur Benutzer- oder Benutzergruppenverwaltung durchführen (für alle Benutzer oder Benutzergruppen). Für die Vergabe von Betriebsmitteln und Benutzerrechten (wie z.B. START-IMMEDIATE, NO-CPU-LIMIT,...) an Benutzerkennungen und Benutzergruppen gibt es keine Begrenzungen.

Bei den POSIX-Benutzerattributen dürfen alle Funktionen der POSIX-Benutzerverwaltung ausgeführt werden.

Bei Auslieferung ist das Privileg USER-ADMINISTRATION an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Der Benutzerverwaltung stehen zur Verfügung:

– die Programmschnittstellen SRMUINF (SVC 185), GETUGR und SRMSUG (SVC 49) für alle Benutzerkennungen, Gruppen und Pubsets

– folgende Kommandos für alle Benutzerkennungen bzw. Benutzergruppen und alle Pubsets:

ADD-USER	ADD-USER-GROUP
MODIFY-USER-ATTRIBUTES	MODIFY-USER-GROUP
REMOVE-USER	REMOVE-USER-GROUP
LOCK-USER	SHOW-USER-GROUP
UNLOCK-USER	
SHOW-USER-ATTRIBUTES	MODIFY-POSIX-USER-ATTRIBUTES
	SHOW-POSIX-USER-ATTRIBUTES
SET-LOGON-PROTECTION	MODIFY-POSIX-USER-DEFAULTS
MODIFY-LOGON-PROTECTION	SHOW-POSIX-USER-DEFAULTS
SHOW-LOGON-PROTECTION	

Der Benutzerkatalog eines Pubset wird beim Importieren dieses Pubset geöffnet und bleibt offen bis zum Exportieren des Pubset. Daher ist ein direkter Zugriff auf den Benutzerkatalog für den Benutzer nicht möglich (das heißt, ein Zugriff über andere als die genannten Schnittstellen).

Eine Benutzerkennung kann auf ein- und demselben Pubset nicht gleichzeitig das Privileg „systemglobaler Benutzerverwalter“ besitzen und als Verwalter einer Benutzergruppe definiert sein. Eine Benutzerkennung kann aber im laufenden System als systemglobaler Benutzerverwalter fungieren (das heißt auf dem Home-Pubset das Privileg USER-ADMINISTRATION haben) und auf einem importierten Pubset Gruppenverwalter sein.

Da der Inhaber des Privilegs USER-ADMINISTRATION den Zugangsschutz für alle Kennungen des Systems festlegen darf, kann er sich Zugang zu allen Benutzerkennungen verschaffen, insbesondere zu den privilegierten (wie z.B. der Kennung des Sicherheitsbeauftragten). Damit könnte er Funktionen ausüben, für die er nicht berechtigt ist, da sie nicht zum Funktionsumfang eines Benutzerverwalters gehören. Hier erweist sich eine Kontrolle durch Protokollierung mit SAT als besonders sinnvoll (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1]).

Das Privileg „systemglobale Benutzerverwaltung“ wird in Kommandos und Meldungen mit USER-ADMINISTRATION, in Makros als USERADM angesprochen.

Verwaltung einer virtuellen Maschine (VIRTUAL-MACHINE-ADMINISTRATION)

Einer Benutzertask mit dem Privileg VIRTUAL-MACHINE-ADMINISTRATION ist es erlaubt, eine Teilmenge der VM2000-Kommandos auszuführen und damit eine virtuelle Maschine als VM-Administrator zu bedienen.

Weitere Informationen zu VM2000 siehe Handbuch „VM2000“ [22].

Bei Auslieferung ist das Privileg VIRTUAL-MACHINE-ADMINISTRATION an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg zur Verwaltung einer virtuellen Maschine wird in Kommandos und Meldungen mit VIRTUAL-MACHINE-ADMINISTRATION, in Makros mit VMPRIV angesprochen.

Verwaltung von VM2000 (VM2000-ADMINISTRATION)

Einer Benutzertask mit dem Privileg VM2000-ADMINISTRATION ist es erlaubt, sämtliche VM2000-Kommandos auszuführen und damit das Gesamtsystem VM2000 und alle virtuellen Maschinen als VM2000-Administrator zu bedienen.

Weitere Informationen zu VM2000 siehe Handbuch „VM2000“ [22].

Bei Auslieferung ist das Privileg VM2000-ADMINISTRATION an die Kennung TSOS vergeben. Der Sicherheitsbeauftragte kann das Privileg an jede andere Kennung (außer an sich selbst) vergeben.

Das Privileg VM2000-Verwaltung wird in Kommandos und Meldungen mit VM2000-ADMINISTRATION, in Makros mit VM2ADM angesprochen.

3.1.6 Privilegienverteilung nach First-Start

Führt man einen First-Start für BS2000 durch, wird die Datei SYSSRPM neu erzeugt; als Standard haben vordefinierte Systemkennungen dann bestimmte Privilegien. Die Zuordnung der Privilegien zu den Systemkennungen ist folgender Tabelle zu entnehmen:

Privileg	**Benutzerkennungen**																			
	TSOS	SERVICE	SYSAUDIT	SYSDB	SYSDUMP	SYSFJAM	SYSGEN	SYSHSMS	SYSMAREN	SYSNAC	SYSSAG	SYSSNAP	SYSSNS	SYSOPR	SYSPRIV[1]	SYSROOT	SYSSOPT	SYSSPOOL	SYSUSER	SYSWSA
ACS-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CUSTOMER-PRIVILEGE-1...8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FT-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FTAC-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
GUARD-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
HARDWARE-MAINTENANCE	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
HSMS-ADMINISTRATION	X	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-
NET-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NOTIFICATION-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-
OPERATING	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	X
POSIX-ADMINISTRATION	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-
PRINT-SERVICE-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	X	-	-
PROP-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SAT-FILE-EVALUATION	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SAT-FILE-MANAGEMENT	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SECURITY-ADMINISTRATION	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-
STD-PROCESSING	X	-	-	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
SUBSYSTEM-MANAGEMENT	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SW-MONITOR-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TAPE-ADMINISTRATION	X	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-
TAPE-KEY-ADMINISTRATION	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-
TSOS	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
USER-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
VIRTUAL-MACHINE-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
VM2000-ADMINISTRATION	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X
	X bedeutet: Das Privileg ist der Benutzerkennung standardmäßig zugeordnet. - bedeutet: Das Privileg ist der Benutzerkennung standardmäßig nicht zugeordnet.																			

Tabelle 1: Privilegienverteilung nach First Start (Standard-Privilegienverteilung)

[1] Wenn in der Startup-Parameterdatei eine Benutzerkennung ungleich SYSPRIV als Benutzerkennung des Sicherheitsbeauftragten angegeben wurde, so gilt diese Spalte für eben diese Benutzerkennung. Die Benutzerkennung SYSPRIV ist in diesem Fall wie z.B. SYSGEN zu behandeln.

3.1.7 Privilegienverteilung nach Nicht-First-Start

Erfolgt nach einem Shutdown ein Startup im System derselben Version mit Kaltstart, Warmstart, SELECTIVE-Start oder ZIP-Start, so ist die Privilegienverteilung dieselbe wie vor dem letzten Shutdown.

Falls die Datei SYSSRPM nicht vorhanden ist oder irreparabel zerstört wurde, ist kein Startup möglich, ohne den Benutzerkatalog entweder zu rekonstruieren, zurückzusetzen oder neu zu erzeugen.
In einem rekonstruierten Benutzerkatalog sind die Privilegien vergeben wie zum Zeitpunkt der Sicherung.
In einem neu erzeugten oder zurückgesetzten Benutzerkatalog erfolgt die Privilegienvergabe wie bei First-Start.

Hinweise zur Sicherung und Rekonstruktion des Benutzerkatalogs finden Sie im Handbuch „Einführung in die Systembetreuung“ [2].

3.1.8 Beispiele für die Privilegienvergabe

Bei der Aufteilung von Privilegien auf einzelne Benutzerkennungen muss Folgendes berücksichtigt werden:

– die Sicherheitspolitik des jeweiligen Rechenzentrum
– die Verteilung der Aufgabengebiete auf einzelne Personen

Die Möglichkeiten der Aufgabenverteilung sollten genutzt werden. Müssen Aufgabengebiete dennoch zusammengefasst werden, bieten sich folgende Schwerpunkte an:

– Datensicherheit/Datenschutz (systemglobale Benutzerverwaltung und FTAC-Verwaltung)
– Netzverwaltung mit FT-Verwaltung
– Datensicherung und Archiv (HSMS-Verwaltung und MAREN-Verwaltung)

Es bietet sich an, Privilegien solcher Funktionsbereiche zu Sammelprivilegien zusammenzufassen.

Datensicherheit/Datenschutz

Die systemglobale Benutzerverwaltung entscheidet über die Benutzerorganisation und delegiert Verwaltungsaufgaben z.B. an die Gruppenverwalter. Das Thema FTAC ist eng damit verbunden, da für jede Benutzerkennung und jeden Rechner festgelegt werden sollte, welche Funktionen mit FT ausgeführt werden dürfen. Die Funktion Folgeverarbeitung sollte z.B. nur ausgewählten Benutzern über FTAC-Profile erlaubt werden. Es müssen zwar auch für jeden Rechner, der dem FT-System bekannt ist, die entsprechenden Sicherheitsstufen bekanntgegeben werden; dennoch sollte man FT-Verwaltung und FTAC-Verwaltung trennen und der FT-Verwaltung ein entsprechendes Konzept der Rechner und Sicherheitsstufen vorgeben.

Netzverwaltung

Netzverwaltung und FT-Verwaltung können zusammengefasst werden, weil dann von einer Instanz aus nach der Netzgenerierung auch der FT-Eintrag, falls vom Antragsteller gefordert, vorgenommen werden kann. Das vorgegebene Sicherheitsstufenkonzept der FTAC-Verwaltung muss berücksichtigt werden. Die Daten für den FT-Eintrag legt die Netzverwaltung bei der Generierung fest (siehe Hinweise bei der Beschreibung der Einzelprivilegien Seite 52f).

Archiv

HSMS dient der Datensicherung und Datenverwaltung. Je nach Aufgabenbeschreibung kann die HSMS-Verwaltung den Archiv-Arbeiten (z.B. Eintragen von Sicherungsdatenträgern, Festlegen von Sicherungszyklen, Auslagern von Daten in andere Sicherungsebenen) oder der Systembetreuung (bei Schwerpunkt Datensicherung) zugeordnet werden.

3.2 Benutzer und ihre Betriebsmittel verwalten

Die Benutzerverwaltung des BS2000 kann auf zwei grundsätzlich verschiedene Arten erfolgen:

– zentral durch die systemglobale Benutzerverwaltung

– dezentral durch die gruppenspezifische Benutzerverwaltung (siehe Seite 72)

Beide Verfahren bieten der Systembetreuung umfassende Möglichkeiten, die Benutzerverwaltung den jeweiligen Erfordernissen angepasst effizient und flexibel zu organisieren. Die Kombination von zentraler und dezentraler Benutzerverwaltung setzt besondere Sorgfalt voraus.

Grundsätzlich umfasst die Benutzerverwaltung auch Funktionen, die sich aus der Zuordnung von Jobklassen zu Benutzerkennungen in der Auftragsverwaltung ergeben. Die folgenden Beschreibungen befassen sich jedoch ausschließlich mit der Verwaltung von Benutzerkennungen und Benutzergruppen.

3.2.1 Berechtigungen zur Benutzerverwaltung

Sicherheitsbeauftragter

Der Sicherheitsbeauftragte verwaltet die systemglobalen Privilegien. Er beeinflusst die Benutzerverwaltung dadurch, dass er einzelne Benutzerkennungen zum systemglobalen Benutzerverwalter ernennt oder absetzt, indem er ihnen das systemglobale Privileg USER-ADMINISTRATION zuteilt bzw. entzieht. Bei Auslieferung ist das Privileg SECURITY-ADMINISTRATION an die bei First-Start eingerichtete Kennung SYSPRIV gebunden. Der Sicherheitsbeauftragte ist als oberste Instanz für die Benutzerverwaltung anzusehen; er selbst kann jedoch keine Funktionen der Benutzerverwaltung ausüben.

Systemglobale Benutzerverwaltung

Die systemglobale Benutzerverwaltung umfasst alle systemglobalen Benutzerverwalter, das heißt alle Benutzerkennungen, denen vom Sicherheitsbeauftragten das systemglobale Privileg USER-ADMINISTRATION zugewiesen wurde. Ein systemglobaler Benutzerverwalter ist zu einer privilegierten Durchführung der Benutzerverwaltung berechtigt. Er kann alle Benutzerkennungen und Benutzergruppen auf allen Pubsets verwalten:

– Benutzerkennungen und Benutzergruppen einrichten, modifizieren oder löschen,

– Gruppenverwalter ernennen, austauschen oder absetzen,

– Betriebsmittel und Benutzerrechte einzelnen Benutzerkennungen und Benutzergruppen zuteilen oder entziehen.

Die systemglobale Benutzerverwaltung ist der gruppenspezifischen Benutzerverwaltung (s.u.) übergeordnet. Insbesondere kann sie den Benutzerkennungen und Benutzergruppen über bestehende Gruppenpotentiale hinaus (siehe Seite 68) Betriebsmittel und Benutzerrechte zuweisen. Als Grenzwerte gelten einzig die physikalischen Grenzwerte des Betriebssystems (z.B. maximal 32.767 Gruppenmitglieder).

Gruppenspezifische Benutzerverwaltung (Gruppenverwaltung)

Siehe Seite 72.

Ernennung/Absetzung eines systemglobalen Benutzerverwalters

Der Sicherheitsbeauftragte kann mit dem Kommando

```
/set-privilege user-id=userid,privilege=user-administration,pubset=...
```

das systemglobale Privileg USER-ADMINISTRATION an eine Benutzerkennung ’userid’ vergeben, das heißt die Benutzerkennung ’userid’ zum systemglobalen Benutzerverwalter ernennen.

Mit dem Kommando

```
/reset-privilege user-id=userid,privilege=user-administration,pubset=...
```

kann er der Benutzerkennung ’userid’ das systemglobale Privileg USER-ADMINISTRATION wieder entziehen und sie damit als systemglobalen Benutzerverwalter absetzen.

Hinweise zum systemglobalen Benutzerverwalter:

– Das systemglobale Privileg USER-ADMINISTRATION kann auf mehreren Pubsets eingetragen werden, ist jedoch nur dann wirksam, wenn es auf dem Pubset, der für den Systemlauf als Home-Pubset gilt, eingetragen ist.

  Beispiel

  Für die Benutzerkennung ’thisuser’ ist das systemglobale Privileg USER-ADMINISTRATION auf dem Pubset A eingetragen, nicht jedoch auf dem Pubset B. Der Systemstart erfolgte mit dem Pubset B als Home-Pubset.
  Ergebnis: Die Benutzerkennung ’thisuser’ besitzt für diesen Systemlauf nicht das systemglobale Privileg USER-ADMINISTRATION.

– Das systemglobale Privileg USER-ADMINISTRATION berechtigt einen systemglobalen Benutzerverwalter zur Verwaltung aller Benutzergruppen auf allen Pubsets.

– Ein systemglobaler Benutzerverwalter kann nicht zum Gruppenverwalter einer Benutzergruppe ernannt werden, da er grundsätzlich über weiterreichende Rechte verfügt.

3.2.2 Benutzergruppen

Mit SRPM können Benutzerkennungen explizit durch Kommandos zu Benutzergruppen zusammengefasst werden. Alle Benutzerkennungen, die keiner definierten Gruppe zugeordnet sind, gehören der Standardgruppe *UNIVERSAL an.

Bei Zugriffen auf Objekte wird immer die Gruppenstruktur auf dem Home-Pubset zur Bestimmung der Gruppenzugehörigkeit herangezogen. Pubset-spezifische Gruppenstrukturen werden nur zu Verwaltungszwecken eingerichtet (siehe Seite 88).

Definition von Benutzergruppen

Eine Benutzergruppe ist die Zusammenfassung einzelner Benutzerkennungen. Jede Benutzergruppe wird durch einen Gruppennamen, das ist die Gruppenkennung, repräsentiert. Sie wird im Benutzerkatalog eines Pubset eingetragen. Eine Benutzergruppe kann auf verschiedenen Pubsets mit unterschiedlichen Attributen eingetragen sein. Zugriffsberechtigungen werden jedoch immer gegen die Gruppenstruktur des Home-Pubset geprüft. Im Benutzerkatalog werden für eine Benutzergruppe folgende Daten hinterlegt:

– Gruppenbeschreibungsdaten (Name der Benutzergruppe, Einordnung in die Gruppenstruktur des Pubset, Gruppenverwalter). Für jede Gruppe kann ein Gruppen-Präfix festgelegt werden, der die Möglichkeit der Namenswahl insoweit beschränkt, dass nun alle Untergruppen dieser Gruppe mit dem festgelegten Präfix beginnen müssen. Auf diese Weise ist die Einordnung einer Gruppe in eine Hierarchie bereits über den Namen möglich.

– Gruppenmitglieder (Benutzerkennungen, die einer Benutzergruppe zugeordnet sind). Wie auch bei der Gruppe kann für die Gruppenmitglieder festgelegt werden, dass ihre Namen mit einem bestimmten Präfix beginnen müssen. Bei der Benennung des Gruppenverwalters wird festgelegt, welche Namens-Präfixe er vergeben darf.

– Gruppenpotential (Betriebsmittel und Rechte, die an eine Benutzergruppe gebunden sind und an die Gruppenmitglieder oder an hierarchisch untergeordnete Benutzergruppen vergeben werden können).

  Das Gruppenpotential kann gegliedert werden in:

  a) Gruppenpotential mit Verrechnung

     – maximale Anzahl der Untergruppen einer Benutzergruppe (MAX-SUB-GROUPS)

     – maximale Anzahl der Gruppenmitglieder einer Benutzergruppe und deren Untergruppen (MAX-GROUP-MEMBERS)

b) Gruppenpotential ohne Verrechnung

- Gruppenverwalterrecht (ADM-AUTHORITY) mit den Ausprägungen MANAGE-MEMBERS, MANAGE-RESOURCES, MANAGE-GROUPS
- Festlegung von Abrechnungsnummern (ADD-ACCOUNT) mit möglichen Ressourcen für:

CPU-LIMIT	(CPU-LIMIT, NO-CPU-LIMIT)
SPOOLOUT-Klasse	(SPOOLOUT-CLASS)
zulässige Ablaufpriorität	(MAX-ALLOWED-PRIORITY)
zulässige Task-Kategorie	(MAX-ALLOWED-CATEGORY)
Scheduling-Recht	(START-IMMEDIATE)
Task-(De-)Aktivierung	(INHIBIT-DEACTIVATION)

- Erzeugung von benutzerspezifischen Abrechnungssätzen (MAX-ACCOUNT-RECORDS)
- Überschreitung des PUBLIC-SPACE-LIMIT (PUBLIC-SPACE-EXCESS)
- Maximaler Speicherplatz (PUBLIC-SPACE-LIMIT)
- Magnetbandzugriff (TAPE-ACCESS)
- Überwachung von Dateien (FILE-AUDIT)
- Nutzung des Memory-Pool-Schutzes (CSTMP-MACRO)
- Test-Privilegierung (TEST-OPTIONS)
- Nutzung von BS2000-Profilen (ADD-PROFILE-ID)
- Verfügbarer Adressraum (ADDRESS-SPACE-LIMIT)
- Anzahl der residenten Hauptspeicherseiten (RESIDENT-PAGES)
- Anzahl der anlegbaren Dateien (FILE-NUMER-LIMIT)
- Anzahl der zugelassenen Jobvariablen (JV-NUMBER-LIMIT)
- Maximaler temporärer Speicherplatz (TEMP-SPACE-LIMIT)

Beispiel: Ausgabe der Attribute einer Benutzergruppe

```
/show-user-group group-identification=manuals
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-02 14:16:42
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              B
GROUP-ADMINISTRATOR              ADAM    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                 MAN    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                *UNIVERSAL

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     10
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     10
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     10
FREE  GROUP-HIERARCHY               9    FREE  USER-ADM                     10

TEST-OPTIONS...
MODIFICATION              *CONTROLLED
READ-PRIVILEGE                     1    WRITE-PRIVILEGE                     1

PUBLIC-SPACE-EXCESS              *NO    PUBLIC-SPACE-LIMIT      2.147.483.647
RESIDENT-PAGES                32.767    ADDRESS-SPACE-LIMIT                16
FILE-AUDIT                       *NO    CSTMP-MACRO                       *NO
MAX-ACCOUNT-RECORDS              100    TAPE-ACCESS                      *STD
TEMP-SPACE-LIMIT       2.147.483.647    DMS-TUNING-RESOURCES            *NONE
FILE-NUMBER-LIMIT         16.777.215    JV-NUMBER-LIMIT           16.777.215
WORK-SPACE-LIMIT       2.147.483.647    PHYSICAL-ALLOCATION      *NOT-ALLOWED
HARDWARE-AUDIT            *ALLOWED    CRYPTO-SESSION-LIMIT              128
LINKAGE-AUDIT             *ALLOWED    NET-STORAGE-USAGE            *ALLOWED

BASIC-ACL-ACCESS       *BY-GROUP-ONLY

PROFILE-IDS             STDPROFILE

+--------+--------------+--------+--------+-----------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+-----------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+-----------+-------+------+------+

NO SUB-GROUP SPECIFIED

GROUP-MEMBERS                 ADAM
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Die Wurzel der Gruppenstruktur: *UNIVERSAL

Mit First-Start wird auf dem Home-Pubset die Benutzergruppe *UNIVERSAL eingerichtet. Sie bildet die Wurzel der Gruppenstruktur auf diesem Pubset. Nach dem First-Start sind in der Benutzergruppe *UNIVERSAL alle vom Betriebssystem vergebenen Benutzerkennungen enthalten. Für die Benutzergruppe *UNIVERSAL gibt es keine Beschränkung – abgesehen von den physikalisch geltenden Grenzwerten – des Gruppenverwalterrechts und des Gruppenpotentials.

Die Benutzergruppe *UNIVERSAL hat implizit keinen Gruppenverwalter; dieser ist explizit festzulegen. Das Gruppenverwalterrecht der Benutzergruppe *UNIVERSAL ist stets MANAGE-GROUPS, so dass ein Gruppenverwalter von *UNIVERSAL auf dem jeweiligen Pubset alle Benutzerkennungen und Benutzergruppen verwalten kann.

Beispiel: Attribute der Benutzergruppe *UNIVERSAL mit Gruppenverwalter und einer Untergruppe

```
/show-user-group group-identification=*universal

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-02 14:20:27
------------------------------------------------------------------------------
GROUP-IDENTIFICATION       *UNIVERSAL    PUBSET                              B
GROUP-ADMINISTRATOR               EVA    ADM-AUTHORITY          *MANAGE-GROUPS

BASIC-ACL-ACCESS       *BY-GROUP-ONLY

SUB-GROUPS                   MANUALS

GROUP-MEMBERS                EVA       SERVICE   SYSAUDIT  SYSDUMP   SYSGEN
                             SYSHSMS   SYSNAC    SYSPRIV   SYSSNAP   SYSSPOOL
                             SYSUSER   TSOS
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                              END OF DISPLAY
```

Mit dem Einrichten eines neuen Pubset und dessen erstmaliger Zuschaltung zum System wird auch auf diesem die Benutzergruppe *UNIVERSAL eingerichtet. Die zuvor genannten Benutzerkennungen werden dort in gleicher Weise zugeordnet.

Untergruppen

Jede weitere Benutzergruppe muss eingerichtet werden. Sie ist immer die Untergruppe einer bereits bestehenden Benutzergruppe (z.B. *UNIVERSAL) und kann weitere Untergruppen besitzen, das heißt eine Gruppenstruktur kann hierarchisch aufgebaut werden.

Gruppenstruktur

Die Gruppenstruktur ist pubset-spezifisch im jeweiligen Benutzerkatalog hinterlegt. Die Gruppenstruktur des Home-Pubset wird zur Bestimmung der Gruppenzugehörigkeit bei Zugriffen auf systemspezifische Objekte (z.B. Memory Pools) sowie auf pubset-spezifische Objekte (Dateien, Jobvariablen) herangezogen.

Gruppenmitglieder

Jede Benutzerkennung ist Gruppenmitglied genau einer Benutzergruppe. Jede Benutzergruppe hat keine, eine oder mehrere Benutzerkennungen als Gruppenmitglieder. Mitglieder von Untergruppen gelten nicht als Mitglieder der übergeordneten Gruppe.

Gruppenverwalter

Die gruppenspezifische Benutzerverwaltung wird von Gruppenverwaltern wahrgenommen, das heißt von Benutzerkennungen, denen durch einen Eintrag im Gruppenpotential einer Benutzergruppe das Gruppenverwalterrecht zugeteilt wurde. Ein Gruppenverwalter kann nur von einem systemglobalen Benutzerverwalter oder von dem Gruppenverwalter einer in der Benutzergruppenstruktur hierarchisch übergeordneten Benutzergruppe ernannt oder abgesetzt werden.

Das Gruppenverwalterrecht gehört zum Gruppenpotential einer Benutzergruppe und kann im Rahmen des Gruppenpotentials nur einer Benutzerkennung der Benutzergruppe zugeteilt werden. Im Gegensatz zu systemglobalen Privilegien oder allgemeinen Benutzerrechten ist das Gruppenverwalterrecht also nicht an eine Benutzerkennung, sondern an eine Benutzergruppe geknüpft.

Eine Benutzergruppe kann (muss aber nicht) von einem Gruppenverwalter verwaltet werden. Eine Benutzerkennung mit dem systemglobalen Privileg der Benutzerverwaltung ist ebenfalls zur Gruppenverwaltung berechtigt. Sie darf jedoch nicht als Gruppenverwalter eingetragen sein, weil sie gegenüber dem Gruppenverwalter mit wesentlich mehr Rechten ausgestattet ist. Jede Benutzergruppe hat nur einen direkt zugeordneten Gruppenverwalter.

Das Gruppenverwalterrecht existiert in drei Ausprägungen, die zueinander in aufsteigender hierarchischer Beziehung stehen:

– MANAGE-RESOURCES (niedrigstes Recht)

– MANAGE-MEMBERS

– MANAGE-GROUPS (höchstes Recht)

MANAGE-RESOURCES

Das Gruppenverwalterrecht MANAGE-RESOURCES berechtigt einen Gruppenverwalter dazu, die Gruppenmitglieder seiner eigenen Benutzergruppe und der ihr untergeordneten Gruppenstruktur im Rahmen des für diese Benutzergruppe festgelegten Gruppenpotentials an Betriebsmitteln und Benutzerrechten zu verwalten. Außerdem kann er Benutzerkennungen, die nicht Gruppenmitglieder sind, den Zugriff auf Dateien und Jobvariablen der Gruppe erlauben, wenn diese durch BACL geschützt sind. Die Berechtigung ist auf bereits eingerichtete Benutzerkennungen und Benutzergruppen beschränkt. Die bestehende Benutzergruppenstruktur und die Zugehörigkeit der Gruppenmitglieder kann also nicht verändert werden. Neue Benutzerkennungen und Benutzergruppen können nicht erzeugt werden.

Für die Verwaltung stehen folgende Kommandos zur Verfügung:

MODIFY-USER-GROUP	MODIFY-USER-ATTRIBUTES
SHOW-USER-GROUP	SHOW-USER-ATTRIBUTES

MANAGE-MEMBERS

Das Gruppenverwalterrecht MANAGE-MEMBERS schließt das Gruppenverwalterrecht MANAGE-RESOURCES ein. Es berechtigt einen Gruppenverwalter zusätzlich dazu, seine eigene Benutzergruppe und die ihr untergeordnete Gruppenstruktur durch Einrichten, Umhängen und Löschen von Gruppenmitgliedern zu verändern.

Für die Verwaltung stehen folgende Kommandos zur Verfügung:

MODIFY-USER-GROUP	ADD-USER	COPY-TERMINAL-SET
SHOW-USER-GROUP	MODIFY-USER-ATTRIBUTES	CREATE-TERMINAL-SET
	REMOVE-USER	DELETE-TERMINAL-SET
	LOCK-USER	MODIFY-TERMINAL-SET
	UNLOCK-USER	SHOW-TERMINAL-SET
	SHOW-USER-ATTRIBUTES	
	SET-LOGON-PROTECTION	
	MODIFY-LOGON-PROTECTION	
	SHOW-LOGON-PROTECTION	

MANAGE-GROUPS

Das Gruppenverwalterrecht MANAGE-GROUPS schließt das Gruppenverwalterrecht MANAGE-MEMBERS ein. Es berechtigt einen Gruppenverwalter zusätzlich dazu, die seiner Benutzergruppe untergeordnete Gruppenstruktur durch Einrichten, Ändern, Löschen oder Umhängen von Untergruppen zu verändern.

Für die Verwaltung stehen folgende Kommandos zur Verfügung:

ADD-USER-GROUP	ADD-USER	COPY-TERMINAL-SET
MODIFY-USER-GROUP	MODIFY-USER-ATTRIBUTES	CREATE-TERMINAL-SET
REMOVE-USER-GROUP	REMOVE-USER	DELETE-TERMINAL-SET
SHOW-USER-GROUP	LOCK-USER	MODIFY-TERMINAL-SET
	UNLOCK-USER	SHOW-TERMINAL-SET
	SHOW-USER-ATTRIBUTES	
	SET-LOGON-PROTECTION	
	MODIFY-LOGON-PROTECTION	
	SHOW-LOGON-PROTECTION	

Die Berechtigung eines Gruppenverwalters gilt stets nur für das Pubset, auf dem die Benutzergruppe eingetragen ist.

Alle Tätigkeiten eines Gruppenverwalters beziehen sich nur auf die eigene Benutzergruppe (bei der Verwaltung der Gruppenmitglieder) oder auf hierarchisch untergeordnete Benutzergruppen eines Pubset (bei der Verwaltung von Untergruppen und deren Gruppenmitgliedern), jedoch nie auf hierarchisch übergeordnete Benutzergruppen oder auf Benutzergruppen in anderen Pubsets.

Das Gruppenpotential einer Benutzergruppe, also insbesondere auch das jeweilige Gruppenverwalterrecht, kann nur durch einen hierarchisch übergeordneten Gruppenverwalter oder einen systemglobalen Benutzerverwalter festgelegt oder geändert werden.

Für eine Benutzergruppe muss kein Gruppenverwalter ernannt werden. Ist für eine Benutzergruppe kein Gruppenverwalter ernannt, so wird sie von einem übergeordneten Gruppenverwalter oder einem systemglobalen Benutzerverwalter (mit-)verwaltet.

Wechsel des Home-Pubset

Im laufenden Betrieb des Betriebssystems ist auf eine sorgfältige Pflege von Home-Pubset und Stand-by-Pubsets zu achten. Da für die Zugriffskontrolle die Benutzergruppenstruktur des Home-Pubset relevant ist, sollten Benutzergruppenstrukturen auf Stand-by-Pubsets immer identisch gehalten werden mit der Benutzergruppenstruktur des Home-Pubset. Vorsicht ist insbesondere geboten beim Austausch eines Home-Pubset oder beim Einsatz des Home-Pubset auf einem anderen Rechner. Durch eine solche Veränderung der Umgebung können abweichende Ergebnisse bei der Zugriffskontrolle entstehen, wenn die Benutzergruppenstrukturen nicht identisch sind.

3.2.3 Aufbau einer Benutzergruppenstruktur

Der Aufbau der Benutzergruppenstruktur sollte in Abhängigkeit von den lokalen Gegebenheiten erfolgen. Eine Gruppenbildung muss immer gut geplant werden, um genau die Systemumgebung bereitzustellen, die von den Gruppenmitgliedern unbedingt benötigt wird. Nur eine genaue Analyse der Ansprüche einer Gruppe führt zu einem sinnvollen Sicherheitskonzept. Generell kann gesagt werden, dass möglichst die Benutzerkennungen und Anwendungen in einer Gruppe zusammengefasst werden sollen, die eine möglichst hohe Übereinstimmung hinsichtlich der Ansprüche an das System haben. Divergieren diese Ansprüche stark, müssen mehr Privilegien an diese Gruppe vergeben werden, als es für ein sicheres System gewünscht sein kann.

Es folgen Beispiele für Gruppenbildungen:

– Zusammenfassung von Benutzerkennungen und Anwendungen nach unterschiedlichen Kriterien (z.B. Sicherheitsabgrenzung, gemeinsame Datenbestände etc.) auf getrennten Pubsets.

– Festlegung von Zugriffsschutzmaßnahmen für Objekte (z.B. Dateien).

– Festlegung von Kontingenten bzw. Zuteilungsvorgaben für die Nutzung von Systemfunktionen und Systemressourcen.

– Festlegung der Organisation der Benutzerverwaltung.

Pubset-bezogener Aufbau der Benutzergruppenstruktur

Die Benutzergruppenstruktur wird pubset-bezogen aufgebaut, das heißt jeder Pubset besitzt eine eigene Benutzergruppenstruktur. Jede Benutzergruppe, die auf einem Pubset eingerichtet wird, ist immer die Untergruppe einer bereits bestehenden Benutzergruppe. Ausgehend von der Wurzel *UNIVERSAL kann die Benutzergruppenstruktur somit hierarchisch (einstufig oder mehrstufig) aufgebaut werden. Die Benutzergruppenstruktur eines Pubset ist im zugehörigen Benutzerkatalog hinterlegt.

Zu beachten ist, dass die Benutzergruppenstruktur auf verschiedenen Pubsets nach unterschiedlichen Aspekten organisiert werden kann, im laufenden Betrieb jedoch stets die Benutzergruppenstruktur des Home-Pubset als aktuelle Benutzergruppenstruktur gilt. Benutzergruppenstrukturen auf Daten-Pubsets werden deshalb sinnvollerweise unter dem Aspekt der Verwaltung von pubset-spezifischen Attributen organisiert.

Pubset-bezogene Organisation der Benutzerverwaltung

Die Benutzergruppenstruktur eines Pubset wird für die Verwaltung der dort eingetragenen Benutzergruppen und Benutzerkennungen herangezogen. Die aktuelle Benutzergruppe ist stets diejenige, die auf dem Home-Pubset abgelegt ist. Benutzergruppenstrukturen auf Daten-Pubsets werden nur dann eingerichtet, wenn Stand-by-Pubsets gewartet oder pubset-spezifische Attribute verwaltet werden sollen.

Zugangskontrolle für Benutzerkennungen im laufenden Betrieb

Die Benutzergruppenstruktur auf das als Home-Pubset zu verwendende Pubset ist dahingehend abzustimmen, dass die Festlegung der Gruppenpotentiale und die Zuordnung der Benutzerkennungen zu Benutzergruppen auf diesen Pubsets den Anforderungen der Benutzer und Anwendungen entspricht:

Bei der LOGON-Validierung wird der Eintrag der Benutzerkennung auf dem Home-Pubset des aktuellen Systemlaufs benutzt. Bei erfolgtem Systemzugang werden für die Benutzerkennung die Attribute wirksam, die für sie im Home-Pubset hinterlegt sind. Mit Verwendung eines anderen Pubset als Home-Pubset kann es demnach möglich sein, dass einer Benutzerkennung unter dem gleichen Namen andere Attribute zugewiesen werden bzw. sogar eine andere LOGON-Zugangskontrolle wirksam werden kann. Formell bedeutet das, dass eine Benutzerkennung erst eindeutig durch ihren Eintrag auf dem jeweiligen Home-Pubset definiert ist, also je nach Home-Pubset verschiedene Benutzerkennungen mit dem gleichen Namen vorliegen.

Zugriffskontrolle für systemspezifische Objekte

Die Benutzergruppenstruktur des aktuellen Home-Pubset wird für die Zugriffskontrolle zur Bestimmung der Gruppenzugehörigkeit einer Benutzerkennung oder Benutzergruppe bei Zugriffen auf Dateien oder Jobvariablen sowie auf systemspezifische Objekte (z.B. Memory Pools) herangezogen.

Pubsetbezogene Festlegung der Nutzung der Plattenkapazität

Durch das Gruppenpotential PUBLIC-SPACE-LIMIT und PUBLIC-SPACE-EXCESS wird der Rahmen abgesteckt, in dem einer Benutzerkennung die Berechtigung eingeräumt werden kann, Dateien auf dem jeweiligen Pubset anzulegen.

Bei der Erzeugung von Dateien und Jobvariablen auf einem Pubset werden die zugehörigen Attribute der Benutzerkennung dieses Namens auf diesem Pubset ausgewertet. Ggf. kann das Erzeugen von Dateien abgelehnt werden.

Festlegung von Zugriffsrechten für Benutzerkennungen für den Zugriff auf Dateien oder Jobvariablen

Die Festlegung von Zugriffsrechten für Benutzerkennungen für den Zugriff auf Dateien oder Jobvariablen ist immer abhängig von deren Zugehörigkeit zu einer Benutzergruppe auf dem Home-Pubset des aktuellen Systemlaufs.

Zusammenfassung

Die Benutzergruppenstruktur des Home-Pubset wird herangezogen, um Zugriffe auf Dateien oder Jobvariablen zu prüfen. Sie ist die allgemein gültige Benutzergruppenstruktur des aktuellen Systemlaufs.

Für Administrationszwecke können zusätzliche Benutzergruppenstrukturen auf Daten-Pubsets eingerichtet werden, um pubset-spezifische Attribute zu verwalten und Pubsets einzurichten und zu pflegen, die als Home-Pubsets eingesetzt werden sollen (Stand-by-Pubsets).

Ernennung/Absetzung eines Gruppenverwalters

Ein systemglobaler Benutzerverwalter oder ein hierarchisch übergeordneter Gruppenverwalter kann eine Benutzerkennung ’userid’ zum Gruppenverwalter ernennen mit dem Kommando:

```
/add-user-group ..., group-administrator=userid [,adm-authority=...]
```

bzw.

```
/modify-user-group ...,group-administrator=userid [,adm-authority=...]
```

In einer bestehenden Gruppe wird eine andere Kennung zum Gruppenverwalter gemacht mit dem Kommando

```
/modify-user-group ...,group-administrator=userid
```

In einer bestehenden Gruppe wird ein Gruppenverwalter seines Amtes enthoben mit dem Kommando

```
/modify-user-group ...,group-administrator=*none
```

3.2.4 Konzept der Verwaltung von Benutzern und Benutzergruppen

Die Vergabe der Berechtigungen zur Benutzerverwaltung im Rechenzentrum orientiert sich an der Auslastung der Anlage, am Anwendungsspektrum und an der Sicherheitspolitik des RZ-Betriebs. Deshalb werden die wichtigsten Einflussfaktoren für die Organisation der Benutzerverwaltung wie folgt zusammengefasst:

– Ein systemglobaler Benutzerverwalter ist für alle Benutzerkennungen und Benutzergruppen auf allen Pubsets uneingeschränkt verwaltungsberechtigt. Geltende (hierarchisch gestaffelte) Vorgaben und Maximalwerte können bei der Festlegung von Gruppenpotentialen außer Kraft gesetzt oder übergangen werden.

– Die Benutzergruppenstruktur ist jeweils für einen Pubset festgelegt, kann also von Pubset zu Pubset verschieden sein. Auf jedem Pubset ist die Benutzergruppe *UNIVERSAL die Wurzel der jeweiligen Benutzergruppenstruktur.

– Im Unterschied zu einem systemglobalen Benutzerverwalter besitzt ein Gruppenverwalter der Benutzergruppe *UNIVERSAL nur auf dem zugehörigen Pubset die Berechtigung zur Verwaltung aller Benutzerkennungen und Benutzergruppen entsprechend dem Gruppenverwaltungsrecht in der Ausprägung MANAGE-GROUPS. Obwohl die Benutzergruppe *UNIVERSAL unbegrenzte Ressourcen besitzt, ist ein Gruppenverwalter von *UNIVERSAL verpflichtet, die Regeln für den Gruppenverwalter zu beachten und Änderungen unter Wahrung einer jeweils in sich geschlossenen und abgestimmten Benutzergruppenstruktur vorzunehmen. Eine Verwaltung im direkten Zugriff wie bei einem systemglobalen Benutzerverwalter ist demnach nicht gegeben.

– Die Ernennung einer Benutzerkennung zum Gruppenverwalter einer Benutzergruppe kann von Pubset zu Pubset verschieden ausfallen, abhängig davon, ob die Benutzerkennung überhaupt auf dem Pubset eingetragen bzw. wie die Benutzergruppe in der jeweiligen Benutzergruppenstruktur angeordnet ist.

– Jeder Gruppenverwalter einer hierarchisch übergeordneten Gruppe ist auch Gruppenverwalter einer hierarchisch niedrigeren Gruppe. Dies bedeutet, dass ein Gruppenverwalter nicht notwendigerweise auch Gruppenmitglied der verwalteten Gruppe sein muss. So kann es Gruppen geben, von denen kein Mitglied Gruppenverwalter ist.

– Ein Gruppenverwalter hat stets die Vorgaben der zugehörigen übergeordneten Benutzergruppe bzw. zugehörigen Benutzergruppe zu beachten. Bei der Änderung der Benutzergruppenstruktur, der Zuordnung von Benutzerkennungen zu Benutzergruppen oder der Verteilung des Gruppenpotentials hat er ggf. erst sukzessive in der über- bzw. untergeordneten Benutzergruppenstruktur Anpassungen vorzunehmen, um die beabsichtigte Verwaltungsmaßnahme überhaupt durchführen zu können.

– Mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-MEMBERS werden die Zugangskontrolldaten für Benutzerkennungen festgelegt. Mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-RESOURCES können nur allgemeine Benutzerrechte (Ressourcen, Nutzungsrechte etc.) verwaltet werden.

- Für die Festlegung des Gruppenpotentials sind Vorgaben und Maximalwerte für allgemeine Benutzerrechte auf dem jeweiligen Pubset ebenso hierarchisch gliederbar wie die Benutzergruppenstruktur. Auf dem Home-Pubset wird festgelegt, welche Nutzungsberechtigung bzw. Vorgaben und Maximalwerte einer Benutzerkennung nach LOGON zugeordnet werden. Eine ggf. missbräuchliche Nutzung von Systemfunktionen und Systemressourcen kann mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-RESOURCES durch entsprechend abgestufte Vorgaben und Maximalwerte verhindert werden.
- Das Konzept der Benutzerverwaltung hat zum Ziel – entsprechend den jeweiligen Erfordernissen – Benutzerkennungen und Benutzergruppen zu organisieren und zugehörige Gruppenverwalter zu ernennen. Auf Grund des weiten Einflussbereiches eines systemglobalen Benutzerverwalters empfiehlt es sich, dessen Eingriffe auf notwendige, ggf. kurzzeitige Korrekturen zu beschränken. Eingriffe mit einer längeren Geltungsdauer sollten in einer abgestimmten Weise in der Benutzergruppenstruktur vorgenommen werden.
- Besonders durch, jeweils pubset-bezogen, unterschiedliche Gruppenverwalter der Benutzergruppe *UNIVERSAL lässt sich ein zentrales und geregeltes Benutzerverwaltungskonzept realisieren.
- Aus organisatorischen Gründen kann es sinnvoll sein, eine Benutzerkennung als systemglobalen Benutzerverwalter auf mehreren Pubsets einzutragen, die nicht Home-Pubset sind. Eine solche Benutzerkennung ist erst dann verwaltungsberechtigt, wenn einer dieser Pubsets zum Home-Pubset wird.

Rechte für die Benutzerverwaltung können in folgenden Abstufungen vergeben werden:

1. Systemglobaler Benutzerverwalter. Dieses Recht muss auf dem Home-Pubset eingetragen sein.
2. Gruppenverwalter der Benutzergruppe *UNIVERSAL mit gemeinsamen Benutzerkennungen auf allen Pubsets.
3. Gruppenverwalter der Benutzergruppe *UNIVERSAL mit pubset-bezogen unterschiedlichen, nur bedingt gemeinsamen Benutzerkennungen.
4. Gruppenverwalter für ausgewählte Benutzergruppen auf einem oder mehreren Pubsets (abhängig von der Benutzergruppenstruktur) als zentraler Gruppenverwalter mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-GROUPS für eine Teilstruktur der Benutzergruppenstruktur.
5. Gruppenverwalter für ausgewählte Benutzergruppen auf einem oder mehreren Pubsets (abhängig von der Benutzergruppenstruktur) als zentraler Gruppenverwalter mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-MEMBERS für eine Teilstruktur der Benutzergruppenstruktur.
6. Gruppenverwalter für ausgewählte Benutzergruppen auf einem oder mehreren Pubsets (abhängig von der Benutzergruppenstruktur) als Gruppenverwalter mit dem Gruppenverwalterrecht in der Ausprägung MANAGE-RESOURCES für eine Teilstruktur der Benutzergruppenstruktur.

3.2.5 Beispiele für Benutzergruppen

Beispiel 1: Gruppenstruktur nach First-Start

Mit dem First-Start des Betriebssystems wird eine flache Gruppenstruktur eingerichtet. Sie besteht aus der Benutzergruppe *UNIVERSAL mit den vom Betriebssystem standardmäßig eingerichteten Benutzerkennungen als Gruppenmitglieder.

Gruppe *UNIVERSAL

Wurzel der Gruppenstruktur	Benutzergruppenkennung *UNIVERSAL
Gruppenmitglieder	alle Systemkennungen (z.B. SERVICE, SYSHSMS, SYSPRIV, TSOS)
Gruppenverwalter	nicht vorhanden
Recht der Gruppenverwaltung	Kennung TSOS, da TSOS standardmäßig das Privileg systemglobale Benutzerverwaltung besitzt
Untergruppen	nicht vorhanden

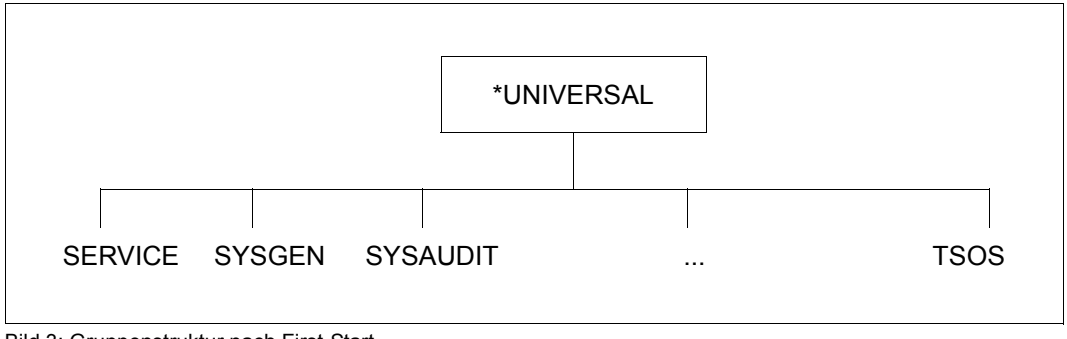


Bild 3: Gruppenstruktur nach First-Start

Beispiel 2: Einstufige Gruppenstruktur

Festlegung:
Systemglobale Benutzerverwaltung: Kennung TSOS

Gruppe *UNIVERSAL

Wurzel der Gruppenstruktur	Benutzergruppenkennung *UNIVERSAL
Gruppenmitglieder	alle Systemkennungen (z.B. SERVICE, SYSHSMS, SYSPRIV, TSOS) (siehe Beispiel 1) Benutzerkennungen uid01, uid02, uid03, uid04
Gruppenverwalter	nicht vorhanden*)
Recht der Gruppenverwaltung	Kennung TSOS
Untergruppen	GRUPPE01, GRUPPE02, GRUPPE03

*) TSOS kann wegen Ämterhäufung nicht Gruppenverwalter sein, er hat bereits das Recht der systemglobalen Benutzerverwaltung.

Gruppe GRUPPE01

Gruppenmitglieder	Benutzerkennungen uid11, uid12, uid13
Gruppenverwalter	Benutzerkennung uid11
Recht der Gruppenverwaltung	Kennung TSOS, uid11
Untergruppen	nicht vorhanden

Gruppe GRUPPE02

Gruppenmitglieder	Benutzerkennungen uid21, uid22, uid23
Gruppenverwalter	nicht vorhanden
Recht der Gruppenverwaltung	Kennung TSOS
Untergruppen	nicht vorhanden

Gruppe GRUPPE03

Gruppenmitglieder	Benutzerkennungen uid31, uid32, uid33, uid34
Gruppenverwalter	Benutzerkennung uid33
Recht der Gruppenverwaltung	Kennung TSOS, uid33
Untergruppen	nicht vorhanden

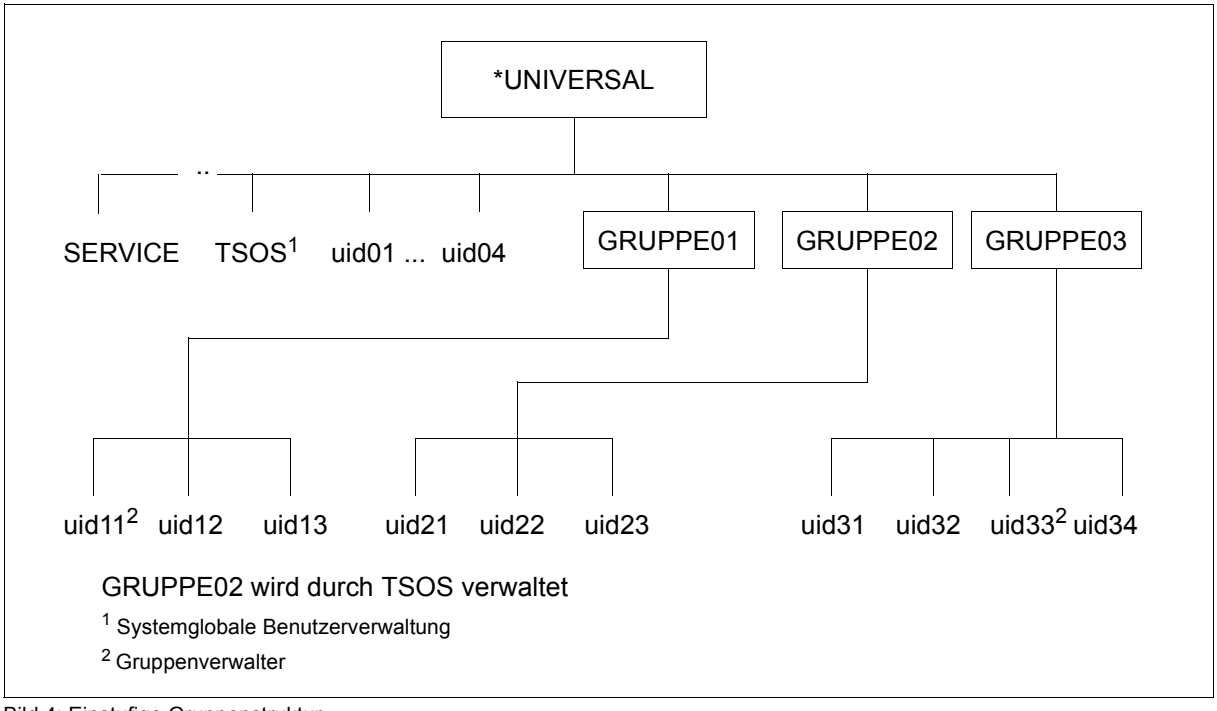


Bild 4: Einstufige Gruppenstruktur

Beispiel 3: Mehrstufige Gruppenstruktur

Festlegung:
Systemglobale Benutzerverwaltung: Kennung TSOS

Gruppe *UNIVERSAL

Wurzel der Gruppenstruktur	Benutzergruppenkennung *UNIVERSAL
Gruppenmitglieder	alle Systemkennungen (z.B. SERVICE, SYSHSMS, SYSPRIV, TSOS) (siehe Beispiel 1) Benutzerkennungen uid01, uid02, uid03, uid04
Gruppenverwalter	nicht vorhanden *)
Recht der Gruppenverwaltung	Kennung TSOS
Untergruppen	GRUPPE01, GRUPPE02, GRUPPE03

*) TSOS kann wegen Ämterhäufung nicht Gruppenverwalter sein, er hat bereits das Recht der systemglobalen Benutzerverwaltung.

Gruppe GRUPPE01

Gruppenmitglieder	Benutzerkennungen uid11, uid12, uid13
Gruppenverwalter	Benutzerkennung uid11
Recht der Gruppenverwaltung	Kennung TSOS und uid11
Untergruppen	GRUPPE04

Gruppe GRUPPE02

Gruppenmitglieder	Benutzerkennungen uid21, uid22, uid23
Gruppenverwalter	nicht vorhanden
Recht der Gruppenverwaltung	Kennung TSOS
Untergruppen	GRUPPE05

Gruppe GRUPPE03

Gruppenmitglieder	Benutzerkennungen uid31, uid32, uid33
Gruppenverwalter	Benutzerkennung uid33
Recht der Gruppenverwaltung	Kennung TSOS und uid33
Untergruppen	nicht vorhanden

Gruppe GRUPPE04

Gruppenmitglieder	Benutzerkennungen uid41, uid42, uid43 uid44, uid45
Gruppenverwalter	Benutzerkennung uid43
Recht der Gruppenverwaltung	Kennung TSOS, uid11 und uid43
Untergruppen	nicht vorhanden

Gruppe GRUPPE05

Gruppenmitglieder	Benutzerkennung uid51
Gruppenverwalter	nicht vorhanden
Recht der Gruppenverwaltung	Kennung TSOS
Untergruppen	GRUPPE06

Gruppe GRUPPE06

Gruppenmitglieder	Benutzerkennungen uid61, uid62, uid63
Gruppenverwalter	Benutzerkennungen uid61
Recht der Gruppenverwaltung	Kennung TSOS und uid61
Untergruppen	GRUPPE07

Gruppe GRUPPE07

Gruppenmitglieder	Benutzerkennungen uid71, uid72, uid73
Gruppenverwalter	Benutzerkennung uid73
Recht der Gruppenverwaltung	Kennung TSOS, uid61 und uid73
Untergruppen	keine

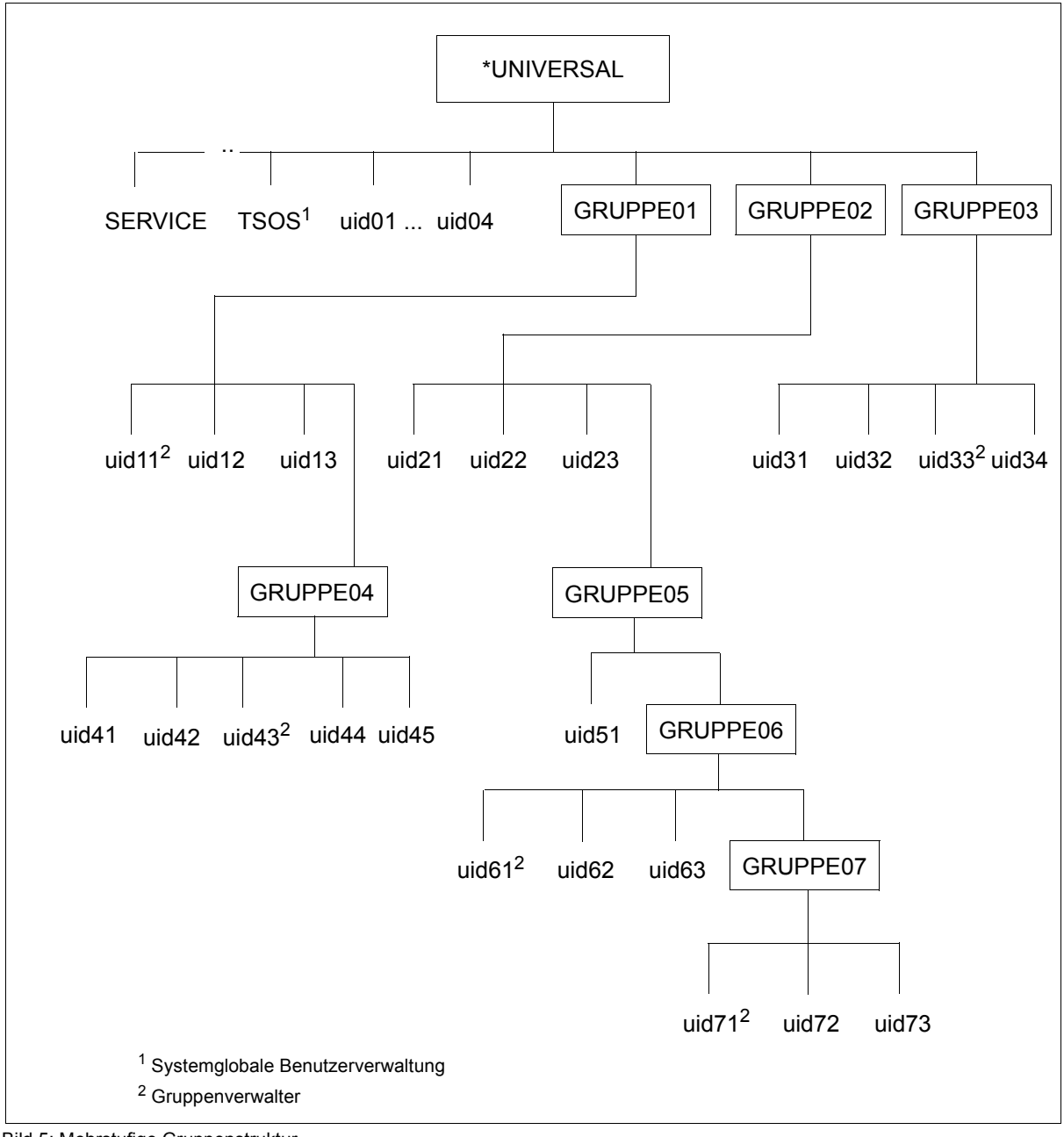


Bild 5: Mehrstufige Gruppenstruktur

3.2.6 Betriebsmittel der Benutzer begrenzen

Die Benutzerverwaltung kann für Benutzerkennungen und Benutzergruppen Vorgaben festlegen, um die Nutzung folgender Betriebsmittel zu begrenzen bzw. deren Missbrauch zu verhindern:

– Nutzung der Plattenspeicherkapazität auf den Pubsets

– Nutzung des Hauptspeichers

– Nutzung der Rechnerleistung (CPU-Kapazität)

Die gruppen- und benutzerbezogenen Betriebsmittel werden wie folgt zugeteilt:

```
/add-user-group group-identification=.., add-group-member=...
```
oder
```
/modify-user-group group-identification=.., add-group-member=...
```

```
/add-user user-identification=...
```
oder
```
/modify-user-attributes user-identification=...
```

Die tatsächliche Verteilungs-Steuerung und -Kontrolle dieser Betriebsmittel im Rahmen der vorgegebenen Werte erfolgt im Betriebssystem (z.B. Verwaltung der Taskkategorien, Steuerung durch PCS, Verwaltung von Jobstreams und Jobklassen,...).

Beispiel

Mit `/ADD-USER USER-ID=..,PUBLIC-SPACE-LIMIT=..,PUBLIC-SPACE-EXCESS=*NO, PUBSET=...` kann die systemglobale Benutzerverwaltung einer Benutzerkennung ein nicht überschreitbares Kontingent an Speicherplatz auf einem Pubset zur Verfügung stellen.

Zur Verwaltung von pubset-spezifischen Betriebsmitteln (PUBLIC-SPACE-LIMIT, PUBLIC-SPACE-EXCESS) ist es sinnvoll, Benutzergruppen auf importierten Pubsets (nicht Home-Pubset) einzurichten.

Alle systemglobalen Betriebsmittel, wie z.B. CPU-Limit, werden über die Gruppenstruktur des Home-Pubset verwaltet.

Festlegung		Kommando	Operanden
Nutzung der Plattenspeicherkapazität auf den Pubsets	Public-Space-Nutzung	ADD-/MODIFY-USER-GROUP	PUBSET=... PUBLIC-SPACE-LIMIT=..., PUBLIC-SPACE-EXCESS=... TEMP-SPACE-LIMIT=... JV-NUMBER-LIMIT=..., FILE-NUMBER-LIMIT=...
		ADD-USER/ MODIFY-USER-ATTRIBUTES	PUBLIC-SPACE-LIMIT=..., PUBLIC-SPACE-EXCESS=..., PUBSET=..., TEMP-SPACE-LIMIT=..., FILE-NUMBER-LIMIT=..., JV-NUMBER-LIMIT=...

Tabelle 2: Begrenzung der Nutzung von pubset-spezifischen Betriebsmitteln

Festlegung		Kommando	Operanden
Nutzung des Hauptspeichers im Rechner	Nutzung des Adressraums	ADD-/MODIFY-USER-GROUP	ADDRESS-SPACE-LIMIT=...
		ADD-USER/ MODIFY-USER-ATTRIBUTES	ADDRESS-SPACE-LIMIT=...
	Nutzung des Hauptspeichers	ADD-/MODIFY-USER-GROUP	RESIDENT-PAGES=...
		ADD-USER/ MODIFY-USER-ATTRIBUTES	RESIDENT-PAGES=...
	Task-(De-)Aktivierung	ADD-/MODIFY-USER-GROUP	ADD-ACCOUNT=..., (MAX-ALLOWED-CATEGORY=..., INHIBIT-DEACTIVATION=...)
		ADD-USER/ MODIFY-USER-ATTRIBUTES	ACCOUNT-ATTRIBUTES= (MAX-ALLOWED-CATEGORY=..., PRIVILEGE=*NO / *PARAMETERS(INHIBIT- DEACTIVATION=...))

Tabelle 3: Begrenzung der Nutzung von systemglobalen Betriebsmitteln (Teil 1 von 2)

Festlegung		Kommando	Operanden
Nutzung der Rechnerleistung (CPU-Kapazität)	CPU-Limit	ADD-/MODIFY-USER-GROUP ADD-USER/ MODIFY-USER-ATTRIBUTES	ADD-ACCOUNT=..., (CPU-LIMIT=..., NO-CPU-LIMIT=...) ACCOUNT-ATTRIBUTES= (CPU-LIMIT=..., PRIVILEGE=*NO / *PARAMETERS(NO-CPU-LIMIT=...))
	zulässige Ablaufpriorität	ADD-/MODIFY-USER-GROUP ADD-USER/ MODIFY-USER-ATTRIBUTES	ADD-ACCOUNT=..., (MAXIMUM-RUN-PRIORITY=...) ACCOUNT-ATTRIBUTES= (MAXIMUM-RUN-PRIORITY=...)
	zulässige Taskkategorien	ADD-/MODIFY-USER-GROUP ADD-USER/ MODIFY-USER-ATTRIBUTES	ADD-ACCOUNT=..., (MAX-ALLOWED-CATEGORY=...) ACCOUNT-ATTRIBUTES= (MAX-ALLOWED-CATEGORY=...)
	Scheduling-Recht	ADD-/MODIFY-USER-GROUP ADD-USER/ MODIFY-USER-ATTRIBUTES	ADD-ACCOUNT=..., (START-IMMEDIATE=...) ACCOUNT-ATTRIBUTES= (PRIVILEGE=*NO / *PARAMETERS(START-IMMEDIATE=...))
	Performance-Maßnahmen	ADD-/MODIFY-USER-GROUP ADD-USER/ MODIFY-USER-ATTRIBUTES	DMS-TUNING-RESOURCES=... DMS-TUNING-RESOURCES=...
Gruppenverwaltung	Präfix für Kennungen	ADD-/MODIFY-USER-GROUP	GROUP-MEMBER-PREFIX=...
	Präfix für Gruppen	ADD-/MODIFY-USER-GROUP	USER-GROUP-PREFIX=...

Tabelle 3: Begrenzung der Nutzung von systemglobalen Betriebsmitteln (Teil 2 von 2)

3.3 Zugangsschutz

Das derzeit am weitesten verbreitete Verfahren zur Zugangskontrolle ist der Schutz durch **Kennwörter**. Der Zugang ist nur den Benutzern erlaubt, denen das Kennwort bekannt ist. Außerdem kann der Zugang auf bestimmte **Zugangswege**, z.B. Dialog oder Batch, oder sogar auf bestimmte Terminals beschränkt werden (Seite 95). Der Einsatz von **Terminal-Sets** (Seite 96) erleichtert erheblich die Verwaltung von Terminals, von denen ein Zugang erlaubt oder verboten ist. Die Zugangswege Dialog und Batch können durch zusätzliche Bedingungen geschützt werden, die in **Guards** (Seite 104) definiert sind. Für Benutzerkennungen, zu denen üblicherweise mehrere Personen Zugang haben, empfiehlt sich der Einsatz der **persönlichen Identifizierung** (Seite 95). **Single Sign On** ermöglicht einem Benutzer durch einen einzigen Authentisierungsvorgang den Zugang zu allen von ihm benötigten Anwendungen, auch auf unterschiedlichen Rechnern. Im BS2000 steht für Single Sign On das Verfahren Single Sign On mit Kerberos (Seite 109) zur Verfügung.

3.3.1 Kennwortschutz

Der Kennwortschutz ist das derzeit gebräuchlichste Authentisierungsverfahren.

Dabei wird mit dem Kommando MODIFY-USER-PROTECTION ein bis zu 8 bzw. 32 Byte langes Kennwort für die Benutzerkennung vereinbart.

Durch organisatorische Maßnahmen kann der Kennwortschutz weiter verbessert werden. Dazu legt die Benutzerverwaltung mit dem Kommando MODIFY-LOGON-PROTECTION für den Benutzer explizit fest, welche Vorgaben er zwingend beachten muss:

– minimale Länge eines Kennwortes
– Komplexität eines Kennwortes
– Lebensdauer eines Kennwortes
– Zeitraum, in dem ein Kennwort nicht erneut verwendet werden darf (Kennwortsperre)

Minimale Länge eines Kennwortes

Die Benutzerverwaltung kann für jede Benutzerkennung eine minimale Länge bestimmen, die bei der Festlegung oder Änderung des Kennworts dieser Kennung eingehalten werden muss. Dadurch kann verhindert werden, dass

– eine Benutzerkennung ungesichert ist, weil überhaupt kein Kennwort definiert ist
– eine Benutzerkennung ungenügend gesichert ist, weil ein zu kurzes Kennwort definiert worden ist

Komplexität eines Kennwortes

Für jede Benutzerkennung kann festgelegt werden, nach welchen Vorgaben die Wahl eines Kennworts zu erfolgen hat. Damit soll verhindert werden, dass ein Benutzer Kennworte festlegt, die leicht zu merken oder zu erraten sind, wie z.B. der eigene Vorname.

Für die Kennwortvergabe einer Benutzerkennung kann definiert werden, dass

– nur höchstens zwei aufeinander folgende Zeichen gleich sein dürfen

– mindestens ein Buchstabe und eine Ziffer Bestandteil des Kennworts sein müssen

– mindestens ein Buchstabe, eine Ziffer und ein Sonderzeichen im Kennwort enthalten sein müssen

Lebensdauer eines Kennworts

Durch regelmäßiges Wechseln des Kennwortes wird die Wahrscheinlichkeit verringert, dass Unbefugte durch systematisches Ausprobieren von Kennwörtern das Kennwort erfahren. Außerdem wird so der Schaden begrenzt, wenn Unbefugte unbemerkt Kenntnis vom Kennwort erlangt haben.

Der Eigentümer einer Benutzerkennung kann dann sein Kennwort jederzeit ändern, wenn ihm dies für seine Kennung erlaubt ist. Sofern beim Einrichten oder Modifizieren festgelegt wird, dass PASSWORD-MANAGEMENT=*BY-ADMINISTRATOR gilt, kann nur der Systemverwalter ein Kennwort ändern. Generell müssen bei der Festlegung eines Kennworts alle Regeln beachtet werden, die für die Bildung von Kennwörtern gelten. Vor Ablauf der Lebensdauer eines Kennworts erhält der Benutzer vom Betriebssystem eine Warnung. Wird das Kennwort bis zum festgelegten Zeitpunkt nicht geändert, sperrt das Betriebssystem den Zugriff auf die Benutzerkennung.

Falls die Benutzerkennung mit `/SET-LOGON-PROTECTION ..., UNLOCK-EXPIRATION=*BY-ADMINISTRATOR-ONLY` eingerichtet wurde, kann dann nur der systemglobale Benutzerverwalter den Zugang wieder zulassen.

Ist die Benutzerkennung mit `/SET-LOGON-PROTECTION ..., UNLOCK-EXPIRATION=*BY-USER` eingerichtet, wird dem Anwender bei Angabe des verfallenen Kennwortes ein eingeschränkter Dialog-Zugang gewährt. Dabei hat der Anwender nur die Möglichkeit ein neues Kennwort zu vereinbaren oder die Dialog-Task wieder zu beenden.

Verbot der Kennwort-Neuvergabe für einen bestimmten Zeitraum (Kennwortsperre)

Das System unterstützt den Kennungsinhaber bei der Wahl eines neuen Kennwortes, indem in einem definierten Zeitraum die erneute Vergabe eines bereits verwendeten Kennwortes verbietet. Damit wird der Missbrauch von Kennwörtern, die Unbefugten bekannt wurden, weiter eingeschränkt.

Der Zeitraum, in dem ein bereits benutztes Kennwort gesperrt ist, ist einstellbar.

Außerdem kann die Häufigkeit von Kennwortänderungen eingeschränkt werden.

Lange Kennwörter

Der Benutzer kann ein „langes Kennwort“ zum Schutz seiner Benutzerkennung vereinbaren. Ein „langes Kennwort“ ist mindestens 9 und maximal 32 Zeichen lang. Damit kann der Benutzer Kennwörter vereinbaren, die leicht zu merken sind und mit der großen Variationsmöglichkeit dem Datenschutz gerecht werden.

Bei der Eingabe eines 9 bis 32 Zeichen langen Kennwortes konvertiert ein Hash-Algorithmus das „lange“ Kennwort in ein 8 Byte langes Kennwort. Das konvertierte, 8 Byte lange Kennwort wird im System zur Kennwortüberprüfung gespeichert (ggf. verschlüsselt).

Folgende Kommandos unterstützen die Eingabe „langer Kennwörter“:
- ADD-USER
- ENTER-JOB und ENTER-PROCEDURE
- MODIFY-LOGON-PROTECTION
- MODIFY-USER-ATTRIBUTES
- MODIFY-USER-PROTECTION
- PRINT-DOCUMENT
- SET-LOGON-PARAMETERS
- SET-LOGON-PROTECTION
- SET-PERSONAL-ATTRIBUTES
- SET-RFA-CONNECTION
- TRANSFER-FILE

Wird die Eingabe „langer Kennwörter“ nicht unterstützt, wie z.B. bei Programmschnittstellen, muss der Benutzer das konvertierte, 8 Byte lange Kennwort ermitteln und eingeben. Mögliche Vorgehensweisen sind:

- Das Subsystem SDF-P ist im lokalen System verfügbar:
  Das konvertierte Kennwort kann mit der Builtin-Funktion HASH-STRING ermittelt werden. Der Aufruf erfolgt mit den Parametern STRING='<langes_kennwort>' und LENGTH=8 (siehe auch Handbuch „SDF-P“ [24]). Da der Parameter STRING im Gegensatz zur Kennwortschnittstelle Groß-/Kleinschreibung unterscheidet, muss das „lange“ Kennwort in Großbuchstaben angegeben werden!
  Bei Kommandos und Anweisungen (SDF-Schnittstelle) kann mit Ausdrucksersetzung gearbeitet werden, d.h. für den Kennwort-Operanden wird z.B. PASSWORD='&(HASH-STRING(STRING='langes_kennwort',LENGTH=8))' eingegeben.
  Falls die Eingabe nicht über die SDF-Schnittstelle erfolgt, wird einer S-Variablen das Ergebnis der Builtin-Funktion zugewiesen und der Variablenwert mit SHOW-VARIABLE als X-Literal (da die konvertierte Zeichenfolge auch nicht eingebbare Zeichen enthalten kann) ausgegeben. Der Variablenwert wird an der Eingabeschnittstelle als Kennwort (<x-string>) eingegeben.
- Das Subsystem SDF-P ist im lokalen System nicht verfügbar:
  – Besteht Zugang zu einem anderen System, in dem SDF-P verfügbar ist, kann das konvertierte, 8 Byte lange Kennwort, wie zuvor beschrieben, über die Builtin-Funktion HASH-STRING ermittelt werden.
  – Das konvertierte, 8 Byte lange Kennwort kann bei der Systembetreuung erfragt werden (wenn im System nicht verschlüsselt wird).
  – Die betroffene Benutzerkennung wird kurzfristig mit einem „kurzen“ Kennwort geschützt.

Bei Einsatz von SECOS können für Kennwörter weitere Sicherheitsüberprüfungen benutzerspezifisch vereinbart werden. Die Default-Werte für die Minimal-Länge und die Minimal-Komplexität eines Kennworts sind mit *NONE (keine Überprüfung dieser Attribute) eingestellt. Die Änderung dieser Attribute auf Maximalwerte kann unter Umständen dazu führen, dass das aus einem „langen“ Kennwort konvertierte, 8 Byte lange Kennwort die Anforderungen nicht erfüllt. Deshalb sollte bei der Minimal-Länge der Wert 6 und bei der Minimal-Komplexität der Wert 2 nicht überschritten werden.

3.3.2 Trennung der Zugangswege

Folgende Zugangswege, die eine Benutzerkennung haben, können aus Sicherheitsgründen getrennt behandelt werden:

– DIALOG-ACCESS
– BATCH-ACCESS
– OPERATOR-ACCESS-TERMINAL
– OPERATOR-ACCESS-PROGRAM
– OPERATOR-ACCESS-CONS
– POSIX-RLOGIN-ACCESS
– POSIX-REMOTE-ACCESS
– NET-DIALOG-ACCESS

Da es nicht möglich ist, alle Zugangswege gleich gut zu sichern, ist es sinnvoll, für besonders zu schützende Benutzerkennungen nur bestimmte Zugangswege zu öffnen. So kann es z.B. sinnvoll sein, für eine Kennung der Systembetreuung den Zugang nur im Dialog zu gestatten.

Das Starten von Folgeaufträgen kann beschränkt werden. Dazu ist ein Guard mit einer Liste von Benutzerkennungen anzulegen, unter denen laufende Aufträge Folgeaufträge für eine bestimmte Benutzerkennung starten können.

Der Zugang zu bestimmten Benutzerkennungen kann auf bestimmte Terminals beschränkt werden, da jedes Terminal über seinen BCAM-Namen eindeutig identifizierbar ist. Diese Maßnahme ist besonders dann von Bedeutung, wenn viele Personen Zugang zu einem Terminal haben (z.B. im Universitätsbetrieb).

3.3.3 Einschränkung des Zugangs über Terminal-Sets

Terminal-Sets haben den Zweck, die Menge der Datensichtstationen, über die der Dialogzugang zu einer Benutzerkennung möglich ist, effektiv verwalten zu können. In einem Terminal-Set wird eine Liste von voll- oder teilqualifizierten Datensichtstationsnamen zusammengefasst. Listen von Terminal-Sets können einer Kennung positiv oder alternativ negativ zugeordnet werden (vgl. Kommando /MODIFY-LOGON-PROTECTION, Operand TERMINAL-SET=..., bzw. TERMINAL-SET=*EXCEPT(TERMINAL-SET=...), im Folgenden als Positivliste, bzw. Negativliste bezeichnet). Die in einer Positivliste definierten Stationen haben Dialogzugang, der Rest nicht. Die in einer Negativliste definierten Stationen haben keinen Zugang, der Rest hat Zugang. Eine Entscheidung für Negativlisten ist sorgfältig abzuwägen, weil die Menge der zugangsberechtigten Stationen unter Umständen unbestimmt ist.

Zusätzlich können Terminal-Sets mit einem Guard des Typs STDAC verknüpft werden. Auf diese Weise ist die Wirkung eines Terminal-Sets auch zeitlich steuerbar (Näheres siehe unter „Zugang zu einer mit Terminal-Sets geschützten Benutzerkennung“ auf Seite 98).

Zur Verwaltung der Terminal-Sets stehen folgende Kommandos zur Verfügung:

CREATE-TERMINAL-SET	Terminal-Set anlegen
MODIFY-TERMINAL-SET	Terminal-Set modifizieren
DELETE-TERMINAL-SET	Terminal-Set löschen
COPY-TERMINAL-SET	Terminal-Set kopieren
SHOW-TERMINAL-SET	Terminal-Set anzeigen

Berechtigt zur Verwaltung sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Terminal-Sets

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen, für Terminal-Sets der Klasse GROUP oder USER. Die Terminal-Sets müssen seiner Gruppe oder deren Mitgliedern zugeordnet sein.

Es gibt 3 Klassen (Namensräume) für Terminal-Sets, die durch ihren Eigentümer unterschieden werden:

– USER

  Eigentümer des Terminal-Sets ist eine bestimmte Benutzerkennung.

  Dieses Terminal-Set kann ausschließlich von der Benutzerkennung benutzt werden, die Eigentümer ist.

  Das Terminal-Set wird automatisch gelöscht, wenn die Kennung gelöscht wird.

– GROUP

  Eigentümer des Terminal-Sets ist eine Benutzer-Gruppe.

  Dieses Terminal-Set kann von allen Mitgliedern der Gruppe benutzt werden, die Eigentümer ist. Wenn eine Kennung die Gruppenmitgliedschaft verliert, verliert sie auch das Recht zur Benutzung des Terminal-Sets. Ist einer solchen Kennung keine zulässige Station mehr zugeordnet, besteht auch kein Dialogzugang mehr.

  Das Terminal-Set wird automatisch gelöscht, wenn die Gruppe gelöscht wird.

– SYSTEM

  Das Terminal-Set ist gemeinschaftlichem Eigentum zugeordnet.

  Berechtigt zur Verwaltung dieses Terminal-Sets ist ausschließlich der systemglobale Benutzer-Verwalter. Gruppenverwalter, die mindestens das Recht MANAGE-MEMBERS besitzen, können solche Terminal-Sets nur kopieren oder zuweisen.

Ein Terminal-Set wird durch seinen Namen und seinen Eigentümer identifiziert.

Im folgenden Beispiel handelt es sich daher um 4 unterschiedliche Terminal-Sets. Sie haben zwar alle denselben Namen, aber unterschiedliche Eigentümer:

Name	**Eigentümer (SCOPE)**
TSET1	*USER(USER-ID=USER1)
TSET1	*USER(USER-ID=USER2)
TSET1	*GROUP(USER-ID=GR1)
TSET1	*SYSTEM

Schutz einer Benutzerkennung mit Terminal-Sets

Der Schutz einer Benutzerkennung mit Terminal-Sets wird mit den Kommandos /SET-LOGON-PROTECTION oder /MODIFY-LOGON-PROTECTION vereinbart.

Dabei kann der Zugang für eine Datensichtstation oder eine Gruppe von Datensichtstationen explizit erlaubt (Positivliste) oder explizit verboten werden (Negativliste).

Zugang zu einer mit Terminal-Sets geschützten Benutzerkennung

Im Einzelnen gilt für den Zugang zu einer Kennung, die mit Terminal-Sets geschützt ist, Folgendes:

- Die Terminal-Sets werden daraufhin überprüft, ob der aktuelle Stationsname durch eine von ihnen erfasst wird (Näheres zu Stationsnamen finden Sie unter „Suche nach Datensichtstationsnamen“ auf Seite 100). Die Terminal-Sets werden in folgender Reihenfolge durchsucht:
  - Klassen USER, GROUP, SYSTEM
  - Innerhalb der Klassen alphabetisch nach den Namen der Terminal-Sets
- Falls eine Kennung über eine Positivliste von Terminal-Sets geschützt ist, gilt:
  Wird kein Terminal-Set gefunden, das den Stationsnamen enthält, besteht kein Zugang. Wird eines gefunden, dann wird geprüft, ob dieses Terminal-Set mit einem Guard des Typs STDAC verknüpft ist. Ist das nicht der Fall, besteht Zugang. Ist das Terminal-Set mit einem Guard verknüpft und liefert die Auswertung der in ihm definierten Zeitbedingungen ’wahr’, besteht Zugang. Ist das Ergebnis der Guard-Auswertung ’falsch’, besteht kein Zugang.

  Hinweis

  Das Ergebnis einer Guard-Auswertung ist immer ’falsch’, wenn das Guard nicht zugreifbar ist oder einen anderen Typ als STDAC aufweist.
- Falls eine Kennung über eine Negativliste von Terminal-Sets geschützt ist, gilt:
  Wird kein Terminal-Set gefunden, das den Stationsnamen enthält, besteht Zugang. Wird eines gefunden, dann wird geprüft, ob dieses Terminal-Set mit einem Guard verknüpft ist. Ist das nicht der Fall, besteht kein Zugang. Ist das Terminal-Set mit einem Guard verknüpft und liefert die Auswertung der in ihm definierten Zeitbedingungen ’wahr’, wird die Negativliste als wirksam betrachtet und es besteht kein Zugang. Ist das Ergebnis der Guard-Auswertung ’falsch’, wird die Negativliste als nicht wirksam betrachtet und es besteht Zugang.

*Hinweis zu den Operandenwerten TERMINAL-SET = *NO-PROTECTION bzw *NONE*

Der Standardwert *NO-PROTECTION definiert, dass kein Schutz über Terminal-Sets besteht.

Der Operandenwert *NONE ordnet der Kennung eine leere Liste von Terminal-Sets zu. Sind der Kennung alle Terminal-Sets entzogen worden, ist ihr ebenfalls die leere Liste (von Terminal-Sets) zugeordnet. In diesem Fall besteht der Schutz der Kennung mittels Terminal-Sets weiterhin, es wird aber kein Terminal-Set mit dem aktuellen Stationsnamen gefunden. Falls die Kennung durch eine Positivliste geschützt ist, besteht kein Zugang. Ist die Kennung durch eine Negativliste geschützt, haben alle Stationen Zugang.

Folgende Tabelle zeigt das Ergebnis der Zugangsprüfung:

Passender Name wurde gefunden in:	**Guard**			
	nicht angegeben	**nicht zugreifbar oder Typ nicht STDAC**	**Bedingungen wahr**	**Bedingungen falsch**
keinem Terminal-Set (Kennung ist durch Positivliste geschützt)	Zugang nicht erlaubt			
keinem Terminal-Set (Kennung ist durch Negativliste geschützt)	Zugang erlaubt			
Terminal-Set in Positivliste	Zugang erlaubt	Zugang nicht erlaubt	Zugang jetzt erlaubt	Zugang jetzt nicht erlaubt
Terminal-Set in Negativliste	Zugang nicht erlaubt	Zugang nicht erlaubt	Zugang jetzt nicht erlaubt	Zugang jetzt erlaubt

Suche nach Datensichtstationsnamen

Der Name, mit dem eine Datensichtstation identifiziert und nach dem in den Terminal-Sets gesucht wird, hängt davon ab, wie der Zugang zur Anwendung $DIALOG realisiert ist:

– Besteht ein unmittelbarer Zugang der Datensichtstation zu $DIALOG, wird diese anhand **eines** Paares von 8 Byte langen Namen identifiziert, die Emulation und PC bezeichnen (STATION und PROC bei der Ausgabe des Kommandos /SHOW-JOB-STATUS).

– Bei zwischengeschalteten Applikationen (wie z.B. OMNIS) gibt es **zwei** Paare 8 Byte langer Namen, und zwar einerseits Applikations- und Rechnername, auf dem die Applikation läuft (STATION und PROC) und den Original-Stations-/Rechnernamen, über den die Applikation bedient wird (O_STAT und O_PROC). Letzteres Paar wird von der Applikation selbst geliefert, es gilt nur dann als vertrauenswürdig, wenn der Applikationsname mit dem Zeichen $ beginnt und die Prüfung auf dem bezeichneten Rechner durchgeführt wird.

Welche Zugangsart vorliegt, kann somit leicht über das Kommando SHOW-JOB-STATUS ermittelt werden.

```
/show-job-status information=*all(terminal=*original)
TSN:      4L9W        TYPE:     3 DIALOG1  NOW:      2018-04-03.171133
JOBNAME:              PRI:      0 209
USERID:   K98USER     JCLASS:   JCDSTD     LOGON:    2018-04-03.1458
ACCNB:    ACCXYZ      CPU-MAX:    9000     CPU-USED:000007.0727
STATION:  BT200683    PROC:     D016ZE04
O_STAT:   DSB17166    O_PROC:   D016KR17
TID:      006001A8    UNP/Q#:     00/000
CMD:      SHOW-JOB-STATUS
```

Im ersten Fall (unmittelbarer Zugang), in dem es nur ein Namenspaar gibt, kann kein Prüfmodus angegeben werden. In das Terminal-Set ist das Namenspaar einzutragen (siehe Kommando /MODIFY-TERMINAL-SET, Operand TERMINAL-ENTRY=*ADD(...)) (siehe Seite 209).

Im zweiten Fall (zwischengeschaltete Applikation, zwei Namenspaare) stehen drei Prüfmodie zur Auswahl:

– CHECK-MODE=*STD: Wenn die Applikation vertrauenswürdig ist, wird nach dem Original Stations-/Rechnernamen gesucht, im Fall 'nicht vertrauenswürdig' besteht kein Zugang.

– CHECK-MODE=*NET-TERMINAL-NAME: Im Terminal-Set wird nach dem Paar Original-Stations-/Rechnernamen wie von der Applikation geliefert, gesucht.

– CHECK-MODE=*APPLICATION-TERMINAL-NAME: Im Terminal-Set wird nach dem Paar Applikations-/Rechnername gesucht.

Beispiel zur Prüfung von Datensichtstationsnamen

Es seien die folgenden 4 Datensichtstationseinträge definiert:

	PROCESSOR	STATION	CHECK-MODE
1	D016KR17	DSB17166	*STD
2	D016KR17	DSB17166	*NET-TERMINAL-NAME
3	D016KR17	DSB17166	*APPLICATION-TERMINAL-NAME
4	D016ZE04	OMNISAPP	*APPLICATION-TERMINAL-NAME

Auf dem Rechner D016ZE04 finden Zugangsversuche von verschiedenen Datensichtstationen statt. Die folgende Tabelle zeigt die Ergebnisse der Prüfung gegen die Datensichtstationseinträge der vorhergehenden Tabelle. Die Bezeichnungen in den Überschriften entsprechen den Feldnamen, die vom Kommando /SHOW-JOB-STATUS ausgegeben werden. „Ja“ als Ergebnis bedeutet, der Datensichtstationseintrag passt zur Datensichtstation, von der der Zugang erfolgt. „Nein“ heißt, der Datensichtstationseintrag passt nicht. Die Ziffern verweisen auf die Begründung für das Ergebnis:

Zwischengeschaltete Applikation	**Datensichtstation**				**Ergebnis der Prüfung gegen Datensichtstationseintrag**			
	PROC	STATION	O_PROC	O_STAT	1	2	3	4
nein	D016KR17	DSB17166	-	-	Ja[1]	Ja[1]	Ja[1]	Nein[4]
ja	D016ZE04	OMNISAPP	D016KR17	DSB17166	Nein[5]	Ja[2]	Nein[4]	Ja[1]
ja	D016ZE07	$APPNAME	D016KR17	DSB17166	Nein[6]	Ja[2]	Nein[4]	Nein[4]
ja	D016ZE04	$APPNAME	D016KR17	DSB17166	Ja[3]	Ja[2]	Nein[4]	Nein[4]

Begründungen:

[1]	PROC/STATION ist korrekt
[2]	O_PROC/O_STAT ist korrekt, PROC/STATION ist irrelevant
[3]	PROC/STATION ist vertrauenswürdig und O_PROC/O_STAT ist korrekt
[4]	PROC/STATION ist nicht korrekt
[5]	PROC/STATION ist nicht vertrauenswürdig, weil STATION nicht mit „$“ beginnt
[6]	PROC/STATION ist nicht vertrauenswürdig, weil PROC nicht der Rechner ist, auf dem der Zugang stattfindet

Beispiele zum Zugangsschutz mit Terminal-Sets

Beispiel 1

Der Dialogzugang zur Benutzerkennung USER0001 soll nur über das Terminal (Processor: D016KR17, Station: DSB17166) zulässig sein. Erfolgt der Zugang über eine Applikation, soll der originale Terminalname geprüft werden.

Das Terminal-Set TERMSET1 soll den Zugang überwachen.

```
/create-terminal-set terminal-set-name=termset1 ————————————————————  (1)
/modify-terminal-set terminal-set-name=termset1,terminal-entry= - ———  (2)
/   *add(processor=d016kr17,station=dsb17166, -
/        check-mode=*net-terminal-name)
/set-logon-protection user-id=user0001, - ———————————————————————————  (3)
/   password=*p(logon-password='userpas1'), -
/   dialog-access=*yes(terminal-set=termset1)
/show-terminal-set terminal-set-name=termset1, - ————————————————————  (4)
/                  information=*attributes(protected-user-ids=*yes)

Terminal-Set Attributes         --- Pubset B30D            2018-03-02 14:49:29
------------------------------------------------------------------------------
Terminal-Set:     TERMSET1/*SYSTEM                  Pubset:   B30D
Guard-Name:       *None
User-Information: *None
Terminal-Entries: (Processor,Station,Check-Mode)
 (D016KR17,DSB17166,N-)
Assigned Userids:
 USER0001
------------------------------------------------------------------------------
Terminal-Set Attributes                                          end of display
/show-job-status job-identification=*tsn(1erj),terminal=*original ———  (5)

TSN:     1ERJ       TYPE:    3 DIALOG   NOW:     2018-03-02.145034
JOBNAME: USER0001   PRI:     0 210
USERID:  USER0001   JCLASS:  JCDSTD     LOGON:   2018-03-02.1450
ACCNB:   USERACC1   CPU-MAX:   9999     CPU-USED:000000.0338
STATION: DSB17166   PROC:    D016KR17
O_STAT:  DSB17166   O_PROC:  D016KR17
TID:     000100A6   UNP/Q#:    17/012
```

(1) Das Terminal-Set TERMSET1 wird eingerichtet.

(2) Der Terminalname wird eingetragen. Das Attribut CHECK-MODE ist beim Zugang über Applikationen wie z.B. OMNIS von Bedeutung. Die Angabe *NET-TERMINAL-NAME bedeutet einen geringeren Schutz, da die Vertrauenswürdigkeit der jeweiligen Applikation selbst nicht vorausgesetzt wird.

(3) Terminal-Set TERMSET1 wird an Benutzerkennung USER0001 zugewiesen.

(4) Anzeige des fertigen Terminal-Sets.

(5) Anzeige des Job-Status nach erfolgtem Logon ohne zwischengeschaltete Applikation. Geprüft wird das Paar (STATION,PROC).

Beispiel 2

Der Dialogzugang zur Benutzerkennung USER0001 soll nur über den PC PGTD1234 zulässig sein. Der PC selbst wird nur innerhalb der Arbeitszeit von 08:00 bis 18:00 Uhr von autorisierten Mitarbeitern genutzt.

Das Terminal-Set TERMSET2 soll exklusiv der Benutzerkennung USER0001 zugeordnet sein und zusammen mit dem Guard GUARD002 den Zugang überwachen.

```
/create-guard guard002,scope=*host-system ————————————————————————  (1)
/add-access-conditions guard002,subjects=*user(user0001), - ————————  (2)
/   admission=*p(time=*interval(from=08:00,to=18:00))
/create-terminal-set termset2(scope=*user(user0001)) ————————————————  (3)
/modify-terminal-set termset2(scope=*user(user0001)), - ——————————————  (4)
/   terminal-entry=*add(processor=pgtd1234,station=*, -
/   check-mode=*net-terminal-name),guard-name=guard002
/set-logon-protection user0001,logon-password='userpas1', - ————————  (5)
/    dialog-access=*yes(terminal-set=termset2(scope=*user))
/show-terminal-set termset2(scope=*user(user0001)), - ————————————————  (6)
/    information=*attributes(protected-user-ids=*yes)

Terminal-Set Attributes          --- Pubset B30D            2018-03-02 14:51:25
------------------------------------------------------------------------------
Terminal-Set:     TERMSET2/*USER /USER0001          Pubset:   B30D
Guard-Name:       $TSOS.GUARD002
User-Information: *None
Terminal-Entries: (Processor,Station,Check-Mode)
 (PGTD1234        ,*               ,N-)
Assigned Userids:
 USER0001
------------------------------------------------------------------------------
Terminal-Set Attributes                                          end of display
/show-job-status job-identification=*tsn(1erk),terminal=*original ————  (7)

TSN:     1ERK       TYPE:    3 DIALOG   NOW:     2018-03-02.145215
JOBNAME: USER0001   PRI:     0 210
USERID:  USER0001   JCLASS:  JCDSTD     LOGON:   2018-03-02.1451
ACCNB:   USERACC1   CPU-MAX:   9999     CPU-USED:000000.0420
STATION: BT201748   PROC:    D016ZE04
O_STAT:  $$$06004   O_PROC:  PGTD1234
TID:     000100A7   UNP/Q#:    17/012
```

(1) Guard GUARD002 wird eingerichtet.

(2) Die Zugangsbedingung für die Benutzerkennung USER0001 wird im Guard vereinbart. Der Zugang zur Benutzerkennung USER0001 ist täglich von 08:00 bis 18:00 erlaubt.

(3) Terminal-Set TERMSET1 wird im Namensraum der Benutzerkennung USER0001 eingerichtet.

(4) In das Terminal-Set werden der PC PGTD1234 als zulässiger Terminalname und das Guard, das den Zugang regelt, eingetragen. Der Stationsname ist nicht von Bedeutung und wird mit Wildcard übergangen.

(5) Das Terminal-Set TERMSET2 wird der Benutzerkennung USER0001 zugewiesen.

(6) Anzeige des fertigen Terminal-Sets.

(7) Anzeige des Job-Status nach erfolgtem Logon über OMNIS. Geprüft wird das Paar (O_STAT,O_PROC).

3.3.4 Zugangsschutz mit Guards

Die Zugangswege Dialog und Batchauftrag können mit Guards geschützt werden. Der Zugang ist in diesem Fall nur dann erlaubt, wenn die Zugriffsbedingungen im entsprechenden Guard erfüllt sind. Das Subjekt, für das die Zugriffsbedingungen geprüft werden, hängt davon ab, ob persönliche Identifizierung verlangt ist oder nicht (siehe „Zusammenwirken der Operanden PERSONAL-LOGON, PASSWORD-CHECK und GUARD-NAME“ auf Seite 106).

Die beiden Instanzen systemglobaler Benutzerverwalter und Gruppenverwalter haben folgende Möglichkeiten, den Zugriffsschutz mit Guards zu verwalten:

– der System-Benutzerverwalter kann GUARDS unter seiner eigenen Benutzerkennung anlegen, verwalten und zum Zwecke der Zugangskontrolle an alle Benutzerkennungen zuweisen.

– der Gruppenverwalter kann GUARDS unter seiner eigenen Benutzerkennung anlegen, verwalten und zum Zwecke der Zugangskontrolle an die Mitglieder seine Gruppen zuweisen.

Handelt es sich bei einer der genannten Instanzen um eine Kennung mit dem Privileg GUARD-ADMINISTRATION, kann diese Guards unter beliebigen Benutzerkennungen anlegen, verwalten und zum Zwecke der Zugangskontrolle an die von ihr verwalteten Benutzerkennungen zuweisen.

ACHTUNG!
Berechtigt zur Verwaltung der Zugriffsbedingungen ist der Eigentümer des Guard, also die Benutzerkennung, unter der das Guard abgelegt ist. Diese Benutzerkennung hat damit das Recht, den Zugriff zu einer ihr unbekannten Zahl von Benutzerkennungen zu manipulieren. Es liegt in der Verantwortung der Systembetreuung, diese Situationen zu vermeiden.

Die gleiche Situation kann auch durch Degradierung eines Gruppenverwalters bzw. System-Benutzerverwalters entstehen.

3.3.5 Persönliche Identifizierung

Aus technischen und organisatorischen Gründen ist es oft notwendig, mehreren Personen Zugang zu einer Benutzerkennung zu verschaffen. Üblicherweise musste dazu allen zugangsberechtigten Personen das Kennwort und die Abrechnungsnummer mitgeteilt werden. Dieses Vorgehen hat den Nachteil, dass die Verantwortung für ein Kennwort nicht mehr auf eine Person begrenzt ist. Außerdem kann die Urheberschaft von Aktionen anhand der SAT-Einträge nur noch einem Personenkreis, nicht aber einer bestimmten Person zugeordnet werden.

Der Operand DIALOG-ACCESS des Kommandos /MODIFY-LOGON-PROTECTION wurde erweitert. Damit können für eine Benutzerkennung andere Benutzerkennungen als zusätzlich zugangsberechtigt festgelegt werden. Es wird eine personenspezifische Identifizierung/Authentisierung während der Dialogzugangsprüfung veranlasst. Die Benutzerkennung, die mit der personenbezogenen Identifizierung angegeben wurde, wird in die SAT-Einträge übernommen. Somit ist es möglich, Personen als Urheber einzelner Aktionen auch nachträglich zu ermitteln.

Für die persönliche Identifizierung steht das Kommando /SET-PERSONAL-ATTRIBUTES zur Verfügung. Es ermöglicht unmittelbar im Anschluss an das Kommando /SET-LOGON-PARAMETERS die Eingabe einer persönlichen Benutzerkennung mit deren Kennwort. Die Aufforderung zur persönlichen Identifikation wird durch Angabe PERSONAL-LOGON= *YES im Kommando /MODIFY-LOGON-PROTECTION bewirkt.

Die persönliche Benutzerkennung ist eine normale Benutzerkennung, die auch selbst als Logon-Benutzerkennung dienen kann.

Ausschlaggebend für die Rechte des Anwenders, der Zugang mittels persönlicher Identifizierung erlangt hat, bleiben allein die Rechte, die für die Logon-Kennung definiert sind. Die Rechte der persönlichen Kennung werden nur bei der Zugangsprüfung (s.u.) ausgewertet.

Im Benutzerkatalog wird prinzipiell nicht zwischen Logon- und persönlichen Benutzerkennungen unterschieden. Daher kann als persönliche Benutzerkennung jede beliebige Benutzerkennung angegeben werden.

Folgende Maßnahmen sind erforderlich, um einen Zugangsschutz mit der persönlichen Identifizierung zu realisieren:

- Einrichten von persönlichen Benutzerkennungen. Wird die Kennung nur zum Zwecke der persönlichen Identifizierung benötigt, genügt die Angabe von Name, Kennwort, Abrechnungsnummer.
- Angabe PERSONAL-LOGON=*YES
- Einrichten eines Guards, in dem Zugriffsbedingungen und persönliche Benutzerkennungen oder Gruppenamen als zugriffsberechtigte Subjekte festgelegt werden.
- Schutz des Dialogzugangs der Benutzerkennung, für die die persönliche Identifizierung eingeschaltet ist, mit diesem Guard.

Zusammenwirken der Operanden PERSONAL-LOGON, PASSWORD-CHECK und GUARD-NAME

Die Werte der Operanden PERSONAL-LOGON, PASSWORD-CHECK und GUARD-NAME (siehe Kommandos /SET- bzw. /MODIFY-LOGON-PROTECTION) können beliebig kombiniert werden. Allgemein gilt:

- Der Operand PASSWORD-CHECK (= *YES/*NO) regelt, ob das Kennwort der Logon-Kennung anzugeben ist oder nicht.
- Der Operand PERSONAL-LOGON (= *YES/*NO) regelt, ob bei Zugang zu dieser Kennung (LOGON) eine persönliche Identifizierung aufgefordert wird oder nicht.

Folgende Möglichkeiten ergeben sich:

- Standard-Einstellung
  (PASSWORD-CHECK=*YES,GUARD-NAME=*NONE, PERSONAL-LOGON=*NO):

  Nur Dialog-Logon mit dem Kennwort der Logon-Kennung ist zugelassen. Der Operand PASSWORD-CHECK regelt, ob das Kennwort der Logon-Kennung anzugeben ist oder nicht.

- Dialogzugangsregelung mittels GUARD ohne persönliche Identifizierung
  (GUARD-NAME = <name>, PERSONAL-LOGON = * NO):

  Über das Guard lassen sich zeitliche Bedingungen für den Dialogzugang einstellen. Mit dem im Guard anzugebenden Subjekt muss die Logon-Kennung erfasst werden (Name der Kennung, Gruppenangabe, *OTHERS-Zweig).

- Persönliche Identifikation ist zugelassen
  (PERSONAL-LOGON=*YES):

  Die Eingabe der persönlichen Kennung und ihres Kennwortes ist erforderlich (Kommando /SET-PERSONAL-ATTRIBUTES). Über ein Guard kann die Menge der für eine persönliche Identifizierung zulässigen Kennungen eingeschränkt werden. Diese Kennungen sind in dem Guard explizit oder über Gruppennamen als Subjekt anzugeben. Ist kein Guard spezifiziert (GUARD-NAME=*NONE), sind alle Kennungen zugelassen.

  Die Kennwortprüfung ist abhängig vom Operanden PASSWORD-CHECK:

  – Bei PASSWORD-CHECK=*YES werden sowohl das Kennwort der Logon-Kennung als auch das der persönlichen Kennung überprüft.

  – Im Falle von PASSWORD-CHECK=*NO ist die Kennwortprüfung ganz auf die Prüfung des Kennwortes der persönlichen Kennung verlagert.

    Falls die Logon-Kennung ein Kennwort besitzt und dieses beim Logon angegeben wird, wird auf die Anforderung einer zusätzlichen persönlichen Identifikation verzichtet. Die Logon-Kennung wird implizit zur persönlichen Identifizierung herangezogen.

Diese Vorgehensweise ermöglicht es insbesondere, dass Anwendungen, die den Zugang zum System über $DIALOG realisieren (wie z.B. RFA), ohne Anpassung Zugang zu Kennungen haben können, für die eine persönliche Identifizierung vereinbart ist.

Relevante Attribute bei der Zugangskontrolle

Zu beachten ist, dass mit dem Zulassen von Kennungen für eine persönliche Identifizierung Zugangsattribute dieser Kennungen wirksam werden. Die folgende Tabelle zeigt, welche Attribute in der Zugangskontrolle geprüft und damit relevant für den Zugang zur Logon-Kennung werden:

Kennung	Logon-	persönlich
Kennung gesperrt	ja	nein
Kennung abgelaufen	ja	ja
Dialog-Zugriff gesperrt	ja	nein
ACCOUNTNUMBER	ja	nein
Kennwort	ja	ja
PASSWORD-CHECK	ja	nein
GUARD	ja	nein
TERMINALS	nein	ja
TERMINAL-SETS	nein	ja

Von der persönlichen Benutzerkennung werden also jene Attribute herangezogen, die für die persönliche Authentisierung des Aufrufers benötigt werden, unabhängig davon, ob die Kennung gesperrt ist oder nicht. Ferner wird angenommen, dass der Zugang zur Logon-Kennung nur über die Sichtstationen der persönlichen Kennung erfolgen darf.

Beispiele zur persönlichen Identifizierung

Beispiel 1

Für den Dialogzugang zur Benutzerkennung USER0001 wird das persönliche Logon vereinbart. Jede persönliche Benutzerkennung soll zulässig sein. Die Kenntnis des Logon-Kennwortes von USER0001 soll nicht erforderlich sein.

```
/modify-logon-protection user-id=user0001, -
/       password=*p(logon-password='userpas1'), -
/       dialog-access=*yes(password-check=*no,personal-logon=*yes)
```

Bei der Einleitung eines Auftrags sind nun zwei Fälle zu unterscheiden:

1. Der Benutzer gibt beim Logon kein Kennwort an

   ```
   /set-logon-parameters user0001,useracc1
   %  SRM3205 PLEASE ENTER '/SET-PERSONAL-ATTRIBUTES' OR '?'
   /set-personal-attributes user0002,'userpas2'
   %  JMS0066 JOB '(NONE)' ACCEPTED ON 2018-03-02 AT 14:57, TSN = 8NI9
   ```

   Der Benutzer muss sich durch Angabe seiner eigenen Benutzerkennung und seines Logon-Kennwortes identifizieren und authentisieren.

2. Der Benutzer gibt beim Logon das Kennwort der Kennung USER01 an

   ```
   /set-logon-parameters user0001,useracc1,'userpas1'
   %  JMS0066 JOB '(NONE)' ACCEPTED ON 2018-03-02 AT 14:58, TSN = 8NJ2
   ```

   Das Logon wird implizit als persönliche Identifizierung gewertet. Damit hat sich der Benutzer als USER0001 authentisiert. Eine weitere Prüfung findet nicht statt.

Beispiel 2

Für den Dialogzugang zur Benutzerkennung USER0001 wird eine persönliche Identifizierung vereinbart. Nur die Benutzerkennungen USER0002 und USER0003 sollen zum Zugang berechtigt sein. Sie werden im Guard GUARD003 definiert. Die Kenntnis des Logon-Kennwortes von USER0001 ist erforderlich.

Zu diesem Zweck wird das Guard GUARD003 für systemweiten Zugriff eingerichtet. Die berechtigten Benutzerkennungen USER0002 und USER0003 werden als Subjekte eingetragen.

```
/create-guard guard003,scope=*host-system
/add-access-conditions guard003,subjects= -
/   *user((user0002,user0003)),admission=*yes
```

Anschließend wird für die Benutzerkennung USER0001 vereinbart, dass eine persönliche Identifizierung verlangt wird und der Zugang über das Guard GUARD003 geschützt wird.

```
/modify-logon-protection user-id=user0001, -
/       password=*p(logon-password='userpas1'), -
/       dialog-access=*yes(guard-name=guard003,personal-logon=*yes)
```

Das Logon muss unter Angabe des Logon-Kennwortes erfolgen. Zusätzlich muss sich der Benutzer persönlich identifizieren und authentisieren.

```
/set-logon-parameters user0001,useracc1,'userpas1'
%  SRM3205 PLEASE ENTER '/SET-PERSONAL-ATTRIBUTES' OR '?'
/set-personal-attributes user0002,'userpas2'
%  JMS0066 JOB '(NONE)' ACCEPTED ON 2018-03-02 AT 14:59, TSN = 8NJ4
```

3.3.6 Single Sign On mit Kerberos

In modernen komplexen Arbeitsumgebungen benötigen Benutzer häufig Zugriff auf mehrere Anwendungen, die sich zudem auf unterschiedlichen Rechnern befinden können. Dazu müssen sie oft verschiedene Kennungen und Kennwörter benutzen. Unterschiedliche Anwendungen legen möglicherweise auch unterschiedliche Regeln fest, denen die Kennwörter entsprechen müssen. Außerdem ist es häufig erforderlich, unterschiedliche Kennwörter in verschiedenen Intervallen zu ändern. All dies bedeutet einen erhöhten Verwaltungsaufwand. Dieser fällt nicht nur bei den Benutzern an, sondern auch bei der Benutzerverwaltung, die vergessene Kennwörter zurücksetzen und wegen abgelaufener Kennwörter gesperrte Kennungen freigeben muss.

Dieser erhöhte Verwaltungsaufwand kann durch den Einsatz eines Single-Sign-On-Systems (SSO-System) vermieden werden. Ein SSO-System ist ein System zur automatischen und komfortablen Anmeldung an Netzressourcen in heterogenen Netzwerken. Nach einer einmaligen Identifikation und Authentifikation – auch mit Hilfe einer Chipkarte – automatisiert ein SSO-System alle weitere Anmeldungen des Benutzers im Netz.

Kerberos-Konzept

Kerberos ist ein standardisiertes Netzwerk-Authentisierungsprotokoll, das am Massachussets Institute of Technology (MIT) entwickelt wurde.

Es handelt sich um ein Sicherheitssystem, das auf kryptographischen Verschlüsselungsverfahren basiert. Bei einer Authentisierung mit Kerberos werden keine Kennwörter im Klartext über das Netzwerk gesendet. Dadurch wird das Abfangen von Kennwörtern im Netzwerk verhindert.

Die aktuelle Version von Kerberos ist in RFC1510 (Request for Comments) standardisiert. Die Standards selber sind definiert durch die Internet Engineering Task Force (IETF) und die Internet Engineering Steering Group (IESG). Umfassende Informationen zu den RFCs sind auf der Homepage der IETF zu finden: http://www.ietf.org/rfc/

Kerberos arbeitet mit symmetrischer Verschlüsselung, d.h. alle Schlüssel liegen an zwei Stellen vor, beim Eigentümer eines Schlüssels (Principal) und beim KDC (Key Distribution Center). Ein Schlüssel wird vom Kennwort eines Principals abgeleitet.

Kerberos-Principal

Der Kerberos-Principal hat einen eindeutigen Namen, der aus beliebig vielen Komponenten bestehen kann. SECOS unterstützt maximal 1800 Bytes für den Principal-Namen. Jede Komponente ist durch den Komponenten-Separator '/' voneinander getrennt. Die letzte Komponente ist der Realm, der von den übrigen Komponenten durch den Realm-Separator '@' getrennt ist.

Der Name des Principal einer Anwendung ist üblicherweise aus drei Komponenten aufgebaut: Anwendung, Instanz und Realm. Das Format eines typischen Kerberos-V5-Principal-Namens ist:

```
Anwendung/Instanz@REALM
```

mit

`Anwendung`	'host' für die Anwendung $DIALOG oder der Name der Anwendung
`Instanz`	DNS-Name des Rechners, auf dem die Anwendung läuft
`REALM`	Name der Kerberos-Domäne, per Konvention in Großbuchstaben dargestellt

Beispiel für einen typischen Kerberos-Principal im BS2000

```
host/bs2osd.fts.net@FTS.NET
```

Im BS2000 muss der Name des Principal mit dem SECOS-Kommando /ADD-KEYTAB-ENTRY in die Key-Tabelle aufgenommen werden.

Der Administrator des Windows Domain Controller muss einen Service Account für den Client einrichten (siehe dazu auch das Beispiel auf Seite 113).

Voraussetzungen für den Einsatz von Kerberos

- KDC

  Es wird ein bestehender KDC vorausgesetzt, z.B. der „Domain Controller“ (PDC) von Windows 2000, der diese Funktionalität unterstützt.

- Client

  Wird am Client-PC über eine Terminal-Emulation eine Verbindungsanforderung zu BS2000 gestellt, so ist es Aufgabe der Terminal-Emulation, sich ein gültiges Ticket zu besorgen und dieses dann an das BS2000-System weiterzureichen.

  Die Client-Betriebssysteme müssen „kerberos-fähig“ sein:

  – Windows-Systeme bieten die Kerberos-Unterstützung standardmäßig ab Windows 2000 (also auch bei Windows XP und Windows Server 2003) in den SSPI-Bibliotheken. Die SSPI-Aufrufe sind bereits ab Windows 95 möglich.

  – für UNIX-Systeme stehen GSSAPI-Bibliotheken frei zur Verfügung, zudem sind sie in manche Betriebssysteme (zum Beispiele Solaris ab Sun OS 5.8) integriert. Die C-Bindings von GSSAPI sind standardisiert (RFC 2744).

  – Die Terminal-Emulation muss die Authentisierung mit Kerberos unterstützen. Wenden Sie sich bitte diesbezüglich an den Hersteller Ihrer Terminal-Emulation.

- Server

  Der Server (BS2000) muss erkennen, dass die Verbindung „kerberos-fähig“ ist. Dazu muss sich der Client (z.B. die Terminal-Emulation) beim Verbindungsaufbau als DSS9763 (Device Type `X'4F'`) anmelden.

Ablauf einer Authentisierung bei Start einer $DIALOG-Verbindung in das BS2000

- Der Benutzer an einer Terminal-Emulation öffnet den BS2000-Dialog wie gewohnt.
- Das BS2000 schickt eine LOGON-Aufforderung an die Emulation.
- Der Benutzer gibt das Kommando /SET-LOGON-PARAMETERS mit Jobname, Benutzerkennung, Abrechnungsnummer und gegebenenfalls weiteren Operanden, jedoch ohne Kennwort, ein.
- Für den Benutzer unsichtbar laufen daraufhin folgende Aktionen ab:

  – Das BS2000 schickt eine Ticket-Anforderung an die Terminal-Emulation.

  – Diese besorgt sich ein Ticket vom Key Distribution Center und schickt es an das BS2000.

  – Dort wird das Ticket durch Entschlüsseln validiert.

– Schließlich wird im BS2000 geprüft, ob der als Kerberos-Principal identifizierte Besitzer des Tickets Zugriff auf die im Kommando /SET-LOGON-PARAMETERS angegebene Benutzerkennung hat. Abhängig vom Ergebnis dieser Prüfung wird der Zugang gewährt oder abgelehnt.

Das Ergebnis der Authentisierung wird in BS2000 in einem SAT-Record abgelegt.

Bei Einsatz des Produkts Jobvariablen enthält die System-Jobvariable $SYSJV.PRINCIPAL den Namen des Principal.

Kommandos zum Zugangsschutz

Die Kommandos zur Vereinbarung des Zugangsschutzes für eine Kennung wurden in der Zugangsklasse NET-DIALOG-ACCESS um die Kerberos-Principals erweitert. Damit kann festgelegt werden, welchen Principals der Zugang zu dieser Kennung erlaubt ist, und ob zur Gewährung des Zugangs ein Kennwort erforderlich ist.

Die betroffenen Kommandos sind:

/SET-LOGON-PROTECTION
/MODIFY-LOGON-PROTECTION
/SHOW-LOGON-PROTECTION

Verwaltung der Schlüssel in der Key-Tabelle

Die geheimen Schlüssel auf dem BS2000-Host werden in der Key-Tabelle verwaltet. Ein Eintrag in der Key-Tabelle besteht aus dem Namen des BS2000-Rechners, wie er im KDC (Key Distribution Center) eingetragen ist, und mehreren Schlüsseln, die über kryptographische Verfahren aus dem angegebenen Kennwort und dem Rechnernamen abgeleitet werden. Das Kennwort selbst wird nicht gespeichert.

Folgende Kommandos verwalten die Key-Tabelle:

/ADD-KEYTAB-ENTRY
/MODIFY-KEYTAB-ENTRY
/REMOVE-KEYTAB-ENTRY
/SHOW-KEYTAB-ENTRY

BS2000-Komponente SECOS-KRB

Die SECOS-Komponente SECOS-KRB enthält die Schnittstelle zur Abwicklung der Kerberos-Authentisierung im BS2000.

Beispiel

Eine BS2000-Benutzerkennung soll in ein Single-Sign-On-Verfahren auf Basis einer Windows-Domänenkennung eingebunden werden, so dass ein an Windows angemeldeter Benutzer beim Kommando /SET-LOGON-PARAMETERS kein Passwort mehr angeben muss.

Für das folgende Beispiel gelten folgende Voraussetzungen für die Software-Konfiguration:

Windows-Server (Domain-Controller)
– Windows 2000 oder Windows Server 2003

Windows-Clients (PCs der BS2000-Nutzer)
– Windows 2000, Windows XP oder Windows Server 2003
– Terminal-Emulation mit Unterstützung des Terminal-Protokolls für Kerberos im BS2000.

Gehen Sie dazu im Windows Domain Controller und im BS2000 wie folgt vor:

1. Im Windows Domain Controller
   – Stellvertreterkennung auf dem Domain Controller einrichten

     Für das BS2000-System müssen auf dem Domain Controller Kerberos-Schlüssel hinterlegt werden. Dazu wird eine Stellvertreterkennung auf dem Domain-Controller eingerichtet:

     ► Starten Sie das Active Directory Management Tool.

     ► Klicken Sie mit der rechten Maustaste auf den Ordner „Benutzer“ und wählen Sie die Funktion *Neu: Benutzer* aus.

     ► Tragen Sie den Namen der Benutzerkennung ein.

     ► Speichern Sie die Benutzerkennung.

     Der Name der Benutzerkennung ist frei wählbar. Es ist sinnvoll, einen Namen zu wählen, der auf die Verwendung als Platzhalter für ein BS2000-System hinweist.

– Im Domain Controller den Kerberos-Namen für das BS2000-System zuweisen

  Der Stellvertreterkennung wird per „Account Mapping“ zusätzlich der Name eines BS2000-Rechners in Kerberos-Notation zugewiesen.

  ► Geben Sie folgendes Kommondo im DOS-Fenster an:

  ```
  ktpass -princ host/hostname@NT-DNS-REALM-NAME -mapuser account
  -pass password -ptype KRB5_NT_PRINCIPAL -out keytab-entry
  ```

  Die Parameter sind:

`hostname`	DNS-Name des BS2000-Systems
`NT-DNS-REALM-NAME`	DNS-Name der Active-Directory-Domäne. Dieser Name ist ein fester Wert für jede Active-Directory-Domäne.
`account`	Stellvertreterkennung
`password`	Kennwort für die Stellvertreterkennung (max.127 Zeichen)
`KRB5_NT_PRINCIPAL`	Kerberos Principal (ab Windows Server 2003)
`keytab-entry`	Ausgabedatei für Keytab-Eintrag

  Hinweise

  – Das Kommando ist in der **englischen** Microsoft Knowledge Base beschrieben. Sie finden die Beschreibung im Internet unter http://support.microsoft.com. Klicken Sie auf *Knowledge Base Suche* und füllen Sie das Formular folgendermaßen aus:
    – Englische Knowledge Base
    – Suchbegriff: ktpass
    – Art der Suche: Nur Titel

  – Das gleiche Kennwort wird im nächsten Schritt auch im BS2000 angegeben. Verwenden Sie auf jeden Fall ein gutes, nicht erratbares Kennwort. Wer dieses Kennwort kennt und über Programmiererfahrung verfügt, kann sich dem BS2000 gegenüber nach Belieben identifizieren.

  – Windows und BS2000 verwenden unterschiedliche Zeichenkodierung (ASCII bzw. EBCDIC). Außerdem können auf beiden Systemen länderspezifische Zeichensatzvarianten installiert sein. Verwenden Sie deshalb nur Zeichen aus dem „Internationalen“ Zeichensatz, also keine Umlaute. Nehmen Sie lieber ein etwas längeres Kennwort, um das „Erraten“ zu erschweren, z. B.

  ```
  ktpass -princ host/d016ze04.mch.fts.net@FTS.NET
  -mapuser d016ze04
  -pass liebereinbisschenlaenger
  -ptype KRB5_NT_PRINCIPAL
  -out keytab-entry
  ```

– Ab Windows Server 2003 versendet das KDC die Tickets mit einer Key Version Number (KVNO). Es muss sichergestellt werden, dass die entsprechende KVNO auch im BS2000 eingetragen wird. Beachten Sie dazu die entsprechende Ausgabe des `ktpass` Kommandos.

```
.
.
.
Successfully mapped host/d016ze04.mch.fts.net to d016ze04.
Key created.
Output keytab to keytab-entry:
Keytab version: 0x502
keysize 46 host/d016ze04.mch.fts.net@FTS.NET ptype 1
(KRB5_NT_PRINCIPAL) vno 3 etype 0x3 …
```

2. Im BS2000

   – Kerberos-Schlüssel im BS2000 einrichten

     Die Verwaltung der Kerberos-Schlüssel im BS2000 unterliegt dem Sicherheitsbeauftragten (standardmäßig die Benutzerkennung SYSPRIV). Das Kommando dazu lautet:

     ```
     /ADD-KEYTAB-ENTRY *STD, 'host/hostname@NT-DNS-REALM-NAME' -
     /  ,KEY    = *PASSWORD('password',KEY-VERSION=<key_version_number>)
     ```

     Für `hostname`, `NT-DNS-REALM-NAME`, `password` und `key version number` müssen dieselben Werte angegeben werden wie im Domain Controller. Bitte beachten Sie, dass speziell NT-DNS-REALM-NAME per Konvention in Großbuchstaben angegeben werden muss.

     Beispiel

     ```
     /ADD-KEYTAB-ENTRY *STD, 'host/dO16ze04.mch.fts.net@FTS.NET' -
     /  ,KEY    = *PASSWORD('liebereinbisschenlaenger',KEY-VERSION=3)
     ```

     Alternativ steht das Kommando CONVERT-KEYTAB zur Verfügung mit dessen Hilfe das Einrichten des Kerberos-Schlüssels im BS2000 vereinfacht wird.

     CONVERT-KEYTAB unterstützt bei Verfügbarkeit von openFT und entsprechender TRANSFER-ADMISSION die Übertragung der Ausgabedatei für den Keytab-Eintrag (im obigen Beispiel "keytab-entry") vom Domain Controller zum BS2000 und die automatische Umsetzung in entsprechende Kommandos zum Eintragen des Schlüssels im BS2000.

     CONVERT-KEYTAB fügt die Schlüssel der verschiedenen Verschlüsselungsarten aus der Keytab-Datei hinzu (falls die Keytab-Datei mit dem ktpass-Befehl und der Option `crypto -all` erstellte wurde).

     Beispiel

     ```
     /CONVERT-KEYTAB TRANSFER-ADMISSION=getktpass,PARTNER=DOMAINCTL
     ```

     Die von CONVERT-KEYTAB erzeugte Kommandodatei CONVKTAB.JCL muss dann unter der Kennung des Sicherheitsbeauftragten zum Ablauf gebracht werden. Hierfür ist es erforderlich, dass die Kennung des Sicherheitsbeauftragten das Privileg STD-PROCESSING besitzt.

– Benutzerkennung für Windows-Domänenkennung freischalten

  Als letzter Schritt wird für eine BS2000-Benutzerkennung festgelegt, welche Windows-Kennungen zugriffsberechtigt sind. Für den „Single-Sign-On“-Gedanken ist es dabei sinnvoll, auf die Prüfung des BS2000-spezifischen Kennworts zu verzichten. Das Kommando, das der Benutzerverwalter eingeben muss, lautet:

```
/MODIFY-LOGON-PROTECTION userid -
/  ,NET-DIALOG-ACCESS=*YES -
/    (PASSWORD-CHECK=*NO -
/    ,ADD-PRINCIPAL='windowsaccount@NT-DNS-REALM-NAME')
```

  Die Parameter sind:

  `userid` BS2000-Benutzerkennung, für die Single Sign On eingeführt werden soll.

  `windowsaccount` Domänen-Kennung des Benutzers, der Zugriff auf die BS2000-Benutzerkennung erhalten soll.

  `NT-DNS-REALM-NAME` DNS-Name der Active-Directory-Domäne, wie schon beim Einrichten des Schlüssels vergeben.

  Beispiel

```
/MODIFY-LOGON-PROTECTION TSOS -
/  ,NET-DIALOG-ACCESS=*YES -
/    (PASSWORD-CHECK=*NO,ADD-PRINCIPAL='MCHHJoer@FTS.NET')
```

  Hinweise

  – Für eine BS2000-Benutzerkennung können auch mehrere Windows-Accounts zugriffsberechtigt sein.

  – Die Windows-Benutzerkennung und der NT-DNS-REALM-NAME werden als Wildcard-Strings interpretiert.

Unterstützte Verschlüsselungsarten

SECOS unterstützt Verbindungen mit folgenden Verschlüsselungsarten:

– DES-CBC-CRC

– DES-CBC-MD5

– ARCFOUR-HMAC

– AES128-CTS-HMAC-SHA1-96

– AES256-CTS-HMAC-SHA1-96

3.3.7 Protokollierung der Zugangsversuche

Um dem Anwender die Überwachung seiner eigenen Benutzerkennung zu ermöglichen, werden die Zugangsversuche protokolliert. Diese Information wird auf zwei Arten ausgegeben.

1. Bei jedem Dialog-Zugang wird mit der Meldung SRM3203 die Information über den letzten **erfolgreichen** Dialog-Zugang ausgegeben.

   Die Ausgabe dieser Meldung wird standardmäßig unterdrückt, kann aber von der Systembetreuung aktiviert werden (siehe „Systemglobale Einstellung der Ausgabe der Meldung SRM3203“ auf Seite 119).

2. Mit dem Kommando /SHOW-LOGON-PROTECTION kann die Information über die letzten Zugangs**versuche** ausgegeben werden.

   Näheres zum Inhalt dieser Information finden Sie bei der Beschreibung des Kommandos /SHOW-LOGON-PROTECTION auf Seite 283.

Die Zugangskontrolle kann maximal 40 Einträge über Zugangsversuche in der SRPM-Datei abspeichern, und versucht dort soviel Information für den Kennungsinhaber zu hinterlegen wie möglich. Daher wird wie folgt verfahren:

– Jede Zugangsklasse wird einer der folgenden Gruppen zugeordnet:
  Dialog, Batch, Remote-Batch, POSIX, Operating und File-Transfer.

– Das Kontingent von 40 Einträgen wird zu gleichen Teilen auf die tatsächlich vorkommenden Gruppen verteilt, ungenutzte Reservierungen entstehen nicht.

– Einträge erfolgreicher Zugänge und erfolgloser Zugangsversuche werden gleichermaßen festgehalten. Ist das Kontingent einer Gruppe ausgeschöpft, werden die ältesten Einträge der größten Gruppe verdrängt. Dabei wird versucht die Anzahl der Einträge für erfolgreiche Zugänge größer zu halten als die der Einträge für erfolglose Zugangsversuche.

Hinweis

Protokolliert werden auch Zugangsversuche durch Dienste, die der Anwender in Anspruch nimmt und die zeitversetzt erfolgen, wie z.B. Open File Transfer. Unter Umständen kann daher die Urheberschaft eines Protokolleintrages nicht unmittelbar einsichtig sein. Will man in solchen Fällen genaueres über den Zugang erfahren, müssen die SAT-Einträge überprüft werden.

Systemglobale Einstellung der Ausgabe der Meldung SRM3203

Die Systembetreuung kann systemglobal festlegen, ob beim Dialog-Zugang die Meldung SRM3203 über den letzten erfolgreichen Dialogzugang ausgegeben werden soll oder nicht. Die Ausgabe dieser Meldung wird standardmäßig unterdrückt. Manche Anwendungen, die über $DIALOG den Zugang zum BS2000 realisieren (z.B. RFA, FT sowie Kundenanwendungen), können diese Meldung möglicherweise nicht verarbeiten.

Das Ein- und Ausschalten der Meldung erfolgt durch einen Eintrag in der Subsysteminformationsdatei von SRPMOPT ($TSOS.SYSSSI.SRPMOPT.<version> auf dem Home-Pubset). Dieser Eintrag beginnt in Spalte 1 der Datei und hat folgende Syntax:

– Wenn die Meldung SRM3203 ausgegeben werden soll:

```
LAST-DIALOG-LOGON-MESSAGE=Y
```

– Wenn die Meldung SRM3203 nicht ausgegeben werden soll:

```
LAST-DIALOG-LOGON-MESSAGE=N
```

Diese Information wird während der Startup-Verarbeitung ausgewertet. Erfolgt beim Zugriff auf die Subsysteminformationsdatei ein Fehler oder enthält sie nicht verwertbare Informationen, wird dies mittels eines Serslog-Eintrags protokolliert.

3.3.8 Sperrung von Terminals/Benutzerkennungen nach erfolglosen Zugangsversuchen

Eine Benutzerkennung bzw. ein Benutzer soll nach einer vorgegebenen Anzahl von abgewiesenen Zugangsversuchen für eine begrenzte Zeit gesperrt werden. Diese Funktion wird „Suspendierung“ genannt. Die Suspendierung einer Benutzerkennung ist zwar die wirksamste Reaktion, kann aber dazu führen, dass neben dem Eindringling auch autorisierte Benutzer blockiert werden. Um dies zu verhindern kann die Suspendierung auf einen Benutzer, auch „Initiator“ genannt, beschränkt werden.

Zur Identifizierung des Initiators steht im Dialog mindestens der Terminal-Name zur Verfügung, im Batch die Initiator-Kennung. Wurde der Batch-Auftrag in einer Dialog-Task abgesetzt, stehen die Dialog-Attribute zur Verfügung. Handelt es sich um einen sekundären Batch-Auftrag, könnte die Audit-Id einen Hinweis auf den ursprünglichen Initiator geben.

Benutzeridentifikation

Um einen Benutzer zu identifizieren stehen je nach Zugangsweg bis zu 4 Attribute zur Verfügung:

1. eine sekundäre **Benutzerkennung**
   im Dialog mit persönlichem Logon die persönliche Benutzerkennung
   im Batch die persönliche bzw. Logon-Benutzerkennung des Initiators

2. der Kerberos-**Principal**
   im Net-Dialog als kennzeichnendes Attribut
   im Batch der Principal des Initiators
3. die **Audit**-Information
   ist ein Attribut mit gemischtem Inhalt für die Protokollierung durch SAT. Es kann die persönliche Kennung oder den Kerberos Principal des Initiators enthalten. Diese Information wird an Batch-Aufträge weiter vererbt.
4. der **Terminal**-Name
   im Dialog das schwächste Attribut zur Bestimmung des Initiators, wenn auch im einfachsten Fall das einzige.
   im Batch der Terminal-Name des Initiators

Über die Attribute 1-3 kann der Initiator direkt identifiziert werden, über Attribut 4 nur indirekt.

Bei abgewiesenen Zugangsversuchen wird versucht, anhand der persönlichen Attribute des aktuellen Initiators eine Zugangsversuchsreihe zu erkennen. Diese Versuche können auch in unterschiedlichen Zugangsklassen stattgefunden haben.

Zwei Zugangsversuche sind dem selben Initiator zuzuordnen, wenn

– mindestens eines seiner Attribute 1-3 bekannt ist und alle übereinstimmen oder
– keines seiner Attribute 1-3 bekannt ist, aber das Terminal übereinstimmt.

Die Suspendierung bezieht sich auf die Benutzerkennung, auf die sich die abgewiesenen Zugangsversuche bezogen. Versucht ein Angreifer sein Glück mit einer anderen Benutzerkennung, beginnt dort die Überwachung neu.

Verwaltung

Die Verwaltung der Suspendierung erfolgt spezifisch für jede Benutzerkennung. Die Attribute können aber auch über die Standard-Attribute der Zugangskontrolle zentral verwaltet werden.

Die Benutzerkennung TSOS und die des Sicherheitsbeauftragten können nicht gesperrt werden, es wird nur der Initiator gesperrt.

Mit dem Kommando /UNLOCK-USER-SUSPEND werden alle Suspendierungen einer Benutzerkennung aufgehoben, mit /SHOW-USER-SUSPEND angezeigt.

3.3.9 Sperrung von Benutzerkennungen bei Inaktivität

Auf einem System mit einer großen Anzahl von Benutzerkennungen kann es vorkommen, dass einzelne Benutzerkennungen nicht mehr benutzt werden und in Vergessenheit geraten. Der Zugang zu diesen Benutzerkennungen soll nach einer vorgegebenen Zeit, dem „Inaktivitätslimit“, automatisch gesperrt werden. Die Sperre tritt ein, wenn nach dem letzten Zugang die mit dem Inaktivitätslimit festgelegte Anzahl von Tagen verstrichen ist.

Eine wegen Inaktivität gesperrte Benutzerkennung kann vom Benutzerverwalter mit dem Kommando /MODIFY-LOGON-PROTECTION freigegeben werden, indem entweder das Inaktivitätslimit abgeschaltet oder das Verfallsdatum zurückgesetzt wird.

Bei einer neu eingerichteten Benutzerkennung gilt das Einrichtungsdatum ersatzweise als Datum des letzten Zugangs.

Bis zum ersten Logon nach Vereinbarung des Inaktivitätslimits gilt das Datum dieser Vereinbarung ersatzweise als Datum des letzten Zugangs.

Bei einem Versionsupgrade gilt für alle Benutzerkennungen das Upgrade-Datum ersatzweise als Datum des letzten Zugangs.

Bei der Rekonstruktion einer Backup-Sicherung des Benutzerkatalogs wird für die Benutzerkennungen, deren Inaktivitätslimit bei der Sicherung noch nicht erreicht war, die Restlaufzeit zum Zeitpunkt der Sicherung wiederhergestellt.

ACHTUNG!
Auf Standby-Pubsets können durch lange Lagerung Inaktivitätslimits überschritten werden. Beim Import als Home-Pubset ist dann kein Logon mehr möglich.
Der Systemverwalter muss daher die Benutzerkataloge von Home- und Standby-Pubset auf dem gleichen Stand halten.

3.3.10 Standardschutz für Kennungen

Wenn die SECOS-Zugangskontrolle ausschließlich benutzerkennungsspezifisch administriert wird, bietet dies maximale Flexibilität beim Feintuning im Einzelfall. Oft ist es aber auch wünschenswert, globale Einstellungen für alle Benutzerkennungen zentral vornehmen zu können.

Für globale Einstellungen bieten die Kommandos /SET-LOGON-PROTECTION und /MODIFY-LOGON-PROTECTION in geeigneten Operanden das Schlüsselwort *LOGON-DEFAULT an. Es bedeutet, dass bei den so gekennzeichneten Attributen der Zugangskontrolle immer die jeweils aktuellen globalen Einstellungen wirksam sind.

Die globalen Einstellungen werden mit den Kommandos /SET-LOGON-DEFAULTS und /MODIFY-LOGON-DEFAULTS vorgenommen und mit /SHOW-LOGON-DEFAULTS angezeigt. Diese Standard-Attribute werden wirksam, wenn keine entsprechenden Attribute direkt für die Benutzerkennungen eingestellt wurden.

Verfallsdaten

Neben den Attributen, die direkt den Standard-Attributen entnommen werden, enthält die Benutzerkennung auch Verfallsdaten, die von den Standard-Attributen abgeleitet sind. Diese Verfallsdaten genießen Vertrauensschutz und bleiben von einer Modifikation ihrer Standard-Attribute zunächst unberührt. Sie berücksichtigen diese erst dann, wenn sie neu berechnet werden. Das sind:

1. Das Verfallsdatum der Benutzerkennung
   wird bei Einrichtung der Benutzerkennung oder explizit durch den Benutzerverwalter gesetzt.
2. Das Verfallsdatum des Kennwortes
   wird bei der Vergabe eines neuen Kennwortes gesetzt.
3. Das Verfallsdatum bei Inaktivität
   wird beim nächsten Logon gesetzt.

Password-Management

Das Attribut PASSWORD-MANAGEMENT ist als Benutzer-Attribut bereits im Grundausbau des BS2000 enthalten. Es wird dort über die Kommandos /ADD-USER und /MODIFY-USER-ATTRIBUTES verwaltet und im Kommando /MODIFY-USER-PROTECTION ausgewertet. Voreingestellt ist der Wert PASSWORD-MANAGEMENT=*BY-USER.

Die Zugangskontrolle erweitert den Grundausbau um die Möglichkeit, die Voreinstellung (LOGON-DEFAULT) frei zu wählen. Beim Zusammenspiel von Benutzerverwaltung und Zugangskontrolle gelten für das PASSWORD-MANAGEMENT folgende Regeln:

1. Beim Kommando /ADD-USER weist die Zugangskontrolle stets das Standard-Attribut *LOGON-DEFAULT zu.
2. Der Wert *LOGON-DEFAULT kann nur mit dem Kommando /MODIFY-LOGON-PROTECTION durch einen anderen Wert ersetzt werden. Änderungsversuche mit dem Kommando /MODIFY-USER-ATTRIBUTES werden kommentarlos ignoriert.
3. Nachdem einer Kennung mit /MODIFY-LOGON-PROTECTION ein von *LOGON-DEFAULT abweichender Wert zugewiesen wurde, kann dieser anschließend auch wieder mit /MODIFY-USER-ATTRIBUTES geändert werden – allerdings nicht zurück auf *LOGON-DEFAULT. Diesen Wert gibt es nur in der Zugangskontrolle, und er kann nur mit dem Kommando /MODIFY-LOGON-PROTECTION explizit zugewiesen werden.
4. Die aktuelle Bedeutung des Wertes *LOGON-DEFAULT kann mit /SHOW-LOGON-DEFAULT ermittelt und mit /MODIFY-LOGON-DEFAULT jederzeit geändert werden. Voreingestellt ist *USER-CHANGE-ONLY.
5. Um deutlich zu machen, dass die Zugangskontrolle aktiv ist, zeigt das Kommando /SHOW-USER-ATTRIBUTES für PASSWORD-MANAGEMENT konstant den Wert *BY-LOGON-PROTECT an. Der tatsächlich gültige Wert kann nur mit dem Kommando /SHOW-LOGON-PROTECTION ermittelt werden.
6. Das Kommando /SHOW-LOGON-PROTECTION gibt stets den effektiv gültigen Wert des PASSWORD-MANAGEMENT aus. Dadurch ist nicht immer erkennbar, ob dieser Wert der Kennung explizit zugewiesen ist, oder ob der Kennung *LOGON-DEFAULT zugewiesen und der ausgegebene Wert die aktuelle Bedeutung von *LOGON-DEFAULT ist.

3.4 SRPM-Kommandos

In den folgenden Abschnitten werden alle SRPM-Kommandos in alphabetischer Reihenfolge aufgeführt. Bei den Kommandos ist vermerkt, mit welcher Privilegierung sie ausgeführt werden dürfen. Die Beschreibung der Kommandos ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion des Kommandos erklärt, dann folgt das Kommandoformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung folgt der Kommando-Returncode und gegebenenfalls ein Anwendungsbeispiel.

Funktionelle Übersicht

Die Kommandoübersichten enthalten auch die Kommandos der Komponente SRPMNUC, die zum BS2000-Grundausbaus gehört. Diese Kommandos sind mit *) gekennzeichnet und werden ausschließlich im Handbuch "Kommandos"[4] der jeweiligen BS2000-Version beschrieben.

Schutzattribute für existierende Benutzerkennungen

MODIFY-LOGON-DEFAULTS	Standardwerte für Schutzattribute ändern
MODIFY-LOGON-PROTECTION	Schutzattribute ändern
MODIFY-USER-PROTECTION *)	Kennwort ändern
SET-LOGON-DEFAULTS	Standardwerte für Schutzattribute vereinbaren
SET-LOGON-PROTECTION	Schutzattribute vereinbaren
SET-PERSONAL-ATTRIBUTES	Persönliche Identifizierung angeben
SHOW-LOGON-DEFAULTS	Standardwerte für Schutzattribute anzeigen
SHOW-LOGON-PROTECTION	Schutzattribute anzeigen
SHOW-PERSONAL-LOGON-ADMISSION	Persönliche Benutzerkennungen anzeigen
SHOW-USER-SUSPEND	Suspendierungen anzeigen
UNLOCK-USER-SUSPEND	Suspendierungen aufheben

Systemglobale Privilegien und Konsolzugangsrechte verwalten

SET-PRIVILEGE	systemglobale Privilegien oder Sammelprivilegien an eine Benutzerkennung vergeben
RESET-PRIVILEGE	einer Benutzerkennung systemglobale Privilegien oder Sammelprivilegien entziehen
SHOW-PRIVILEGE	Zuordnung von systemglobalen Privilegien bzw. Sammelprivilegien zu Benutzerkennungen anzeigen
CREATE-OPERATOR-ROLE *)	Name und Routing-Codes einer neuen Operator-Rolle definieren
DELETE-OPERATOR-ROLE *)	Operator-Rolle löschen
MODIFY-OPERATOR-ATTRIBUTES *)	Zuordnung von Operator-Rollen zu Benutzerkennungen ändern
MODIFY-OPERATOR-ROLE *)	Zuordnung von Routing-Codes zu Operator-Rolle ändern
SHOW-OPERATOR-ATTRIBUTES *)	Zuordnung von Operator-Rollen zu Benutzerkennungen anzeigen
SHOW-OPERATOR-ROLE *)	Zuordnung von Routing-Codes zu Operator-Rolle anzeigen

Sammelprivilegien verwalten:

CREATE-PRIVILEGE-SET	Namen eines Sammelprivilegs festlegen und Einzelprivilegien dem Sammelprivileg zuweisen
MODIFY-PRIVILEGE-SET	Sammelprivileg ändern (enthaltene Einzelprivilegien hinzufügen oder entziehen)
DELETE-PRIVILEGE-SET	Sammelprivileg-Namen und zugehörige Definitionen (enthaltene Einzelprivilegien) löschen
SHOW-PRIVILEGE-SET	Sammelprivileg-Namen und zugehörige Definitionen anzeigen

Verwaltung von Benutzergruppen

ADD-USER-GROUP	Benutzergruppe in Benutzerkatalog des angegebenen Pubset eintragen
MODIFY-USER-GROUP	Benutzergruppeneintrag im Benutzerkatalog des angegebenen Pubset ändern
REMOVE-USER-GROUP	Benutzergruppe aus dem Benutzerkatalog des angegebenen Pubset löschen
SHOW-USER-GROUP	Information über einen Benutzergruppeneintrag im Benutzerkatalog des angegebenen Pubset ausgeben lassen

Verwaltung von Benutzerkennungen

ADD-USER *)	Für einen Benutzer einen Eintrag im Benutzerkatalog erstellen und Zuordnung zu einer bestehenden Benutzergruppe treffen
EDIT-POSIX-USER-ATTRIBUTES *)	Geführten Dialog für MODIFY-POSIX-USER-ATTRIBUTES aktivieren
EDIT-POSIX-USER-DEFAULTS *)	Geführten Dialog für MODIFY-POSIX-USER-DEFAULTS aktivieren
EDIT-USER-ATTRIBUTES *)	Geführten Dialog für MODIFY-USER-ATTRIBUTES aktivieren
EDIT-USER-PUBSET-ATTRIBUTES *)	Geführten Dialog für MODIFY-USER-PUBSET-ATTRIBUTES aktivieren
LOCK-USER *)	Zugang zum System über eine bestimmte Benutzerkennung vorübergehend sperren
MODIFY-DEFAULT-ACCOUNT *)	Standardabrechnungsnummern ändern
MODIFY-POSIX-USER-ATTRIBUTES *)	POSIX-Benutzerattribute ändern
MODIFY-POSIX-USER-DEFAULTS *)	POSIX-Standardattribute ändern
MODIFY-USER-ATTRIBUTES *)	Katalogeintrag eines Benutzers ändern
MODIFY-USER-PUBSET-ATTRIBUTES *)	Pubset-spezifische Benutzerattribute einer Benutzerkennung ändern
REMOVE-USER *)	Katalogeintrag eines Benutzers im Benutzerkatalog löschen

SHOW-POSIX-USER-ATTRIBUTES *)	POSIX-Benutzerattribute anzeigen
SHOW-POSIX-USER-DEFAULTS *)	POSIX-Standardattribute anzeigen
SHOW-USER-ATTRIBUTES *)	Informationen über die Einträge im Benutzerkatalog ausgeben, darunter auch die direkte Gruppenzugehörigkeit einer Benutzerkennung
UNLOCK-USER *)	Zugang zum System über eine bestimmte Benutzerkennung wieder erlauben

Verwaltung von Terminal-Sets

CREATE-TERMINAL-SET	Terminal-Set anlegen
MODIFY-TERMINAL-SET	Terminal-Set modifizieren
DELETE-TERMINAL-SET	Terminal-Set löschen
COPY-TERMINAL-SET	Terminal-Set kopieren
SHOW-TERMINAL-SET	Terminal-Set anzeigen

Verwaltung der Key-Tabelle

ADD-KEYTAB-ENTRY	Key-Tabellen-Eintrag anlegen
CONVERT-KEYTAB	Keytab-Ausgabedatei umsetzen
MODIFY-KEYTAB-ENTRY	Key-Tabellen-Eintrag ändern
REMOVE-KEYTAB-ENTRY	Key-Tabellen-Eintrag löschen
SHOW-KEYTAB-ENTRY	Key-Tabellen-Eintrag anzeigen

Tabelle der Privilegien

Hier werden die Privilegien in alphabetischer Reihenfolge aufgelistet. Bei den einzelnen Operanden steht in den Kommandos nur noch ein Hinweis auf diese Tabelle.

Privileg	Abkürzung
ACS-ADMINISTRATION	ACS-ADM
CUSTOMER-PRIVILEGE-1 ... 8	CUST-PRIV-1 ... 8
FT-ADMINISTRATION	FT-ADM
FTAC-ADMINISTRATION	FTAC-ADM
GUARD-ADMINISTRATION	GUA-ADM
HARDWARE-MAINTENANCE	HARD-MAINT
HSMS-ADMINISTRATION	HSMS-ADM
NET-ADMINISTRATION	NET-ADM
NOTIFICATION-ADMINISTRATION	NOTIF-ADM
OPERATING	OPERATING
POSIX-ADMINISTRATION	POSIX-ADM
PRINT-SERVICE-ADMINISTRATION	PRINT-SERVICE-ADM
PROP-ADMINISTRATION	PROP-ADM
SAT-FILE-EVALUATION	SAT-FILE-EVAL
SAT-FILE-MANAGEMENT	SAT-FILE-MANAGE
SECURITY-ADMINISTRATION	SEC-ADM
STD-PROCESSING	STD-PROCESS
SUBSYSTEM-MANAGEMENT	SUBSYS-MANAGE
SW-MONITOR-ADMINISTRATION	SW-MON-ADM
TAPE-ADMINISTRATION	TAPE-ADM
TAPE-KEY-ADMINISTRATION	TAPE-KEY-ADM
TSOS	TSOS
USER-ADMINISTRATION	USER-ADM
VIRTUAL-MACHINE-ADMINISTRATION	VIRT-MACH-ADM
VM2000-ADMINISTRATION	VM2000-ADM

Hinweis

Ausnahmeregeln zu einzelnen Kommandos sind den einzelnen Operandenbeschreibungen zu entnehmen.

ADD-KEYTAB-ENTRY
Key-Tabellen-Eintrag hinzufügen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Mit diesem Kommando kann der Sicherheitsbeauftragte (standardmäßig die Benutzerkennung SYSPRIV) einen neuen Eintrag in der Key-Tabelle erstellen.

Ein Eintrag besteht aus dem Namen des BS2000-Rechners, wie er im KDC (Key Distribution Center) eingetragen ist, und mehreren Schlüsseln, die über kryptographische Verfahren aus dem angegebenen Kennwort und dem Rechnernamen abgeleitet werden. Das Kennwort selber wird nicht gespeichert.

```
ADD-KEYTAB-ENTRY

 ENTRY-IDENTIFICATION = *STD / <name 1..8>
,PRINCIPAL = <c-string 1..1800 with-low>
,PUBSET = *HOME / <cat-id 1..4>
,KEY = *NONE / *PASSWORD(…)
    *PASSWORD(…)
        PASSWORD = *SECRET-PROMPT(…) / <c-string 1..127 with-low>
          *SECRET-PROMPT(…)
              KEY-PASSWORD = *SECRET / <c-string 1..127 with-low>
              ,CONFIRM-PASSWORD = *SECRET / <c-string 1..127 with-low>
        ,KEY-VERSION = 0 / <integer 0..2147483647>
,KEY-OVERLAP-PERIOD = *UNLIMITED / *NO / <integer 0..32767>(…)
    <integer 0..32767>(…)
        DIMENSION = *MINUTES / *HOURS / *DAYS
,SYSTEM-DEFAULT = *NO / *YES
```

ENTRY-IDENTIFICATION = *STD / <name 1..8>
Beliebige Identifikation des Eintrags zur Bezugnahme mit den Kommandos /MODIFY-, /REMOVE- oder /SHOW-KEYTAB-ENTRY.

ENTRY-IDENTIFICATION = *STD
Legt einen Standard-Eintrag an. Dieser ist für die Anwendung $DIALOG vorgesehen.

PRINCIPAL = <c-string 1..1800 with-low>
Kerberos-Name des BS2000-Rechners, zu dem der Zugang gewährt werden soll.

Der Name des Principal einer Anwendung ist üblicherweise aus drei Komponenten aufgebaut: Anwendung, Instanz und Realm. Das Format eines typischen Kerberos-V5-Principal-Namens ist:

```
Anwendung/Instanz@REALM
```

mit

`Anwendung`	'host' für die Anwendung $DIALOG oder der Name der Anwendung
`Instanz`	DNS-Name des Rechners, auf dem die Anwendung läuft
`REALM`	Name der Kerberos-Domäne, per Konvention in Großbuchstaben dargestellt

PUBSET = *HOME / <cat-id 1..4>
Katalogkennung des Pubsets, in dessen Benutzerkatalog die Schlüssel eingetragen werden. Im laufenden Betrieb sind die Schlüssel des Home-Pubsets maßgebend.

KEY =
Gibt an, ob Schlüssel eingetragen werden sollen.

KEY = *NONE
Es werden vorläufig keine Schlüssel eingetragen.

KEY = *PASSWORD(…)
Die Schlüssel werden aus einem Kennwort erzeugt.

PASSWORD =
Kennwort des BS2000-Rechners.

PASSWORD = *SECRET-PROMPT(…)
Das Kennwort soll verdeckt eingegeben werden.

KEY-PASSWORD =
Kennwort des BS2000-Rechners, wie es auch im KDC vereinbart wurde.

KEY-PASSWORD = *SECRET
Das Kennwort wird verdeckt angefordert.

KEY-PASSWORD = <c-string 1..127 with-low>
Angabe des Kennworts.

CONFIRM-PASSWORD = *SECRET / <c-string 1..127 with-low>
Wiederholung des verdeckt eingegebenen Kennworts.

CONFIRM-PASSWORD = *SECRET
Das Kennwort wird verdeckt angefordert.

CONFIRM-PASSWORD = <c-string 1..127 with-low>
Wiederholte Angabe des Kennworts.

PASSWORD = <c-string 1..127 with-low>
Kennwort des BS2000-Rechners, wie es auch im KDC vereinbart wurde.

KEY-VERSION = 0 / <integer 0..2147483647>
Angabe der Schlüsselversion.

KEY-OVERLAP-PERIOD = *UNLIMITED / *NO / <integer 0..32767>(…)
Gibt an wie lange Schlüssel gültig bleiben, nachdem sie durch einen Schlüssel desselben Verschlüsselungstyps (ENCRYPTION-TYPE) mit höherer Schlüsselversion (KEY-VERSION) ersetzt wurden.

KEY-OVERLAP-PERIOD = *UNLIMITED
Veraltete Schlüssel bleiben unbegrenzt gültig.

KEY-OVERLAP-PERIOD = *NO
Veraltete Schlüssel werden sofort gelöscht.

KEY-OVERLAP-PERIOD = <integer 0..32767>(…)
Veraltete Schlüssel werden nach Ablauf der angegebenen Zeitspanne gelöscht. Veraltet ist ein Schlüssel, wenn er und der Schlüssel mit der nächsthöheren Version älter als die Zeitspanne sind.

DIMENSION = *MINUTES / *HOURS / *DAYS
Einheit und Genauigkeit der angegebenen Zeitspanne.

SYSTEM-DEFAULT = *NO / *YES
Gibt an, ob dieser Eintrag zum System-Standard erhoben werden soll. Ist keiner der benannten Einträge zum System-Standard erklärt worden, erbt automatisch der Eintrag *STD diese Eigenschaft. Alle Anwendungen, die keinen bestimmten Eintrag für die Ticket-Anforderung und Entschlüsselung angeben, benutzen den System-Standard.

ADD-USER-GROUP
Benutzergruppe in Benutzerkatalog eintragen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Trägt eine Benutzergruppe in den Benutzerkatalog des angegebenen Pubset ein.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter zu jeder Zeit für beliebige Gruppen. Ebenso gibt es für ihn keine Einschränkungen bezüglich der Vergabe von Potentialen und Gruppengrenzwerten.

– Gruppenverwalter mit der MANAGE-GROUPS-Berechtigung (ADM-AUTHORITY). Das Kommando gilt nur für die untergeordnete Gruppenhierarchie.

Die Prüfung, ob das Kommando von einem systemglobalen Benutzerverwalter gegeben wird, erfolgt gegen den Home-Pubset der laufenden Sitzung.

Die Prüfung, ob das Kommando von einem Gruppenverwalter gegeben wird, erfolgt gegen den unter dem Operanden PUBSET angegebenen Pubset.

ADD-USER-GROUP

GROUP-**ID**ENTIFICATION = <name 1..8>

,**PUBSET** = ***HOME** / <cat-id 1..4>

,**UP**PER-**GR**OUP = ***OWN** / ***UNIV**ERSAL / <name 1..8>

,**GR**OUP-**ADM**INISTRATOR = ***NONE** / <name 1..8>

,**ADD-GR**OUP-**MEM**BER = ***NONE** / list-poss(127): <name 1..8>

,**ADM-AUTHORITY** = ***MANAG**E-**RES**OURCES / ***MANAG**E-**MEMB**ERS / ***MANAG**E-**GR**OUPS

,**MAX-GROUP-MEMB**ERS = ***STD** / <integer 0..32767>

,**GR**OUP-**MEM**BER-**PREFIX** = ***ANY** / <name 1..7>

,**MAX-SUB-GR**OUPS = ***STD** / <integer 0..32767>

,**USER-GROUP-PREFIX** = ***ANY** / <name 1..7>

,**PUB**LIC-**SPACE-LIM**IT = ***MAX**IMUM / <integer 0..2147483647>

,**PUB**LIC-**SPACE-EXC**ESS = ***NO** / ***TEMP**ORARILY-**ALLOW**ED / ***ALLOW**ED

,**FILE-NUM**BER-**LIM**IT = ***MAX**IMUM / <integer 0..16777215>

,**JV-NUM**BER-**LIM**IT = ***MAX**IMUM / <integer 0..16777215>

(Teil 1 von 2)

,**TEMP-SPACE-LIM**IT = ***MAX**IMUM / <integer 0..2147483647>

,**WORK-SPACE-LIM**IT = ***MAX**IMUM / <integer 0..2147483647>

,**DMS-TUNING-RES**OURCES = ***NONE** / ***CONCURRENT-USE** / ***EXCL**USIVE-**USE**

,**TAPE-ACCESS** = ***STD** / ***PRIVIL**EGED / ***READ** / ***BYPASS-LABEL** / ***ALL**

,**F**ILE-**AUD**IT = ***NO** / ***Y**ES

,**CSTMP-MACRO** = ***NO** / ***Y**ES

,**RESID**ENT-**PAGE**S = ***MAX**IMUM / ***STD** / <integer 0..2147483647>

,**ADDR**ESS-**SPACE**-LIMIT = ***STD** / <integer 1..2147483647>

,**TEST-OPT**IONS = ***PAR**AMETERS(...)

***PAR**AMETERS(...)

READ-PRIVILEGE = ***STD** / <integer 1..9>

,**WR**ITE-**PRIVIL**EGE = ***STD** / <integer 1..9>

,**MODIF**ICATION = ***CONTR**OLLED / ***UNCONTR**OLLED

,**ADD-PROF**ILE-**ID** = ***NONE** / list-poss(127): <structured-name 1..30>

,**MAX-ACC**OUNT-**REC**ORDS = ***STD** / ***NO-LIM**IT / <integer 0..32767>

,**PHYSICAL-ALLOCATION** = ***NOT-ALLOWE**D / ***ALLOWE**D

,**HARD**WARE-**AUDIT** = ***ALLOWE**D / ***NOT-ALLOWE**D

,**LINKAGE-AUDIT** = ***ALLOWE**D / ***NOT-ALLOWE**D

,**CRYPTO-SESSION-LIM**IT = ***STD** / ***MAX**IMUM / <integer 0..32767>

,**NET-STOR**AGE-**USAGE** = ***ALLOWE**D / ***NOT-ALLOWE**D

,**ADD-ACCOUNT** = ***NONE** / list-poss(127): <alphanum-name 1..8>(...)

<alphanum-name>(...)

CPU-LIMIT = ***MAX**IMUM / <integer 0..2147483647>

,**SP**OOLOUT-**CL**ASS = ***STD** / <integer 1..255>

,**MAX**IMUM-**RUN-PRI**ORITY = ***STD** / <integer 30..255>

,**MAX-ALLOWE**D-**CAT**EGORY = ***STD** / ***TP** / ***SYS**TEM

,**NO-CPU-LIM**IT = ***NO** / ***Y**ES

,**START-IMMED**IATE = ***NO** / ***Y**ES

,**INHIB**IT-**DEACT**IVATION = ***NO** / ***Y**ES

,**BASIC-ACL-ACCESS** = ***BY-GR**OUP-**ONLY** / ***EXTENDED-BY-GUARD**(…)

***EXTENDED-BY-GUARD(...)**

GUARD-NAME = <filename 1..18 without-cat-gen-vers>

(Teil 2 von 2)

GROUP-IDENTIFICATION = <name 1..8>
Benutzergruppenkennung, die in den Benutzerkatalog des unter PUBSET angegebenen Pubset eingetragen wird. Im Gegensatz zur Benutzerkennung (Kommando /ADD-USER) gibt es keine reservierten oder mit besonderen Rechten ausgestatteten Benutzergruppenkennungen. Eine Benutzergruppe und eine Benutzerkennung können den gleichen Namen tragen.

PUBSET =
Pubset, dessen Benutzerkatalog den neuen Benutzergruppeneintrag aufnehmen soll. Soll eine Benutzergruppe mehrere Pubsets benutzen dürfen, muss für jedes einzelne Pubset ein Gruppeneintrag erstellt werden. Soll ein Gruppenverwalter auf mehreren Pubsets tätig werden, muss ein systemglobaler Benutzerverwalter bzw. der berechtigte Gruppenverwalter die Benutzergruppe und die Zuordnung des Gruppenverwalters auf jedem dieser Pubsets neu eintragen.

PUBSET = *HOME
Gruppen werden im Benutzerkatalog des Home-Pubset eingetragen.

PUBSET = <cat-id 1..4>
Katalogkennung des Pubset, das den Gruppeneintrag aufnehmen soll. Ist der Pubset auf dem lokalen System nicht aktiv, wird das Kommando abgewiesen.

UPPER-GROUP =
Benutzergruppe, die der neuen Benutzergruppe in der Gruppenhierarchie übergeordnet ist. Wenn der Kommandoausführende ein Gruppenverwalter ist, darf die übergeordnete Gruppe nur eine Gruppe aus der Teilhierarchie sein, zu deren Verwaltung er berechtigt ist. Ein systemglobaler Benutzerverwalter darf beliebige hierarchische Gruppenbeziehungen herstellen.

UPPER-GROUP = *OWN
Die Benutzergruppe desjenigen Gruppenverwalters, der das Kommando /ADD-USER-GROUP ausführt, wird zur übergeordneten Benutzergruppe. Auch wenn der Kommandoausführende ein systemglobaler Benutzerverwalter ist, ist die übergeordnete Gruppe nicht standardmäßig die *UNIVERSAL-Gruppe, sondern diejenige Benutzergruppe, der er zugeordnet ist.

UPPER-GROUP = *UNIVERSAL
Mit diesem Operandenwert hat ein systemglobaler Benutzerverwalter bzw. ein Gruppenverwalter von *UNIVERSAL die Möglichkeit, eine Benutzergruppe auf der obersten Ebene der Gruppenhierachie neu anzulegen. Hat der Kommandogeber nicht das Privileg systemglobale Benutzerverwaltung oder ist er nicht Gruppenverwalter der *UNIVERSAL-Gruppe, wird ein Kommando mit diesem Operandenwert abgewiesen.

UPPER-GROUP = <name 1..8>
Die angegebene Benutzergruppe wird zur übergeordneten Benutzergruppe. Diese Gruppe muss bereits auf dem jeweiligen Pubset eingerichtet sein.

GROUP-ADMINISTRATOR =
Benutzerkennung, die für die Verwaltung der Benutzergruppe verantwortlich sein soll (Gruppenverwalter). Die hier vereinbarte Benutzerkennung wird der Benutzergruppe als Mitglied zugeordnet. Ist die angegebene Benutzerkennung bereits Gruppenverwalter einer anderen Benutzergruppe, wird das Kommando abgewiesen. Dies wird nur auf dem angegebenen Pubset geprüft. Soll diese Benutzerkennung unbedingt Verwalter der neuen Benutzergruppe werden, muss vorher ihrer bisherigen Gruppe ein neuer Verwalter zugewiesen werden (oder *NONE).

Wird kein Gruppenverwalter eingetragen, wird die neue Benutzergruppe durch den Gruppenverwalter einer hierarchisch höherstehenden Benutzergruppe, der die entsprechende ADM-AUTHORITY besitzt, oder durch einen systemglobalen Benutzerverwalter verwaltet.

Besitzt die als Gruppenverwalter vorgesehene Benutzerkennung das Privileg USER-ADMINISTRATION oder das Privileg SECURITY-ADMINISTRATION, wird das Kommando abgewiesen, da die Ämterhäufung ’Gruppenverwalter + Privileg USER-ADMINISTRATION’ oder ’Gruppenverwalter + SECURITY-ADMINISTRATION’ unzulässig ist. Eine Ämterhäufung wird sowohl gegen den Home-Pubset der laufenden Sitzung als auch gegen den unter dem Operanden PUBSET angegebenen Pubset geprüft.

Sollte dennoch die inkonsistente Form der Ämterhäufung entstanden sein, wird eine Warnung ausgegeben. Das Privileg USER-ADMINISTRATION wird bei der Kommandoverarbeitung vorrangig behandelt.

GROUP-ADMINISTRATOR = *NONE
Es wird kein Gruppenverwalter eingetragen.

GROUP-ADMINISTRATOR = <name 1..8>
Benutzerkennung des Gruppenverwalters. Die Benutzerkennung muss vor der Zuordnung als Gruppenverwalter mit dem Kommando /ADD-USER auf dem jeweiligen Pubset angelegt worden sein.

ADD-GROUP-MEMBER =
Die angegebenen Benutzerkennungen werden der Benutzergruppe zugeordnet. Eine bestehende Zuordnung zu einer anderen Benutzergruppe wird damit aufgehoben. Die Benutzerkennungen müssen innerhalb der Gruppenhierarchie liegen, zu deren Verwaltung der Kommandogeber berechtigt ist. Dies gilt für Gruppenverwalter, deren Benutzergruppe mindestens MANAGE-GROUPS-Autorisierung besitzt.

In der Liste dürfen keine Gruppenverwalter anderer Gruppen enthalten sein.

ADD-GROUP-MEMBER = *NONE
Die Benutzergruppe wird ohne Mitglieder definiert.

ADD-GROUP-MEMBER = list-poss(127): <name 1..8>
Liste von Benutzerkennungen, die der aktuellen Benutzergruppe schon zum Zeitpunkt der Definition zugeordnet werden, sofern im Operanden MAX-GROUP-MEMBERS erlaubt. Sollen mehr als 127 Benutzerkennungen zugeordnet werden, geschieht das durch nachfolgende Kommandos /MODIFY-USER-GROUP. Die Benutzerkennungen müssen innerhalb der Gruppenhierarchie liegen, zu deren Verwaltung der Kommandogeber berechtigt ist. Keine der Benutzerkennungen darf bereits Gruppenverwalter auf dem angegebenen Pubset sein bzw. das Recht „Benutzerverwaltung“ oder „Sicherheitsbeauftragter“ auf dem angegebenen Pubset oder dem Home-Pubset besitzen.

ADM-AUTHORITY =
Rechte des Gruppenverwalters der neu angelegten Benutzergruppe.

ADM-AUTHORITY = *MANAGE-RESOURCES
Der Gruppenverwalter ist berechtigt, Betriebsmittel und Rechte der Benutzerkennungen, die zu seiner Gruppe gehören bzw. in der Gruppenhierarchie tiefer stehen, zu verwalten. Er hat kein Recht, Benutzerkennungen anzulegen, zu löschen und von einer Benutzergruppe zur anderen zu übertragen. Der Gruppenverwalter ist berechtigt, Betriebsmittel und Rechte seiner Benutzergruppe, bzw. der Benutzergruppen, die hierarchisch unter seiner Benutzergruppe liegen, zu verwalten. Er hat kein Recht, die Organisation (Hierarchie) der Benutzergruppen zu ändern, d.h. er kann Benutzergruppen und Gruppenmitglieder weder anlegen, noch übertragen oder löschen.

ADM-AUTHORITY = *MANAGE-MEMBERS
Der Gruppenverwalter ist berechtigt, Benutzerkennungen innerhalb seiner oder einer untergeordneten Benutzergruppe neu anzulegen, zu löschen oder zu deaktivieren (/LOCK-USER und /UNLOCK-USER) und zwischen Benutzergruppen zu übertragen. Die MANAGE-MEMBERS-Berechtigung beinhaltet automatisch die MANAGE-RESOURCES-Berechtigung.

ADM-AUTHORITY = *MANAGE-GROUPS
Der Gruppenverwalter ist berechtigt, die Organisation der hierarchisch unter seiner Benutzergruppe liegenden Gruppen durch Neuanlage, Löschen und Übertragen von Benutzergruppen zu verändern. Die MANAGE-GROUPS-Berechtigung beinhaltet automatisch die MANAGE-MEMBERS-Berechtigung.

MAX-GROUP-MEMBERS =
Maximale Anzahl von Benutzerkennungen, die der Gruppenverwalter dieser Benutzergruppe zuweisen darf. Diese Begrenzung gilt für die Summe der Benutzerkennungen der aktuellen Benutzergruppe und der ihr hierarchisch untergeordneten Benutzergruppen. Sie gilt nicht für den systemglobalen Benutzerverwalter - dieser darf die angegebene Anzahl auch überschreiten.

MAX-GROUP-MEMBERS = *STD
Der Benutzergruppe dürfen keine Benutzerkennungen zugewiesen werden.

MAX-GROUP-MEMBERS = <integer 0..32767>
Maximale Anzahl der Benutzerkennungen, die dieser Benutzergruppe zugewiesen werden können.

GROUP-MEMBER-PREFIX =
Legt fest, mit welchem Präfix die Namen von Gruppenmitgliedern beginnen müssen. Dieser oder jeder andere Präfix, der eine Untermenge dieses Präfix bildet, kann von Gruppenverwaltern, deren Benutzergruppe die ADM-AUTHORITY MANAGE-MEMBERS besitzt, an Untergruppen vergeben werden. (SRPM ist z.B. eine Untermenge zum Präfix SRP.)

GROUP-MEMBER-PREFIX = *ANY
Jeder Präfix ist erlaubt.

GROUP-MEMBER-PREFIX = <name 1..7>
Vorgegebener Name für Gruppenmitgliedernamen.

MAX-SUB-GROUPS =
Maximale Anzahl von Benutzergruppen, die einer Benutzergruppe untergeordnet werden können (Untergruppen). Diese Begrenzung umfasst die Summe der Benutzergruppen der unter der aktuellen Benutzergruppe aufzubauenden Hierarchie von Untergruppen.

MAX-SUB-GROUPS = *STD
Der Gruppenverwalter darf keine Benutzerkennungen zuweisen.

MAX-SUB-GROUPS = <integer 0..32767>
Maximale Anzahl der Untergruppen.

USER-GROUP-PREFIX =
Legt fest, mit welchem Präfix die Namen der Untergruppen beginnen müssen. Dieser oder jeder andere Präfix, der eine Untermenge dieses Präfix bildet, kann von Gruppenverwaltern, deren Benutzergruppe die ADM-AUTHORITY MANAGE-GROUPS besitzt, an Gruppenmitglieder vergeben werden. (SECOS ist z.B. eine Untermenge zum Präfix SEC.)

USER-GROUP-PREFIX = *ANY
Jeder Präfix ist erlaubt.

USER-GROUP-PREFIX = <name 1..7>
Es kann nur der angegebene Name für Untergruppen verwendet werden.

PUBLIC-SPACE-LIMIT = *MAXIMUM / <integer 0..2147483647>
Legt den maximalen Speicherplatz fest, den ein Gruppenverwalter an Gruppenmitglieder und Untergruppen für ihre Dateien auf gemeinschaftlichen Datenträgern des beim Operanden PUBSET zugewiesenen Pubset zuweisen darf .

PUBLIC-SPACE-LIMIT = *MAXIMUM
Der Gruppenverwalter darf die volle Kapazität von 2.147.483.647 PAM-Seiten zuweisen.

PUBLIC-SPACE-EXCESS =
Gibt dem Gruppenverwalter die Berechtigung zur weiteren Verwaltung des Rechtes, den im Operanden PUBLIC-SPACE-LIMIT zugewiesenen Wert zu überschreiten (bezüglich Mitgliedern oder Untergruppen).

PUBLIC-SPACE-EXCESS = *NO
Die Berechtigung darf nicht weiterverwaltet werden.

PUBLIC-SPACE-EXCESS = *ALLOWED
Die Berechtigung darf für Gruppenmitglieder und Untergruppen verwaltet werden.

PUBLIC-SPACE-EXCESS = *TEMPORARILY-ALLOWED
Die Speicherplatzgrenze darf überschritten werden, sofern die Obergrenze zum Zeitpunkt des LOGON noch nicht erreicht war.

FILE-NUMBER-LIMIT =
Vereinbart die maximale Anzahl von Dateien, die angelegt werden dürfen. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

FILE-NUMBER-LIMIT = *MAXIMUM
Die maximale Anzahl von Dateien ist 16.777.215.

FILE-NUMBER-LIMIT = <integer 0..16777215>
Angabe der genauen Anzahl der maximal möglichen Katalogeinträge.

JV-NUMBER-LIMIT =
Vereinbart die maximale Anzahl von Job-Variablen, die angelegt werden dürfen. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

JV-NUMBER-LIMIT = *MAXIMUM
Die maximale Anzahl von Job-Variablen ist 16.777.215.

JV-NUMBER-LIMIT = <integer 0..16777215>
Angabe der genauen Anzahl der maximal möglichen Job-Variablen.

TEMP-SPACE-LIMIT =
Vereinbart den maximalen temporären Speicherplatz, der auf dem im Operanden PUBSET angegebenen, gemeinschaftlichen Datenträger belegt werden darf. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

TEMP-SPACE-LIMIT = *MAXIMUM
Das maximale Gruppenpotential ist 2.147.483.647.

TEMP-SPACE-LIMIT = <integer 0..2147483647>
Angabe des genauen Gruppenpotentials.

WORK-SPACE-LIMIT = *MAXIMUM / <integer 0..2147483647>
Legt die Obergrenze für den Wert fest, den ein Gruppenverwalter als WORK-SPACE-LIMIT für seine Untergruppe bzw. seine Gruppenmitglieder für einen Pubset vergeben darf. Die Angabe dieses Operanden ist nur für einen SM-Pubset sinnvoll.

WORK-SPACE-LIMIT = *MAXIMUM
Die Obergrenze für den Wert, den ein Gruppenverwalter als WORK-SPACE-LIMIT angeben darf, soll auf 2147483647 festgelegt werden.

DMS-TUNING-RESOURCES =
Vereinbart, welche Performance-Maßnahmen ergriffen und in welcher Form sie genutzt werden dürfen. Diese Berechtigung oder eine geringere darf an Untergruppen oder Gruppenmitglieder weitergegeben werden. Die Auswirkungen der verschiedenen Performance-Maßnahmen sind unter „Zugelassene Performance-Maßnahmen für Home- und Daten-Pubset“ auf Seite 140 beschrieben.

DMS-TUNING-RESOURCES = *NONE
Es dürfen keine Performance-Maßnahmen angewendet werden.

DMS-TUNING-RESOURCES = *CONCURRENT-USE
Der Benutzer darf bevorzugte Ressourcen reservieren, steht dabei aber in Konkurrenz zu allen anderen Benutzern mit der gleichen Berechtigung.

DMS-TUNING-RESOURCES = *EXCLUSIVE-USE
Der Benutzer darf bevorzugte Ressourcen exklusiv reservieren.

Zugelassene Performance-Maßnahmen für Home- und Daten-Pubset

PUBSET = *HOME				
DMS-TUNING-RESOURCES=	ISAM-Pools resident	FAST-PAM-Environment resident	Dateiattribut PERFORMANCE	
			=*HIGH	=*VERY-HIGH
*NONE	nein	nein	nein	-
*CONCURRENT-USE	ja	nein	-	-
*EXCLUSIVE-USE	ja	ja	-	-

PUBSET = <Daten-Pubset>				
DMS-TUNING-RESOURCES=	ISAM-Pools resident	FAST-PAM-Environment resident	Dateiattribut PERFORMANCE	
			=*HIGH	=*VERY-HIGH
*NONE	-	-	nein	nein
*CONCURRENT-USE	-	-	ja	nein
*EXCLUSIVE-USE	-	-	ja	ja

TAPE-ACCESS =
Regelt die Rechte des Gruppenverwalters, die TAPE-ACCESS-Berechtigung zu verwalten (siehe Kommando /ADD-USER und /MODIFY-USER-ATTRIBUTES).

TAPE-ACCESS = *STD
Fehlermeldungen dürfen nicht ignoriert werden.

TAPE-ACCESS = *PRIVILEGED
Fehlermeldungen bei Ausgabedateien dürfen ignoriert werden.

TAPE-ACCESS = *READ
Fehlermeldungen bei Eingabedateien dürfen ignoriert werden.

TAPE-ACCESS = *BYPASS-LABEL
Abschaltung der Kennsatzprüfung bei Bändern, die im INPUT- oder REVERSE-Modus verarbeitet werden (umfasst TAPE-ACCESS=READ).

TAPE-ACCESS = *ALL
Alle Fehlermeldungen dürfen ignoriert werden (umfasst TAPE-ACCESS=*READ, TAPE-ACCESS=*PRIVILEGED und TAPE-ACCESS=*BYPASS-LABEL). Gibt der Gruppenverwalter ein Kommando für ein Gruppenmitglied, wobei er den Operanden TAPE-ACCESS mit einem bestimmten Wert besetzt, so gilt folgende Regel: akzeptiert

Wert im Kommando **Wert im Gruppenpotential**	**STD**	**PRIV**	**READ**	**BLP**	**ALL**
STD	YES	NO	NO	NO	NO
PRIV	YES	YES	NO	NO	NO
READ	YES	NO	YES	NO	NO
BLP	YES	NO	YES	YES	NO
ALL	YES	YES	YES	YES	YES

YES = akzeptiert, NO=nicht akzeptiert

FILE-AUDIT =
Vereinbart, ob das Recht, den AUDIT-Modus einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

FILE-AUDIT = *NO
Die Berechtigung darf nicht weitergegeben werden.

FILE-AUDIT = *YES
Die Berechtigung darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

CSTMP-MACRO =
Regelt die Verwaltungsrechte des Gruppenverwalters bezüglich der CSTMP-MACRO-Berechtigung (siehe Kommando /ADD-USER und /MODIFY-USER-ATTRIBUTES).

CSTMP-MACRO = *NO
Die Berechtigung kann nicht an Gruppenmitglieder oder Untergruppen weitergegeben werden.

CSTMP-MACRO = *YES
Die Berechtigung kann an Gruppenmitglieder und Untergruppen weitergegeben werden.

RESIDENT-PAGES =
Regelt die Berechtigung, residente Teile des Arbeitsspeichers zu verwenden. Gegen diesen Maximal-Wert (und zusätzlich gegen den im MODIFY-SYSTEM-BIAS gesetzten Wert) wird der Operand RESIDENT-PAGES=*PARAMETERS (MINIMUM=<integer 0..2147483647>) der Kommandos LOAD-/START-EXECUTABLE-PROGRAM (bzw. LOAD-/START-PROGRAM) geprüft. Der Maximalwert – oder ein kleinerer – kann an Gruppenmitglieder oder Untergruppen weitergereicht werden.

RESIDENT-PAGES = *MAXIMUM
Die Obergrenze wird auf 2.147.483.647 residente Hauptspeicherseiten festgelegt.

RESIDENT-PAGES = *STD
Der Benutzer darf keine residenten Hauptspeicherseiten in Anspruch nehmen (Wert 0).

RESIDENT-PAGES = <integer 0..2147483647>
Die Obergrenze wird auf die angegebenen residenten Hauptspeicherseiten festgelegt.

ADDRESS-SPACE-LIMIT =
Vereinbart den maximal verfügbaren Benutzeradressraum (Einheit: Megabyte). Diese Obergrenze oder ein geringerer Wert kann an Gruppenmitglieder oder Untergruppen vergeben werden.

ADDRESS-SPACE-LIMIT = *STD
Der Wert des Systemparameters SYSGJASL wird zugewiesen (der Systemparameter SYSGJASL hat den Standardwert 16 MByte, siehe Kommando SHOW-SYSTEM-PARAMETERS im Handbuch „Kommandos“ [4]).

ADDRESS-SPACE-LIMIT = <integer 1..2147483647>
Ein Wert von 1 bis 2.147.483.647 Megabyte wird zugewiesen.

TEST-OPTIONS = *PARAMETERS(...)
Legt das Gruppenprivileg bezüglich Vergabe der Testprivilegierung fest. Die vergebenen Werte regeln die Rechte des Gruppenverwalters bei der Verwaltung der Mitglieder seiner Benutzergruppe bzw. der Gruppenstruktur. Der Gruppenverwalter hat das Recht, ein Lese- und Schreibprivileg kleiner/gleich Gruppenprivileg an seine Gruppenmitglieder bzw. Untergruppen zu vergeben.

READ-PRIVILEGE =
Maximale Leseprivilegierung.

READ-PRIVILEGE = *STD
Das maximale Leseprivileg nimmt den Wert 1 an.

READ-PRIVILEGE = <integer 1..9>
Wert des maximalen Leseprivilegs.

WRITE-PRIVILEGE =
Maximale Schreibprivilegierung.

WRITE-PRIVILEGE = *STD
Das maximale Schreibprivileg nimmt den Wert 1 an.

WRITE-PRIVILEGE = <integer 1..9>
Wert des maximalen Schreibprivilegs.

MODIFICATION =
Legt das Recht des Gruppenverwalters fest, das MODIFICATION-Recht festzusetzen.

MODIFICATION = *CONTROLLED
Der Gruppenverwalter hat nur das Recht, das MODIFICATION-Recht CONTROLLED an Gruppenmitglieder bzw. Untergruppen weiterzureichen. Er ist nicht berechtigt, das MODIFICATION-Recht auf UNCONTROLLED zu ändern.

MODIFICATION = *UNCONTROLLED
Der Gruppenverwalter hat das Recht, das MODIFICATION-Recht CONTROLLED oder UNCONTROLLED Gruppenmitgliedern bzw. Untergruppen weiterzureichen.

ADD-PROFILE-ID =
Vereinbart ein Gruppenpotential an SDF-Profile-Ids, die der Gruppenverwalter Gruppenmitgliedern und Untergruppen zuordnen kann.

ADD-PROFILE-ID = *NONE
Der Gruppe wird kein Potential von Profile-Ids zugeordnet.

ADD-PROFILE-ID = list-poss(127): <structured-name 1..30>
Profile-Ids der Gruppensyntaxdateien, die dem Gruppenpotential zugeordnet werden.

MAX-ACCOUNT-RECORDS =
Legt das Gruppenrecht bezüglich Vergabe der Rechte zum Sammeln benutzerspezifischer Abrechnungssätze fest. Die vergebenen Werte regeln die Rechte des Gruppenverwalters bei der Verwaltung der Mitglieder seiner Benutzergruppe bzw. der Gruppenstruktur.

MAX-ACCOUNT-RECORDS = *STD
Der Benutzer darf pro Auftrag bzw. Programm bis zu 100 benutzerspezifische Abrechnungssätze in die Abrechnungsdatei schreiben. Eigene Abrechnungssätze (mit eigener Satzkennung) darf er nicht schreiben.

MAX-ACCOUNT-RECORDS = *NO-LIMIT
Der Benutzer darf pro Auftrag bzw. Programm unbegrenzt benutzerspezifische Abrechnungssätze und eigene Abrechnungssätze (mit eigener Satzkennung) in die Abrechnungsdatei schreiben.

MAX-ACCOUNT-RECORDS = <integer 0..32767>
Der Benutzer darf pro Auftrag bzw. Programm bis zur festgelegten Grenze benutzerspezifische Abrechnungssätze in die Abrechnungsdatei schreiben. Eigene Abrechnungssätze (mit eigener Satzkennung) darf er nicht schreiben.

PHYSICAL-ALLOCATION = *NOT-ALLOWED / *ALLOWED
Legt fest, ob der Gruppenverwalter das Recht, auf dem Pubset die absolute Speicherplatz-Zuweisung (Direktallokierung) zu nutzen, an Gruppenmitglieder oder Untergruppen vergeben darf.

HARDWARE-AUDIT = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, den Sprungfolgemodus (Hardware-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

LINKAGE-AUDIT = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, die Unterprogrammverfolgung (Linkage-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

CRYPTO-SESSION-LIMIT = *STD / *MAXIMUM / <integer 0..32767>
Vereinbart die maximale Anzahl openCRYPT-Sessions innerhalb einer BS2000-Session, die vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

NET-STORAGE-USAGE = *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, Speicherplatz auf einem Net-Storage-Volume zu belegen, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

ADD-ACCOUNT =
Die vergebenen Abrechnungsnummern können an Gruppenmitglieder vergeben oder dem Gruppenpotential von Untergruppen zugeordnet werden.

ADD-ACCOUNT = *NONE
Dem Gruppenpotential wird keine Abrechnungsnummer zugeordnet.

ADD-ACCOUNT = list-poss(127): <alphanum-name 1..8>(...)
Liste von Abrechnungsnummern, die dem Potential der Benutzergruppenkennung zugeordnet werden.

CPU-LIMIT =
Legt das Gruppenpotential an CPU-Sekunden fest, das an Gruppenmitglieder und Untergruppen weitergegeben werden kann. CPU-Zeit bis zu dieser Grenze steht den Gruppenmitgliedern zur Auftragsausführung unter der jeweiligen Abrechnungsnummer zur Verfügung.

CPU-LIMIT = *MAXIMUM
Das Gruppenpotential beläuft sich auf 2.147.483.647 CPU-Sekunden.

CPU-LIMIT = <integer 0..2147483647>
Anzahl CPU-Sekunden, die dem Gruppenpotential zugewiesen werden (Maximalwert für jede Gruppenkennung).

SPOOLOUT-CLASS =
Legt die höchstmögliche SPOOLOUT-Klasse fest, die an Gruppenmitglieder oder Benutzergruppen weitergegeben werden kann. Bei der Bewertung der Zulässigkeit wird – um eine Rangfolge zu erreichen – STD (=0) bzw. 1 als die höchstmögliche Klasse angesehen und 255 als die niedrigstmögliche.

SPOOLOUT-CLASS = *STD
Die maximale SPOOLOUT-Klasse ist mit dem Wert 0 vorbesetzt.

SPOOLOUT-CLASS = <integer 1..255>
Wert der maximalen SPOOLOUT-Klasse.

MAXIMUM-RUN-PRIORITY =
Legt die maximale RUN-Priorität als Gruppenpotential fest, die an Gruppenmitglieder oder Untergruppen weitergegeben werden kann.

MAXIMUM-RUN-PRIORITY = *STD
Standardwert aus dem Systemparameter SYSGJPRI.

MAXIMUM-RUN-PRIORITY = <integer 30..255>
Maximale RUN-Priorität.

MAX-ALLOWED-CATEGORY =
Legt fest, mit welchen Task-Attributen der Benutzer arbeiten darf. Ein Recht, das andere Rechte umfasst (SYSTEM umfasst STD und TP, TP umfasst STD), kann für Gruppenmitglieder bzw. Untergruppen eingeschränkt werden.

MAX-ALLOWED-CATEGORY = *STD
Tasks unter der angegebenen Abrechnungsnummer dürfen nicht mit dem Task-Attribut TP arbeiten.

MAX-ALLOWED-CATEGORY = *TP
Tasks unter der angegebenen Abrechnungsnummer dürfen das Task-Attribut TP verwenden.

MAX-ALLOWED-CATEGORY = *SYSTEM
Tasks unter der angegebenen Abrechnungsnummer dürfen die Task-Attribute TP und SYS verwenden.

NO-CPU-LIMIT =
Legt die Berechtigung des Gruppenverwalters fest, das NO-CPU-LIMIT-Recht an Gruppenmitglieder bzw. Untergruppen weiterzugeben.

NO-CPU-LIMIT = *NO
Das Recht kann nicht weitergegeben werden.

NO-CPU-LIMIT = *YES
Das Recht kann an Gruppenmitglieder und Untergruppen weitergegeben werden.

START-IMMEDIATE =
Legt die Rechte des Gruppenverwalters bezüglich der Job-Express-Funktion fest.

START-IMMEDIATE = *NO
Die Express-Berechtigung kann weder an Gruppenmitglieder noch an Untergruppen weitergegeben werden.

START-IMMEDIATE = *YES
Die Express-Berechtigung darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

INHIBIT-DEACTIVATION =
Regelt die Berechtigung des Gruppenverwalters, Gruppenmitgliedern oder Untergruppen das Recht des Deaktivierungsverbotes für Aufträge unter dieser Abrechnungsnummer weiterzugeben.

INHIBIT-DEACTIVATION = *NO
Das Recht darf nicht weitergegeben werden.

INHIBIT-DEACTIVATION = *YES
Das Recht darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

BASIC-ACL-ACCESS =
Regelt den Gruppenzugriff für Dateien und Jobvariablen, die mit BACL geschützt sind.

BASIC-ACL-ACCESS = *BY-GROUP-ONLY
Beim Zugriff auf Dateien und Jobvariablen, die durch BACL geschützt sind, ist nur die tatsächliche Gruppenmitgliedschaft von Bedeutung.

BASIC-ACL-ACCESS = *EXTENDED-BY-GUARD(…)
Beim Zugriff auf Dateien und Jobvariablen, die durch BACL geschützt sind, werden bestimmte Benutzer so behandelt, als ob sie Gruppenmitglieder wären.

GUARD-NAME = <filename 1…18 without-cat-gen-vers>
Name des Guards, in dem Zugriffsbedingungen festgelegt sind. Sind diese Bedingungen für einen Benutzer zum Zeitpunkt des Zugriffs erfüllt, hat dieser dieselben Rechte wie ein Gruppenmitglied.

Wenn das Guard zum Zeitpunkt der Auswertung nicht existiert oder nicht zugreifbar ist, gilt die Bedingung als nicht erfüllt.

Bei der Zugriffsrechteprüfung für Dateien und Jobvariablen, die durch BACL geschützt sind, wird die Gruppenstruktur auf dem Home-Pubset zugrunde gelegt. Die Guards der Gruppenverwaltung müssen daher ebenfalls auf dem Home-Pubset der laufenden Sitzung abgelegt sein. Deshalb muss der Name des Guards ohne Katalogkennung angegeben werden. Wird der Name des Guards ohne Benutzerkennung angegeben, wird das Guard unter der Benutzerkennung vorausgesetzt, unter der das Kommando ADD-USER-GROUP aufgerufen wurde.

Der Gruppenverwalter ist dafür verantwortlich, dass das Guard existiert und zugreifbar ist. Gegebenenfalls muss er das Guard unter seiner Benutzerkennung auf dem Home-Pubset mit SCOPE-Attribut für die betreffende Gruppe anlegen.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

CONVERT-KEYTAB
Keytab-Ausgabedatei umsetzen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Das Kommando CONVERT-KEYTAB dient zum Umsetzen der Keytab-Ausgabedatei des ktpass-Kommandos in eine Prozedur-Datei mit entsprechenden SECOS-Kommandos.

Die Übertragung der Keytab-Ausgabedatei auf das BS2000-System kann durch Angabe einer entsprechenden TRANSFER-ADMISSION und des zugehörigen Partnersystems gesteuert werden.

In diesem Fall muss im Berechtigungsprofil der Verzeichnispfad und im Kommandoparameter der Name der Keytab-Ausgabedatei im Partnersystem angegeben werden.

Falls openFT nicht zur Verfügung steht, muss die Keytab-Ausgabedatei mit FTP im binary mode auf das BS2000-System übertragen werden.

Einsatzvoraussetzungen

- Das Kommando CONVERT-KEYTAB setzt voraus, dass SDF-P verfügbar ist.
- Für die Ausführung der erzeugten Prozedur-Datei muss der Sicherheitsbeauftragte zusätzlich das Privileg STD-PROCESSING besitzen.

  Hierzu muss

  – die SRPMOPT-Option (Datei: SYSSSI.SRPMOPT.<version>) SECURITY-ADMIN-STD-PROCESSING=Y gesetzt werden,

  und

  – der Sicherheitsbeauftragte sich selber das Privileg STD-PROCESSING zuweisen.

CONVERT-KEYTAB

KEYTAB-FILE = **CONVKTAB.KEYTAB** / <filename 1..54> / <c-string 1..512 with-low>

,**JCL-FILE** = **CONVKTAB.JCL** / <filename 1..54>

,**TRANSFER-ADMISSION** = ***NONE** / <alphanum-name 8..32> / <c-string 8..32 with-low> / <x-string 15..64>

,**PARTNER-NAME** = ***NONE** / <name 1..8>

,**ENTRY-IDENTIFICATION** = ***STD** / <name 1..8>

KEYTAB-FILE = CONVKTAB.KEYTAB / <filename 1..54> / <c-string 1..512 with-low>
Angabe des Namens der Keytab-Ausgabedatei des ktpass-Kommandos. Abhängig von der Angabe des Operanden TRANSFER-ADMISSION bezieht sich der Name auf

– die ins BS2000-System übertragene Keytab-Ausgabedatei (TRANSFER-ADMISSION = *NONE)

– bzw. auf die Keytab-Ausgabedatei in Windows (in den anderen Fällen).

Voreingestellt ist CONVKTAB.KEYTAB als Standardname für die ins BS2000-System übertragenen Keytab-Ausgabedatei.

KEYTAB-FILE = <filename 1..54>
Dieses Format dient zur Angabe des Namens der ins BS2000-System übertragenen Keytab-Ausgabedatei.

KEYTAB-FILE = <c-string 1..512 with-low>
Dieses Format dient zur Angabe des Namens der Keytab-Ausgabedatei des ktpass-Kommandos im Windows-System. Da Windows die Gross-/Kleinschreibung ignoriert, ist diese optional.

JCL-FILE = CONVKTAB.JCL / <filename 1..54>
Angabe des Namens der Datei zur Aufnahme der entsprechenden SECOS-Kommandos Diese Datei muss unter der Kennung des Sicherheitsbeauftragten (Privileg SECURITY-ADMINISTRATION) ausgeführt werden.

Voreingestellt ist der Standardname CONVKTAB.JCL.

TRANSFER-ADMISSION = *NONE / <alphanum-name 8..32>
Angabe, die festlegt, ob die Keytab-Ausgabedatei mit openFT auf das BS2000-System übertragen werden soll.

TRANSFER-ADMISSION = *NONE
Die Keytab-Ausgabedatei wurde bereits auf das BS2000-System übertragen.

TRANSFER-ADMISSION = <alphanum-name 8..32> / <c-string 8..32 with-low> / <x-string 15..64>
Zugangsberechtigung zur Dateiübertragung mit openFT im fernen System.

PARTNER-NAME = *NONE / <name 1..8>
Name des Partnerrechners, von dem die Keytab-Ausgabedatei übertragen werden soll.

PARTNER-NAME = *NONE
Kein Partnerrechner angegeben.

PARTNER-NAME = <name 1..8>
Partnerrechner, von dem die Keytab-Ausgabedatei übertragen werden soll.

ENTRY-IDENTIFICATION = *STD / <name 1..8>
Identifikation des Eintrags in der BS2000-Key-Tabelle

ENTRY-IDENTIFICATION = *STD
Standard-Eintrag

ENTRY-IDENTIFICATION = <name 1..8>
Identifikation des Eintrags in der BS2000-Key-Tabelle

Einschränkungen

Das Kommando CONVERT-KEYTAB verarbeitet derzeit nur Keytab-Ausgabedateien mit folgenden Eigenschaften:

– maximale Dateigroesse: 4096 Byte;

– KEYTAB-Version x'502';

COPY-TERMINAL-SET
Terminal-Set kopieren

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Kopiert ein Terminal-Set.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Terminal-Sets

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen. Das Ziel des Kopiervorgangs muss ein Terminal-Set der Klasse GROUP oder USER. Es muss der Gruppe des Gruppenverwalters oder einem ihrer Mitglieder zugeordnet sein.

Der Kopiervorgang wird nur innerhalb eines Pubsets unterstützt.

```
COPY-TERMINAL-SET

 FROM-TERMINAL-SET = <name 1..8>(…)

    <name 1..8>(…)
       SCOPE = *STD / *USER(…) / *GROUP(…) / *SYSTEM
          *USER(…)
             USER-IDENTIFICATION = *OWN / <name 1..8>
          *GROUP(…)
             GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>
 TO-TERMINAL-SET = <name 1..8>(…)

    <name 1..8>(…)
       SCOPE = *STD / *USER(…) / *GROUP(…) / *SYSTEM
          *USER(…)
             USER-IDENTIFICATION = *OWN / <name 1..8>
          *GROUP(…)
             GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>
,PUBSET = *HOME / <catid 1..4>
,WRITE-MODE = *NEW / *REPLACE
```

FROM-TERMINAL-SET = <name 1..8>(...)
Name des Terminal-Sets, das kopiert wird.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *OWN / <name 1..8>)
Ein Terminal-Set aus dem Eigentum einer Benutzerkennung wird kopiert.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>)
Ein Terminal-Set aus dem Eigentum einer Benutzergruppe wird kopiert.

SCOPE = *SYSTEM
Ein Terminal-Set aus gemeinschaftlichem Eigentum wird kopiert.

TO-TERMINAL-SET = <name 1..8>(...)
Name des Terminal-Sets, das erzeugt oder ersetzt wird.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *OWN / <name 1..8>)
Das Terminal-Set wird in das Eigentum einer Benutzerkennung kopiert.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>)
Das Terminal-Set wird in das Eigentum einer Benutzergruppe kopiert.

SCOPE = *SYSTEM
Diesen Wert darf nur ein systemglobaler Benutzerverwalter angeben.

Das Terminal-Set wird in das gemeinschaftliche Eigentum kopiert.

PUBSET =
Pubset, in dessen Benutzerkatalog das Terminal-Set kopiert wird.

PUBSET = *HOME
Das Terminal-Set wird auf dem Home-Pubset kopiert.

PUBSET = <catid 1..4>
Das Terminal-Set wird auf dem angegebenen Pubset kopiert.

WRITE-MODE =
Angabe, ob ein vorhandenes Terminal-Set gleichen Namens überschrieben werden soll.

WRITE-MODE = *NEW
Ein vorhandenes Terminal-Set wird nicht überschrieben.

WRITE-MODE = *REPLACE
Ein vorhandenes Terminal-Set wird überschrieben.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

CREATE-PRIVILEGE-SET
Sammelprivileg erzeugen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Dieses Kommando richtet ein Sammelprivileg ein. Erläuterungen zu Sammelprivilegien finden Sie auf Seite 43f.

CREATE-**PRIVIL**EGE-**SET**
PRIVILEGE-**SET-NAME** = <name 1..8> ,**PRIVIL**EGE = ***NONE** / list-poss(64): <text> ,**PUBSET** = ***HOME** / <cat-id 1..4>

PRIVILEGE-SET-NAME = <name 1..8>
Name des zu erzeugenden Sammelprivilegs, welches dann in den Benutzerkatalog eingetragen wird.

PRIVILEGE = *NONE / list-poss(64)
Bestimmt, ob einem Sammelprivileg Einzelprivilegien zugeordnet werden.

PRIVILEGE = *NONE
Dem Sammelprivileg werden keine Einzelprivilegien zugeordnet; es wird lediglich der Name für zukünftige Definitionen erzeugt.

PRIVILEGE = list-poss(64): <text>
Es werden die angegebenen Privilegien zugeordnet. Mögliche Privilegien siehe Seite 128.
Ausnahmen: TSOS und SECURITY-ADMINISTRATION

PUBSET = *HOME / <cat-id 1..4>
Pubset, auf dem das Sammelprivileg eingetragen werden soll.

PUBSET = *HOME
Das Sammelprivileg wird auf dem Home-Pubset angelegt.

PUBSET = <cat-id 1..4>
Das Sammelprivileg wird auf dem angegebenen Pubset angelegt.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel

Es soll ein Sammelprivileg für die Bandverarbeitung erzeugt werden. Dem Sammelprivileg (es erhält den Namen ARCHIV) sollen die Privilegien HSMS-ADMINISTRATION und TAPE-ADMINISTRATION zugeordnet werden.

```
/create-privilege-set privilege-set-name=archive, -
/      privilege=(hsms-administration, tape-administration)
```

Zur Überprüfung der Zuordnung wird das Kommando SHOW-PRIVILEGE-SET gegeben:

```
/show-privilege-set information=privilege(privilege-set-name=archiv)

THE FOLLOWING PRIVILEGES ARE ASSIGNED TO PRIVILEGE-SET ARCHIV ON PVS ABC1
HSMS-ADMINISTRATION TAPE-ADMINISTRATION
```

CREATE-TERMINAL-SET
Terminal-Set anlegen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Legt ein neues Terminal-Set an.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Terminal-Sets

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen, für Terminal-Sets der Klasse GROUP oder USER. Die Terminal-Sets müssen der Gruppe des Gruppenverwalters oder ihren Mitgliedern zugeordnet werden.

```
CREATE-TERMINAL-SET

 TERMINAL-SET-NAME = <name 1..8>(...)

    <name 1..8>(...)
        SCOPE = *STD / *USER(...) / *GROUP(...) / *SYSTEM
            *USER(...)
                USER-IDENTIFICATION = *OWN / <name 1..8>
            *GROUP(...)
                GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>
,PUBSET = *HOME / <catid 1..4>
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
,USER-INFORMATION = *NONE / <c-string 1..80 with-lower>
,SORT-TERMINAL-ENTRY = *BY-PROCESSOR / *BY-STATION
```

TERMINAL-SET-NAME = <name 1..8>(...)
Name des Terminal-Sets.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *OWN / <name 1..8>)
Die angegebene Benutzerkennung ist Eigentümer.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>)
Die angegebene Benutzergruppe ist Eigentümer.

SCOPE = *SYSTEM
Diesen Wert darf nur ein systemglobaler Benutzerverwalter angeben.

Das Terminal-Set wird dem gemeinschaftlichen Eigentum zugeordnet.

PUBSET =
Pubset, in dessen Benutzerkatalog das Terminal-Set angelegt wird.

PUBSET = *HOME
Das Terminal-Set wird auf dem Home-Pubset angelegt.

PUBSET = <catid 1..4>
Das Terminal-Set wird auf dem angegebenen Pubset angelegt.

GUARD-NAME =
Gibt an, ob der Zugang von den angegebenen Datensichtstationen aus über ein Guard zeitlich eingeschränkt wird.

GUARD-NAME = *NONE
Der Zugang erfolgt zeitlich unbeschränkt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Das Terminal-Set wird mit den Zugriffsbedingungen im angegebenen Guard verknüpft.

USER-INFORMATION = *NONE / <c-string 1..80 with-lower>
Benutzerinformation. Hier kann der Benutzer einen Kommentar hinterlegen.

SORT-TERMINAL-ENTRY =
Sortierung der Terminal-Einträge. Diese Angabe wirkt sich nur bei der Ausgabe mit dem Kommando /SHOW-TERMINAL-SET aus.

SORT-TERMINAL-ENTRY = *BY-PROCESSOR
Bei der Sortierung besitzt die Prozessor-Angabe eine höhere Wertigkeit als die Stations-Angabe.

SORT-TERMINAL-ENTRY = *BY-STATION
Bei der Sortierung besitzt die Stations-Angabe eine höhere Wertigkeit als die Prozessor-Angabe.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

DELETE-PRIVILEGE-SET
Sammelprivileg löschen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Dieses Kommando löscht ein Sammelprivileg aus dem Benutzerkatalog. Name und Definitionen werden gelöscht. Das Kommando wird abgewiesen, wenn das Sammelprivileg noch einer Kennung zugewiesen ist.

DELETE-**PRIVIL**EGE-**SET**
PRIVILEGE-**SET-NAME** = <name 1..8> ,**PUBSET** = ***HOME** / <cat-id 1..4>

PRIVILEGE-SET-NAME = <name 1..8>
Namen des zu löschenden Sammelprivilegs.

PUBSET = *HOME / <cat-id 1..4>
Angabe des Pubset, auf dem das Sammelprivileg gelöscht werden soll.

PUBSET = *HOME
Das Sammelprivileg wird auf dem Home-Pubset gelöscht.

PUBSET = <cat-id 1..4>
Das Sammelprivileg wird auf dem angegebenen Pubset gelöscht.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel

Ein Sammelprivileg kann erst gelöscht werden, wenn es keiner Kennung mehr zugewiesen ist. Hier die Kommandofolge, um ein Sammelprivileg zu löschen, welches beim ersten Aufruf des Kommandos /DELETE-PRIVILEGE-SET noch einer Kennung zugewiesen ist:

```
/delete-privilege-set privilege-set-name=archiv
% SRM4050 PRIVILEGE SET 'ARCHIV' IS STILL ASSIGNED TO AT LEAST ONE USER
ID ON PVS 'ABC1'. COMMAND REJECTED

/show-privilege information=user-identification( -
/               privilege=privilege-set(privilege-set-name=archiv))

USER-IDENTIFICATIONS HAVING PRIVILEGE SET ARCHIV ON PVS ABC1
USERID1

/reset-privilege privilege=privilege-set(privilege-set-name=archiv), -
/                user-identification=userid1

/delete-privilege-set privilege-set-name=archiv
```

Da das Sammelprivileg ARCHIV für die Sammelprivileg-Beispiele das einzige Sammelprivileg war, führt ein /SHOW-PRIVILEGE-SET zu folgender Reaktion:

```
/show-privilege-set information=privilege(privilege-set-name=*all)
% SRM4052 NO PRIVILEGE SET DEFINED ON PUBSET 'ABC1'
```

DELETE-TERMINAL-SET
Terminal-Set löschen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Löscht Terminal-Sets.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Terminal-Sets

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen. Das Ziel des Kopiervorgangs muss ein Terminal-Set der Klasse GROUP oder USER. Es muss der Gruppe des Gruppenverwalters oder einem ihrer Mitglieder zugeordnet sein.

Wenn ein Terminal-Set noch für den Schutz mindestens einer Benutzerkennung verwendet wird, wird es im Normalfall nicht gelöscht. Allerdings kann das Löschen in diesem Fall mit dem Operanden REMOVE-ASSIGNMENT=*YES erzwungen werden. Dabei werden vor dem Löschen alle Zuweisungen aufgehoben.

DELETE-TERMINAL-SET

TERMINAL-SET = <name 1..8>(…)

<name 1..8>(…)

SCOPE = ***STD** / ***USER**(…) / ***GROUP**(…) / ***SYSTEM**

***USER**(…)

USER-IDENTIFICATION = ***OWN** / <name 1..8>

***GROUP**(…)

GROUP-IDENTIFICATION = ***OWN** / ***UNIVERSAL** / <name 1..8>

,**PUBSET** = ***HOME** / <catid 1..4>

,**REMOVE-ASSIGNMENT** = ***NO** / ***YES**

TERMINAL-SET = <name 1..8>(…)
Name des Terminal-Sets, das gelöscht wird.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *OWN / <name 1..8>)
Ein Terminal-Set aus dem Eigentum einer Benutzerkennung wird gelöscht.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *OWN / *UNIVERSAL / <name 1..8>)
Ein Terminal-Set aus dem Eigentum einer Benutzergruppe wird gelöscht.

SCOPE = *SYSTEM
Ein Terminal-Set aus gemeinschaftlichem Eigentum wird gelöscht.

PUBSET =
Pubset, aus dessen Benutzerkatalog das Terminal-Set gelöscht wird.

PUBSET = *HOME
Das Terminal-Set wird aus dem Home-Pubset gelöscht.

PUBSET = <catid 1..4>
Das Terminal-Set wird aus dem angegebenen Pubset gelöscht.

REMOVE-ASSIGNMENT =
Angabe ob alle Zuweisungen des zu löschenden Terminal-Sets ebenfalls gelöscht werden sollen.

REMOVE-ASSIGNMENT = *NO
Das Löschen wird abgewiesen, wenn noch mindestens eine Zuweisung besteht.

REMOVE-ASSIGNMENT = *YES
Bestehende Zuweisungen werden vor dem Löschen aufgehoben.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

MODIFY-KEYTAB-ENTRY
Key-Tabellen-Eintrag ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

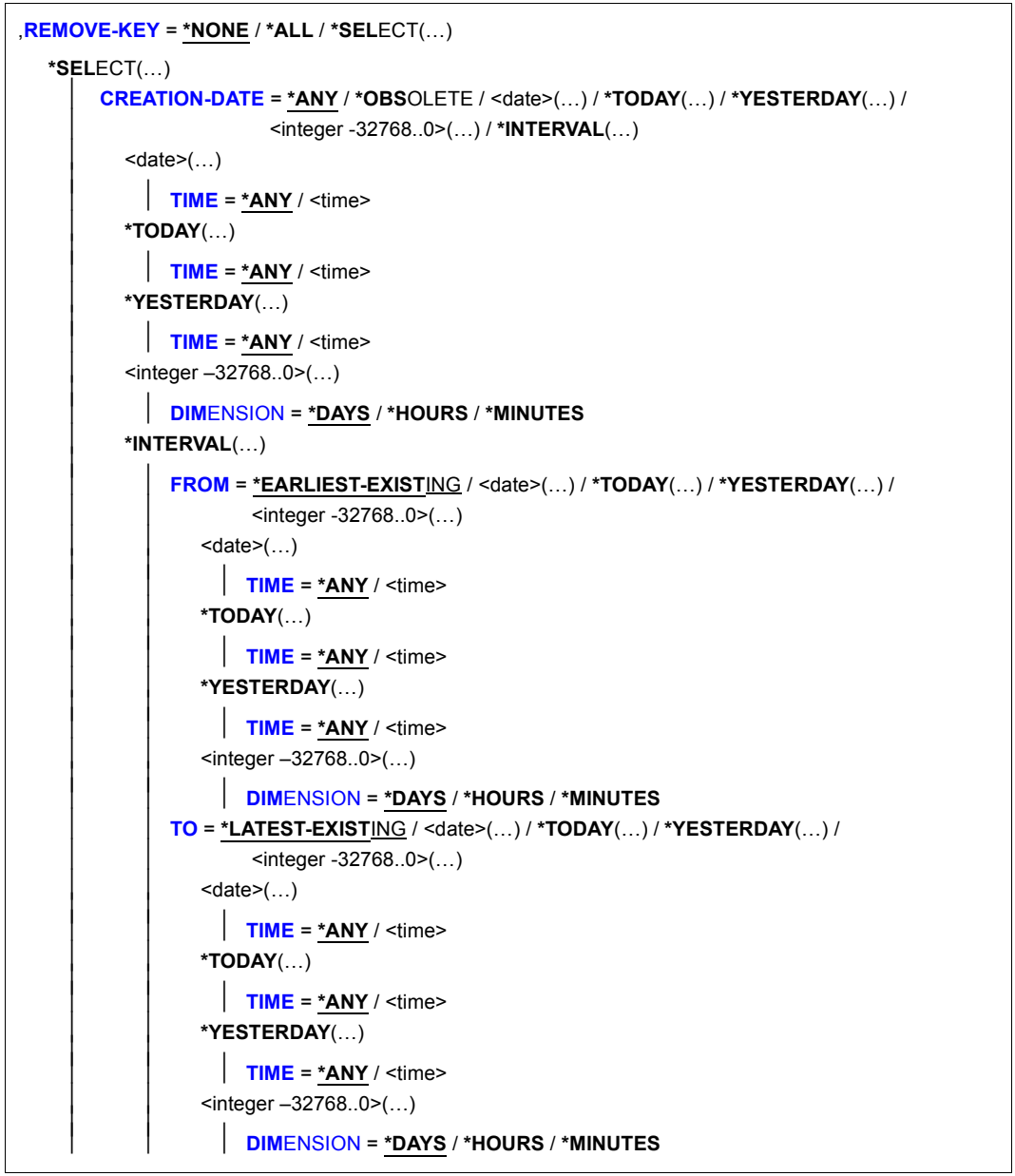
Mit diesem Kommando kann der Sicherheitsbeauftragte (standardmäßig die Benutzerkennung SYSPRIV) einen Eintrag in der Key-Tabelle ändern.

Ein bestehender Eintrag wird mit einem neuen Kennwort versehen. Bei der Vergabe eines neuen Kennwortes werden die Schlüssel der laufenden Session um die neuen ergänzt, so dass bei der Zugangsprüfung unterschiedliche Versionen der Schlüssel berücksichtigt werden können. Dieses Verfahren gestattet einen unterbrechungsfreien Betrieb auch während der Zeitspanne zwischen dem Kennwortwechsel im BS2000 und dem KDC.

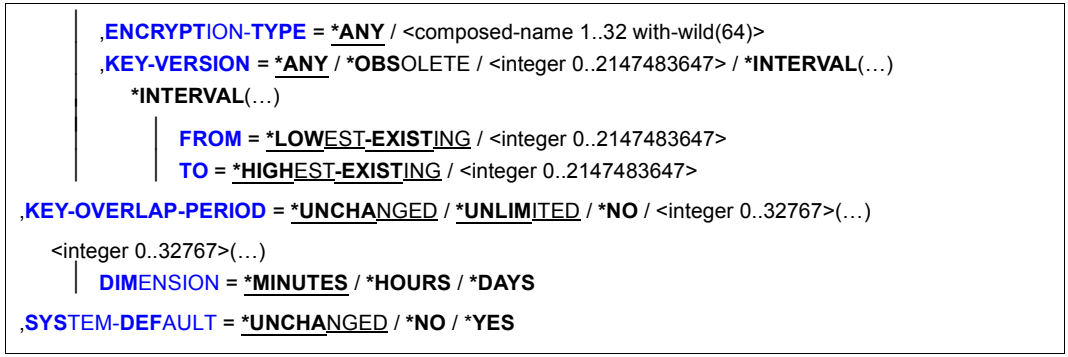
```
MODIFY-KEYTAB-ENTRY

 ENTRY-IDENTIFICATION = *STD / *SYSTEM-DEFAULT / <name 1..8>
,NEW-IDENTIFICATION = *SAME / *STD / <name 1..8>
,PUBSET = *HOME / <cat-id 1..4>
,ADD-KEY = *NONE / *PASSWORD(…)
    *PASSWORD(…)
        PASSWORD = *SECRET-PROMPT(…) / <c-string 1..127 with-low>
            *SECRET-PROMPT(…)
                KEY-PASSWORD = *SECRET / <c-string 1..127 with-low>
                ,CONFIRM-PASSWORD = *SECRET / <c-string 1..127 with-low>
        ,KEY-VERSION = *INCREMENT / <integer 0..2147483647>
```

(Teil 1 von 3)


,REMOVE-KEY = *NONE / *ALL / *SELECT(…)
*SELECT(…)
CREATION-DATE = *ANY / *OBSOLETE / <date>(…) / *TODAY(…) / *YESTERDAY(…) /
<integer -32768..0>(…) / *INTERVAL(…)
<date>(…)
TIME = *ANY / <time>
*TODAY(…)
TIME = *ANY / <time>
*YESTERDAY(…)
TIME = *ANY / <time>
<integer –32768..0>(…)
DIMENSION = *DAYS / *HOURS / *MINUTES
*INTERVAL(…)
FROM = *EARLIEST-EXISTING / <date>(…) / *TODAY(…) / *YESTERDAY(…) /
<integer -32768..0>(…)
<date>(…)
TIME = *ANY / <time>
*TODAY(…)
TIME = *ANY / <time>
*YESTERDAY(…)
TIME = *ANY / <time>
<integer –32768..0>(…)
DIMENSION = *DAYS / *HOURS / *MINUTES
TO = *LATEST-EXISTING / <date>(…) / *TODAY(…) / *YESTERDAY(…) /
<integer -32768..0>(…)
<date>(…)
TIME = *ANY / <time>
*TODAY(…)
TIME = *ANY / <time>
*YESTERDAY(…)
TIME = *ANY / <time>
<integer –32768..0>(…)
DIMENSION = *DAYS / *HOURS / *MINUTES

(Teil 2 von 3)



(Teil 3 von 3)

ENTRY-IDENTIFICATION = *STD / *SYSTEM-DEFAULT / <name 1..8>
Identifikation des Eintrags, der geändert werden soll.

NEW-IDENTIFICATION = *SAME / *STD / <name 1..8>
Neue Identifikation, in die der Eintrag umbenannt werden soll.

PUBSET = *HOME / <cat-id 1..4>
Katalogkennung des Pubsets, in dessen Benutzerkatalog die Schlüssel geändert werden. Im laufenden Betrieb sind die Schlüssel des Home-Pubsets maßgebend.

ADD-KEY = *NONE / *PASSWORD(…)
Gibt an, ob Schlüssel hinzugefügt werden sollen.

ADD-KEY = *NONE
Es werden keine Schlüssel hinzugefügt.

ADD-KEY = *PASSWORD(…)
Die Schlüssel werden aus einem Kennwort erzeugt.

PASSWORD =
Kennwort des BS2000-Rechners.

PASSWORD = *SECRET-PROMPT(…)
Das Kennwort soll verdeckt eingegeben werden.

KEY-PASSWORD =
Kennwort des BS2000-Rechners, wie es auch im KDC vereinbart wurde.

KEY-PASSWORD = *SECRET
Das Kennwort wird verdeckt angefordert.

KEY-PASSWORD = <c-string 1..127 with-low>
Angabe des Kennworts.

CONFIRM-PASSWORD = *SECRET / <c-string 1..127 with-low>
Wiederholung des verdeckt eingegebenen Kennworts.

CONFIRM-PASSWORD = *SECRET
Das Kennwort wird verdeckt angefordert.

CONFIRM-PASSWORD = <c-string 1..127 with-low>
Wiederholte Angabe des Kennworts.

PASSWORD = <c-string 1..127 with-low>
Kennwort des BS2000-Rechners, wie es auch im KDC vereinbart wurde.

KEY-VERSION = *INCREMENT / <integer 0..2147483647>
Angabe der Schlüsselversion.

KEY-VERSION = *INCREMENT
Die bisher höchste Schlüsselversion wird um 1 erhöht.

REMOVE-KEY =
Gibt an, ob Schlüssel gelöscht werden sollen.

REMOVE-KEY = *NONE
Es werden keine Schlüssel gelöscht.

REMOVE-KEY = *ALL
Alle Schlüssel werden gelöscht.

REMOVE-KEY = *SELECT(…)
Alle Schlüssel, die allen nachfolgend angegebenen Kriterien entsprechen, werden gelöscht.

CREATION-DATE = *ANY / *OBSOLETE / <date>(…) / *TODAY(…) / *YESTERDAY(…) / <integer –32768..0>(…) / *INTERVAL(…)
Auswahl der Schlüssel abhängig vom Zeitpunkt ihrer Erstellung.

CREATION-DATE = *ANY
Die Auswahl erfolgt unabhängig vom Erstellungszeitpunkt der Schlüssel.

CREATION-DATE = *OBSOLETE
Auswahl aller Schlüssel außer dem jüngsten.

CREATION-DATE = <date>(…) / *TODAY(…) / *YESTERDAY(…)
Auswahl aller Schlüssel mit dem angegebenen Erstellungsdatum.

TIME = *ANY / <time>
Zusätzliche Einschränkung der Auswahl auf die angegebene Uhrzeit.

CREATION-DATE = <integer –32768..0>(…)
Auswahl aller Schlüssel mit der angegebenen Erstellungszeit.
Die Erstellungszeit wird relativ zum aktuellen Zeitpunkt angegeben und liegt in der Vergangenheit.

DIMENSION = *DAYS / *HOURS / *MINUTES
Einheit und Genauigkeit der relativen Zeitangabe.

CREATION-DATE = *INTERVAL(…)
Auswahl aller Schlüssel, deren Erstellungszeitpunkt im angegebenen Intervall liegt.

FROM =
Beginn des Intervalls, in dem der Erstellungszeitpunkt der auszuwählenden Schlüssel liegen soll.

FROM = *EARLIEST-EXISTING
Das Intervall beginnt mit dem Erstellungszeitpunkt des ältesten Schlüssels.

FROM = <date>(…) / *TODAY(…) / *YESTERDAY(…)
Das Intervall beginnt mit dem angegebenen Datum.

TIME = *ANY / <time>
Zusätzliche Einschränkung des Intervallbeginns auf die angegebene Uhrzeit.

FROM = <integer –32768..0>(…)
Der Intervallbeginn wird relativ zum aktuellen Zeitpunkt angegeben und liegt in der Vergangenheit.

DIMENSION = *DAYS / *HOURS / *MINUTES
Einheit und Genauigkeit der relativen Zeitangabe.

TO =
Ende des Intervalls, in dem der Erstellungszeitpunkt der auszuwählenden Schlüssel liegen soll.

TO = *LATEST-EXISTING
Das Intervall endet mit dem Erstellungszeitpunkt des jüngsten Schlüssels.

TO = <date>(…) / *TODAY(…) / *YESTERDAY(…)
Das Intervall endet mit dem angegebenen Datum.

TIME = *ANY / <time>
Zusätzliche Einschränkung des Intervallendes auf die angegebene Uhrzeit.

TO = <integer –32768..0>(…)
Das Intervallende wird relativ zum aktuellen Zeitpunkt angegeben und liegt in der Vergangenheit.

DIMENSION = *DAYS / *HOURS / *MINUTES
Einheit und Genauigkeit der relativen Zeitangabe.

ENCRYPTION-TYPE = *ANY / <composed-name 1..32 with-wild(64)>
Auswahl der Schlüssel abhängig vom Verschlüsselungstyp.

ENCRYPTION-TYPE = *ANY
Die Auswahl erfolgt unabhängig vom Verschlüsselungstyp.

KEY-VERSION =
Auswahl der Schlüssel abhängig von der Schlüsselversion.

KEY-VERSION = *ANY
Die Auswahl erfolgt unabhängig von der Schlüsselversion.

KEY-VERSION = *OBSOLETE
Auswahl aller Schlüssel außer dem mit der höchsten Schlüsselversion.

KEY-VERSION = *INTERVAL(…)
Auswahl aller Schlüssel mit einer Version im angegebenen Versionsbereich.

FROM = *LOWEST-EXISTING / <integer 0..2147483647>
Wählt alle Schlüssel mit mindestens dieser Version aus.

TO = *HIGHEST-EXISTING / <integer 0..2147483647>
Wählt alle Schlüssel mit maximal dieser Version aus.

KEY-OVERLAP-PERIOD =
Gibt an wie lange Schlüssel gültig bleiben, nachdem sie durch einen Schlüssel desselben Verschlüsselungstyps (ENCRYPTION-TYPE) mit höherer Schlüsselversion (KEY-VERSION) ersetzt wurde.
Die neue Restlaufzeit wirkt sich sofort auf alle gespeicherten Schlüssel aus.

KEY-OVERLAP-PERIOD = *UNCHANGED
Die Gültigkeit von veralteten Schlüsseln wird nicht verändert.

KEY-OVERLAP-PERIOD = *UNLIMITED
Veraltete Schlüssel bleiben unbegrenzt gültig.

KEY-OVERLAP-PERIOD = *NO
Veraltete Schlüssel werden sofort gelöscht.

KEY-OVERLAP-PERIOD = <integer 0..32767>(…)
Veraltete Schlüssel werden nach Ablauf der angegebenen Zeitspanne gelöscht. Veraltet ist ein Schlüssel, wenn er und der Schlüssel mit der nächsthöheren Version älter als die Zeitspanne sind.

DIMENSION = *MINUTES / *HOURS / *DAYS
Einheit und Genauigkeit der angegebenen Zeitspanne.

SYSTEM-DEFAULT = *UNCHANGED / *NO / *YES
Gibt an, ob dieser Eintrag zum System-Standard erhoben werden soll. Ist keiner der benannten Einträge zum System-Standard erklärt worden, erbt automatisch der Eintrag *STD diese Eigenschaft. Alle Anwendungen, die keinen bestimmten Eintrag für die Ticket-Anforderung und Entschlüsselung angeben, benutzen den System-Standard.

MODIFY-LOGON-DEFAULTS
Standardwerte für Schutzattribute ändern

Anwendungsbereich: USER-ADMINISTRATION

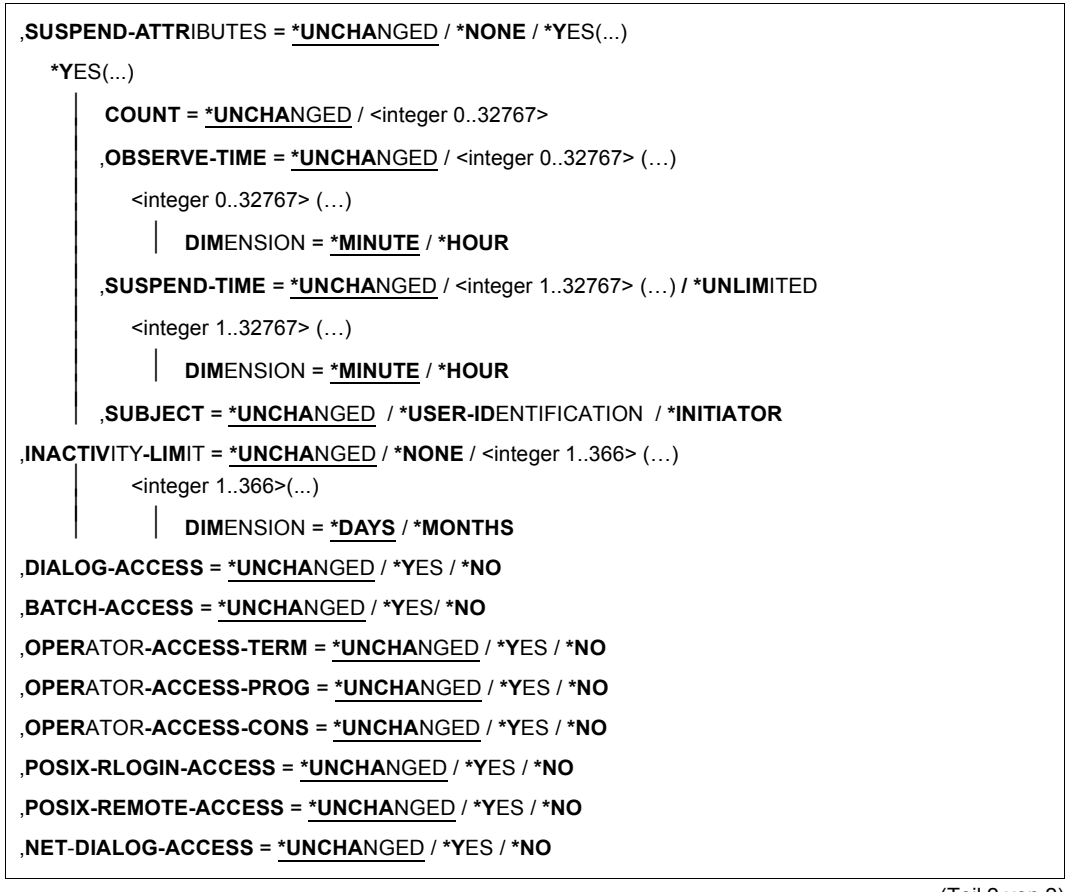
Privilegierung: USER-ADMINISTRATION

Mit diesem Kommando kann der systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) Standard-Schutzattribute für die Zugangskontrolle ändern. Diese Einstellungen gelten als Standardwerte für die Kommandos /SET- und /MODIFY-LOGON-PROTECTION.

```
MODIFY-LOGON-DEFAULTS

 PUBSET = *HOME / <cat-id 1..4>
,EXPIRATION-DATE = *UNCHANGED / *NONE / <integer 0..366>
,EXPIRATION-WARNING = *UNCHANGED / *STD / <integer 0..366>
,PASSWORD = *UNCHANGED / *PARAMETERS(...)
   *PARAMETERS(...)
      MANAGEMENT = *UNCHANGED / *USER-CHANGE-ONLY / *BY-ADMINISTRATOR / *BY-USER
      ,MINIMAL-LENGTH = *UNCHANGED / *NONE / <integer 1..8>
      ,MINIMAL-COMPLEXITY = *UNCHANGED / *NONE / <integer 1..4>
      ,INITIAL-LIFETIME = *UNCHANGED / *STD / *EXPIRED / <integer 0..366>
      ,LIFETIME-INTERVAL = *UNCHANGED / *UNLIMITED / <integer 1..366>(...)
         <integer 1..366>(...)
            DIMENSION = *DAYS / *MONTHS
      ,EXPIRATION-WARNING = *UNCHANGED / *STD / <integer 0..366>
      ,UNLOCK-EXPIRATION = *UNCHANGED / *BY-ADMINISTRATOR-ONLY / *BY-USER
      ,PASSWORD-MEMORY = *UNCHANGED / *NONE / *YES(…)
         *YES(…)
            PERIOD = 1 / <integer 1..32767>
            ,CHANGES-PER-PERIOD = 1 / <integer 1..100>
            ,BLOCKING-TIME = 100 / <integer 1..32767>
```

(Teil 1 von 2)



(Teil 2 von 2)

Bedeutung der Operanden siehe Kommando /MODIFY-LOGON-PROTECTION (Seite 172).

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

MODIFY-LOGON-PROTECTION
Schutzattribute ändern

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Ändert bereits bestehende Schutzattribute für Benutzerkennungen.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Benutzerkennungen

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen, für die ihrer Benutzergruppe zu- und untergeordneten Benutzerkennungen.

Nicht angegebene Operanden bleiben unverändert (Standardwert *UNCHANGED oder *NONE).

Das Kommando /MODIFY-LOGON-PROTECTION ist das gegebene Mittel, um Benutzerkennungen zu reaktivieren, die wegen Überschreitung ihres Verfallsdatums, wegen Inaktivität oder wegen zu lange nicht geändertem Kennwort vom System gesperrt wurden. Im ersten Fall muss ein neues, in der Zukunft liegendes Verfallsdatum (EXPIRATION-DATE) eingetragen, im zweiten INACTIVITY-LIMIT=*RENEW und im dritten ein neues Kennwort vereinbart werden.

MODIFY-**LOGON-PROT**ECTION

USER-IDENTIFICATION = <name 1..8>

,**PUBSET** = ***HOME** / <cat-id 1..4>

,**EXPIR**ATION-**DATE** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / <date 8..10> / <integer 0..366>

,**EXPIR**ATION-**WARNING** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***STD** / <integer 0..366>

,**PASS**WORD = ***UNCHA**NGED / ***PAR**AMETERS(...)

***PAR**AMETERS(...)

LOGON-PASSWORD = ***UNCHA**NGED / ***NONE** / ***SECRET** / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>

(Teil 1 von 11)

,**ENCR**YPTION = ***YES** / ***NO**

,**MANAG**EMENT = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***USER-CHA**NGE**-ONLY** / ***BY-USER** / ***BY-ADM**INISTRATOR

,**MIN**IMAL**-LENGTH** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / <integer 1..8>

,**MIN**IMAL**-COMPLEX**ITY = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / <integer 1..4>

,**INIT**IAL**-LIFE**TIME = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***STD** / ***EXPIR**ED / <integer 0..366> / <date 8..10>

,**LIFE**TIME**-INTER**VAL = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***UNLIM**ITED / <integer 1..366>(...)

<integer 1..366>(...)

DIMENSION = ***DAYS** / ***MONTHS**

,**EXPIR**ATION**-WARNING** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***STD** / <integer 0..366>

,**UNLOCK-EXPIR**ATION = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***BY-ADM**INISTRATOR**-ONLY** / ***BY-USER**

,**PASS**WORD**-MEMORY** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / ***YES**(…)

***YES**(…)

PERIOD = **1** / <integer 1..32767>

,**CHA**NGES**-PER-PER**IOD = **1** / <integer 1..100>

,**BLOCK**ING**-TIME** = **100** / <integer 1..32767>

,**SUSPEND-ATTR**IBUTES = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / ***Y**ES(...)

***Y**ES(...)

COUNT = ***UNCHA**NGED / ***LOGON-DEF**AULT / <integer 0..32767>

,**OBSERVE-TIME** = ***UNCHA**NGED / ***LOGON-DEF**AULT / <integer 0..32767> (…)

<integer 0..32767> (…)

DIMENSION = ***MINUTE** / ***HOUR**

,**SUSPEND-TIME** = ***UNCHA**NGED / ***LOGON-DEF**AULT / <integer 1..32767> (…) **/** ***UNLIM**ITED

<integer 1..32767> (…)

DIMENSION = ***MINUTE** / ***HOUR**

,**SUBJECT** = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***USER-ID**ENTIFICATION / ***INITIATOR**

,**INACTIV**ITY**-LIM**IT = ***UNCHA**NGED / ***LOGON-DEF**AULT / ***NONE** / <integer 1..366> (…) / ***RENEW**

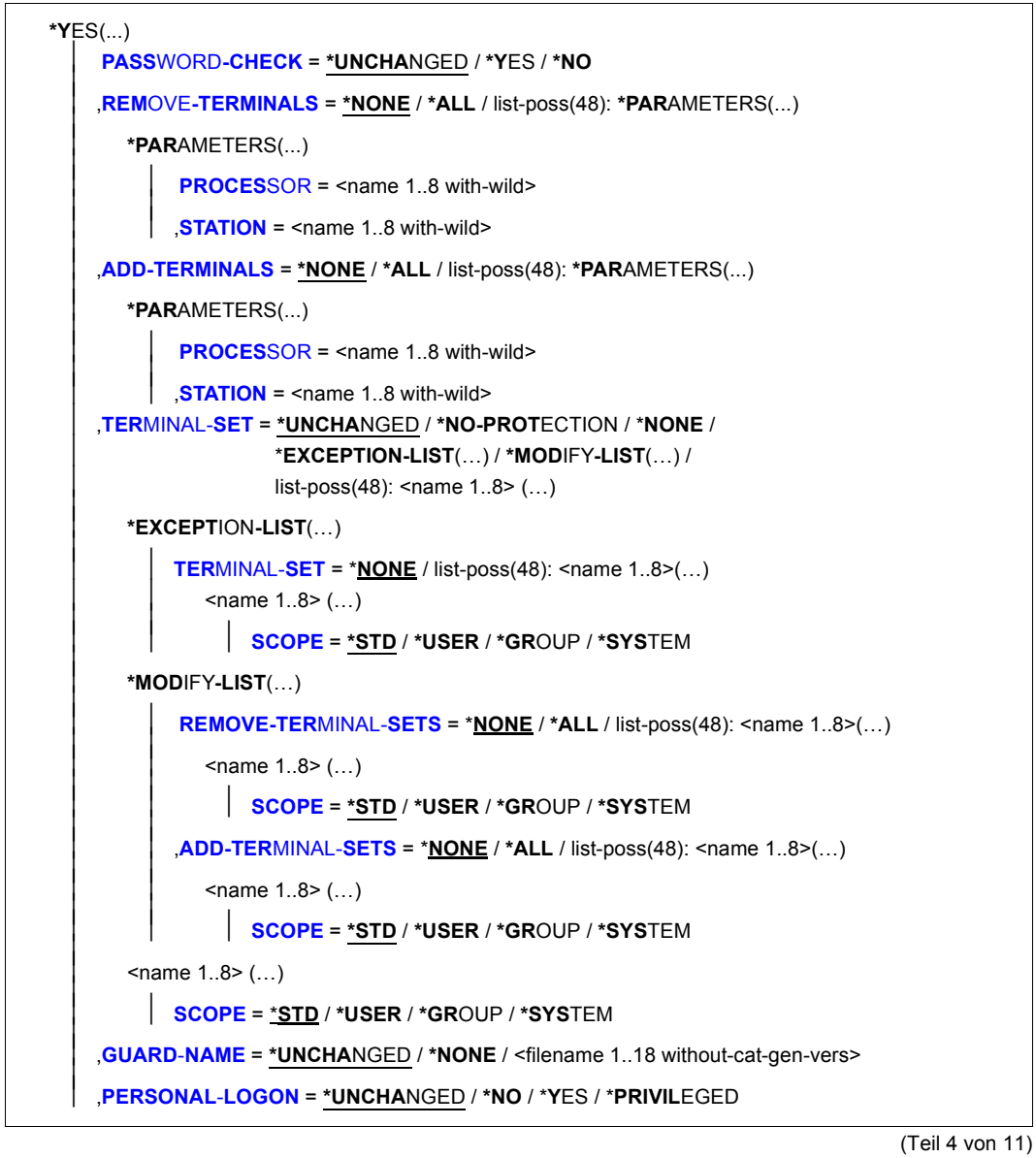
<integer 1..366>(...)

DIMENSION = ***DAYS** / ***MONTHS**

(Teil 2 von 11)

```
,DIALOG-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *NO / *YES(...)
    *LOGON-DEFAULT(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
        ,REMOVE-TERMINALS = *NONE / *ALL / list-poss(48): *PARAMETERS(...)
            *PARAMETERS(...)
                PROCESSOR = <name 1..8 with-wild>
                ,STATION = <name 1..8 with-wild>
        ,ADD-TERMINALS = *NONE / *ALL / list-poss(48): *PARAMETERS(...)
            *PARAMETERS(...)
                PROCESSOR = <name 1..8 with-wild>
                ,STATION = <name 1..8 with-wild>
        ,TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE /
                        *EXCEPTION-LIST(...) / *MODIFY-LIST(...) /
                        list-poss(48): <name 1..8> (...)
            *EXCEPTION-LIST(...)
                TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            *MODIFY-LIST(...)
                REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
                ,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            <name 1..8> (...)
                SCOPE = *STD / *USER / *GROUP / *SYSTEM
        ,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
        ,PERSONAL-LOGON = *UNCHANGED / *NO / *YES / *PRIVILEGED
```

(Teil 3 von 11)


*YES(...)
PASSWORD-CHECK = *UNCHANGED / *YES / *NO
,REMOVE-TERMINALS = *NONE / *ALL / list-poss(48): *PARAMETERS(...)
*PARAMETERS(...)
PROCESSOR = <name 1..8 with-wild>
,STATION = <name 1..8 with-wild>
,ADD-TERMINALS = *NONE / *ALL / list-poss(48): *PARAMETERS(...)
*PARAMETERS(...)
PROCESSOR = <name 1..8 with-wild>
,STATION = <name 1..8 with-wild>
,TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE /
*EXCEPTION-LIST(…) / *MODIFY-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
*MODIFY-LIST(…)
REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
,PERSONAL-LOGON = *UNCHANGED / *NO / *YES / *PRIVILEGED

(Teil 4 von 11)

,**BATCH-ACCESS** = ***UNCHA**NGED / ***LOGON-DEF**AULT(...) / ***Y**ES(...) / ***NO**

***LOGON-DEF**AULT(...)

PASSWORD-**CHECK** = ***UNCHA**NGED / ***Y**ES / ***NO** / ***GUARD(...)**

*GUARD(...)

GUARD-NAME = <filename 1..18 without-cat-gen-vers>)

,**REM**OVE-**USER-ACCESS** = ***NONE** / ***ALL** / list-poss(48): ***OWNER** / ***GR**OUP / ***OTHERS** / ***CONSOLE** / <name 1..8>

,**ADD-USER-ACCESS** = ***NONE** / ***ALL** / list-poss(48): ***OWNER** / ***GR**OUP / ***OTHERS** / ***CONSOLE** / <name 1..8>

,**GUARD-NAME** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>

***Y**ES(...)

PASSWORD-**CHECK** = ***UNCHA**NGED / ***Y**ES / ***NO** / ***GUARD(...)**

*GUARD(...)

GUARD-NAME = <filename 1..18 without-cat-gen-vers>)

,**REM**OVE-**USER-ACCESS** = ***NONE** / ***ALL** / list-poss(48): ***OWNER** / ***GR**OUP / ***OTHERS** / ***CONSOLE** / <name 1..8>

,**ADD-USER-ACCESS** = ***NONE** / ***ALL** / list-poss(48): ***OWNER** / ***GR**OUP / ***OTHERS** / ***CONSOLE** / <name 1..8>

,**GUARD-NAME** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>

,**OPER**ATOR-**ACCESS-TERM** = ***UNCHA**NGED / ***LOGON-DEF**AULT(...) / ***NO** / ***Y**ES(...)

***LOGON-DEF**AULT(...)

PASSWORD-**CHECK** = ***UNCHA**NGED / ***Y**ES / ***NO**

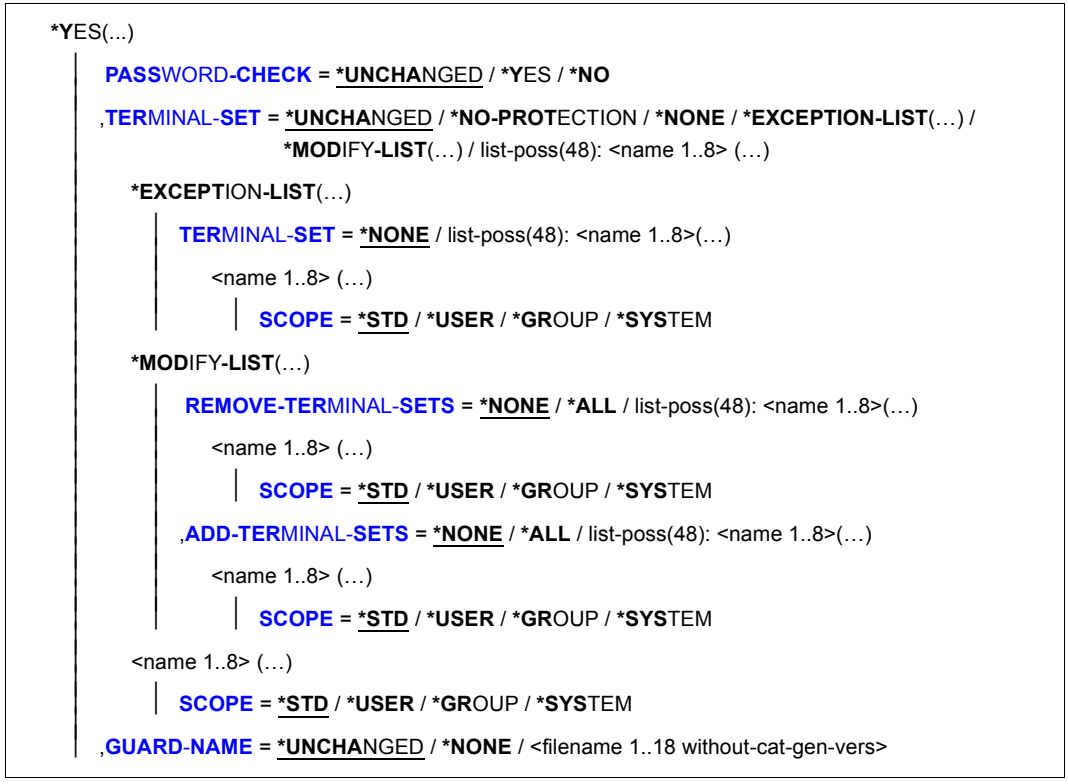
***Y**ES(...)

PASSWORD-**CHECK** = ***UNCHA**NGED / ***Y**ES / ***NO**

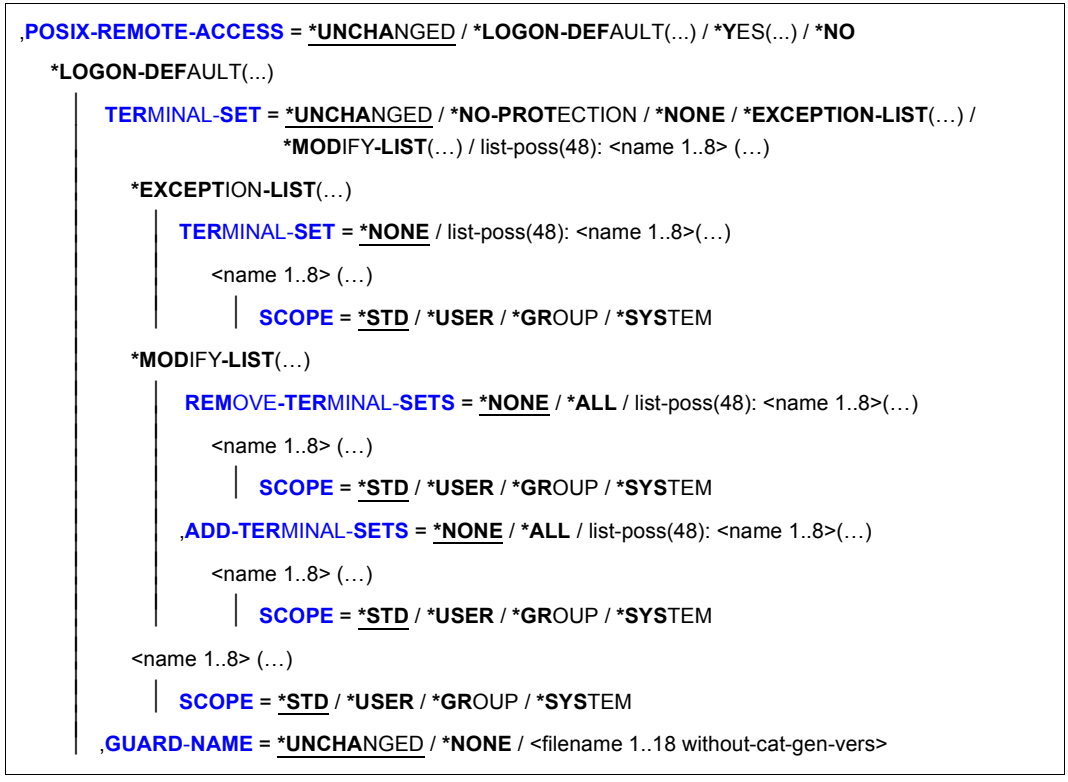
(Teil 5 von 11)

```
,OPERATOR-ACCESS-PROG = *UNCHANGED / *LOGON-DEFAULT(...) / *NO / *YES(...)
    *LOGON-DEFAULT(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
    *YES(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
,OPERATOR-ACCESS-CONS = *UNCHANGED / *LOGON-DEFAULT(...) / *NO / *YES(...)
    *LOGON-DEFAULT(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
    *YES(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
,POSIX-RLOGIN-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
    *LOGON-DEFAULT(...)
        PASSWORD-CHECK = *UNCHANGED / *YES / *NO
        ,TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(...) /
                        *MODIFY-LIST(...) / list-poss(48): <name 1..8> (...)
            *EXCEPTION-LIST(...)
                TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            *MODIFY-LIST(...)
                REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
                ,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(...)
                    <name 1..8> (...)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            <name 1..8> (...)
                SCOPE = *STD / *USER / *GROUP / *SYSTEM
        ,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
```

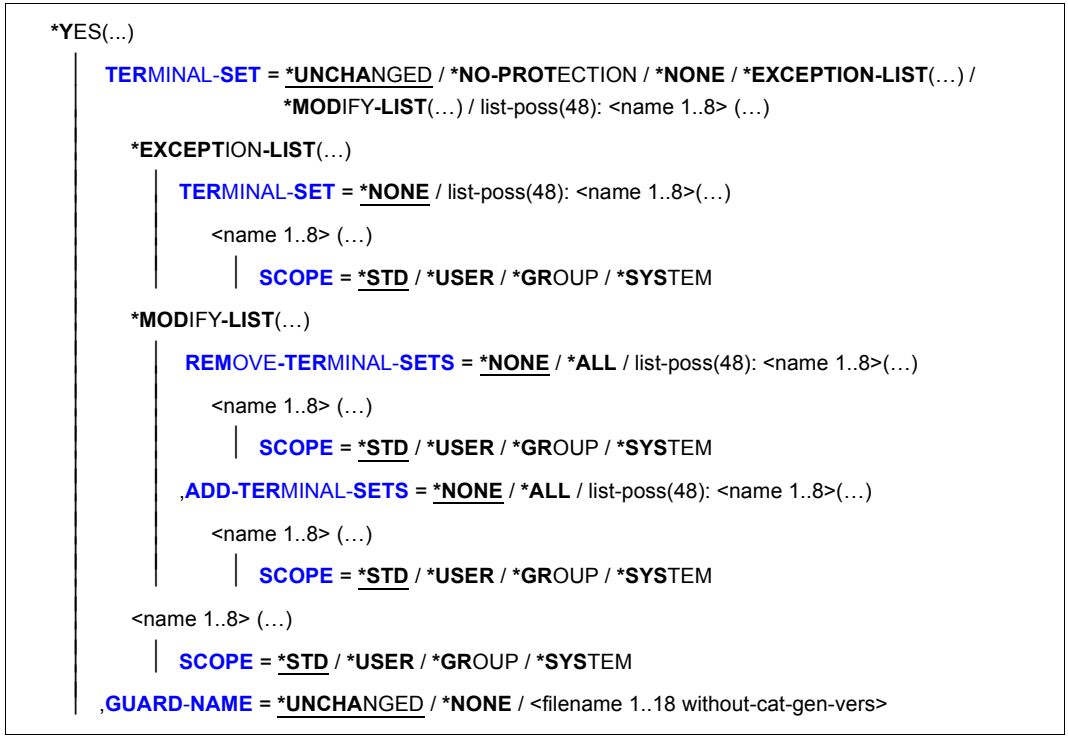
(Teil 6 von 11)


*YES(...)
PASSWORD-CHECK = *UNCHANGED / *YES / *NO
,TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
*MODIFY-LIST(…) / list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
*MODIFY-LIST(…)
REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 7 von 11)

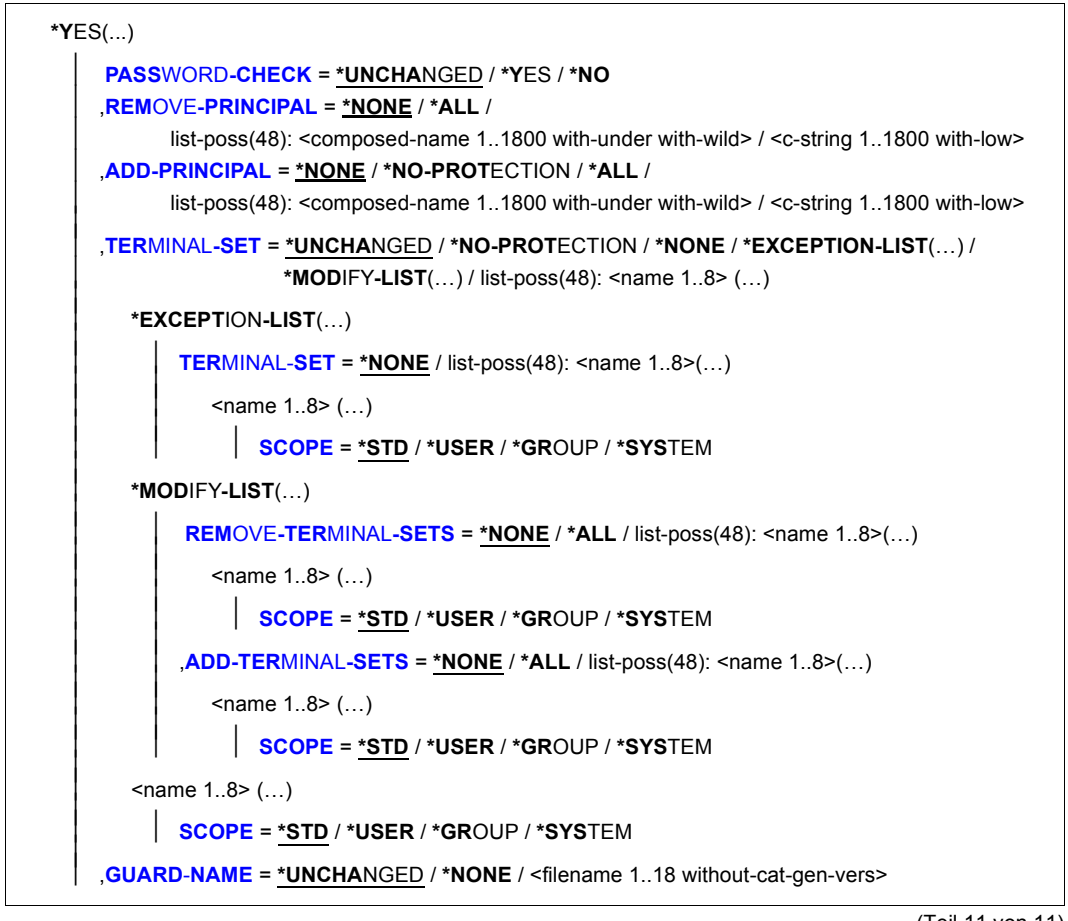

,POSIX-REMOTE-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) / *MODIFY-LIST(…) / list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
*MODIFY-LIST(…)
REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 8 von 11)


*YES(...)
TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
*MODIFY-LIST(…) / list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
*MODIFY-LIST(…)
REMOVE-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,ADD-TERMINAL-SETS = *NONE / *ALL / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 9 von 11)

(Teil 10 von 11)



(Teil 11 von 11)

Der Operandenwert *LOGON-DEFAULT bedeutet, dass die mit dem Kommando /SET- oder /MODIFY-LOGON-DEFAULTS festgelegte Standard-Einstellung für den Operanden übernommen wird.

USER-IDENTIFICATION = <name 1..8>
Benutzerkennung, deren Schutzattribute geändert werden sollen.

PUBSET = *HOME / <cat-id 1..4>
Pubset, in dessen Benutzerkatalog die Vereinbarungen eingetragen werden sollen.

PUBSET = *HOME
Der Eintrag erfolgt auf dem Home-Pubset.

PUBSET = <cat-id 1..4>
Der Eintrag erfolgt auf dem angegebenen Pubset.

EXPIRATION-DATE = *UNCHANGED / *LOGON-DEFAULT / *NONE / <date 8..10> / <integer 0..366>
Nach dem angegebenen Datum wird die Benutzerkennung gesperrt, d.h. sie ist über LOGON nicht mehr zugänglich. Die für die Benutzerkennung katalogisierten Dateien bleiben erhalten. Während des Zeitraums, der im Operanden EXPIRATION-WARNING angegeben ist, erhält der Benutzer bei jedem LOGON die Meldung SRM3201 auf SYSOUT.

EXPIRATION-DATE = *NONE
Die Benutzerkennung wird nicht zu einem bestimmten Datum gesperrt.

EXPIRATION-DATE = <date 8..10>
Verfallsdatum der Benutzerkennung.

EXPIRATION-DATE = <integer 0..366>
Lebensdauer der Benutzerkennung.

EXPIRATION-WARNING = *STD / *LOGON-DEFAULT / <integer 0..366>
Definiert den Zeitraum in Tagen, innerhalb dessen der Benutzer vor dem Überschreiten des Verfallsdatums der Benutzerkennung gewarnt wird. Der Standardwert beträgt 28 Tage.

PASSWORD = *UNCHANGED / *PARAMETERS(...)
Vereinbarungen bezüglich des Kennworts.

PASSWORD = *PARAMETERS(...)
Die Vereinbarungen für das Kennwort werden wie angegeben geändert.

LOGON-PASSWORD = *UNCHANGED / *NONE / *SECRET / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
Vom Benutzer einzugebendes Kennwort.

LOGON-PASSWORD = *NONE
Für den Zugang zu dieser Benutzerkennung wird kein Kennwort vereinbart.

LOGON-PASSWORD = *SECRET
Das Kennwort wird dunkelgesteuert angefordert. Dieser Operandenwert kann nur im ungeführten Dialog angegeben werden. Im geführten Dialog (Menü) steht für die Kennworteingabe generell ein dunkelgesteuertes Feld zur Verfügung.

ENCRYPTION = *YES / *NO
Gibt an, ob das Kennwort unverändert oder verschlüsselt abgelegt wird.

ENCRYPTION = *YES
Es wird gemäß dem Systemparameter ENCRYPT verschlüsselt.

MANAGEMENT = *UNCHANGED / *LOGON-DEFAULT / *USER-CHANGE-ONLY / *BY-USER / *BY-ADMINISTRATOR
Definiert die Berechtigung zur Verwaltung des Kennworts.

MANAGEMENT = *USER-CHANGE-ONLY
Der Benutzer darf das Kennwort vereinbaren und ändern, aber nicht löschen.

MANAGEMENT = *BY-USER
Der Benutzer darf das Kennwort vereinbaren, ändern und löschen.

MANAGEMENT = *BY-ADMINISTRATOR
Das Kennwort kann nur mit den Systembetreuungs-Kommandos /MODIFY-USER-ATTRIBUTES und /MODIFY-LOGON-PROTECTION verändert werden.

MINIMAL-LENGTH = *UNCHANGED / *LOGON-DEFAULT / *NONE / <integer 1..8>
Gibt die minimale Länge an, die ein vom Benutzer vereinbartes Kennwort haben muss (in Zeichen).

MINIMAL-LENGTH = *NONE
Es wird keine minimale Länge festgelegt. Der Benutzer darf Kennwörter bis zu einer Länge von 8 Zeichen vereinbaren.

MINIMAL-LENGTH = <integer 1..8>
Gibt die minimale Länge an, die ein vom Benutzer vereinbartes Kennwort haben muss (in Zeichen). Bei Verwendung dieses Operanden muss das Kennwort mit einem Zeichen ungleich Leerzeichen enden.

MINIMAL-COMPLEXITY = *UNCHANGED / *LOGON-DEFAULT / *NONE / <integer 1..4>
Gibt die minimale Komplexität an, die ein vom Benutzer vereinbartes Kennwort haben muss.

MINIMAL-COMPLEXITY = *NONE
Der Benutzer darf Kennwörter beliebiger Komplexität vereinbaren.

MINIMAL-COMPLEXITY = <integer 1..4>
Komplexitätsstufen mit folgenden Vorschriften (jede Stufe beinhaltet alle anderen Stufen mit kleinerer Kennziffer):

Stufe 1: Keine Einschränkungen.

Stufe 2: Maximal zwei aufeinander folgende Zeichen dürfen gleich sein.

Stufe 3: Es muss mindestens je ein Buchstabe und eine Ziffer im Kennwort angegeben sein.

Stufe 4: Es müssen mindestens je ein Buchstabe, eine Ziffer und ein Sonderzeichen (d.h. ein Zeichen aus der Restmenge) angegeben sein.
Das Leerzeichen zählt nicht als Sonderzeichen.

INITIAL-LIFETIME = *UNCHANGED / *LOGON-DEFAULT / *STD / *EXPIRED / <integer 0..366> / <date 8..10>
Definiert den ersten Lebensdauer-Zyklus.

INITIAL-LIFETIME = *STD
Das Verfallsdatum des Kennwortes wird aus LIFETIME-INTERVAL berechnet.

INITIAL-LIFETIME = *EXPIRED
Das eingetragene Logon-Kennwort wird als 'verfallen' gekennzeichnet. Der Eigentümer der Benutzerkennung muss zunächst ein neues Logon-Kennwort vereinbaren, bevor er mit seiner Benutzerkennung arbeiten kann. Näheres hierzu siehe Operand UNLOCK-EXPIRATION.

INITIAL-LIFETIME = <integer 0..366>
Lebensdauer des Kennwortes.

INITIAL-LIFETIME = <date 8..10>
Verfallsdatum des Kennwortes.

LIFETIME-INTERVAL = *UNCHANGED / *LOGON-DEFAULT / *UNLIMITED / <integer 1..366>(...)
Definiert den Zeitraum, in dem das Kennwort vom Benutzer immer wieder geändert werden muss. Ändert der Benutzer das Kennwort nicht rechtzeitig, wird die Benutzerkennung gesperrt. Während des Zeitraums, der im Operanden EXPIRATION-WARNING des Kennwortes angegeben ist, erhält der Benutzer bei jedem LOGON die Meldung SRM3201 auf SYSOUT.

LIFETIME-INTERVAL = *UNLIMITED
Das Kennwort muss vom Benutzer nicht geändert werden.

LIFETIME-INTERVAL = <integer 1..366>(...)
Gibt den Zeitraum an, in dem das Kennwort vom Benutzer geändert werden muss.

DIMENSION = *DAYS / *MONTHS
Einheit des angegebenen Zahlenwertes. Bei Angabe von *MONTHS ist der maximal zulässige Wert 12.

EXPIRATION-WARNING = *UNCHANGED / *LOGON-DEFAULT / *STD / <integer 0..366>
Definiert den Zeitraum in Tagen, innerhalb dessen der Benutzer vor dem Überschreiten des Verfallsdatums des Kennwortes gewarnt wird. Der Standardwert beträgt 28 Tage.

UNLOCK-EXPIRATION = *UNCHANGED / *LOGON-DEFAULT / *BY-ADMINISTRATOR-ONLY / *BY-USER
Gibt an, wer berechtigt ist, ein verfallenes Kennwort durch ein neues zu ersetzen.

UNLOCK-EXPIRATION = *BY-ADMINISTRATOR-ONLY
Nach Überschreiten des Verfallsdatums des Kennwortes wird die Kennung gesperrt. Die Systembetreuung muss ein neues Logon-Kennwort eintragen, um damit dem Eigentümer der Benutzerkennung den Zugang wieder zu ermöglichen.

UNLOCK-EXPIRATION = *BY-USER
Nach Überschreiten des Verfallsdatums wird dem Anwender bei Angabe des verfallenen Kennwortes ein eingeschränkter Dialog-Zugang gewährt. Dabei hat der Anwender nur die Möglichkeit ein neues Kennwort zu vereinbaren oder die Dialog-Task wieder zu beenden.

PASSWORD-MEMORY = *UNCHANGED / *LOGON-DEFAULT / *NONE / YES(…)
Gibt an, ob bei einer Änderung des Kennwortes das alte Kennwort in einer Liste abgelegt wird. Kennwörter, die in dieser Liste enthalten sind, dürfen bei einer Kennwortänderung nicht als neues Kennwort vergeben werden. Außerdem kann die Häufigkeit von Kennwortänderungen eingeschränkt werden.

PASSWORD-MEMORY = *NONE
Es wird keine Kennwortliste angelegt. Falls bereits eine existiert, wird sie gelöscht. Die Häufigkeit von Kennwortänderungen wird nicht eingeschränkt.

PASSWORD-MEMORY = *YES(…)
Es wird eine Kennwortliste angelegt. Außerdem wird eine Maximalzahl für Kennwortänderungen festgelegt, die innerhalb eines definierten Zeitraums erlaubt sind.

Die Operanden PERIOD, CHANGES-PER-PERIOD und BLOCKING-TIME hängen folgendermaßen voneinander ab:

– PERIOD ≤ BLOCKING-TIME

– CHANGES-PER-PERIOD ≤ (100 * PERIOD) / BLOCKING-TIME

PERIOD = <integer 1..32767>
Legt den Zeitraum fest, für den mit dem Operanden CHANGES-PER-PERIOD ein Maximalwert für die Anzahl von Kennwortänderungen festgelegt wird. Die Dauer wird in Tagen angegeben.

CHANGES-PER-PERIOD = <integer 1..100>
Gibt die maximale Anzahl erlaubter Kennwortänderungen innerhalb des Zeitraums an, der im Operanden PERIOD festgelegt wird. Kennwortänderungen auf das Kennwort *NONE werden bei dieser Zählung nicht berücksichtigt.

BLOCKING-TIME = <integer 1..32767>
Legt fest, wie lange ein Kennwort in der Kennwortliste gespeichert bleibt. Die Dauer wird in Tagen angegeben und beginnt an dem Tag, an dem ein Kennwort durch ein anderes ersetzt wird.

SUSPEND-ATTRIBUTES = *UNCHANGED / *LOGON-DEFAULT / *NONE / *YES(...)
Legt die Attribute für die Suspendierung fest. Die temporäre Sperre einer Benutzerkennung bzw. des Benutzers einer Benutzerkennung nach einer Anzahl fehlerhafter Zugangsversuche kann lokal für diese Benutzerkennung oder global in den Standard-Attributen festgelegt werden.

SUSPEND-ATTRIBUTES = *NONE
Es findet keine Suspendierung statt.

SUSPEND-ATTRIBUTES = *YES(...)
Vereinbart die Parameter für die Suspendierung.

COUNT = *UNCHANGED / *LOGON-DEFAULT / <integer 0..32767>
Anzahl fehlerhafter Zugangsversuche, die innerhalb des mit OBSERVE-TIME festgelegten Zeitraums erlaubt sind. Weitere fehlerhafte Zugangsversuche haben eine Suspendierung zur Folge.

OBSERVE-TIME = *UNCHANGED / *LOGON-DEFAULT / <integer 0..32767> (…)
Zeitraum, innerhalb dessen die mit dem Operanden COUNT angegebene Anzahl fehlerhafter Zugangsversuche stattfinden muss. Der Zeitraum beginnt mit dem ersten fehlerhaften Zugangsversuch. Ist der Beobachtungszeitraum beendet, ohne dass eine Suspendierung erfolgt ist, beginnt die Zählung beim nächsten Fehlversuch von vorne.

OBSERVE-TIME = <integer 0..32767> (…)
Angabe des Beobachtungszeitraums.

DIMENSION = *MINUTE / *HOUR
Zeiteinheit für den Beobachtungszeitraum.

SUSPEND-TIME = *UNCHANGED / *LOGON-DEFAULT / <integer 1..32767> (…) / *UNLIMITED
Vereinbart die Dauer der Suspendierung. Während der Suspendierung wird ein Benutzer mit den Meldungen SRM3208 oder SRM3209 über die Tatsache und ggf. Dauer der Suspendierung informiert.

SUSPEND-TIME = <integer 1..32767> (…)
Dauer der Suspendierung.

DIMENSION = *MINUTE / *HOUR
Zeiteinheit für die Suspendierung.

SUSPEND-TIME = *UNLIMITED
Die Suspendierung ist von unbegrenzter Dauer.

SUBJECT = *UNCHANGED / *LOGON-DEFAULT / *USER-IDENTIFICATION / *INITIATOR
Legt fest, ob die Benutzerkennung oder die Person, die die Zugangsversuche unternommen hat, suspendiert werden soll.

SUBJECT = *USER-IDENTIFICATION
Die Benutzerkennung wird suspendiert.
Diese Angabe ist bei der Systemkennung TSOS und der Benutzerkennung des Sicherheitsbeauftragten nicht erlaubt und wird mit Meldung SRM3672 abgewiesen.

SUBJECT = *INITIATOR
Die „Person“, die die Zugangsversuche unternommen hat, wird suspendiert (siehe Abschnitt „Sperrung von Terminals/Benutzerkennungen nach erfolglosen Zugangsversuchen“ auf Seite 119).

INACTIVITY-LIMIT = *UNCHANGED / *LOGON-DEFAULT / *NONE / <integer 1..366> (…) / *RENEW
Vereinbart die Zeit der Inaktivität, also die seit dem letzten Logon verstrichene Zeit, nach der die Benutzerkennung gesperrt werden soll, oder hebt eine Sperre wieder auf.

INACTIVITY-LIMIT = *NONE
Es findet keine Überwachung der Inaktivität statt.

INACTIVITY-LIMIT = <integer 1..366> (…)
Angabe der Zeit bis zum Eintritt der Sperre (Inaktivitätslimit).
Diese Angabe ist bei Systemkennungen nicht erlaubt und wird mit Meldung SRM3673 abgewiesen.

DIMENSION = *DAYS / *MONTHS
Zeiteinheit für das Inaktivitätslimit.

INACTIVITY-LIMIT = *RENEW
Erneuert aufgrund des eingestellten Inaktivitäts-Limits das Datum für die Sperre der Benutzerkennung. Dadurch wird eine Sperre wegen Inaktivität wieder aufgehoben und die Überwachungsphase beginnt von neuem.

DIALOG-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *NO / *YES(...)
Definiert die im Dialogbetrieb wirksamen Zugangskontrollen.

DIALOG-ACCESS = *NO
Dialogzugang ist prinzipiell verboten.

DIALOG-ACCESS = *YES(...)
Legt fest, dass Zugangskontrollen durchgeführt werden.

PASSWORD-CHECK = *UNCHANGED / *YES / *NO
Legt fest, ob im Dialog eine Kennwortprüfung stattfindet.

REMOVE-TERMINALS =
Liste der Datensichtstationen, von denen Dialog-LOGON nicht mehr möglich ist. Dieser Operand wird aus Kompatibilitätsgründen unterstützt. Die Steuerung über den Operanden TERMINAL-SET ist zu bevorzugen.

REMOVE-TERMINALS = *NONE
Es werden keine Datensichtstationen aus der Zugriffsliste entfernt.

REMOVE-TERMINALS = *ALL
Alle Datensichtstationen werden aus der Zugriffsliste entfernt.

REMOVE-TERMINALS = *PARAMETERS(...)
Explizite Angabe von Datensichtstationen, die aus der Zugriffsliste entfernt werden. Die explizite Angabe von Datensichtstationen ist nicht möglich, falls zuvor mit *ALL alle Datensichtstationen zugelassen waren.

PROCESSOR = <name 1..8 with-wild>
BCAM-Name des Rechners, von dem aus die Verbindung zu $DIALOG aufgebaut wird (z.B. ein PC, auf dem eine Datensichtstations-Emulation läuft).

STATION = <name 1..8 with-wild>
Logischer Name der Datensichtstation.

ADD-TERMINALS =
Liste der Datensichtstationen, von denen zusätzlich Dialog-LOGON möglich ist (BCAM-Namen). Dieser Operand wird aus Kompatibilitätsgründen unterstützt. Die Steuerung über den Operanden TERMINAL-SET ist zu bevorzugen.

ADD-TERMINALS = *NONE
Es werden keine zusätzlichen Datensichtstationen zugelassen.

ADD-TERMINALS = *ALL
Alle Datensichtstationen sind zugelassen. Etwaige Listen explizit angegebener Datensichtstationen werden gelöscht. ADD-TERMINALS=*ALL ist nur in Verbindung mit REMOVE-TERMINALS=*NONE zulässig.

ADD-TERMINALS = *PARAMETERS(...)
Explizite Angabe von Datensichtstationen, die zugelassen werden.

PROCESSOR = <name 1..8 with-wild>
BCAM-Name des Rechners, von dem aus die Verbindung zu $DIALOG aufgebaut wird.

STATION = <name 1..8 with-wild>
Logischer Name der Datensichtstation.

TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(...) / *MODIFY-LIST(…) / list-poss(48): <name 1..8>(…)
Angabe, ob der Dialog-Zugang der Kennung mit Terminal-Sets geschützt wird.

TERMINAL-SET = *NO-PROTECTION
Der Schutz der Kennung durch Terminal-Sets wird abgeschaltet.

TERMINAL-SET = *NONE
Der Kennung wird für den Dialog-Zugang eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Dialogzugang erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = list-poss(48): <name 1..8>(…)

Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Dialogzugang verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = *MODIFY-LIST(…)
Es werden Änderungen an einer bereits definierten Terminal-Set-Liste vorgenommen. Die Eigenschaft der Liste, ob sie eine Positiv- oder Negativliste ist, bleibt von der Modifikation unberührt.

REMOVE-TERMINAL-SETS =
Angabe von Terminal-Sets, die aus der Terminal-Set-Liste für den Dialog-Zugang der Benutzerkennung entfernt werden sollen.

Falls für den Dialog-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird eine Warnung ausgegeben und die Kommandobearbeitung fortgesetzt. Dasselbe gilt, wenn eines oder mehrere der zu entfernenden Terminal-Sets nicht in der Liste enthalten sind.

REMOVE-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = *ALL
Alle Terminal-Sets werden aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden aus der Terminal-Set-Liste entfernt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

ADD-TERMINAL-SETS =
Angabe von Terminal-Sets, die in die definierte Terminal-Set-Liste für den Dialog-Zugang der Benutzerkennung eingefügt werden sollen.

Falls für den Dialog-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird implizit eine Positivliste angelegt. Wenn eines oder mehrere der einzufügenden Terminal-Sets bereits in der Liste enthalten sind, wird eine Warnung ausgegeben.

ADD-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets in die definierte Terminal-Set-Liste eingefügt.

ADD-TERMINAL-SETS = *ALL
Alle Terminal-Sets werden in dieTerminal-Set-Liste eingefügt.

ADD-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden in die definierte Terminal-Set-Liste eingefügt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Dialogzugang erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID= *OWN).

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Gibt an, ob der Dialog-Zugang zu einer Benutzerkennung mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Dialog-Zugang zur Benutzerkennung wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang zur Benutzerkennung ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Welche Benutzerkennung als Subjekt in der Zugriffsbedingung des Guards zugelassen sein muss, hängt vom Operanden PERSONAL-LOGON ab. Bei PERSONAL-LOGON=*NO gilt die geschützte Benutzerkennung als Subjekt der Zugriffsbedingung. Bei PERSONAL-LOGON=*YES ist das die persönliche Benutzerkennung.

PERSONAL-LOGON = *UNCHANGED / *NO / *YES / *PRIVILEGED
Legt fest, ob beim Dialogzugang neben der Logon- auch eine persönliche Benutzerkennung verlangt wird.

PERSONAL-LOGON = *NO
Es wird nur die Logon-Benutzerkennung verlangt.

PERSONAL-LOGON = *YES
Es wird zusätzlich zur Logon- eine persönliche Benutzerkennung verlangt.

PERSONAL-LOGON = *PRIVILEGED
Es wird zusätzlich zur Logon- eine persönliche Benutzerkennung verlangt.

Außerdem erhält die Dialog-Task zusätzlich zu den Privilegien der Logon-Kennung auch die der persönlichen Kennung (außer TSOS, falls vorhanden).

Die Vorgabe zur Protokollierung aller Ereignisse (AUDIT-SWITCH=*ON) wird aus den Einstellungen der SAT-Preselection für die Protokollierung der persönlichen Benutzerkennung (USER-AUDITING) in die Dialog-Task übernommen.

Ist die Logon-Kennung Gruppenverwalter und die persönliche Kennung Benutzerverwalter, übernimmt die Dialog-Task die Rolle des Gruppenverwalters und erhält nicht das Privileg USER-ADMINISTRATION.

Einschränkung für Systeme mit BS2000 OSD/BC ≤ V11.0A:

Die systeminterne SCI-Schnittstelle (Synchronous Console Interface) ermöglicht die Eingabe von Operator-Kommandos aus einer Benutzer-Task. Diese Operator-Kommandos schlagen fehl, wenn sie erst durch ein persönliches Logon mit der Übernahme der Privilegien der persönlichen Benutzerkennung in den Kommandovorrat aufgenommen werden (z.B. diverse BCAM-Kommandos über das Privileg NET-ADMINISTRATION).

Die Vereinigungsmenge der Privilegien kann mit folgendem Kommando angezeigt werden:

```
/SHOW-PRIVILEGE INFORMATION = *RUN-PRIVILEGE(…)
```

BATCH-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *NO / *YES(...)
Definiert die im Batchbetrieb wirksamen Zugangskontrollen.

BATCH-ACCESS = *NO
Der Zugang im Batchbetrieb ist prinzipiell verboten.

BATCH-ACCESS = *YES(...)
Legt die im Batchbetrieb wirksamen Zugangskontrollen fest.

PASSWORD-CHECK = *UNCHANGED / *YES / *NO / *GUARD(...)
Legt fest, ob für Batchaufträge Kennwortprüfung stattfindet.

PASSWORD-CHECK = *GUARD(...)
Das Recht, Batchaufträge ohne Kennwort zu starten, wird über ein Guard verwaltet.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Batchaufträge dürfen ohne Kennwort gestartet werden, wenn für die aufrufende Benutzerkennung die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards sind zwei Fälle zu unterscheiden:

– Wurde der Batchauftrag im BS2000 angefordert, werden alle Bedingungen berücksichtigt. Subjekt der Zugriffsbedingung ist die Benutzerkennung, unter der das Kommando ENTER-JOB eingegeben wurde.
– Wurde der Batchauftrag unter POSIX angefordert, werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

REMOVE-USER-ACCESS =
Legt fest, von welchen Benutzerkennungen keine Batchaufträge auf der Benutzerkennung gestartet werden dürfen.

REMOVE-USER-ACCESS = *NONE
Keine Einschränkungen gegenüber der bisher definierten Berechtigung.

REMOVE-USER-ACCESS = *ALL
Alle in der bisherigen Liste zugelassenen Benutzerkennungen werden entfernt.

REMOVE-USER-ACCESS = *OWNER
Von der unter USER-IDENTIFICATION angegebenen Benutzerkennung selbst dürfen keine Batchaufträge mehr gestartet werden.

REMOVE-USER-ACCESS = *GROUP
Von keiner der zur Gruppe der USER-IDENTIFICATION gehörigen Benutzerkennungen (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung selbst) dürfen Batchaufträge auf dieser Benutzerkennung gestartet werden.

REMOVE-USER-ACCESS = *OTHERS
Von keiner der Benutzerkennungen des Rechners (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung und deren Benutzergruppe) dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

REMOVE-USER-ACCESS = *CONSOLE
Von einem Operator ohne eigene Benutzerkennung dürfen auf dieser Benutzerkennung keine Batchaufträge gestartet werden.

REMOVE-USER-ACCESS = <name 1..8>
Von keiner der in der Liste aufgeführten Benutzerkennungen dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

ADD-USER-ACCESS =
Legt fest, von welchen Benutzerkennungen zusätzlich auf der Benutzerkennung Batchaufträge gestartet werden dürfen.

ADD-USER-ACCESS = *NONE
Keine zusätzliche Zugangsberechtigung wird vergeben.

ADD-USER-ACCESS = *ALL
Von allen Benutzerkennungen dürfen Batchaufträge gestartet werden. Etwaige Listen explizit angegebener Benutzerkennungen werden gelöscht. ADD-USER-ACCESS=*ALL ist nur in Verbindung mit REMOVE-USER-ACCESS=*NONE zulässig.

ADD-USER-ACCESS = *OWNER
Von der unter USER-IDENTIFICATION angegebenen Benutzerkennung selbst dürfen Batchaufträge gestartet werden.

ADD-USER-ACCESS = *GROUP
Von allen zur Gruppe der USER-IDENTIFICATION gehörigen Benutzerkennungen (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung selbst) dürfen Batchaufträge auf dieser Benutzerkennung gestartet werden.

ADD-USER-ACCESS = *OTHERS
Von allen Benutzerkennungen des Rechners (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung und deren Benutzergruppe) dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

ADD-USER-ACCESS = *CONSOLE
Von einem Operator ohne eigene Benutzerkennung dürfen auf dieser Benutzerkennung Batchaufträge gestartet werden.

ADD-USER-ACCESS = <name 1..8>
Von allen in der Liste aufgeführten Benutzerkennungen dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Gibt an, ob der Batch-Zugang zu einer Benutzerkennung mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Batch-Zugang zur Benutzerkennung wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Batch-Zugang zur Benutzerkennung ist nur erlaubt, wenn für die aufrufende Benutzerkennung die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards sind zwei Fälle zu unterscheiden:

– Wurde der Batchauftrag im BS2000 angefordert, werden alle Bedingungen berücksichtigt. Subjekt der Zugriffsbedingung ist die Benutzerkennung, unter der das Kommando ENTER-JOB eingegeben wurde.

– Wurde der Batchauftrag unter POSIX angefordert, werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

OPERATOR-ACCESS-TERM = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert die im Operating-Betrieb für Dialog-Partner wirksamen Authentisierungsverfahren. Die Möglichkeiten der Operator-Authentisierung sind detailliert im Handbuch „Einführung in die Systembetreuung“ [2] beschrieben.

OPERATOR-ACCESS-TERM = *YES(...)
Operating-Betrieb ist für diese Kennung erlaubt.

PASSWORD-CHECK = *UNCHANGED / *YES / *NO
Legt fest, ob im Dialog eine Kennwortprüfung stattfindet.

OPERATOR-ACCESS-TERM = *NO
Es ist kein Operating-Betrieb für diese Kennung möglich.

OPERATOR-ACCESS-PROG = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert die im Operating-Betrieb für Programmierte Operatoren (PROP-XT) wirksamen Authentisierungsverfahren.
Die Möglichkeiten der Operator-Authentisierung sind detailliert im Handbuch „Einführung in die Systembetreuung“ [2] beschrieben.

OPERATOR-ACCESS-PROG = *YES(...)

PASSWORD-CHECK = *UNCHANGED / *YES / *NO
Legt fest, ob für den programmierten Operator eine Kennwortprüfung stattfindet oder nicht.

OPERATOR-ACCESS-PROG = *NO
Die Zugangsklasse OPERATOR-ACCESS-PROGRAM ist für den programmierten Operator gesperrt.

OPERATOR-ACCESS-CONS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Bestimmt, ob unter dieser Benutzerkennung ein Zugang an der physikalischen Konsole im inkompatiblen Modus erlaubt ist.

OPERATOR-ACCESS-CONS = *YES(...)
Der Konsol-Zugang ist erlaubt.

PASSWORD-CHECK = *UNCHANGED / *YES / *NO
Legt fest, ob beim Konsol-Zugang eine Kennwortprüfung stattfindet.

OPERATOR-ACCESS-CONS = *NO
Es ist kein Konsol-Zugang möglich.

POSIX-RLOGIN-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Die Zugangsklassen-Attribute für POSIX-Remote-Login können festgelegt werden.

POSIX-RLOGIN-ACCESS = *YES(...)
Die BS2000-Benutzerkennung ist für den Systemzugang über POSIX-Remote-Login offen.

PASSWORD-CHECK = *UNCHANGED / *YES / *NO
Legt fest, ob beim Zugang über POSIX-Remote-Login eine Kennwortprüfung stattfindet.

TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(...) / *MODIFY-LIST(…) / list-poss(48): <name 1..8>(…)
Angabe, ob die Kennung für den Zugang über POSIX-Remote-Login mit Terminal-Sets geschützt wird. Im entsprechenden Eintrag des Terminal-Sets darf nur der Prozessorname des UNIX-Clients angegeben werden. Als Stationsname ist *ANY anzugeben.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird für den Zugang über POSIX-Remote-Login eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein POSIX-Remote-Login erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE
Die Negativliste ist leer, d.h. POSIX-Remote-Login ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über POSIX-Remote-Login verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = *MODIFY-LIST(…)
Es werden Änderungen an einer bereits definierten Terminal-Set-Liste vorgenommen. Die Eigenschaft der Liste, ob sie eine Positiv- oder Negativliste ist, bleibt von der Modifikation unberührt.

REMOVE-TERMINAL-SETS =
Angabe von Terminal-Sets, die aus der Terminal-Set-Liste für den POSIX-Remote-Login-Zugang der Benutzerkennung entfernt werden sollen.

Falls für den POSIX-Remote-Login-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird eine Warnung ausgegeben und die Kommandobearbeitung fortgesetzt. Dasselbe gilt, wenn eines oder mehrere der zu entfernenden Terminal-Sets nicht in der Liste enthalten sind.

REMOVE-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = *ALL
Alle Terminal-Sets werden aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden aus der Terminal-Set-Liste entfernt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

ADD-TERMINAL-SETS =
Angabe von Terminal-Sets, die in die definierte Terminal-Set-Liste für den POSIX-Remote-Login-Zugang der Benutzerkennung eingefügt werden sollen.

Falls für den POSIX-Remote-Login-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird implizit eine Positivliste angelegt. Wenn eines oder mehrere der einzufügenden Terminal-Sets bereits in der Liste enthalten sind, wird eine Warnung ausgegeben.

ADD-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets in die definierte Terminal-Set-Liste eingefügt.

ADD-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden in die definierte Terminal-Set-Liste eingefügt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über POSIX-Remote-Login erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD

Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Gibt an, ob der Zugang über POSIX-Remote-Login mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Zugang über POSIX-Remote-Login wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang über POSIX-Remote-Login ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

POSIX-RLOGIN-ACCESS = NO
Die BS2000-Benutzerkennung ist für den Systemzugang über POSIX-Remote-Login gesperrt.

POSIX-REMOTE-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Die BS2000-Benutzerkennung wird für den Systemzugang über ein POSIX-Remote-Kommando geöffnet oder gesperrt.

TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE / *EXCEPTION-LIST(...) / *MODIFY-LIST(…) / list-poss(48): <name 1..8>(…)
Angabe, ob die Kennung für den Zugang über ein POSIX-Remote-Kommando mit Terminal-Sets geschützt wird. Im entsprechenden Eintrag des Terminal-Sets darf nur der Prozessorname des UNIX-Clients angegeben werden. Als Stationsname ist *ANY anzugeben.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird für den Zugang über ein POSIX-Remote-Kommando eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Zugang über ein POSIX-Remote-Kommando erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. der Zugang über ein POSIX-Remote-Kommando ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über ein POSIX-Remote-Kommando verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = *MODIFY-LIST(…)
Es werden Änderungen an einer bereits definierten Terminal-Set-Liste vorgenommen. Die Eigenschaft der Liste, ob sie eine Positiv- oder Negativliste ist, bleibt von der Modifikation unberührt.

REMOVE-TERMINAL-SETS =
Angabe von Terminal-Sets, die aus der Terminal-Set-Liste für den POSIX-Remote-Kommando-Zugang der Benutzerkennung entfernt werden sollen.

Falls für den POSIX-Remote-Kommando-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird eine Warnung ausgegeben und die Kommandobearbeitung fortgesetzt. Dasselbe gilt, wenn eines oder mehrere der zu entfernenden Terminal-Sets nicht in der Liste enthalten sind.

REMOVE-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = *ALL
Alle Terminal-Sets werden aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden aus der Terminal-Set-Liste entfernt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

ADD-TERMINAL-SETS =
Angabe von Terminal-Sets, die in die definierte Terminal-Set-Liste für den POSIX-Remote-Kommando-Zugang der Benutzerkennung eingefügt werden sollen.

Falls für den POSIX-Remote-Kommando-Zugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird implizit eine Positivliste angelegt. Wenn eines oder mehrere der einzufügenden Terminal-Sets bereits in der Liste enthalten sind, wird eine Warnung ausgegeben.

ADD-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets in die definierte Terminal-Set-Liste eingefügt.

ADD-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden in die definierte Terminal-Set-Liste eingefügt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über ein POSIX-Remote-Kommando erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD
Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Gibt an, ob der Zugang über ein POSIX-Remote-Kommando mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Zugang über ein POSIX-Remote-Kommando wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang über ein POSIX-Remote-Kommando ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die UNIX/POSIX-Benutzerkennung, unter der das Kommando `rsh` bzw. `rcp` eingegeben wurde. Es ist nicht notwendig, dass diese Kennung im BS2000 existiert.

POSIX-REMOTE-ACCESS = *NO
Die BS2000-Benutzerkennung ist für den Systemzugang über ein POSIX-Remote-Kommando gesperrt.

NET-DIALOG-ACCESS = *UNCHANGED / *LOGON-DEFAULT(...) / *YES(...) / *NO
Angabe, ob der Dialogzugang aus dem Netzwerk erlaubt ist.

NET-DIALOG-ACCESS = *YES(…)
Der Dialogzugang aus dem Netzwerk ist zugelassen.

PASSWORD-CHECK = *YES / *NO
Legt fest, ob beim Netzwerk-Zugang die Prüfung des Logon-Kennwortes stattfinden soll.

REMOVE-PRINCIPAL =
Angabe für den Zugang unter Nutzung der Kerberos-Authentisierung.
Löschen von Kerberos-Namen aus der Liste von Kerberos-Namen, die Zugang zu dieser Benutzerkennung haben.

REMOVE-PRINCIPAL = *NONE
Aus der Liste von Kerberos-Namen werden keine Namen entfernt.

REMOVE-PRINCIPAL = *ALL
Die Liste der Kerberos-Namen wird geleert, bleibt aber gültig. Clients, die auf Nachfrage ein Kerberos-Ticket vorweisen können, werden abgewiesen.

REMOVE-PRINCIPAL = list-poss(48):
<composed-name 1..1800 with-under with-wild> / <c-string 1..1800 with-low>
Die angegebenen Kerberos-Namen werden aus der Liste gelöscht.

ADD-PRINCIPAL =
Angabe für den Zugang unter Nutzung der Kerberos-Authentisierung.
Hinzufügen von Kerberos-Namen zu der Liste von Kerberos-Namen, die Zugang zu dieser Benutzerkennung haben.

ADD-PRINCIPAL = *NONE
Der Liste von Kerberos-Namen wird kein weiterer Name hinzugefügt.

ADD-PRINCIPAL = *NO-PROTECTION
Für die Benutzerkennung wird der Schutz durch Kerberos-Authentisierung aufgehoben. Eine eventuell bestehende Liste von Kerberos-Namen wird gelöscht. Der Client wird nicht zur Vorlage eines Kerberos-Ticket aufgefordert, der Zugang wird direkt der Klasse DIALOG-ACCESS zugeordnet.

ADD-PRINCIPAL = *ALL
Für die Benutzerkennung wird der Schutz durch Kerberos-Authentisierung aufgehoben. Eine eventuell bestehende Liste von Kerberos-Namen wird gelöscht. Der Client wird aber zur Vorlage eines Kerberos-Tickets aufgefordert. Der darin enthaltenen Kerberos-Name wird in der Logon-History angezeigt und als Audit-Identifikation verwendet. Unterstützt der Client keine Kerberos-Authentisierung, wird der Zugang der Klasse DIALOG-ACCESS zugeordnet.

ADD-PRINCIPAL = list-poss(48):
<composed-name 1..1800 with-under with-wild> / <c-string 1..1800 with-low>
Die angegebenen Kerberos-Namen werden der Liste hinzugefügt.

TERMINAL-SET = *UNCHANGED / *NO-PROTECTION / *NONE /
***EXCEPTION-LIST(...) / *MODIFY-LIST(…) / list-poss(48): <name 1..8>(…)**
Angabe, ob die Kennung für den Netzwerkzugang mit Terminal-Sets geschützt wird.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Netzwerkzugang erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. der Netzwerkzugang ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Netzwerkzugang verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET.

TERMINAL-SET = *MODIFY-LIST(…)
Es werden Änderungen an einer bereits definierten Terminal-Set-Liste vorgenommen. Die Eigenschaft der Liste, ob sie eine Positiv- oder Negativliste ist, bleibt von der Modifikation unberührt.

REMOVE-TERMINAL-SETS =
Angabe von Terminal-Sets, die aus der Terminal-Set-Liste für den Netzwerkzugang der Benutzerkennung entfernt werden sollen.
Falls für den Netzwerkzugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird eine Warnung ausgegeben und die Kommandobearbeitung fortgesetzt. Dasselbe gilt, wenn eines oder mehrere der zu entfernenden Terminal-Sets nicht in der Liste enthalten sind.

REMOVE-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = *ALL
Alle Terminal-Sets werden aus der Terminal-Set-Liste entfernt.

REMOVE-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden aus der Terminal-Set-Liste entfernt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

ADD-TERMINAL-SETS =
Angabe von Terminal-Sets, die in die definierte Terminal-Set-Liste für den Netzwerkzugang der Benutzerkennung eingefügt werden sollen.

Falls für den Netzwerkzugang der Benutzerkennung noch keine Terminal-Set-Liste definiert ist, wird implizit eine Positivliste angelegt. Wenn eines oder mehrere der einzufügenden Terminal-Sets bereits in der Liste enthalten sind, wird eine Warnung ausgegeben.

ADD-TERMINAL-SETS = *NONE
Es werden keine Terminal-Sets in die definierte Terminal-Set-Liste eingefügt.

ADD-TERMINAL-SETS = list-poss(48): <name 1..8>(…)
Die Terminal-Sets mit den angegebenen Namen werden in die definierte Terminal-Set-Liste eingefügt.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET=list-poss(48): <name 1..8>(...).

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Netzwerkzugang erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD

Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Gibt an, ob der Netzwerkzugang mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Netzwerkzugang wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Netzwerkzugang ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

NET-DIALOG-ACCESS = *NO
Die BS2000-Benutzerkennung ist für den Netzwerkzugang gesperrt.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel

Ausgegangen werde von folgendem SET-LOGON-PROTECTION-Kommando:

```
/set-logon-protection user-identification=tsos,
   password=*par(logon-pass='********',lifetime-interval=60),
   dialog-access=*yes(terminal-set=area52)
/modify-logon-protection user-identification=tsos,
   dialog-access=*yes(terminal-set=*modify-list(
   remove-terminal-sets=area52, add-terminal-sets=homebase))
```

Damit kann von den im Terminal-Set AREA52 angegebenen Terminals kein Dialog-LOGON mehr für TSOS durchgeführt werden. Stattdessen sind alle Terminals, die im Terminal-Set HOMEBASE enthalten sind, zugangsberechtigt.

```
/modify-logon-protection user-identification=tsos,
password=*parameters(lifetime-interval=3(dimension=*months))
```

Das Kennwort muss jetzt mindestens alle drei Monate gewechselt werden.

```
/modify-logon-protection user-identification=tsos,
  batch-access=*yes(add-user-access=(*group,X,Y))
```

Zusätzlich zu TSOS selbst können jetzt auch alle Mitglieder der Gruppe von TSOS sowie die Kennungen X und Y Batchaufträge auf der Kennung TSOS starten.

Ausgegeben wird:

```
/show-logon-protection user-identification=tsos

 LOGON PROTECTION FOR USERID TSOS     ON PUBSET A
 EXPIRATION DATE:     NONE              EXPIRATION WARNING:  28
 PASSWORD:            YES
     MANAGEMENT:      USER CHANGE ONLY
     MINIMAL LENGTH:  NONE              MINIMAL COMPLEXITY:  NONE
     LIFETIME:        3   MONTHS        EXPIRATION DATE:     2018-06-22
     UNLOCK EXPIR:    BY ADMINISTRATOR  EXPIRATION WARNING:  28
     PASSWORD MEMORY: NO
 DIALOG ACCESS:       YES               PASSWORD CHECK:      YES
     TERMINAL NAME:   ANY               CHIPCARD:            NO PROTECTION
     TERMINAL SET:    POSITIVE LIST
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     HOMEBASE
     GUARD:           *NONE
     PERSONAL LOGON:  NO
 BATCH ACCESS:        YES               PASSWORD CHECK:      YES
     CALLER USERID:   SEE LIST BELOW
     LIST OF AUTHORIZED USER IDENTIFICATIONS:
     *OWNER    *GROUP
     X         Y
     GUARDS:          NONE
  OPERATOR ACCESS TERM:YES               PASSWORD CHECK:      YES
     CHIPCARD:        NO PROTECTION
 OPERATOR ACCESS PROG:YES               PASSWORD CHECK:      YES
 OPERATOR ACCESS CONS:YES               PASSWORD CHECK:      YES
 POSIX RLOGIN ACCESS: YES               PASSWORD CHECK:      YES
     TERMINAL SET:    NO PROTECTION
     GUARD:           *NONE
 POSIX REMOTE ACCESS: YES
     TERMINAL SET:    NO PROTECTION
     GUARD:           *NONE
  NET DIALOG ACCESS:   YES               PASSWORD CHECK:      YES
     TERMINAL SET:    NO PROTECTION     CERTIFICATE:         NO PROTECTION
     PRINCIPAL:       NO PROTECTION
     GUARD:           *NONE
```

MODIFY-PRIVILEGE-SET
Sammelprivileg ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Dieses Kommando ändert ein bestehendes Sammelprivileg. Erläuterungen zu Sammelprivilegien finden Sie auf Seite 43f.

Eine Änderung eines Sammelprivilegs ändert damit auch immer die Rechte der Kennungen, denen das zu ändernde Sammelprivileg zugewiesen ist. Diese Änderung wird dann wirksam, wenn sie auf dem Home-Pubset gegeben wurde.

Soll in einem Sammelprivileg das Privileg SAT-FILE-MANAGEMENT aufgenommen werden, muss Folgendes beachtet werden:

– Einem der Kennung TSOS zugeordneten Sammelprivileg darf nicht das Privileg SAT-FILE-MANAGEMENT zugewiesen werden.

– Für jede Kennung, die ein Sammelprivileg besitzt, dem das Privileg SAT-FILE-MANAGEMENT zugewiesen ist, wird die SAT-Protokollierung eingeschaltet.

– Jede Kennung, die ein Sammelprivileg besitzt, dem das Privileg SAT-FILE-MANAGEMENT zugewiesen ist, gilt für SAT als nicht schaltbar.

Soll in einem Sammelprivileg das Privileg SAT-FILE-EVALUATION aufgenommen werden, muss Folgendes beachtet werden:

– Für jede Kennung, die ein Sammelprivileg besitzt, dem das Privileg SAT-FILE-EVALUATION zugewiesen ist, wird die SAT-Protokollierung eingeschaltet.

Soll in einem Sammelprivileg das Privileg USER-ADMINISTRATION aufgenommen werden, muss Folgendes beachtet werden:

– Einem Sammelprivileg, das einem Gruppenverwalter zugeordnet ist, darf nicht das Privileg USER-ADMINISTRATION zugewiesen werden.

MODIFY-**PRIVIL**EGE-**SET**

PRIVILEGE-**SET-NAME** = <name 1..8>

,**ADD-PRIVIL**EGE = ***NONE** / list-poss(64): <text>

,**REM**OVE-**PRIVIL**EGE = ***NONE** / list-poss(64): <text>

,**PUBSET** = ***HOME** / <cat-id 1..4>

PRIVILEGE-SET-NAME = <name 1..8>
Name des zu ändernden Sammelprivilegs.

ADD-PRIVILEGE = *NONE / list-poss(64): <text>
Definition, welche Privilegien diesem Sammelprivileg hinzugefügt werden sollen.

ADD-PRIVILEGE = *NONE
Es wird kein Privileg hinzugefügt.

ADD-PRIVILEGE = list-poss(64): <text>
Angabe, welche Privilegien hinzugefügt werden sollen. Mögliche Privilegien siehe Seite 128. Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

REMOVE-PRIVILEGE = *NONE / list-poss(64): <text>
Definition, welche Privilegien aus diesem Sammelprivileg entfernt werden sollen.

REMOVE-PRIVILEGE = *NONE
Es wird kein Privileg entfernt.

REMOVE-PRIVILEGE = list-poss(64): <text>
Angabe, welche Privilegien entfernt werden sollen. Mögliche Privilegien siehe Seite 128.
Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

PUBSET = *HOME / <cat-id 1..4>
Angabe des Pubset, auf dem das Sammelprivileg geändert werden soll.

PUBSET = *HOME
Das Sammelprivileg wird auf dem Home-Pubset geändert.

PUBSET = <cat-id 1..4>
Das Sammelprivileg wird auf dem angegebenen Pubset geändert.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

MODIFY-TERMINAL-SET
Terminal-Set modifizieren

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Modifiziert ein bestehendes Terminal-Set.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Terminal-Sets

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen, für Terminal-Sets der Klasse GROUP oder USER. Die Terminal-Sets müssen der Gruppe des Gruppenverwalters oder ihren Mitgliedern zugeordnet sein.

MODIFY-**TER**MINAL-**SET**

TERMINAL-**SET-NAME** = <name 1..8>(…)

<name 1..8>(…)
SCOPE = ***STD** / ***USER**(…) / ***GR**OUP(…) / ***SYS**TEM
***USER**(…)
USER-IDENTIFICATION = ***OWN** / <name 1..8>
***GR**OUP(…)
GROUP-**ID**ENTIFICATION = ***OWN** / ***UNIV**ERSAL / <name 1..8>

,**PUBSET** = ***HOME** / <catid 1..4>

,**TER**MINAL-**ENTRY** = ***UNCHA**NGED / list-poss(100): ***ADD**(…) / ***REMOVE**(…)

***ADD**(…)
PROCESSOR = ***ANY** / <name 1..8 with-wild(16)>
,**STATION** = ***ANY** / <name 1..8 with-wild(16)>
,**CHECK-MODE** = ***STD** / list-poss(2): ***NET-TER**MINAL-**NAME** / ***APPLI**CATION-**TER**MINAL-**NAME**

***REMOVE**(…)
PROCESSOR = ***ANY** / <name 1..8 with-wild(16)>
,**STATION** = ***ANY** / <name 1..8 with-wild(16)>

,**GUARD-NAME** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>

,**USER-INF**ORMATION = ***UNCHA**NGED / ***NONE** / <c-string 1..80 with-lower>

TERMINAL-SET-NAME = <name 1..8>(…)
Angabe des Terminal-Set-Namens.

SCOPE = *STD
Für systemglobale Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *OWN / <name 1..8>)
Die eigene oder die angegebene Benutzerkennung ist Eigentümer.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *OWN / *UNIVERSAL <name 1..8>)
Die eigene oder die angegebene Benutzergruppe ist Eigentümer.

SCOPE = *SYSTEM
Diesen Wert darf nur ein systemglobaler Benutzerverwalter angeben.

Das Terminal-Set wird dem gemeinschaftlichen Eigentum zugeordnet.

PUBSET =
Pubset, in dessen Benutzerkatalog das Terminal-Set angelegt wird.

PUBSET = *HOME
Das Terminal-Set wird auf dem Home-Pubset angelegt.

PUBSET = <catid 1..4>
Das Terminal-Set wird auf dem angegebenen Pubset angelegt.

TERMINAL-ENTRY =
Gibt an, welche Datensichtstationseinträge hinzugefügt oder gelöscht werden sollen.

TERMINAL-ENTRY = *ADD(…)
Der angegebene Datensichtstationseintrag wird erzeugt.

PROCESSOR = *ANY / <name 1..8 with-wild(16)>
Prozessor- oder Hostname des neuen Datensichtstationseintrags.

STATION = *ANY / <name 1..8 with-wild(16)>
Stations- oder Applikationsname des neuen Datensichtstationseintrags.

CHECK-MODE =
Gibt an, wie der Datensichtstationsname zu prüfen ist.

CHECK-MODE = *STD
Der eingetragene Datensichtstationsname wird bei zwischengeschalteten Applikationen (z.B. OMNIS, CFS) abhängig von deren Vertrauenswürdigkeit geprüft. Ist die Applikation vertrauenswürdig, erfolgt die Prüfung gegen den Namen der Datensichtstation.

CHECK-MODE = *NET-TERMINAL-NAME
Der eingetragene Datensichtstationsname wird gegen den Namen der Datensichtstation geprüft.

CHECK-MODE = *APPLICATION-TERMINAL-NAME
Der eingetragene Datensichtstationsname wird gegen den Namen der Applikation geprüft.

TERMINAL-ENTRY = *REMOVE(…)
Der angegebene Datensichtstationseintrag wird gelöscht.

PROCESSOR = *ANY / <name 1..8 with-wild(16)>
Prozessor- oder Hostname des vorhandenen Datensichtstationseintrags.

STATION = *ANY / <name 1..8 with-wild(16)>
Stations- oder Applikationsname des vorhandenen Datensichtstationseintrags.

GUARD-NAME = *UNCHANGED / *NONE / <filename 1..18 without-cat-gen-vers>
Angabe eines Guards, das den zeitlichen Zugang zu den erfassten Datensichtstationen regelt.

GUARD-NAME = *NONE
Der Zugang erfolgt zeitlich unbeschränkt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Das Terminal-Set wird mit den Zugriffsbedingungen im angegebenen Guard verknüpft.

USER-INFORMATION = *UNCHANGED / *NONE / <c-string 1..80 with-lower>
Benutzerinformation. Hier kann der Benutzer einen Kommentar hinterlegen.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

MODIFY-USER-GROUP
Benutzergruppeneintrag ändern

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Ändert einen Benutzergruppeneintrag im Benutzerkatalog des angegebenen Pubset.

Für einen systemglobalen Benutzerverwalter gibt es keine Einschränkung bezüglich der Gruppenhierarchie; er darf das Kommando zu jeder Zeit für beliebige Gruppen aufrufen.

Für Gruppenverwalter bestehen folgende Einschränkungen in Abhängigkeit von der ADM-AUTHORITY seiner Benutzergruppe:

MANAGE-RESOURCES:	Die hierarchische Zuordnung einer Gruppe (UPPER-GROUP) darf nicht verändert werden. Die Übertragung von Gruppenmitgliedern (ADD-MEMBERS) ist ausgeschlossen.
MANAGE-MEMBERS:	Die hierarchische Zuordnung einer Gruppe (UPPER-GROUP) darf nicht verändert werden.

Eine Besonderheit gilt für die Benutzergruppe *UNIVERSAL:

Da die Potentiale und Rechte der Gruppe *UNIVERSAL nicht beschränkt sind, ist nur die Verwendung der Operanden ADD-GROUP-MEMBERS, GROUP-ADMINISTRATOR, PUBSET und GROUP-IDENTIFICATION sinnvoll und zulässig.

Die Prüfung, ob das Kommando von einem systemglobalen Benutzerverwalter gegeben wird, erfolgt gegen den Home-Pubset der laufenden Sitzung.

Die Prüfung, ob das Kommando von einem Gruppenverwalter gegeben wird, erfolgt gegen den unter dem Operanden PUBSET angegebenen Pubset.

MODIFY-**USER-GR**OUP

GROUP-**ID**ENTIFICATION = ***OWN** / ***UNIV**ERSAL / <name 1..8>

,**PUBSET** = ***HOME** / <cat-id 1..4>

,**UP**PER-**GR**OUP = ***UNCHA**NGED / ***OWN** / ***UNIV**ERSAL / <name 1..8>

,**GR**OUP-**ADM**INISTRATOR = ***UNCHA**NGED / ***NONE** / <name 1..8>

,**ADD-GR**OUP-**MEM**BER = ***NONE** / list-poss(127): <name 1..8>

,**ADM-AUTHORITY** = ***UNCHA**NGED / ***MANAG**E-**RES**OURCES / ***MANAG**E-**MEMB**ERS /
***MANAG**E-**GR**OUPS

,**MAX-GROUP-MEMB**ERS = ***UNCHA**NGED / ***STD** / <integer 0..32767>

,**GR**OUP-**MEM**BER-**PREFIX** = ***UNCHA**NGED / ***ANY** / <name 1..7>

,**MAX-SUB-GR**OUPS = ***UNCHA**NGED / ***STD** / <integer 0..32767>

,**USER-GR**OUP-**PRE**FIX = ***UNCHA**NGED / ***ANY** / <name 1..7>

,**PUB**LIC-**SPACE-LIM**IT = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..2147483647>

,**PUB**LIC-**SPACE-EXC**ESS = ***UNCHA**NGED / ***NO** / ***TEMP**ORARILY-**ALLOW**ED / ***ALLOW**ED

,**FILE-NUM**BER-**LIMIT** = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..16777215>

,**JV-NUM**BER-**LIM**IT = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..16777215>

,**TEMP-SPACE-LIMIT** = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..2147483647>

,**WORK-SPACE-LIM**IT = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..2147483647>

,**DMS-TUNING-RES**OURCES = ***UNCHA**NGED / ***NONE** / ***CONCURRENT-USE** / ***EXCL**USIVE-**USE**

,**TAPE-ACCESS** = ***UNCHA**NGED / ***STD** / ***PRIVIL**EGED / ***READ** / ***BYPASS-LABEL** / ***ALL**

,**F**ILE-**AUD**IT = ***UNCHA**NGED / ***NO** / ***Y**ES

,**CSTMP-MACRO** = ***UNCHA**NGED / ***NO** / ***Y**ES

,**RESID**ENT-**PAGE**S = ***UNCHA**NGED / ***STD** / <integer 0..2147483647> / ***MAX**IMUM

,**ADDR**ESS-**SPACE-LIMIT** = ***UNCHA**NGED / ***STD** / <integer 1..2147483647>

,**TEST-OPT**IONS = ***UNCHA**NGED / ***PAR**AMETERS(...)

***PAR**AMETERS(...)

READ-PRIVILEGE = ***UNCHA**NGED / ***STD** / <integer 1..9>

,**WR**ITE-**PRIVIL**EGE = ***UNCHA**NGED / ***STD** / <integer 1..9>

,**MODIF**ICATION = ***UNCHA**NGED / ***CONTR**OLLED / ***UNCONTR**OLLED

(Teil 1 von 2)

,**ADD-PROF**ILE-**ID** = ***NONE** / list-poss(127): <structured-name 1..30>

,**REM**OVE-**PROF**ILE-**ID** = ***NONE** / ***ALL** / list-poss(127): <structured-name 1..30>

,**MAX-ACC**OUNT-**REC**ORDS = ***UNCHA**NGED / ***STD** / ***NO-LIM**IT / <integer 0..32767>

,**PHYSICAL-ALLOCATION** = ***UNCHA**NGED / ***NOT-ALLOW**ED / ***ALLOW**ED

,**HARD**WARE-**AUDIT** = ***UNCHA**NGED / ***ALLOW**ED / ***NOT-ALLOW**ED

,**LINKAGE-AUDIT** = ***UNCHA**NGED / ***ALLOW**ED / ***NOT-ALLOW**ED

,**CRYPTO-SESSION-LIM**IT = ***UNCHA**NGED / ***STD** / ***MAX**IMUM / <integer 0..32767>

,**NET-STOR**AGE-**USAGE** = ***UNCHA**NGED / ***ALLOW**ED / ***NOT-ALLOW**ED

,**ADD-ACCOUNT** = ***NONE** / list-poss(127): <alphanum-name 1..8>(...)

<alphanum-name 1..8>(...)

CPU-LIMIT = ***MAX**IMUM / <integer 0..2147483647>

,**SP**OOLOUT-**CL**ASS = ***STD** / <integer 1..255>

,**MAX**IMUM-**RUN-PRI**ORITY = ***STD** / <integer 30..255>

,**MAX-ALLOW**ED-**CAT**EGORY = ***STD** / ***TP** / ***SYS**TEM

,**NO-CPU-LIM**IT = ***NO** / ***Y**ES

,**START-IMMED**IATE = ***NO** / ***Y**ES

,**INHIB**IT-**DEACT**IVATION = ***NO** / ***Y**ES

,**MOD**IFY-**ACCOUNT** = ***NONE** / list-poss(127): <alphanum-name 1..8>(...)

<alphanum-name 1..8>(...)

CPU-LIMIT = ***UNCHA**NGED / ***MAX**IMUM / <integer 0..2147483647>

,**SP**OOLOUT-**CL**ASS = ***UNCHA**NGED / ***STD** / <integer 1..255>

,**MAX**IMUM-**RUN-PRI**ORITY = ***UNCHA**NGED / ***STD** / <integer 30..255>

,**MAX-ALLOW**ED-**CAT**EGORY = ***UNCHA**NGED / ***STD** / ***TP** / ***SYS**TEM

,**NO-CPU-LIM**IT = ***UNCHA**NGED / ***NO** / ***Y**ES

,**START-IMMED**IATE = ***UNCHA**NGED / ***NO** / ***Y**ES

,**INHIB**IT-**DEACT**IVATION = ***UNCHA**NGED / ***NO** / ***Y**ES

,**REM**OVE-**ACCOUNT** = ***NONE** / ***ALL** / list-poss(127): <alphanum-name 1..8>

,**BASIC-ACL-ACCESS** = ***UNCHA**NGED / ***BY-GR**OUP-**ONLY** / ***EXTENDED-BY-GUARD** (…)

***EXTENDED-BY-GUARD(...)**

GUARD-NAME = <filename 1..18 without-cat-gen-vers>

(Teil 2 von 2)

GROUP-IDENTIFICATION =
Benutzergruppenkennung, für die ein Eintrag im Benutzerkatalog des unter PUBSET angegebenen Pubset geändert wird.

GROUP-IDENTIFICATION = *OWN
Die Benutzergruppe, zu der der Kommandogeber gehört, wird geändert.

GROUP-IDENTIFICATION = *UNIVERSAL
Dieser Wert ermöglicht es einem systemglobalen Benutzerverwalter, erstmalig einen Gruppenverwalter für die *UNIVERSAL-Gruppe einzusetzen. Dieser hat die Möglichkeit, Gruppen auf der obersten Hierarchiestufe in der Gruppenverwalterrolle zu verwalten.

Bei der Adressierung der Benutzergruppe *UNIVERSAL ist ausschließlich die Angabe der Operanden GROUP-ADMINISTRATOR, PUBSET und ADD-GROUP-MEMBER zulässig. Alle anderen Operanden sind unzulässig und werden nach Warnung SRM5012 ignoriert; das Kommando wird ausgeführt.

GROUP-IDENTIFICATION = <name 1..8>
Benutzergruppenkennung, die geändert wird. Ist der Kommandogeber Gruppenverwalter, ist sein Recht zur Änderung von Benutzergruppen auf die hierarchisch unter seiner Gruppe liegende Gruppenhierarchie beschränkt. Ist der Kommandogeber mit dem Recht „systemglobale Benutzerverwaltung“ ausgestattet, darf er beliebige Benutzergruppeneinträge ändern.

PUBSET =
Pubset, in dessen Benutzerkatalog ein Benutzergruppeneintrag geändert werden soll.

PUBSET = *HOME
Der Benutzergruppeneintrag wird im Benutzerkatalog des Home-Pubset geändert (bezogen auf den aktuellen Systemlauf).

PUBSET = <cat-id 1..4>
Katalogkennung des Pubset, auf dem ein Benutzergruppeneintrag geändert werden soll. Ist das Pubset auf dem lokalen System nicht aktiv, wird das Kommando abgewiesen.

UPPER-GROUP = *UNCHANGED / *OWN / *UNIVERSAL / <name 1..8>
Benutzergruppe, die der Benutzergruppe in der Gruppenhierarchie neu übergeordnet ist (Umhängen einer Benutzergruppe). Folgende Fälle sind zu unterscheiden:

– Wenn der Kommandoausführende ein Gruppenverwalter ist, darf die übergeordnete Gruppe nur eine Gruppe aus der Teilhierarchie sein, zu deren Verwaltung er berechtigt ist (Voraussetzung ist ADM-AUTHORITY=*MANAGE-GROUPS).

– Wenn der Kommandoausführende ein systemglobaler Benutzerverwalter ist, darf er auf alle Gruppen im Gruppenbaum zugreifen und diese strukturieren.

UPPER-GROUP = *OWN
Die Benutzergruppe desjenigen Gruppenverwalters, der das Kommando /MODIFY-USER-GROUP ausführt, wird zur übergeordneten Benutzergruppe. Auch wenn der Kommandoausführende ein systemglobaler Benutzerverwalter ist, ist die übergeordnete Gruppe nicht standardmäßig die *UNIVERSAL-Gruppe, sondern diejenige Benutzergruppe, der er zugeordnet ist.

UPPER-GROUP = *UNIVERSAL
Gibt einem systemglobalen Benutzerverwalter bzw. dem Gruppenverwalter von *UNIVERSAL die Möglichkeit, eine Benutzergruppe auf die oberste Ebene der Gruppenhierachie zu heben. Bei einem anderen Kommandogeber wird das Kommando abgewiesen.

UPPER-GROUP = <name 1..8>
Die angegebene Benutzergruppe wird zur übergeordneten Benutzergruppe. Diese Gruppe muss bereits auf dem jeweiligen Pubset eingerichtet sein.

GROUP-ADMINISTRATOR = *UNCHANGED / *NONE / <name 1..8>
Benutzerkennung, die für die Verwaltung dieser Benutzergruppe verantwortlich sein soll (Gruppenverwalter). Nur eine bereits der jeweiligen Benutzergruppe angehörige Benutzerkennung kann explizit als Gruppenverwalter vereinbart werden. Diese Bedingung gilt als erfüllt, wenn die Benutzerkennung im Kommando MODIFY-USER-GROUP unter dem Operanden ADD-GROUP-MEMBER genannt ist.

Das Kommando wird abgewiesen, wenn die angegebene Benutzerkennung bereits Gruppenverwalter einer anderen Benutzergruppe ist (dies wird nur innerhalb des unter PUBSET genannten Pubset überprüft). Soll diese Benutzerkennung unbedingt neuer Verwalter der Benutzergruppe werden, muss vorher seiner bisherigen Gruppe ein neuer Verwalter zugewiesen werden (oder *NONE).

Besitzt die als Gruppenverwalter vorgesehene Benutzerkennung das Privileg USER-ADMINISTRATION oder das Privileg SECURITY-ADMINISTRATION, wird das Kommando abgewiesen, da die Ämterhäufung ’Gruppenverwalter + Privileg USER-ADMINISTRATION’ oder ’Gruppenverwalter + SECURITY-ADMINISTRATION’ unzulässig ist. Eine Ämterhäufung wird sowohl gegen den Home-Pubset der laufenden Sitzung als auch gegen den unter dem Operanden PUBSET angegebenen Pubset geprüft.

Sollte dennoch die inkonsistente Form der Ämterhäufung entstanden sein, wird eine Warnung ausgegeben. Das Privileg USER-ADMINISTRATION wird bei der Kommandoverarbeitung vorrangig behandelt.

GROUP-ADMINISTRATOR = *NONE
Der Benutzergruppe wird kein eigener Gruppenverwalter zugeordnet. In diesem Fall wird diese Benutzergruppe verwaltet durch den Gruppenverwalter einer hierarchisch höherstehenden Benutzergruppe oder durch einen systemglobalen Benutzerverwalter.

War vor Wirkung des Kommandos /MODIFY-USER-GROUP ein Gruppenverwalter zugeordnet, wird dessen Benutzerkennung auf den Status eines „normalen“ Gruppenmitgliedes zurückgestuft.

GROUP-ADMINISTRATOR = <name 1..8>
Benutzerkennung des neu zuzuordnenden Gruppenverwalters. Die Benutzerkennung muss vor der Zuordnung als Gruppenverwalter mit einem Kommando /ADD-USER für das jeweilige Pubset angelegt worden sein. War vor Wirkung des Kommandos /MODIFY-USER-GROUP ein Gruppenverwalter zugeordnet, wird dessen Benutzerkennung auf den Status eines „normalen“ Gruppenmitgliedes zurückgestuft.

War die angebene Benutzerkennung bereits vorher der Gruppenverwalter der angegebenen Benutzergruppe, wird der Operand ignoriert und der Rest des Kommandos verarbeitet.

ADD-GROUP-MEMBER =
Die angegebenen Benutzerkennungen werden der aktuellen Benutzergruppe hinzugefügt. Eine bestehende Zuordnung zu einer anderen Benutzergruppe wird damit aufgehoben. Die Benutzerkennungen müssen innerhalb der Gruppenhierarchie liegen, zu deren Verwaltung der Kommandogeber berechtigt ist. Dies gilt für Gruppenverwalter, deren Benutzergruppe mindestens ADM-AUTHORITY = *MANAGE-MEMBERS besitzt. In der Liste dürfen keine Gruppenverwalter anderer Gruppen enthalten sein.

Die POSIX-Gruppennummer der transferierten Benutzerkennung wird auf den Wert der Standard-Gruppennummer gesetzt (vgl. Kommando /MODIFY-POSIX-USER-DEFAULTS im Handbuch „Kommandos“ [4]).

ADD-GROUP-MEMBER = *NONE
Die bestehenden Zuordnungen bleiben erhalten.

ADD-GROUP-MEMBER = <name 1..8>
Die angegebenen Benutzerkennungen werden aus ihren bisherigen Gruppenzuordnungen gelöst und der aktuellen Benutzergruppe zugeordnet. Sollen mehr als 127 Benutzerkennungen zugeordnet werden, geschieht das durch eine Folge von /MODIFY-USER-GROUP-Kommandos. Die Benutzerkennungen, müssen innerhalb der Gruppenhierarchie liegen, zu deren Verwaltung der Kommandogeber berechtigt ist.

ADM-AUTHORITY =
Vereinbart die Rechte des Gruppenverwalters.

ADM-AUTHORITY = *MANAGE-RESOURCES
Der Gruppenverwalter ist berechtigt, Betriebsmittel und Rechte der Benutzerkennungen, die zu seiner Gruppe gehören bzw. in der Gruppenhierarchie tiefer stehen, zu verwalten. Er hat kein Recht, Benutzerkennungen anzulegen, zu löschen und von einer Benutzergruppe zur anderen zu übertragen. Der Gruppenverwalter ist berechtigt, Betriebsmittel und Rechte seiner Benutzergruppe, bzw. der Benutzergruppen, die hierarchisch unter seiner Benutzergruppe liegen, zu verwalten. Er hat kein Recht, die Organisation (Hierarchie) der Benutzergruppen zu ändern, d.h. er kann Benutzergruppen weder anlegen, noch übertragen oder löschen.

ADM-AUTHORITY = *MANAGE-MEMBERS
Der Gruppenverwalter ist berechtigt, Benutzerkennungen innerhalb seiner oder einer untergeordneten Benutzergruppe neu anzulegen, zu löschen oder zu deaktivieren (LOCK-USER und UNLOCK-USER) und zwischen Benutzergruppen zu übertragen. Die MANAGE-MEMBERS-Berechtigung beinhaltet automatisch die MANAGE-RESOURCES-Berechtigung.

ADM-AUTHORITY = *MANAGE-GROUPS
Der Gruppenverwalter ist berechtigt, die Organisation der hierarchisch unter seiner Benutzergruppe liegenden Gruppen durch Neuanlage, Löschen und Übertragen von Benutzergruppen zu verändern. Die MANAGE-GROUPS-Berechtigung beinhaltet automatisch die MANAGE-MEMBERS-Berechtigung.

MAX-GROUP-MEMBERS = *UNCHANGED / *STD / <integer 0..32767>
Maximale Anzahl von Benutzerkennungen, die der Gruppenverwalter dieser Benutzergruppe zuweisen darf. Diese Begrenzung gilt für die Summe der Benutzerkennungen der aktuellen Benutzergruppe und der ihr hierarchisch unterzuordnenden Benutzergruppen. Sie gilt nicht für den systemglobalen Benutzerverwalter - dieser darf die angegebene Anzahl auch überschreiten.

MAX-GROUP-MEMBERS = *STD
Der Benutzergruppe dürfen keine Benutzerkennungen zugewiesen werden.

MAX-GROUP-MEMBERS = <integer 0..32767>
Maximale Anzahl der Benutzerkennungen, die dieser Benutzergruppe zugewiesen werden können.

GROUP-MEMBER-PREFIX =
Legt fest, mit welchem Präfix die Namen von Gruppenmitgliedern (Benutzerkennungen) beginnen müssen. Dieser oder jeder andere Präfix, der eine Untermenge dieses Präfix bildet, kann von Gruppenverwaltern, deren Benutzergruppe die ADM-AUTHORITY MANAGE-GROUPS besitzt, an Gruppenmitglieder vergeben werden. (SECOS ist z.B. eine Untermenge zum Präfix SEC.)

GROUP-MEMBER-PREFIX = *ANY
Jeder Präfix ist erlaubt.

GROUP-MEMBER-PREFIX = <name 1..7>
Vorgegebener Name für Gruppenmitgliedernamen.

MAX-SUB-GROUPS = *UNCHANGED / *STD / <integer 0..32767>
Maximale Anzahl an Benutzergruppen, die einer Benutzergruppe untergeordnet werden können (Untergruppen). Diese Begrenzung umfasst die Summe der Benutzergruppen der unter der aktuellen Benutzergruppe aufzubauenden Hierarchie von Untergruppen.

MAX-SUB-GROUPS = *STD
Der Benutzergruppe dürfen keine Untergruppen zugewiesen werden.

MAX-SUB-GROUPS = <integer 0..32767>
Maximale Anzahl der Untergruppen, die dieser Benutzergruppe zugewiesen werden können.

USER-GROUP-PREFIX =
Legt fest, mit welchem Präfix die Namen der Untergruppen beginnen müssen. Dieser oder jeder andere Präfix, der eine Untermenge dieses Präfix bildet, kann von Gruppenverwaltern, deren Benutzergruppe die ADM-AUTHORITY MANAGE-MEMBERS besitzt, an Untergruppen vergeben werden. (SRPM ist z.B. eine Untermenge zum Präfix SRP.)

USER-GROUP-PREFIX = *ANY
Jedes Präfix ist erlaubt.

USER-GROUP-PREFIX = <name 1..7>
Es kann nur der angegebene Name für Untergruppen verwendet werden.

PUBLIC-SPACE-LIMIT = *UNCHANGED / *MAXIMUM / <integer 0..2147483647>
Legt den maximalen Speicherplatz fest, den ein Gruppenverwalter an Gruppenmitglieder und Untergruppen für ihre Dateien auf gemeinschaftlichen Datenträgern des beim Operanden PUBSET zugewiesenen Pubset zuweisen darf .

PUBLIC-SPACE-LIMIT = *MAXIMUM
Der Gruppenverwalter darf die volle Kapazität von 2.147.483.647 PAM-Seiten zuweisen.

PUBLIC-SPACE-LIMIT = <integer 0..2147483647>
Anzahl der PAM-Blöcke, die als Obergrenze festgelegt werden.

PUBLIC-SPACE-EXCESS = *UNCHANGED / *NO / *TEMPORARILY-ALLOWED / *ALLOWED
Ändert die Berechtigung des Gruppenverwalters zur weiteren Verwaltung des Rechtes, den im Operanden PUBLIC-SPACE-LIMIT zugewiesenen Wert zu überschreiten (bezüglich Mitgliedern oder Untergruppen).

PUBLIC-SPACE-EXCESS = *NO
Die Berechtigung darf nicht weiterverwaltet werden.

PUBLIC-SPACE-EXCESS = *TEMPORARILY-ALLOWED
Die Speicherplatzgrenze darf überschritten werden, sofern die Obergrenze zum Zeitpunkt des LOGON noch nicht erreicht war.

PUBLIC-SPACE-EXCESS = *ALLOWED
Die Berechtigung darf für Gruppenmitglieder und Untergruppen verwaltet werden.

FILE-NUMBER-LIMIT =
Vereinbart die maximale Anzahl von Dateien, die angelegt werden dürfen. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

FILE-NUMBER-LIMIT = *MAXIMUM
Die maximale Anzahl von Dateien ist 16.777.215.

FILE-NUMBER-LIMIT = <integer 0..16777215>
Angabe der genauen Anzahl der maximal möglichen Katalogeinträge.

JV-NUMBER-LIMIT =
Vereinbart die maximale Anzahl von Job-Variablen, die angelegt werden dürfen. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

JV-NUMBER-LIMIT = *MAXIMUM
Die maximale Anzahl von Job-Variablen ist 16.777.215.

JV-NUMBER-LIMIT = <integer 0..16777215>
Angabe der genauen Anzahl der maximal möglichen Job-Variablen.

TEMP-SPACE-LIMIT =
Vereinbart den maximalen temporären Speicherplatz, der auf dem Im Operanden PUBSET angegebenen, gemeinschaftlichen Datenträger belegt werden darf. Diese Obergrenze oder ein geringerer Wert darf an Untergruppen oder Gruppenmitglieder weitergegeben werden.

TEMP-SPACE-LIMIT = *MAXIMUM
Das maximale Gruppenpotential ist 2.147.483.647.

TEMP-SPACE-LIMIT = <integer 0..2147483647>
Angabe des genauen Gruppenpotentials.

WORK-SPACE-LIMIT = *MAXIMUM / <integer 0..2147483647>
Legt die Obergrenze für den Wert fest, den ein Gruppenverwalter als WORK-SPACE-LIMIT für seine Untergruppe bzw. seine Gruppenmitglieder für einen Pubset vergeben darf. Die Angabe dieses Operanden ist nur für einen SM-Pubset sinnvoll.

WORK-SPACE-LIMIT = *MAXIMUM
Die Obergrenze für den Wert, den ein Gruppenverwalter als WORK-SPACE-LIMIT angeben darf, soll auf 2147483647 festgelegt werden.

DMS-TUNING-RESOURCES =
Vereinbart, welche Performance-Maßnahmen ergriffen und in welcher Form sie genutzt werden dürfen. Diese Berechtigung oder eine geringere darf an Untergruppen oder Gruppenmitglieder weitergegeben werden. Die Auswirkungen der verschiedenen Performance-Maßnahmen sind im Kommando ADD-USER-GROUP beschrieben (siehe „Zugelassene Performance-Maßnahmen für Home- und Daten-Pubset“ auf Seite 140) .

DMS-TUNING-RESOURCES = *NONE
Es dürfen keine Performance-Maßnahmen angewendet werden.

DMS-TUNING-RESOURCES = *CONCURRENT-USE
Der Benutzer darf bevorzugte Ressourcen reservieren, steht dabei aber in Konkurrenz zu allen anderen Benutzer mit der gleichen Berechtigung.

DMS-TUNING-RESOURCES = *EXCLUSIVE-USE
Der Benutzer darf bevorzugte Ressourcen exklusiv reservieren.

TAPE-ACCESS =
Regelt die Verwaltungsrechte des Gruppenverwalters bezüglich der TAPE-ACCESS-Berechtigung (siehe Kommando /ADD-USER und /MODIFY-USER-ATTRIBUTES).

TAPE-ACCESS = *STD
Fehlermeldungen dürfen nicht ignoriert werden.

TAPE-ACCESS = *PRIVILEGED
Fehlermeldungen bei Ausgabedateien dürfen ignoriert werden.

TAPE-ACCESS = *READ
Fehlermeldungen bei Eingabedateien dürfen ignoriert werden.

TAPE-ACCESS = *BYPASS-LABEL
Abschaltung der Kennsatzprüfung bei Bändern, die im INPUT- oder REVERSE-Modus verarbeitet werden (umfasst TAPE-ACCESS=*READ).

TAPE-ACCESS = *ALL
Alle Fehlermeldungen dürfen ignoriert werden (umfasst TAPE-ACCESS=*READ, TAPE-ACCESS=*PRIVILEGED und TAPE-ACCESS=*BYPASS-LABEL). Gibt der Gruppenverwalter ein Kommando für ein Gruppenmitglied, wobei er den Operanden TAPE-ACCESS mit einem bestimmten Wert besetzt, so gilt folgende Regel:

Wert im Kommando **Wert im Gruppenpotential**	**STD**	**PRIV**	**READ**	**BLP**	**ALL**
STD	YES	NO	NO	NO	NO
PRIV	YES	YES	NO	NO	NO
READ	YES	NO	YES	NO	NO
BLP	YES	NO	YES	YES	NO
ALL	YES	YES	YES	YES	YES

YES = akzeptiert, NO=nicht akzeptiert

FILE-AUDIT = *UNCHANGED / *NO / *YES
Vereinbart, ob das Recht, den AUDIT-Modus einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

FILE-AUDIT = *NO
Die Berechtigung darf nicht weitergegeben werden.

FILE-AUDIT = *YES
Die Berechtigung darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

CSTMP-MACRO = *UNCHANGED / *NO / *YES
Regelt die Verwaltungsrechte des Gruppenverwalters bezüglich der CSTMP-MACRO-Berechtigung (siehe Kommando /ADD-USER und /MODIFY-USER-ATTRIBUTES).

CSTMP-MACRO = *NO
Die Berechtigung kann nicht an Gruppenmitglieder oder Untergruppen weitergegeben werden.

CSTMP-MACRO = *YES
Die Berechtigung kann an Gruppenmitglieder und Untergruppen weitergegeben werden.

RESIDENT-PAGES = *UNCHANGED / *STD / *MAXIMUM / <integer 0..2147483647>
Regelt die Berechtigung, residente Teile des Arbeitsspeichers zu verwenden. Gegen diesen Maximal-Wert (und zusätzlich gegen den im MODIFY-SYSTEM-BIAS gesetzten Wert) wird der Operand RESIDENT-PAGES=*PARAMETERS (MINIMUM=<integer 0..2147483647>) der Kommandos LOAD-/START-EXECUTABLE-PROGRAM (bzw. LOAD-/START-PROGRAM) geprüft. Der Maximalwert oder ein kleinerer kann an Gruppenmitglieder oder Untergruppen weitergereicht werden.

RESIDENT-PAGES = *STD
Der Benutzer darf 32767 residente Hauptspeicherseiten in Anspruch nehmen.

RESIDENT-PAGES = *MAXIMUM
Die Obergrenze wird auf 2.147.483.647 residente Hauptspeicherseiten festgelegt.

RESIDENT-PAGES = <integer 0..2147483647>
Die Obergrenze wird auf die angegebenen residenten Hauptspeicherseiten festgelegt.

ADDRESS-SPACE-LIMIT = *UNCHANGED / *STD / <integer 1..2147483647>
Vereinbart den maximal verfügbaren Benutzeradressraum (Einheit: Megabyte). Diese Obergrenze oder ein geringerer Wert kann an Gruppenmitglieder oder Untergruppen vergeben werden.

ADDRESS-SPACE-LIMIT = *STD
Der Wert des Systemparameters SYSGJASL wird zugewiesen (der Systemparameter SYSGJASL hat den Standardwert 16 MByte, siehe Kommando SHOW-SYSTEM-PARAMETERS im Handbuch „Kommandos“ [4]).

ADDRESS-SPACE-LIMIT = <integer 1..2147483647>
Ein Wert zwischen 1 und 2.147.483.647 Megabyte wird zugewiesen.

TEST-OPTIONS = *UNCHANGED / *PARAMETERS(...)
Legt das Gruppenprivileg bezüglich Vergabe der Testprivilegierung fest.

TEST-OPTIONS = *PARAMETERS(...)
Die vergebenen Werte regeln die Rechte des Gruppenverwalters bei der Verwaltung der Mitglieder seiner Benutzergruppe bzw. der Gruppenstruktur.

READ-PRIVILEGE = *UNCHANGED / *STD / <integer 1..9>
Maximale Leseprivilegierung.

READ-PRIVILEGE = *STD
Das maximale Leseprivileg nimmt den Wert 1 an.

READ-PRIVILEGE = <integer 1..9>
Wert des maximalen Leseprivilegs.

WRITE-PRIVILEGE = *UNCHANGED / *STD / <integer 1..9>
Maximale Schreibprivilegierung.

WRITE-PRIVILEGE = *STD
Das maximale Schreibprivileg nimmt den Wert 1 an.

WRITE-PRIVILEGE = <integer 1..9>
Wert des maximalen Schreibprivilegs.

MODIFICATION = *UNCHANGED / *CONTROLLED / *UNCONTROLLED
Ändert das Recht des Gruppenverwalters, das MODIFICATION-Recht festzusetzen.

MODIFICATION = *CONTROLLED
Der Gruppenverwalter hat nur das Recht, das MODIFICATION-Recht CONTROLLED an Gruppenmitglieder bzw. Untergruppen weiterzureichen. Er ist nicht berechtigt, das MODIFICATION-Recht auf UNCONTROLLED zu ändern.

MODIFICATION = *UNCONTROLLED
Der Gruppenverwalter hat das Recht, das MODIFICATION-Recht CONTROLLED oder UNCONTROLLED an Gruppenmitglieder bzw. Untergruppen weiterzugeben.

ADD-PROFILE-ID =
Fügt dem Gruppenpotential an SDF-Profile-Ids, die der Gruppenverwalter Gruppenmitgliedern und Untergruppen zuordnen kann, eine oder mehrere hinzu. Es gibt keine Wechselwirkung zum Operanden REMOVE-PROFILE-ID: Wird sowohl bei ADD-PROFILE-ID wie auch bei REMOVE-PROFILE-ID ein identischer Wert angegeben, wird das Kommando abgewiesen (REMOVE-PROFILE-ID=*ALL wirkt wie die Eingabe einer Liste aller gespeicherten Profile-Ids).

ADD-PROFILE-ID = *NONE
Die bestehende Festlegung bleibt erhalten.

ADD-PROFILE-ID = list-poss(127): <structured-name 1..30>
Profile-Ids der Gruppensyntaxdateien, die dem Gruppenpotential zusätzlich zugeordnet werden.

REMOVE-PROFILE-ID =
Löscht eine, mehrere oder alle Profile-Ids von SDF-Syntax-Dateien, die der Gruppenverwalter Gruppenmitgliedern und Untergruppen zuordnen kann, aus dem Gruppenpotential. Es gibt keine Wechselwirkung zum Operanden ADD-PROFILE-ID: Wird sowohl bei ADD-PROFILE-ID wie auch bei REMOVE-PROFILE-ID ein identischer Wert angegeben, wird das Kommando abgewiesen.

REMOVE-PROFILE-ID = *NONE
Die bestehende Festlegung bleibt erhalten.

REMOVE-PROFILE-ID = *ALL
Alle Einträge werden gelöscht. Ist einer der bisher gespeicherten Namen gleich einem Namen bei ADD-PROFILE-ID wird das Kommando abgewiesen.

REMOVE-PROFILE-ID = list-poss(127): <structured-name 1..30>
Profile-Ids der Gruppensyntaxdateien, die aus dem Gruppenpotential gelöscht werden.

MAX-ACCOUNT-RECORDS = *UNCHANGED / *STD / *NO-LIMIT / <integer 0..32767>
Legt das Gruppenrecht bezüglich Vergabe der Rechte zum Sammeln benutzerspezifischer Abrechnungssätze fest. Die vergebenen Werte regeln die Rechte des Gruppenverwalters bei der Administration der Mitglieder seiner Benutzergruppe bzw. der Gruppenstruktur.

MAX-ACCOUNT-RECORDS = *STD
Der Benutzer darf pro Auftrag bzw. Programm bis zu 100 benutzerspezifische Abrechnungssätze in die Abrechnungsdatei schreiben. Eigene Abrechnungssätze (mit eigener Satzkennung) darf er nicht schreiben.

MAX-ACCOUNT-RECORDS = *NO-LIMIT
Der Benutzer darf pro Auftrag bzw. Programm unbegrenzt benutzerspezifische Abrechnungssätze und eigene Abrechnungssätze (mit eigener Satzkennung) in die Abrechnungsdatei schreiben.

MAX-ACCOUNT-RECORDS = <integer 0..32767>
Der Benutzer darf pro Auftrag bzw. Programm bis zur festgelegten Grenze benutzerspezifische Abrechnungssätze in die Abrechnungsdatei schreiben. Eigene Abrechnungssätze (mit eigener Satzkennung) darf er nicht schreiben.

PHYSICAL-ALLOCATION = *UNCHANGED / *NOT-ALLOWED / *ALLOWED
Legt fest, ob der Gruppenverwalter das Recht, auf dem Pubset die absolute Speicherplatz-Zuweisung (Direktallokierung) zu nutzen, an Gruppenmitglieder oder Untergruppen vergeben darf.

HARDWARE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, den Sprungfolgemodus (Hardware-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

LINKAGE-AUDIT = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, die Unterprogrammverfolgung (Linkage-Audit-Modus) einzuschalten, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

CRYPTO-SESSION-LIMIT = *UNCHANGED / *STD / *MAXIMUM / <integer 0..32767>
Vereinbart die maximale Anzahl openCRYPT-Sessions innerhalb einer BS2000-Session, die vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

NET-STORAGE-USAGE = *UNCHANGED / *ALLOWED / *NOT-ALLOWED
Vereinbart, ob das Recht, Speicherplatz auf einem Net-Storage-Volume zu belegen, vom Gruppenverwalter an Benutzergruppenmitglieder bzw. Untergruppen vergeben werden darf.

ADD-ACCOUNT =
Die folgenden Angaben beziehen sich auf eine Abrechnungsnummer, die dem Gruppenpotential zusätzlich zugeordnet wird.

ADD-ACCOUNT = *NONE
Die bestehenden Festlegungen bleiben erhalten.

ADD-ACCOUNT = list-poss(127): <alphanum-name 1..8>(...)
Neue Abrechnungsnummer für die Benutzergruppenkennung. Ist eine der Abrechnungsnummern zusätzlich in den Operanden MOD-ACCOUNT oder REMOVE-ACCOUNT angegeben, wird das Kommando abgewiesen (REMOVE-ACCOUNT=*ALL wirkt wie die Eingabe einer Liste aller bisher gespeicherten Abrechnungsnummern).

CPU-LIMIT =
Legt das Gruppenpotential an CPU-Sekunden fest, das an Gruppenmitglieder und Untergruppen weitergegeben werden kann. Dieses aufgeteilte Gruppenpotential steht den Gruppenmitgliedern zur Auftragsausführung unter der Abrechnungsnummer zur Verfügung.

CPU-LIMIT = *MAXIMUM
Das Gruppenpotential beläuft sich auf 2.147.483.647 CPU-Sekunden.

CPU-LIMIT = <integer 0..2147483647>
Anzahl CPU-Sekunden, die dem Gruppenpotential zugewiesen werden (Maximalwert für jede Gruppenkennung).

SPOOLOUT-CLASS =
Legt die höchstmögliche SPOOLOUT-Klasse fest, die an Gruppenmitglieder oder Benutzergruppen weitergegeben werden kann. Bei der Bewertung der Zulässigkeit wird – um eine Rangfolge zu erreichen – STD (=0) bzw. 1 als die höchstmögliche Klasse angesehen und 255 als die niedrigstmögliche.

SPOOLOUT-CLASS = *STD
Die maximale SPOOLOUT-Klasse ist mit dem Wert 0 vorbesetzt.

SPOOLOUT-CLASS = <integer 1..255>
Wert der maximalen SPOOLOUT-Klasse.

MAXIMUM-RUN-PRIORITY =
Legt die maximale RUN-Priorität als Gruppenpotential fest, die an Gruppenmitglieder oder Untergruppen weitergegeben werden kann.

MAXIMUM-RUN-PRIORITY = *STD
Standardwert aus dem Systemparameter SYSGJPRI.

MAXIMUM-RUN-PRIORITY = <integer 30..255>
Maximale RUN-Priorität.

MAX-ALLOWED-CATEGORY =
Legt fest, mit welchen Task-Attributen der Benutzer arbeiten darf. Ein Recht, das andere Rechte umfasst (SYSTEM umfasst STD und TP, TP umfasst STD), kann für Gruppenmitglieder bzw. Untergruppen eingeschränkt werden.

MAX-ALLOWED-CATEGORY = *STD
Tasks unter der angegebenen Abrechnungsnummer dürfen weder mit dem Task-Attribut TP noch SYS arbeiten.

MAX-ALLOWED-CATEGORY = *TP
Tasks unter der angegebenen Abrechnungsnummer dürfen das privilegierte Task-Attribut TP verwenden.

MAX-ALLOWED-CATEGORY = *SYSTEM
Tasks unter der angegebenen Abrechnungsnummer dürfen die Task-Attribute TP und SYS verwenden.

NO-CPU-LIMIT =
Legt die Berechtigung des Gruppenverwalters fest, das NO-CPU-LIMIT-Recht an Gruppenmitglieder bzw. Untergruppen weiterzugeben.

NO-CPU-LIMIT = *NO
Das Recht kann nicht weitergegeben werden.

NO-CPU-LIMIT = *YES
Das Recht kann an Gruppenmitglieder und Untergruppen weitergegeben werden.

START-IMMEDIATE =
Legt die Rechte des Gruppenverwalters bezüglich der Job-Express-Funktion fest.

START-IMMEDIATE = *NO
Die Express-Berechtigung kann weder an Gruppenmitglieder noch an Untergruppen weitergegeben werden.

START-IMMEDIATE = *YES
Die Express-Berechtigung darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

INHIBIT-DEACTIVATION =
Regelt die Berechtigung des Gruppenverwalters, Gruppenmitgliedern oder Untergruppen das Recht des Deaktivierungsverbotes für Aufträge unter dieser Abrechnungsnummer weiterzugeben.

INHIBIT-DEACTIVATION = *NO
Das Recht darf nicht weitergegeben werden.

INHIBIT-DEACTIVATION = *YES
Das Recht darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

MODIFY-ACCOUNT =
Die folgenden Angaben beziehen sich auf eine Abrechnungsnummer, die geändert wird. Ist eine der Abrechnungsnummern zusätzlich in den Operanden ADD-ACCOUNT oder REMOVE-ACCOUNT angegeben, wird das Kommando abgewiesen.

MODIFY-ACCOUNT = *NONE
Die bestehenden Festlegungen bleiben erhalten.

MODIFY-ACCOUNT = <list-poss(127): alphanum-name 1..8>(...)
Zu ändernde Abrechnungsnummer.

CPU-LIMIT = *UNCHANGED / *MAXIMUM / <integer 0..2147483647>
Legt das Gruppenpotential an CPU-Sekunden fest, das an Gruppenmitglieder und Untergruppen weitergegeben werden kann.

CPU-LIMIT = *MAXIMUM
Das Gruppenpotential beläuft sich auf 2.147.483.647 CPU-Sekunden.

CPU-LIMIT = <integer 1..2147483647>
Anzahl CPU-Sekunden, die dem Gruppenpotential zugewiesen werden.

SPOOLOUT-CLASS = *UNCHANGED / *STD / <integer 1..255>
Legt die höchstmögliche SPOOLOUT-Klasse fest, die an Gruppenmitglieder oder Benutzergruppen weitergegeben werden kann.

SPOOLOUT-CLASS = *STD
Die maximale SPOOLOUT-Klasse ist mit dem Wert 0 vorbesetzt.

SPOOLOUT-CLASS = <integer 1..255>
Wert der maximalen SPOOLOUT-Klasse.

MAXIMUM-RUN-PRIORITY = *UNCHANGED / *STD / <integer 30..255>
Legt die maximale RUN-Priorität als Gruppenpotential fest, die an Gruppenmitglieder oder Untergruppen weitergegeben werden kann.

MAXIMUM-RUN-PRIORITY = *STD
Standardwert aus dem Systemparameter SYSGJPRI.

MAXIMUM-RUN-PRIORITY = <integer 30..255>
Maximale RUN-Priorität.

MAX-ALLOWED-CATEGORY = *UNCHANGED / *STD / *TP / *SYSTEM
Legt fest, mit welchen Task-Attributen der Benutzer arbeiten darf. Ein Recht, das andere Rechte umfasst (SYSTEM umfasst STD und TP, TP umfasst STD), kann für Gruppenmitglieder bzw. Untergruppen eingeschränkt werden.

MAX-ALLOWED-CATEGORY = *STD
Tasks unter der angegebenen Abrechnungsnummer dürfen nicht mit dem Task-Attribut TP arbeiten.

MAX-ALLOWED-CATEGORY = *TP
Tasks unter der angegebenen Abrechnungsnummer dürfen das Task-Attribut TP verwenden.

MAX-ALLOWED-CATEGORY = *SYSTEM
Tasks unter der angegebenen Abrechnungsnummer dürfen die Task-Attribute TP und SYS verwenden.

NO-CPU-LIMIT = *UNCHANGED / *NO / *YES
Legt die Berechtigung des Gruppenverwalters fest, das NO-CPU-LIMIT-Recht an Gruppenmitglieder bzw. Untergruppen weiterzugeben.

NO-CPU-LIMIT = *NO
Das Recht kann nicht weitergegeben werden.

NO-CPU-LIMIT = *YES
Das Recht kann an Gruppenmitglieder und Untergruppen weitergegeben werden.

START-IMMEDIATE = *UNCHANGED / *NO / *YES
Legt die Rechte des Gruppenverwalters bezüglich der Job-Express-Funktion fest.

START-IMMEDIATE = *NO
Die Express-Berechtigung kann weder an Gruppenmitglieder noch an Untergruppen weitergegeben werden.

START-IMMEDIATE = *YES
Die Express-Berechtigung darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

INHIBIT-DEACTIVATION = *UNCHANGED / *NO / *YES
Regelt die Berechtigung des Gruppenverwalters, Gruppenmitgliedern oder Untergruppen das Recht des Deaktivierungsverbotes für Aufträge unter dieser Abrechnungsnummer weiterzugeben.

INHIBIT-DEACTIVATION = *NO
Das Recht darf nicht weitergegeben werden.

INHIBIT-DEACTIVATION = *YES
Das Recht darf an Gruppenmitglieder und Untergruppen weitergegeben werden.

REMOVE-ACCOUNT =
Gibt an, welche Abrechnungsnummern aus dem Gruppenpotential gelöscht werden sollen.

REMOVE-ACCOUNT = *NONE
Die bestehenden Festlegungen bleiben erhalten.

REMOVE-ACCOUNT = *ALL
Alle Einträge werden gelöscht. Ist einer der bisher gespeicherten Namen gleich einem Namen in der ADD-ACCOUNT- oder MOD-ACCOUNT-Liste, wird das Kommando abgewiesen.

REMOVE-ACCOUNT = list-poss(127): <alphanum-name 1..8>
Zu löschende Abrechnungsnummer. Ist eine der Abrechnungsnummern zusätzlich in den Operanden ADD-ACCOUNT oder MOD-ACCOUNT angegeben, wird das Kommando abgewiesen.

BASIC-ACL-ACCESS = *UNCHANGED / *BY-GROUP-ONLY / *EXTENDED-BY-GUARD(...)
Regelt den Gruppenzugriff für Dateien und Jobvariablen, die mit BACL geschützt sind.

BASIC-ACL-ACCESS = *BY-GROUP-ONLY
Beim Zugriff auf Dateien und Jobvariablen, die durch BACL geschützt sind, ist nur die tatsächliche Gruppenmitgliedschaft von Bedeutung.

BASIC-ACL-ACCESS = *EXTENDED-BY-GUARD(…)
Beim Zugriff auf Dateien und Jobvariablen, die durch BACL geschützt sind, werden bestimmte Benutzer so behandelt, als ob sie Gruppenmitglieder wären.

GUARD-NAME = <filename 1…18 without-cat-gen-vers>
Name des Guards, in dem Zugriffsbedingungen festgelegt sind. Sind diese Bedingungen für einen Benutzer zum Zeitpunkt des Zugriffs erfüllt, hat dieser dieselben Rechte wie ein Gruppenmitglied.

Wenn das Guard zum Zeitpunkt der Auswertung nicht existiert oder nicht zugreifbar ist, gilt die Bedingung als nicht erfüllt.

Bei der Zugriffsrechteprüfung für Dateien und Jobvariablen, die durch BACL geschützt sind, wird die Gruppenstruktur auf dem Home-Pubset zugrunde gelegt. Die Guards der Gruppenverwaltung müssen daher ebenfalls auf dem Home-Pubset der laufenden Sitzung abgelegt sein. Deshalb muss der Name des Guards ohne Katalogkennung angegeben werden. Wird der Name des Guards ohne Benutzerkennung angegeben, wird das Guard unter der Benutzerkennung vorausgesetzt, unter der das Kommando /ADD-USER-GROUP aufgerufen wurde.

Der Gruppenverwalter ist dafür verantwortlich, dass das Guard existiert und zugreifbar ist. Gegebenenfalls muss er das Guard unter seiner Benutzerkennung auf dem Home-Pubset mit SCOPE-Attribut für die betreffende Gruppe anlegen.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

REMOVE-KEYTAB-ENTRY
Key-Tabellen-Eintrag löschen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Mit diesem Kommando kann der Sicherheitsbeauftragte (standardmäßig die Benutzerkennung SYSPRIV) einen Eintrag aus der Key-Tabelle löschen.

```
REMOVE-KEYTAB-ENTRY

 ENTRY-IDENTIFICATION = *STD / *ALL / list-poss(20): *STD / *SYSTEM-DEFAULT /
                        <name 1..8 with-wild(32)>
,PUBSET = *HOME / <cat-id 1..4>
,SELECT = *ALL / *BY-ATTRIBUTES(…)
    *BY-ATTRIBUTES(…)
        PRINCIPAL = *ANY / <c-string 1..1800 with-low>
```

ENTRY-IDENTIFICATION = *STD / *ALL /
list-poss(20): *STD / *SYSTEM-DEFAULT / <name 1..8 with-wild(32)>
Identifikation des Eintrags an, der gelöscht werden soll

ENTRY-IDENTIFICATION = *ALL
Alle Einträge werden gelöscht.

PUBSET = *HOME / <cat-id 1..4>
Katalogkennung des Pubsets, in dessen Benutzerkatalog die Schlüssel gelöscht werden. Im laufenden Betrieb sind die Schlüssel des Home-Pubsets maßgebend.

SELECT =
Angabe von Kriterien, nach dem die zu löschenden Einträge ausgewählt werden.

SELECT = *ALL
Einträge werden unabhängig von zusätzlichen Kriterien gelöscht.

SELECT = *BY-ATTRIBUTES(…)
Einträge werden nur gelöscht, wenn sie dem nachfolgend angegebenen Kriterium entsprechen.

PRINCIPAL = *ANY / <c-string 1..1800 with-low>
Kerberos-Name des BS2000-Rechners, dessen Eintrag gelöscht werden soll. Im Namen befindliche Wildcard-Zeichen werden berücksichtigt, falls sie nicht durch Voranstellen des Zeichens '\' entwertet werden.

REMOVE-USER-GROUP
Benutzergruppe löschen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Löscht eine Benutzergruppe aus dem Benutzerkatalog des angegebenen Pubset.

Voraussetzung ist, dass der Benutzergruppe weder Gruppenmitglieder angehören noch Untergruppen zugeordnet sind.

Soll eine Hierarchie von Benutzergruppen gelöscht werden, müssen im ersten Schritt die Gruppenmitglieder gelöscht oder anderen Benutzergruppen zugeordnet werden. Im zweiten Schritt kann dann die Gruppenstruktur (hierarchisch) von „unten nach oben“ gelöscht werden.

Freiwerdende Gruppenpotentiale werden der in der Gruppenhierarchie nächsthöheren Gruppe (UPPER-GROUP) zugeordnet (die maximale Anzahl von Untergruppen und Gruppenmitgliedern).

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter zu jeder Zeit für beliebige Gruppen
– Gruppenverwalter mit der MANAGE-GROUPS-Berechtigung (ADM-AUTHORITY). Das Kommando gilt nur für die untergeordnete Gruppenhierarchie

Die Prüfung, ob das Kommando von einem systemglobalen Benutzerverwalter gegeben wird, erfolgt gegen den Home-Pubset der laufenden Sitzung

Die Prüfung, ob das Kommando von einem Gruppenverwalter gegeben wird, erfolgt gegen den unter dem Operanden PUBSET angegebenen Pubset

REMOVE-**USER-GR**OUP
GROUP-**ID**ENTIFICATION = list-poss(127): <name 1..8> ,**PUBSET** = ***HOME** / <cat-id 1..4>

GROUP-IDENTIFICATION =
Benutzergruppenkennung, deren Eintrag gelöscht wird.

GROUP-IDENTIFICATION = list-poss(127): <name 1..8>
Name der Benutzergruppe.

PUBSET = *HOME / <cat-id 1..4>
Pubset, aus dessen Benutzerkatalog der Gruppeneintrag gelöscht wird.

PUBSET = *HOME
Der Gruppeneintrag im Benutzerkatalog des Home-Pubset wird gelöscht.

PUBSET = <cat-id 1..4>
Katalogkennung des Pubset, in dessen Benutzerkatalog der Gruppeneintrag gelöscht wird.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

RESET-PRIVILEGE
Systemglobale Privilegien entziehen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Entzieht einer Benutzerkennung systemglobale Privilegien oder Sammelprivilegien.

Einer Kennung, die auf dem im Kommando angegebenen Pubset das Privileg SECURITY-ADMINISTRATION besitzt, kann kein Privileg oder Sammelprivileg entzogen werden.

Nur wenn das Kommando für eine Benutzerkennung auf dem Home-Pubset gegeben wird, wird diese Änderung auch im System wirksam, d.h. verfügt die Benutzerkennung nicht mehr über den mit dem Privileg verknüpften Rechteumfang.

Die Änderung wirkt sich nicht auf aktive Benutzeraufträge unter der Benutzerkennung aus, sondern wird erst nach dem nächsten LOGON unter der Benutzerkennung wirksam.

```
RESET-PRIVILEGE

 PRIVILEGE = *ALL / *PRIVILEGE-SET(...) / list-poss(64): <text>
    *PRIVILEGE-SET(...)
       | PRIVILEGE-SET-NAME = list-poss(20): <name 1..8>
,USER-IDENTIFICATION = <name 1..8>
,PUBSET = *HOME / <cat-id 1..4>
```

PRIVILEGE =
Name des Privilegs, das einer Benutzerkennung entzogen werden soll. Der Operand muss angegeben werden. Die Einzelprivilegien sind ab Seite 40 beschrieben.

PRIVILEGE = *ALL
Der Kennung werden die Privilegien zugewiesen, die sie nach First-Start hatte (siehe Abschnitt „Privilegienverteilung nach First-Start“ auf Seite 62).

PRIVILEGE = *PRIVILEGE-SET(...)
Angabe eines oder mehrerer Sammelprivilegien.

PRIVILEGE-SET-NAME = list-poss(20): <name 1..8>
Sammelprivileg, das der Benutzerkennung entzogen werden soll, bzw. Liste der Sammelprivilegien.

PRIVILEGE = list-poss(64): <text>
Privileg, das einer Benutzerkennung entzogen werden soll. Mögliche Privilegien siehe Seite 128. Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

USER-IDENTIFICATION = <name 1..8>
Benutzerkennung, der das angegebene Privileg oder Sammelprivileg entzogen werden soll.

PUBSET = *HOME / <cat-id 1..4>
Pubset, auf dem das angegebene Privileg für die Benutzerkennung rückgesetzt werden soll.

PUBSET = *HOME
Der Eintrag erfolgt auf dem Home-Pubset. Der Entzug der Berechtigung wird im System wirksam!

PUBSET = <cat-id 1..4>
Der Eintrag erfolgt auf dem angegebenen Pubset.

Hinweise

– Ist die Benutzerkennung bzgl. eines Einzelprivilegs die einzige Kennung, die dieses Privileg auf dem angegebenen Pubset besitzt, muss über die Meldung SRM4006 im Dialog über das Entziehen des Privilegs entschieden werden.

  Für andere im Kommando angegebene Rechte wird das Kommando ausgeführt, unabhängig, wie die Meldung beantwortet wurde.

– Sammelprivilegien werden ohne Rückfrage entzogen.

– Wird das Privileg SAT-FILE-MANAGEMENT oder SAT-FILE-EVALUATION einer Benutzerkennung entzogen, so wird die SAT-Protokollierung für diese Benutzerkennung nicht automatisch ausgeschaltet.

– Jede Kennung muss mindestens ein Einzelprivileg besitzen. Der Versuch, einer Kennung das letzte Einzelprivileg zu entziehen, wird abgewiesen. Diese Regelung gilt nur für Einzelprivilegien. Sammelprivilegien zählen nicht als Einzelprivilegien und bleiben daher bei der Zählung der Privilegien unberücksichtigt.

– Wird einer Kennung, die neben den Privilegien SAT-FILE-MANAGEMENT, SAT-FILE-EVALUATION oder HARDWARE-MAINTENANCE auch das Privileg STD-PROCESSING besitzt, das Privileg STD-PROCESSING entzogen, so dürfen unter dieser Kennung trotzdem noch einige Benutzerkommandos ausgeführt werden.

– Der Sicherheitsbeauftragte kann einige Benutzerkommandos ausführen, obwohl er das Privileg STD-PROCESSING nicht besitzt.

– Das Privileg POSIX-ADMINISTRATION kann der Kennung SYSROOT nicht entzogen werden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

SET-LOGON-DEFAULTS
Standardwerte für Schutzattribute vereinbaren

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: USER-ADMINISTRATION

Mit diesem Kommando kann der systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) Standard-Schutzattribute für die Zugangskontrolle festlegen. Diese Einstellungen gelten als Standardwerte für die Kommandos /SET- und /MODIFY-LOGON-PROTECTION.

```
SET-LOGON-DEFAULTS

 PUBSET = *HOME / <cat-id 1..4>
,EXPIRATION-DATE = *NONE / <integer 0..366>
,EXPIRATION-WARNING = *STD / <integer 0..366>
,PASSWORD = *PARAMETERS(...)
   *PARAMETERS(...)
      MANAGEMENT = *USER-CHANGE-ONLY / *BY-ADMINISTRATOR / *BY-USER
      ,MINIMAL-LENGTH = *NONE / <integer 1..8>
      ,MINIMAL-COMPLEXITY = *NONE / <integer 1..4>
      ,INITIAL-LIFETIME = *STD / *EXPIRED / <integer 0..366>
      ,LIFETIME-INTERVAL = *UNLIMITED / <integer 1..366>(...)
         <integer 1..366>(...)
            DIMENSION = *DAYS / *MONTHS
      ,EXPIRATION-WARNING = *STD / <integer 0..366>
      ,UNLOCK-EXPIRATION = *BY-ADMINISTRATOR-ONLY / *BY-USER
      ,PASSWORD-MEMORY = *NONE / *YES(…)
         *YES(…)
            PERIOD = 1 / <integer 1..32767>
            ,CHANGES-PER-PERIOD = 1 / <integer 1..100>
            ,BLOCKING-TIME = 100 / <integer 1..32767>
```

(Teil 1 von 2)

```
,SUSPEND-ATTRIBUTES = *NONE / *YES(...)
    *YES(...)
        COUNT = 5 / <integer 0..32767>
        ,OBSERVE-TIME = 30 / <integer 0..32767> (…)
            <integer 0..32767> (…)
                DIMENSION = *MINUTE / *HOUR
        ,SUSPEND-TIME = 30 / <integer 1..32767> (…) / *UNLIMITED
            <integer 1..32767> (…)
                DIMENSION = *MINUTE / *HOUR
        ,SUBJECT = *USER-IDENTIFICATION  / *INITIATOR
,INACTIVITY-LIMIT = *NONE / <integer 1..366> (…)
            <integer 1..366>(...)
                DIMENSION = *DAYS / *MONTHS
,DIALOG-ACCESS = *YES / *NO
,BATCH-ACCESS = *YES / *NO
,OPERATOR-ACCESS-TERM = *YES / *NO
,OPERATOR-ACCESS-PROG = *YES / *NO
,OPERATOR-ACCESS-CONS = *YES / *NO
,POSIX-RLOGIN-ACCESS = *YES / *NO
,POSIX-REMOTE-ACCESS = *YES / *NO
,NET-DIALOG-ACCESS = *YES / *NO
```

(Teil 2 von 2)

Bedeutung der Operanden siehe Kommando /SET-LOGON-PROTECTION (Seite 241).

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

SET-LOGON-PROTECTION
Schutzattribute vereinbaren

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Vereinbart Schutzattribute für existierende Benutzerkennungen.

Berechtigt zur Ausführung des Kommandos sind:

– Systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) für alle Benutzerkennungen

– Gruppenverwalter, die mindestens das Attribut MANAGE-MEMBERS besitzen, für die ihrer Benutzergruppe zu- und untergeordneten Benutzerkennungen

SET-LOGON-PROTECTION
USER-IDENTIFICATION = <name 1..8>
,**PUBSET** = ***HOME** / <cat-id 1..4>
,**EXPIR**ATION-**DATE** = ***LOGON-DEF**AULT / ***NONE** / <date 8..10> / <integer 0..366>
,**EXPIR**ATION-**WARNING** = ***LOGON-DEF**AULT / ***STD** / <integer 0..366>

(Teil 1 von 7)

,**PASS**WORD = ***PAR**AMETERS(...)

***PAR**AMETERS(...)

LOGON-PASSWORD = ***NONE** / ***SECRET** / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>

,**ENCR**YPTION = ***Y**ES / ***NO**

,**MANAG**EMENT = ***LOGON-DEF**AULT / ***USER-CHA**NGE-**ONLY** / ***BY-USER** / ***BY-ADM**INISTRATOR

,**MIN**IMAL-**LENGTH** = ***LOGON-DEF**AULT / ***NONE** / <integer 1..8>

,**MIN**IMAL-**COMPLEX**ITY = ***LOGON-DEF**AULT / ***NONE** / <integer 1..4>

,**INITIAL-LIFE**TIME = ***LOGON-DEF**AULT / ***STD** / ***EXPIR**ED / <integer 0..366> / <date 8..10>

,**LIFE**TIME-**INTERVAL** = ***LOGON-DEF**AULT / ***UNLIM**ITED / <integer 1..366>(...)

<integer 1..366>(...)

DIMENSION = ***DAYS** / ***MONTHS**

,**EXPIR**ATION-**WARNING** = ***LOGON-DEF**AULT / ***STD** / <integer 0..366>

,**UNLOCK-EXPIR**ATION = ***LOGON-DEF**AULT / ***BY-ADM**INISTRATOR-ONLY / ***BY-USER**

,**PASS**WORD-**MEMORY** = ***LOGON-DEF**AULT / ***NONE** / ***YES**(…)

***YES**(…)

PERIOD = **1** / <integer 1..32767>

,**CHA**NGES-**PER-PER**IOD = **1** / <integer 1..100>

,**BLOCK**ING-**TIME** = **100** / <integer 1..32767>

,**SUSPEND-ATTR**IBUTES = ***LOGON-DEF**AULT / ***NONE** / ***Y**ES(...)

***Y**ES(...)

COUNT = ***LOGON-DEF**AULT / <integer 0..32767>

,**OBSERVE-TIME** = ***LOGON-DEF**AULT / <integer 0..32767> (…)

<integer 0..32767> (…)

DIMENSION = ***MINUTE** / ***HOUR**

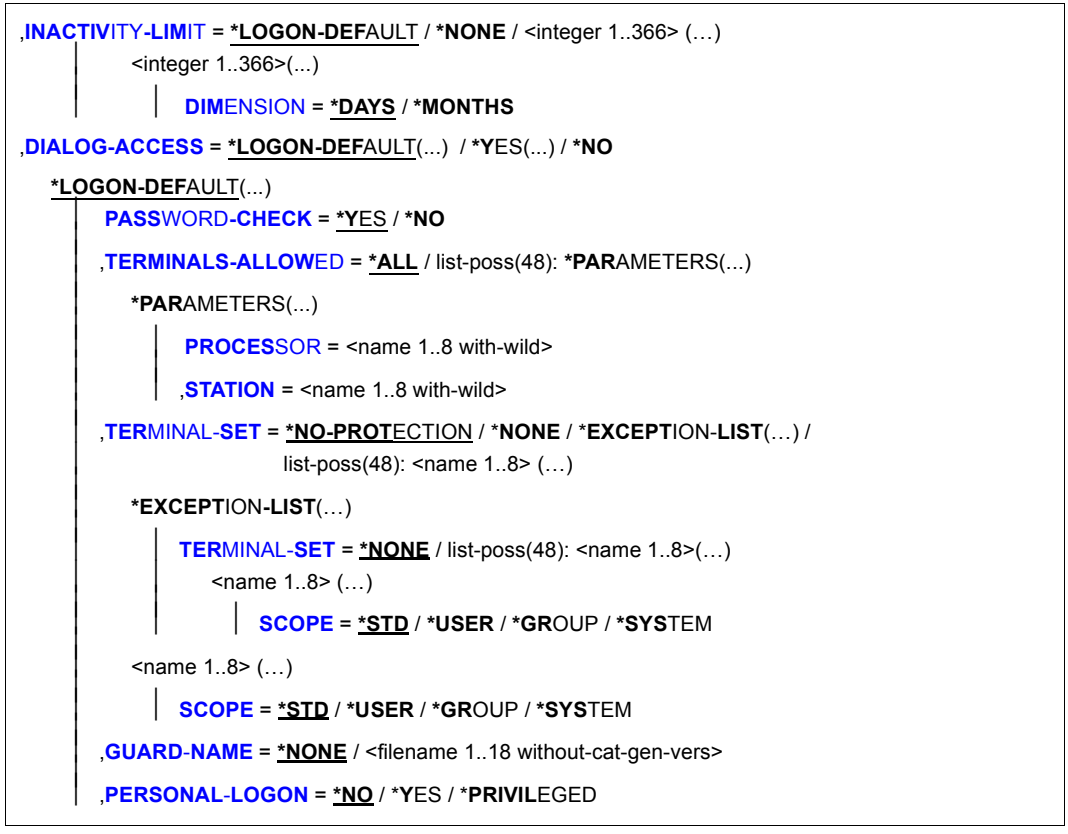
,**SUSPEND-TIME** = ***LOGON-DEF**AULT / <integer 1..32767> (…) / ***UNLIM**ITED

<integer 1..32767> (…)

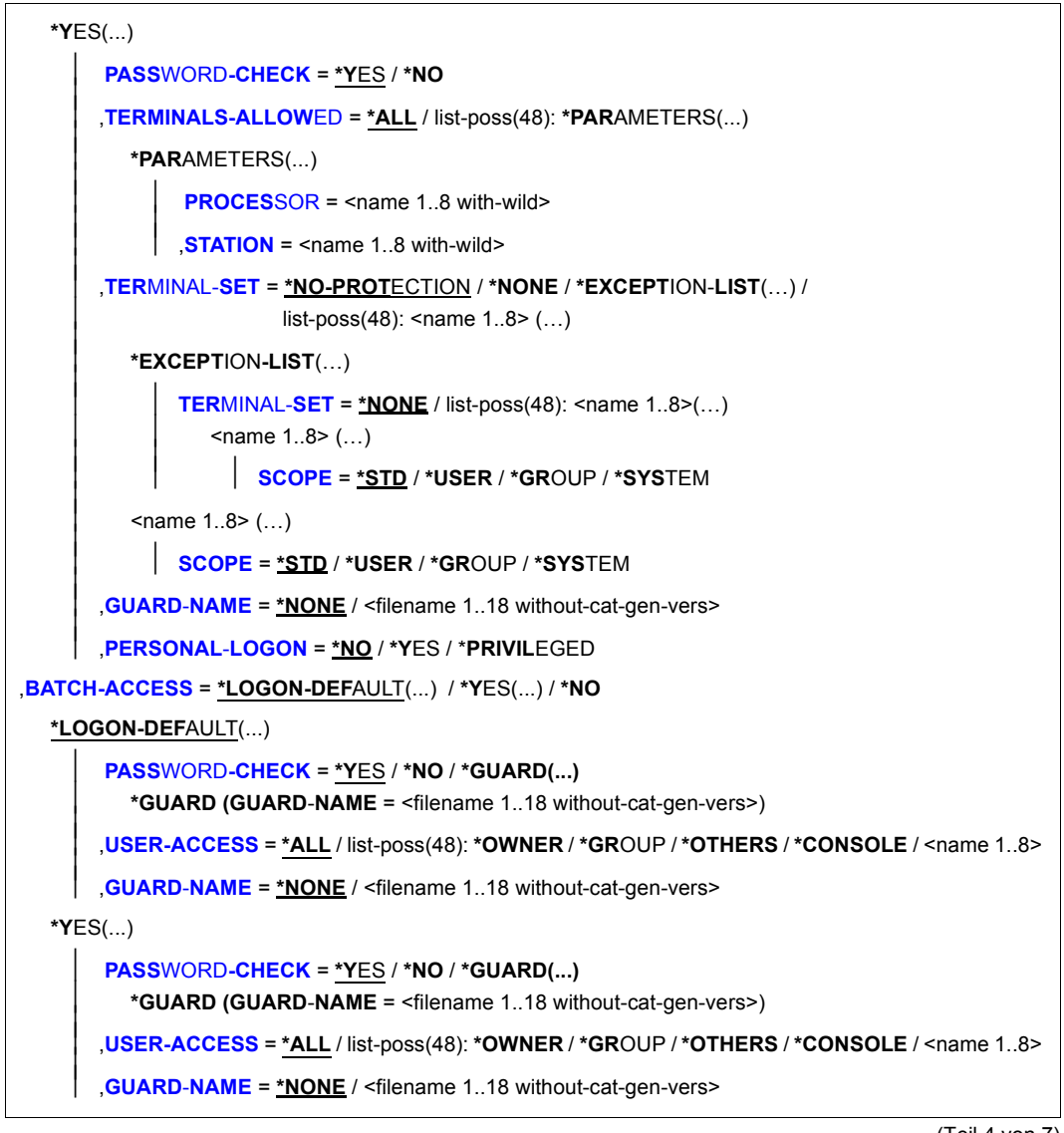
DIMENSION = ***MINUTE** / ***HOUR**

,**SUBJECT** = ***LOGON-DEF**AULT / ***USER-ID**ENTIFICATION / ***INITIATOR**

(Teil 2 von 7)


,INACTIVITY-LIMIT = *LOGON-DEFAULT / *NONE / <integer 1..366> (…)
<integer 1..366>(...)
DIMENSION = *DAYS / *MONTHS
,DIALOG-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO
,TERMINALS-ALLOWED = *ALL / list-poss(48): *PARAMETERS(...)
*PARAMETERS(...)
PROCESSOR = <name 1..8 with-wild>
,STATION = <name 1..8 with-wild>
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
,PERSONAL-LOGON = *NO / *YES / *PRIVILEGED

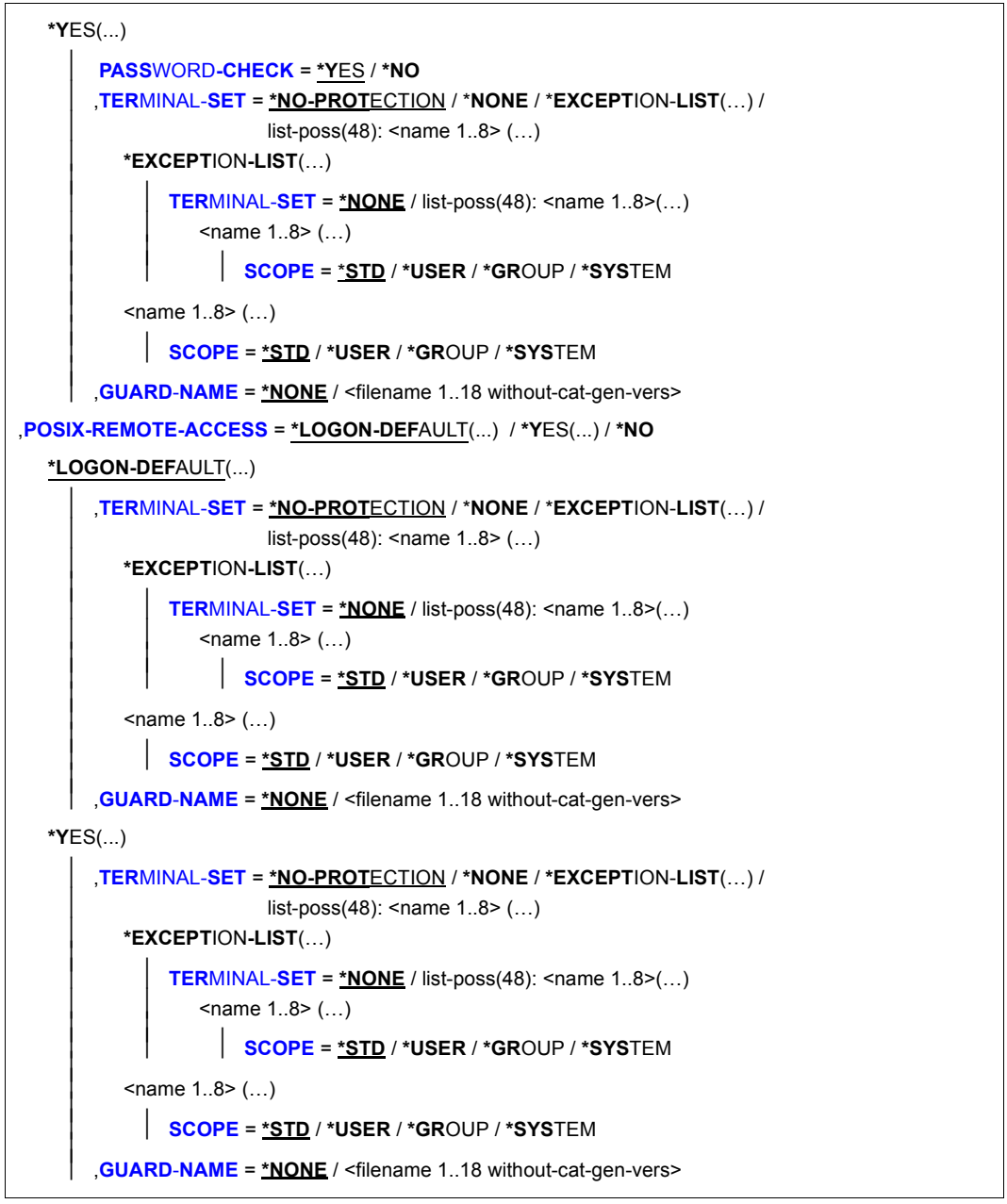
(Teil 3 von 7)


*YES(...)
PASSWORD-CHECK = *YES / *NO
,TERMINALS-ALLOWED = *ALL / list-poss(48): *PARAMETERS(...)
*PARAMETERS(...)
PROCESSOR = <name 1..8 with-wild>
,STATION = <name 1..8 with-wild>
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
,PERSONAL-LOGON = *NO / *YES / *PRIVILEGED
,BATCH-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO / *GUARD(...)
*GUARD (GUARD-NAME = <filename 1..18 without-cat-gen-vers>)
,USER-ACCESS = *ALL / list-poss(48): *OWNER / *GROUP / *OTHERS / *CONSOLE / <name 1..8>
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
*YES(...)
PASSWORD-CHECK = *YES / *NO / *GUARD(...)
*GUARD (GUARD-NAME = <filename 1..18 without-cat-gen-vers>)
,USER-ACCESS = *ALL / list-poss(48): *OWNER / *GROUP / *OTHERS / *CONSOLE / <name 1..8>
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 4 von 7)


,OPERATOR-ACCESS-TERM = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO
*YES(...)
PASSWORD-CHECK = *YES / *NO
,OPERATOR-ACCESS-PROG = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO
*YES(...)
PASSWORD-CHECK = *YES / *NO
,OPERATOR-ACCESS-CONS = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO
*YES(...)
PASSWORD-CHECK = *YES / *NO
,POSIX-RLOGIN-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
PASSWORD-CHECK = *YES / *NO
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 5 von 7)


*YES(...)
PASSWORD-CHECK = *YES / *NO
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
,POSIX-REMOTE-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
*LOGON-DEFAULT(...)
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
*YES(...)
,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
list-poss(48): <name 1..8> (…)
*EXCEPTION-LIST(…)
TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
<name 1..8> (…)
SCOPE = *STD / *USER / *GROUP / *SYSTEM
,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>

(Teil 6 von 7)

```
,NET-DIALOG-ACCESS = *LOGON-DEFAULT(...)  / *YES(...) / *NO
    *LOGON-DEFAULT(...)
        PASSWORD-CHECK = *YES / *NO
        ,PRINCIPAL = *NO-PROTECTION / *NONE / *ALL /
                list-poss(48): <composed-name 1..1800 with-under with-wild> / <c-string 1..1800 with-low>
        ,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
                        list-poss(48): <name 1..8> (…)
            *EXCEPTION-LIST(…)
                TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
                    <name 1..8> (…)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            <name 1..8> (…)
                SCOPE = *STD / *USER / *GROUP / *SYSTEM
        ,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
    *YES(...)
        PASSWORD-CHECK = *YES / *NO
        ,PRINCIPAL = *NO-PROTECTION / *NONE / *ALL /
                list-poss(48): <composed-name 1..1800 with-under with-wild> / <c-string 1..1800 with-low>
        ,TERMINAL-SET = *NO-PROTECTION / *NONE / *EXCEPTION-LIST(…) /
                        list-poss(48): <name 1..8> (…)
            *EXCEPTION-LIST(…)
                TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
                    <name 1..8> (…)
                        SCOPE = *STD / *USER / *GROUP / *SYSTEM
            <name 1..8> (…)
                SCOPE = *STD / *USER / *GROUP / *SYSTEM
        ,GUARD-NAME = *NONE / <filename 1..18 without-cat-gen-vers>
```

(Teil 7 von 7)

Der Operandenwert *LOGON-DEFAULT bedeutet, dass die mit dem Kommando SET- oder MODIFY-LOGON-DEFAULTS festgelegte Standard-Einstellung für den Operanden übernommen wird.

USER-IDENTIFICATION = <name 1..8>
Benutzerkennung, deren Schutzattribute festgelegt werden sollen.

PUBSET = *HOME / <cat-id 1..4>
Pubset, in dessen Benutzerkatalog die Schutzattribute eingetragen werden sollen.

PUBSET = *HOME
Der Eintrag erfolgt auf dem Home-Pubset.

PUBSET = <cat-id 1..4>
Der Eintrag erfolgt auf dem angegebenen Pubset.

EXPIRATION-DATE = *LOGON-DEFAULT / *NONE / <date 8..10> / <integer 0..366>
Nach dem angegebenen Datum wird die Benutzerkennung gesperrt, d.h. für LOGON nicht mehr zugänglich. Die für die Benutzerkennung katalogisierten Dateien bleiben erhalten. Während des Zeitraums, der im Operanden EXPIRATION-WARNING angegeben ist, erhält der Benutzer bei jedem LOGON die Meldung SRM3201 auf SYSOUT.

EXPIRATION-DATE = *NONE
Die Benutzerkennung wird nicht zu einem bestimmten Datum gesperrt.

EXPIRATION-DATE = <date 8..10>
Verfallsdatum der Benutzerkennung.

EXPIRATION-DATE = <integer 0..366>
Lebensdauer der Benutzerkennung.

EXPIRATION-WARNING = *LOGON-DEFAULT / *STD / <integer 0..366>
Definiert den Zeitraum in Tagen, innerhalb dessen der Benutzer vor dem Überschreiten des Verfallsdatums der Benutzerkennung gewarnt wird. Der Standardwert beträgt 28 Tage.

PASSWORD = *PARAMETERS(...)
Vorgaben für Kennwörter festlegen.

LOGON-PASSWORD = *NONE / *SECRET / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
Vom Benutzer einzugebendes Kennwort.

LOGON-PASSWORD = *NONE
Für den Zugang zu dieser Benutzerkennung wird kein Kennwort vereinbart.

LOGON-PASSWORD = *SECRET
Das Kennwort wird dunkelgesteuert angefordert.

ENCRYPTION = *YES / *NO
Gibt an, ob das Kennwort unverändert oder verschlüsselt abgelegt wird.

ENCRYPTION = *YES
Es wird gemäß dem Systemparameter ENCRYPT verschlüsselt.

MANAGEMENT = *LOGON-DEFAULT / *USER-CHANGE-ONLY / *BY-USER / *BY-ADMINISTRATOR
Definiert die Berechtigung zur Verwaltung des Kennworts.

MANAGEMENT = *USER-CHANGE-ONLY
Der Benutzer darf das Kennwort vereinbaren und ändern, aber nicht löschen.

MANAGEMENT = *BY-USER
Der Benutzer darf das Kennwort vereinbaren, ändern und löschen.

MANAGEMENT = *BY-ADMINISTRATOR
Das Kennwort kann nur mit den Systembetreuungs-Kommandos /MODIFY-USER-ATTRIBUTES und /MODIFY-LOGON-PROTECTION verändert werden.

MINIMAL-LENGTH = *LOGON-DEFAULT / *NONE / <integer 1..8>
Gibt die minimale Länge an, die ein vom Benutzer vereinbartes Kennwort haben muss. Bei Verwendung von langen Kennwörtern, beachten Sie bitte die Hinweise auf Seite 94.

MINIMAL-LENGTH = *NONE
Es wird keine minimale Länge festgelegt. Der Benutzer darf Kennwörter bis zu einer Länge von 8 Zeichen vereinbaren.

MINIMAL-LENGTH = <integer 1..8>
Gibt die minimale Länge an, die ein vom Benutzer vereinbartes Kennwort haben muss (in Zeichen). Bei Verwendung dieses Operanden muss das Kennwort mit einem Zeichen ungleich Leerzeichen enden.

MINIMAL-COMPLEXITY = *LOGON-DEFAULT / *NONE / <integer 1..4>
Gibt die minimale Komplexität an, die ein vom Benutzer vereinbartes Kennwort haben muss. Bei Verwendung von langen Kennwörtern, beachten Sie bitte die Hinweise auf Seite 94.

MINIMAL-COMPLEXITY = *NONE
Der Benutzer darf Kennwörter beliebiger Komplexität vereinbaren.

MINIMAL-COMPLEXITY = <integer 1..4>
Komplexitätsstufen mit folgenden Vorschriften (jede Stufe beinhaltet alle anderen Stufen mit kleinerer Kennziffer):

Stufe 1: Keine Einschränkungen.

Stufe 2: Maximal zwei aufeinander folgende Zeichen dürfen gleich sein.

Stufe 3: Es muss mindestens je ein Buchstabe und eine Ziffer im Kennwort angegeben sein.

Stufe 4: Es müssen mindestens je ein Buchstabe, eine Ziffer und ein Sonderzeichen (d.h. ein Zeichen aus der Restmenge) angegeben sein.
Das Leerzeichen zählt nicht als Sonderzeichen.

INITIAL-LIFETIME = *LOGON-DEFAULT / *STD / *EXPIRED / <integer 0..366> / <date 8..10>
Definiert den ersten Lebensdauer-Zyklus.

INITIAL-LIFETIME = *STD
Das Verfallsdatum des Kennwortes wird aus LIFETIME-INTERVAL berechnet.

INITIAL-LIFETIME = *EXPIRED
Das eingetragene Logon-Kennwort wird als 'verfallen' gekennzeichnet. Der Eigentümer der Benutzerkennung muss zunächst ein neues Logon-Kennwort vereinbaren, bevor er mit seiner Benutzerkennung arbeiten kann. Näheres hierzu siehe Operand UNLOCK-EXPIRATION.

INITIAL-LIFETIME = <integer 0..366>
Lebensdauer des Kennwortes.

INITIAL-LIFETIME = <date 8..10>
Verfallsdatum des Kennwortes.

LIFETIME-INTERVAL = *LOGON-DEFAULT / *UNLIMITED / <integer 1..366>(...)
Definiert den Zeitraum, in dem das Kennwort vom Benutzer immer wieder geändert werden muss. Ändert der Benutzer das Kennwort nicht rechtzeitig, wird die Benutzerkennung gesperrt. Während des Zeitraums, der im Operanden EXPIRATION-WARNING des Kennwortes angegeben ist, erhält der Benutzer bei jedem LOGON die Meldung SRM3201 auf SYSOUT.

LIFETIME-INTERVAL = *UNLIMITED
Das Kennwort muss vom Benutzer nicht geändert werden.

LIFETIME-INTERVAL = <integer 1..366>(...)
Gibt den Zeitraum an.

DIMENSION = *DAYS / *MONTHS
Einheit des angegebenen Zahlenwertes. Bei Angabe von *MONTHS ist der maximal zulässige Wert für integer 12.

EXPIRATION-WARNING = *LOGON-DEFAULT / *STD / <integer 0..366>
Definiert den Zeitraum in Tagen, innerhalb dessen der Benutzer vor dem Überschreiten des Verfallsdatums des Kennwortes gewarnt wird. Der Standardwert beträgt 28 Tage.

UNLOCK-EXPIRATION = *LOGON-DEFAULT / *BY-ADMINISTRATOR-ONLY / *BY-USER
Gibt an, wer berechtigt ist, ein verfallenes Kennwort durch ein neues zu ersetzen.

UNLOCK-EXPIRATION = *BY-ADMINISTRATOR-ONLY
Nach Überschreiten des Verfallsdatums des Kennwortes wird die Kennung gesperrt. Die Systembetreuung muss ein neues Logon-Kennwort eintragen, um damit dem Eigentümer der Benutzerkennung den Zugang wieder zu ermöglichen.

UNLOCK-EXPIRATION = *BY-USER
Nach Überschreiten des Verfallsdatums wird dem Anwender bei Angabe des verfallenen Kennwortes ein eingeschränkter Dialog-Zugang gewährt. Dabei hat der Anwender nur die Möglichkeit ein neues Kennwort zu vereinbaren oder die Dialog-Task wieder zu beenden.

PASSWORD-MEMORY = *LOGON-DEFAULT / *NONE / *YES(…)
Gibt an, ob bei einer Änderung des Kennwortes das alte Kennwort in einer Liste abgelegt wird. Kennwörter, die in dieser Liste enthalten sind, dürfen bei einer Kennwortänderung nicht als neues Kennwort vergeben werden. Außerdem kann die Häufigkeit von Kennwortänderungen eingeschränkt werden.

PASSWORD-MEMORY = *NONE
Es wird keine Kennwortliste angelegt. Falls bereits eine existiert, wird sie gelöscht. Die Häufigkeit von Kennwortänderungen wird nicht eingeschränkt.

PASSWORD-MEMORY = *YES(…)
Es wird eine Kennwortliste angelegt. Außerdem wird eine Maximalzahl für Kennwortänderungen festgelegt, die innerhalb eines definierten Zeitraums erlaubt sind.

Die Operanden PERIOD, CHANGES-PER-PERIOD und BLOCKING-TIME hängen folgendermaßen voneinander ab:

– PERIOD ≤ BLOCKING-TIME

– CHANGES-PER-PERIOD ≤ (100 * PERIOD) / BLOCKING-TIME

PERIOD = 1 / <integer 1..32767>
Legt den Zeitraum fest, für den mit dem Operanden CHANGES-PER-PERIOD ein Maximalwert für die Anzahl von Kennwortänderungen festgelegt wird. Die Dauer wird in Tagen angegeben. Standardmäßig wird ein Zeitraum von einem Tag eingestellt.

CHANGES-PER-PERIOD = 1 / <integer 1..100>
Gibt die maximale Anzahl erlaubter Kennwortänderungen innerhalb des Zeitraums an, der im Operanden PERIOD festgelegt wird. Kennwortänderungen auf das Kennwort *NONE werden bei dieser Zählung nicht berücksichtigt. Standardmäßig kann das Kennwort ein Mal pro Tag geändert werden.

BLOCKING-TIME = 100 / <integer 1..32767>
Legt fest, wie lange ein Kennwort in der Kennwortliste gespeichert bleibt. Die Dauer wird in Tagen angegeben und beginnt an dem Tag, an dem ein Kennwort durch ein anderes ersetzt wird. Standardmäßig wird ein verbrauchtes Kennwort 100 Tage gesperrt.

SUSPEND-ATTRIBUTES = *LOGON-DEFAULT / *NONE / *YES(...)
Legt die Attribute für die Suspendierung fest. Die temporäre Sperre einer Benutzerkennung bzw. des Benutzers einer Benutzerkennung nach einer Anzahl fehlerhafter Zugangsversuche kann lokal für diese Benutzerkennung oder global in den Standard-Attributen festgelegt werden.

SUSPEND-ATTRIBUTES = *NONE
Es findet keine Suspendierung statt.

SUSPEND-ATTRIBUTES = *YES(...)
Vereinbart die Parameter für die Suspendierung.

COUNT = *LOGON-DEFAULT / <integer 0..32767>
Anzahl fehlerhafter Zugangsversuche, die innerhalb des mit OBSERVE-TIME festgelegten Zeitraums erlaubt sind. Weitere fehlerhafte Zugangsversuche haben eine Suspendierung zur Folge.

OBSERVE-TIME = *LOGON-DEFAULT / <integer 0..32767> (…)
Zeitraum, innerhalb dessen die mit dem Operanden COUNT angegebene Anzahl fehlerhafter Zugangsversuche stattfinden muss. Der Zeitraum beginnt mit dem ersten fehlerhaften Zugangsversuch. Ist der Beobachtungszeitraum beendet, ohne dass eine Suspendierung erfolgt ist, beginnt die Zählung beim nächsten Fehlversuch von vorne.

OBSERVE-TIME = <integer 0..32767> (…)
Angabe des Beobachtungszeitraums.

DIMENSION = *MINUTE / *HOUR
Zeiteinheit für den Beobachtungszeitraum.

SUSPEND-TIME = *LOGON-DEFAULT / <integer 1..32767> (…) / *UNLIMITED
Vereinbart die Dauer der Suspendierung. Während der Suspendierung wird ein Benutzer mit den Meldungen SRM3208 oder SRM3209 über die Tatsache und ggf. Dauer der Suspendierung informiert.

SUSPEND-TIME = <integer 1..32767> (…)
Dauer der Suspendierung.

DIMENSION = *MINUTE / *HOUR
Zeiteinheit für die Suspendierung.

SUSPEND-TIME = *UNLIMITED
Die Suspendierung ist von unbegrenzter Dauer.

SUBJECT = *LOGON-DEFAULT / *USER-IDENTIFICATION / *INITIATOR
Legt fest, ob die Benutzerkennung oder die Person, die die Zugangsversuche unternommen hat, suspendiert werden soll.

SUBJECT = *USER-IDENTIFICATION
Die Benutzerkennung wird suspendiert.
Diese Angabe ist bei der Systemkennung TSOS und der Benutzerkennung des Sicherheitsbeauftragten nicht erlaubt und wird mit Meldung SRM3672 abgewiesen.

SUBJECT = *INITIATOR
Die „Person“, die die Zugangsversuche unternommen hat, wird suspendiert (siehe Abschnitt „Sperrung von Terminals/Benutzerkennungen nach erfolglosen Zugangsversuchen“ auf Seite 119).

INACTIVITY-LIMIT = *LOGON-DEFAULT / *NONE / <integer 1..366> (…)
Vereinbart die Zeit der Inaktivität, also die seit dem letzten Logon verstrichene Zeit, nach der die Benutzerkennung gesperrt werden soll. Die Sperre kann mit dem Kommando /MODIFY-USER-ATTRIBUTES aufgehoben werden.

INACTIVITY-LIMIT = *NONE
Es findet keine Überwachung der Inaktivität statt.

INACTIVITY-LIMIT = <integer 1..366> (…)
Angabe der Zeit bis zum Eintritt der Sperre (Inaktivitätslimit).
Diese Angabe ist bei den Systemkennungen nicht erlaubt und wird mit Meldung SRM3673 abgewiesen.

DIMENSION = *DAYS / *MONTHS
Zeiteinheit für das Inaktivitätslimit.

DIALOG-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert die im Dialogbetrieb wirksamen Zugangskontrollen.

DIALOG-ACCESS = *YES(...)
Legt fest, dass Zugangskontrollen durchgeführt werden.

PASSWORD-CHECK = *YES / *NO
Legt fest, ob im Dialog eine Kennwortprüfung stattfindet.

TERMINALS-ALLOWED =
Legt die Datensichtstationen fest, von denen aus der Zugang erlaubt ist. Dieser Operand wird aus Kompatibilitätsgründen unterstützt. Die Steuerung über den Operanden TERMINAL-SET ist zu bevorzugen.

Bei gleichzeitiger Angabe der Operanden TERMINALS-ALLOWED und TERMINAL-SET beachten Sie bitte den Hinweis beim Operanden TERMINAL-SET auf Seite 254.

TERMINALS-ALLOWED = *ALL
Alle Datensichtstationen sind zugelassen.

TERMINALS-ALLOWED = *PARAMETERS(...)
Schränkt den Zugang zur Benutzerkennung auf bestimmte Datensichtstationen ein (BCAM-Namen).

PROCESSOR = <name 1..8 with-wild>
BCAM-Name des Rechners, von dem aus die Verbindung zu $DIALOG aufgebaut wird (z.B. ein PC, auf dem eine Datensichtstations-Emulation läuft).

STATION = <name 1..8 with-wild>
Logischer Name der Datensichtstation.

TERMINAL-SET =
Angabe, ob die Kennung mit Terminal-Sets geschützt wird.

Hinweis

Bei gleichzeitiger Angabe der Operanden TERMINALS-ALLOWED (≠*ALL) und TERMINAL-SET (≠ *NO-PROTECTION) ist Folgendes zu beachten:

Die Prüfung der Datensichtstation erfolgt zunächst anhand der Terminal-Liste (TERMINALS-ALLOWED). Gewährt diese den Zugang, wird die Terminal-Set-Liste nicht mehr überprüft. Eventuell widersprechende Angaben in einer Negativ-Liste oder im Guard eines Terminal-Sets bleiben unberücksichtigt. Nur falls die Prüfung der Terminal-Liste das Ergebnis „Kein Zugang“ liefert, findet eine Prüfung der Terminal-Set-Liste statt. Das Ergebnis dieser Prüfung entscheidet dann, ob ein Zugang zum aktuellen Zeitpunkt erlaubt ist oder nicht.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Dialogzugang erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. der Dialogzugang ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Dialogzugang verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Dialogzugang erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD
Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME =
Gibt an, ob der Dialog-Zugang zu einer Benutzerkennung mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Dialog-Zugang zur Benutzerkennung wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang zur Benutzerkennung ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Welche Benutzerkennung als Subjekt in der Zugriffsbedingung des Guards zugelassen sein muss, hängt vom Operanden PERSONAL-LOGON ab. Bei PERSONAL-LOGON=*NO gilt die geschützte Benutzerkennung als Subjekt der Zugriffsbedingung. Bei PERSONAL-LOGON=*YES ist das die persönliche Benutzerkennung.

PERSONAL-LOGON =
Legt fest, ob beim Dialogzugang neben der Logon- auch eine persönliche Benutzerkennung verlangt wird.

PERSONAL-LOGON = *NO
Es wird nur die Logon-Benutzerkennung verlangt.

PERSONAL-LOGON = *YES
Es wird zusätzlich zur Logon- eine persönliche Benutzerkennung verlangt.

PERSONAL-LOGON = *PRIVILEGED
Es wird zusätzlich zur Logon- eine persönliche Benutzerkennung verlangt.

Außerdem erhält die Dialog-Task zusätzlich zu den Privilegien der Logon-Kennung auch die der persönlichen Kennung (außer TSOS, falls vorhanden).

Die Vorgabe zur Protokollierung aller Ereignisse (AUDIT-SWITCH=*ON) wird aus den Einstellungen der SAT-Preselection für die Protokollierung der persönlichen Benutzerkennung (USER-AUDITING) in die Dialog-Task übernommen.

Ist die Logon-Kennung Gruppenverwalter und die persönliche Kennung Benutzerverwalter, übernimmt die Dialog-Task die Rolle des Gruppenverwalters und erhält nicht das Privileg USER-ADMINISTRATION.

Einschränkung für Systeme mit BS2000 OSD/BC ≤ V11.0A:

Die systeminterne SCI-Schnittstelle (Synchronous Console Interface) ermöglicht die Eingabe von Operator-Kommandos aus einer Benutzer-Task. Diese Operator-Kommandos schlagen fehl, wenn sie erst durch ein persönliches Logon mit der Übernahme der Privilegien der persönlichen Benutzerkennung in den Kommandovorrat aufgenommen werden (z.B. diverse BCAM-Kommandos über das Privileg NET-ADMINISTRATION).

Die Vereinigungsmenge der Privilegien kann mit folgendem Kommando angezeigt werden:

```
/SHOW-PRIVILEGE INFORMATION = *RUN-PRIVILEGE(…)
```

DIALOG-ACCESS = *NO
Die Zugangsklasse DIALOG ist für diese Benutzerkennung gesperrt.

BATCH-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert, ob und welche Zugangskontrollen im Batchbetrieb wirksam sein sollen.

BATCH-ACCESS = *YES(...)
Definiert die im Batchbetrieb wirksamen Zugangskontrollen.

PASSWORD-CHECK = *YES / *NO / *GUARD(...)
Legt fest, ob für Batchaufträge eine Kennwortprüfung stattfindet.

PASSWORD-CHECK = *GUARD(...)
Das Recht, Batchaufträge ohne Kennwort zu starten, wird über ein Guard verwaltet.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Batchaufträge dürfen ohne Kennwort gestartet werden, wenn für die aufrufende Benutzerkennung die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards sind zwei Fälle zu unterscheiden:
- Wurde der Batchauftrag im BS2000 angefordert, werden alle Bedingungen berücksichtigt. Subjekt der Zugriffsbedingung ist die Benutzerkennung, unter der das Kommando ENTER-JOB eingegeben wurde.
- Wurde der Batchauftrag unter POSIX angefordert, werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

USER-ACCESS =
Legt fest, von welchen Benutzerkennungen auf dieser Benutzerkennung Batchaufträge gestartet werden dürfen.

Bei gleichzeitiger Angabe der Operanden USER-ACCESS und GUARD-NAME beachten Sie bitte den Hinweis beim Operanden GUARD-NAME auf Seite 258.

USER-ACCESS = *ALL
Von allen Benutzerkennungen und Bedienstationen dürfen Batchaufträge gestartet werden.

USER-ACCESS = *OWNER
Von der unter USER-IDENTIFICATION angegebenen Benutzerkennung selbst dürfen Batchaufträge gestartet werden.

USER-ACCESS = *GROUP
Von allen zur Gruppe der USER-IDENTIFICATION gehörigen Benutzerkennungen (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung selbst) dürfen Batchaufträge auf dieser Benutzerkennung gestartet werden.

USER-ACCESS = *OTHERS
Von allen Benutzerkennungen des Rechners (ohne die unter USER-IDENTIFICATION angegebene Benutzerkennung und deren Benutzergruppe) dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

USER-ACCESS = *CONSOLE
Von einem Operator ohne eigene Benutzerkennung dürfen auf dieser Benutzerkennung Batchaufträge gestartet werden.

USER-ACCESS = <name 1..8>
Von allen angegebenen Benutzerkennungen dürfen Batchaufträge unter der Benutzerkennung gestartet werden.

GUARD-NAME =
Gibt an, ob der Batch-Zugang zu einer Benutzerkennung mit einem Guard geschützt wird.

Hinweis

Bei gleichzeitiger Angabe der Operanden USER-ACCESS (≠*ALL) und GUARD-NAME (≠*NONE) ist Folgendes zu beachten:

Die Prüfung der Benutzerkennung des Aufrufers erfolgt zunächst anhand der User-Access-Liste. Gewährt diese den Zugang, wird das Guard nicht mehr überprüft. Eventuell widersprechende Angaben im Guard bleiben unberücksichtigt. Nur falls die Prüfung der User-Access-Liste das Ergebnis „Kein Zugang“ liefert, findet eine Prüfung des Guards statt. Das Ergebnis dieser Prüfung entscheidet dann, ob ein Zugang zum aktuellen Zeitpunkt erlaubt ist oder nicht.

GUARD-NAME = *NONE
Der Batch-Zugang zur Benutzerkennung wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Batch-Zugang zur Benutzerkennung ist nur erlaubt, wenn für die aufrufende Benutzerkennung die Zugriffsbedingungen im angegebenen Guard erfüllt sind.

Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards sind zwei Fälle zu unterscheiden:

– Wurde der Batchauftrag im BS2000 angefordert, werden alle Bedingungen berücksichtigt. Subjekt der Zugriffsbedingung ist die Benutzerkennung, unter der das Kommando ENTER-JOB eingegeben wurde.

– Wurde der Batchauftrag unter POSIX angefordert, werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

BATCH-ACCESS = *NO
Die Zugangsklasse BATCH ist für die Benutzerkennung gesperrt.

OPERATOR-ACCESS-TERM = *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert die im Operator-Betrieb für einen über Terminal angeschlossenen Dialogpartner wirksamen Authentisierungsverfahren. Die Möglichkeiten der Operator-Authentisierung sind detailliert im Handbuch „Einführung in die Systembetreuung“ [2] beschrieben.

OPERATOR-ACCESS-TERM = *YES(...)
Die Zugangsklasse Operating-Betrieb ist für diese Kennung erlaubt.

PASSWORD-CHECK = *YES / *NO
Legt fest, ob im Operating-Betrieb eine Kennwortprüfung stattfindet oder nicht.

OPERATOR-ACCESS-TERM = *NO
Die Zugangsklasse Operating-Betrieb ist für diese Kennung gesperrt.

OPERATOR-ACCESS-PROG = *LOGON-DEFAULT(...) / *YES(...) / *NO
Definiert die im Operating-Betrieb für programmierte Operator (PROP-XT) wirksamen Authentisierungsverfahren.

OPERATOR-ACCESS-PROG = *YES(...)

PASSWORD-CHECK = *YES / *NO
Legt fest, ob für den programmierten Operator eine Kennwortprüfung stattfindet oder nicht.

OPERATOR-ACCESS-PROG = *NO
Die Zugangsklasse OPERATOR-ACCESS-PROGRAM ist für den programmierten Operator gesperrt.

OPERATOR-ACCESS-CONS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Bestimmt, ob unter dieser Benutzerkennung ein Zugang an der physikalischen Konsole im inkompatiblen Modus erlaubt ist.

OPERATOR-ACCESS-CONS = *YES(...)

PASSWORD-CHECK = *YES / *NO
Legt fest, ob beim Konsol-Zugang eine Kennwortprüfung stattfindet.

OPERATOR-ACCESS-CONS = *NO
Es ist kein Konsol-Zugang möglich.

POSIX-RLOGIN-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Die Zugangsklassen-Attribute für POSIX-Remote-Login können festgelegt werden.

POSIX-RLOGIN-ACCESS = *YES(...)
Die BS2000-Benutzerkennung ist für den Systemzugang über POSIX-Remote-Login offen.

PASSWORD-CHECK = *YES / *NO
Legt fest, ob beim Zugang über POSIX-Remote-Login eine Kennwortprüfung stattfindet.

TERMINAL-SET =
Angabe, ob die Kennung für den Zugang über POSIX-Remote-Login mit Terminal-Sets geschützt wird.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein POSIX-Remote-Login erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. POSIX-Remote-Login ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über POSIX-Remote-Login verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über POSIX-Remote-Login erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD

Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME =
Gibt an, ob der Zugang über POSIX-Remote-Login mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Zugang über POSIX-Remote-Login wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang über POSIX-Remote-Login ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

POSIX-RLOGIN-ACCESS = *NO
Die BS2000-Benutzerkennung ist für den Systemzugang über POSIX-Remote-Login gesperrt.

POSIX-REMOTE-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Die BS2000-Benutzerkennung wird für den Systemzugang über ein POSIX-Remote-Kommando geöffnet oder gesperrt.

TERMINAL-SET =
Angabe, ob die Kennung für den Zugang über ein POSIX-Remote-Kommando mit Terminal-Sets geschützt wird.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Zugang über ein POSIX-Remote-Kommando erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. der Zugang über ein POSIX-Remote-Kommando ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über ein POSIX-Remote-Kommando verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den UNIX-Clients mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Zugang über ein POSIX-Remote-Kommando erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD

Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME =
Gibt an, ob der Zugang über ein POSIX-Remote-Kommando mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Zugang über ein POSIX-Remote-Kommando wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Zugang über ein POSIX-Remote-Kommando ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die UNIX/POSIX-Benutzerkennung, unter der das Kommando `rsh` bzw. `rcp` eingegeben wurde. Es ist nicht notwendig, dass diese Kennung im BS2000 existiert.

POSIX-REMOTE-ACCESS = *NO
Die BS2000-Benutzerkennung ist für den Systemzugang über ein POSIX-Remote-Kommando gesperrt.

NET-DIALOG-ACCESS = *LOGON-DEFAULT(...) / *YES(...) / *NO
Angabe, ob der Dialogzugang aus dem Netzwerk erlaubt ist.

NET-DIALOG-ACCESS = *YES(…)
Der Dialogzugang aus dem Netzwerk ist zugelassen.

PASSWORD-CHECK = *YES / *NO
Legt fest, ob beim Netzwerk-Zugang die Prüfung des Logon-Kennwortes stattfinden soll.

PRINCIPAL =
Angabe, ob der Zugang unter Nutzung der Kerberos-Authentisierung erlaubt ist.

PRINCIPAL = *NO-PROTECTION
Für diese Benutzerkennung ist keine Kerberos-Authentisierung vorgesehen. Der Client wird nicht zur Vorlage eines Kerberos-Tickets aufgefordert, sondern der Zugang direkt der Klasse DIALOG-ACCESS zugeordnet.

PRINCIPAL = *NONE
Die Liste der Kerberos-Namen wird leer angelegt, der Netzwerkzugang ist ausgeschlossen.

PRINCIPAL = *ALL
Für diese Benutzerkennung ist keine Kerberos-Authentisierung vorgesehen. Der Client wird aber zur Vorlage eines Kerberos-Tickets aufgefordert. Der darin enthaltene Kerberos-Name wird in der Logon-History angezeigt und als Audit-Identifikation verwendet. Unterstützt der Client keine Kerberos-Authentisierung, wird der Zugang der Klasse DIALOG-ACCESS zugeordnet.

PRINCIPAL = list-poss(48): <composed-name 1..1800 with-under with-wild> / <c-string 1..1800 with-low>
Gibt die Liste der Kerberos-Namen der Clients an, die zu dieser Benutzerkennung Zugang haben, wenn sie über ein gültiges Kerberos-Ticket verfügen. Unterstützt der Client keine Kerberos-Authentisierung wird der Zugang der Klasse DIALOG-ACCESS zugeordnet. Die Prüfung des Kerberos-Namens berücksichtigt nicht die Groß- und Kleinschreibung. Bei der Prüfung werden Wildcard-Zeichen ausgewertet. Einzelne Wildcard-Zeichen können im Format <c-string> durch Voranstellen des Zeichens '\' entwertet werden.

TERMINAL-SET =
Angabe, ob die Kennung für den Netzwerkzugang mit Terminal-Sets geschützt wird.

TERMINAL-SET = *NO-PROTECTION
Die Kennung wird nicht mit Terminal-Sets geschützt.

TERMINAL-SET = *NONE
Der Kennung wird eine leere Terminal-Set-Liste zugewiesen, d.h. es ist kein Netzwerkzugang erlaubt.

TERMINAL-SET = *EXCEPTION-LIST(...)
Es wird eine Negativliste von Terminal-Sets zugewiesen.

TERMINAL-SET = *NONE / list-poss(48): <name 1..8>(…)
Die Negativliste ist leer, d.h. der Netzwerkzugang ist uneingeschränkt erlaubt.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Netzwerkzugang verboten.

Die Bedeutung der untergeordneten Operanden ist wie beim folgenden Operanden TERMINAL-SET.

TERMINAL-SET = list-poss(48): <name 1..8>(…)
Es wird eine Positivliste von Terminal-Sets zugewiesen. Den Datensichtstationen mit den Namen, die auf die Datensichtstationsnamen in den angegebenen Terminal-Sets passen, wird der Netzwerkzugang erlaubt.

SCOPE =
Klasse des Terminal-Set Namens.

SCOPE = *STD

Ein systemglobaler Benutzerverwalter weist standardmäßig globale, ein Gruppenverwalter lokale Terminal-Sets zu.

SCOPE = *USER
Es wird ein Terminal-Set aus dem Eigentum der Benutzerkennung zugewiesen.

SCOPE = *GROUP
Es wird ein Terminal-Set aus dem Eigentum der Gruppe der Benutzerkennung zugewiesen.

SCOPE = *SYSTEM
Es wird ein Terminal-Set aus gemeinschaftlichem Eigentum zugewiesen.

GUARD-NAME =
Gibt an, ob der Netzwerkzugang mit einem Guard geschützt wird.

GUARD-NAME = *NONE
Der Netzwerkzugang wird nicht mit einem Guard geschützt.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Der Netzwerkzugang ist nur erlaubt, wenn die Zugriffsbedingungen im angegebenen Guard erfüllt sind. Die geschützte Benutzerkennung muss berechtigter Benutzer des angegebenen Guards sein. Bei der Auswertung des Guards werden nur die Zeitbedingungen Date, Time und Weekday berücksichtigt. Subjekt der Zugriffsbedingung ist die geschützte Benutzerkennung.

NET-DIALOG-ACCESS = *NO
Die BS2000-Benutzerkennung ist für den Netzwerkzugang gesperrt.

Hinweis

Das Zusammenspiel mit dem Kommando /ADD-USER kann durch den Operanden LOCK-USER dieser Kommandos erfolgen:

Beim Eintragen des Benutzers kann dieser mit LOCK-USER=*YES gesperrt werden, um LOGON-Versuche bis zur Eingabe des Kommandos /SET-LOGON-PROTECTION zu verhindern. Nach Vereinbarung von Schutzattributen kann die Benutzerkennung mit /UNLOCK-USER freigegeben werden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel

```
/set-logon-protection tsos, -
/    password=parameters(logon-password=?xyzabcde?,lifetime=60),-
/    dialog-access=*yes(terminal-set=area52)
```

Damit muss TSOS sein Kennwort spätestens alle 60 Tage wechseln. Zugang im Dialogbetrieb ist nur von den im Terminal-Set AREA52 angegebenen Terminals möglich. Batchaufträge dürfen nur von Benutzeraufträgen gestartet werden, die ihrerseits unter TSOS laufen.

```
/set-logon-protection xy, -
/     password=(logon-password=secret, -
/                minimal-length=8, -
/                minimal-complexity=4)
```

Der Benutzer XY darf nur Kennwörter vergeben, die mindestens 8 Zeichen lang sind und mindestens je einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten (siehe Erläuterung zu MINIMAL-COMPLEXITY=4).

SET-PERSONAL-ATTRIBUTES
Persönliche Identifizierung angeben

Anwendungsbereich: JOB

Privilegierung: alle Privilegien

Mit diesem Kommando wird die persönliche Identifizierung durchgeführt, falls im Kommando /SET-LOGON-PROTECTION oder /MODIFY-LOGON-PROTECTION der Operand PERSONAL-LOGON=*YES gesetzt wurde.

SET-PERSONAL**-ATTR**IBUTES
USER-IDENTIFICATION = ***SAME** / <name 1..8> ,**PASS**WORD = ***NONE** / ***SECRET** / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>

USER-IDENTIFICATION = <name 1..8>
Persönliche Benutzerkennung.

USER-IDENTIFICATION = *SAME
Die Logon-Benutzerkennung soll als persönliche Benutzerkennung angenommen werden. Dieser Wert ist nur erlaubt, wenn für die Logon-Benutzerkennung ein Kennwort und im Kommando /SET- oder /MODIFY-LOGON-PROTECTION für den Dialog-Zugang PASSWORD-CHECK=*NO vereinbart ist. Bei PASSWORD-CHECK=*YES müssen persönliche und Logon-Benutzerkennung voneinander verschieden sein.

PASSWORD = *NONE / *SECRET / <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
Kennwort der persönlichen Benutzerkennung.
Die Eingabe eines „langen“ Kennworts (entspricht <c-string 9..32>) wird unterstützt. Ein Hash-Algorithmus konvertiert das „lange“ Kennwort in ein 8 Byte langes Kennwort, das zur Kennwortüberprüfung verwendet wird. Zur Vereinbarung „langer“ Kennwörter siehe Funktionsbeschreibung.
Der Operand PASSWORD ist als „geheim“ definiert:
- Der eingegebene Wert wird nicht protokolliert.
- Im geführten Dialog ist das Eingabefeld automatisch dunkelgesteuert.
- Die Angabe *SECRET oder ^ ermöglicht im ungeführten Dialog und in Vordergrundprozeduren die verdeckte Eingabe des gewünschten Wertes. SDF fordert zur Eingabe des „geheimen“ Wertes auf und stellt ein dunkelgesteuertes Eingabefeld zur Verfügung.

SET-PRIVILEGE
Systemglobale Privilegien vergeben

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Vergibt systemglobale Privilegien an eine Benutzerkennung.

Einer Kennung, die auf dem im Kommando angegebenen Pubset das Privileg SECURITY-ADMINISTRATION besitzt, kann kein Privileg oder Sammelprivileg zugewiesen werden.

Wird das Kommando für eine Benutzerkennung auf dem Home-Pubset gegeben, so wird diese Änderung auch im System wirksam, d.h. nur dann kann die Benutzerkennung über den mit dem Privileg verknüpften Rechteumfang verfügen.

Die Änderung wirkt sich nicht auf aktive Benutzeraufträge unter der Benutzerkennung aus, sondern wird erst nach dem nächsten LOGON unter der Benutzerkennung wirksam.

```
SET-PRIVILEGE

 PRIVILEGE = *PRIVILEGE-SET(...) / list-poss(64): <text>

    *PRIVILEGE-SET(...)

       | PRIVILEGE-SET-NAME = list-poss(20): <name 1..8>

,USER-IDENTIFICATION = <name 1..8>

,PUBSET = *HOME / <cat-id 1..4>
```

PRIVILEGE =
Privileg, das an eine Benutzerkennung vergeben werden soll. Der Operand muss angegeben werden. Es können Einzelprivilegien oder die Namen von Sammelprivilegien angegeben werden. Die Einzelprivilegien sind ab Seite 40 beschrieben.

PRIVILEGE = *PRIVILEGE-SET(...)
Angabe eines oder mehrerer Sammelprivilegien.

PRIVILEGE-SET-NAME = list-poss(20): <name 1..8>
Sammelprivileg, das an die Benutzerkennung vergeben werden soll, bzw. Liste der Sammelprivilegien.

PRIVILEGE = list-poss(64): <text>
Privileg, das an eine Benutzerkennung vergeben werden soll. Mögliche Privilegien siehe Seite 128. Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

USER-IDENTIFICATION = <name 1..8>
Benutzerkennung, die das angegebene Privileg erhalten soll.

PUBSET = *HOME / <cat-id 1..4>
Pubset, auf dem das angegebene Recht für die Benutzerkennung eingetragen werden soll.

PUBSET = *HOME
Der Eintrag erfolgt auf dem Home-Pubset. Die vergebene Berechtigung wird im System wirksam!

PUBSET = <cat-id 1..4>
Der Eintrag erfolgt auf dem angegebenen Pubset.

Hinweise

– Das Privileg USER-ADMINISTRATION kann nicht (weder als Einzel- noch als Sammelprivileg) an eine Benutzerkennung vergeben werden, die auf dem im Operanden PUBSET angegebenen Pubset bereits Gruppenverwalter ist.

– Wird das Privileg SAT-FILE-MANAGEMENT oder ein Sammelprivileg, dem das Privileg SAT-FILE-MANAGEMENT zugeordnet ist, an eine Benutzerkennung vergeben, so wird für diese Kennung die SAT-Protokollierung eingeschaltet und gilt bezüglich einer Änderung der Protokolliereinstellung als „nicht schaltbar“ (siehe Handbuch „SECOS - Security Control System - Beweissicherung“ [1]).

– Wird das Privileg SAT-FILE-EVALUATION oder ein Sammelprivileg, dem das Privileg SAT-FILE-EVALUATION zugeordnet ist, an eine Benutzerkennung vergeben, so wird für diese Kennung die SAT-Protokollierung eingeschaltet. Die SAT-Protokollierung kann für diese Kennung wieder abgeschaltet werden, sofern SAT-FILE-EVALUATION das einzige Privileg ist, welches eine SAT-Protokollierung auslöst.

– Das Privileg SAT-FILE-MANAGEMENT oder ein Sammelprivileg, dem das Privileg SAT-FILE-MANAGEMENT zugeordnet ist, kann nicht an die Kennung TSOS vergeben werden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

SHOW-KEYTAB-ENTRY
Key-Tabellen-Eintrag anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Mit diesem Kommando kann der Sicherheitsbeauftragte (standardmäßig die Benutzerkennung SYSPRIV) Einträge der Key-Tabelle anzeigen.

```
SHOW-KEYTAB-ENTRY

 ENTRY-IDENTIFICATION = *STD / *ALL / list-poss(20): *STD / *SYSTEM-DEFAULT /
                        <name 1..8 with-wild(32)>
,PUBSET = *ALL / list-poss(2000): *HOME / <cat-id 1..4>
,SELECT = *ALL / *BY-ATTRIBUTES(…)
    *BY-ATTRIBUTES(…)
      | PRINCIPAL = *ANY / <c-string 1..1800 with-low>
,INFORMATION = *ALL / *ATTRIBUTES
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
```

ENTRY-IDENTIFICATION = *STD / *ALL /
list-poss(20): *STD / *SYSTEM-DEFAULT / <name 1..8 with_wild(32)>
Identifikation des Eintrags, der angezeigt werden soll.

ENTRY-IDENTIFICATION = *ALL
Alle Einträge werden angezeigt.

PUBSET = *ALL / list-poss(2000): *HOME / <cat-id 1..4>
Katalogkennung des Pubsets, aus deren Benutzerkatalogen die Schlüssel angezeigt werden. Im laufenden Betrieb sind die Schlüssel des Home-Pubsets maßgebend.

SELECT =
Angabe von Kriterien, nach dem die anzuzeigenden Einträge ausgewählt werden.

SELECT = *ALL
Einträge werden unabhängig von zusätzlichen Kriterien angezeigt.

SELECT = *BY-ATTRIBUTES(…)
Einträge werden nur angezeigt, wenn sie das nachfolgend angegebene Kriterium erfüllen.

PRINCIPAL = *ANY / <c-string 1..1800 with-low>
Kerberos-Name des BS2000-Rechners, dessen Eintrag angezeigt werden soll. Im Namen befindliche Wildcard-Zeichen werden berücksichtigt, falls sie nicht durch Voranstellen des Zeichens '\' entwertet werden.

INFORMATION =
Legt den Ausgabeumfang fest.

INFORMATION = *ALL
Die Attribute werden zusammen mit den Kerberos-Schlüsseln ausgegeben.

INFORMATION = *ATTRIBUTES
Nur die Attribute werden ausgegeben, ohne die Kerberos-Schlüssel.

OUTPUT =
Definiert das Ausgabemedium für die Information.

OUTPUT = *SYSOUT
Es wird auf die Systemdatei SYSOUT (im Dialog die Datensichtstation) ausgegeben.

OUTPUT = *SYSLST
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *ALL INFORMATION = *ATTRIBUTES	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Einheit der Gültigkeitsdauer veralteter Schlüssel	var(*LIST).DIM	S	*DAYS *HOURS *MINUTES	1, 2
Entry-ID	var(*LIST).ENTRY-ID	S	<name 1..8>	1, 2
Erstellungsdatum der Schlüssel	var(*LIST).KEY(*LIST).DATE	S	<date 10>	1
Schlüssel	var(*LIST).KEY(*LIST).NAME	S	<name 1..32>	1

(Teil 1 von 2)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
System-Default	var(*LIST).KEY(*LIST).SYS-DEF	S	*NO *YES	1, 2
Erstellungszeit der Schlüssel	var(*LIST).KEY(*LIST).TIME	S	<time 8>	1
Schlüsselversion	var(*LIST).KEY(*LIST).VERSION	I	<integer 0.. 2147483647>	1
Gültigkeitsdauer veralteter Schlüssel	var(*LIST).KEY-OVERLAP	I	<integer 0..32767>	1, 2
Gültigkeit veralteter Schlüssel	var(*LIST).KEY-OVERLAP-DEFI	S	*NO *UNLIMITED *LIMITED	1, 2
Principal	var(*LIST).PRINCIPAL	S	<name 1..1800>	1, 2
Pubset	var(*LIST).PUBSET	S	<catid 1..4>	1, 2

(Teil 2 von 2)

Beispiel: Ausgabe eine Key-Tabellen-Eintrags in S-Variablen

```
/exec-cmd (show-keytab-entry),s-out=ops
/show-var var,inf=*par(value=*c-literal)

OPS(*LIST).ENTRY-ID = '*STD'
OPS(*LIST).PUBSET = 'A'
OPS(*LIST).PRINCIPAL = 'host/bs2osd.domain.de@REALM.DOMAIN.DE'
OPS(*LIST).KEY-OVERLAP-DEFI= '*LIMITED'
OPS(*LIST).KEY-OVERLAP = 5
OPS(*LIST).DIM = '*MINUTES'
OPS(*LIST).KEY(*LIST).NAME = 'DES-CBC-CRC'
OPS(*LIST).KEY(*LIST).VERSION = 0
OPS(*LIST).KEY(*LIST).DATE = '2018-01-30'
OPS(*LIST).KEY(*LIST).TIME = '09:48:17'
*END-OF-VAR
OPS(*LIST).KEY(*LIST).NAME = 'DES-CBC-MD5'
OPS(*LIST).KEY(*LIST).VERSION = 0
OPS(*LIST).KEY(*LIST).DATE = '2018-01-30'
OPS(*LIST).KEY(*LIST).TIME = '09:48:17'
*END-OF-VAR
OPS(*LIST).KEY(*LIST).NAME = 'DES3-CBC-MD5'
OPS(*LIST).KEY(*LIST).VERSION = 0
OPS(*LIST).KEY(*LIST).DATE = '2018-01-30'
OPS(*LIST).KEY(*LIST).TIME = '09:48:17'
*END-OF-VAR
OPS(*LIST).KEY(*LIST).NAME = 'ARCFOUR-HMAC-MD5'
OPS(*LIST).KEY(*LIST).VERSION = 0
OPS(*LIST).KEY(*LIST).DATE = '2018-01-30'
OPS(*LIST).KEY(*LIST).TIME = '09:48:17'
*END-OF-VAR
*END-OF-VAR
```

SHOW-LOGON-DEFAULTS
Standardwerte für Schutzattribute anzeigen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: USER-ADMINISTRATION

Mit diesem Kommando kann der systemglobale Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) die Standard-Schutzattribute für die Zugangskontrolle anzeigen, die mit /SET- oder /MODIFY-LOGON-DEFAULTS festgelegt wurden.

SHOW-LOGON-DEFAULTS
PUBSET = ***ALL** / list-poss(2000): ***HOME** / <cat-id 1..4> **,OUT**PUT = list-poss(2): ***SYSOUT** / ***SYSLST**

PUBSET = *ALL / list-poss(2000): *HOME / <cat-id 1..4>
Angabe der Pubsets, in deren Benutzerkatalogen sich die Standard-Attribute der Zugangskontrolle befinden.

PUBSET = *ALL
Alle angeschlossenen Pubsets werden ausgewertet.

PUBSET = *HOME
Ausgewertet wird der Benutzerkatalog des Home-Pubset.

PUBSET = <cat-id 1..4>
Ausgewertet wird der Benutzerkatalog des angegebenen Pubset.

OUTPUT =
Definiert das Ausgabemedium für die Information.

OUTPUT = *SYSOUT
Es wird auf die Systemdatei SYSOUT (im Dialog die Datensichtstation) ausgegeben.

OUTPUT = *SYSLST
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel: Ausgabe der Standard-Schutzattribute

```
/show-logon-defaults

LOGON DEFAULT PROTECTION ON PUBSET A
 EXPIRATION DATE:     180 DAYS          EXPIRATION WARNING:  30
 PASSWORD:
     MANAGEMENT:      USER CHANGE ONLY
     MINIMAL LENGTH:  2                 MINIMAL COMPLEXITY:  1
     LIFETIME:        90  DAYS          INITIAL LIFETIME:    3   DAYS
     UNLOCK EXPIR:    BY USER           EXPIRATION WARNING:  15
     PASSWORD MEMORY: YES
     PERIOD:          7     DAYS
     CHANGES/PERIOD:  10
     BLOCKING TIME:   56    DAYS
 SUSPEND:             YES
     COUNT:           5                 OBSERVE TIME:        15    MINUTES
     SUBJECT:         USERID            SUSPEND TIME:        30    MINUTES
 INACTIVITY:          YES
     LIFETIME:        12  MONTHS
 DIALOG ACCESS:       YES
 BATCH ACCESS:        YES
 OPERATOR ACCESS TERM:YES
 OPERATOR ACCESS PROG:YES
 OPERATOR ACCESS CONS:YES
 POSIX RLOGIN ACCESS: YES
 POSIX REMOTE ACCESS: YES
 NET DIALOG ACCESS:   YES
```

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Zugangskontrolle im Batch-Betrieb aktiv	var(*LIST).BATCH.ACCESS	S	*NO *YES	
Zugangskontrolle im Dialog-Betrieb aktiv	var(*LIST).DIALOG.ACCESS	S	*NO *YES	
Verfallsdatum der Benutzerkennung	var(*LIST).EXPIR-DATE	S	*NONE <integer 0..366>	
Dimension des Verfallsdatums der Benutzerkennung	var(*LIST).EXPIR-DIM	S	” *DAYS	
Zeitangabe (in Tagen), ab der eine Verfallswarnung für die Benutzerkennung ausgegeben wird	var(*LIST).EXPIR-WARN	I	<integer 0..366>	
Dimension des Inaktivitätslimit	var(*LIST).INACTIVITY.DIM	S	” *DAYS *MONTHS	
Inaktivitätslimit	var(*LIST).INACTIVITY.LIFETIME	I	<integer 1..366>	
Inaktivitätslimit aktiv	var(*LIST).INACTIVITY.PAR	S	*NO *YES	
Zugangskontrolle im Network-Dialog-Betrieb aktiv	var(*LIST).NET-DIALOG.ACCESS	S	*YES *NO	
Zugangskontrolle beim Konsol-Zugang aktiv	var(*LIST).OPER-CONS.ACCESS	S	*YES *NO	
Authentisierungsverfahren für programmierten Operator wirksam (Operating-Betrieb)	var(*LIST).OPER-PROG.ACCESS	S	*NO *YES	
Authentisierungsverfahren für via Terminal angeschlossenen Dialogpartner wirksam (Operating-Betrieb)	var(*LIST).OPER-TER.ACCESS	S	*NO *YES	
Sperrdauer für Kennwörter	var(*LIST).PASS.BLOCKING-TIME	I	<integer 1..32767>	
Anzahl der erlaubten Kennwortänderungen	var(*LIST).PASS.CHA-PER-PER	I	<integer 1..100>	
Dimension der Kennwort-Lebensdauer	var(*LIST).PASS.DIM	S	” *DAYS *MONTHS	
Zeitangabe (in Tagen), ab der eine Verfallswarnung für das Kennwort ausgegeben wird	var(*LIST).PASS.EXPIR-WARN	I	<integer 1..366>	
Dimension der ersten Kennwort-Lebensdauer	var(*LIST).PASS.INIT-DIM	S	” *DAYS	

(Teil 1 von 2)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Erste Lebensdauer des Kennwortes	var(*LIST).PASS.INIT-LIFETIME	S	*STD <integer 1..366>	
Lebensdauer des Kennwortes	var(*LIST).PASS.LIFETIME	S	*UNLIM <integer 1..366>	
Berechtigte zur Verwaltung des Kennwortes	var(*LIST).PASS.MANAGE	S	*BY-ADM *BY-USER *USER-CHA-ONLY	
Minimale Komplexität des Kennwortes	var(*LIST).PASS.MIN-COMPLEX	S	*NONE <integer 1..4>	
Minimale Länge des Kennwortes	var(*LIST).PASS.MIN-LEN	S	*NONE <integer 1..8>	
Liste der Kennwortänderungen aktiv	var(*LIST).PASS.PASS-MEMORY	S	*NO *YES	
Zeitraum in Tagen, für den die Beschränkung der Anzahl von Kennwortänderungen gilt	var(*LIST).PASS.PER	I	<integer 1..32767>	
Erlaubnis zum Ersetzen eines abgelaufenen Kennworts	var(*LIST).PASS.UNLOCK-EXPIR	S	*BY-ADM *BY-USER	
Zugangskontrolle beim POSIX-Remote-Zugang aktiv	var(*LIST).POSIX-REM.ACCESS	S	*YES *NO	
Zugangskontrolle beim POSIX-Zugang über rlogin aktiv?	var(*LIST).POSIX-RLOG.ACCESS	S	*NO *YES	
Katalogkennung des Pubsets	var(*LIST).PUBSET	S	<cat-id 1..4>	
Erlaubte Anzahl von Fehlversuchen	var(*LIST).SUSPEND.COUNT	I	<integer 0..32767>	
Dimension der Beobachtungszeit	var(*LIST).SUSPEND.OBS-DIM	S	'' *MINUTES *HOURS	
Beobachtungszeit	var(*LIST).SUSPEND.OBS-TIME	I	<integer 0..32767>	
Suspendierung aktiv	var(*LIST).SUSPEND.PAR	S	*NO *YES	
Zu suspendierendes Subjekt	var(*LIST).SUSPEND.SUBJECT	S	*USER-ID *INITIATOR	
Dimension der Suspendierungszeit	var(*LIST).SUSPEND.SUS-DIM	S	'' *MINUTES *HOURS	
Suspendierungszeit	var(*LIST).SUSPEND.SUS-TIME	I	<integer 0..32767>	

(Teil 2 von 2)

SHOW-LOGON-PROTECTION
Schutzattribute anzeigen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, SECURITY-ADMINISTRATION, USER-ADMINISTRATION

Zeigt die Schutzattribute oder die Zugangshistorie von Benutzerkennungen an.

Es dürfen dabei angegeben werden:

– vom systemglobalen Benutzerverwalter (USER-ADMINISTRATION) alle Benutzerkennungen auf allen Pubsets

– vom Gruppenverwalter alle ihm zu- und untergeordneten Benutzerkennungen des angesprochenen Pubset

– von jedem anderen Benutzer nur seine eigene Benutzerkennung

Falls USER-ID=*ALL angegeben ist, wird jedem Benutzer die Information ausgegeben, die ihm nach den oben genannten Regeln zugänglich ist.

SHOW-LOGON-PROTECTION Kurzname: **SHLGPT**

USER-IDENTIFICATION = ***ALL** / list-poss(48): ***OWN** / <name 1..8 with-wild(32)>
,PUBSET = ***ALL** / list-poss(2000): ***HOME** / <cat-id 1..4>
,OUTPUT = list-poss(2): ***SYSOUT** / ***SYSLST**
,INFORMATION = ***ATTR**IBUTES(...) / ***LOGON-HIST**ORY(...)
***ATTR**IBUTES(...)
SCOPE = ***LOGON-DEF**AULT / ***USER-ID**ENTIFICATION / ***ALL**
***LOGON-HIST**ORY(...)
ACCESS-TYPE = ***ALL** / list-poss(6): ***DIALOG** / ***BATCH** / ***POSIX** / ***OPER**ATOR / ***FT**
,RESULT = ***ALL** / ***ACCEPT**ED / ***LAST-ACCEPT**ED / ***REJECT**ED
,SORT-LIST = ***BY-DATE-AND-TIME** / ***BY-ACCESS-TYPE**
,LINES = ***STD** / <integer 1..40>
,PRINCIPAL = ***SHORT** / ***FULL**

USER-IDENTIFICATION = *ALL / list-poss(48): *OWN / <name 1..8 with-wild>
Benutzerkennungen, deren vereinbarte Schutzattribute oder Zugangshistorie angezeigt werden sollen.

PUBSET = *ALL / list-poss(2000): *HOME / <cat-id 1..4>
Pubset, dessen Benutzerkatalog ausgewertet werden soll.

PUBSET = *ALL
Alle angeschlossenen Pubsets werden ausgewertet.

PUBSET = *HOME
Ausgewertet wird der Benutzerkatalog des Home-Pubset.

PUBSET = <cat-id 1..4>
Ausgewertet wird der Benutzerkatalog des angegebenen Pubset.

OUTPUT =
Definiert das Ausgabemedium für die Information.

OUTPUT = *SYSOUT
Es wird auf die Systemdatei SYSOUT (im Dialog die Datensichtstation) ausgegeben.

OUTPUT = *SYSLST
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

INFORMATION = *ATTRIBUTES(...) / *LOGON-HISTORY(...)
Legt den Ausgabeumfang fest.

INFORMATION = *ATTRIBUTES(...)
Die Schutzattribute werden ausgegeben.

SCOPE =
Gibt an, welche Schutzattribute ausgegeben werden.

SCOPE = *LOGON-DEFAULT
Die aktuell wirksamen Schutzattribute für die Zugangskontrolle werden angezeigt.

Die Ausgabe zeigt neben den Attributen, die explizit für die Benutzerkennung festgelegt wurden, die aktuellen Standard-Attribute für die Zugangskontrolle, soweit sie für die Benutzerkennung gelten.

SCOPE = *USER-IDENTIFICATION
Es wird angezeigt, für welche Attribute die Standard-Attribute für die Zugangskontrolle gelten und welche Attribute explizit für die Benutzerkennung festgelegt wurden.

SCOPE = *ALL
Die Ausgabe zeigt neben den Attributen, die explizit für die Benutzerkennung festgelegt wurden, die aktuellen Standard-Attribute für die Zugangskontrolle, soweit sie für die Benutzerkennung gelten. Die Standard-Attribute sind durch einen Stern (*) gekennzeichnet.

INFORMATION = *LOGON-HISTORY(...)
Die Zugangshistorie wird ausgegeben (siehe auch Abschnitt „Protokollierung der Zugangsversuche“ auf Seite 118).

ACCESS-TYPE =
Auswahl der Zugangstypen, die protokolliert werden sollen.

ACCESS-TYPE = *ALL
Alle Zugangsversuche werden unabhängig von ihrem Typ protokolliert.

ACCESS-TYPE = list-poss(6): *DIALOG / *BATCH / *POSIX / *OPERATOR / *FT
Nur die Zugangsversuche des angegebenen Typs werden protokolliert: Dialog, Batch, POSIX, Operating und File-Transfer.

RESULT =
Steuert die Protokollierung in Abhängigkeit vom Resultat der Zugangsversuche.

RESULT = *ALL
Die Zugangsversuche werden unabhängig von ihrem Resultat protokolliert.

RESULT = *ACCEPTED
Die erfolgreichen Zugänge werden protokolliert.

RESULT = *LAST-ACCEPTED
Nur der letzte erfolgreiche Zugang jedes Zugangstyps wird protokolliert.

RESULT = *REJECTED
Die erfolglosen Zugangsversuche werden protokolliert.

SORT-LIST =
Angabe einer Sortierreihenfolge für die Protokollierung.

SORT-LIST = *BY-DATE-AND-TIME
Die Einträge werden in ihrer zeitlichen Reihenfolge protokolliert.

SORT-LIST = *BY-ACCESS-TYPE
Die Einträge werden nach Zugangstyp geordnet protokolliert. Die Reihenfolge der Zugangstypen ist: Dialog, Batch, POSIX, Operating und File-Transfer.

LINES =
Angabe, ob die Anzahl der auszugebenden Einträge beschränkt wird.

LINES = *STD
Die Anzahl der auszugebenden Einträge wird nicht beschränkt. Die Ausgabe kann durch Drücken der K2-Taste abgebrochen werden.

LINES = <integer 1..40>
Gibt die maximale Anzahl der auszugebenden Einträge an.

PRINCIPAL =
Länge der Anzeige des Kerberos-Namens in der Logon-History.

PRINCIPAL = *SHORT
Der Kerberos-Name wird in der Logon-History gekürzt angezeigt.

PRINCIPAL = *FULL
Der Kerberos-Name wird in der Logon-History in voller Länge zusammen mit dem Prozessor- und Stationsnamen des Terminals angezeigt.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiele: Ausgabe der Schutzattribute

```
/show-logon-protection user-identification=user1

 LOGON PROTECTION FOR USERID USER1    ON PUBSET A
 EXPIRATION DATE:     2019-01-27        EXPIRATION WARNING:  30
 PASSWORD:            YES
     MANAGEMENT:      USER CHANGE ONLY
     MINIMAL LENGTH:  2                 MINIMAL COMPLEXITY:  1
     LIFETIME:        90  DAYS          EXPIRATION DATE:     2018-10-29
     UNLOCK EXPIR:    BY USER           EXPIRATION WARNING:  15
     PASSWORD MEMORY: YES
     PERIOD:          7     DAYS
     CHANGES/PERIOD:  10                ACTUAL CHANGES:      1
     BLOCKING TIME:   56    DAYS        PASSWORDS BLOCKED:   1
 SUSPEND:             YES
     COUNT:           5                 OBSERVE TIME:        15    MINUTES
     SUBJECT:         USERID            SUSPEND TIME:        30    MINUTES
 INACTIVITY:          YES
     LIFETIME:        12  MONTHS        EXPIRATION DATE:     2019-07-31
 DIALOG ACCESS:       YES               PASSWORD CHECK:      YES
     TERMINAL NAME:   SEE LIST BELOW    CHIPCARD:            NO PROTECTION
     TERMINAL SET:    POSITIVE LIST
     LIST OF AUTHORIZED TERMINALS (PROCESSOR,STATION):
     (PROCESS1,STATION1)
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET1
     GUARD:           $TSOS.GUARD1
     PERSONAL LOGON:  NO
 BATCH ACCESS:        YES               PASSWORD CHECK:      GUARD
     CALLER USERID:   SEE LIST BELOW
     LIST OF AUTHORIZED USER IDENTIFICATIONS:
     USERID1
     GUARDS:
     PASSWORD CHECK:  $TSOS.GUARD2
     USER ACCESS:     $TSOS.GUARD3
 OPERATOR ACCESS TERM:YES               PASSWORD CHECK:      YES
     CHIPCARD:        NO PROTECTION
 OPERATOR ACCESS PROG:YES               PASSWORD CHECK:      YES
 OPERATOR ACCESS CONS:YES               PASSWORD CHECK:      YES
 POSIX RLOGIN ACCESS: YES               PASSWORD CHECK:      YES
     TERMINAL SET:    POSITIVE LIST
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET2
     GUARD:           $TSOS.GUARD4
 POSIX REMOTE ACCESS: YES
     TERMINAL SET:    POSITIVE LIST
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET3
     GUARD:           $TSOS.GUARD5
 NET DIALOG ACCESS:   YES               PASSWORD CHECK:      NO
     TERMINAL SET:    POSITIVE LIST
     PRINCIPAL:       SEE LIST BELOW
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET4
     LIST OF AUTHORIZED PRINCIPALS:
     ADMINISTRATOR@MYCOMPANY.NET
     GUARD:           $TSOS.GUARD6
```

```
/show-logon-protection user-identification=user1, -
/     information=*attributes(scope=*user-identification)

 LOGON PROTECTION FOR USERID USER1    ON PUBSET A
 EXPIRATION DATE:     LOGON-DEFAULT     EXPIRATION WARNING:  LOGON-DEFAULT
 PASSWORD:            YES
     MANAGEMENT:      LOGON-DEFAULT
     MINIMAL LENGTH:  LOGON-DEFAULT     MINIMAL COMPLEXITY:  LOGON-DEFAULT
     LIFETIME:        LOGON-DEFAULT     EXPIRATION DATE:     LOGON-DEFAULT
     UNLOCK EXPIR:    LOGON-DEFAULT     EXPIRATION WARNING:  LOGON-DEFAULT
     PASSWORD MEMORY: LOGON-DEFAULT
 SUSPEND:             LOGON-DEFAULT
     COUNT:           LOGON-DEFAULT     OBSERVE TIME:        LOGON-DEFAULT
     SUBJECT:         LOGON-DEFAULT     SUSPEND TIME:        LOGON-DEFAULT
 INACTIVITY:          LOGON-DEFAULT
 DIALOG ACCESS:       LOGON-DEFAULT     PASSWORD CHECK:      YES
     TERMINAL NAME:   SEE LIST BELOW    CHIPCARD:            NO PROTECTION
     TERMINAL SET:    POSITIVE LIST
     LIST OF AUTHORIZED TERMINALS (PROCESSOR,STATION):
     (PROCESS1,STATION1)
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET1
     GUARD:           $TSOS.GUARD1
     PERSONAL LOGON:  NO
 BATCH ACCESS:        LOGON-DEFAULT     PASSWORD CHECK:      GUARD
     CALLER USERID:   SEE LIST BELOW
     LIST OF AUTHORIZED USER IDENTIFICATIONS:
     USERID1
     GUARDS:
     PASSWORD CHECK:  $TSOS.GUARD2
     USER ACCESS:     $TSOS.GUARD3
 OPERATOR ACCESS TERM:LOGON-DEFAULT     PASSWORD CHECK:      YES
     CHIPCARD:        NO PROTECTION
 OPERATOR ACCESS PROG:LOGON-DEFAULT     PASSWORD CHECK:      YES
 OPERATOR ACCESS CONS:LOGON-DEFAULT     PASSWORD CHECK:      YES
 POSIX RLOGIN ACCESS: LOGON-DEFAULT     PASSWORD CHECK:      YES
     TERMINAL SET:    POSITIVE LIST
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET2
     GUARD:           $TSOS.GUARD4
 POSIX REMOTE ACCESS: LOGON-DEFAULT
     TERMINAL SET:    POSITIVE LIST
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET3
     GUARD:           $TSOS.GUARD5
 NET DIALOG ACCESS:   LOGON-DEFAULT     PASSWORD CHECK:      NO
     TERMINAL SET:    POSITIVE LIST
     PRINCIPAL:       SEE LIST BELOW
     LIST OF TERMINAL-SETS, SCOPE: SYSTEM
     TERMSET4
     LIST OF AUTHORIZED PRINCIPALS:
     ADMINISTRATOR@MYCOMPANY.NET
     GUARD:           $TSOS.GUARD6
```

Beispiel: Ausgabe der Zugangshistorie

```
/show-logon-protection user-identification=user1,information=*logon-history
```

```
Logon history for userid USER1    on pubset A
Date        Time      Type        Cnt  Result          TSN   Subject
2017-11-10  17:45:45  DIALOG        1  ACCEPT          0015  PROZESSO STATION
2017-11-10  17:45:38  NET-KRBROS    1  ACCEPT          0015  SYSADMIN@MYCOMPANY.NET
2017-11-10  17:45:27  BATCH         1  ACCEPT                TSOS     0015
2017-11-10  17:45:22  RLOGIN        1  ACCEPT                PROCPOSX
2017-11-10  17:45:18  POS-BATCH     1  ACCEPT                HUGO     0015
2017-11-10  17:45:12  POS-REMOTE    1  ACCEPT                PROCPOSX USER123
2017-11-10  17:45:03  FT            1  ACCEPT
2017-11-10  17:44:57  FT-NO-PASS    1  ACCEPT
2017-11-10  17:44:52  FT-BATCH      1  ACCEPT
```

Bedeutung der Ausgabe

Folgende Tabelle erläutert die Bedeutung der einzelnen Feldnamen:

Feldname	**Bedeutung**	
Date	Datum des letzten Zugangsversuches	
Time	Uhrzeit des letzten Zugangsversuches	
Type	Typ des Zugangs (siehe Tabelle „Typen der Zugangshistorie“ auf Seite 284)	
Cnt	Anzahl der Versuche (inkl. Fehlversuche)	
Result	erfolgreich / Grund der Ablehnung (siehe Tabelle „Ergebnisse der Zugangshistorie“ auf Seite 285)	
TSN	TSN des Dialog-Tasks	
Subject	Die Bedeutung ist abhängig vom Typ des Zugangs:	
	BATCH	Benutzerkennung und TSN des Batch-Task-Initiators
	DIALOG	Prozessorname und Stationsname des Terminals
	DIA-KRBROS	Kerberos-Name
	DIA-PERSON	Prozessorname und Stationsname des Terminals
	DIA-USERID	Persönliche Benutzerkennung des Dialog-Task-Initiators
	NET-KRBROS	Kerberos-Name
	OPER-CONS	Name der Operator-Console
	POS-BATCH	Benutzerkennung und TSN des Batch-Task-Initiators
	POS-REMOTE	Rechnername und ggf. Benutzerkennung des UNIX-Clients
	RLOGIN	Rechnername
	STANDARD	Benutzerkennung und TSN des Task-Initiators

Tabelle 4: Felder der Zugangshistorie

Folgende Tabelle zeigt die möglichen Inhalte im Feld Type der Zugangshistorie und deren Bedeutung:

Type	**Bedeutung**
BATCH	Batch
DIALOG	Dialog
DIA-KRBROS	Dialog persönliche Benutzerkennung mit Kerberos-Authentisierung
DIA-PERSON	Dialog persönliche Benutzerkennung
DIA-USERID	Dialog Logon-Benutzerkennung
FT	File-Transfer Admission
FT-BATCH	File-Transfer Batch ohne Kennwortprüfung
FT-NO-PASS	File-Transfer Admission ohne Kennwortprüfung
NET-KRBROS	Dialog mit Kerberos-Authentisierung
OPER-CONS	Operator an der physikalischen Konsole im inkompatiblen Modus
OPER-PROG	Operator mit dynamischen Berechtigungsnamen als Programm (@CONSOLE)
OPER-TERM	Operator mit dynamischen Berechtigungsnamen im Dialog ($CONSOLE)
POS-BATCH	POSIX-Batch-Kommandos `at`, `cron` oder `batch`
POS-REMOTE	POSIX-Remote-Kommandos `rcp` oder `rsh`
RLOGIN	POSIX Remote-Login
STANDARD	Kein bestimmter Zugangstyp
UCON	Operator mit generierten Berechtigungsnamen

Tabelle 5: Typen der Zugangshistorie

Folgende Tabelle zeigt die möglichen Inhalte im Feld Result der Zugangshistorie und deren Bedeutung:

Result	**Bedeutung**	
ACCEPT		Zugang wurde gestattet
ACCESS LOCK	Zugangstyp	gesperrt (Zugangstyp-ACCESS)
ACCNUM INVALID	Abrechnungsnummern	nicht eingetragen (ACCOUNT)
BGUARD DENIED	Guard	Batch-Zugang verweigert (GUARD-NAME)
CALLER INVALID	Aufruferkennung	nicht eingetragen (USER-ACCESS)
CERTIF INVALID	Zertifikat	nicht eingetragen (CERTIFICATE)
CLIENT KRBxxxx	Kerberos-Ticket	Ungültiges Ticket, der Kerberos-Name des Client wird protokolliert. /HELP-MSG KRBxxxx
DGUARD DENIED	Guard	Dialog-Zugang verweigert (GUARD-NAME)
DIALOG KRBxxxx	Kerberos-Ticket	Fehlerhaftes Ticket, der Stationsname wird protokolliert. /HELP-MSG KRBxxxx
NGUARD DENIED	Guard	Network-Dialog-Zugang verweigert (GUARD-NAME)
PASSWD EXPIRED	Logon-Kennwort	Verfallsdatum überschritten (LIFETIME-INTERVAL)
PASSWD INVALID	Logon-Kennwort	fehlerhaft (LOGON-PASSWORD)
PGUARD DENIED	Guard	POSIX-Zugang verweigert (GUARD-NAME)
PLOGON REJECT	persönliches Logon	Dialog-Zugang verweigert (PERSONAL-LOGON)
PRIPAL INVALID	Kerberos-Principal	nicht eingetragen (PRINCIPAL)
SERIAL ERROR	Benutzerkennung	Benutzerkennung wurde modifiziert
SERVER KRBxxxx	Kerberos-Ticket	Fehlerhaftes Ticket, der Server-Principal wird protokolliert. /HELP-MSG KRBxxxx
SUSPND DENIED	Benutzerkennung	Benutzerkennung suspendiert (SUSPEND-ATTRIBUTES)
TERMIN INVALID	Terminal	nicht eingetragen (TERMINAL)
TERSET DENIED	Terminal-Set	Zugang verweigert (TERMINAL-SET)
TGUARD DENIED	Terminal-Set Guard	Zugang verweigert (TERM-SET/GUARD-NAME)
USERID EXPIRED	Benutzerkennung	Verfallsdatum überschritten (EXPIRATION-DATE)
USERID INACTIV	Benutzerkennung	Benutzerkennung inaktiv (INACTIVITY-LIMIT)
USERID INVALID	Benutzerkennung	interne Inkonsistenz
USERID LOCK	Benutzerkennung	gesperrt (LOCK-USER)

Tabelle 6: Ergebnisse der Zugangshistorie

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *ATTRIBUTES(SOPE=*LOGON-DEF/*USER-ID) INFORMATION = *ATTRIBUTES(SCOPE=*ALL) INFORMATION = *LOGON-HISTORY	1 2 3

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Aufruferkennung in Zugangshistorie bei Batchbetrieb	var(*LIST).ACCESS(*LIST).CALLER	S	<name 1..8>	3
Zähler in Zugangshistorie	var(*LIST).ACCESS(*LIST).COUNT	I	<integer 1..999>	3
Datum in Zugangshistorie	var(*LIST).ACCESS(*LIST).DATE	S	<date 10>	3
persönliche Benutzerkennung in Zugangshistorie	var(*LIST).ACCESS(*LIST).PERS-USER-ID	S	<name 1..8>	3
Principal-Name	var(*LIST).ACCESS(*LIST).PRINCIPAL	S	<name 1..1800>	3
Prozessor in Zugangshistorie bei Dialogzugang	var(*LIST).ACCESS(*LIST).PROCESSOR	S	<name 1..8>	3
Resultat in Zugangshistorie	var(*LIST).ACCESS(*LIST).RESULT	S	ACCEPT ACCESS LOCK ACCNUM INVALID BGUARD DENIED CALLER INVALID CERTIF INVALID CLIENT KRBxxxx DGUARD DENIED DIALOG KRBxxxx NGUARD DENIED PASSWD EXPIRED PASSWD INVALID PGUARD DENIED PLOGON REJECT PRIPAL INVALID SERIAL ERROR SERVER KRBxxxx SUSPND DENIED TERMIN INVALID TERSET DENIED TGUARD DENIED USERID EXPIRED USERID INACTIV USERID INVALID USERID LOCK	3

(Teil 1 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Aufrufer-TSN in Zugangshistorie bei Batchbetrieb	var(*LIST).ACCESS(*LIST).RTSN	S	<alphanum-name 1..4>	3
Station in Zugangshistorie bei Dialogzugang	var(*LIST).ACCESS(*LIST).STATION	S	<name 1..8>	3
Uhrzeit in Zugangshistorie	var(*LIST).ACCESS(*LIST).TIME	S	<time 8>	3
TSN in Zugangshistorie	var(*LIST).ACCESS(*LIST).TSN	S	<alphanum-name 1..4>	3
Typ in Zugangshistorie	var(*LIST).ACCESS(*LIST).TYPE	S	BATCH DIALOG DIA-KRBROS DIA-PERSON DIA-USERID FT FT-BATCH FT-NO-PASS NET-KRBROS OPER-CONS OPER-PROG OPER-TERM POS-BATCH POS-REMOTE RLOGIN STANDARD UCON	3
Zugangskontrolle im Batch-Betrieb aktiv	var(*LIST).BATCH.ACCESS	S	*LOGON-DEF *NO *YES	1
Ist Zugangskontrolle im Batch-Betrieb Standard-Attribut?	var(*LIST).BATCH.ACCESS-DEF	B	FALSE TRUE	2
Name des Guards, mit dem der Batch-Zugang geschützt wird	var(*LIST).BATCH.GUARD	S	*NONE <filename 1..18>	1
Kennwortprüfung im Batch-Betrieb aktiv	var(*LIST).BATCH.PASS-CHECK	S	*NO *YES <filename 1..18>	1
Auswahl der zugriffsberechtigten Benutzerkennungen im Batch-Betrieb	var(*LIST).BATCH.USER-ACCESS-DEFI	S	*ALL *LIST	1
zugriffsberechtigte Benutzerkennungen im Batch-Betrieb	var(*LIST).BATCH.USER-ACCESS(*LIST)	S	'' *CONSOLE *GROUP *OTHER *OWN <name 1..8>	1

(Teil 2 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Zugangskontrolle im Dialog-Betrieb aktiv	var(*LIST).DIALOG.ACCESS	S	*LOGON-DEF *NO *YES	1
Ist Zugangskontrolle im Dialog-Betrieb Standard-Attribut?	var(*LIST).DIALOG.ACCESS-DEF	B	FALSE TRUE	2
Obsolet. Ausgabe nur aus Kompatibilitätsgründen.	var(*LIST).DIALOG.CHIP-DEFI	S	*NO-PROT	1
Obsolet. Ausgabe nur aus Kompatibilitätsgründen.	var(*LIST).DIALOG.CHIP(*LIST)	S	''	1
Name des Guards, mit dem der Dialog-Zugang geschützt wird	var(*LIST).DIALOG.GUARD	S	*NONE <filename 1..18>	1
Kennwortprüfung im Dialog-Betrieb aktiv	var(*LIST).DIALOG.PASS-CHECK	S	*NO *YES	1
Persönliches Logon für Dialog-Zugang aktiv	var(*LIST).DIALOG.PERS-LOGON	S	*NO *YES	1
Auswahl der zugelassenen Datensichtstationen für den Dialog-Betrieb	var(*LIST).DIALOG.TER-DEFI	S	*ALL *LIST	1
Dialog-Zugang mit Terminal-Sets geschützt	var(*LIST).DIALOG.TER-SET-DEFI	S	*NO-PROT *LIST *EXCEPT	1
Gruppenname	var(*LIST).DIALOG.TER-SET.GROUP-ID	S	<name 1..8> *UNIV	1
Terminal-Sets der Klasse GROUP	var(*LIST).DIALOG.TER-SET.GROUP(*LIST)	S	<name 1..8>	1
Terminal-Sets der Klasse SYSTEM	var(*LIST).DIALOG.TER-SET.SYSTEM(*LIST)	S	<name 1..8>	1
Benutzerkennung	var(*LIST).DIALOG.TER-SET.USER-ID	S	<name 1..8>	1
Terminal-Sets der Klasse USER	var(*LIST).DIALOG.TER-SET.USER(*LIST)	S	<name 1..8>	1
Bezeichnung des Vorrechners, an dem die Datensichtstation generiert ist, von der aus ein LOGON im Dialog möglich ist	var(*LIST).DIALOG.TER(*LIST).PROCESS	S	'' <name 1..8>	1
BCAM-Name des Rechners, von dem aus die Verbindung zu $DIALOG aufgebaut werden darf	var(*LIST).DIALOG.TER(*LIST).STATION	S	'' <name 1..8>	1
Verschlüsselungstyp des Tickets bei KRB0009	var(*LIST).ENC-TYPE	I	<integer 0..2147483647>	3
Verfallsdatum der Benutzerkennung	var(*LIST).EXPIR-DATE	S	*LOGON-DEF *NONE <date 10>	1

(Teil 3 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Ist Verfallsdatum der Benutzerkennung Standard-Attribut?	var(*LIST).EXPIR-DATE-DEF	B	FALSE TRUE	2
Zeitangabe (in Tagen), ab der eine Verfallswarnung für die Benutzerkennung ausgegeben wird	var(*LIST).EXPIR-WARN	I	*LOGON-DEF <integer 0..366>	1
Ist Verfallswarnung für die Benutzerkennung Standard-Attribut?	var(*LIST).EXPIR-WARN-DEF	B	FALSE TRUE	2
Dimension des Inaktivitätslimit	var(*LIST).INACTIVITY.DIM	S	” *DAYS *MONTHS	1
Ende des Inaktivitäts-Zeitraums	var(*LIST).INACTIVITY.EXPIR-DATE	S	<date 10>	1
Inaktivitätslimit	var(*LIST).INACTIVITY.LIFETIME	I	<integer 1..366>	1
Inaktivitätslimit aktiv	var(*LIST).INACTIVITY.PAR	S	*LOGON-DEF *NO *YES	1
Ist Inaktivitätslimit Standard-Attribut?	var(*LIST).INACTIVITY.PAR-DEF	B	FALSE TRUE	2
Schlüsselversion des Tickets bei KRB0011	var(*LIST).KEY-VERSION	I	<integer 0..2147483647>	3
Zugangskontrolle im Network-Dialog-Betrieb aktiv	var(*LIST).NET-DIALOG.ACCESS	S	*LOGON-DEF *YES *NO	1
Ist Zugangskontrolle im Network-Dialog-Betrieb Standard-Attribut?	var(*LIST).NET-DIALOG.ACCESS-DEF	B	FALSE TRUE	2
Schutz durch Zertifikate beim Network-Dialog-Zugang aktiv	var(*LIST).NET-DIALOG.CERT-DEFI	S	*NO-PROT *LIST	1
Nummer der Zertifizierungsinstanz	var(*LIST).NET-DIALOG.CERT(*LIST).AUTHORITY	S	*ANY <integer 1..2147483647>	1
Zertifikatsnummer	var(*LIST).NET-DIALOG.CERT(*LIST).NUMBER	S	<integer 0..2147483647>	1
Name des Guards, mit dem der Network-Dialog-Zugang geschützt wird	var(*LIST).NET-DIALOG.GUARD	S	*NONE <filename 1..18>	1
Kennwortprüfung im Network-Dialog-Betrieb aktiv	var(*LIST).NET-DIALOG.PASS-CHECK	S	*YES *NO	1
Network-Dialog-Zugang via KERBEROS	var(*LIST).NET-DIALOG.PRINCIPAL-DEFI	S	*ALL *NO-PROT *LIST	1
Principal-Name	var(*LIST).NET-DIALOG.PRINCIPAL(*LIST)	S	<name 1..1800>	1

(Teil 4 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Network-Dialog-Zugang mit Terminal-Sets geschützt	var(*LIST).NET-DIALOG.TER-SET-DEFI	S	*NO-PROT *LIST *EXCEPT	1
Gruppenname	var(*LIST).NET-DIALOG.TER-SET. GROUP-ID	S	<name 1..8> *UNIV	1
Terminal-Sets der Klasse GROUP	var(*LIST).NET-DIALOG.TER-SET. GROUP(*LIST)	S	<name 1..8>	1
Terminal-Sets der Klasse SYSTEM	var(*LIST).NET-DIALOG.TER-SET. SYSTEM(*LIST)	S	<name 1..8>	1
Benutzerkennung	var(*LIST).NET-DIALOG.TER-SET.USER-ID	S	<name 1..8>	1
Terminal-Sets der Klasse USER	var(*LIST).NET-DIALOG.TER-SET. USER(*LIST)	S	<name 1..8>	1
Zugangskontrolle beim Konsol-Zugang aktiv	var(*LIST).OPER-CONS.ACCESS	S	*LOGON-DEF *YES *NO	1
Ist Zugangskontrolle beim Konsol-Zugang Standard-Attribut?	var(*LIST).OPER-CONS.ACCESS-DEF	B	FALSE TRUE	2
Kennwortprüfung beim Konsol-Zugang aktiv	var(*LIST).OPER-CONS.PASS-CHECK	S	*YES *NO	1
Authentisierungsverfahren für programmierten Operator wirksam (Operating-Betrieb)	var(*LIST).OPER-PROG.ACCESS	S	*LOGON-DEF *NO *YES	1
Ist Authentisierungsverfahren für programmierten Operator Standard-Attribut?	var(*LIST).OPER-PROG.ACCESS-DEF	B	FALSE TRUE	2
Kennwortprüfung für programmierten Operator wirksam (Operating-Betrieb)	var(*LIST).OPER-PROG.PASS-CHECK	S	*NO *YES	1
Authentisierungsverfahren für via Terminal angeschlossenen Dialogpartner wirksam (Operating-Betrieb)	var(*LIST).OPER-TER.ACCESS	S	*LOGON-DEF *NO *YES	1
Ist Authentisierungsverfahren für via Terminal angeschlossenen Dialogpartner Standard-Attribut?	var(*LIST).OPER-TER.ACCESS-DEF	B	FALSE TRUE	2
Obsolet. Ausgabe nur aus Kompatibilitätsgründen.	var(*LIST).OPER-TER.CHIP-DEFI	S	*NO-PROT	1
Obsolet. Ausgabe nur aus Kompatibilitätsgründen.	var(*LIST).OPER-TER.CHIP(*LIST)	S	''	1
Kennwortprüfung für via Terminal angeschlossene Dialogpartner aktiv (Operating-Betrieb)	var(*LIST).OPER-TER.PASS-CHECK	S	*NO *YES	1

(Teil 5 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Anzahl der gesperrten Kennwörter	var(*LIST).PASS.ACT-BLOCKED	I	<integer 0..100>	1
Tatsächliche Anzahl von Kennwortänderungen	var(*LIST).PASS.ACT-CHA	I	<integer 0..100>	1
Sperrdauer für Kennwörter	var(*LIST).PASS.BLOCKING-TIME	I	<integer 1..32767>	1
Anzahl der erlaubten Kennwortänderungen	var(*LIST).PASS.CHA-PER-PER	I	<integer 1..100>	1
Dimension der Kennwort-Lebensdauer	var(*LIST).PASS.DIM	S	'' *DAYS *MONTHS	1
Verfallsdatum des Kennwortes	var(*LIST).PASS.EXPIR-DATE	S	*LOGON-DEF '' *NONE <date 10>	1
Ist Verfallsdatum des Kennworts Standard-Attribut?	var(*LIST).PASS.EXPIR-DATE-DEF	B	FALSE TRUE	2
Zeitangabe (in Tagen), ab der eine Verfallswarnung für das Kennwort ausgegeben wird	var(*LIST).PASS.EXPIR-WARN	I	*LOGON-DEF <integer 0..366>	1
Ist Verfallswarnung des Kennworts Standard-Attribut?	var(*LIST).PASS.EXPIR-WARN-DEF	B	FALSE TRUE	2
Lebensdauer des Kennwortes	var(*LIST).PASS.LIFETIME	S	*LOGON-DEF *UNLIM <integer 1..366>	1
Ist Lebensdauer des Kennwortes Standard-Attribut?	var(*LIST).PASS.LIFETIME-DEF	B	FALSE TRUE	2
Kennwort für Benutzerkennung vereinbart	var(*LIST).PASS.LOGON-PASS	B	FALSE TRUE	1
Berechtigte zur Verwaltung des Kennwortes	var(*LIST).PASS.MANAGE	S	*LOGON-DEF *BY-ADM *BY-USER *USER-CHA-ONLY	1
Ist Berechtigtung zur Verwaltung des Kennwortes Standard-Attribut?	var(*LIST).PASS.MANAGE-DEF	B	FALSE TRUE	2

(Teil 6 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
minimale Komplexität des Kennwortes *NONE = beliebige Komplexität Stufe 1 = keine Einschränkungen Stufe 2 = max. 2 aufeinander folgende Zeichen gleich Stufe 3 = mind. 1 Buchstabe und 1 Ziffer im Kennwort Stufe 4 = Stufe 3 + 1 Sonderzeichen	var(*LIST).PASS.MIN-COMPLEX	S	*LOGON-DEF *NONE <integer 1..4>	1
Ist minimale Komplexität des Kennwortes Standard-Attribut?	var(*LIST).PASS.MIN-COMPLEX-DEF	B	FALSE TRUE	2
minimale Länge des Kennwortes *NONE = max. 8 Zeichen	var(*LIST).PASS.MIN-LEN	S	*LOGON-DEF *NONE <integer 1..8>	1
Ist minimale Länge des Kennwortes Standard-Attribut?	var(*LIST).PASS.MIN-LEN-DEF	B	FALSE TRUE	2
Liste der Kennwortänderungen aktiv	var(*LIST).PASS.PASS-MEMORY	S	*LOGON-DEF *NO *YES	1
Ist Liste der Kennwortänderungen Standard-Attribut?	var(*LIST).PASS.PASS-MEMORY-DEF	B	FALSE TRUE	2
Zeitraum in Tagen, für den die Beschränkung der Anzahl von Kennwortänderungen gilt	var(*LIST).PASS.PER	I	<integer 1..32767>	1
Erlaubnis zum Ersetzen eines abgelaufenen Kennworts	var(*LIST).PASS.UNLOCK-EXPIR	S	*LOGON-DEF *BY-ADM *BY-USER	1
Ist Erlaubnis zum Ersetzen eines abgelaufenen Kennworts Standard-Attribut?	var(*LIST).PASS.UNLOCK-EXPIR-DEF	B	FALSE TRUE	2
Zugangskontrolle beim POSIX-Remote-Zugang aktiv	var(*LIST).POSIX-REM.ACCESS	S	*LOGON-DEF *YES *NO	1
Ist Zugangskontrolle beim POSIX-Remote-Zugang Standard-Attribut?	var(*LIST).POSIX-REM.ACCESS-DEF	B	FALSE TRUE	2
Name des Guards, mit dem der POSIX-Remote-Zugang geschützt wird	var(*LIST).POSIX-REM.GUARD	S	*NONE <filename 1..18>	1
POSIX-Remote-Zugang mit Terminal-Sets geschützt	var(*LIST).POSIX-REM.TER-SET-DEFI	S	*NO-PROT *LIST *EXCEPT	1

(Teil 7 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Gruppenname	var(*LIST).POSIX-REM.TER-SET.GROUP-ID	S	<name 1..8> *UNIV	1
Terminal-Sets der Klasse GROUP	var(*LIST).POSIX-REM.TER-SET. GROUP(*LIST)	S	<name 1..8>	1
Terminal-Sets der Klasse SYSTEM	var(*LIST).POSIX-REM.TER-SET. SYSTEM(*LIST)	S	<name 1..8>	1
Benutzerkennung	var(*LIST).POSIX-REM.TER-SET.USER-ID	S	<name 1..8>	1
Terminal-Sets der Klasse USER	var(*LIST).POSIX-REM.TER-SET. USER(*LIST)	S	<name 1..8>	1
Zugangskontrolle beim POSIX-Zugang über rlogin aktiv?	var(*LIST).POSIX-RLOG.ACCESS	S	*LOGON-DEF *NO *YES	1
Ist Zugangskontrolle beim POSIX-Zugang über rlogin Standard-Attribut??	var(*LIST).POSIX-RLOG.ACCESS-DEF	B	FALSE TRUE	2
Name des Guards, mit dem der POSIX-Rlogin-Zugang geschützt wird	var(*LIST).POSIX-RLOG.GUARD	S	*NONE <filename 1..18>	1
Kennwortprüfung beim POSIX-Zugang über rlogin aktiv?	var(*LIST).POSIX-RLOG.PASS-CHECK	S	*NO *YES	1
POSIX-Rlogin-Zugang mit Terminal-Sets geschützt	var(*LIST).POSIX-RLOG.TER-SET-DEFI	S	*NO-PROT *LIST *EXCEPT	1
Gruppenname	var(*LIST).POSIX-RLOG.TER-SET. GROUP-ID	S	<name 1..8> *UNIV	1
Terminal-Sets der Klasse GROUP	var(*LIST).POSIX-RLOG.TER-SET. GROUP(*LIST)	S	<name 1..8>	1
Terminal-Sets der Klasse SYSTEM	var(*LIST).POSIX-RLOG.TER-SET. SYSTEM(*LIST)	S	<name 1..8>	1
Benutzerkennung	var(*LIST).POSIX-RLOG.TER-SET.USER-ID	S	<name 1..8>	1
Terminal-Sets der Klasse USER	var(*LIST).POSIX-RLOG.TER-SET. USER(*LIST)	S	<name 1..8>	1
Katalogkennung des Pubsets, in dessen Benutzerkatalog die Schutzattribute eingetragen sind	var(*LIST).PUBSET	S	<cat-id 1..4>	1, 2
Erlaubte Anzahl von Fehlversuchen	var(*LIST).SUSPEND.COUNT	I	<integer 0..32767>	1
Ist erlaubte Anzahl von Fehlversuchen Standard-Attribut?	var(*LIST).SUSPEND.COUNT-DEF	B	FALSE TRUE	2

(Teil 8 von 9)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Dimension der Beobachtungszeit	var(*LIST).SUSPEND.OBS-DIM	S	'' *MINUTES *HOURS	1
Beobachtungszeit	var(*LIST).SUSPEND.OBS-TIME	I	<integer 0..32767>	1
BIst Beobachtungszeit Standard-Attribut?	var(*LIST).SUSPEND.OBS-TIME-DEF	B	FALSE TRUE	2
Suspendierung aktiv	var(*LIST).SUSPEND.PAR	S	*LOGON-DEF *NO *YES	
Ist Suspendierung Standard-Attribut?	var(*LIST).SUSPEND.PAR-DEF	B	FALSE TRUE	2
Zu suspendierendes Subjekt	var(*LIST).SUSPEND.SUBJECT	S	*USER-ID *INITIATOR	1
Ist zu suspendierendes Subjekt Standard-Attribut?	var(*LIST).SUSPEND.SUBJECT-DEF	B	FALSE TRUE	2
Dimension der Suspendierungszeit	var(*LIST).SUSPEND.SUS-DIM	S	'' *MINUTES *HOURS	1
Suspendierungszeit	var(*LIST).SUSPEND.SUS-TIME	I	<integer 0..32767>	1
Ist Suspendierungszeit Standard-Attribut?	var(*LIST).SUSPEND.SUS-TIME-DEF	B	FALSE TRUE	2
Benutzerkennung	var(*LIST).USER-ID	S	<name 1..8>	1, 3
Sperrung der Benutzerkennung aktiviert	var(*LIST).USER-ID-LOCK	B	FALSE TRUE	1

(Teil 9 von 9)

SHOW-PERSONAL-LOGON-ADMISSION
Persönliche Benutzerkennungen anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION, USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Das Kommando prüft, ob bzw. unter welchen Bedingungen eine Benutzerkennung zum persönlichen Logon unter einer anderen Benutzerkennung berechtigt ist.

```
SHOW-PERSONAL-LOGON-ADMISSION

 PERSONAL-USER-ID = *ALL / list-poss(20): *OWN / <name 1..8>
,LOGON-USER-ID = *ALL / list-poss(20): *OWN / <name 1..8>
,PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
,INFORMATION = *ATTRIBUTES / *USER-LIST
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST(…)
    *SYSLST(…)
        SYSLST-NUMBER = *STD / <integer 1..99>
        ,LINES-PER-PAGE = 64 / <integer 20..255>
```

PERSONAL-USER-ID =
Gibt die Benutzerkennungen an, deren Berechtigung zum persönlichen Logon an den mit dem Operanden LOGON-USER-ID spezifizierten Kennungen geprüft werden soll.

PERSONAL-USER-ID = *ALL
Es werden alle Benutzerkennungen geprüft.

PERSONAL-USER-ID = *OWN
Es wird die Berechtigung der eigenen Benutzerkennung angezeigt.

PERSONAL-USER-ID = <name 1..8>
Es wird die Berechtigung der angegebenen Benutzerkennung angezeigt.

LOGON-USER-ID =
Gibt die Benutzerkennungen an, die geprüft werden sollen, ob und unter welchen Bedingungen sie den mit dem Operanden PERSONAL-USER-ID angegebenen Kennungen das persönliche Logon gestatten.

LOGON-USER-ID = *ALL
Es werden alle Benutzerkennungen geprüft.

LOGON-USER-ID = *OWN
Die Prüfung wird für die eigene Benutzerkennung durchgeführt.

LOGON-USER-ID = <name 1..8>
Die angegebenen Benutzerkennungen werden geprüft.

PUBSET =
Gibt das Pubset an auf das sich die Prüfungen beziehen. Im Allgemeinen ist nur die Angabe *HOME (Standardwert) sinnvoll.

PUBSET = *ALL
Alle Pubsets werden in die Prüfung einbezogen.

PUBSET = *HOME
Die Prüfung bezieht sich auf den Home-Pubset.

PUBSET = <cat-id 1..4>
Die Prüfung bezieht sich auf die angegebenen Pubsets.

INFORMATION =
Legt den Ausgabeumfang fest.

INFORMATION = *ATTRIBUTES
Die persönlichen Benutzerkennungen werden zusammen mit den für die Logon-Benutzerkennung gültigen Zeitbedingungen protokolliert. Die Ausgabe erfolgt analog zu der des Kommandos /SHOW-ACCESS-ADMISSION.

INFORMATION = *USER-LIST
Es wird eine Liste der Benutzerkennungen protokolliert.

OUTPUT =
Gibt an, wohin die Information auszugeben ist.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt nach SYSOUT.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt nach SYSLST.

SYSLST-NUMBER = *STD / <integer 0..99>
Ausgabe nach SYSLST (Angabe *STD) oder in eine SYSLST-Datei aus der Menge SYSLST01 bis SYSLST99.

LINES-PER-PAGE = 64 / <integer 20..255>
Gibt an, nach wie vielen Ausgabesätze eine neue Druckseite beginnen soll..
Voreingestellt ist, dass eine neue Druckseite nach 64 Ausgabesätzen beginnt.

Hinweis

Bei der Angabe von PERSONAL-USER-ID=*ALL und/oder LOGON-USER-ID=*ALL hängt die Menge der ausgegebenen Benutzerkennungen vom Privileg des Kommandoaufrufers ab. Dasselbe gilt, wenn mit PERSONAL-USER-ID und/oder LOGON-USER-ID eine bestimmte Benutzerkennung ausgewählt wird:

– Ein Benutzerverwalter (Privileg USER-ADMINISTRATION) erhält Informationen über alle Benutzerkennungen.

– Einem Gruppenverwalter werden nur solche Benutzerkennungen angezeigt, die Logon-Benutzerkennungen seiner Gruppenmitglieder sind.

– Alle anderen Anwender erhalten alle Informationen, die sie persönlich betreffen, d.h.:

  PERSONAL-USER-ID muss entweder die eigene Logon- oder persönliche Benutzerkennung sein.
  LOGON-USER-ID können alle Benutzerkennungen sein, zu denen die eigene Logon- oder persönliche Benutzerkennung Zugangsberechtigung hat.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	CMD2009	OPS nicht verfügbar
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *ATTRIBUTES INFORMATION = *USER-LIST	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Persönliche Benutzerkennung	Var(*LIST).PERSID	S	<name 1..8> *ALL	1 2
Pubset	Var(*LIST).PUBSET	S	<cat-id 1..4>	1, 2
Logon-Benutzerkennung	Var(*LIST).USERID	S	<name 1..8>	1
Logon-Benutzerkennungen	Var(*LIST).USERID(*LIST)	S	<name 1..8>	2
Zugriffserlaubnis für das Subjekt USER, GROUP oder OTHERS	Var(*LIST).USER.ADMIS	S	*NO *PAR *YES	1
Definition der Zeitbedingung	Var(*LIST).USER.TIME-KIND	S	*ANY *EXCEPT *INTERVAL	1
Beginn des Zeitintervalls	Var(*LIST).USER.TIME(*LIST).FROM	S	‘‘ <time 5>	1
Ende des Zeitintervalls	Var(*LIST).USER.TIME(*LIST).TO	S	‘‘ <time 5>	1
Definition der Datumbedingung	Var(*LIST).USER.DATE-KIND	S	*ANY *EXCEPT *INTERVAL	1
Begin des Datumintervalls	Var(*LIST).USER.DATE(*LIST).FROM	S	‘‘ <date 10>	1
Ende des Datumintervalls	Var(*LIST).USER.DATE(*LIST).TO	S	‘‘ <date 10>	1
Definition der Wochentagbedingung	Var(*LIST).USER.WEEKDAY-KIND	S	*ANY *EXCEPT *INTERVAL	1
Wochentage	Var(*LIST).USER.WEEKDAY(*LIST)	S	‘‘ *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1

(Teil 1 von 2)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Zugriffserlaubnis für ALL-USERS	Var(*LIST).WHEN.ADMIS	S	“ *NO *PAR *YES	1
Definition der Zeitbedingung	Var(*LIST).WHEN.TIME-KIND	S	*ANY *EXCEPT *INTERVAL	1
Begin des Zeitintervalls	Var(*LIST).WHEN.TIME(*LIST).FROM	S	“ <time 5>	1
Ende des zeitintervalls	Var(*LIST).WHEN.TIME(*LIST).TO	S	“ <time 5>	1
Definition der Datunbedingung	Var(*LIST).WHEN.DATE-KIND	S	*ANY *EXCEPT *INTERVAL	1
Begin des Datumintervalls	Var(*LIST).WHEN.DATE(*LIST).FROM	S	“ <date 10>	1
Ende des Datumintervalls	Var(*LIST).WHEN.DATE(*LIST).TO	S	“ <date 10>	1
Definition der Wochentagbedingung	Var(*LIST).WHEN.WEEKDAY-KIND	S	*ANY *EXCEPT *INTERVAL	1
Wochentage	Var(*LIST).WHEN.WEEKDAY(*LIST)	S	“ *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1

(Teil 2 von 2)

Beispiele

In einem Guard wurden auf folgende Weise Bedingungen festgelegt, die das persönliche Logon unter der Benutzerkennung HUGO erlauben.

```
/create-guard guard-name=$tsos.dguard,scope=*host-system
/add-access-conditions -
/           guard-name=$tsos.dguard,subjects=*all-users,-
/           admission=*parameters(-
/                 time=*interval(from=07:00,to=20:00),-
/                 weekday=(*monday,*tuesday,*wednesday,*thursday,*friday))
/add-access-conditions guard-name=$tsos.dguard,-
/           subjects=*user(user-identification=otto),-
/           admission=*parameters(-
```

```
/                  date=*interval(from=2018-01-01,to=2018-12-31),-
/                  weekday=(*monday,*tuesday,*wednesday))
/modify-logon-protection user-identification=hugo,-
/             dialog-access=*yes(guard-name=$tsos.dguard,personal-logon=*yes)
```

Die Bedingungen, die eine persönliche Identifikation mit der Benutzerkennung OTTO unter der Benutzerkennung HUGO erlauben, werden folgendermaßen angezeigt:

```
/show-personal-logon-admission personal-user-id=otto,logon-user-id=hugo
```

```
 PERSONAL-LOGON ATTRIBUTES --- PUBSET A                      2018-02-15 14:45:00
 ------------------------------------------------------------------------------
 User OTTO     has access admission to userid HUGO     when
    Date      IN ( <2018-01-01,2018-12-31> )
    Weekday   IN ( MO, TU, WE )
  and when
    Time      IN ( <07:00,20:00> )
    Weekday   IN ( MO, TU, WE, TH, FR )
 ------------------------------------------------------------------------------
 PERSONAL-LOGON ATTRIBUTES                                      END OF DISPLAY
```

Die entsprechenden S-Variablen haben diesen Inhalt:

```
OPS(*LIST).PERSID = 'OTTO'
OPS(*LIST).USERID = 'HUGO'
OPS(*LIST).PUBSET = 'A'
OPS(*LIST).USER.ADMIS = '*PAR'
OPS(*LIST).USER.TIME-KIND = '*ANY'
OPS(*LIST).USER.TIME(*LIST).FROM = ''
OPS(*LIST).USER.TIME(*LIST).TO = ''
*END-OF-VAR
OPS(*LIST).USER.DATE-KIND = '*INTERVAL'
OPS(*LIST).USER.DATE(*LIST).FROM = '2018-01-01'
OPS(*LIST).USER.DATE(*LIST).TO = '2018-12-31'
*END-OF-VAR
OPS(*LIST).USER.WEEKDAY-KIND = '*INTERVAL'
OPS(*LIST).USER.WEEKDAY(*LIST) = '*MONDAY'
OPS(*LIST).USER.WEEKDAY(*LIST) = '*TUESDAY'
OPS(*LIST).USER.WEEKDAY(*LIST) = '*WEDNESDAY'
OPS(*LIST).WHEN.ADMIS = '*PAR'
OPS(*LIST).WHEN.TIME-KIND = '*INTERVAL'
OPS(*LIST).WHEN.TIME(*LIST).FROM = '07:00'
OPS(*LIST).WHEN.TIME(*LIST).TO = '20:00'
*END-OF-VAR
OPS(*LIST).WHEN.DATE-KIND = '*ANY'
OPS(*LIST).WHEN.DATE(*LIST).FROM = ''
OPS(*LIST).WHEN.DATE(*LIST).TO = ''
*END-OF-VAR
OPS(*LIST).WHEN.WEEKDAY-KIND = '*INTERVAL'
OPS(*LIST).WHEN.WEEKDAY(*LIST) = '*MONDAY'
OPS(*LIST).WHEN.WEEKDAY(*LIST) = '*TUESDAY'
OPS(*LIST).WHEN.WEEKDAY(*LIST) = '*WEDNESDAY'
OPS(*LIST).WHEN.WEEKDAY(*LIST) = '*THURSDAY'
OPS(*LIST).WHEN.WEEKDAY(*LIST) = '*FRIDAY'
*END-OF-VAR
```

SHOW-PRIVILEGE
Systemglobale Privilegien anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION, USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, SAT-FILE-EVALUATION, SAT-FILE-MANAGEMENT, SECURITY-ADMINISTRATION

Informiert, welche Privilegien an eine bestimmte Benutzerkennung vergeben sind oder welche Benutzerkennungen ein bestimmtes Privileg besitzen.

Wird das Kommando unter einer anderen Benutzerkennung als der des Sicherheitsbeauftragten gegeben, werden nur die Privilegien bzw. Tasks der eigenen Benutzerkennung angezeigt.

Kommandosyntax für den Sicherheitsbeauftragten

```
SHOW-PRIVILEGE

INFORMATION = *PRIVILEGE(...) / *USER-IDENTIFICATION(...) / *RUN-PRIVILEGE(...) / *TASK(...)
  *PRIVILEGE(...)
    | USER-IDENTIFICATION = *ALL / list-poss(20): *OWN / <name 1..8>
  *USER-IDENTIFICATION(...)
    | PRIVILEGE = *ALL / *PRIVILEGE-SET(...) / list-poss(64): <text>
    |   *PRIVILEGE-SET(...)
    |     | PRIVILEGE-SET-NAME = *ALL / list-poss(20): <name 1..8>
  *RUN-PRIVILEGE(...)
    | JOB-ID = *ALL / *TID(...) / list-poss(20): *OWN / <c-string 1..4> / <alphanum-name 1..4>
    |   *TID(...)
    |     | TID = *ALL / list-poss(20): *OWN / <x-string 1..8> / <x-text 1..8>
  *TASK(...)
    | PRIVILEGE = *ALL / list-poss(64): <text>
,PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
```

INFORMATION =
Art der auszugebenden Information.

INFORMATION = *PRIVILEGE(...)
Es soll angezeigt werden, welche Rechte die angegebenen Benutzerkennungen besitzen.

USER-IDENTIFICATION =
Benutzerkennung, deren Rechte angezeigt werden sollen.

USER-IDENTIFICATION = *ALL
Ausgabe der Rechte aller Benutzerkennungen.

USER-IDENTIFICATION = *OWN
Ausgabe der Rechte der eigenen Benutzerkennung.

INFORMATION = *USER-IDENTIFICATION(...)
Es soll angezeigt werden, welche Benutzerkennungen die angegebenen Privilegien bzw. Sammelprivilegien besitzen.

PRIVILEGE =
Es sollen die Benutzerkennungen angezeigt werden, die das angegebene Privileg besitzen. Folgende Werte können angegeben werden (für die Einzelwerte ist auch eine Liste möglich):

PRIVILEGE = *ALL
Für alle Systemprivilegien soll angezeigt werden, welche Benutzerkennungen diese Privilegien besitzen. Die Einzelprivilegien sind ab Seite 40 beschrieben.

PRIVILEGE = *PRIVILEGE-SET(...)
Es sollen Informationen über ein Sammelprivileg gegeben werden.

PRIVILEGE-SET-NAME = *ALL / list-poss(20): <name 1..8>
Es wird über alle oder die explizit angegebenen Sammelprivilegien die Information ausgegeben.

PRIVILEGE = list-poss (64): <text>
Für das angegebene Privileg soll angezeigt werden, welche Benutzerkennungen dieses Privileg besitzen. Mögliche Privilegien siehe Seite 128.
Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

INFORMATION = *RUN-PRIVILEGE(...)
Die aktuellen Privilegien der angegebenen Tasks sollen angezeigt werden. Folgende Werte können angegeben werden (für die Einzelwerte ist auch eine Liste möglich):

JOB-ID = *OWN
Die Privilegien der eigenen Task werden angezeigt.

JOB-ID = *ALL
Die Privilegien aller Tasks werden angezeigt.

JOB-ID = <c-string 1..4> / <alphanum-name 1..4>
Die Privilegien der Task mit der angegebenen TSN werden angezeigt.

JOB-ID = *TID(...)
Die Privilegien der Task mit der angegebenen TID werden angezeigt. Folgende Werte können angegeben werden (für die Einzelwerte ist auch eine Liste möglich):

TID = *OWN
Die Privilegien der eigenen Task werden angezeigt.

TID = *ALL
Die Privilegien aller Tasks werden angezeigt.

TID = <x-string 1..8> / <x-text 1..8>
Die Privilegien der Task mit der angegebenen TID werden angezeigt.

INFORMATION = *TASK(PRIVILEGE = *ALL / list-poss(64): <text>)
Es soll alle Tasks angezeigt werden, die eines der angegebenen Privilegien besitzen.

PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
Pubset, dessen Privilegienverteilung angezeigt werden soll.

PUBSET = *ALL
Es soll die angezeigt werden, welche Privilegien und Sammelprivilegien die Benutzerkennung auf allen lokal importierten Pubsets hat.

PUBSET = *HOME
Es soll die angezeigt werden, welche Privilegien und Sammelprivilegien die Benutzerkennung auf dem Home-Pubset hat.

PUBSET = <cat-id 1..4>
Es soll die Rechteverteilung des angebenen Pubset angezeigt werden.

OUTPUT =
Gibt an, wo die Information aufzulisten ist.

OUTPUT = *SYSOUT
Die Information wird auf die Systemdatei SYSOUT ausgegeben.

OUTPUT = *SYSLST
Die Information wird auf die Systemdatei SYSLST ausgegeben.

Kommandosyntax für alle anderen Benutzer

```
SHOW-PRIVILEGE

INFORMATION = *PRIVILEGE / *RUN-PRIVILEGE(...) / *TASK(...)
  *RUN-PRIVILEGE(...)
    JOB-ID = *ALL / *TID(...) / list-poss(20): *OWN / <c-string 1..4> / <alphanum-name 1..4>
      *TID(...)
        TID = *ALL / list-poss(20): *OWN / <x-string 1..8> / <x-text 1..8>
  *TASK(...)
    PRIVILEGE = *ALL / list-poss(64): <text>
PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
```

INFORMATION = *PRIVILEGE(...)
Die Rechte der eigenen Benutzerkennung werden angezeigt.

INFORMATION = *RUN-PRIVILEGE(...)
Die aktuellen Privilegien der angegebenen Tasks sollen angezeigt werden. Folgende Werte können angegeben werden (für die Einzelwerte ist auch eine Liste möglich):

JOB-ID = *OWN
Die Privilegien der eigenen Task werden angezeigt.

JOB-ID = *ALL
Die Privilegien aller Tasks werden angezeigt.

JOB-ID = <c-string 1..4> / <alphanum-name 1..4>
Die Privilegien der Task mit der angegebenen TSN werden angezeigt.

JOB-ID = *TID(...)
Die Privilegien der Task mit der angegebenen TID werden angezeigt. Folgende Werte können angegeben werden (für die Einzelwerte ist auch eine Liste möglich):

TID = *OWN
Die Privilegien der eigenen Task werden angezeigt.

TID = *ALL
Die Privilegien aller Tasks werden angezeigt.

TID = <x-string 1..8> / <x-text 1..8>
Die Privilegien der Task mit der angegebenen TID werden angezeigt.

INFORMATION = *TASK(PRIVILEGE = *ALL / list-poss(64): <text>)
Es soll alle Tasks angezeigt werden, die eines der angegebenen Privilegien besitzen.

PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
Pubset, dessen Rechteverteilung angezeigt werden soll.

PUBSET = *ALL
Es soll angezeigt werden, welche Rechte die Benutzerkennung auf allen angeschlossenen Pubsets hat.

PUBSET = *HOME
Es soll angezeigt werden, welche Rechte die Benutzerkennung auf dem Home-Pubset hat.

OUTPUT =
Gibt an, wo die Information aufzulisten ist (Liste möglich).

OUTPUT = *SYSOUT
Die Information wird auf die Systemdatei SYSOUT ausgegeben.

OUTPUT = *SYSLST
Die Information wird auf die Systemdatei SYSLST ausgegeben.

Hinweis zum Spin-off-Verhalten

Ein SPIN-OFF wird nicht ausgelöst, solange gültige Angaben in einer Liste von Benutzerkennungen oder Pubsets vorhanden sind. Eine nicht existierende Benutzerkennung bzw. ein nicht angeschlossenes Pubset wird nur dann SPIN-OFF auslösen, wenn in der Liste überhaupt keine gültigen Angaben zur Informationsausgabe waren.

Der SPIN-OFF-Mechanismus wird immer ausgelöst, wenn es keine Informationen entsprechend den Auswahlkriterien gibt.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiele

Der Sicherheitsbeauftragte möchte überprüfen, welche Privilegien die Kennung USER1 hat:

```
/show-privilege information=*privilege(user-identification=user1)

PRIVILEGES AVAILABLE TO USER-IDENTIFICATION USER1    ON PUBSET ABC1
PRIVILEGES:
STD-PROCESSING
PRIVILEGE SETS:
ARCHIV
```

Die Anzeige der als Einzelprivilegien zugeordneten Privilegien zeigt keine Einzelprivilegien, die über Sammelprivilegien zugeordnet sind. Um zu erfahren, welche Privilegien in PRIVILEGE-SET-NAME=ARCHIV definiert und damit dem USER1 zugewiesen sind, muss zusätzlich das Kommando /SHOW-PRIVILEGE-SET abgesetzt werden.

Es soll angezeigt werden, welche Kennung das Sammelprivileg ARCHIV hat:

```
/show-privilege information=*user-identification(privilege= -
/               *privilege-set(privilege-set-name=archiv))

USER-IDENTIFICATIONS HAVING PRIVILEGE SET ARCHIV    ON PUBSET ABC1
USER1
```

Es soll angezeigt werden, welche Kennungen das Privileg HSMS-ADMINISTRATION besitzen:

```
/show-privilege information=*user-identification( -
/               privilege=*hsms-administration)

USER-IDENTIFICATIONS WITH PRIVILEGE HSMS-ADMINISTRATION
ON PUBSET ABC1
SYSHSMS TSOS
```

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *PRIVILEGE(...)	1
INFORMATION = *USER-ID(PRIVILEGE=...)	2
INFORMATION = *USER-ID(PRIVILEGE=PRIVILEGE-SET(...))	3
INFORMATION = *RUN-PRIVILEGE(...)	4
INFORMATION = *TASK(...)	5

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Privilegs	var(*LIST).PRIVIL	S	*ACS-ADM	2, 5
	var(*LIST).PRIVIL(*LIST)	S	*CUST-PRIV-1 *CUST-PRIV-2 *CUST-PRIV-3 *CUST-PRIV-4 *CUST-PRIV-5 *CUST-PRIV-6 *CUST-PRIV-7 *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *NOTIF-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-FILE-EVALUATION *SAT-FILE-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SW-MONITOR-ADM *TAPE-ADM *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1, 4
Name des Sammelprivilegs	var(*LIST).PRIVIL-SET	S	<name 1..8>	3
	var(*LIST).PRIVIL-SET(*LIST)	S	<name 1..8>	1

(Teil 1 von 2)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Katalogkennung des Pubsets, dessen Rechteverteilung ausgegeben wird	var(*LIST).PUBSET	S	<cat-id 1..4>	1, 2, 3
Benutzerkennung, deren Rechteverteilung ausgegeben wird	var(*LIST).USER-ID	S	<name 1..8>	1, 4
	var(*LIST).USER-ID(*LIST)	S	<name 1..8>	2, 3
TID der Task, deren Rechteverteilung ausgegeben wird	var(*LIST).TID	S	'' <x-text 8>	4
TSN der Task, deren Rechteverteilung ausgegeben wird	var(*LIST).TSN	S	'' <alphanum-name 4>	4
TSN der Task, die das angegebene Privileg besitzt	var(*LIST).TASK(*LIST).TSN	S	<alphanum-name 4>	5
Benutzerkennung der Task, die das angegebene Privileg besitzt	var(*LIST).TASK(*LIST).USER-ID	S	<name 1..8>	5

(Teil 2 von 2)

Beispiele

```
/exec-cmd (show-privilege *run-privilege (job-id=0015)),s-out=ops
/show-var ops,inf=*par(value=*c-literal)

OPS(*LIST).TID = ''
OPS(*LIST).TSN = '0015'
OPS(*LIST).USER-ID = 'TSOS'
OPS(*LIST).PUBSET = ''
OPS(*LIST).PRIVIL(*LIST) = '*ACS-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*FT-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*FTAC-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*GUA-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*HSMS-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*NET-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*OPER'
OPS(*LIST).PRIVIL(*LIST) = '*PRINT-SERVICE-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*PROP-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*STD-PROCESS'
OPS(*LIST).PRIVIL(*LIST) = '*SUBSYS-MANAGE'
OPS(*LIST).PRIVIL(*LIST) = '*SW-MONITOR-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*TAPE-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*TSOS'
OPS(*LIST).PRIVIL(*LIST) = '*USER-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*USSYSFOP'
OPS(*LIST).PRIVIL(*LIST) = '*VIRT-MACHINE-ADM'
OPS(*LIST).PRIVIL(*LIST) = '*VM2000-ADM'
*END-OF-VAR
```

```
/exec-cmd (show-privilege *run-privilege(job-id=*tid(x'00010034')),s-out=ops
/show-var ops,inf=*par(value=*c-literal)

OPS(*LIST).TID = '00010034'
OPS(*LIST).TSN = ''
OPS(*LIST).USER-ID = 'HUGO'
OPS(*LIST).PUBSET = ''
OPS(*LIST).PRIVIL(*LIST) = '*STD-PROCESS'
*END-OF-VAR
```

```
/exec-cmd (show-privilege *task(privilege=*std-proc)),s-out=ops
/show-var ops,inf=*par(value=*c-literal)

OPS(*LIST).PRIVIL = '*STD-PROCESS'
OPS(*LIST).TASK(*LIST).TSN = '0015'
OPS(*LIST).TASK(*LIST).USER-ID = 'TSOS'
*END-OF-VAR
OPS(*LIST).TASK(*LIST).TSN = '0AAB'
OPS(*LIST).TASK(*LIST).USER-ID = 'HUGO'
*END-OF-VAR
*END-OF-VAR
```

SHOW-PRIVILEGE-SET
Sammelprivileg-Definition anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: SECURITY-ADMINISTRATION

Dieses Kommando kann Privilegienzuordnungen auf zwei Weisen anzeigen:

– Zuordnung Einzelprivileg zu Sammelprivileg. Diese Funktion gibt Auskunft, welche Einzelprivilegien einem benannten Sammelprivileg zugeordnet sind.

– Zuordnung Sammelprivileg zu Einzelprivileg. Diese Funktion gibt Auskunft, welchen Sammelprivilegien ein benanntes Einzelprivileg zugeordnet ist.

Der Sicherheitsbeauftragte kann so überprüfen, welche Zuordnungen bestehen. Diese Funktion ist besonders dann wichtig, wenn überprüft werden sollen, ob bestimmte, besonders sicherheitsrelevante Privilegien nur einem begrenzten Kreis zur Verfügung stehen.

SHOW-PRIVILEGE**-SET**

INFORMATION = ***PRIVIL**EGE**-SET**(...) / ***PRIV**ILEGE(...)

*PRIVILEGE-SET(...)

PRIVILEGE = ***ALL** / list-poss(64): <text>

*PRIVILEGE(...)

PRIVILEGE-SET-NAME = ***ALL** / list-poss(20): <name 1..8>

,**PUBSET** = *ALL / list-poss(20): ***HOME** / <cat-id 1..4>

,**OUT**PUT = list-poss(2): ***SYSOUT** / ***SYSLST**

INFORMATION = *PRIVILEGE-SET(...)
Auswahl nach Privileg: es wird angegeben, in welchen Sammelprivilegien das angegebene Einzelprivileg enthalten ist.

PRIVILEGE = *ALL
Es werden die Zuordnungen geordnet nach Einzelprivilegien angezeigt. Für alle Einzelprivilegien wird angegeben, in welchen Sammelprivilegien es verwendet wird. Mögliche Privilegien siehe Seite 128. Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

PRIVILEGE = list-poss(64): <text>
Es werden die Zuordnungen geordnet nach Einzelprivilegien angezeigt. Für jedes angegebene Einzelprivileg wird angegeben, in welchen Sammelprivilegien es verwendet wird. Mögliche Privilegien siehe Seite 128. Ausnahmen: TSOS und SECURITY-ADMINISTRATION.

INFORMATION = *PRIVILEGE(...)
Es wird angezeigt, welche Einzelprivilegien den explizit genannten Sammelprivilegien (oder allen Sammelprivilegien) zugeordnet sind.

PRIVILEGE-SET-NAME = *ALL / list-poss(20): <name 1..8>
*ALL zeigt die Definitionen aller Sammelprivilegien an.

PUBSET = *ALL / list-poss(20): *HOME / <cat-id 1..4>
Pubset, dessen Sammelprivileg-Definitionen angezeigt werden sollen.

PUBSET = *ALL
Es sollen die Sammelprivileg-Definitionen aller lokal importierten Pubsets angezeigt werden.

PUBSET = *HOME
Es sollen die Sammelprivileg-Definitionen des Home-Pubsets angezeigt werden.

PUBSET = <cat-id 1..4>
Pubset-Bezeichnung

OUTPUT =
Gibt an, wohin die Information auszugeben ist.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt nach SYSOUT.

OUTPUT = *SYSLST
Die Ausgabe erfolgt nach SYSLST.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Beispiel

Es soll für das im Beispiel zu /CREATE-PRIVILEGE-SET erzeugte Sammelprivileg ARCHIV das /SHOW-PRIVILEGE-SET angewendet werden:

Es soll überprüft werden, welche Privilegien im Sammelprivileg ARCHIV enthalten sind:

```
/show-privilege-set information=*privilege(privilege-set-name=archiv)

THE FOLLOWING PRIVILEGES ARE ASSIGNED TO PRIVILEGE-SET ARCHIV    ON PVS ABC1
HSMS-ADMINISTRATION TAPE-ADMINISTRATION
```

Es soll überprüft werden, in welchen Sammelprivilegien die Privilegien TAPE-ADMINISTRATION und HSMS-ADMINISTRATION enthalten sind:

```
/show-privilege-set information=*privilege-set( -
/                     privilege=(*hsms-administration,*tape-administration))

PRIVILEGE-SETS CONTAINING PRIVILEGE HSMS-ADMINISTRATION
ON PVS ABC1
ARCHIV
PRIVILEGE-SETS CONTAINING PRIVILEGE TAPE-ADMINISTRATION
ON PVS ABC1
ARCHIV
```

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = PRIVILEGE-SET(...) INFORMATION = PRIVILEGE(...)	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Einzelprivilegs	var(*LIST).PRIVIL	S	*ACS-ADM *CUST-PRIV-1 *CUST-PRIV-2 *CUST-PRIV-3 *CUST-PRIV-4 *CUST-PRIV-5 *CUST-PRIV-6 *CUST-PRIV-7 *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *NOTIF-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-FILE-EVALUATION *SAT-FILE-MANAGE *STD-PROCESS *SUBSYS-MANAGE *SW-MONITOR-ADM *TAPE-ADM *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1
	var(*LIST).PRIVIL(*LIST)	S		2
Definition des Sammelprivilegs *NONE = dem Sammelprivileg wird kein Einzelprivileg zugeordnet *LIST = dem Sammelprivileg wird eine Liste von Einzelprivilegien zugeordnet	var(*LIST).PRIVIL-DEFI	S	*LIST *NONE	2
Name des Sammelprivilegs	var(*LIST).PRIVIL-SET	S	<name 1..8>	2
	var(*LIST).PRIVIL-SET(*LIST)	S	<name 1..8>	1
Katalogkennung des Pubsets, auf dem das Sammelprivileg eingetragen ist	var(*LIST).PUBSET	S	<cat-id 1..4>	1, 2

SHOW-TERMINAL-SET
Terminal-Set anzeigen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Zeigt Terminal-Sets an.

Der System-Benutzerverwalter kann sich alle Terminal-Sets anzeigen lassen.

Ein Gruppenverwalter kann sich nur die Terminal-Sets mit SCOPE=*SYSTEM und die Terminal-Sets seiner Gruppe und die deren Mitglieder anzeigen lassen.

Ein Benutzer ohne Verwalterrechte kann sich nur jene Terminal-Sets anzeigen lassen, die seiner Benutzerkennung zugewiesen sind.

Dabei kann sowohl die Menge der auszugebenden Terminal-Sets, als auch der Umfang der auszugebenden Information für jedes Terminal-Set festgelegt werden

Die Menge der Terminal-Sets kann auf zwei Arten beschränkt werden

- auf bestimmte Klassen und innerhalb der Klassen hinsichtlich der Eigentümer.
- anhand ihrer Attribute, d.h. sie werden ausgewählt, wenn eine oder mehrere der folgenden Aussagen auf sie zutreffen:
  - Terminal-Sets die (nicht) zum Schutz einer Benutzerkennung verwendet werden
  - Terminal-Sets, die mit keinem, einem beliebigen oder einem bestimmten Guard verknüpft sind.
  - Terminal-Sets, die einen bestimmten Datensichtstationsnamen enthalten. Ein Terminal-Name, voll- oder teilqualifiziert definiert, kann explizit angegeben oder über Wildcard gesucht werden.
  - Terminal-Sets, die eine bestimmte Dialogstation erfassen.

    Die Selektion kann eine Zugangskontrolle mit direkter Verbindung oder eine Terminal-Emulation simulieren.

    Im Falle der Terminal-Emulation stehen 3 Protokolle zur Verfügung:

    1. Prüfung gegen den Namen der Dialogstation unter der Annahme einer beliebigen, privilegierten Terminal-Emulation.
    2. Prüfung gegen den Namen der Dialogstation unter der Annahme einer beliebigen Terminal-Emulation.
    3. Prüfung gegen den Namen der Terminal-Emulation unter der Annahme einer beliebigen Dialogstation.

Die folgende Tabelle zeigt, unter welchen Vorbedingungen eine Prüfung des Terminal-Names stattfindet (+) oder die Bedingung von vornherein nicht erfüllt ist (-):

TYPE der Terminalselektion	**TYPE-Definition der Terminaleinträge**		
	***STD**	***NET-TERM-NAME**	***APP-TERM-NAME**
*NONE	+	+	+
*STD	+	+	-
*NET-TERMINAL-NAME	-	+	-
*APPLICATION-TERMINAL-NAME	-	-	+

Der Umfang der ausgegebenen Information kann folgendermaßen festgelegt werden:

– Ausgabe von Terminal-Sets mit ihren Attributen.
  Die Attribute Guard, Benutzerinformation, Datensichtstationen und Benutzerkennungen können einzeln auswählt werden. Die Ausgabe des Attributs Datensichtstation kann auf bestimmte Datensichtstationen eingeschränkt werden.
  Die Benutzerkennungen, die durch das Terminal-Set geschützt werden, werden standardmäßig nicht ausgegeben.

– Ausgabe Liste von Terminal-Set-Namen.

SHOW-TERMINAL-SET

TERMINAL-SET-NAME = ***ALL(...)** / list-poss(100): <name 1..8>(…)

***ALL(...)**
- **SCOPE** = ***STD** / ***USER**(…) / ***GROUP**(…) / ***SYSTEM** / ***ANY**
  - ***USER**(…)
    - **USER-IDENTIFICATION** = ***OWN** / <name 1..8>
  - ***GROUP**(…)
    - **GROUP-IDENTIFICATION** = ***OWN** / ***UNIVERSAL** / <name 1..8>

<name 1..8>(…)
- **SCOPE** = ***STD** / ***USER**(…) / ***GROUP**(…) / ***SYSTEM**
  - ***USER**(…)
    - **USER-IDENTIFICATION** = ***OWN** / <name 1..8>
  - ***GROUP**(…)
    - **GROUP-IDENTIFICATION** = ***OWN** / ***UNIVERSAL** / <name 1..8>

,**PUBSET** = ***ALL** / list-poss(100): ***HOME** / <catid 1..4>

,**SELECT** = ***ALL** / ***BY-ATTRIBUTES**(…)

***BY-ATTRIBUTES(...)**
- **ASSIGNED** = ***ANY** / ***YES** / ***NO** / ***OWN** / <name 1..8>
- ,**GUARD-NAME** = ***ANY** / ***YES** / ***NONE** / <filename 1..18 without-cat-gen-vers>
- ,**TERMINAL** = ***ANY** / ***BY-ENTRY-DEFINITION**(…) / ***BY-LOGON-ACCESS**(…)
  - ***BY-ENTRY-DEFINITION**(…)
    - **PROCESSOR** = ***ANY** / <c-string 1..16> / <name 1..8 with-wild(16)>
    - ,**STATION** = ***ANY** / <c-string 1..16> / <name 1..8 with-wild(16)>
  - ***BY-LOGON-ACCESS**(…)
    - **PROCESSOR** = <name 1..8>
    - ,**STATION** = <name 1..8>
    - ,**CHECK-MODE** = ***NONE** / ***STD** / ***NET-TERMINAL-NAME** / ***APPLICATION-TERMINAL-NAME**

,**INFORMATION** = ***ATTRIBUTES**(…) / ***NAMES-ONLY**

***ATTRIBUTES**(…)
- **GUARD-NAME** = ***YES** / ***NO**
- ,**USER-INFORMATION** = ***YES** / ***NO**
- ,**TERMINALS** = ***YES** / ***NO** / ***SELECTED**
- ,**PROTECTED-USER-IDS** = ***NO** / ***YES**

,**OUTPUT** = list-poss: ***SYSOUT** / ***SYSLST**(…)

***SYSLST**(…)
- **SYSLST-NUMBER** = ***STD** / <integer 1..99>

TERMINAL-SET-NAME = *ALL(...) / list-poss: <name 1..8>(…)
Gibt an welche Terminal-Sets angezeigt werden.

TERMINAL-SET-NAME = *ALL(...)
Alle Terminal-Sets werden angezeigt.
Bedeutung des Operanden SCOPE siehe TERMINAL-SET-NAME = <name 1..8>(…).

TERMINAL-SET-NAME = <name 1..8>(…)
Nur Terminal-Sets mit dem angegebenen Namen werden angezeigt.

SCOPE = *STD
Für systemglobaler Benutzerverwalter wirkt diese Angabe wie SCOPE=*SYSTEM.

Für Gruppenverwalter wirkt die Angabe wie SCOPE=*GROUP(GROUP-ID=*OWN).

SCOPE = *USER(USER-IDENTIFICATION = *ALL / *OWN / <name 1..8>)
Nur Terminal-Sets der angegebene Benutzerkennung werden angezeigt.

SCOPE = *GROUP(GROUP-IDENTIFICATION = *ALL / *OWN / *UNIVERSAL / <name 1..8>)
Nur Terminal-Sets der angegebenen Benutzergruppe werden angezeigt.

SCOPE = *SYSTEM
Terminal-Sets aus dem gemeinschaftlichen Eigentum werden angezeigt.

SCOPE = *ANY
Terminal-Sets werden unabhängig von ihrer Klasse und ihrem Eigentümer angezeigt.

PUBSET = *ALL / list-poss(100): *HOME / <catid 1..4>
Pubset, aus dessen Benutzerkatalog Terminal-Sets angezeigt werden.

PUBSET = *ALL
Terminal-Sets aus allen lokal importierten Pubsets werden angezeigt.

PUBSET = *HOME
Terminal-Sets aus dem Home-Pubset werden angezeigt.

PUBSET = <catid 1..4>
Terminal-Sets aus dem angegebenen Pubset werden angezeigt.

SELECT =
Legt Auswahlkriterien für Terminal-Sets fest, die angezeigt werden sollen.

SELECT = *ALL
Terminal-Sets werden unabhängig von ihren Attributen angezeigt.

SELECT = *BY-ATTRIBUTES(…)
Terminal-Sets werden nur angezeigt, wenn sie bestimmte Attribute besitzen.

ASSIGNED =
Gibt an, ob die Terminal-Set abhängig davon ausgewählt werden, ob sie zum Schutz einer Benutzerkennung eingesetzt werden.

ASSIGNED = *ANY
Terminal-Sets werden unabhängig davon angezeigt, ob sie zum Schutz einer Benutzerkennung eingesetzt werden.

ASSIGNED = *YES
Nur solche Terminal-Sets werden angezeigt, die zum Schutz mindestens einer Benutzerkennung eingesetzt werden.

ASSIGNED = *NO
Nur solche Terminal-Sets werden angezeigt, die zum Schutz keiner Benutzerkennung eingesetzt werden.

ASSIGNED = *OWN
Nur solche Terminal-Sets werden angezeigt, die zum Schutz der eigenen Benutzerkennung eingesetzt werden.

ASSIGNED = <name 1..8>
Nur solche Terminal-Sets werden angezeigt, die zum Schutz der angegebenen Benutzerkennung eingesetzt werden.

GUARD-NAME =
Gibt an, ob Terminal-Sets abhängig von der Verknüpfung mit einem Guard ausgewählt werden.

GUARD-NAME = *ANY
Terminal-Sets werden unabhängig von der Verknüpfung mit einem Guard angezeigt.

GUARD-NAME = *YES
Nur die Terminal-Sets werden angezeigt, die mit einem Guard verknüpft sind.

GUARD-NAME = *NONE
Nur die Terminal-Sets werden angezeigt, die mit keinem Guard verknüpft sind.

GUARD-NAME = <filename 1..18 without-cat-gen-vers>
Nur die Terminal-Sets werden angezeigt, die mit dem angegebenen Guard verknüpft sind.

TERMINAL =
Gibt an, ob Terminal-Sets abhängig von den darin enthaltenen Datensichtstationsnamen ausgewählt werden.

TERMINAL = *ANY
Terminal-Sets werden unabhängig von den Datensichtstationsnamen ausgewählt, die in ihnen enthalten sind.

TERMINAL = *BY-ENTRY-DEFINITION(…)
Es werden Terminal-Sets ausgewählt, die bestimmte Datensichtstationsnamen enthalten.

PROCESSOR =
Prozessoranteil im Datensichtstationsnamen.

PROCESSOR = <c-string 1..16>
Es werden Terminal-Entries durch Vergleich ihrer Terminal-Namen mit einer Musterzeichenfolge ausgewählt.

PROCESSOR = <name 1..8 with-wild(16)>
Es wird ein bestimmter Datensichtstationseintrag durch Vorgabe seines Datensichtstationsnamens ausgewählt.

STATION =
Stationsanteil im Datensichtstationsnamen.

STATION = <c-string 1..16>
Es werden Datensichtstationseinträge durch Vergleich ihrer Datensichtstationsnamen mit einer Musterzeichenfolge ausgewählt.

STATION = <name 1..8 with-wild(16)>
Es wird ein bestimmter Datensichtstationseintrag durch Vorgabe seines Datensichtstationsnamens ausgewählt.

TERMINAL = *BY-LOGON-ACCESS(…)
Die Auswahl der Terminal-Sets wird durch einen simulierten Dialogzugang getroffen. Es werden Terminal-Sets ausgewählt, deren Datensichtstationseinträge eine bestimmte Dialogstation erfassen.

CHECK-MODE =
Angabe des zu verwendenden Prüfprotokolls. Der Logon kann einen direkten Zugang oder eine Terminal-Emulation simulieren.

CHECK-MODE = *NONE
Simulation eines direkten Zugangs. Das Attribut CHECK-MODE der Datensichtstationseinträge bleibt unberücksichtigt. Es werden alle Datensichtstationseinträge erfasst.

CHECK-MODE = *STD
Simulation einer vertrauenswürdigen Terminal-Emulation. Der Name der Dialogstation ist vorgegeben. Es werden Datensichtstationseinträge mit CHECK-MODE=*STD oder CHECK-MODE=*NET-TERMINAL-NAME erfasst.

CHECK-MODE = *NET-TERMINAL-NAME
Simulation einer Terminal-Emulation. Der Name der Dialogstation ist vorgegeben. Es werden Datensichtstationseinträge mit dem CHECK-MODE=*NET-TERMINAL-NAME erfasst.

CHECK-MODE = *APPLICATION-TERMINAL-NAME
Simulation einer Terminal-Emulation, ihr Name ist vorgegeben. Es werden Datensichtstationseinträge mit CHECK-MODE=*APPLICATION-TERMINAL-NAME erfasst.

INFORMATION = *ATTRIBUTES(…) / *NAMES-ONLY
Bestimmt, welche Information ausgegeben wird.

***ATTRIBUTES(…)**
Die folgenden Attribute des Terminal-Sets werden ausgegeben.

GUARD-NAME = *YES / *NO
Gibt an, ob das verknüpfte Guard ausgegeben wird.

USER-INFORMATION = *YES / *NO
Gibt an, ob die Benutzerinformation ausgegeben wird.

TERMINALS = *YES / *NO / *SELECTED
Gibt an, ob die Datensichtstationseinträge ausgegeben werden.

TERMINALS = *SELECTED
Nur die im Operand SELECT ausgewählten Datensichtstationen werden ausgegeben.

PROTECTED-USER-IDS = *NO / *YES
Es werden die Benutzerkennungen angezeigt, die durch das Terminal-Set geschützt werden.

***NAMES-ONLY**
Nur die Namen der ausgewählten Terminal-Sets werden ausgegeben.

OUTPUT =
Gibt an, wohin die Information auszugeben ist.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt nach SYSOUT.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt nach SYSLST.

SYSLST-NUMBER = *STD / <integer 0..99>
Ausgabe nach SYSLST (Angabe *STD) oder in eine SYSLST-Datei aus der Menge SYSLST01 bis SYSLST99.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	1	SRM6010	Syntaxfehler im Kommando
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen
	130	CMD2009	OPS nicht verfügbar

Beispiel: Ausgabe der Terminal-Sets

```
/show-terminal-set terminal-set-name=TERMSET1, -
/                  information=*attributes(protected-user-ids=*yes)

Terminal-Set Attributes         --- Pubset B               2018-03-02 17:14:22
------------------------------------------------------------------------------
Terminal-Set:     TERMSET1/*GROUP/SYSUID             Pubset:   B
Guard-Name:       $TSOS.MYGUARD
User-Information: This should protect one's UserID
Terminal-Entries: (Processor,Station,Check-Mode)
 (D016KR27,DSB23571,--) (D017KR12,DSB15837,-N)
 (D016ZE04        ,*               ,-A) (PGTD1563        ,$$$060//        ,NA)
Assigned Userids:
 SYSDUMP  SYSPRIV  SYSUSER  TSOS
------------------------------------------------------------------------------
Terminal-Set Attributes                                        end of display
```

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *ATTRIBUTES INFORMATION = *NAMES-ONLY	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Terminal-Sets	var(*LIST).NAME	S	<name 1..8>	1
Eigentümer des Terminal-Sets	var(*LIST).OWNER	S	<name 1..8>	1
Klasse des Terminal-Sets	var(*LIST).SCOPE	S	*USER *GR *SYS	1
Liste der Terminal-Sets	var(*LIST).TER-SET(*LIST).NAME	S	<name 1..8>	2
Liste der Eigentümer	var(*LIST).TER-SET(*LIST).OWNER	S	<name 1..8>	2
Liste der Klassen	var(*LIST).TER-SET(*LIST).SCOPE	S	*USER *GR *SYS	2
CatID des Pubset	var(*LIST).PUBSET	S	<catid 1..4>	1,2
Name des Guard	var(*LIST).GUARD	S	<filename 1..18>	1
Benutzerinformation	var(*LIST).USER-INFO	S	*NONE <c-string 1..80>	1
Sortierung der Terminal-Einträge	var(*LIST).SORT-TER	S	*BY-PROCESSOR *BY-STATION	1
Prozessorname	var(*LIST).TER(*LIST).PROCESSOR	S	<name 1..16>	1
Stationsname	var(*LIST).TER(*LIST).STATION	S	<name 1..16>	1
Terminaltyp	var(*LIST).TER(*LIST).CHECK-MODE	S	*STD *NET-TER-NAME *APP-TER-NAME	1
Liste der Benutzerkennungen	var(*LIST).USER-ID(*LIST)	S	<name 1..8>	1

Beispiel: Ausgabe der Terminal-Sets in S-Variable

```
VAR(*LIST).NAME = 'TERMSET1'
VAR(*LIST).SCOPE = '*GR'
VAR(*LIST).OWNER = 'SYSUID'
VAR(*LIST).PUBSET = 'B'
VAR(*LIST).GUARD = '$TSOS.MYGUARD'
VAR(*LIST).USER-INFO = '''This should protect one''''s UserID'''
VAR(*LIST).SORT-TER = '*BY-PROCESSOR'
VAR(*LIST).TER(*LIST).PROCESSOR = 'D016KR27'
VAR(*LIST).TER(*LIST).STATION = 'DSB23571'
VAR(*LIST).TER(*LIST).CHECK-MODE(*LIST) = '*STD'
*END-OF-VAR
VAR(*LIST).TER(*LIST).PROCESSOR = 'D017KR12'
VAR(*LIST).TER(*LIST).STATION = 'DSB15837'
VAR(*LIST).TER(*LIST).CHECK-MODE(*LIST) = '*NET-TER-NAME'
*END-OF-VAR
VAR(*LIST).TER(*LIST).PROCESSOR = 'D016ZE04'
VAR(*LIST).TER(*LIST).STATION = '*'
VAR(*LIST).TER(*LIST).CHECK-MODE(*LIST) = '*APP-TER-NAME'
*END-OF-VAR
VAR(*LIST).TER(*LIST).PROCESSOR = 'PGTD1563'
VAR(*LIST).TER(*LIST).STATION = '$$$060//'
VAR(*LIST).TER(*LIST).CHECK-MODE(*LIST) = '*NET-TER-NAME'
VAR(*LIST).TER(*LIST).CHECK-MODE(*LIST) = '*APP-TER-NAME'
*END-OF-VAR
VAR(*LIST).USER-ID(*LIST) = 'SYSDUMP'
VAR(*LIST).USER-ID(*LIST) = 'SYSPRIV'
VAR(*LIST).USER-ID(*LIST) = 'SYSUSER'
VAR(*LIST).USER-ID(*LIST) = 'TSOS'
*END-OF-VAR
```

SHOW-USER-GROUP
Benutzergruppeneintrag anzeigen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Informiert über einen Benutzergruppeneintrag im Benutzerkatalog des angegebenen Pubset.

Die Funktionalität des Kommandos hängt von der Privilegierung des Kommandogebers ab (bezogen auf die Pubsets, für die das Kommando gegeben wird).

Fall 1:
Kommandogeber ist ein systemglobaler Benutzerverwalter auf dem Home-Pubset der laufenden BS2000-Sitzung.

Informationsumfang:

Gruppenhierarchie:	keine Einschränkung
Informationsart:	keine Einschränkung
Pubset:	keine Einschränkung

Fall 2:
Kommandogeber ist ein Gruppenverwalter auf dem unter PUBSET angegebenen Pubset:

Informationsumfang:

Gruppenhierarchie:	nur Informationen über Benutzergruppen, zu deren Verwaltung der Kommandogeber berechtigt ist (Gruppenhierarchie)
Informationsart:	keine Einschränkung
Pubset:	keine Einschränkung

Fall 3:
Kommandogeber ist ein nicht-privilegierter Benutzer auf dem unter PUBSET angegebenen Pubset:

Informationsumfang:	
Gruppenhierarchie:	nur Information über die eigene Benutzergruppe
Informationsart:	nur Name der Benutzergruppe und Mitgliederliste (keine Mitgliederliste, wenn die eigene Gruppe *UNIVERSAL ist)
Pubset:	nur Information über den Home-Pubset der laufenden BS2000-Sitzung.

Die Prüfung, ob das Kommando von einem privilegierten Benutzer gegeben wird, erfolgt gegen den unter dem Operanden PUBSET angegebenen Pubset.

```
SHOW-USER-GROUP

 GROUP-IDENTIFICATION = *OWN / *ALL / *UNIVERSAL / list-poss(127): <name 1..8>
,PUBSET = *HOME / *ALL / list-poss(127): <cat-id 1..4>
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
,INFORMATION = *ALL / *MEMBER-LIST / *SUB-GROUP-LIST / *GROUP-ATTRIBUTES /
                *ACCOUNT-NUMBER(...) / *SUMMARY
   *ACCOUNT-NUMBER(...)
      | ACCOUNT-NUMBER = *ALL / list-poss(127): <alphanum-name 1..8>
```

GROUP-IDENTIFICATION =
Benutzergruppe, für die Informationen gewünscht werden.

GROUP-IDENTIFICATION = *OWN
Über die Benutzergruppe, der der Kommandogeber angehört, werden Informationen bereitgestellt.

GROUP-IDENTIFICATION = *ALL
Über alle Benutzergruppen werden Informationen bereitgestellt.

GROUP-IDENTIFICATION = *UNIVERSAL
Über die Benutzergruppe *UNIVERSAL werden Informationen bereitgestellt.

*UNIVERSAL ist ein Sonderfall. Für die Gruppe selbst (GROUP-ATTRIBUTES) werden nur folgende Informationen bereitgestellt:
– Gruppenverwalter und dessen ADMINISTRATION-AUTHORITY
– Angaben über den Gruppenzugriff auf Dateien und Jobvariablen, die mit BACL geschützt sind (BASIC-ACL-ACCESS).

Die übrigen zusammengefassten Informationen (SUB-GROUP-LIST, MEMBER-LIST) werden mit Ausnahme von ACCOUNT-NUMBER wie bei anderen Gruppen zur Verfügung gestellt.

Diese Informationen sind nur dem systemglobalen Benutzerverwalter und dem *UNIVERSAL-Gruppenverwalter zugänglich.

GROUP-IDENTIFICATION = list-poss(127): <name 1..8>
Benutzergruppenkennung, über die Informationen bereitgestellt werden. Ist der Kommandogeber Gruppenverwalter, ist sein Recht zur Informationsanforderung auf seine eigene Gruppe und die hierarchisch unter seiner Gruppe liegende Gruppenhierarchie beschränkt.

Ist der Kommandogeber mit dem Recht „systemglobale Benutzerverwaltung“ ausgestattet, darf er Informationen über beliebige Benutzergruppeneinträge einholen. Für einen nicht-privilegierten Benutzer ist nur die Angabe der eigenen Gruppenkennung erlaubt.

PUBSET =
Pubset, aus dessen Benutzerkatalog Informationen bereitgestellt werden sollen. Für einen nicht-privilegierten Benutzer ist hier nur die Angabe des Home-Pubset der laufenden Sitzung erlaubt.

PUBSET = *HOME
Die Information wird dem Benutzerkatalog des Home-Pubset entnommen (bezogen auf den aktuellen Systemlauf).

PUBSET = *ALL
Die Information wird den Benutzerkatalogen aller zum Zeitpunkt der Kommandoeingabe zugreifbaren Pubsets entnommen. Für einen nicht-privilegierten Benutzer wird nur Information geliefert, die im Benutzerkatalog des Home-Pubset abgelegt ist.

PUBSET = list-poss(127): <cat-id 1..4>
Katalogkennungen der Pubsets, aus deren Benutzerkatalogen Information entnommen werden soll. Für einen nicht-privilegierten Benutzer ist nur die Angabe des Home-Pubset erlaubt.

OUTPUT =
Legt fest, auf welche Systemdatei die Ausgabe der Information erfolgen soll.

OUTPUT = *SYSOUT
Die Information wird auf die Systemdatei SYSOUT ausgegeben.

OUTPUT = *SYSLST
Die Information wird auf die Systemdatei SYSLST ausgegeben.

INFORMATION =
Steuert Art und Umfang der auszugebenden Informationen. Für einen nicht-privilegierten Benutzer wird nur die Mitgliederliste ausgegeben (INFORMATION=*ALL).

INFORMATION = *ALL
Sämtliche Informationen zu einer Benutzergruppe werden bereitgestellt.

INFORMATION = *MEMBER-LIST
Es wird eine Liste der Benutzergruppenmitglieder bereitgestellt.

INFORMATION = *SUB-GROUP-LIST
Es wird eine Liste der Benutzergruppen bereitgestellt.

INFORMATION = *GROUP-ATTRIBUTES
Merkmale der Benutzergruppe werden bereitgestellt.

INFORMATION = *ACCOUNT-NUMBER(...)
Abrechnungsnummern, für die Informationen bereitgestellt werden.

ACCOUNT-NUMBER = *ALL
Information über alle Abrechnungsnummern, die zum Gruppenpotential gehören, wird bereitgestellt.

ACCOUNT-NUMBER = list-poss(127): <alphanum-name 1..8>
Information über diese Abrechnungsnummern wird bereitgestellt.

INFORMATION = *SUMMARY
Ausgabe von zusammengefasster Information über Gruppen- und Systempotentiale.

Hinweis

Die Informationsausgabe erfolgt je nach vergebenen Privilegien. So kann sich der Informationsumfang z.B. unterscheiden, wenn ein Kommandogeber auf einigen Pubsets Gruppenverwalter, auf anderen jedoch nur ein nicht-privilegierter Benutzer ist.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Wurden bei der Kommandoeingabe Teilinformationen ausgegeben, wird statt

(SC2)	SC1	Maincode	Bedeutung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung

folgender Returncode ausgegeben:

(SC2)	SC1	Maincode	Bedeutung
2	0	SRM6001	Kommando mit Warnung ausgeführt

Beispiel: Ausgabe der Attribute einer Benutzergruppe

```
/show-user-group group-identification=manuals
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                              2018-03 14:16:42
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              B
GROUP-ADMINISTRATOR              ADAM    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                 MAN    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                *UNIVERSAL

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                      10
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                      10
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                      10
FREE  GROUP-HIERARCHY               9    FREE  USER-ADM                      10

TEST-OPTIONS...
MODIFICATION              *CONTROLLED
READ-PRIVILEGE                      1    WRITE-PRIVILEGE                     1

PUBLIC-SPACE-EXCESS               *NO    PUBLIC-SPACE-LIMIT      2.147.483.647
RESIDENT-PAGES                32.767    ADDRESS-SPACE-LIMIT                16
FILE-AUDIT                        *NO    CSTMP-MACRO                     *NO
MAX-ACCOUNT-RECORDS               100    TAPE-ACCESS                     *STD
TEMP-SPACE-LIMIT        2.147.483.647    DMS-TUNING-RESOURCES            *NONE
FILE-NUMBER-LIMIT          16.777.215    JV-NUMBER-LIMIT           16.777.215
WORK-SPACE-LIMIT        2.147.483.647    PHYSICAL-ALLOCATION      *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED    CRYPTO-SESSION-LIMIT             128
LINKAGE-AUDIT                 *ALLOWED    NET-STORAGE-USAGE            *ALLOWED

BASIC-ACL-ACCESS   *EXTENDED-BY-GUARD    GUARDNAME                  $TSOS.GUARD

PROFILE-IDS             STDPROFILE

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

GROUP-MEMBERS                ADAM
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Erhält eine S-Variable keinen aktuellen Wert, wird ihr ein Leerstring (Typ S) oder die Zahl 0 (Typ I) zugewiesen. Dies gilt insbesondere bei GROUP-IDENTIFICATION=*UNIVERSAL für die S-Variablen, denen kein sinnvoller Wert zugewiesen werden kann.

Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *ALL	1
INFORMATION = *GROUP-ATTRIBUTES	2
INFORMATION = *ACCOUNT-NUMBER	3
INFORMATION = *MEMBER-LIST	4
INFORMATION = *SUB-GROUP-LIST	5
INFORMATION = *SUMMARY	6

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Abrechnungsnummer der Benutzergruppenkennung	var(*LIST).ACCOUNT(*LIST).ACCOUNT	S	<alphanum-name 1..8>	1,2,3
CPU-Limit für Benutzergruppenkennung	var(*LIST).ACCOUNT(*LIST).CPU-LIM	I	<integer 0..2147483647>	1,2,3
Weitergabe des Deaktivierungsverbotes durch den Gruppenverwalter an die Gruppenmitglieder oder Untergruppen	var(*LIST).ACCOUNT(*LIST). INHIBIT-DEACTIVATE	S	*NO *YES	1,2,3
Task-Attribut für Benutzer; das Recht *SYS umfasst *STD und *TP, *TP umfasst *STD	var(*LIST).ACCOUNT(*LIST). MAX-ALLOW-CATEG	S	*STD *SYS *TP	1,2,3
max. Run-Priorität	var(*LIST).ACCOUNT(*LIST). MAX-RUN-PRIO	I	<integer 30..255>	1,2,3
Gruppenverwalter ist berechtigt, das NO-CPU-LIMIT-Recht an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).ACCOUNT(*LIST).NO-CPU-LIM	S	*NO *YES	1,2,3
max. SPOOLOUT-Klasse (1 ist die höchstmögliche, 255 die niedrigste Klasse)	var(*LIST).ACCOUNT(*LIST).SPOOL-CLASS	I	<integer 1..255>	1,2,3
Gruppenverwalter ist berechtigt, die Job-Express-Funktion an Gruppenmitglieder und Untergruppen weiterzugeben	var(*LIST).ACCOUNT(*LIST).START-IMMED	S	*NO *YES	1,2,3

(Teil 1 von 5)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Gibt an, ob die Listenvariable ACCOUNT(*LIST) mindestens ein Element enthält (*LIST) oder ob die Listenvariable überhaupt nicht angelegt ist (*NONE)	var(*LIST).ACCOUNT-DEFI	S	*LIST *NONE	1,2,3
Limit für Benutzeradressraum	var(*LIST).ADDR-SPACE-LIM	I	<integer 1..2147483647>	1,2
Recht des Gruppenverwalters	var(*LIST).ADM-AUTHOR	S	*MANAGE-GROUP *MANAGE-MEMB *MANAGE-RESOURCE	1,2,6
max. Anzahl openCRYPT-Sessions in einer BS2000-Session	var(*LIST).CRYPTO-SESSION-LIM	I	<integer 1..32767>	1,2
Gruppenverwalter ist berechtigt, die CSTMP-Makro-Berechtigung an Gruppenmitglieder und Untergruppen weiterzugeben	var(*LIST).CSTMP	S	*NO *YES	1,2
Nutzungsart der DMS-Tuning-Ressourcen	var(*LIST).DMS-TUNING-RESOURCE	S	*CONCURRENT-USE *EXCL-USE *NONE	1,2
Gruppenverwalter ist berechtigt, das Recht, die AUDIT-Funktion einzuschalten, an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).F-AUDIT	S	*NO *YES	1,2
max. Anzahl an Dateien, die angelegt werden dürfen	var(*LIST).F-NUM-LIM	I	<integer 0..16777215>	1,2
Name des Guards in dem die Gruppenerweiterung für BACL-Zugriffe spezifiziert ist	var(*LIST).GUARD	S	<filename 1..18>	1,2
Gruppenverwalter (für Benutzergruppe verantwortliche Benutzerkennung)	var(*LIST).GROUP-ADM	S	*NONE <name 1..8>	1,2,6
Benutzergruppenkennung	var(*LIST).GROUP-ID	S	*UNIV <name 1..8>	1,2,3,4,5,6
Name des Gruppenmitgliedes (Benutzerkennung)	var(*LIST).GROUP-MEMB(*LIST)	S	<name 1..8>	1,4
Gibt an, ob die Listenvariable GROUP-MEMB(*LIST) mindestens ein Element enthält (*LIST) oder ob die Listenvariable überhaupt nicht angelegt ist (*NONE)	var(*LIST).GROUP-MEMB-DEFI	S	*LIST *NONE	1,4

(Teil 2 von 5)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Präfix für Gruppenmitgliedernamen	var(*LIST).GROUP-MEMB-PREFIX	S	*ANY <name 1..7>	1,2
Gruppenverwalter ist berechtigt, das Recht zur Steuerung des Hardware-AUDIT an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).HARDWARE-AUDIT	S	*ALLOW *NOT-ALLOW	1,2
max. Anzahl Jobvariablen	var(*LIST).JV-NUM-LIM	I	<integer 0..16777215>	1,2
Gruppenverwalter ist berechtigt, das Recht zur Steuerung des Linkage-AUDIT an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).LINKAGE-AUDIT	S	*ALLOW *NOT-ALLOW	1,2
Limit für Abrechnungssätze	var(*LIST).MAX-ACCOUNT-REC	S	*NO-LIM <0..32767>	1,2
Anzahl der Benutzerkennungen, die der Gruppenverwalter auf Grund der Gruppenhierarchie noch einrichten kann	var(*LIST).MAX-GROUP-MEMB. FREE-GROUP-HIERARCHY	I	<integer 0..32767>	1,2,6
Anzahl der Benutzerkennungen, die der Gruppenverwalter auf Grund der Zuteilung durch den systemglobalen Benutzerverwalter noch einrichten kann	var(*LIST).MAX-GROUP-MEMB. FREE-USER-ADM	I	<integer 0..32767>	1,2,6
maximale Anzahl der Benutzerkennungen, die der Gruppenverwalter auf Grund der Gruppenhierarchie einrichten kann	var(*LIST).MAX-GROUP-MEMB. LIM-GROUP-HIERARCHY	I	<integer 0..32767>	1,2,6
maximale Anzahl der Benutzerkennungen, die der Gruppenverwalter auf Grund der Zuteilung durch den systemglobalen Benutzerverwalter einrichten kann	var(*LIST).MAX-GROUP-MEMB. LIM-USER-ADM	I	<integer 0..32767>	1,2,6
Anzahl der Untergruppen, die der Gruppenverwalter auf Grund der Gruppenhierarchie noch einrichten kann	var(*LIST).MAX-SUB-GROUP. FREE-GROUP-HIERARCHY	I	<integer 0..32767>	1,2,6
Anzahl der Untergruppen, die der Gruppenverwalter auf Grund der Zuteilung durch den systemglobalen Benutzerverwalter noch einrichten kann	var(*LIST).MAX-SUB-GROUP. FREE-USER-ADM	I	<integer 0..32767>	1,2,6

(Teil 3 von 5)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
maximale Anzahl der Untergruppen, die der Gruppenverwalter auf Grund der Gruppenhierarchie einrichten kann	var(*LIST).MAX-SUB-GROUP. LIM-GROUP-HIERARCHY	I	<integer 0..32767>	1,2,6
maximale Anzahl der Untergruppen, die der Gruppenverwalter auf Grund der Zuteilung durch den systemglobalen Benutzerverwalter einrichten kann	var(*LIST).MAX-SUB-GROUP. LIM-USER-ADM	I	<integer 0..32767>	1,2,6
Gruppenverwalter ist berechtigt, das MODIFICATION-Recht für die Test-Optionen (CONTROLLED/UNCONTROLLED) an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).MODIF	S	*CONTR *UNCONTR	1,2
Gruppenverwalter ist berechtigt, das Recht zur Nutzung von Net-Storage-Volumes an Gruppenmitglieder bzw. Untergruppen weiterzugeben	var(*LIST).NET-STOR-USAGE	S	*NO *ALLOW	1,2
Gibt an, ob der Benutzergruppe für den Pubset die absolute Speicherplatz-Zuweisung erlaubt ist (Direktallokierung).	var(*LIST).PHYS-ALLOC	S	*NO *ALLOW	1,2
Profile-Ids der Gruppensyntaxdateien	var(*LIST).PROF-ID(*LIST)	S	<filename 1..54> <struc.-name 1..30>	1,2
Gibt an, ob die Listenvariable PROF-ID(*LIST) mindestens ein Element enthält (*LIST) oder ob die Listenvariable überhaupt nicht angelegt ist (*NONE)	var(*LIST).PROF-ID-DEFI	S	*LIST *NONE	1,2
Gruppenverwalter ist berechtigt, das Recht, den im Operanden PUBLIC-SPACE-LIMIT zugewiesenen Wert zu überschreiten, weiterzugeben	var(*LIST).PUB-SPACE-EXC	S	*ALLOW *NO *TEMP-ALLOW	1,2
max. Speicherplatz für Benutzerkennung	var(*LIST).PUB-SPACE-LIM	I	<integer 0..2147483647>	1,2
Katalogkennung des Pubsets von dem die Daten gelesen werden	var(*LIST).PUBSET	S	<cat-id 1..4>	1,2,3,4,5,6
max. Leseprivilegierung bei Nutzung von AID	var(*LIST).READ-PRIVIL	I	<integer 1..9>	1,2
max. Anzahl residenter Hauptspeicherseiten	var(*LIST).RESID-PAGE	I	<integer 0..32767>	1,2

(Teil 4 von 5)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Untergruppe	var(*LIST).SUB-GROUP(*LIST)	S	<name 1..8>	1,5
Angabe, ob Fehler bei der Kennsatzprüfung von Bändern ignoriert werden dürfen	var(*LIST).TAPE-ACCESS	S	*ALL *BYPASS-LABEL *PRIVIL *READ *STD	1,2
max. temporärer Speicherplatz	var(*LIST).TEMP-SPACE-LIM	I	<integer 0..2147483647>	1,2
Name der übergeordneten Benutzergruppe	var(*LIST).UPPER-GROUP	S	*UNIV <name 1..8>	1,2,6
Präfix für Untergruppen-Name	var(*LIST).USER-GROUP-PREFIX	S	*ANY <name 1..7>	1,2
Obergrenze für den Wert, den ein Gruppenverwalter als WORK-SPACE-LIMIT für seine Untergruppe bzw. seine Benutzer angeben darf	var(*LIST).WORK-SPACE-LIM	I	<integer 0..2147483647>	1,2
max. Schreibprivilegierung bei Nutzung von AID	var(*LIST).WRITE-PRIVIL	I	<integer 1..9>	1,2

(Teil 5 von 5)

SHOW-USER-SUSPEND
Suspendierungen anzeigen

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Dieses Kommando zeigt Suspendierungen von Benutzerkennungen an.

Es dürfen dabei angegeben werden:

– vom systemglobalen Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) alle Benutzerkennungen auf allen Pubsets

– vom Gruppenverwalter, der mindestens das Attribut MANAGE-MEMBERS besitzt, alle ihm zu- und untergeordneten Benutzerkennungen des angesprochenen Pubsets

Falls USER-ID=*ALL angegeben ist, wird jedem Benutzer die Information ausgegeben, die ihm nach den oben genannten Regeln zugänglich ist.

SHOW-USER-SUSPEND
USER-IDENTIFICATION = ***ALL** / list-poss(20): ***OWN** / <name 1..8 with-wild(32)>
,PUBSET = ***ALL** / list-poss(2000): ***HOME** / <cat-id 1..4>
,INFORMATION = ***SUMM**ARY / ***ALL**
,OUTPUT = list-poss(2): ***SYSOUT** / ***SYSLST**

USER-IDENTIFICATION = *ALL / list-poss(20): *OWN / <name 1..8 with-wild>
Benutzerkennungen, deren Suspendierungen angezeigt werden sollen.

PUBSET = *ALL / list-poss(2000): *HOME / <cat-id 1..4>
Pubset, in dessen Benutzerkatalog sich die Benutzerkennungen befinden.

INFORMATION =
Legt den Ausgabeumfang fest.

INFORMATION = *SUMMARY
Es wird die Information ausgegeben, ob eine Benutzerkennung beobachtet wird oder bereits suspendiert ist und ggf. wie lange.

INFORMATION = *ALL
Falls ein Initiator als Person beobachtet wird oder suspendiert ist, werden zusätzlich zu der mit INFORMATION = *SUMMARY ausgegebenen Information die Identifikationsmerkmale des Initiators ausgegeben.

OUTPUT =
Definiert das Ausgabemedium für die Information.

OUTPUT = *SYSOUT
Es wird auf die Systemdatei SYSOUT (im Dialog die Datensichtstation) ausgegeben.

OUTPUT = *SYSLST
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	CMD0009	Interner Fehler bei Ausgabe in S-Variable
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	OPS0002	Ausgabe in S-Variable abgebrochen
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	64	CMD0009	Ausgabe in S-Variable steht nicht zur Verfügung
	130	OPS0001	Speicherengpass beim Erzeugen einer S-Variablen
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *SUMMARY INFORMATION = *ALL	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Audit-Id	var(*LIST).AUDIT-ID	S	<alpha-name 1..16>	2
Anzahl der Fehlversuche	var(*LIST).COUNT	I	<integer 1..32767>	1, 2
Maximum der Fehlversuche	var(*LIST).COUNT-LIM	I	<integer 1..32767>	1, 2
Ende-Datum	var(*LIST).DATE	S	<date>	1, 2
Persönliche Kennung	var(*LIST).PERS-ID	S	<name 1..8>	2
Kerberos-Principal	var(*LIST).PRINCIPAL	S	<alpha-name 1..1800>	2
Terminal-Prozessor	var(*LIST).PROCESSOR	S	<name 1..8>	2
Catid des Pubsets	var(*LIST).PUBSET	S	<catid 1..4>	1, 2
Status “Beobachtung” oder “Suspendierung”	var(*LIST).STATE	S	*OBSERVE *SUSPEND	1, 2
Terminal-Station	var(*LIST).STATION	S	<name 1..8>	2
Ende-Uhrzeit	var(*LIST).TIME	S	<time>	1, 2
Benutzerkennung	var(*LIST).USER-ID	S	<name 1..8>	1, 2

UNLOCK-USER-SUSPEND
Suspendierungen aufheben

Anwendungsbereich: USER-ADMINISTRATION

Privilegierung: STD-PROCESSING, USER-ADMINISTRATION

Dieses Kommando hebt die Suspendierungen von Benutzerkennungen auf.

Es dürfen dabei angegeben werden:

– vom systemglobalen Benutzerverwalter (Inhaber des Privilegs USER-ADMINISTRATION) alle Benutzerkennungen auf allen Pubsets

– vom Gruppenverwalter, der mindestens das Attribut MANAGE-MEMBERS besitzt, alle ihm zu- und untergeordneten Benutzerkennungen des angesprochenen Pubsets

Falls USER-ID=*ALL angegeben ist, hebt jeder Verwalter die Suspendierung der Benutzerkennungen auf, die ihm nach den oben genannten Regeln zugänglich sind.

```
UNLOCK-USER-SUSPEND

 USER-IDENTIFICATION = *ALL / list-poss(20): *OWN / <name 1..8 with-wild(32)>
,PUBSET = *HOME / <cat-id 1..4>
```

USER-IDENTIFICATION = *ALL / list-poss(20): *OWN / <name 1..8 with-wild>
Benutzerkennungen, deren Suspendierungen aufgehoben werden sollen.

PUBSET = *HOME / <cat-id 1..4>
Pubset, in dessen Benutzerkatalog sich die Benutzerkennungen befinden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando fehlerfrei ausgeführt
2	0	SRM6001	Kommando mit Warnung ausgeführt
	32	SRM6020	Systemfehler während der Kommandobearbeitung
	64	SRM6040	Semantikfehler während der Kommandobearbeitung
	130	SRM6030	Kommando kann vorübergehend nicht ausgeführt werden

3.5 SRPM-Makros

In den folgenden Abschnitten werden die Makros beschrieben, die ausschließlich verwendet werden können, wenn SECOS (SRPM) geladen ist. Diejenigen Makros, die auch ohne SECOS verwendet werden können, sind im Handbuch „Makroaufrufe an den Ablaufteil“ [16] beschrieben.

Die Beschreibung der Makros ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion des Makros erklärt, dann folgt das Makroformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung sind die DSECTS expandiert dargestellt, die Returncodes werden erklärt und es folgt gegebenenfalls ein Anwendungsbeispiel.

Funktionelle Übersicht

Folgende Makros stehen zur Verfügung:

Folgende Makros sind im vorliegenden Handbuch SECOS (SRPM) beschrieben

GETUGR	Gruppenzugehörigkeit einer Benutzerkennung ermitteln
SRMKPR	Namen des Principal ausgeben
SRMPID	Persönliche Benutzerkennung ermitteln
SRMSUG	Gruppeninformation ausgeben

Folgende Makros sind im Handbuch „Makroaufrufe an den Ablaufteil“ [16] beschrieben:

CHKPRV	Systemprivilegien abfragen
RDUID	Benutzerkennung lesen
SRMUINF	Eintrag im Benutzerkatalog ausgeben und Ausgabebereich generieren

GETUGR
Gruppenzugehörigkeit einer Benutzerkennung ermitteln

Der Makro GETUGR liefert zu einer Benutzerkennung den zugehörigen Gruppennamen. Zur Ermittlung der Gruppenzugehörigkeit wird die Gruppenstruktur herangezogen, die auf dem Home-Pubset der laufenden Sitzung hinterlegt ist. Ist die Benutzerkennung der Standardgruppe *UNIVERSAL zugeordnet, so ist der Gruppenname nicht definiert und der Returncode wird mit einem entsprechenden Wert versehen.

Anwendung: Systemverwaltermakro

Makrotyp: S-Typ (Standardform / E-Form / L-Form / C-Form / D-Form)

Makro	**Operanden**	
GETUGR	MF=	C / D / L / E
	,PREFIX =	p / S
	,PARAM =	(r) / addr

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Vor dem Aufruf des Makros GETUGR muss das Feld SRMUUID mit der Benutzerkennung versorgt werden, deren Gruppenname ermittelt werden soll.

Wenn ein Benutzergruppenverwalter oder systemglobaler Benutzerverwalter die Gruppenzugehörigkeit einer Benutzerkennung ermitteln will, die nicht auf dem Home-Pubset eingetragen ist, muss er zusätzlich die Katalogkennung dieses Pubsets in das Feld SRMUPVS eintragen. Gibt ein Benutzer, der keines dieser Verwaltungsprivilegien hat, das Pubset explizit an, wird der Aufruf mit Parameterfehler zurückgewiesen.

Ausgabe-Operanden:

Der Gruppenname wird im Feld SRMGGID der Parameterliste abgelegt. Gehört die Benutzerkennung zur Standardgruppe *UNIVERSAL, so ist der Inhalt des Feldes nicht definiert und der Returncode enthält einen entsprechenden Wert.

Parameterliste (GETUGR MF=D)

```
SRMUGT   DSECT ,
               *,##### PREFIX=S, MACID=RMU #####
*
SRMUFHDR FHDR  MF=(C,SRMU),EQUATES=NO                    standard header
SRMUFHDR DS    0A
SRMUFHE  DS    0XL8            0   GENERAL PARAMETER AREA HEADER
*
SRMUIFID DS    0A              0   INTERFACE IDENTIFIER
SRMUFCTU DS    AL2             0   FUNCTION UNIT NUMBER
*                                  BIT 15    HEADER FLAG BIT,
*                                  MUST BE RESET UNTIL FURTHER NOTICE
*                                  BIT 14-12 UNUSED, MUST BE RESET
*                                  BIT 11-0  REAL FUNCTION UNIT NUMBER
SRMUFCT  DS    AL1             2   FUNCTION NUMBER
SRMUFCTV DS    AL1             3   FUNCTION INTERFACE VERSION NUMBER
*
SRMURET  DS    0A              4   GENERAL RETURN CODE
SRMUSRET DS    0AL2            4   SUB RETURN CODE
SRMUSR2  DS    AL1             4   SUB RETURN CODE 2
SRMUSR1  DS    AL1             5   SUB RETURN CODE 1
SRMUMRET DS    0AL2            6   MAIN RETURN CODE
SRMUMR2  DS    AL1             6   MAIN RETURN CODE 2
SRMUMR1  DS    AL1             7   MAIN RETURN CODE 1
SRMUFHL  EQU   8               8   GENERAL OPERAND LIST HEADER LENGTH
*
*   main return codes
SRMUOK   EQU   0                       group id of user valid
SRMUUNI  EQU   1                       user is in group *UNIVERSAL
SRMUUND  EQU   2                       user not defined on pubset
SRMUPER  EQU   3                       parameter error
SRMUPNA  EQU   5                       pubset not available
SRMUSER  EQU   255                     system error
*
SRMUUID  DS    CL8                     user id for which information
*                                      is sought
SRMUPVS  DS    CL4                     pubset on which user is
*                                      defined
SRMUGID  DS    CL8                     group id for user on pubset
SRMU#    EQU   *-SRMUFHDR
```

Hinweis

Der Aufruf GETUGR verändert die Register R1, R14 und R15.

Returncodes

Zusätzlich zu den Standardreturncodes können folgende Returncodes auftreten:

SC1	Maincode	Erläuterung
ESMRFSP	SRMUOK	Gruppenname wurde ermittelt und im Parameterfeld SRMGGID hinterlegt.
ESMRFSP	SRMUUNI	Die Benutzerkennung gehört zur Standardgruppe *UNIVERSAL.
ESMRFSP	SRMUUND	Die Benutzerkennung ist auf dem Pubset nicht eingetragen.
ESMRCAR	SRMUPER	Parameterfehler
ESMRCAR	SRMUPNA	Pubset nicht verfügbar
ESMRIER	SRMUSER	Systemfehler

Beispiel

Ermitteln des Gruppennamens zur Benutzerkennung ’SRPMUSER’ und prüfen, ob ein Fehler aufgetreten ist.

```
GETUGR   START
*-------------------------------------------------------------------*
*  PROGRAMM: HANDBUCH-BEISPIEL GETUGR  SRPM-TESTS                   *
*-------------------------------------------------------------------*
GETUGR   RMODE ANY
GETUGR   AMODE ANY
         GPARMOD 31
         BALR  3,0
         USING *,3
*-------------------------------------------------------------------*
*    LESEN DER BENUTZERGRUPPE FUER BENUTZER "SRPMUSER"              *
*-------------------------------------------------------------------*
         MVC   SRMUUID,='SRPMUSER'
         GETUGR MF=E,PARAM=GICHKL
         CLI   SRMUMR1,SRMUOK
         BNE   FEHLER
*                           BEARBEITEN DER USER-GROUPID
         B     ENDE
FEHLER   EQU   *
*                           ANDERE BEHANDLUNG
ENDE     TERM
**------------------------------------------------------------------*
GICHKC   GETUGR MF=C
         ORG   GICHKC
GICHKL   GETUGR MF=L
         END
```

SRMKPR
Namen des Principal ausgeben

Der Makro legt den Namen des Principals des Client in einem angegebenen Speicherbereich ab, wenn der Dialog über Kerberos initiiert wurde.

Diese Information ist identisch mit dem Inhalt der System-Jobvariablen $SYSJV.PRINCIPAL.

Anwendung: Benutzermakro, Gruppenverwaltermakro, Systemverwaltermakro

Makrotyp: S-Typ (Standardform / E-Form / L-Form / C-Form / D-Form)

Makro	Operanden	
SRMKPR	MF=	C / D / L / E
	,PREFIX =	p / S
	,DATA =	structure(2): (1) data_addr: *NONE / <var: pointer> (2) data_len: 0 / <integer 1..1800> / <var: int:2>
	,PARAM =	<name 1..27>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DATA Speicherbereich, in den der Name des Principal des Clients abgelegt wird.

data_addr: Adresse des Speicherbereichs

data_len: Länge des Speicherbereichs

Returncodes

Zusätzlich zu den Standardreturncodes können folgende Returncodes auftreten:

SC1	Maincode	Erläuterung
00	0000	normale Ausführung
40	0001	Warnung: Ausgabe abgeschnitten
40	0002	Task hat keinen Principal
40	0003	Task nicht gefunden
01	000A	Ungültige Parameter
20	000B	Interner Fehler aufgetreten

SRMPID
Persönliche Benutzerkennung ermitteln

Dieser Makro ermittelt die persönliche Benutzerkennung des Client, wenn der Dialog über persönliches Logon initiiert wurde.

Diese Information ist identisch mit dem Inhalt der System-Jobvariablen $SYSJV.PERS-ID.

Anwendung: Benutzermakro, Gruppenverwaltermakro, Systemverwaltermakro

Makrotyp: S-Typ (Standardform / E-Form / L-Form / C-Form / D-Form)

Makro	Operanden	
SRMPID	MF= ,PREFIX = ,TID= ,PARAM =	C / D / L / E p / S *OWN / <integer 0..2147483647> / <var: int:4> <name 1..27>

TID Task-Id der Task, deren persönliche Benutzerkennung ermittelt werden soll

=*OWN Die persönliche Benutzerkennung der eigenen Task wird ermittelt.

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Returncodes

Zusätzlich zu den Standardreturncodes können folgende Returncodes auftreten:

SC1	Maincode	Erläuterung
00	0000	normale Ausführung
40	0001	Task hat keinen persönliche Benutzerkennung
01	000A	Ungültige Parameter
20	000B	Interner Fehler aufgetreten

SRMSUG
Gruppeninformation ausgeben

Aufruf aus der Kennung eines systemglobalen Benutzerverwalters:

Es werden alle gruppenbezogenen Daten beliebiger Benutzergruppen bereitgestellt.

Aufruf aus der Kennung eines Gruppenverwalters:

Die volle Information über Gruppenmitglieder und Untergruppen zur Benutzergruppe des Gruppenverwalters kann angefordert werden.

Aufruf aus einer Benutzerkennung, die weder das Privileg Benutzerverwaltung besitzt, noch Gruppenverwalter ist:

Der Benutzer erhält über seine Benutzergruppe, die auf dem Home-Pubset der laufenden Sitzung hinterlegt ist, nur zwei Informationen:

– den Namen der Benutzergruppenkennung

– die Namen der Benutzerkennungen der Mitglieder seiner Gruppe (dies gilt wiederum nicht für Mitglieder von *UNIVERSAL)

Die Information über Benutzergruppen wird auf jedem Pubset im Benutzerkatalog abgelegt. Verantwortlich für die Verwaltung der Einträge für Benutzergruppen sind Gruppenverwalter und systemglobaler Benutzerverwalter.

Informationen über Benutzergruppen stellt der Makro SRMSUG aus dem Benutzerkatalog bereit.

Anwendung: Benutzermakro, Gruppenverwaltermakro, Systemverwaltermakro

Makrotyp: S-Typ (Standardform / E-Form / L-Form / C-Form / D-Form)

Makro	Operanden	
SRMSUG	MF=	C / D / L / E
	,PREFIX =	p / S
	,XPAND =	PARAM / INFO
	,AREA@ =	addr
	,AREALG =	length
	,VERSION =	1 / 2 / 3 / 4 / 5 / 6
	,GROUPID =	*FIRST / groupid
	,MEMBER =	*FIRST / userid
	,SUBGID =	*FIRST / groupid
	,ACCOUNT =	*FIRST / account
	,ACTION =	READ / READNEXT
	,PVS =	*HOME / catid
	,INFO =	ATTRIBUT / MEMBERS / SUBGROUP /ACCNTRES / PROFILE
	,PARAM =	(r) / addr

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=INFO Die Modelle der Teilbereiche der Ausgabe.

AREA@ Adresse des Bereiches, in dem die Benutzergruppeninformation bereitgestellt werden soll.

= addr Symbolischer Name der Adresse

AREALG Definiert die Länge von AREA@. Die Länge, die zur Aufnahme der vollständigen Information benötigt wird, ist vom Wert des Operanden INFO abhängig. Wenn die spezifizierte Länge nicht ausreichend ist, werden die einzutragenden Daten abgeschnitten und der entsprechende Returncode wird gesetzt. Die jeweils benötigte Länge kann mit den durch den Parameter XPAND erzeugten Werten spezifiziert werden.

= length Länge des Speicherbereiches.

VERSION Gibt an, welche Ausgabebereiche generiert werden sollen. Die Ausgabebereiche werden in Abhängigkeit vom Operanden INFO generiert.

VERSION = 1 gilt ab SECOS V1.0A.
VERSION = 2 gilt ab SECOS V2.0A.
VERSION = 3 gilt ab SECOS V2.2A.
VERSION = 4 gilt ab SECOS V3.0A.
VERSION = 5 gilt ab SECOS V5.1A.
VERSION = 6 gilt ab SECOS V5.4A.

Der Operand VERSION muss bezüglich eines Funktionsaufrufs konsistent sein. Das heißt, dass der Wert von Version gleich bleiben muss, wenn Parameterbereiche einer Aufruffolge getrennt generiert werden (MF=E/L). Beim Generieren der zugehörigen DSECT, CSECT muss ebenfalls der gleiche Wert eingetragen werden.

GROUPID Vereinbart die Benutzergruppenkennung, über die Information angefordert wird.

= *OWN Information über die Benutzergruppe, der der Aufrufer zugeordnet ist, wird ausgegeben.

= *FIRST Die Angabe von *FIRST ist nur in Verbindung mit ACTION = READNEXT zulässig.

Wenn der Aufrufer ein systemglobaler Benutzerverwalter ist, wird die Information für jede auf dem angegebenen Pubset eingetragene Benutzergruppe geliefert.

Ist der Aufrufer ein Gruppenverwalter, erhält er die volle Information über seine Benutzergruppe und alle hierarchisch darunter liegenden.

Ist der Aufrufer weder Gruppenverwalter noch systemglobaler Benutzerverwalter, erhält er nur Informationen über seine eigene Benutzergruppe.

= groupid Benutzergruppenkennung (8 Zeichen).

MEMBER Vereinbart das Benutzergruppenmitglied, über das Information angefordert wird.

= *FIRST Die Angabe von *FIRST ist nur in Verbindung mit ACTION = READNEXT zulässig.

= userid Benutzerkennung (8 Zeichen).

SUBGID Vereinbart die Benutzergruppenkennung einer Untergruppe, über die Information angefordert wird.

= *FIRST Die Angabe von *FIRST ist nur in Verbindung mit ACTION = READNEXT zulässig.

= groupid Benutzergruppenkennung (8 Zeichen).

ACCOUNT Vereinbart die Abrechnungsnummer, über die Informationen bereitgestellt werden sollen.

= *FIRST Die erste Abrechnungsnummer einer Benutzergruppenkennung wird herangezogen. Der Operand ist nur unter Angabe von GROUPID und ACTION = READNEXT zulässig.

= account Abrechnungsnummer (8 Zeichen)

ACTION

= READ Daten aus dem Eintrag der unter GROUPID angegebenen Benutzergruppenkennung werden bereitgestellt.

= READNEXT
Die jeweils nächste Informationseinheit zu dem unter INFO= angeforderten Objekt wird bereitgestellt.

PVS Vereinbart das PVS, aus dessen Benutzerkatalog Informationen über Benutzergruppen bereitgestellt werden sollen.

= *HOME Die Informationen werden dem Home-Pubset entnommen.

= catid Katalogkennung des Pubsets, dem die Information entnommen werden soll (4 Zeichen).

INFO Vereinbart die Art der Information, die aus dem Benutzergruppeneintrag bereitgestellt werden soll.

= ATTRIBUT
Die Merkmale der Benutzergruppe werden ausgegeben.

= MEMBERS
Die Benutzerkennungen der Gruppenmitglieder werden bereitgestellt (je Aufruf eine Benutzerkennung). Der Operand ist nur unter Angabe von GROUPID und ACTION = READNEXT zulässig.

= SUBGROUP
Die Benutzergruppenkennungen der Untergruppen werden bereitgestellt (je Aufruf eine Benutzergruppenkennung). Der Operand ist nur unter Angabe von GROUPID und ACTION = READNEXT zulässig.

= ACCNTRES

Informationen über die Privilegien und Ressourcen der Abrechnungsnummern aus dem jeweiligen Gruppenpotential werden bereitgestellt.

= PROFILE

Die Profile-Ids der Benutzergruppe werden ausgegeben. Der Operand ist nur unter Angabe von GROUPID und ACTION = READ zulässig.

PARAM Adresse der durch MF = L erzeugten Parameterliste (nur bei MF=E).

= (r) Die Adresse steht im angegebenen Register

= addr Symbolischer Name der Adresse (ausgerichtet auf Wortgrenze).

Parameterliste SRMSUG MF=D,XPAND=PARAM

```
SRMSUG   DSECT ,
               *,##### PREFIX=S, MACID=RMS #####
**
SRMSUGPL DS    OF                    SHOW USERGROUP PL
SRMSFHDR FHDR  MF=(C,SRMS),EQUATES=NO
SRMSFHDR DS    0A
SRMSFHE  DS    0XL8            0     GENERAL PARAMETER AREA HEADER
*
SRMSIFID DS    0A              0     INTERFACE IDENTIFIER
SRMSFCTU DS    AL2             0     FUNCTION UNIT NUMBER
*                                    BIT 15    HEADER FLAG BIT,
*                                    MUST BE RESET UNTIL FURTHER NOTICE
*                                    BIT 14-12 UNUSED, MUST BE RESET
*                                    BIT 11-0  REAL FUNCTION UNIT NUMBER
SRMSFCT  DS    AL1             2     FUNCTION NUMBER
SRMSFCTV DS    AL1             3     FUNCTION INTERFACE VERSION NUMBER
*
SRMSRET  DS    0A              4     GENERAL RETURN CODE
SRMSSRET DS    0AL2            4     SUB RETURN CODE
SRMSSR2  DS    AL1             4     SUB RETURN CODE 2
SRMSSR1  DS    AL1             5     SUB RETURN CODE 1
SRMSMRET DS    0AL2            6     MAIN RETURN CODE
SRMSMR2  DS    AL1             6     MAIN RETURN CODE 2
SRMSMR1  DS    AL1             7     MAIN RETURN CODE 1
SRMSFHL  EQU   8               8     GENERAL OPERAND LIST HEADER LENGTH
*
**
**  SRPM SPECIFIC RETURN CODE IN &P.RMSMR1
**
SRMSOK   EQU   X'00'                 OK
SRMSINV  EQU   X'04'                 INVALID
SRMSNFD  EQU   X'08'                 NOT FOUND
SRMSPNA  EQU   X'0C'                 PVS NOT AVAILABLE
SRMSRES  EQU   X'10'                 SHORTAGE OF RESOURCES
SRMSSYS  EQU   X'FF'                 SYSTEM ERROR
**
**  SRPM SPECIFIC RETURN CODE IN &P.RMSMR2
**                                                      |   MR1:
SRMSEOF  EQU   X'04'                 LOGICAL EOF        |   OK
SRMSCUT  EQU   X'08'                 ENTRY CUTTED       |   OK
SRMSPL   EQU   X'00'                 PARAMETERLIST      |   INV
SRMSAR@  EQU   X'04'                 AREA@              |   INV
SRMSGRP  EQU   X'00'                 GROUP ENTRY        |   NFD
SRMSACC  EQU   X'04'                 ACCOUNTNUMBER      |   NFD
SRMSUID  EQU   X'08'                 USERID/MEMBERID    |   NFD
**
```

```
**
SRMSA@   DS    A                   ADDRESS OF INFORMATION AREA
SRMSALG  DS    H                   LENGTH OF INFORMATION AREA
SRMSACT  DS    X                   ACTION CODE:
SRMSARD  EQU   X'01'                  READ
SRMSANXT EQU   X'02'                  READ NEXT
SRMSINFO DS    X                   INFORMATION:
SRMSIATT EQU   X'01'                  ATTRIBUTES OF USERGROUP
SRMSIMEM EQU   X'02'                  MEMBERS OF USERGROUP
SRMSISUB EQU   X'03'                  GROUPIDS OF SUBGROUPS
SRMSIRES EQU   X'04'                  RESOURCES AND PRIVILEGES
SRMSIPID EQU   X'05'                  PROFILE_IDS
SRMSACC# DS    CL8                 ACCOUNT NUMBER
SRMSMBR  DS    CL8                 MEMBER ID
SRMSSUB  DS    CL8                 SUBGROUP ID
SRMSGID  DS    CL8                 USERGROUP
SRMSPVS  DS    CL4                 PVS
**
SRMSUG#  EQU   *-SRMSUGPL         LENGTH OF PARAMETER LIST       *V103
```

Returncodes

Zusätzlich zu den Standardreturncodes können folgende Returncodes auftreten:

SC1	Maincode	Erläuterung
00	0000	normale Ausführung
00	0400	logisches Dateiende nach READNEXT
00	0800	Eintrag abgeschnitten
40	0004	Operandenfehler
40	0404	AREA@: Ausrichtungsfehler
00	0008	Gruppeneintrag nicht gefunden
00	0408	Abrechnungsnummer nicht gefunden
00	0808	Benutzerkennung auf Pubset nicht gefunden
00	1008	Untergruppenkennung auf Pubset nicht gefunden
40	000C	Pubset nicht verfügbar
80	0010	Betriebsmittelengpass
20	00FF	Systemfehler

Die Werte des SUBCODE1 entsprechen folgenden Vereinbarungen im Function-Header (FHDR):

X’00’ : ESMRFSP (FCT SUCCESSFUL)

X’04’ : ESMRAER (ALIGNEMENT ERROR)

X’20’ : ESMRIER (INTERNAL ERROR)

X’40’ : ESMRCAR (CORRECT AND RETRY)

X’80’ : ESMRWAR (WAIT AND RETRY)

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=1

```
SRMAUG   DSECT ,
               *,##### PREFIX=S, MACID=RMA #####
**
SRMAUGAT DS    OF                  SHOW USERGROUP ATTRIBUTES
**
SRMAGID  DS    CL8                 GROUP IDENTIFICATION
SRMAGUNI EQU   ' '                    UNIVERSAL GROUP
SRMAUPPR DS    CL8                 UPPER GROUP
** GUNI  EQU   ' '                    UNIVERSAL GROUP
SRMAADM  DS    CL8                 GROUP ADMINISTRATOR
SRMAADNO EQU   ' '                    GROUP WITHOUT GROUP ADMIN
SRMAMGMG DS    H                   MAX GROUP MEMBERS GROUP
SRMAMGMS DS    H                   MAX GROUP MEMBERS SYSTEM       *V103
SRMAMSGG DS    H                   MAX SUB GROUPS GROUP
SRMAMSGS DS    H                   MAX SUB GROUPS SYSTEM          *V103
SRMAPSLI DS    F                   PUBLIC SPACE LIMIT             *V106
SRMAADDR DS    H                   ADDRESS SPACE LIMIT
SRMARPAG DS    H                   RESIDENT PAGES
SRMAACRC DS    H                   MAX ACCOUNT RECORDS
SRMATOP  DS    OX                  TEST OPTIONS:
SRMATRDP DS    X                      READ PRIVILEGE
SRMATWRP DS    X                      WRITE PRIVILEGE
SRMATMOD DS    X                      MODIFICATION BY:
SRMATMAD EQU   1                         ADMINISTRATOR
SRMATMUS EQU   2                         USER
SRMAATH  DS    X                   ADM AUTHORITY:
SRMAARES EQU   1                      MANAGE RESOURCES
SRMAAMEM EQU   2                      MANAGE MEMBERS
SRMAAGRP EQU   3                      MANAGE GROUPS
SRMATPIG DS    X                   TPIGNORE (TAPE ACCESS):
SRMATPN  EQU   1                      NO (STD): MSG NOT IGNORED
SRMATPY  EQU   2                      YES: ERROR MSG IGNORED
SRMATPRD EQU   3                      READ: ERROR MSG IGNORED - INPUT
SRMATPBP EQU   4                      BYPASS LABEL
```

```
SRMATPAL EQU   5                     ALL ERROR MSG IGNORED
SRMAIND1 DS    X                   INDICATOR BYTE 1:
SRMAACNL EQU   X'80'                 MAX ACCOUNT RECORDS:
**                                      S: NO LIMIT
**                                      R: VALID
SRMAENF  EQU   X'40'                 ENFORCEMENT:
**                                      S: PERMITTED
**                                      R: NOT PERMITTED
SRMAAUDT EQU   X'20'                 AUDIT:
**                                      S: ALLOWED
**                                      R: NOT ALLOWED
SRMACSTM EQU   X'10'                 CSTMP MAKRO:
**                                      S: ALLOWED
**                                      R: NOT ALLOWED
**
SRMAAT#  EQU   *-SRMAUGAT         LENGTH OF ATTRIBUTES ENTRY     *V103
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=2

```
SRMAUG   DSECT ,
              *,##### PREFIX=S, MACID=RMA #####
*************************************************************** V205
*        V E R S I O N  =  0 0 2                               * V205
*************************************************************** V205
SRMAUGAT DS    0F                  SHOW USERGROUP ATTRIBUTES      V205
**                                                               V205
SRMAGID  DS    CL8                 GROUP IDENTIFICATION           V205
SRMAGUNI EQU   ' '                    UNIVERSAL GROUP             V205
SRMAUPPR DS    CL8                 UPPER GROUP                    V205
** GUNI  EQU   ' '                    UNIVERSAL GROUP             V205
SRMAADM  DS    CL8                 GROUP ADMINISTRATOR            V205
SRMAADNO EQU   ' '                    GROUP WITHOUT GROUP ADMIN   V205
SRMAGPF  DS    CL7                 USER GROUP PREFIX              V205
SRMAMPF  DS    CL7                 GROUP MEMBER PREFIX            V205
SRMAANY  EQU   ' '                    NO PREFIX SPECIFIED         V205
SRMARES1 DS    CL2                 RESERVED                       V205
SRMAMGMG DS    H                   MAX GROUP MEMBERS GROUP        V205
SRMAMGMS DS    H                   MAX GROUP MEMBERS SYSTEM       V205
SRMAMSGG DS    H                   MAX SUB GROUPS GROUP           V205
SRMAMSGS DS    H                   MAX SUB GROUPS SYSTEM          V205
SRMAPSLI DS    F                   PUBLIC SPACE LIMIT             V205
SRMAADDR DS    H                   ADDRESS SPACE LIMIT            V205
SRMARPAG DS    H                   RESIDENT PAGES                 V205
SRMAACRC DS    H                   MAX ACCOUNT RECORDS            V205
SRMARES2 DS    CL2                 RESERVED                       V205
SRMAFIL  DS    F                   FILE NUMBER LIMIT              V205
SRMAJVL  DS    F                   JV NUMBER LIMIT                V205
```

```
SRMATMSL DS    F                  TEMPORARY SPACE LIMIT           V205
SRMAPSE  DS    X                  PUBLIC SPACE EXCESS/ENFORCEMENT V205
SRMAPSEN EQU   1                     NO                           V205
SRMAPSET EQU   2                     TEMPORARILY ALLOWED          V205
SRMAPSEY EQU   3                     YES                          V205
SRMATUN  DS    X                  DMS TUNING RESOURCES            V205
SRMATUNN EQU   1                     NONE                         V205
SRMATUNC EQU   2                     CONCURRENT USE               V205
SRMATUNE EQU   3                     EXCLUSIVE USE                V205
SRMATOP  DS    OX                 TEST OPTIONS:                   V205
SRMATRDP DS    X                     READ PRIVILEGE               V205
SRMATWRP DS    X                     WRITE PRIVILEGE              V205
SRMATMOD DS    X                     MODIFICATION BY:             V205
SRMATMCO EQU   1                        CONTROLLED                V205
SRMATMUN EQU   2                        UNCONTROLLED              V205
SRMAATH  DS    X                  ADM AUTHORITY:                  V205
SRMAARES EQU   1                     MANAGE RESOURCES             V205
SRMAAMEM EQU   2                     MANAGE MEMBERS               V205
SRMAAGRP EQU   3                     MANAGE GROUPS                V205
SRMATPIG DS    X                  TPIGNORE (TAPE ACCESS):         V205
SRMATPN  EQU   1                     NO (STD): MSG NOT IGNORED    V205
SRMATPY  EQU   2                     YES: ERROR MSG IGNORED       V205
SRMATPRD EQU   3                     READ: ERROR MSG IGNORED - INPV205
SRMATPBP EQU   4                     BYPASS LABEL                 V205
SRMATPAL EQU   5                     ALL ERROR MSG IGNORED        V205
SRMAIND1 DS    X                  INDICATOR BYTE 1:               V205
SRMAACNL EQU   X'80'                  MAX ACCOUNT RECORDS:         V205
**                                       S: NO LIMIT              V205
**                                       R: VALID                 V205
SRMAAUDT EQU   X'20'                  AUDIT:                       V205
**                                       S: ALLOWED               V205
**                                       R: NOT ALLOWED           V205
SRMACSTM EQU   X'10'                  CSTMP MAKRO:                 V205
**                                       S: ALLOWED               V205
**                                       R: NOT ALLOWED           V205
**                                                                V205
SRMAAT#  EQU   *-SRMAUGAT         LENGTH OF ATTRIBUTES ENTRY      V205
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=3

```
SRMAUG   DSECT ,
              *,##### PREFIX=S, MACID=RMA #####
*************************************************************** V310
*        V E R S I O N  =  0 0 3                                * V310
*************************************************************** V310
SRMAUGAT DS    OF                  SHOW USERGROUP ATTRIBUTES    V310
**                                                              V310
SRMAGID  DS    CL8                 GROUP IDENTIFICATION         V310
SRMAGUNI EQU   ' '                    UNIVERSAL GROUP           V310
SRMAUPPR DS    CL8                 UPPER GROUP                  V310
** GUNI  EQU   ' '                    UNIVERSAL GROUP           V310
SRMAADM  DS    CL8                 GROUP ADMINISTRATOR          V310
SRMAADNO EQU   ' '                    GROUP WITHOUT GROUP ADMIN V310
SRMAGPF  DS    CL7                 USER GROUP PREFIX            V310
SRMAMPF  DS    CL7                 GROUP MEMBER PREFIX          V310
SRMAANY  EQU   ' '                    NO PREFIX SPECIFIED       V310
SRMARES1 DS    CL2                 RESERVED                     V310
SRMAMGMG DS    H                   MAX GROUP MEMBERS GROUP      V310
SRMAMGMS DS    H                   MAX GROUP MEMBERS SYSTEM     V310
SRMAMSGG DS    H                   MAX SUB GROUPS GROUP         V310
SRMAMSGS DS    H                   MAX SUB GROUPS SYSTEM        V310
SRMAPSLI DS    F                   PUBLIC SPACE LIMIT           V310
SRMAADDR DS    H                   ADDRESS SPACE LIMIT          V310
SRMARPAG DS    H                   RESIDENT PAGES               V310
SRMAACRC DS    H                   MAX ACCOUNT RECORDS          V310
SRMARES2 DS    CL2                 RESERVED                     V310
SRMAFIL  DS    F                   FILE NUMBER LIMIT            V310
SRMAJVL  DS    F                   JV NUMBER LIMIT              V310
SRMATMSL DS    F                   TEMPORARY SPACE LIMIT        V310
SRMAPSE  DS    X                   PUBLIC SPACE EXCESS/ENFORCEMENT V310
SRMAPSEN EQU   1                      NO                        V310
SRMAPSET EQU   2                      TEMPORARILY ALLOWED       V310
SRMAPSEY EQU   3                      YES                       V310
SRMATUN  DS    X                   DMS TUNING RESOURCES         V310
SRMATUNN EQU   1                      NONE                      V310
SRMATUNC EQU   2                      CONCURRENT USE            V310
SRMATUNE EQU   3                      EXCLUSIVE USE             V310
SRMATOP  DS    OX                  TEST OPTIONS:                V310
SRMATRDP DS    X                      READ PRIVILEGE            V310
SRMATWRP DS    X                      WRITE PRIVILEGE           V310
SRMATMOD DS    X                      MODIFICATION BY:          V310
SRMATMCO EQU   1                         CONTROLLED             V310
SRMATMUN EQU   2                         UNCONTROLLED           V310
SRMAATH  DS    X                   ADM AUTHORITY:               V310
SRMAARES EQU   1                      MANAGE RESOURCES          V310
SRMAAMEM EQU   2                      MANAGE MEMBERS            V310
```

```
SRMAAGRP EQU   3                     MANAGE GROUPS                V310
SRMATPIG DS    X                   TPIGNORE (TAPE ACCESS):       V310
SRMATPN  EQU   1                     NO (STD): MSG NOT IGNORED    V310
SRMATPY  EQU   2                     YES: ERROR MSG IGNORED       V310
SRMATPRD EQU   3                     READ: ERROR MSG IGNORED - INPV310
SRMATPBP EQU   4                     BYPASS LABEL                 V310
SRMATPAL EQU   5                     ALL ERROR MSG IGNORED        V310
SRMAIND1 DS    X                   INDICATOR BYTE 1:             V310
SRMAACNL EQU   X'80'                 MAX ACCOUNT RECORDS:        V310
**                                      S: NO LIMIT              V310
**                                      R: VALID                 V310
SRMAAUDT EQU   X'20'                 AUDIT:                      V310
**                                      S: ALLOWED               V310
**                                      R: NOT ALLOWED           V310
SRMACSTM EQU   X'10'                 CSTMP MAKRO:                V310
**                                      S: ALLOWED               V310
**                                      R: NOT ALLOWED           V310
SRMAPHYS EQU   X'08'                 PHYSICAL ALLOCATION:        V310
**                                      S: ALLOWED               V310
**                                      R: NOT ALLOWED           V310
SRMAWRKL DS    F                     WORK SPACE LIMIT            V310
**                                                              V310
SRMAAT#  EQU   *-SRMAUGAT         LENGTH OF ATTRIBUTES ENTRY    V310
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=4

```
SRMAUG   DSECT ,
              *,##### PREFIX=S, MACID=RMA #####
*****************************************************************  V400
*        V E R S I O N  =  0 0 4                                 *  V400
*****************************************************************  V400
SRMAUGAT DS    OF                  SHOW USERGROUP ATTRIBUTES       V400
**                                                                   V400
SRMAGID  DS    CL8                 GROUP IDENTIFICATION            V400
SRMAGUNI EQU   ' '                    UNIVERSAL GROUP              V400
SRMAUPPR DS    CL8                 UPPER GROUP                     V400
** GUNI  EQU   ' '                    UNIVERSAL GROUP              V400
SRMAADM  DS    CL8                 GROUP ADMINISTRATOR             V400
SRMAADNO EQU   ' '                    GROUP WITHOUT GROUP ADMIN    V400
SRMAGPF  DS    CL7                 USER GROUP PREFIX               V400
SRMAMPF  DS    CL7                 GROUP MEMBER PREFIX             V400
SRMAANY  EQU   ' '                    NO PREFIX SPECIFIED          V400
SRMARES1 DS    CL2                 RESERVED                        V400
SRMAMGMG DS    H                   MAX GROUP MEMBERS GROUP         V400
SRMAMGMS DS    H                   MAX GROUP MEMBERS SYSTEM        V400
SRMAMSGG DS    H                   MAX SUB GROUPS GROUP            V400
SRMAMSGS DS    H                   MAX SUB GROUPS SYSTEM           V400
SRMAPSLI DS    F                   PUBLIC SPACE LIMIT              V400
SRMAADDR DS    H                   ADDRESS SPACE LIMIT             V400
SRMARPAG DS    H                   RESIDENT PAGES                  V400
SRMAACRC DS    H                   MAX ACCOUNT RECORDS             V400
SRMARES2 DS    CL2                 RESERVED                        V400
SRMAFIL  DS    F                   FILE NUMBER LIMIT               V400
SRMAJVL  DS    F                   JV NUMBER LIMIT                 V400
SRMATMSL DS    F                   TEMPORARY SPACE LIMIT           V400
SRMAPSE  DS    X                   PUBLIC SPACE EXCESS/ENFORCEMENT V400
SRMAPSEN EQU   1                      NO                           V400
SRMAPSET EQU   2                      TEMPORARILY ALLOWED          V400
SRMAPSEY EQU   3                      YES                          V400
SRMATUN  DS    X                   DMS TUNING RESOURCES            V400
SRMATUNN EQU   1                      NONE                         V400
SRMATUNC EQU   2                      CONCURRENT USE               V400
SRMATUNE EQU   3                      EXCLUSIVE USE                V400
SRMATOP  DS    OX                  TEST OPTIONS:                   V400
SRMATRDP DS    X                      READ PRIVILEGE               V400
SRMATWRP DS    X                      WRITE PRIVILEGE              V400
SRMATMOD DS    X                      MODIFICATION BY:             V400
SRMATMCO EQU   1                         CONTROLLED                V400
SRMATMUN EQU   2                         UNCONTROLLED              V400
SRMAATH  DS    X                   ADM AUTHORITY:                  V400
SRMAARES EQU   1                      MANAGE RESOURCES             V400
SRMAAMEM EQU   2                      MANAGE MEMBERS               V400
```

```
SRMAAGRP EQU   3                     MANAGE GROUPS                V400
SRMATPIG DS    X                   TPIGNORE (TAPE ACCESS):        V400
SRMATPN  EQU   1                     NO (STD): MSG NOT IGNORED    V400
SRMATPY  EQU   2                     YES: ERROR MSG IGNORED       V400
SRMATPRD EQU   3                     READ: ERROR MSG IGNORED - INPV400
SRMATPBP EQU   4                     BYPASS LABEL                 V400
SRMATPAL EQU   5                     ALL ERROR MSG IGNORED        V400
SRMAIND1 DS    X                   INDICATOR BYTE 1:              V400
SRMAACNL EQU   X'80'                 MAX ACCOUNT RECORDS:         V400
**                                      S: NO LIMIT               V400
**                                      R: VALID                  V400
SRMAAUDT EQU   X'20'                 AUDIT:                       V400
**                                      S: ALLOWED                V400
**                                      R: NOT ALLOWED            V400
SRMACSTM EQU   X'10'                 CSTMP MAKRO:                 V400
**                                      S: ALLOWED                V400
**                                      R: NOT ALLOWED            V400
SRMAPHYS EQU   X'08'                 PHYSICAL ALLOCATION:         V400
**                                      S: ALLOWED                V400
**                                      R: NOT ALLOWED            V400
SRMAWRKL DS    F                     WORK SPACE LIMIT             V400
**                                                                V400
SRMABAGN DS    CL18                GUARD_NAME FOR EXTENDED       V400
**                                 BASIC-ACL-ACCESS              V400
SRMABAGO EQU   ' '                 *BY-GROUP-ONLY                V400
SRMARES4 DS    CL2                 RESERVED                      V400
**                                                               V400
SRMAAT#  EQU   *-SRMAUGAT         LENGTH OF ATTRIBUTES ENTRY     V400
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=5

```
SRMSUG5  DSECT ,
               *,##### PREFIX=S, MACID=RMA #####
*****************************************************************V402
*        V E R S I O N  =  0 0 5                                *V402
*****************************************************************V402
SRMAUGAT DS    OF                  SHOW USERGROUP ATTRIBUTES     V402
**                                                               V402
SRMAGID  DS    CL8                 GROUP IDENTIFICATION          V402
SRMAGUNI EQU   ' '                   UNIVERSAL GROUP             V402
SRMAUPPR DS    CL8                 UPPER GROUP                   V402
** GUNI  EQU   ' '                   UNIVERSAL GROUP             V402
SRMAADM  DS    CL8                 GROUP ADMINISTRATOR           V402
SRMAADNO EQU   ' '                   GROUP WITHOUT GROUP ADMIN   V402
SRMAGPF  DS    CL7                 USER GROUP PREFIX             V402
SRMAMPF  DS    CL7                 GROUP MEMBER PREFIX           V402
SRMAANY  EQU   ' '                   NO PREFIX SPECIFIED         V402
```

```
SRMARES1 DS    CL2
SRMAMGMG DS    H
SRMAMGMS DS    H
SRMAMSGG DS    H
SRMAMSGS DS    H
SRMAPSLI DS    F
SRMAADDR DS    H
SRMARPAG DS    H
SRMAACRC DS    H
SRMARES2 DS    CL2
SRMAFIL  DS    F
SRMAJVL  DS    F
SRMATMSL DS    F
SRMAPSE  DS    X
SRMAPSEN EQU   1
SRMAPSET EQU   2
SRMAPSEY EQU   3
SRMATUN  DS    X
SRMATUNN EQU   1
SRMATUNC EQU   2
SRMATUNE EQU   3
SRMATOP  DS    OX
SRMATRDP DS    X
SRMATWRP DS    X
SRMATMOD DS    X
SRMATMCO EQU   1
SRMATMUN EQU   2
SRMAATH  DS    X
SRMAARES EQU   1
SRMAAMEM EQU   2
SRMAAGRP EQU   3
SRMATPIG DS    X
SRMATPN  EQU   1
SRMATPY  EQU   2
SRMATPRD EQU   3
SRMATPBP EQU   4
SRMATPAL EQU   5
SRMAIND1 DS    X
SRMAACNL EQU   X'80'
**
**
SRMAAUDT EQU   X'20'
**
**
SRMACSTM EQU   X'10'
**
**
SRMAPHYS EQU   X'08'
```

```
RESERVED                          V402
MAX GROUP MEMBERS GROUP           V402
MAX GROUP MEMBERS SYSTEM          V402
MAX SUB GROUPS GROUP              V402
MAX SUB GROUPS SYSTEM             V402
PUBLIC SPACE LIMIT                V402
ADDRESS SPACE LIMIT               V402
RESIDENT PAGES                    V402
MAX ACCOUNT RECORDS               V402
RESERVED                          V402
FILE NUMBER LIMIT                 V402
JV NUMBER LIMIT                   V402
TEMPORARY SPACE LIMIT             V402
PUBLIC SPACE EXCESS/ENFORCEMENT V402
   NO                             V402
   TEMPORARILY ALLOWED            V402
   YES                            V402
DMS TUNING RESOURCES              V402
   NONE                           V402
   CONCURRENT USE                 V402
   EXCLUSIVE USE                  V402
TEST OPTIONS:                     V402
   READ PRIVILEGE                 V402
   WRITE PRIVILEGE                V402
   MODIFICATION BY:               V402
      CONTROLLED                  V402
      UNCONTROLLED                V402
ADM AUTHORITY:                    V402
   MANAGE RESOURCES               V402
   MANAGE MEMBERS                 V402
   MANAGE GROUPS                  V402
TPIGNORE (TAPE ACCESS):           V402
   NO (STD): MSG NOT IGNORED      V402
   YES: ERROR MSG IGNORED         V402
   READ: ERROR MSG IGNORED - INPV402
   BYPASS LABEL                   V402
   ALL ERROR MSG IGNORED          V402
INDICATOR BYTE 1:                 V402
   MAX ACCOUNT RECORDS:           V402
      S: NO LIMIT                 V402
      R: VALID                    V402
   AUDIT:                         V402
      S: ALLOWED                  V402
      R: NOT ALLOWED              V402
   CSTMP MAKRO:                   V402
      S: ALLOWED                  V402
      R: NOT ALLOWED              V402
   PHYSICAL ALLOCATION:           V402
```

```
**                                        S: ALLOWED                V402
**                                        R: NOT ALLOWED            V402
SRMAHAUD EQU   X'04'                    HARDWARE AUDIT              V402
**                                        S: ALLOWED                V402
**                                        R: NOT ALLOWED            V402
SRMALAUD EQU   X'02'                    LINKAGE AUDIT               V402
**                                        S: ALLOWED                V402
**                                        R: NOT ALLOWED            V402
SRMAWRKL DS    F                      WORK SPACE LIMIT             V402
**                                                                  V402
SRMABAGN DS    CL18                   GUARD_NAME FOR EXTENDED      V402
**                                    BASIC-ACL-ACCESS             V402
SRMABAGO EQU   ' '                    *BY-GROUP-ONLY               V402
SRMARES4 DS    CL2                    RESERVED                     V402
SRMAADSL DS    F                      ADDRESS SPACE LIMIT          V402
SRMAREPA DS    F                      RESIDENT PAGES               V402
SRMACRSL DS    F                      CRYPTO SESSION LIMIT         V402
**                                                                  V402
SRMAAT#  EQU   *-SRMAUGAT           LENGTH OF ATTRIBUTES ENTRY      V402
         END
               =X'1801272327557865' CONSISTENCY CONSTANT FOR AID
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ATTRIBUT,VERSION=6

```
SRMSUG6  DSECT ,
               *,##### PREFIX=S, MACID=RMA #####
****************************************************************** V403
*        V E R S I O N  =  0 0 6                                 * V403
****************************************************************** V403
SRMAUGAT DS    OF                     SHOW USERGROUP ATTRIBUTES    V403
**                                                                  V403
SRMAGID  DS    CL8                    GROUP IDENTIFICATION         V403
SRMAGUNI EQU   ' '                       UNIVERSAL GROUP           V403
SRMAUPPR DS    CL8                    UPPER GROUP                  V403
** GUNI  EQU   ' '                       UNIVERSAL GROUP           V403
SRMAADM  DS    CL8                    GROUP ADMINISTRATOR          V403
SRMAADNO EQU   ' '                       GROUP WITHOUT GROUP ADMIN V403
SRMAGPF  DS    CL7                    USER GROUP PREFIX            V403
SRMAMPF  DS    CL7                    GROUP MEMBER PREFIX          V403
SRMAANY  EQU   ' '                       NO PREFIX SPECIFIED       V403
SRMARES1 DS    CL2                    RESERVED                     V403
SRMAMGMG DS    H                      MAX GROUP MEMBERS GROUP      V403
SRMAMGMS DS    H                      MAX GROUP MEMBERS SYSTEM     V403
SRMAMSGG DS    H                      MAX SUB GROUPS GROUP         V403
SRMAMSGS DS    H                      MAX SUB GROUPS SYSTEM        V403
SRMAPSLI DS    F                      PUBLIC SPACE LIMIT           V403
SRMAADDR DS    H                      ADDRESS SPACE LIMIT          V403
```

```
SRMARPAG DS    H                RESIDENT PAGES                    V403
SRMAACRC DS    H                MAX ACCOUNT RECORDS               V403
SRMARES2 DS    CL2              RESERVED                          V403
SRMAFIL  DS    F                FILE NUMBER LIMIT                 V403
SRMAJVL  DS    F                JV NUMBER LIMIT                   V403
SRMATMSL DS    F                TEMPORARY SPACE LIMIT             V403
SRMAPSE  DS    X                PUBLIC SPACE EXCESS/ENFORCEMENT V403
SRMAPSEN EQU   1                   NO                             V403
SRMAPSET EQU   2                   TEMPORARILY ALLOWED            V403
SRMAPSEY EQU   3                   YES                            V403
SRMATUN  DS    X                DMS TUNING RESOURCES              V403
SRMATUNN EQU   1                   NONE                           V403
SRMATUNC EQU   2                   CONCURRENT USE                 V403
SRMATUNE EQU   3                   EXCLUSIVE USE                  V403
SRMATOP  DS    OX               TEST OPTIONS:                     V403
SRMATRDP DS    X                   READ PRIVILEGE                 V403
SRMATWRP DS    X                   WRITE PRIVILEGE                V403
SRMATMOD DS    X                   MODIFICATION BY:               V403
SRMATMCO EQU   1                      CONTROLLED                  V403
SRMATMUN EQU   2                      UNCONTROLLED                V403
SRMAATH  DS    X                ADM AUTHORITY:                    V403
SRMAARES EQU   1                   MANAGE RESOURCES               V403
SRMAAMEM EQU   2                   MANAGE MEMBERS                 V403
SRMAAGRP EQU   3                   MANAGE GROUPS                  V403
SRMATPIG DS    X                TPIGNORE (TAPE ACCESS):           V403
SRMATPN  EQU   1                   NO (STD): MSG NOT IGNORED      V403
SRMATPY  EQU   2                   YES: ERROR MSG IGNORED         V403
SRMATPRD EQU   3                   READ: ERROR MSG IGNORED - INPV403
SRMATPBP EQU   4                   BYPASS LABEL                   V403
SRMATPAL EQU   5                   ALL ERROR MSG IGNORED          V403
SRMAIND1 DS    X                INDICATOR BYTE 1:                 V403
SRMAACNL EQU   X'80'                MAX ACCOUNT RECORDS:          V403
**                                     S: NO LIMIT                V403
**                                     R: VALID                   V403
SRMAAUDT EQU   X'20'                AUDIT:                         V403
**                                     S: ALLOWED                 V403
**                                     R: NOT ALLOWED             V403
SRMACSTM EQU   X'10'                CSTMP MAKRO:                   V403
**                                     S: ALLOWED                 V403
**                                     R: NOT ALLOWED             V403
SRMAPHYS EQU   X'08'                PHYSICAL ALLOCATION:           V403
**                                     S: ALLOWED                 V403
**                                     R: NOT ALLOWED             V403
SRMAHAUD EQU   X'04'                HARDWARE AUDIT                 V403
**                                     S: ALLOWED                 V403
**                                     R: NOT ALLOWED             V403
SRMALAUD EQU   X'02'                LINKAGE AUDIT                  V403
**                                     S: ALLOWED                 V403
```

```
**                                        R: NOT ALLOWED           V403
SRMANSTU EQU   X'01'                   NET-STORAGE-USAGE           V403
**                                        S: ALLOWED               V403
**                                        R: NOT ALLOWED           V403
SRMAWRKL DS    F                     WORK SPACE LIMIT             V403
**                                                                 V403
SRMABAGN DS    CL18                  GUARD_NAME FOR EXTENDED      V403
**                                   BASIC-ACL-ACCESS             V403
SRMABAGO EQU   ' '                   *BY-GROUP-ONLY               V403
SRMARES4 DS    CL2                   RESERVED                     V403
SRMAADSL DS    F                     ADDRESS SPACE LIMIT          V403
SRMAREPA DS    F                     RESIDENT PAGES               V403
SRMACRSL DS    F                     CRYPTO SESSION LIMIT         V403
**                                                                 V403
SRMAAT#  EQU   *-SRMAUGAT           LENGTH OF ATTRIBUTES ENTRY     V403
         END
               =X'1801272328427865' CONSISTENCY CONSTANT FOR AID
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=MEMBERS

```
SRMMUG   DSECT ,
               *,##### PREFIX=S, MACID=RMM #####
**
SRMMUGMB DS    OF                    SHOW USERGROUP MEMBERS
**
SRMMUID  DS    CL8                   USERID OF MEMBER
**
SRMMMB#  EQU   *-SRMMUGMB           LENGTH OF ONE MEMBER ENTRY     *V103
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=SUBGROUP

```
SRMRUG   DSECT ,
               *,##### PREFIX=S, MACID=RMM #####

**
SRMGUGSG DS    OF                  SHOW USERGROUP SUBGROUP
**
SRMGGID  DS    CL8                 GROUPID OF SUBGROUP
**
SRMGSG#  EQU   *-SRMGUGSG         LENGTH OF ONE SUBGROUP ENTRY   *V103**
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=ACCNTRES

```
SRMRUG   DSECT ,
               *,##### PREFIX=S, MACID=RMR #####
**
SRMRUGAC DS    OF                  SHOW USERGROUP ACCNTRES
**
SRMRACT  DS    CL8                 ACCOUNT NUMBER
SRMRCPU  DS    F                   CPU TIME LIMIT
SRMRSCLA DS    CL1                 SPOOLOUT-CLASS
SRMRPRI  DS    CL1                 MAXIMUM RUN PRIORITY
SRMRTYPL DS    X                   LIMIT OF TASK TYPE (MAX-ALLOW-C):
SRMRTSTD EQU   1                      STD
SRMRTTP  EQU   2                      TP
SRMRTSYS EQU   3                      SYS
SRMRIND1 DS    X                   INDICATOR BYTE 1:
SRMRNTL  EQU   X'80'                  NTL INFORMATION (NO-CPU-LIMIT):
**                                        S: NTL ALLOWED
**                                        R: NTL NOT ALLOWED
SRMREXP  EQU   X'40'                  EXPRESS INFO (START-IMMEDIATE):
**                                        S: EXPRESS ALLOWED
**                                        R: EXPRESS NOT ALLOWED
SRMRNHD  EQU   X'20'                  INHIBIT DEACTIVATION:
**                                        S: INHIBIT DEACT. ALLOWED
**                                        R: INHIBIT DEACT. NOT ALL.
**
SRMRAC#  EQU   *-SRMRUGAC         LENGTH OF ONE ACC ENTRY        *V103
```

Ausgabebereich SRMSUG MF=D,XPAND=INFO,INFO=PROFILE

```
SRMPHD   DSECT ,
               *,##### PREFIX=S, MACID=RMP #####
**                                                              *V104
SRMPUGPH DS    OF                  SHOW USERGROUP PROFILE_IDS   *V104
**                                 HEADER INFORMATION           *V104
SRMPNPT  DS    H                   NR. OF PROFILE_IDS TRANSFERRED *V104
**                                 INTO CALLERS AREA            *V104
SRMPNPA  DS    H                   NR. OF PROFILE_IDS ACTUALLY  *V104
**                                 ASSOCIATED WITH USER-GROUP   *V104
**                                                              *V104
SRMPPH#  EQU   *-SRMPUGPH         LENGTH OF HEADER INFORMATION  *V104
**
*LABEL   IDLKG ID=UG,SECT=&MF,P=&P,SCD=RMP,VER=&VERSION,ALIGN=F   V205
         MFCHK DNAME=RMPUG,MF=D,PREFIX=S,MACID=RMP,DMACID=RMP,    V311C
               ALIGN=F
SRMPUG   DSECT ,
               *,##### PREFIX=S, MACID=RMP #####
**                                                              *V104
SRMPUGPI DS    OF                  SHOW USERGROUP PROFILE_IDS
**
SRMPPID  DS    CL54                PROFILE_ID
**
SRMPPI#  EQU   *-SRMPUGPI         LENGTH OF ONE PROFILE_ID      *V103
         END
```

Hinweis

Da alle Profile-Ids auf einmal ausgegeben werden, ist ein Ausgabebereich in Vielfachen von SRMPPI# bereitzustellen.

Im Header der Profile-Id-Information wird die Anzahl der Profile-Ids abgelegt, die im Ausgabebereich gespeichert werden konnten. Wurde die Information abgeschnitten, kann die zusätzlich abgelegte Anzahl der für die betreffende Benutzergruppe aktuell gespeicherten Profile-Ids benutzt werden, um einen ausreichend dimensionierten Bereich bereitzustellen.

Beispiel

```
SRMSUG   START
*--------------------------------------------------------------------*
*  PROGRAMM: HANDBUCH-BEISPIEL FUER SRMSUG                           *
*--------------------------------------------------------------------*
SRMSUG   RMODE ANY
SRMSUG   AMODE ANY
         GPARMOD 31
         BALR  3,0
         BCTR  3,0
         BCTR  3,0
         USING SRMSUG,3
*--------------------------------------------------------------------*
*    SETZEN DER PARAMETERLISTE                                       *
*--------------------------------------------------------------------*
         LA    5,SRMAUGAT              * BEGINN DES PARAMETERBEREICHES
         ST    5,SRMSA@
         LA    5,SRMAAT#               * LAENGE DES PARAMETERBEREICHES
         STH   5,SRMSALG
         MVC   SRMSGID,=CL8'SRPMGRP'   * NAME DER BENUTZERGRUPPE
         MVI   SRMSINFO,SRMSIATT       * INFO=ATTRIBUT
*--------------------------------------------------------------------*
*    LESEN DER GRUPPENINFORMATIONEN FUER BENUTZERGRUPPE 'SRPMGRP'    *
*--------------------------------------------------------------------*
         SRMSUG  MF=E,PARAM=SRMPL,VERSION=3
         CLI SRMSMR1,SRMSOK            * AUSWERTEN DES RETURNCODE
         BNE   FEHLER
*                                        VERARBEITUNG DER GRUPPENINFOS
         B     ENDE
FEHLER   EQU   *
*                                        ANDERE VERARBEITUNG
ENDE     TERM
*--------------------------------------------------------------------*
*  AUSGABEBEREICH MAKRO SRMSUG                                       *
*--------------------------------------------------------------------*
         DS    OF
SRMAUS   SRMSUG  MF=C,XPAND=INFO,INFO=ATTRIBUT,VERSION=3
*--------------------------------------------------------------------*
*  PARAMETERBEREICH MAKRO SRMSUG                                     *
*--------------------------------------------------------------------*
         DS    OF
SRMPL    SRMSUG  MF=C,XPAND=PARAM,VERSION=3
         ORG   SRMSUGPL
         SRMSUG  MF=L,AREA@=0,AREALG=0,VERSION=3
         END SRMSUG
```

3.6 Beispiele zur Benutzerverwaltung

Für die Verwaltung von Benutzerkennungen und Benutzergruppen sind die nachfolgend beschriebenen Regeln zu beachten. Wichtig ist insbesondere, dass für gleiche Verwaltungsmaßnahmen teilweise unterschiedliche Regeln gelten, abhängig davon, ob die jeweilige Maßnahme von einem Gruppenverwalter oder von einem systemglobalen Benutzerverwalter durchgeführt wird.

Zur Erläuterung der Regeln sind Beispiele für die wichtigsten Verwaltungsmaßnahmen angefügt. In den einzelnen Beispielen werden jeweils nur die Attribute beschrieben, die für die gerade betrachtete Verwaltungsmaßnahme relevant sind.

In den folgenden Beispielen soll eine Benutzergruppenstruktur für ein Software-Haus aufgebaut und bei sich ändernden Ansprüchen geändert werden. Es gilt folgende Ausgangssituation:

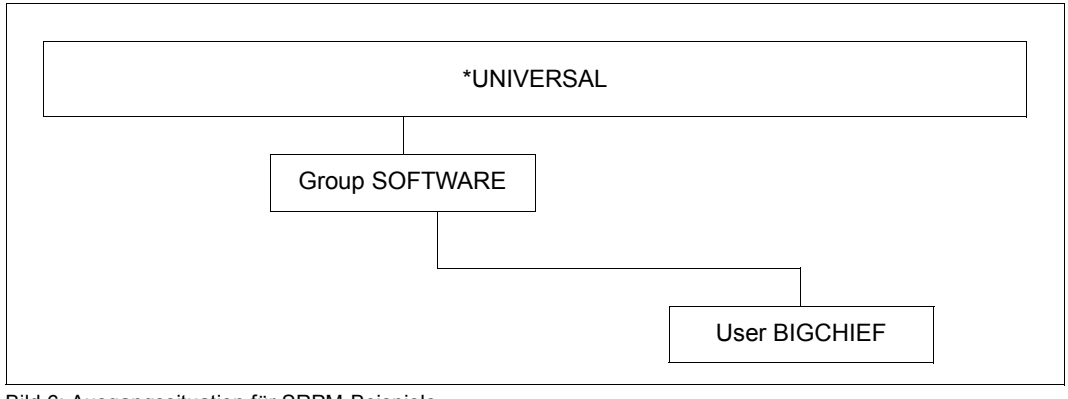


Bild 6: Ausgangssituation für SRPM-Beispiele

Diese Ausgangssituation wurde wie folgt erstellt:

Erzeugen der Gruppenverwalterkennung BIGCHIEF

```
/add-user user-identification=bigchief,public-space-excess=*allowed, -
/    profile-id=pro1,pubset=x,default-pubset=x, -
/    account-attributes=*parameters(account=acc1)
```

Erzeugen der Gruppe SOFTWARE

```
/add-user-group group-identification=software,pubset=x, -
/    group-administrator=bigchief,add-group-member=bigchief, -
/    adm-authority=*manage-groups,max-group-members=100,max-sub-groups=100, -
/    public-space-excess=*allowed,add-profile-id=(pro1,pro2), -
/    add-account=(acc1,acc2)
```

3.6.1 Beispiel 1: Gruppenpotential verwalten

Die hier aufgeführten Beispiele gelten für Kennungen mit dem Gruppenverwalterrecht, nicht jedoch den systemglobalen Benutzerverwalter.

Regeln für die Verwaltung des Gruppenpotentials, das nicht der Verrechnung unterliegt

– Das Gruppenpotential einer bestehenden oder neu einzurichtenden Benutzergruppe muss stets kleiner oder gleich dem Gruppenpotential der ihr übergeordneten Benutzergruppe sein. Gruppenpotentiale können unter Beachtung dieser Regel von einem Gruppenverwalter stets modifiziert werden, auch wenn sie zuvor von einem systemglobalen Benutzerverwalter festgelegt wurden.

– Die im Gruppenpotential einer Benutzergruppe festgelegten Werte gelten als Obergrenze für die Benutzergruppe und die ihr untergeordnete Gruppenstruktur. Die Festlegung des Gruppenpotentials einer Benutzergruppe wird deshalb abgelehnt, wenn ein eingegebener Wert die jeweils gültige Obergrenze überschreitet. In diesem Fall wird eine Meldung ausgegeben, die den Gruppenverwalter über diejenige Benutzergruppe und ihr Gruppenpotential informiert, die die Ursache für die Ablehnung war.

– Ein für eine Benutzergruppe festgelegtes Gruppenpotential kann von ihrem Gruppenverwalter an die Mitglieder der Benutzergruppe vergeben und/oder an die ihr untergeordnete Gruppenstruktur weitergegeben werden.

– Profile-Ids oder Abrechnungsnummern können nur an Gruppenmitglieder oder Untergruppen vergeben werden, wenn sie im Gruppenpotential der Benutzergruppe enthalten sind.

– Wenn ein systemglobaler Benutzerverwalter bei einer Benutzergruppe Profile-Ids oder Abrechnungsnummern anfügt oder verändert, die nicht oder nicht in vollem Umfang im Gruppenpotential der übergeordneten Benutzergruppe enthalten sind, kann ein Gruppenverwalter diese nur aus dem Gruppenpotential löschen oder entsprechend dem Gruppenpotential der übergeordneten Benutzergruppe verändern. Das Löschen kann nur rückgängig gemacht werden, wenn das Gruppenpotential der übergeordneten Benutzergruppe dies zulässt.

– Die zugeteilten allgemeinen Benutzerrechte bzw. das Gruppenpotential bleiben beim Umhängen einer Benutzerkennung oder -gruppe durch einen Gruppenverwalter erhalten, wenn sie kleiner oder gleich dem Gruppenpotential der Benutzergruppe sind, in die umgehängt wurde. Andernfalls sind die Gruppenpotentiale vorher anzupassen. Das gilt auch für allgemeine Benutzerrechte von Benutzerkennungen und Gruppenpotentiale von Benutzergruppen, die vor dem Umhängen von einem systemglobalen Benutzerverwalter festgelegt wurden.

– Beim Umhängen einer Benutzerkennung oder Benutzergruppe in eine andere Benutzergruppe durch einen systemglobalen Benutzerverwalter bleiben die zugeteilten allgemeinen Benutzerrechte bzw. das Gruppenpotential stets erhalten.

Verwaltung des Gruppenpotentials, das nicht der Verrechnung unterliegt

Die Kennung BIGCHIEF ist Gruppenverwalter der Gruppe SOFTWARE. Unterhalb der Gruppe SOFTWARE wird die Gruppe SYSTEMSW eingerichtet.

Zu den Aufgaben der Erstellung von Systemsoftware gehört die Erstellung von Handbüchern (Gruppe MANUALS) sowie deren Übersetzung (Gruppe TRANSLAT), eine Tätigkeit, die von den Mitgliedern der Gruppe MANUALS gesteuert wird. Das Potential der Gruppe TRANSLAT muss dem schwankenden Übersetzungsaufkommen, z.B. bei der Herausgabe einer neuen Betriebssystemversion angepasst werden. Zu den Aufgaben gehört auch, dass Kennungen für Benutzer (in diesem Fall die Kennung EVAPRINT) eingerichtet werden.

Gruppenverwalter BIGCHIEF richtet Benutzergruppe SYSTEMSW ein

```
/add-user-group group-identification=systemsw,pubset=x, -
/    adm-authority=*manage-groups,max-group-members=50,max-sub-groups=50, -
/    public-space-excess=*allowed,add-profile-id=(pro1,pro2), -
/    max-account-records=100,add-account=(acc1,acc2)
```

```
/show-user-group group-identification=systemsw,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 10:34:18
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY                50    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY                50    FREE  USER-ADM                     0

TEST-OPTIONS...
MODIFICATION               *CONTROLLED
READ-PRIVILEGE                       1    WRITE-PRIVILEGE                    1

PUBLIC-SPACE-EXCESS           *ALLOWED    PUBLIC-SPACE-LIMIT       2.147.483.647
RESIDENT-PAGES                  32.767    ADDRESS-SPACE-LIMIT                16
FILE-AUDIT                         *NO    CSTMP-MACRO                       *NO
MAX-ACCOUNT-RECORDS                100    TAPE-ACCESS                      *STD
TEMP-SPACE-LIMIT         2.147.483.647    DMS-TUNING-RESOURCES             *NONE
FILE-NUMBER-LIMIT           16.777.215    JV-NUMBER-LIMIT             16.777.215
WORK-SPACE-LIMIT         2.147.483.647    PHYSICAL-ALLOCATION       *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED    CRYPTO-SESSION-LIMIT              128
LINKAGE-AUDIT                 *ALLOWED    NET-STORAGE-USAGE             *ALLOWED

BASIC-ACL-ACCESS         *BY-GROUP-ONLY

PROFILE-IDS               PRO1
                          PRO2

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

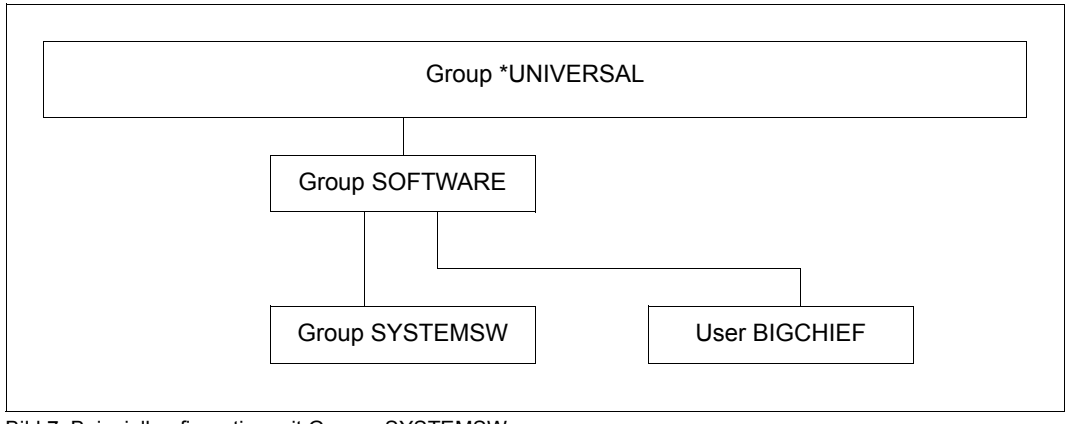


Bild 7: Beispielkonfiguration mit Gruppe SYSTEMSW

Gruppenverwalter BIGCHIEF richtet als Untergruppe zu SYSTEMSW die Gruppe MANUALS ein

```
/add-user-group group-identification=manuals,pubset=x, -
/   upper-group=systemsw,adm-authority=*manage-members,max-group-members=5, -
/   max-sub-groups=5,add-profile-id=(pro1,pro2),max-account-records=100, -
/   add-account=(acc1,acc2)
```

```
/show-user-group group-identification=manuals,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 10:54:04
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                5    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                5    FREE  USER-ADM                      0

TEST-OPTIONS...
MODIFICATION              *CONTROLLED
READ-PRIVILEGE                       1    WRITE-PRIVILEGE                     1

PUBLIC-SPACE-EXCESS                *NO    PUBLIC-SPACE-LIMIT      2.147.483.647
RESIDENT-PAGES                 32.767     ADDRESS-SPACE-LIMIT                16
FILE-AUDIT                         *NO    CSTMP-MACRO                      *NO
MAX-ACCOUNT-RECORDS                100    TAPE-ACCESS                     *STD
TEMP-SPACE-LIMIT         2.147.483.647    DMS-TUNING-RESOURCES           *NONE
FILE-NUMBER-LIMIT           16.777.215    JV-NUMBER-LIMIT           16.777.215
WORK-SPACE-LIMIT         2.147.483.647    PHYSICAL-ALLOCATION      *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED    CRYPTO-SESSION-LIMIT             128
LINKAGE-AUDIT                 *ALLOWED    NET-STORAGE-USAGE             *ALLOWED

BASIC-ACL-ACCESS   *BY-GROUP-ONLY

PROFILE-IDS              PRO1
                         PRO2

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

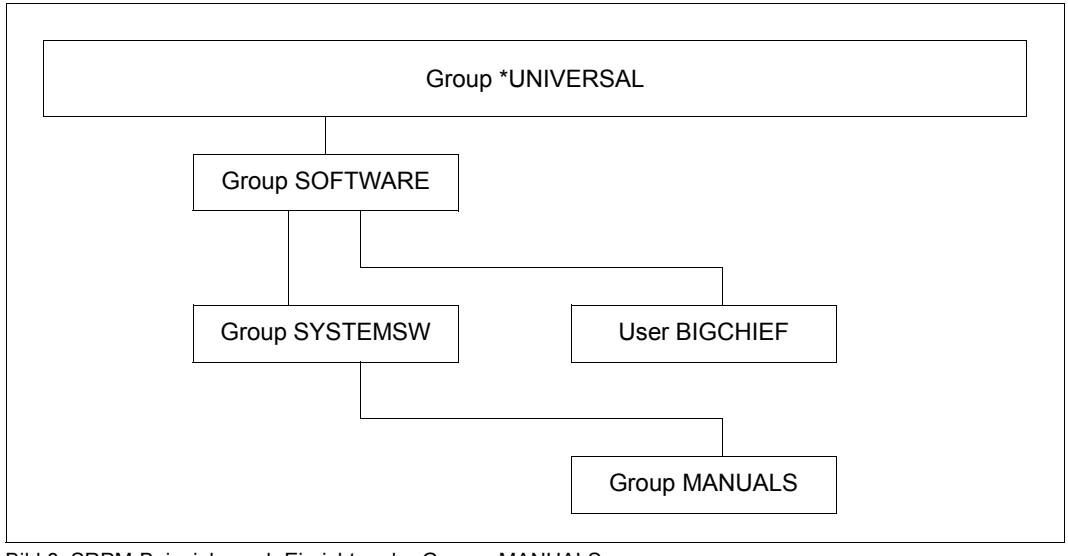


Bild 8: SRPM-Beispiele nach Einrichten der Gruppe MANUALS

Gruppenverwalter BIGCHIEF richtet die Gruppe TRANSLAT als Untergruppe zu MANUALS ein

```
/add-user-group group-identification=translat,pubset=x,
/    upper-group=manuals,adm-authority=*manage-members, -
/    add-profile-id=(pro1,pro2),add-account=(acc1,acc2)
```

```
/show-user-group group-identification=translat,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 10:56:57
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          TRANSLAT    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-MEMBERS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                    MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                       0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                       0

TEST-OPTIONS...
MODIFICATION               *CONTROLLED
READ-PRIVILEGE                        1    WRITE-PRIVILEGE                      1

PUBLIC-SPACE-EXCESS                 *NO    PUBLIC-SPACE-LIMIT       2.147.483.647
RESIDENT-PAGES                    32.767   ADDRESS-SPACE-LIMIT                 16
FILE-AUDIT                          *NO    CSTMP-MACRO                        *NO
MAX-ACCOUNT-RECORDS                100     TAPE-ACCESS                      *STD
TEMP-SPACE-LIMIT          2.147.483.647    DMS-TUNING-RESOURCES              *NONE
FILE-NUMBER-LIMIT            16.777.215    JV-NUMBER-LIMIT             16.777.215
WORK-SPACE-LIMIT          2.147.483.647    PHYSICAL-ALLOCATION       *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED     CRYPTO-SESSION-LIMIT                128
LINKAGE-AUDIT                 *ALLOWED     NET-STORAGE-USAGE             *ALLOWED

BASIC-ACL-ACCESS   *BY-GROUP-ONLY

PROFILE-IDS                PRO1
                           PRO2

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT    !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !               ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

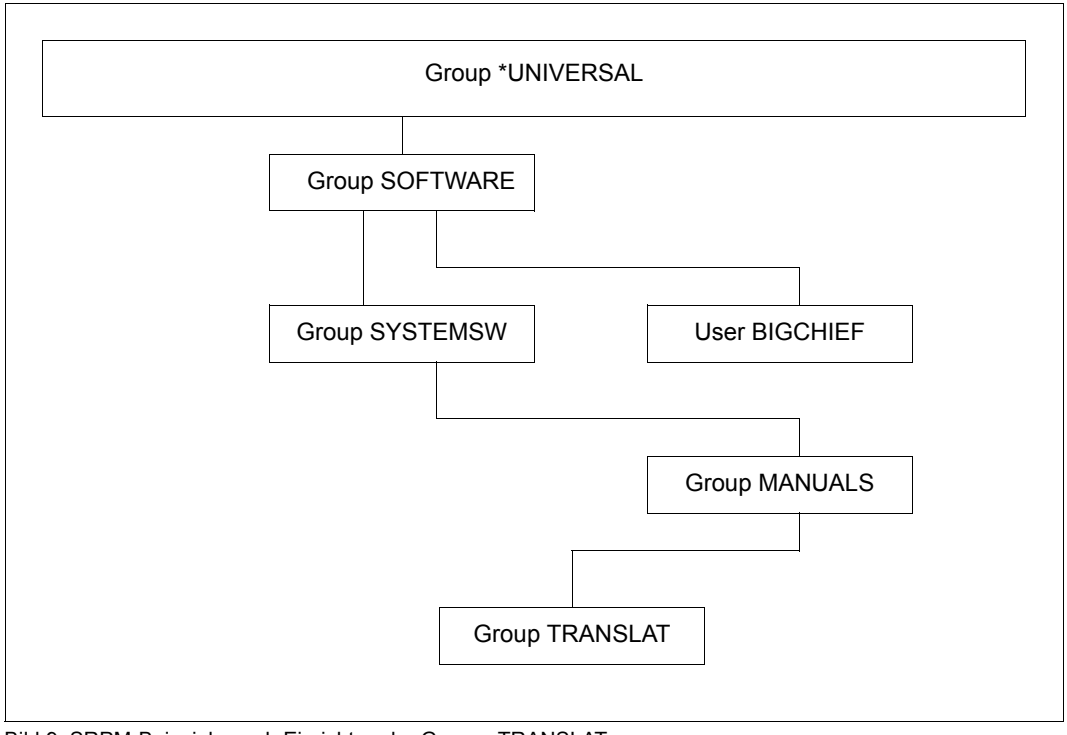


Bild 9: SRPM-Beispiele nach Einrichten der Gruppe TRANSLAT

Der systemglobale Benutzerverwalter ändert das Potential der Gruppe TRANSLAT

```
/modify-user-group group-identification=translat,pubset=x, -
/       public-space-excess=*allowed,file-audit=*yes,address-space-limit=32, -
/       add-profile-id=pro3,max-account-records=200,add-account=acc3
```

```
/show-user-group group-identification=translat,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:01:04
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          TRANSLAT    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-MEMBERS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                    MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                      0

TEST-OPTIONS...
MODIFICATION               *CONTROLLED
READ-PRIVILEGE                        1    WRITE-PRIVILEGE                     1

PUBLIC-SPACE-EXCESS           *ALLOWED    PUBLIC-SPACE-LIMIT       2.147.483.647
RESIDENT-PAGES                  32.767    ADDRESS-SPACE-LIMIT                 32
FILE-AUDIT                        *YES    CSTMP-MACRO                       *NO
MAX-ACCOUNT-RECORDS               200     TAPE-ACCESS                       *STD
TEMP-SPACE-LIMIT        2.147.483.647     DMS-TUNING-RESOURCES             *NONE
FILE-NUMBER-LIMIT          16.777.215     JV-NUMBER-LIMIT             16.777.215
WORK-SPACE-LIMIT        2.147.483.647     PHYSICAL-ALLOCATION       *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED    CRYPTO-SESSION-LIMIT                128
LINKAGE-AUDIT                 *ALLOWED    NET-STORAGE-USAGE             *ALLOWED

BASIC-ACL-ACCESS   *BY-GROUP-ONLY

PROFILE-IDS             PRO1
                        PRO2
                        PRO3

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC3    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Gruppenverwalter BIGCHIEF reduziert Potential von Benutzergruppe TRANSLAT

```
/modify-user-group group-identification=translat, pubset=x, -
/    adm-authority=*manage-resources,file-audit=*no,address-space-limit=16, -
/    remove-profile-id=pro3,max-account-records=100,remove-account=acc3
```

```
/show-user-group group-identification=translat,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:03:45
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          TRANSLAT    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                    MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                 0    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                 0    FREE  USER-ADM                      0

TEST-OPTIONS...
MODIFICATION               *CONTROLLED
READ-PRIVILEGE                        1    WRITE-PRIVILEGE                     1

PUBLIC-SPACE-EXCESS           *ALLOWED    PUBLIC-SPACE-LIMIT      2.147.483.647
RESIDENT-PAGES                  32.767    ADDRESS-SPACE-LIMIT                16
FILE-AUDIT                         *NO    CSTMP-MACRO                      *NO
MAX-ACCOUNT-RECORDS                100    TAPE-ACCESS                      *STD
TEMP-SPACE-LIMIT        2.147.483.647    DMS-TUNING-RESOURCES            *NONE
FILE-NUMBER-LIMIT          16.777.215    JV-NUMBER-LIMIT            16.777.215
WORK-SPACE-LIMIT        2.147.483.647    PHYSICAL-ALLOCATION      *NOT-ALLOWED
HARDWARE-AUDIT                *ALLOWED    CRYPTO-SESSION-LIMIT              128
LINKAGE-AUDIT                 *ALLOWED    NET-STORAGE-USAGE             *ALLOWED

BASIC-ACL-ACCESS   *BY-GROUP-ONLY

PROFILE-IDS             PRO1
                        PRO2

+--------+--------------+--------+--------+------------+-------+------+------+
!ACCNT-NB!  CPU-LIMIT   !SPOOLOUT!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!        !              ! CLASS  !PRIORITY!  CATEGORY  ! LIMIT !IMMED !DEACT !
+--------+--------------+--------+--------+------------+-------+------+------+
!ACC1    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
!ACC2    ! 2.147.483.647!    0   !  255   !  *STD      !  *NO  ! *NO  ! *NO  !
+--------+--------------+--------+--------+------------+-------+------+------+

NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Gruppenverwalter BIGCHIEF richtet Benutzerkennung EVAPRINT in der Gruppe MANUALS ein

```
/add-user user-identification=evaprint,group-identification=manuals, -
/    max-account-records=50,profile-id=pro1,pubset=x, -
/    default-pubset=x,account-attributes=*parameters(account=acc1)
```

```
/show-user-attributes user-identification=evaprint,pubset=x
```

```
SHOW-USER-ATTRIBUTES --- PVS X    - USER EVAPRINT          2018-03-05 11:06:17
------------------------------------------------------------------------------
USER-ID                      EVAPRINT          PUBLIC-SPACE-USED               0
GROUP-ID                      MANUALS          PUBLIC-SPACE-LIMIT       16777215
DEFAULT-PUBSET                      X          PUBLIC-SPACE-EXCESS           *NO
MAX-ACCOUNT-RECORDS                50          TEMP-SPACE-USED                 0
DEFAULT-MSG-LANGUAGE                           TEMP-SPACE-LIMIT       2147483647
                                               FILES                           0
PROTECTION-ATTRIBUTES...                       FILE-NUMBER-LIMIT        16777215
LOGON-PASSWORD                  *NO            JOB-VARIABLES                   0
PASSWORD-MGMT                *BY-USER          JV-NUMBER-LIMIT          16777215
TAPE-ACCESS                     *STD           RESIDENT-PAGES              32767
FILE-AUDIT                       *NO           ADDRESS-SPACE-LIMIT            16
                                               DMS-TUNING-RESOURCES        *NONE
TEST-OPTIONS...                                CSTMP-MACRO-ALLOWED            *NO
READ-PRIVILEGE                     1           CODED-CHARACTER-SET        EDF03IRV
WRITE-PRIVILEGE                    1           PHYSICAL-ALLOCATION            *NO
MODIFICATION            *CONTROLLED            USER-LOCKED                    *NO
                                               CRYPTO-SESSION-USED             0
AUDIT...                                       CRYPTO-SESSION-LIMIT          128
HARDWARE-AUDIT              *ALLOWED           NET-STORAGE-USAGE         *ALLOWED
LINKAGE-AUDIT               *ALLOWED           NET-CODED-CHAR-SET        *ISO

PROFILE-ID  PRO1
MAIL-ADDRESS  *NONE

+---------+-----------+---------+--------+------------+-------+------+------+
!ACCOUNT-#! CPU-LIMIT !SPOOLOUT-!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
!         !           !  CLASS  !PRIORITY!  CATEGORY  ! LIMIT ! IMMED! DEACT!
+---------+-----------+---------+--------+------------+-------+------+------+
! ACC1    !      65535!     0   !   255  !     STD    !   NO  !   NO !   NO !
+---------+-----------+---------+--------+------------+-------+------+------+
DEFAULT-ACCOUNT-# FOR LOGON:        *NONE
DEFAULT-ACCOUNT-# FOR REMOTE-LOGIN: *NONE

DEFAULT-JOB-CLASS FOR BATCH-JOBS:  JC1B
DEFAULT-JOB-CLASS FOR DIALOG-JOBS: JC1D
LIST OF JOB-CLASSES ALLOWED:
JC1B     JC1D
------------------------------------------------------------------------------
SHOW-USER-ATTRIBUTES              END OF DISPLAY FOR USER USER007  ON PUBSET X
```

```
/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:06:51
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              5    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              4    FREE  USER-ADM                       0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              5    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              4    FREE  USER-ADM                       0
.
.
.
SUB-GROUPS                   TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Hinweis

Will der Gruppenverwalter der Benutzergruppe SOFTWARE (Benutzerkennung BIGCHIEF) im Gruppenpotential der Benutzergruppe SYSTEMSW den Wert für PUBLIC-SPACE-EXCESS von *ALLOWED auf *NO ändern, so muss er vorher im Gruppenpotential der untergeordneten Benutzergruppe TRANSLAT den entsprechenden Wert auf *NO setzen. Andernfalls wird die Änderung abgelehnt.

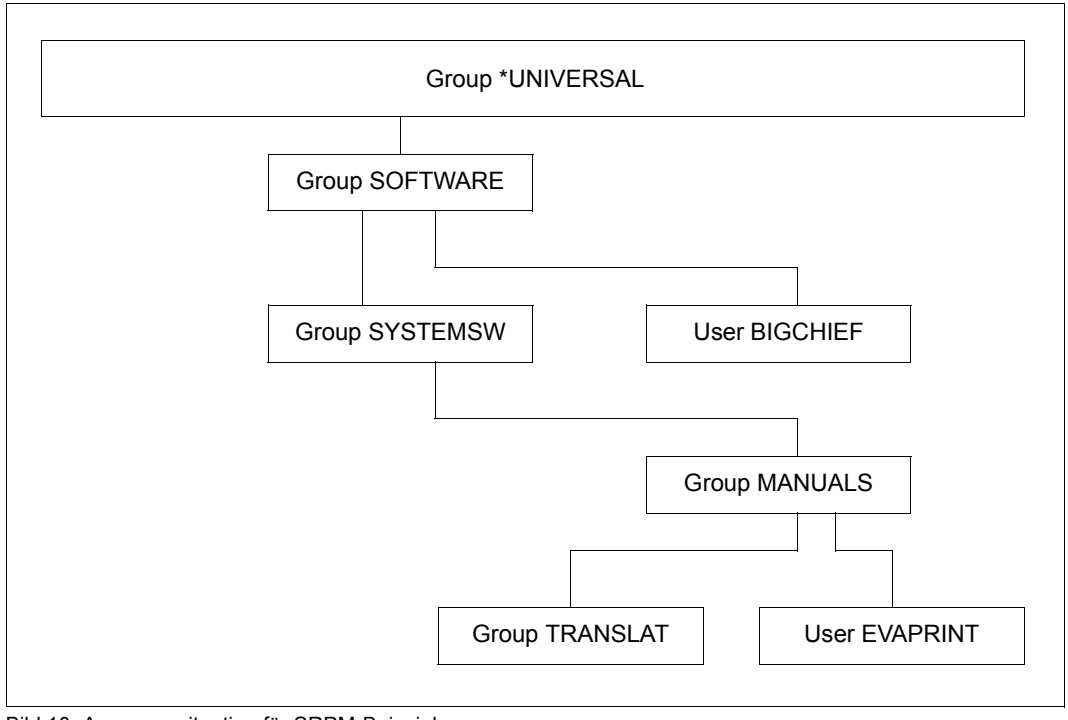


Bild 10: Ausgangssituation für SRPM-Beispiele

Regeln für die Verwaltung des Gruppenverwalterrechts

– Das Gruppenverwalterrecht ist dem Gruppenpotential einer Benutzergruppe zugeordnet. Für die Verwaltung des Gruppenverwalterrechts gelten die gleichen Regeln, wie für die Verwaltung des Gruppenpotentials, das nicht der Verrechnung unterliegt.

– Ein Gruppenverwalter kann entsprechend der für seine Benutzergruppe festgelegten Ausprägung des Gruppenverwalterrechts in der seiner Benutzergruppe untergeordneten Gruppenstruktur Gruppenverwalter ernennen, absetzen oder ändern.

– Ein Gruppenverwalter kann sich nicht selbst absetzen oder ein anderes Mitglied seiner Benutzergruppe zum Gruppenverwalter ernennen.

– Ein Gruppenverwalter kann für sich selbst (seine eigene Benutzerkennung) Betriebsmittel und Benutzerrechte entsprechend dem Gruppenpotential seiner Benutzergruppe festlegen.

Regeln für die Verwaltung des Gruppenpotentials, das der Verrechnung unterliegt

Die Potentialtypen MAX-SUB-GROUPS und MAX-GROUP-MEMBERS des Gruppenpotentials einer Benutzergruppe unterliegen der Verrechnung.

Verrechnung bedeutet

– einerseits, dass die mit den Kommandos /ADD- oder /MODIFY-USER-GROUP bzw. /ADD- oder /MODIFY-USER angegebenen Betriebsmittel einer Quelle entnommen werden. Die für die beiden Potentialtypen angegebenen Werte legen maximal verfügbare Kontingente fest, d.h. in höchstens welchem Umfang die Betriebsmittel einem Gruppenverwalter zur Verfügung stehen.

– andererseits, dass die Betriebsmittel belegt und wieder freigegeben werden können. Über Belegung und Freigabe wird Buch geführt.

Bei der Verrechnung ist die gegenseitige Beeinflussung von Gruppenverwalter und systemglobalem Benutzerverwalter zu berücksichtigen:

– Ein Gruppenverwalter unterliegt den festgelegten Werten eines maximal vorhandenen bzw. jeweils noch frei verfügbaren Gruppenpotentials.

– Ein systemglobaler Benutzerverwalter unterliegt keinen Beschränkungen bzgl. eines Gruppenpotentials.

– Infolgedessen gibt es eine zweifache Buchführung, abhängig davon, ob eine Verwaltungsmaßnahme von einem Gruppenverwalter oder von einem systemglobalen Benutzerverwalter durchgeführt wird.

Für die Verrechnung des Gruppenpotentials gilt folgendes Prinzip:

– Das durch einen Gruppenverwalter zugeteilte Gruppenpotential soll stets zuerst verbraucht werden.

– Das durch einen systemglobalen Benutzerverwalter zugeteilte Gruppenpotential soll solange wie möglich unangetastet bleiben bzw. so schnell wie möglich wieder frei verfügbar werden.

Hinweise zu den Potentialtypen MAX-GROUP-MEMBERS und MAX-SUB-GROUPS

– Soweit nichts anderes gesagt wird, beziehen sich im folgenden die Aussagen bzgl. der Potential-Werte
  – LIMIT-GROUP-HIERARCHY
  – FREE-GROUP-HIERARCHY
  – LIMIT-USER-ADM
  – FREE-USER-ADM

  jeweils auf die beiden Potentialtypen MAX-GROUP-MEMBERS und MAX-SUB-GROUPS.

- Der Wert von LIMIT-GROUP-HIERARCHY dokumentiert jeweils das für eine Benutzergruppe festgelegte Gruppenpotential. Ein Gruppenverwalter kann mit den Kommandos /ADD- bzw. /MODIFY-USER-GROUP nur den Wert für LIMIT-GROUP-HIERARCHY verwalten.
- Der Wert von LIMIT-USER-ADM dokumentiert jeweils das einer Benutzergruppe durch einen systemglobalen Benutzerverwalter zusätzlich zur Verfügung gestellte Gruppenpotential. Dieser Wert wird bei der systemglobalen Benutzerverwaltung mit den Kommandos /ADD- bzw. /MODIFY-USER-GROUP verwaltet.
- Das Gruppenpotential, über das ein Gruppenverwalter insgesamt verfügen kann, wird jeweils bezeichnet durch die Summe der Werte von LIMIT-GROUP-HIERARCHY und LIMIT-USER-ADM.
- Das gesamte aktuell frei verfügbare Gruppenpotential wird jeweils bezeichnet durch die Summe der Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM. Die Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM sind stets kleiner oder gleich den Werten von LIMIT-GROUP-HIERARCHY bzw. LIMIT-USER-ADM. Gleichheit besteht, wenn in Benutzerkennungen oder Untergruppen kein entsprechendes Potential gebunden ist, z.B. wenn die Benutzergruppe leer ist.
  - Ein Gruppenverwalter kann beim Einrichten und Verwalten von Benutzerkennungen und Benutzergruppen jeweils höchstens über das Gruppenpotential in der Höhe der Summe aus diesen beiden Werten verfügen. Er kann keine Verwaltungsmaßnahme durchführen, deren Potentialverbrauch diese Summe überschreiten würde.
  - Ein systemglobaler Benutzerverwalter kann Verwaltungsmaßnahmen durchführen, die bei nichtnegativen Werten von FREE-USER-ADM die Summe von FREE-GROUP-HIERARCHY und FREE-USER-ADM übersteigt. In diesem Fall entsteht eine „Systemschuld“, die als negativer Wert in FREE-USER-ADM hinterlegt wird. Bei vollständig ausgeschöpftem freien Gruppenpotential (FREE-USER-ADM=0, FREE-GROUP-HIERARCHY=0) oder negativen Werten von FREE-USER-ADM kann er Verwaltungsmaßnahmen durchführen, die zu einer weiteren Erhöhung dieser Systemschuld führen. Eine derartige Systemschuld kann nur durch einen systemglobalen Benutzerverwalter entstehen.
- Der Wert von FREE-GROUP-HIERARCHY ist nie negativ.
- Bei der Verwaltung einer Benutzergruppe wird stets zuerst das verfügbare Gruppenpotential FREE-GROUP-HIERARCHY verbraucht, bis es den Wert 0 erreicht hat. Dann erfolgt die Entnahme aus FREE-USER-ADM.
- Werden in einer bestehenden Benutzergruppe durch Einrichten oder Umhängen neue Untergruppen oder Benutzerkennungen erzeugt und ihnen ein Gruppenpotential zugeteilt, so verkleinern sich die Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM der Benutzergruppe entsprechend dem verbrauchten Gruppenpotential.

– Werden Benutzergruppen oder Benutzerkennungen durch Löschen oder Umhängen entfernt oder ein ihnen zugeteiltes Gruppenpotential verkleinert, so wird das bisher von ihnen belegte Gruppenpotential frei und erzeugt einen Potentialrückfluss.

– Bei einem Potentialrückfluss an eine Benutzergruppe oder beim Vergrößern des ihr zugeteilten Gruppenpotentials wird grundsätzlich zuerst FREE-USER-ADM aufgefüllt, bis der Wert von LIMIT-USER-ADM erreicht wird. Danach wird FREE-GROUP-HIERARCHY aufgefüllt.

3.6.2 Beispiel 2: Einrichten neuer Benutzergruppen

Es werden weitere Benutzergruppen benötigt. Die Benutzergruppen werden teilweise vom Gruppenverwalter und teilweise vom systemglobalen Benutzerverwalter eingetragen.

Einrichten einer Benutzergruppe durch einen Gruppenverwalter

Beim Einrichten einer neuen Benutzergruppe durch einen Gruppenverwalter wird das dieser Benutzergruppe zugeteilte Gruppenpotential stets der übergeordneten Benutzergruppe entnommen.

Eingerichtete Benutzergruppe

LIMIT-GROUP-HIERARCHY und FREE-GROUP-HIERARCHY der neuen Benutzergruppe erhalten jeweils die im Kommando /ADD-USER-GROUP angegebenen Werte.

LIMIT-USER-ADM und FREE-USER-ADM der neuen Benutzergruppe erhalten jeweils den Wert 0.

Übergeordnete Benutzergruppe

Die Summe der Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM der übergeordneten Benutzergruppe wird jeweils um die angegebenen Werte verkleinert.

– Zunächst wird FREE-GROUP-HIERARCHY verkleinert, bis minimal der Wert 0 erreicht ist.

– Verbleibt noch ein Rest, wird anschließend FREE-USER-ADM um diesen Wert verkleinert.

– Für FREE-GROUP-HIERARCHY des Potentialtyps MAX-SUB-GROUPS wird zusätzlich der Wert -1 berechnet.

Das Einrichten einer neuen Benutzergruppe wird abgelehnt, wenn sich bei der Verrechnung des Gruppenpotentials in der übergeordneten Benutzergruppe ein negativer Wert ergibt, d.h. dort kein freies Gruppenpotential mehr vorhanden ist.

Einrichten einer Benutzergruppe durch einen systemglobalen Benutzerverwalter

Beim Einrichten einer neuen Benutzergruppe durch einen systemglobalen Benutzerverwalter wird das dieser Benutzergruppe zugeteilte Gruppenpotential nicht dem Gruppenpotential der übergeordneten Benutzergruppe entnommen, sondern ihr gewissermaßen als „Sonderkontingent“ zugewiesen.

Ein aus dieser Verwaltungsmaßnahme resultierendes freies Gruppenpotential kann an die Gruppenmitglieder der neu eingerichteten Benutzergruppe und die ihr untergeordnete Benutzergruppenstruktur weitergegeben werden, jedoch nicht an die ihr übergeordnete Benutzergruppe zurückfließen.

Eingerichtete Benutzergruppe

LIMIT-USER-ADM und FREE-USER-ADM der neuen Benutzergruppe erhalten die im Kommando ADD-USER-GROUP angegebenen Werte.

LIMIT-GROUP-HIERARCHY und FREE-GROUP-HIERARCHY der neuen Benutzergruppe erhalten jeweils den Wert 0.

Übergeordnete Benutzergruppe

FREE-GROUP-HIERARCHY des Potentialtyps MAX-SUB-GROUPS der übergeordneten Benutzergruppe wird um den Wert 1 verkleinert. Besitzt FREE-GROUP-HIERARCHY bereits den Wert 0, wird FREE-USER-ADM um den Wert 1 verkleinert.

Teil 1: Gruppenverwalter BIGCHIEF richtet Benutzergruppe DEVELOPS als Untergruppe zu SYSTEMSW ein

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:09:29
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              44     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              45     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/add-user-group group-identification=develops,pubset=x, -
/    upper-group=systemsw,adm-authority=*manage-members, -
/    max-group-members=10,max-sub-groups=10
```

```
/show-user-group group-identification=systemsw,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:11:31
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              33    FREE  USER-ADM                       0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                       0
.
.
.
SUB-GROUPS                   DEVELOPS  MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

```
/show-user-group group-identification=develops,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:11:58
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                       0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                       0
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                       0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

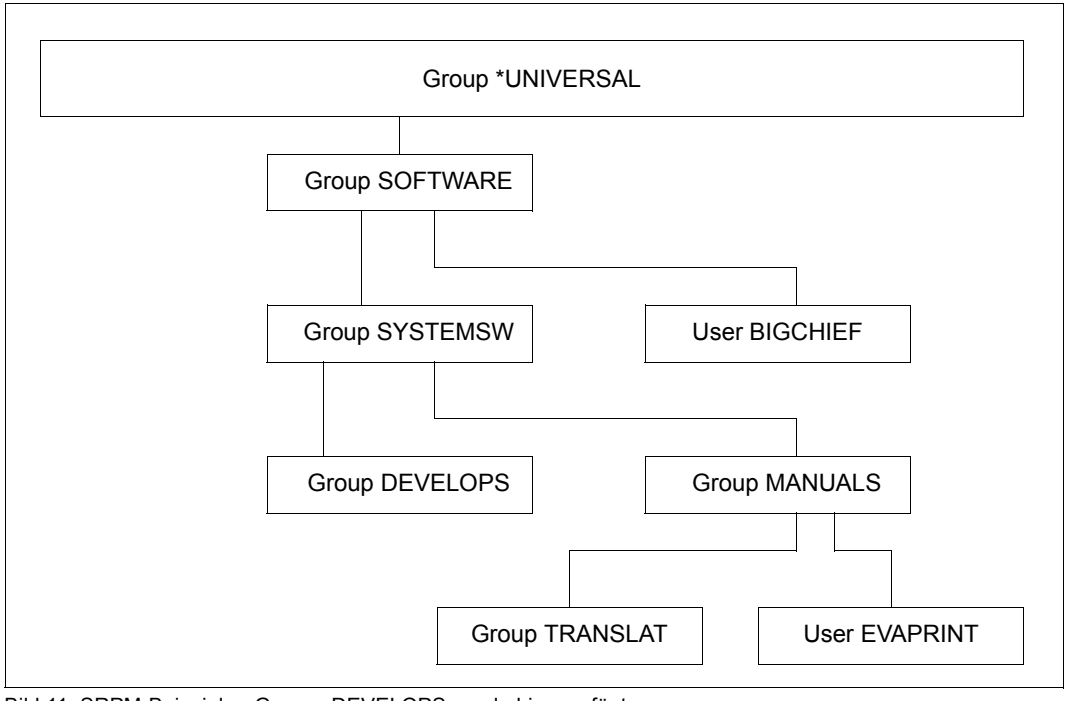


Bild 11: SRPM-Beispiele - Gruppe DEVELOPS wurde hinzugefügt

Teil 2: Der systemglobale Benutzerverwalter richtet DIAGNOSE als Untergruppe zu SYSTEMSW ein

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:13:18
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              33    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   DEVELOPS  MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Hinzufügen der Gruppe DIAGNOSE

```
/add-user-group group-identification=diagnose,pubset=x, -
/     upper-group=systemsw,adm-authority=*manage-members, -
/     max-group-members=5,max-sub-groups=5

/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:15:27
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              32    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

```
/show-user-group group-identification=diagnose,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:15:51
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          DIAGNOSE    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-MEMBERS
USER-GROUP-PREFIX                 *ANY    GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                   SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                0    LIMIT USER-ADM                      5
FREE  GROUP-HIERARCHY                0    FREE  USER-ADM                      5
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                0    LIMIT USER-ADM                      5
FREE  GROUP-HIERARCHY                0    FREE  USER-ADM                      5
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

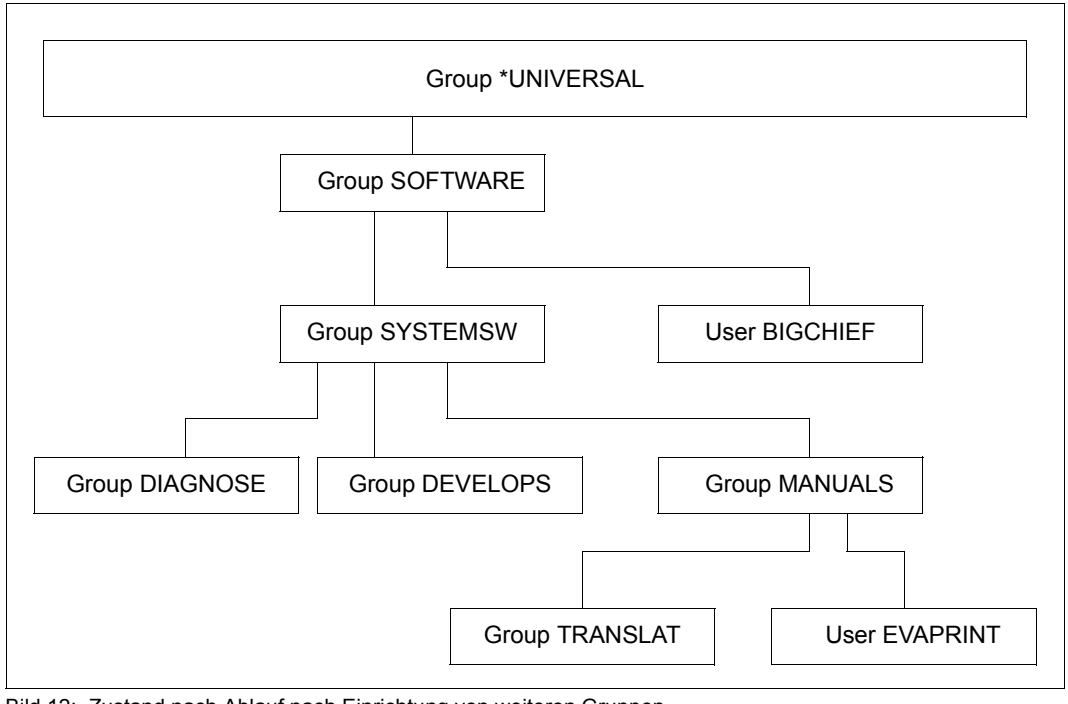


Bild 12: Zustand nach Ablauf nach Einrichtung von weiteren Gruppen

3.6.3 Beispiel 3: Vergrößern des Gruppenpotentials einer Benutzergruppe

Es wird ein größeres Gruppenpotential benötigt. Das Gruppenpotential wird entweder durch einen Gruppenverwalter vergrößert oder durch einen systemglobalen Benutzerverwalter.

Vergrößern des Gruppenpotentials durch einen Gruppenverwalter

Modifizierte Benutzergruppe

LIMIT-GROUP-HIERARCHY der Benutzergruppe wird jeweils auf die im Kommando /MODIFY-USER-GROUP angegebenen Werte erhöht.

Die Summe der Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM der Benutzergruppe wird jeweils um die Differenz der im Kommando angegebenen Werte und der bisherigen Werte erhöht.

– Ist FREE-USER-ADM kleiner als LIMIT-USER-ADM, wird zunächst FREE-USER-ADM erhöht, bis maximal der Wert LIMIT-USER-ADM erreicht ist
– Anschließend wird FREE-GROUP-HIERARCHY um den verbleibenden Rest erhöht

Der Wert von LIMIT-USER-ADM bleibt unverändert.

Übergeordnete Benutzergruppe

Die Entnahme des Gruppenpotentials und die Verrechnung in der übergeordneten Benutzergruppe erfolgt wie beim Einrichten einer neuen Benutzergruppe.

Vergrößern des Gruppenpotentials durch einen systemglobalen Benutzerverwalter

Modifizierte Benutzergruppe

LIMIT-USER-ADM und FREE-USER-ADM der Benutzergruppe werden jeweils um die Differenz der im Kommando MODIFY-USER-GROUP angegebenen Werte und der Summe der bisherigen Werte von LIMIT-GROUP-HIERARCHY und LIMIT-USER-ADM erhöht.

Übergeordnete Benutzergruppe

Das Gruppenpotential der übergeordneten Benutzergruppe bleibt unverändert.

Teil 1: Systemglobaler Benutzerverwalter erhöht Gruppenpotential von Benutzergruppe DEVELOPS

Es werden die Potentialtypen MAX-SUB-GROUPS und MAX-GROUP-MEMBERS erhöht.

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:17:16
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                            X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              32    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY

/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:18:00
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                            X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Änderung des Potentials der Gruppe DEVELOPS

```
/modify-user-group group-identification=develops,pubset=x, -
/      max-group-members=15,max-sub-groups=15
```

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:19:02
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              32    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:19:22
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     5
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     5
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Teil 2: Gruppenverwalter BIGCHIEF erhöht das Gruppenpotential der Benutzergruppe MANUALS

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:21:00
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              32    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              35    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

```
/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:21:17
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               5    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               5    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Änderung des Potential der Gruppe MANUALS

```
/modify-user-group group-identification=manuals,pubset=x, -
/       max-group-members=15,max-sub-groups=15
```

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:22:16
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                            X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              22     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              25     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:22:33
------------------------------------------------------------------------------
GROUP-IDENTIFICATION           MANUALS    PUBSET                            X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              15     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              14     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              15     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              14     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    TRANSLAT

GROUP-MEMBERS                 EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

3.6.4 Beispiel 4: Verkleinern des Gruppenpotentials einer Benutzergruppe

Es wird ein kleineres Gruppenpotential benötigt. Das Gruppenpotential wird entweder durch einen Gruppenverwalter verkleinert oder durch einen systemglobalen Benutzerverwalter.

Verkleinern des Gruppenpotentials durch einen Gruppenverwalter

Ein Gruppenverwalter kann im Gruppenpotential einer Untergruppe den Wert von FREE-GROUP-HIERARCHY maximal auf den Wert von LIMIT-GROUP-HIERARCHY setzen. Sind von diesem Gruppenverwalter bereits andere Untergruppen eingerichtet worden, verringern die Anzahl der bereits eingerichteten Gruppen die Zahl der noch möglicherweise einrichtbaren Untergruppen. Alle Werte, die als FREE-GROUP-HIERARCHIE an Untergruppen vergeben wurden, dürfen addiert maximal den Wert LIMIT-GROUP-HIERARCHY des Gruppenverwalters der übergeordneten Gruppe ergeben.

Modifizierte Benutzergruppe

LIMIT-GROUP-HIERARCHY wird jeweils auf die im Kommando MODIFY-USER-GROUP angegebenen Werte verkleinert.

LIMIT-USER-ADM bleibt jeweils unverändert.

FREE-GROUP-HIERARCHY wird jeweils um die Differenz der bisherigen Werte und der im Kommando angegebenen Werte verkleinert.

FREE-USER-ADM bleibt jeweils unverändert.

Übergeordnete Benutzergruppe

Die Summe der Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM der übergeordneten Benutzergruppe wird jeweils um die im Kommando angegebenen Werte erhöht.

– Zunächst wird FREE-USER-ADM erhöht, bis maximal der Wert von LIMIT-USER-ADM erreicht ist.

– Verbleibt noch ein Rest, wird anschließend FREE-GROUP-HIERARCHY um diesen Wert erhöht.

Verkleinern des Gruppenpotentials durch einen systemglobalen Benutzerverwalter

Ein systemglobaler Benutzerverwalter kann das Gruppenpotential einer Benutzergruppe höchstens um die Summe der Werte von LIMIT-GROUP-HIERARCHY und LIMIT-USER-ADM verkleinern.

Modifizierte Benutzergruppe

Die Summe der Werte von LIMIT-GROUP-HIERARCHY und LIMIT-USER-ADM der Benutzergruppe wird jeweils auf die im Kommando MODIFY-USER-GROUP angegebenen Werte neu festgelegt.

– Zunächst wird LIMIT-USER-ADM verkleinert, bis minimal der Wert 0 erreicht ist.

– Verbleibt noch ein Rest, wird anschließend LIMIT-GROUP-HIERARCHY um diesen Wert verkleinert.

Die Summe der Werte von FREE-GROUP-HIERARCHY und FREE-USER-ADM wird jeweils analog verkleinert.

– Zunächst wird FREE-USER-ADM verkleinert, bis minimal der Wert 0 erreicht ist.

– Verbleibt noch ein Rest, wird anschließend FREE-GROUP-HIERARCHY um diesen Wert verkleinert, bis ebenfalls minimal der Wert 0 erreicht ist. Verbleibt noch immer ein Rest, wird FREE-USER-ADM um diesen Wert verkleinert, wird also negativ.

In der Höhe, in der jeweils LIMIT-USER-ADM verkleinert wird, entsteht ein freigewordenes Gruppenpotential, das nicht der übergeordneten Benutzergruppe zurückgegeben wird.

In der Höhe, in der jeweils LIMIT-GROUP-HIERARCHY verkleinert wird, entsteht ein freies Gruppenpotential, das der übergeordneten Benutzergruppe zurückgegeben wird.

Übergeordnete Benutzergruppe

Ein zurückgegebenes Gruppenpotential wird in der übergeordneten Benutzergruppe jeweils so verrechnet, dass zunächst FREE-USER-ADM erhöht wird, bis maximal der Wert von LIMIT-USER-ADM erreicht ist. Um den Rest wird FREE-GROUP-HIERARCHY erhöht.

Teil 1: Gruppenverwalter BIGCHIEF richtet Benutzergruppe INTRFACE in DEVELOPS ein

Aus einer Modifizierung der Aufgaben ergibt sich, dass sich in DEVELOPS eine Arbeitsgruppe bildet, die sich mit den Benutzerschnittstellen befassen soll. Dies wird in der Gruppenstruktur widergespiegelt.

```
/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:24:00
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     5
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY              10    FREE  USER-ADM                     5
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Hinzufügen der Gruppe INTRFACE

```
/add-user-group group-identification=intrface,pubset=x, -
/     upper-group=develops,max-group-members=5,max-sub-groups=5

/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 11:26:25
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                     5
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY               5    FREE  USER-ADM                     5
.
.
.
SUB-GROUPS                   INTRFACE

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/show-user-group group-identification=intrface,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 11:27:09
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          INTRFACE    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                 *ANY    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   DEVELOPS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY                5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                5    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY                5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY                5    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

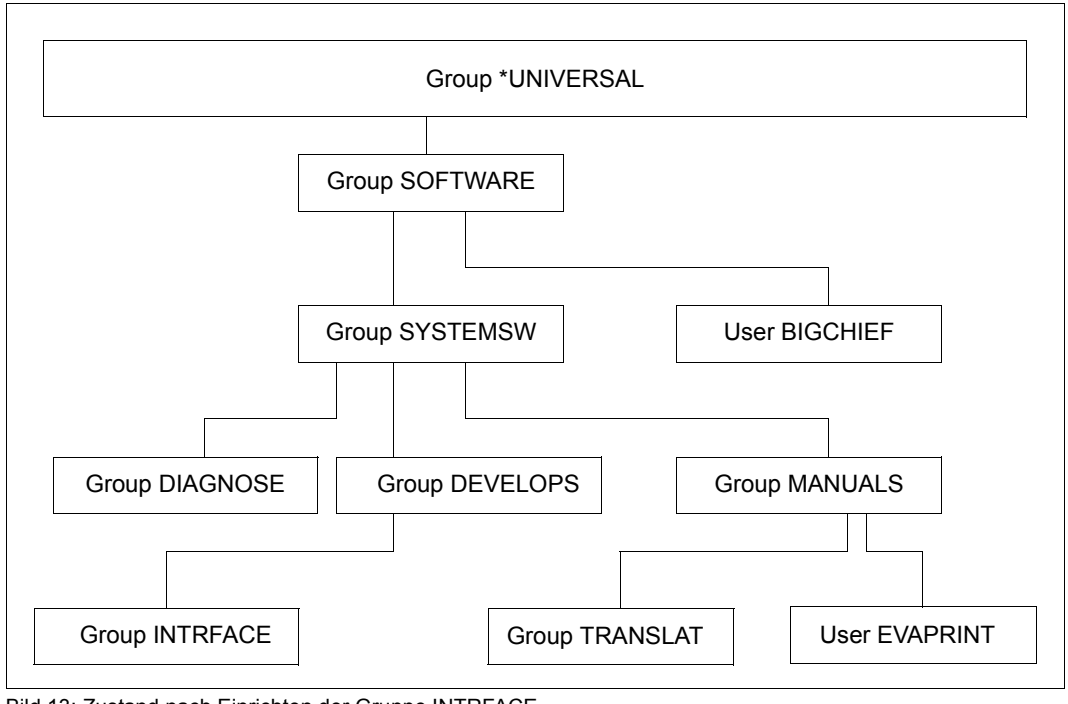


Bild 13: Zustand nach Einrichten der Gruppe INTRFACE

Teil 2: Gruppenverwalter BIGCHIEF richtet Benutzergruppe INDEX als Untergruppe zu MANUALS ein

Diese Arbeitsgruppe erstellt den MASTER-Index aller BS2000-Handbücher.

```
/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:17:25
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY             15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY             14    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY             15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY             14    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY


/add-user-group group-identification=index,pubset=x, -
/     upper-group=manuals,max-group-members=4,max-sub-groups=4

/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:20:36
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY             15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              9    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY             15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY             10    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   INDEX     TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/show-user-group group-identification=index,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:21:00
------------------------------------------------------------------------------
GROUP-IDENTIFICATION            INDEX    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               4    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               4    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

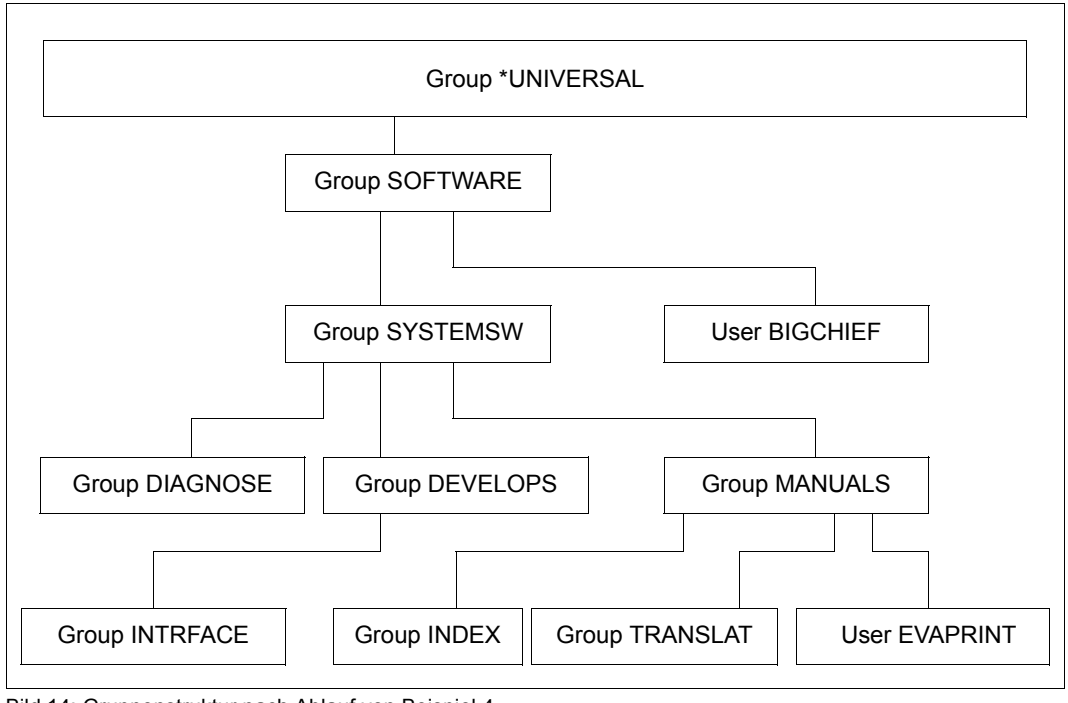


Bild 14: Gruppenstruktur nach Ablauf von Beispiel 4

Teil 3: Gruppenverwalter BIGCHIEF reduziert das Gruppenpotential von Benutzergruppe INDEX

```
/modify-user-group group-identification=index,pubset=x, -
/       max-group-members=2,max-sub-groups=2
```

```
/show-user-group group-identification=manuals,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:23:30
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY         *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              15    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              11    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              15    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              12    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   INDEX     TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

```
/show-user-group group-identification=index,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:23:53
------------------------------------------------------------------------------
GROUP-IDENTIFICATION            INDEX    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                     0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Teil 4: Systemglobaler Benutzerverwalter reduziert das Gruppenpotential von Benutzergruppe DEVELOPS

Eigenschaften der Gruppe SYSTEMSW vor der Änderung

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:25:48
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                            X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              22    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              25    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Eigenschaften der Gruppe DEVELOPS vor der Änderung

```
/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:26:10
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                            X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY               4    FREE  USER-ADM                     5
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              10    LIMIT USER-ADM                     5
FREE  GROUP-HIERARCHY               5    FREE  USER-ADM                     5
.
.
.
SUB-GROUPS                   INTRFACE

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Änderung der Eigenschaften der Gruppe DEVELOPS

```
/modify-user-group group-identification=develops,pubset=x, -
/       max-group-members=8,max-sub-groups=8
```

Eigenschaften der Gruppe SYSTEMSW nach der Änderung

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:28:39
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              24    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              27    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   INTRFACE

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Eigenschaften der Gruppe DEVELOPS nach der Änderung

```
/show-user-group group-identification=develops,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:29:00
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               3    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   INTRFACE

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

3.6.5 Beispiel 5: Umhängen einer Benutzergruppe

Eine Benutzergruppe soll umgehängt werden. Dazu ist entweder ein Gruppenverwalter berechtigt oder ein systemglobaler Benutzerverwalter.

Umhängen einer Benutzergruppe durch einen Gruppenverwalter

Ein Gruppenverwalter ist zum Umhängen einer Benutzergruppe berechtigt, wenn er

– sowohl zur Verwaltung der übergeordneten Benutzergruppe der umzuhängenden Benutzergruppe berechtigt ist

– als auch zur Verwaltung der (neuen übergeordneten) Benutzergruppe, die das Ziel dieser Verwaltungsmaßnahme darstellt

Umzuhängende Benutzergruppe

Das der umzuhängenden Benutzergruppe von einem systemglobalen Benutzerverwalter zugeteilte Gruppenpotential bleibt der Benutzergruppe als zusätzliches Kontingent erhalten. Für die Überprüfung, ob das Kontingent der neuen übergeordneten Benutzergruppe ausreicht, ist der Wert von LIMIT-GROUP-HIERARCHY entscheidend.

Neue übergeordnete Benutzergruppe

FREE-GROUP-HIERARCHY und FREE-USER-ADM der neuen übergeordneten Benutzergruppe muss jeweils in einer Höhe verfügbar sein, die das Einrichten der umzuhängenden Benutzergruppe mit dem ihr zugeteilten Gruppenpotential als Untergruppe zulassen. Ggf. ist das Gruppenpotential der umzuhängenden Benutzergruppe oder der neuen übergeordneten Benutzergruppe anzupassen.

Das Gruppenpotential in der neuen übergeordneten Benutzergruppe wird in der gleichen Weise verrechnet wie beim Einrichten einer neuen Benutzergruppe.

Bisherige übergeordnete Benutzergruppe

Das Gruppenpotential in der bisherigen übergeordneten Benutzergruppe wird wie beim Löschen einer Benutzergruppe verrechnet.

Umhängen einer Benutzergruppe durch einen systemglobalen Benutzerverwalter

Eine Benutzergruppe wird umgehängt durch einen systemglobalen Benutzerverwalter analog zum Umhängen einer Benutzergruppe durch einen Gruppenverwalter.

Neue übergeordnete Benutzergruppe

FREE-USER-ADM kann durch das Umhängen einen negativen Wert (Systemschuld) erhalten, wenn das frei verfügbare Gruppenpotential der neuen übergeordneten Benutzergruppe nicht ausreicht. Eine Anpassung der umzuhängenden Benutzergruppe ist nicht erforderlich.

Bisherige übergeordnete Benutzergruppe

Das Gruppenpotential wird in der bisherigen übergeordneten Benutzergruppe so verrechnet wie beim Löschen einer Benutzergruppe.

Es gelten die Voraussetzungen und Werte für Benutzergruppe INTRFACE und TRANSLAT wie in Beispiel 4.

Teil 1: Gruppenverwalter BIGCHIEF hängt Benutzergruppe INTRFACE direkt an die Gruppe SYSTEMSW

Die Gruppe INTRFACE nimmt ihr Potential mit. Dadurch ändern sich die Potentiale von DEVELOPS und SYSTEMSW.

Eigenschaften der Gruppe SYSTEMSW vor der Änderung

```
/show-user-group group-identification=systemsw,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:31:28
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              24    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              27    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Eigenschaften der Gruppe DEVELOPS vor der Änderung

```
/show-user-group group-identification=develops,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:32:36
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                             X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               3    FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                   INTRFACE

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

Eigenschaften der Gruppe INTRFACE vor der Änderung

```
/show-user-group group-identification=intrface,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:32:57
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          INTRFACE    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   DEVELOPS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               5     LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               5     FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               5     LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               5     FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Durchführung der Änderung

```
/modify-user-group group-identification=intrface,pubset=x, -
/       upper-group=systemsw
```

Eigenschaften der Gruppe SYSTEMSW nach der Änderung

```
/show-user-group group-identification=systemsw,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:34:06
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              18     FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              22     FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   INTRFACE  MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Eigenschaften der Gruppe DEVELOPS nach der Änderung

```
/show-user-group group-identification=develops,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:34:27
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         DEVELOPS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               8    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               8    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               8    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Eigenschaften der Gruppe INTRFACE nach der Änderung

```
/show-user-group group-identification=intrface,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:34:48
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         INTRFACE    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               5    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               5    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               5    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

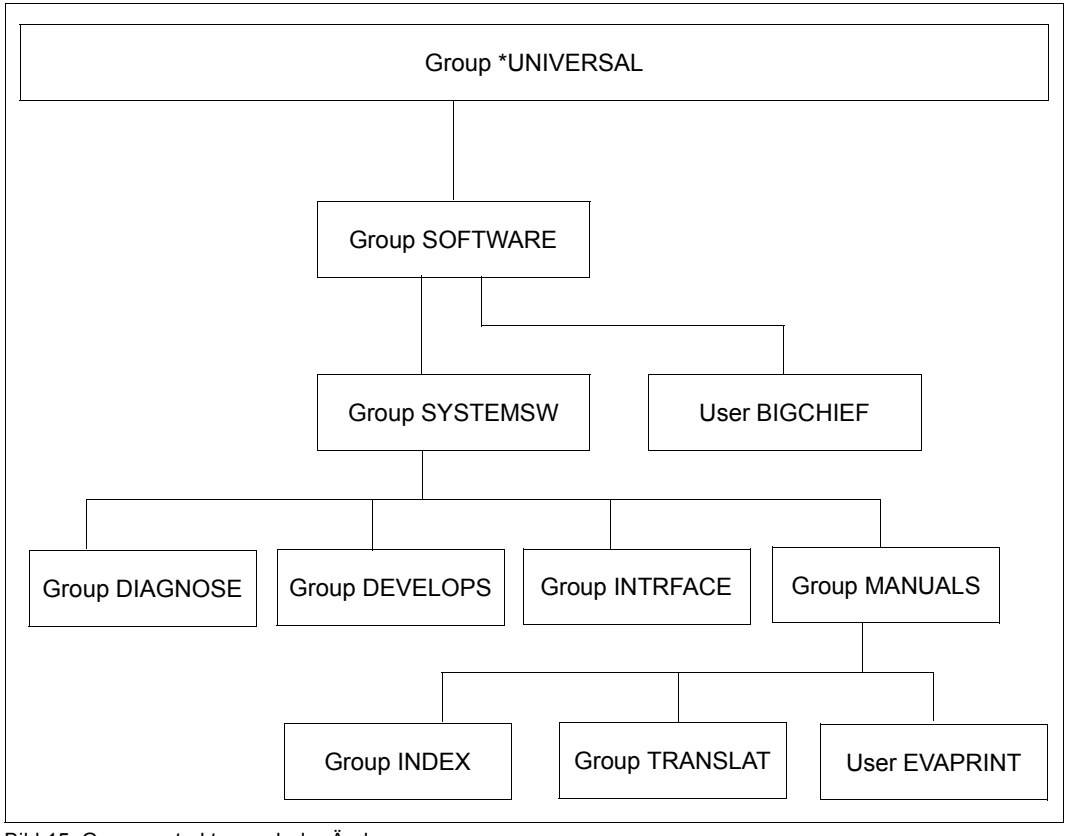


Bild 15: Gruppenstruktur nach der Änderung

Teil 2: Systemglobaler Benutzerverwalter hängt Benutzergruppe INDEX direkt an SYSTEMSW

Die Gruppe INDEX nimmt ihr Potential mit.

Eigenschaften der Gruppe SYSTEMSW vor der Änderung

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:35:44
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              18     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              22     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   INTRFACE  MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Eigenschaften der Gruppe MANUALS vor der Änderung

```
/show-user-group group-identification=manuals,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:36:03
------------------------------------------------------------------------------
GROUP-IDENTIFICATION           MANUALS    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY        *MANAGE-MEMBERS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                   SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              15     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              11     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              15     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              12     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    INDEX     TRANSLAT

GROUP-MEMBERS                 EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Eigenschaften der Gruppe INDEX vor der Änderung

```
/show-user-group group-identification=index,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:36:21
------------------------------------------------------------------------------
GROUP-IDENTIFICATION            INDEX    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   MANUALS

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Die Gruppe INDEX wird umgehängt

```
/modify-user-group group-identification=index,pubset=x, -
/       upper-group=systemsw
```

Das Potential der Gruppe SYSTEMSW ändert sich

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:37:06
------------------------------------------------------------------------------
GROUP-IDENTIFICATION         SYSTEMSW    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                  SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              15    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              20    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   DEVELOPS  DIAGNOSE   INTRFACE  INDEX     MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Das Potential der Gruppe MANUALS ändert sich

```
/show-user-group group-identification=manuals,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:37:28
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          MANUALS    PUBSET                              X
GROUP-ADMINISTRATOR             *NONE    ADM-AUTHORITY          *MANAGE-MEMBERS
USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              14    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              15    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY              14    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                   TRANSLAT

GROUP-MEMBERS                EVAPRINT
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Das Potential der Gruppe INDEX

```
/show-user-group group-identification=index,pubset=x
```

```
SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:37:47
------------------------------------------------------------------------------
GROUP-IDENTIFICATION             INDEX    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX                *ANY
UPPER-GROUP                  SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               2    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               2    FREE  USER-ADM                      0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Hinweis

INTRFACE und TRANSLAT behalten ihre Gruppenpotentiale.

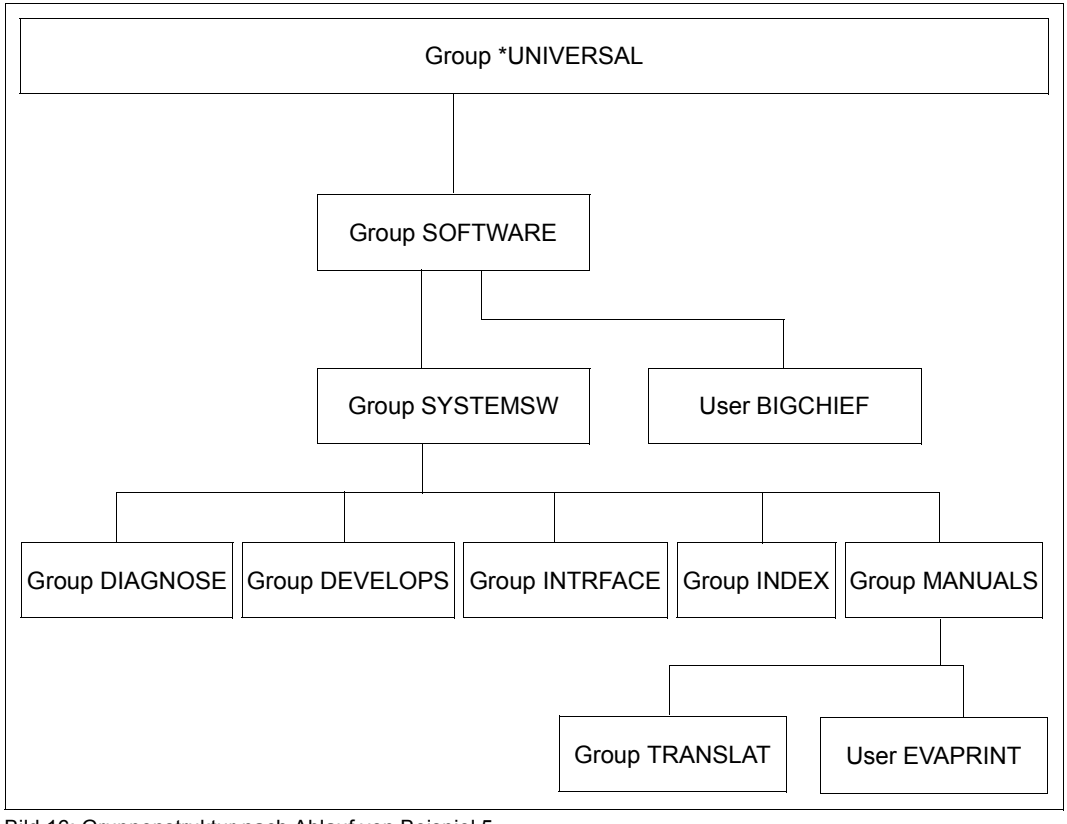


Bild 16: Gruppenstruktur nach Ablauf von Beispiel 5

3.6.6 Beispiel 6: Löschen einer Benutzergruppe

Eine Benutzergruppe kann erst dann gelöscht werden, wenn sie keine Gruppenmitglieder oder Untergruppen mehr enthält.

Löschen einer Benutzergruppe durch einen Gruppenverwalter

Übergeordnete Benutzergruppe

Die Verrechnung des zurückgegebenen Gruppenpotentials in der übergeordneten Benutzergruppe erfolgt wie beim Verkleinern des Gruppenpotentials.

Ein freigewordenes Gruppenpotential LIMIT-USER-ADM wird nicht an die übergeordnete Benutzergruppe zurückgegeben.

Löschen einer Benutzergruppe durch einen systemglobalen Benutzerverwalter

Das Löschen einer Benutzergruppe durch einen systemglobalen Benutzerverwalter erfolgt analog zum Löschen einer Benutzergruppe durch einen Gruppenverwalter.

Teil 1: Gruppenverwalter BIGCHIEF löscht Benutzergruppe INTRFACE

Zustand der Gruppe SYSTEMSW, bevor INTRFACE gelöscht wird.

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:39:09
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                            X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              15     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              20     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   INTRFACE  INDEX     MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Potential der Gruppe INTRFACE

```
/show-user-group group-identification=intrface,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                        2018-03-05 12:39:32
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          INTRFACE    PUBSET                            X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX               *ANY
UPPER-GROUP                   SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               5     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               5     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               5     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               5     FREE  USER-ADM                     0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Entfernen der Gruppe INTRFACE

```
/remove-user-group group-identification=intrface,pubset=x
```

Geändertes Potential der Gruppe SYSTEMSW

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:40:07
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                              X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                 *ANY    GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               21    FREE  USER-ADM                      0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               50    LIMIT USER-ADM                      0
FREE  GROUP-HIERARCHY               25    FREE  USER-ADM                      0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   INDEX     MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

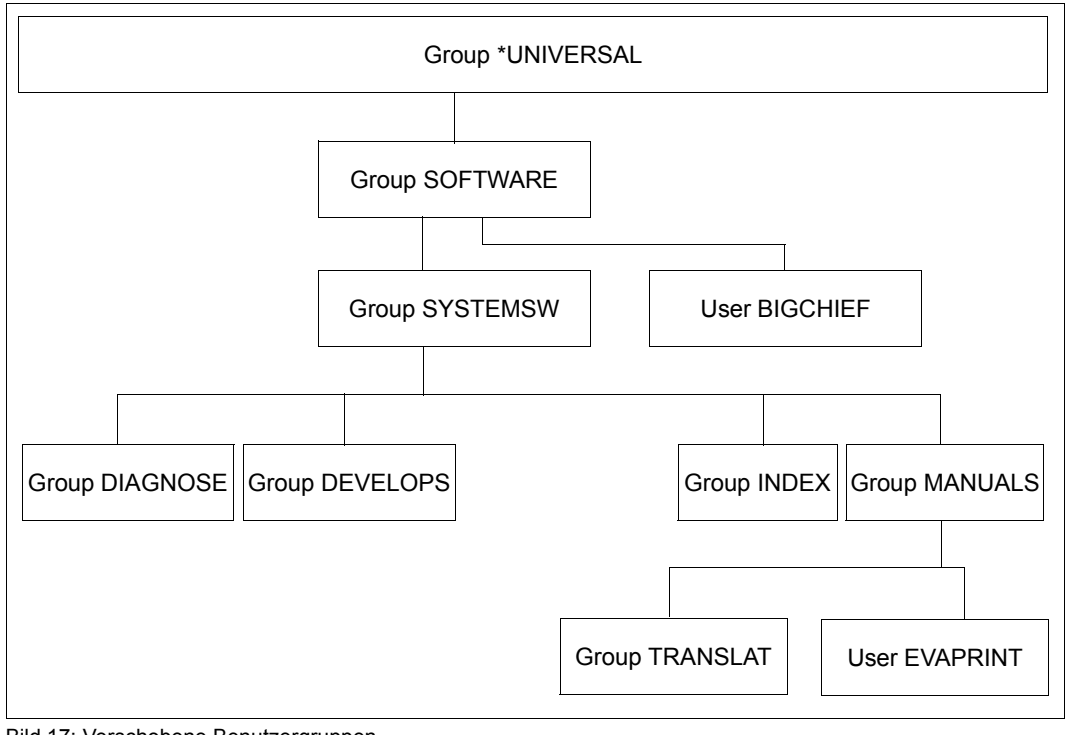


Bild 17: Verschobene Benutzergruppen

Teil 2: Systemglobaler Benutzerverwalter löscht Benutzergruppe INDEX

Nach der Erstellung des MASTER-Indexes wird die Gruppe INDEX gelöscht.

```
/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:40:46
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              21     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              25     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   INDEX     MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY

/show-user-group group-identification=index,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:41:09
------------------------------------------------------------------------------
GROUP-IDENTIFICATION             INDEX    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY       *MANAGE-RESOURCES
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SYSTEMSW

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY               2     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY               2     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY               2     FREE  USER-ADM                     0
.
.
.
NO SUB-GROUP SPECIFIED

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                            END OF DISPLAY
```

Entfernen der Gruppe INDEX

```
/remove-user-group group-identification=index,pubset=x

/show-user-group group-identification=systemsw,pubset=x

SHOW-USER-GROUP   INFORMATION = *ALL                          2018-03-05 12:41:44
------------------------------------------------------------------------------
GROUP-IDENTIFICATION          SYSTEMSW    PUBSET                             X
GROUP-ADMINISTRATOR              *NONE    ADM-AUTHORITY          *MANAGE-GROUPS
USER-GROUP-PREFIX                *ANY     GROUP-MEMBER-PREFIX              *ANY
UPPER-GROUP                   SOFTWARE

MAX-SUB-GROUPS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              24     FREE  USER-ADM                     0
MAX-GROUP-MEMBERS...
LIMIT GROUP-HIERARCHY              50     LIMIT USER-ADM                     0
FREE  GROUP-HIERARCHY              27     FREE  USER-ADM                     0
.
.
.
SUB-GROUPS                    DEVELOPS  DIAGNOSE   MANUALS

NO GROUP-MEMBER SPECIFIED
------------------------------------------------------------------------------
SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

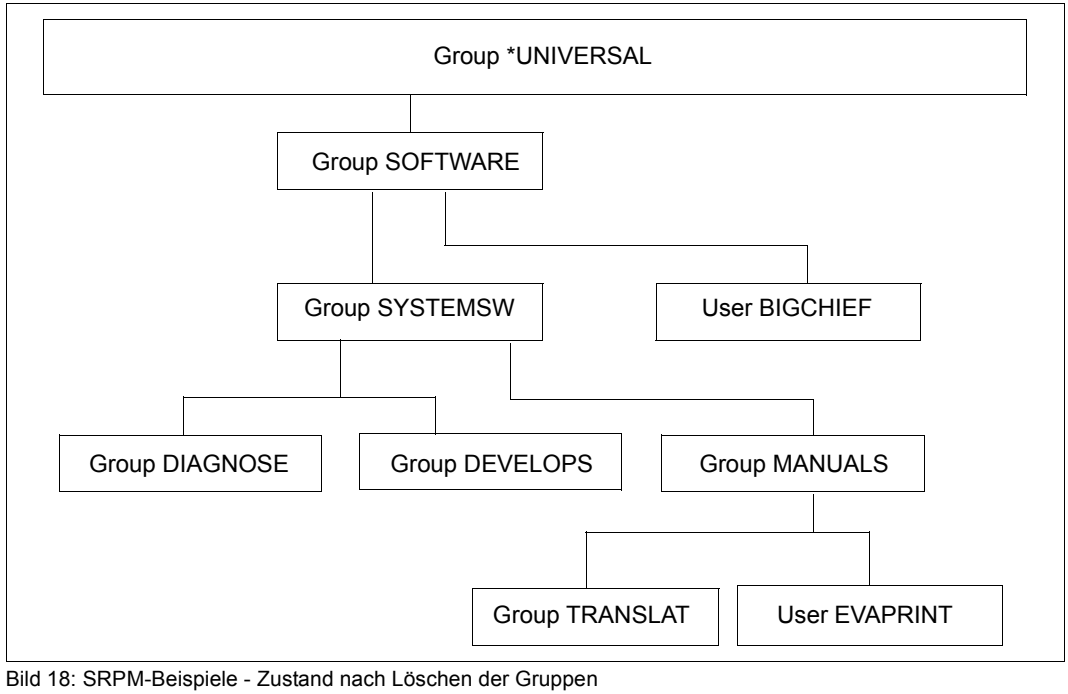


Bild 18: SRPM-Beispiele - Zustand nach Löschen der Gruppen

4 Zugriffsschutzmechanismen des BS2000

BS2000 bietet für den Zugriffsschutz unterschiedliche Mechanismen an. Davon gehören einige zum Grundausbau des BS2000, während andere nur bei Einsatz von SECOS genutzt werden können. Alle Zugriffsschutzmechanismen sind objektorientiert, das heißt, für ein Objekt wird festgelegt, welche Subjekte zugreifen dürfen und welche nicht.

Als **Objekt** wird hierbei das Element bezeichnet, das geschützt werden soll. Hierbei handelt es sich in erster Linie um Dateien. In Abhängigkeit vom verwendeten Schutzmechanismus sind aber auch andere Objekte, wie zum Beispiel Jobvariable, möglich.

Als **Subjekt** wird die Instanz bezeichnet, die auf ein Objekt zugreifen möchte. Dies sind vor allem die Systembenutzer (User).

Für jedes zu schützende Objekt muss einzeln oder als Bestandteil einer Menge festgelegt werden, welche Subjekte zugriffsberechtigt sind. Die Zugriffsschutzmechanismen unterscheiden sich durch folgende Kriterien:

– Methode, mit der der Zugriffsschutz für Objekte festgelegt wird

– Detaillierungsgrad, mit dem der Zugriffsschutz für Objekte festgelegt werden kann

4.1 Übersicht über Zugriffsschutzmechanismen

Folgende Zugriffsschutzmechanismen sind Bestandteil des BS2000-Grundausbaus:

– Begrenzter Pubset-Zugriff (Maßnahme der Systemverwaltung)
  Die Verteilung von Benutzerkennungen auf unterschiedliche Pubsets ermöglicht es, Objekte (z.B. Dateien) auf einem Pubset vor dem Zugriff durch Benutzer auf einem anderen Pubset zu schützen.

– Schutzattribute ACCESS und USER-ACCESS
  Mit den Operanden ACCESS und USER-ACCESS der Kommandos /CREATE-FILE und /MODIFY-FILE-ATTRIBUTES legt der Benutzer Zugriffsrechte für sich und systemweit alle anderen fest (siehe Seite 424).

– Einfache Zugriffskontrollliste (Basic Access Control List, BACL)
  Mit dem Zugriffsschutzmechanismus BACL kann der Benutzer Zugriffsrechte auf Objekte (z.B. Dateien) für eine differenzierte Menge von Subjekten festlegen. Die Zugriffsrechte Lesen (read), Schreiben (write) und Ausführen (exec) können für jede der Benutzerklassen Owner, Group und Others getrennt vergeben werden (siehe Seite 425).

– Kennwort
  Für jede seiner Dateien kann der Benutzer Kennwörter (Lese-, Schreib- und Ausführungs-Kennwort) vereinbaren. Vor der Verarbeitung kennwortgeschützter Dateien ist das entsprechende Kennwort anzugeben. Kennwörter können verschlüsselt werden.

– Schutzfrist
  Ein Benutzer kann seiner Datei eine Schutzfrist zuordnen, innerhalb der diese Datei nicht geändert werden darf (siehe Handbuch „Kommandos“ [4]).

– Dateiverschlüsselung
  Es besteht die Möglichkeit, Dateien verschlüsselt abzulegen. Näheres hierzu finden Sie im Handbuch „Einführung in das DVS“ [6].

Von den genannten Schutzmöglichkeiten des BS2000-Grundausbaus sollen im Folgenden nur die Schutzmechanismen ACCESS/USER-ACCESS und die einfache Zugriffskontrollliste (BACL) näher betrachtet werden.

SECOS bietet zusätzlich den Zugriffsschutz mit GUARDS

– Mit GUARDS können Zugriffsbedingungen für unterschiedlichste Objekte definiert und bei Objektzugriffen ausgewertet werden. Der Zugriffsschutz wird dabei über so genannte Guards realisiert, in die die Zugriffsbedingungen eingetragen sind.

  Der wesentliche Unterschied zu den anderen Schutzmechanismen ist die Aufhebung der 1:1-Beziehung zwischen Objekt und Subjekt. Die in einem Guard eingetragenen Zugriffsbedingungen gelten nicht zwangsweise nur für ein bestimmtes Objekt. Mit einem einzigen Guard können beliebig viele Objekte, auch unterschiedlichen Typs, mit demselben Schutz versehen werden. Näheres zu GUARDS finden Sie ab Seite 427.

Einsatzmöglichkeit der Schutzmechanismen

Die folgende Tabelle zeigt, welche Objekttypen mit welchem Schutzmechanismus geschützt werden können:

Objekt	Schutzmechanismus	Begrenzter Pubset-Zugriff	ACCESS USER-ACCESS	BACL	Kennwort	Schutzfrist	GUARDS
Datei[1]	public	+	+	+	+	+	+
	temporär	-	-	-	-	-	-
	privat	-	+	+	+	+	-
	Band	-	+	-	+	+	-
Dateigenerationsgruppe	Index public, FGen public	-	+	+	+	+	+
	Index public, FGen Band	-	+	+	+	+	+
	Index privat, FGen privat	-	+	+	+	+	-
Jobvariable	permanent	+	+	+	+	+	+
	temporär	-	-	-	-	-	-
Bibliotheks-Element[2]		-	-	+	-	-	+
FITC-Port		-	-	-	-	-	+
Storage-Klassen		-	-	-	-	-	+
HSMS-Managementklassen		-	-	-	-	-	+

+: Schutzmechanismus anwendbar, -: Schutzmechanismus nicht anwendbar
[1] Falls Datei eine Bibliothek ist, siehe „Besonderheiten bei Bibliothekszugriffen“ auf Seite 422
[2] siehe „Besonderheiten bei Bibliothekszugriffen“ auf Seite 422

Tabelle 7: Schutzmechanismen für Objekte

Wie die Tabelle zeigt, können manche Objekte mit mehreren Schutzmechanismen geschützt werden. Von den Schutzmechanismen ACCESS/USER-ACCESS, BACL und GUARDS kann jeweils nur einer für ein Objekt wirksam sein (siehe „Hierarchie der Schutzmechanismen ACCESS/USER-ACCESS - BACL - GUARDS“ auf Seite 422). Alle übrigen Schutzmechanismen gelten zusätzlich.

Hierarchie der Schutzmechanismen ACCESS/USER-ACCESS - BACL - GUARDS

Beim gleichzeitigen Einsatz der Schutzmechanismen ACCESS/USER-ACCESS, BACL und GUARDS für dasselbe Objekt könnten widersprüchliche Situationen entstehen. Um diese zu vermeiden, gilt folgende Hierarchie:

– Wenn der Schutz eines Objektes über Guards definiert ist,
dann gelten ausschließlich die in den Guards festgelegten Zugriffsbedingungen. Eine ggf. für das Objekt definierte BACL und die Schutzattribute ACCESS/USER-ACCESS bleiben unberücksichtigt.

– Wenn kein Guardschutz für ein Objekt definiert ist, aber eine BACL,
dann gilt die in der BACL festgelegte Schutzeinstellung. Die Schutzattribute ACCESS und USER-ACCESS bleiben unberücksichtigt.

– Wenn der Schutz eines Objektes weder mit Guards noch mit BACL geregelt ist,
dann werden für den Schutzmechanismus die Schutzattribute ACCESS und USER-ACCESS herangezogen.

In allen Fällen gelten zusätzlich der Kennwortschutz und die Schutzfrist.

Besonderheiten bei Bibliothekszugriffen

PLAM-Bibliotheks**dateien** können als Ganzes wie eine Datei geschützt werden. Davon unabhängig können Bibliotheks**elemente** mit der LMS-Anweisung //MODIFY-ELEMENT-PROTECTION geschützt werden.

Beim Zugriff auf Bibliotheken und Bibliothekselemente ist daher Folgendes zu beachten:

– Der Zugriff auf einzelne Bibliothekselemente wird durch die mit //MODIFY-ELEMENT-PROTECTION festgelegten Schutzmechanismen geregelt. Unabhängig vom Elementschutz ist dieser Zugriff jedoch nur möglich, wenn die Bibliotheksdatei in ihrer Gesamtheit gelesen werden darf.

– Beim Zugriff auf eine Bibliothek in ihrer Gesamtheit (mit ARCHIVE, mit File-Transfer oder mit dem DVS-Kommando /COPY-FILE) gilt Folgendes:

  a) Ist die Bibliothek weder durch eine BACL noch durch Guards geschützt, kann auf sie zugegriffen werden wie auf eine beliebige Datei.

b) Für den Zugriff auf eine Bibliothek, die durch eine BACL oder ein Guard geschützt ist, können die Zugriffsregelungen folgender Tabelle entnommen werden:

		Bibliothek enthält mindestens ein Element, das mit einer BACL oder einem Guard geschützt ist	Bibliothek enthält **kein** Element, das mit einer BACL oder einem Guard geschützt ist
Zugriff durch	**Eigentümer**	*	*
	Miteigentümer	*	*
	andere	Zugriff verboten	*
* Zugriff hängt von den Zugriffsregelungen der gesamten Bibliothek ab			

Tabelle 8: Zugriffsregelungen beim Zugriff auf Bibliotheken

4.2 Zugriffskontrolle des Grundausbaus von BS2000

Im Folgenden werden die wichtigsten Zugriffsschutzmechanismen des BS2000-Grundausbaus erläutert.

4.2.1 Zugriffsschutz mit ACCESS/USER-ACCESS

Die Zugriffsregelung über die Schutzattribute ACCESS und USER-ACCESS bildet in der Hierarchie der Schutzmechanismen die niedrigste Stufe. Sie wird für ein Objekt nur dann wirksam, wenn für das Objekt weder eine BACL noch ein Guard definiert ist.

Kennwortschutz und die Schutzfrist bleiben jedoch immer zusätzlich wirksam.

Schutzattribut ACCESS

Mit dem Schutzattribut ACCESS kann für ein Objekt Schreib- oder Leserecht festgelegt werden. Das Schreibrecht schließt hierbei das Leserecht ein.

Schutzattribut USER-ACCESS

Mit dem Schutzattribut USER-ACCESS kann für eine Datei festgelegt werden, ob nur der Eigentümer (*USER-ONLY) oder alle Systembenutzer (*ALL-USERS) auf sie zugreifen dürfen.

Eine Benutzerkennung mit dem Privileg HARDWARE-MAINTENANCE (Online-Wartung) wird dabei besonders behandelt. Sie zählt standardmäßig **nicht** zur Menge aller Benutzer, die mit *ALL-USERS bezeichnet werden. Benutzerkennungen mit dem Privileg HARDWARE-MAINTENANCE erhalten nur Zugriff, wenn Folgendes gilt:

- Falls die Datei mit Guards geschützt ist, müssen im Guard Zugriffsbedingungen festgelegt sein, die der privilegierten Benutzerkennung den Zugriff erlauben.
- Falls die Datei nicht mit Guards geschützt ist, aber durch eine einfache Zugriffskontrollliste (BACL), muss diese der privilegierten Benutzerkennung den Zugriff erlauben.
- Wenn die Datei weder mit Guards noch mit einer BACL geschützt ist, muss USER-ACCESS=*SPECIAL gesetzt sein.

Beispiel

```
/modify-file-attributes file-name=test,protection=*par( -
/                       access=*read,user-access=*all-users)
```

```
/show-file-attributes file-name=test,information=*par(security=*yes)

00000003 :2OSG:$QM212.TEST
  ------------------------------ SECURITY     ------------------------------
  READ-PASS  = NONE        WRITE-PASS = NONE        EXEC-PASS  = NONE
  USER-ACC   = ALL-USERS   ACCESS     = READ        ACL        = NO
  AUDIT      = NONE        FREE-DEL-D = *NONE       EXPIR-DATE = 2004-10-08
  DESTROY    = NO          FREE-DEL-T = *NONE       EXPIR-TIME =   00:00:00
  SP-REL-LOCK= NO
:2OSG: PUBLIC:      1 FILE  RES=        3  FREE=        2  REL=        0 PAGES
```

Weitere Informationen zu dieser Art des Datei-Zugriffsschutz erhalten Sie im Handbuch „Einführung in das DVS“ [6].

4.2.2 Einfache Zugriffskontrollliste (BACL)

Eine Stufe über den Schutzattributen ACCESS/USER-ACCESS liegt in der Hierarchie der Zugriffsschutzmechanismen die einfache Zugriffskontrollliste (Basic Access Control List, BACL). Sie ist für ein Objekt dann wirksam, wenn für das Objekt kein Guards-Schutz definiert ist. Kennwortschutz und Schutzfrist sind zusätzlich wirksam.

Mit einer BACL können für den Objekt-Eigentümer, für die Mitglieder seiner Benutzergruppe und für alle anderen Benutzer unterschiedliche Zugriffsrechte definiert werden. Eine Festlegung von Zugriffsrechten für einzelne Benutzerkennungen ist mit diesem Zugriffsschutzmechanismus jedoch nicht möglich.

Eine einfache Zugriffskontrollliste für Dateien wird mit dem Operanden BASIC-ACL der Kommandos /CREATE-FILE oder /MODIFY-FILE-ATTRIBUTES definiert.

Einfache Zugriffskontrolllisten für Jobvariablen können entsprechend mit den Kommandos /CREATE-JV oder /MODIFY-JV-ATTRIBUTES definiert werden.

Benutzerklassen

Aufbauend auf dem Konzept der Benutzergruppen gibt es beim Schutzmechanismus BACL Benutzerklassen, die jeweils unterschiedliche Zugriffsrechte erhalten können. Die Benutzerklassen unterteilen die Menge aller Benutzer in folgende Teilmengen:

– OWNER: Eigentümer eines Objekts – die Benutzerkennung, unter der die Datei oder Jobvariable katalogisiert ist

  Auch Miteigentümer, die mit Hilfe des Miteigentümerschutzes festgelegt wurden (siehe Seite 471), fallen unter diese Benutzerklasse.

– GROUP: Alle Benutzerkennungen, die derselben Benutzergruppe wie der Eigentümer angehören, mit Ausnahme des Eigentümers selbst und der Miteigentümer

– OTHERS: Alle übrigen Benutzer mit Ausnahme der Miteigentümer

Die Benutzer werden individuell aus der Sicht des Objekteigentümers klassifiziert. Bezüglich eines Objekts sind die Benutzerklassen OWNER, GROUP und OTHERS immer disjunkte Mengen von Benutzern.

Hinweise zur Benutzerklasse GROUP

Alle Benutzer, die keiner explizit eingerichteten Gruppe zugeordnet sind, sind automatisch Mitglied der implizit eingerichteten Gruppe *UNIVERSAL. Dies gilt insbesondere dann, wenn gar keine Gruppen explizit eingerichtet wurden. In diesem Fall sind alle Systembenutzer Mitglied derselben Gruppe. Bei der Auswertung einer BACL erhalten daher alle zugreifenden Benutzerkennungen außer dem Objekteigentümer selbst die Zugriffsrechte aus dem GROUP-Eintrag und nicht die des OTHERS-Eintrags.

Für Mitglieder der Benutzergruppe *UNIVERSAL wird daher dringend empfohlen, für die Benutzerklassen GROUP und OTHERS die gleichen Zugriffsrechte zu vergeben.

Zugriffsrechte

Für jede der Benutzerklassen können drei Zugriffsrechte festgelegt werden:

- Lesen (R)
- Schreiben (W)
- Ausführen (X)

Im Gegensatz zum Schutzattribut ACCESS schließt keines der Rechte ein anderes ein.

Beispiel

Der Eigentümer einer Datei will auf diese lesend, schreibend und ausführend zugreifen. Den Mitgliedern seiner Benutzergruppe will er den lesenden und schreibenden Zugriff gestatten. Allen anderen Benutzern soll nur der lesende Zugriff erlaubt sein.

```
/create-file file-name=test,protection=(basic-acl=( -
/                              owner=(read=*yes,write=*yes,exec=*yes), -
/                              group=(read=*yes,write=*yes), -
/                              others=(read=*yes)))
/show-file-attr file-name=test,information=(security=*yes)

%00000003 :AAAA:$EVA.TEST
%  ------------------------------ SECURITY     --------------------------------
%  READ-PASS  = NONE        WRITE-PASS = NONE       EXEC-PASS  = NONE
%  USER-ACC   = OWNER-ONLY  ACCESS     = WRITE      ACL        = NO
%  OWNER      = R W X       GROUP      = R W -      OTHERS     = R - -
%  AUDIT      = NONE        FREE-DEL-D = *NONE      EXPIR-DATE = NONE
%  DESTROY    = NO          FREE-DEL-T = *NONE      EXPIR-TIME = NONE
%  SP-REL-LOCK= NO
```

Weitere Informationen zur BACL finden Sie im Handbuch „Einführung in das DVS“ [6].

5 GUARDS – Schutz für Objekte

GUARDS (Generally Usable Access contRol aDministration System) ermöglicht es, unterschiedliche Schutzmechanismen für Objekte des BS2000 einzurichten. GUARDS stellt spezielle Behälter – die Guards – zur Verfügung, in denen die gewünschten Schutzmechanismen eingetragen werden. Entsprechend dieser Eintragungen werden die Objektzugriffe überwacht.

Zum besseren Verständnis von GUARDS, der in den Guards eingetragenen Schutzmechanismen und deren Überwachung wird zwischen folgenden Hauptaufgabenbereichen unterschieden:

1. Verwaltung der Guards hinsichtlich ihrer Funktion als Behälter
2. Verwaltung des Inhalts der Guards
3. Zuordnung der Guards zu ihren Schutzobjekten

Verwaltung der Guards hinsichtlich ihrer Funktion als Behälter

Diese Verwaltung ist unabhängig vom Inhalt und Zweck der einzelnen Guards. Zur Verwaltung beliebiger Guards stehen die Kommandos und Makros der GUARDS-Verwaltung zur Verfügung.

Näheres dazu finden Sie im Abschnitt „GUARDS-Verwaltung“ auf Seite 434.

Verwaltung des Inhalts der Guards

Abhängig von der Art des Inhalts, den ein Guard hat, sind verschiedene Instanzen für die Verwaltung dieses Inhalts zuständig. Welche Objekte mit diesen Guards auf welche Weise geschützt werden sollen, ist in diesem Zusammenhang nicht von Belang.

Es gibt folgende unterschiedliche Guardinhalte:

- Zugriffsbedingungen

  Hierbei handelt es sich um Bedingungen, die bestimmten Subjekttypen (Benutzer, Gruppen, alle übrigen) einen Zugriff generell gestatten, generell verbieten oder unter bestimmten Umständen gestatten. Es können beliebig viele Guards mit Zugriffsbedingungen angelegt werden.

  – Die GUARDS-Verwaltung verwaltet diese Guards unter dem Guardtyp STDAC.

  – Die Verwaltung der Dateninhalte dieser Guards übernimmt die Standardbedingungsverwaltung mit entsprechenden Kommandos und Makros.

  Näheres hierzu finden Sie im Abschnitt „Zugriffs- und Zugangsschutz“ auf Seite 438.

- Standardschutzregeln

  Diese Regeln bestimmen, welche Objekte standardmäßig mit bestimmten Schutzattributwerten versehen werden sollen. Es können beliebig viele Guards mit Standardschutzregeln angelegt werden.

  – Die GUARDS-Verwaltung verwaltet diese Guards unter dem Guardtyp DEFAULTP.

  – Die Verwaltung der Dateninhalte dieser Guards des Typs DEFAULTP übernimmt die Standardschutzverwaltung mit entsprechenden Kommandos und Makros.

  Näheres hierzu finden Sie im Abschnitt „Standardschutz (Default protection)“ auf Seite 449.

- Schutzattribute

  Hier handelt es sich um die Festlegung besonderer Schutzattributwerte.

  Es können beliebig viele Guards mit Standardwerten für Schutzattribute angelegt werden.

  – Die GUARDS-Verwaltung verwaltet diese Guards unter dem Guardtyp DEFPATTR.

  – Die Verwaltung der Dateninhalte dieser Guards übernimmt die Standardschutzverwaltung mit entsprechenden Kommandos und Makros.

  Näheres hierzu finden Sie im Abschnitt „Festlegung der Schutzattribut-Standardwerte“ auf Seite 453.

- Benutzerkennungs- und Benutzergruppenlisten (nur für die Systemverwaltung)

  Hier können Festlegungen getroffen werden, die einer pubsetglobalen eindeutigen Objektnamenszuordnung dienen. Zum Beispiel kann die Festlegung: USER-ID=HUGO der pubsetglobal eindeutigen Identifizierung aller Objekte namens $HUGO.OBJ* dienen. Es können beliebig viele Guards mit Listen von Benutzerkennungen und Benutzergruppen angelegt werden.

  – Die GUARDS-Verwaltung verwaltet diese Guards unter dem Guardtyp DEFPUID.

  – Die Verwaltung der Dateninhalte dieser Guards übernimmt die Standardschutzverwaltung mit entsprechende Kommandos und Makros.

  Näheres hierzu finden Sie im Abschnitt „Festlegung der Benutzer- und Gruppenkennungen für Pfadnamen (nur für Systemverwaltung)“ auf Seite 461.

- Miteigentümerschutzregeln

  Hierbei handelt es sich um Regeln, die für bestimmte Subjekttypen (Benutzer, Gruppen, alle übrigen) festlegen, welche Objekte sie unter bestimmten Bedingungen mitverwalten dürfen. Es können beliebig viele Guards mit Miteigentümerschutzregeln angelegt werden.

  – Die GUARDS-Verwaltung verwaltet diese Guards unter dem Guardtyp COOWNERP.

  – Die Verwaltung der Dateninhalte dieser Guards übernimmt die Miteigentümerverwaltung mit entsprechende Kommandos und Makros.

  Näheres hierzu finden Sie im Abschnitt „Miteigentümerschutz (Co-owner protection)“ auf Seite 471.

Zuordnung der Guards zu ihren Schutzobjekten

Die Schutzmechanismen sind in den einzelnen Guards unabhängig von den zu schützenden Objekten festgelegt. Damit sie wirksam werden können, muss zusätzlich festgelegt werden, welche Guards zum Einsatz kommen und welche Aufgaben sie dabei übernehmen sollen. Es wird zwischen drei Arten unterschieden:

- Direkte Verknüpfung mit dem Schutzobjekt.

  Die Objektverwaltung, die einen GUARDS-Schutz für ihre Objekte anbietet, stellt spezielle Kommando- oder Schnittstellenoperanden zur Verfügung. Über diese werden die zu schützenden Objekte mit den Guards verknüpft, die die gewünschten Schutzmechanismen enthalten.

  Zum Beispiel bietet die Objektverwaltung DVS zum Schutz von DVS-Dateien im Kommando /CREATE-FILE den Operanden PROTECTION=(GUARDS=()) an, über den Guardnamen für den Lese-, Schreib- und Ausführschutz zugeordnet werden können.

  Näheres über die direkte Verknüpfung zwischen Guards und Schutzobjekt finden Sie im Abschnitt „Zugriffs- und Zugangsschutz“ auf Seite 438.

- Vergabe eines vorgeschriebenen Guardnamens.

  Ein Schutzmechanismus wird dadurch aktiviert, dass ein Guard mit einem fest vorgeschriebenen Namen existiert.

  Zum Beispiel werden Regeln über die Miteigentümerschaft bestimmter DVS-Dateien dadurch wirksam, dass sie in ein Guard mit dem Namen SYS.UCF eingetragen werden.

  Näheres über die Verwendung vorgeschriebener Guardnamen finden Sie in den Abschnitten „Standardschutz (Default protection)“ auf Seite 449 und „Miteigentümerschutz (Co-owner protection)“ auf Seite 471.

- Indirekte Verknüpfung mit dem Schutzobjekt.

  Guards, in denen Regeln für einen Schutzmechanismus eingetragen werden, enthalten einen Verweis auf ein weiteres Guard.

  Zum Beispiel können in einem Guard Regeln angegeben sein, die festlegen, welchen Objekten standardmäßig bestimmte Schutzattributwerte zugewiesen werden sollen. Diese Regeln verweisen auf ein weiteres Guard, in dem diese Attributwerte definiert sind.

  Näheres über die in indirekte Verknüpfung zwischen Guards und Schutzobjekt finden Sie im Abschnitt „Standardschutz (Default protection)“ auf Seite 449 und Abschnitt „Miteigentümerschutz (Co-owner protection)“ auf Seite 471.

Die folgende Tabelle zeigt, welche Objektverwaltungen für welche ihrer Objekte einen GUARDS-Schutz anbieten und welche Guardtypen dafür ausgewertet werden.

Objektverwaltung	**Objekt**	**Schutzmechanismus**			
		Zugriffs-schutz	**Zugangs-schutz**	**Stan-dard-schutz**	**Miteigen-tümer-schutz**
DVS (Dateiverwaltungs-system)	Dateien	STDAC		DEFAULTP DEFPATTR DEFPUID	COOWNERP STDAC
	Storage-Klassen	STDAC			
LMS (Library Management System)	Bibliothekselemente	STDAC			
	Bibliothek mit dem Schutzmechanismus Miteigentümerschutz				COOWNERP STDAC
HSMS (Hierarchisches Speicher Management System)	HSMS-Management-Klassen	STDAC			
JVS (Jobvariablen-system)	Jobvariablen	STDAC		DEFAULTP DEFPATTR DEFPUID	COOWNERP STDAC
FITC (Fast Intertask Communication)	Ports	STDAC			
SRPM (System Resources and Privileges Management)	Gruppenzuordnung		STDAC		
	Terminal-Sets		STDAC		
	Dialog-Zugang zu einer Benutzerkennung		STDAC		
	Batch-Zugang zu einer Benutzerkennung		STDAC		
	POSIX-Rlogin-Zugang zu einer Benutzerken-nung		STDAC		
	POSIX-Remote-Zugang zu einer Benutzerken-nung		STDAC		
	Netzdialog-Zugang zu einer Benutzerkennung		STDAC		

Tabelle 9: Objektverwaltungen und zugehörige Objekte

Die entsprechenden Verknüpfungsmechanismen sind in den folgenden Abschnitten beschrieben:

- „Zugangsschutz“ auf Seite 91 und die Unterabschnitte „Einschränkung des Zugangs über Terminal-Sets“ auf Seite 96 und „Zugangsschutz mit Guards“ auf Seite 104
- „Zugriffs- und Zugangsschutz“ auf Seite 438
- „Standardschutz (Default protection)“ auf Seite 449
- „Miteigentümerschutz (Co-owner protection)“ auf Seite 471

Die Bedeutung der Guardtypen finden Sie in der Tabelle „Guardtypen und ihre Bedeutung“ auf Seite 437.

Systemtechnisch ist die gesamte Schutzfunktionalität, die in einzelnen Guards spezifiziert werden kann, auf drei Subsysteme verteilt:

GUARDS	Dieses Subsystem beinhaltet die Verwaltung aller Guards in ihrer Funktion als Datenbehälter (GUARDS-Verwaltung) und die Verwaltung der Inhalte aller Guards des Typs STDAC (Standardbedingungsverwaltung).
GUARDDEF	Dieses Subsystem beinhaltet sowohl die Standardschutzverwaltung als auch die sie unterstützende Attribut- und Objektpfadverwaltung.
GUARDCOO	Dieses Subsystem beinhaltet die Miteigentümerschutzverwaltung.

Hinzu kommt das Dienstprogramm:

GUARDS-SAVE	ist ein Dienstprogramm, mit dem alle oder einzelne Guards gesichert werden können, indem sie aus dem aktuellen Guardskatalog selektiert und in eine Datei geschrieben werden. Umgekehrt können Guards restauriert werden, indem sie aus dieser Datei wieder in den aktuellen Guardskatalog eingespielt werden.

Diese Beschreibung ist wie folgt gegliedert:

- Die Beschreibung der GUARDS-Verwaltung finden Sie in den Abschnitten
  - „GUARDS-Verwaltung“ auf Seite 434
  - „GUARDS administrieren“ auf Seite 503
- Die einzelnen, in Guards spezifizierbaren Schutzmechanismen sind im Abschnitt „Schutzmechanismen von GUARDS im Überblick“ auf Seite 437 beschrieben, sowie in den Unterabschnitten
  - „Zugangsschutz“ auf Seite 91
  - „Zugriffs- und Zugangsschutz“ auf Seite 438
  - „Standardschutz (Default protection)“ auf Seite 449 und
  - „Miteigentümerschutz (Co-owner protection)“ auf Seite 471
- Hinweise zur Anwendung des Dienstprogramms GUARDS-SAVE finden Sie im Abschnitt „Dienstprogramm GUARDS-SAVE“ auf Seite 881.
- Bei der Beschreibung der GUARDS-Funktionen wird auf die GUARDS-Kommandos und -Makros bezug genommen.
  - Die Beschreibung der GUARDS-Kommandos finden Sie ab Seite 517.
  - Die GUARDS-Makros sind ab Seite 704 beschrieben.
  - Hinweise zur SDF-Metasyntax finden Sie im Handbuch „Kommandos“ [4].

5.1 GUARDS-Verwaltung

Ein Guard besteht aus einem Verwaltungsteil und einem Datenteil. Der Verwaltungsteil enthält Verwaltungsinformationen wie zum Beispiel den Typ des Guards. Der Datenteil enthält die Angaben über durchzuführende Schutzmaßnahmen wie zum Beispiel Zugriffsbedingung oder Miteigentümerschutzregeln.

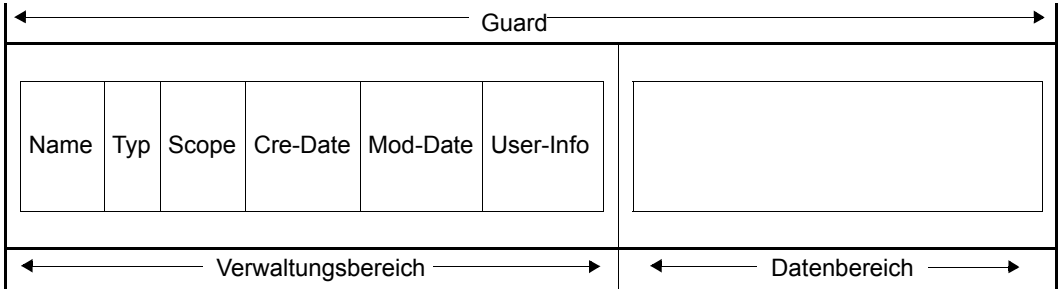
Die GUARDS-Verwaltung besitzt keine Kenntnis über Inhalt und semantische Bedeutung des Datenteils. Sie nimmt keinerlei Auswertung vor, die sich auf den Inhalt des Datenteils bezieht. Dieses ist Aufgabe der Standardbedingungs-, Standardschutz- und Miteigentümerschutzverwaltung, die die erforderlichen Kommandos dafür anbieten (Näheres ist in den nachfolgenden Kapiteln beschrieben).

Ein Benutzer, der ein Guard einrichtet, ist sein Eigentümer und darf es verwalten. Ein Guard kann jedoch so eingerichtet werden, dass es auch von anderen Benutzern zum Schutz ihrer Objekte verwendet werden kann. Benutzerkennungen, die das Privileg GUARD-ADMINISTRATION besitzen, sind Miteigentümer aller Guards im System. Sie dürfen diese deshalb wie der Eigentümer verwalten und ihren Inhalt modifizieren.

Die Guard-Verwaltung bietet zur Verwaltung der Guards als Behälter folgende Kommandos an:

CREATE-GUARD	Erzeugen eines Guards vom Typ UNDEF.
COPY-GUARD	Kopieren eines Guards beliebigen Typs, wobei der Typ unverändert bleibt.
DELETE-GUARD	Löschen eines Guards beliebigen Typs.
MODIFY-GUARD-ATTRIBUTES	Umbenennen eines Guards beliebigen Typs oder Modifizieren seiner Verwaltungsattribute.

Die folgende Grafik zeigt den Aufbau eines Guards, das über die zuvor genannten Kommandos verwaltet werden kann:



Bedeutung der Verwaltungsinformation:

Name: Frei wählbarer Name des Guards

Typ: Typ des Guards entsprechend seines Inhalts.

Scope: Angabe über den Benutzerkreis, der das Guard verwenden darf (USER-ID, GROUP-ID, HOST-SYSTEM).

Cre-Date: Datum der Erstellung des Guards.

Mod-Date: Datum der letzten Modifikation.

User-Info: Frei wählbare Zusatzinformation.

5.2 Rollen der Eigentümer von Objekten

Der Eigentümer eines Objekts kann bei dessen Bearbeitung zwei unterschiedliche Rollen annehmen:

Verwalten: Der Eigentümer verwaltet die Zugriffsvorschriften seines Objekts, indem er die Schutzattribute einstellt.
Diese Aktion ist ihm erlaubt, weil er der Eigentümer des Objekts ist.

Zugreifen: Der Eigentümer greift auf den Datenbereich seines Objekts zu.
Dabei unterliegt er allen durch seine Verwaltungsmaßnahmen festgelegten Zugriffsvorschriften.

Für einen Objekteigentümer, der **eigene Guards** zum Schutz seines Objekts verwendet, gilt:

Verwalten: Der Eigentümer verwaltet die Zugriffsvorschriften seines Objekts, das mit seinen eigenen Guards geschützt ist, indem er die Schutzattribute einstellt.
Diese Aktion ist ihm erlaubt, weil er der Eigentümer der Guards ist.

Zugreifen: Der Eigentümer greift auf den Datenbereich seines Objekts zu, das mit seinen eigenen Guards geschützt ist.
Dabei unterliegt er allen Zugriffsbedingungen, die er durch seine Verwaltungsmaßnahmen in seinen eigenen Guards festgelegt hat.

Für einen Objekteigentümer, der **fremde Guards** zum Schutz seines Objekts verwendet, gilt hingegen:

Verwalten: Der Eigentümer darf die Zugriffsvorschriften seines Objekts, das mit fremden Guards geschützt ist, **nicht** verwalten.
Diese Aktion ist ihm verboten, weil er nicht der Eigentümer der Guards ist.

Zugreifen: Der Eigentümer greift auf den Datenbereich seines Objekts zu, das mit fremden Guards geschützt ist.

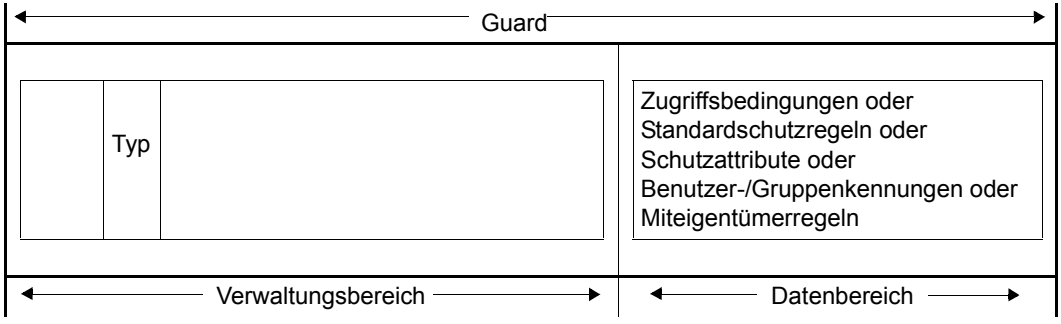
Bei dieser Aktion muss er die Erlaubnis haben, die fremden Guards zum Schutz seiner Objekte verwenden zu dürfen. Eine solche Erlaubnis kann aber nur ein Guardeigentümer über das Guardattribut SCOPE regeln.

Das heißt: Der Zugriff auf ein durch Guards geschütztes Objekt wird immer verweigert, wenn die Berechtigung zur Verwendung eines (fremden) Guards nicht erteilt ist, oder das Guard aus anderen Gründen nicht zugreifbar ist.

ACHTUNG!
Ob ein Guard zugreifbar ist oder verwendet werden darf, wird nicht bei der Verknüpfung eines Objekts mit einem Guard überprüft, sondern erst zum Zeitpunkt eines Objektzugriffs.

5.3 Schutzmechanismen von GUARDS im Überblick

Im Datenteil eines Guards sind die Informationen der unterschiedlichen Schutzmechanismen hinterlegt:



Abhängig vom Guardtyp im Verwaltungsbereich können im Datenbereich folgende Einträge enthalten sein:

Guardtyp	**Eintrag**
UNDEF	Leerer Behälter, der noch keine Schutzmechanismen enthält.
STDAC	Zugriffsbedingungen. Diese bestehen aus Datum, Uhrzeit, Wochentag, Privileg der Zugreifertask und Name eines zugreifenden Programms, die spezifizierte Subjekte (USER, GROUP, OTHERS, ALL-USERS) erfüllen müssen.
DEFAULTP	Regeln für den Standardschutz. Diese bestehen aus Regelname, Objektname, Name eines Attributguards und optional nur für den Systemverwalter Name eines Benutzerkennungsguards.
DEFPATTR	Schutzattribute. Sie bestehen aus ACCESS, USER-ACCESS, BASIC-ACL, GUARDS, READ-/WRITE-/EXEC-PASSWORD, DESTROY-BY-DELETE, SPACE-RELEASE-LOCK, EXPIRATION-DATE und FREE-FOR-DELETION.
DEFPUID	Benutzer- und Benutzergruppenkennungen für die eindeutige Objektnamenszuordnungen beim pubsetglobalen Standardschutz (nur für die Systemverwaltung).
COOWNERP	Regeln für den Miteigentümerschutz. Sie bestehen aus Regelname, Objektname, Name eines Bedingungsguards und einer Angabe bezüglich der speziellen Zugriffsberechtigung des Benutzers TSOS.

Tabelle 10: Guardtypen und ihre Bedeutung

5.4 Zugriffs- und Zugangsschutz

Die folgenden Objektverwaltungen unterstützen einen **Zugriffsschutz** für ihre Objekte:

– DVS für Dateien und Storage-Klassen

– LMS für Bibliothekselemente

– JVS für Jobvariablen

– HSMS für HSMS-Management-Klassen und

– FITC für FITC-Ports.

SRPM als Objektverwaltung bietet einen **Zugangsschutz** für Terminal-Sets, Benutzerkennungen und Gruppenzuordnungen sowie für POSIX-Zugänge (POSIX-Rlogin, POSIX-Remote).

Verantwortlich für die Zugriffs- und Zugangskontrolle ist die Standardbedingungsverwaltung als Bestandteil des Subsystems GUARDS. Sie stellt eine von den Objektverwaltungen unabhängige Instanz dar, mit der Zugriffsbedingungen definiert, verwaltet und ausgewertet werden können. Die Zugriffsbedingungen werden in den von der GUARDS-Verwaltung verwalteten Guards hinterlegt.

Einrichten und Verwalten des GUARDS-Schutzes

Um den Schutz mit GUARDS zu ermöglichen, müssen folgende Vorkehrungen getroffen werden:

- Einrichtung von Guards,
  Hierzu stehen die Kommandos der GUARDS-Verwaltung zur Verfügung (siehe Abschnitt „GUARDS-Verwaltung“ auf Seite 434)
- Definition von Zugriffsbedingungen
  Zugriffsbedingungen können sein:
  – Eine Liste von Benutzern denen der Zugriff gestattet ist,
  – Privilegien, die ein Benutzer für einen Zugriff besitzen muss,
  – Zeitintervalle, in denen ein Zugriff erlaubt oder verboten ist, oder
  – bestimmte Systembedingungen.

  Weitere Hinweise zu diesem Themenkreis finden Sie ab Seite 443.
- Verknüpfung der Guards mit den zu schützenden Objekten.

  Weitere Hinweise zu diesem Themenkreis finden Sie ab Seite 440.

5.4.1 Zugriffs- und Zugangsschutz einrichten

Die Einrichtung des Zugriffs-/Zugangschutzes umfasst drei Schritte:

1. Einrichten von Guards (siehe Seite 434)
2. Die Festlegung der Zugriffsbedingungen
3. Die Verknüpfung von Guards mit den zu schützenden Objekten (siehe Seite 440).

Festlegen der Zugriffsbedingungen

Zugriffsbedingungen werden mit dem Kommando /ADD-ACCESS-CONDITIONS festgelegt, mit dem Kommando /MODIFY-ACCESS-CONDITIONS geändert, mit dem Kommando /SHOW-ACCESS-CONDITIONS angezeigt und mit dem Kommando /REMOVE-ACCESS-CONDITIONS wieder entfernt.

Mit dem Kommando /SHOW-ACCESS-ADMISSION erhält ein Benutzer Auskunft über die Bedingungen, die er erfüllen muss, damit ihm der Zugriff auf ein bestimmtes Objekt erlaubt ist.

Die Zugriffsbedingungen können unter folgenden Gesichtspunkten festgelegt werden:

- Ein Zugriff soll generell gestattet oder verboten sein.
- Ein Zugriff soll nur unter bestimmten Umständen gestattet sein:
  - Zeitraum (Uhrzeit, Datum, Wochentag) – es kann eine Liste von zulässigen Zeiträumen oder der Ausschluss bestimmter Zeiträume angegeben werden. Die Zeiträume sind untereinander mit dem logischen ODER verknüpft.
  - Privileg (nur mit bestimmten Privilegien darf der Zugriff erfolgen) – es kann eine Liste von zulässigen Privilegien oder der Ausschluss bestimmter Privilegien angegeben werden. Die Privilegien in der Liste sind mit dem logischen ODER verknüpft.
  - Programm (der Zugriff darf nur über ein bestimmtes Programm erfolgen, wobei geprüft wird, ob das Programm geladen ist und auch die Kontrolle übernommen hat). Die Programmnamen in der Liste sind mit dem logischen ODER verknüpft.

Diese Zugriffsbedingungen können für verschiedene Subjekttypen (USER/GROUP/OTHERS/ALL-USERS) in unterschiedlichen Ausprägungen festgelegt werden. Weitergehende Erläuterungen zur Auswertelogik für die Subjekttypen siehe Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

Verknüpfen mit den zu schützenden Objekten

Um ein Objekt mit Hilfe von Guards vor unberechtigtem Zugriff/Zugang zu schützen, muss eine Verknüpfung zwischen dem zu schützenden Objekt und den Guards hergestellt werden, in denen die entsprechenden Zugriffsbedingungen definiert sind. Das bedeutet: der Objekteigentümer gibt der für sein Objekt zuständigen Objektverwaltung bekannt, in welchen Guards die Zugriffsbedingungen hinterlegt sind. Die Kommandos und Programmschnittstellen, die von den verschiedenen Objektverwaltungen zur Verknüpfung ihrer Objekte mit Guards angeboten werden, sind in den Abschnitten „Schutz von ...“ ab Seite 441 dargestellt.

Da eine Verknüpfung nur den jeweiligen Objektverwaltungen bekannt ist, nicht aber in den Guards hinterlegt wird, kann ein Guard zum Schutz mehrerer unterschiedlicher Objekttypen (wie Datei, Bibliothekselement, Jobvariable usw.) verwendet werden.

Eine Verknüpfung kann nur vom Eigentümer oder Miteigentümer des Objekts hergestellt oder gelöst werden, nicht aber vom Eigentümer des Guards (sofern die beiden Eigentümer nicht identisch sind).

ACHTUNG!
Da ein Objekt und die mit ihm verknüpften Guards verschiedene Eigentümer haben können, ist besonders sorgfältig darauf zu achten, dass beim Löschen von Guards auch deren Verknüpfungen mit ihren Schutzobjekten von den jeweiligen Objekteigentümern aufgelöst werden. Zum Beispiel bei einer Datei durch:
`/MODIFY-FILE-ATTRIBUTES <filename>, PROTECTION=(GUARDS=*NONE).`

Solange eine Verknüpfung mit einem bereits gelöschten Guard nicht gelöst ist, ist ein Zugriff auf das verknüpfte Objekt auch für den Objekteigentümer nicht möglich.

Schutz von Dateien, Jobvariablen und Bibliothekselementen

Bei Verwendung von Guards werden von DVS, JVS und LMS nur Zugriffe gestattet, die explizit erlaubt sind. Im Gegensatz zu SHARE/ACCESS schließen Guards beim Schreibrecht nicht auch das Leserecht ein.

Für Dateien wird der zum Schutz zu verwendende Guard-Name mit dem Operanden PROTECTION der Kommandos /CREATE-FILE bzw. /MODIFY-FILE-ATTRIBUTES festgelegt. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Dateien finden Sie im Handbuch „Einführung in das DVS“ [6].

Für Bibliothekselemente wird der zum Schutz zu verwendende Guard-Name mit den LMS-Anweisungen //CREATE-ELEMENT bzw. //MODIFY-ELEMENT-PROTECTION festgelegt. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Bibliothekselemente finden Sie im Handbuch „LMS“ [23].

Für Jobvariablen wird der zum Schutz zu verwendende Guard-Name mit dem Operanden PROTECTION der Kommandos /CREATE-JV bzw. /MODIFY-JV-ATTRIBUTES festgelegt. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Jobvariablen finden Sie im Handbuch „JV“ [32].

Schutz von Storage-Klassen

Für Storage-Klassen wird der zum Schutz zu verwendende Guard-Name mit dem Operanden PROTECTION der Kommandos /CREATE-STORAGE-CLASS bzw. /MODIFY-STORAGE-CLASS festgelegt. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Storage-Klassen finden Sie im Handbuch „SMS“ [33].

Schutz von HSMS-Management-Klassen

Für HSMS-Management-Klassen wird der zum Schutz zu verwendende Guard-Name mit dem Operanden PROTECTION der HSMS-Anweisungen //CREATE-MANAGEMENT-CLASS bzw. //MODIFY-MANAGEMENT-CLASS festgelegt. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für HSMS-Management-Klassen finden Sie im Handbuch „HSMS“ [13].

Gruppenzuordnung

Beim Zugriff auf Dateien und Jobvariablen, die durch BACL geschützt sind, können bestimmte Benutzer so behandelt werden, als ob sie Gruppenmitglieder wären. Diese Gruppenzuordnung wird im Operanden BASIC-ACL-ACCESS der Kommandos /ADD-USER-GROUP (Seite 132) und /MODIFY-USER-GROUP (Seite 212) festgelegt.

Schutz von Zugangsklassen

Der Zugang zu einer Benutzerkennung kann je nach Zugangsart durch ein separates Guard geregelt werden. Die Zuordnung der Guards erfolgt mit den folgenden Operanden der Kommandos /SET- und /MODIFY-LOGON-PROTECTION (siehe Seiten 241 und 172):

– DIALOG-ACCESS
– BATCH-ACCESS
– POSIX-RLOGIN-ACCESS
– POSIX-REMOTE-ACCESS
– NET-DIALOG-ACCESS

Insbesondere können persönliche Benutzerkennungen (siehe Abschnitt „Persönliche Identifizierung“ auf Seite 105) durch Guards geschützt werden.

Zugangsschutz mit Terminal-Sets

Beim Zugangsschutz mit Terminal-Sets kann der Zugang zusätzlich über ein Guard geregelt werden. Dieses wird mit dem Operanden GUARD-NAME der Kommandos /CREATE-TERMINAL-SET (Seite 156) bzw. /MODIFY-TERMINAL-SET (Seite 209) festgelegt.

5.4.2 Zugriffsbedingungen definieren

Die Definition von Zugriffsbedingungen umfasst zwei Schritte:

1. Die Festlegung der Subjekttypen, für die die Bedingungen gelten sollen. Subjekttypen sind USER, GROUP, OTHERS und das GUARDS-Pseudosubjekt ALL-USERS
2. Die Definition der Zugriffsbedingungen

Um Zugriffsbedingungen optimal formulieren zu können, ist die Kenntnis der Logik der Bedingungsauswertung unerläßlich. Für die Bedingungsauswertung ordnet GUARDS die Bedingungen und deren Auswertung nach Subjekttypen. Die Auswertung der Subjekttypen USER, GROUP und OTHERS wird abgebrochen, sobald der erste Treffer erzielt wurde. Die Auswertung kann immer nur eines von zwei Ergebnissen liefern: WAHR (Bedingungen sind erfüllt) oder FALSCH (Bedingungen sind nicht erfüllt).

Einträge für die Subjekttypen USER, GROUP, OTHERS und ALL-USERS sind optional. Wurden überhaupt keine Bedingungen definiert, lautet das Ergebnis der Auswertung immer, dass die Bedingungen nicht erfüllt sind. Ein leeres Guard existiert z.B. in der Zeit zwischen seiner Erzeugung mit dem Kommando CREATE-GUARD und der Definition der ersten Bedingung mit /ADD-ACCESS-CONDITIONS oder nachdem alle Definitionen mit /REMOVE-ACCESS-CONDITIONS gelöscht wurden.

Reihenfolge der Auswertung der Subjekttypen:

USER die Bedingungen von USER werden als Erstes ausgewertet. Bei USER sind die Bedingungen hinterlegt, die explizit für eine Kennung (userid) gelten sollen. Bei der logischen Auswertung werden zuerst die Einträge für USER durchsucht, ob für die zur Prüfung anstehende Kennung ein Eintrag vorhanden ist. Wird eine Übereinstimmung gefunden, werden die für diese Kennung hinterlegten Bedingungen ausgewertet.

Lautet das Ergebnis der Auswertung WAHR, wird gleich mit der Auswertung der Bedingungen des Subjekttyps ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung FALSCH, wird die Auswertung abgebrochen, und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

GROUP spricht die Bedingungen an, die explizit für eine Benutzergruppe gelten sollen. Bei der logischen Auswertung werden als Zweites die Einträge für GROUP durchsucht, ob für die Gruppe, zu der die zur Prüfung anstehende Kennung gehört, ein Eintrag vorhanden ist. Wird eine Übereinstimmung gefunden, werden die für diese Gruppe hinterlegten Bedingungen ausgewertet.

Lautet das Ergebnis der Auswertung WAHR, wird gleich mit der Auswertung der Bedingungen des Subjekttyps ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung FALSCH, wird die Auswertung abgebrochen, und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

OTHERS spricht die Bedingungen an, die für alle Benutzer gelten sollen, die nicht durch Einträge für USER oder GROUP erfasst worden sind.

Lautet das Ergebnis der Auswertung WAHR, wird mit der Auswertung der Bedingungen von ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung FALSCH, wird die Auswertung abgebrochen und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

Sind in einem Guard weder Einträge für den Subjekttyp USER noch für GROUP oder OTHERS vorhanden, lautet das Ergebnis der Auswertung immer FALSCH.

ALL-USERS ist ein Pseudo-Subjekttyp, über den Zusatzbedingungen hinterlegt werden können, die nur dann ausgewertet werden, wenn die vorangegangenen Prüfungen für USER, GROUP und OTHERS zum Ergebnis WAHR geführt haben.

Auf diese Weise können Zugriffsbedingungen in ein Guard eintragen werden, die für alle im Guard festgelegten Subjekttypen und Subjekte gelten, ohne dass sie dafür bei jedem einzelnen Subjekttyp selber festgemacht werden müssen.

Beispiel

In einem Guard wurden unter dem Subjekttyp USER für die Benutzerkennungen PETER, PAUL und MARY und unter dem Subjekttyp GROUP für die Benutzergruppe TEAM festgelegt, dass ein Zugriff erlaubt ist. Über den Subjekttyp OTHERS wird vereinbart, dass "alle Anderen" keine Zugriffsberechtigung haben.

```
%   User   PAUL     has ADMISSION
%   User   PETER    has ADMISSION
%   User   MARY     has ADMISSION
%   Group  TEAM     has ADMISSION
%   Others          has NO ADMISSION
```

Kurzfristig soll der Zugriff auch für die unter USER und GROUP festgelegten Subjekte (PETER, PAUL, MARY, TEAM) verboten werden. Um nun nicht alle betroffenen Zugriffsbedingungen in ADMISSION=*NO abändern zu müssen, wird der Pseudo-Subjekttyp ALL-USERS verwendet, mit dem die Zugriffsbedingung ADMISSION=*NO nur einmal festgelegt werden muss und trotzdem für "Alle" gilt:

```
%   User   PAUL     has ADMISSION
%   User   PETER    has ADMISSION
%   User   MARY     has ADMISSION
%   Group  TEAM     has ADMISSION
%   Others          has NO ADMISSION
%   Alluser         has NO ADMISSION
```

Greift z.B. Subjekt MARY zu, wird nach Überwindung der ersten Schutzhürde (WAHR) die zusätzlichen ALL-USERS-Prüfung durchlaufen, die das Prüfergebnis FALSCH liefert. Greift ein Subjekt zu, das nicht unter die Kategorien USER und GROUP fällt, wird die OTHERS-Prüfung durchlaufen, die das Ergebnis FALSE liefert. In diesem Fall wird die Prüfung abgebrochen, ohne dass die ALL-USERS-Prüfung durchlaufen wird.

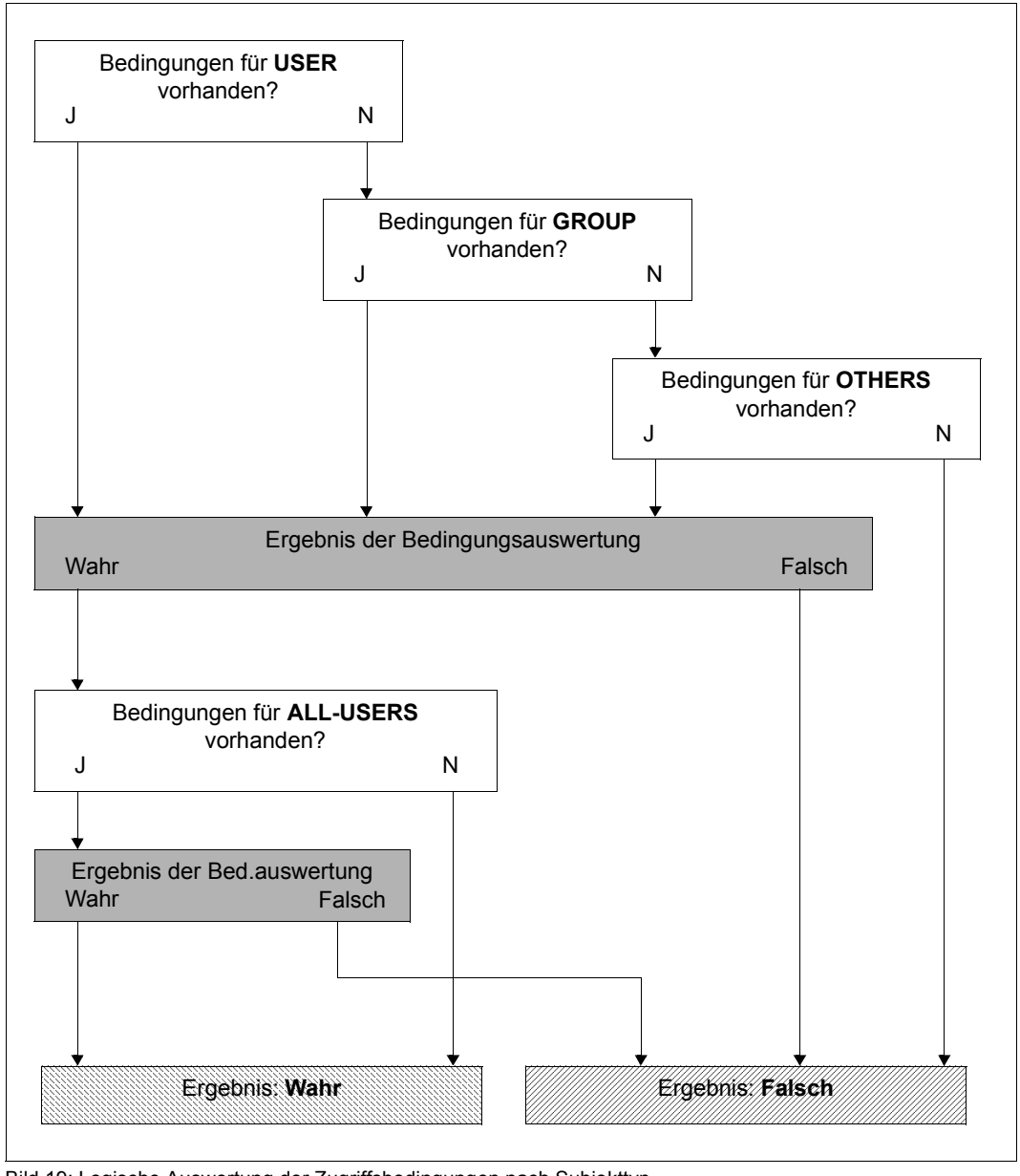


Bild 19: Logische Auswertung der Zugriffsbedingungen nach Subjekttyp

Hinweis

Die für den Subjekttyp USER, GROUP oder OTHERS festgelegten Zugriffsbedingungen (Bedingung a) und diejenigen für Pseudo-Subjekttyp ALL-USERS (Bedingung b) sind durch logisches UND miteinander verknüpft. Das bedeutet, ein Zugriff ist nur dann erlaubt, wenn sowohl Bedingung a, als auch Bedingung b zutrifft. GUARDS überprüft bei der Definition von Zugriffsbedingungen jedoch nicht, ob widersprüchliche Bedingungen vorliegen. Daher muss der Eigentümer eines Guards sorgfältig prüfen, ob Unstimmigkeiten zwischen den Zugriffsbedingungen für die Subjekttypen USER, GROUP oder OTHERS einerseits und denen für den Pseudo-Subjekttyp ALL-USERS andererseits existieren. Diese können dazu führen, dass ein Zugriff, der eigentlich erlaubt sein sollte, abgewiesen wird.

Beispiel

Die Zugriffsbedingung für den Subjekttyp USER legt einen Zeitraum von 08:00 bis 13:00 fest, die Bedingung für ALL-USERS bestimmt dagegen einen Zeitraum von 12:00 bis 18:00. Der Zugriff für einen in der Bedingung für USER festgelegten Benutzer ist nur erlaubt, wenn beide Bedingungen zutreffen. Dies ist in diesem Beispiel von 12:00 bis 13:00 der Fall. Ein Zugriff dieses Benutzers um 9:00 würde dagegen abgewiesen, obwohl die Bedingung für den Subjekttyp USER erfüllt ist.

Dieses Verhalten kann allerdings auch erwünscht sein, z.B. um ein Objekt für einen bestimmten Zeitraum generell zu sperren. Daher liegt es in der Verantwortung des Eigentümers eines Guards, zu beurteilen, ob unerwünschte Widersprüche vorliegen oder nicht.

Beispiel für die Verwendung von ALL-USERS

Auf eine Datei soll nur über das Programm EDT zugegriffen werden dürfen.
Die Bedingung „Zugriff nur über das Programm EDT“ wird nur für den Pseudo-Subjekttyp ALL-USERS festgelegt.

Definition für USER:

```
/add-access-conditions guard-name=guardexa, -
/           subjects=*user(user-identification=edtuser), -
/           admission=*yes
```

Definition für GROUP:

```
/add-access-conditions guard-name=guardexa, -
/           subjects=*group(group-identification=edtgroup), -
/            admission=*yes
```

Definition für OTHERS:

```
/add-access-conditions guard-name=guardexa, -
/                      subjects=*others, -
/                      admission=*yes
```

Definition für ALL-USERS:

```
/add-access-conditions guard-name=guardexa,-
/                    subjects=*all-users, -
/                      admission=*parameters(program=$edt)
```

Obwohl weder für USER, noch für GROUP oder OTHERS die Bedingung „Zugriff nur über das Programm EDT“ festgelegt ist, wird der Zugriff wunschgemäß über die für ALL-USERS eingetragene Bedingung geregelt.

Zusätzlich soll dem Benutzer EDTUSER der Dateizugriff über das Programm SORT erlaubt sein:

```
/modify-access-conditions guard-name=guardexa, -
/              subjects=*user(user-identification=edtuser), -
/               admission=*parameters(program=($edt,$sort))
```

Für den Benutzer unter der Kennung EDTUSER sind die Bedingungen weiterhin WAHR, wenn er mit dem Programm EDT auf die mit Hilfe von GUARDS geschützte Datei zugreift. Wenn er jedoch einen Zugriff auf die Datei mit dem Programm $SORT versucht, wird die Bedingungsauswertung durch GUARDS als Prüfergebnis FALSCH liefern, da die Zugriffsbedingung für ALL-USERS einen Zugriff nur über das Programm $EDT erlaubt. GUARDS überprüft die Bedingungen in einem Guard nicht auf Folgerichtigkeit. Der Eigentümer des Guards muss selbst beurteilen, ob Unstimmigkeiten dieser Art gewollt sind oder nicht.

5.4.3 Arbeiten mit Objekten, die mit Guards geschützt werden

Der Zugriffschutzmechanismus über Guards wird explizit vom Eigentümer eines Objekts über Kommandos oder Programmschnittstellen aktiviert oder deaktiviert.

Neben dem Schutzmechanismus über Bedingungsguards (Guardtyp STDAC) gibt es immer folgenden zusätzlichen Zugriffsschutz:

– Kennwörter (WRITE-PASSWORD, READ-PASSWORD, EXEC-PASSWORD)
  Schreibende oder lesende Zugriffe auf eine Datei oder Jobvariable sowie ausführende Zugriffe auf eine Datei sind nur nach Eingabe des entsprechenden Kennworts erlaubt.

– Schutzfrist (EXPIRATION-DATE)
  Innerhalb einer festgelegten Zeitspanne ist es nicht erlaubt eine Datei oder Jobvariable zu ändern oder zu löschen.

5.5 Standardschutz (Default protection)

Mit dem Standardschutz können pubsetglobal und benutzerspezifisch Schutzattribut-Standardwerte voreingestellt werden, die von den herkömmlichen System-Standardwerten abweichen. Pubsetglobale Voreinstellungen können nur von Systemverwalter durchgeführt werden. Benutzerspezifische Standardwerte kann jeder Benutzer für seine Objekte unter seiner Benutzerkennung selber vereinbaren. Objekte, für die über den Standardschutz neue Standardwerte festgelegt werden können, sind Dateien und Jobvariablen.

Neu festgelegte Standardwerte werden in Form von Regeln mit den Namen der Objekte verknüpft, für die sie gelten sollen. Die Objektmenge kann dabei mit Hilfe von Musterzeichen umschrieben werden.

Die Regeln werden sessionübergreifend in Regelbehältern (Guards des Typs DEFAULTP) gespeichert. Ein Anwender kann unter seiner Kennung beliebig viele solcher Regelbehälter erstellen. Entspricht der Name eines Regelbehälters einer ganz bestimmten Namenskonvention (z.B. SYS.UDF), gilt er als aktiv und wird bei anfallenden Standardwertzuordnungen verwendet (z.B. bei Ausführung des Kommandos /CREATE-FILE FILE-NAME=FILE). Näheres ist dem Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458 zu entnehmen.

Hierarchie bei der Vergabe von Standardwerten

Anwender können zu jedem Zeitpunkt einige oder alle Schutzattribute explizit selber vergeben.

Beispiel

```
/CREATE-FILE FILE-NAME=TEST, USER-ACCESS=*ALL-USERS
```

Müssen Schutzattribute mit Standardwerten versorgt werden, weil nicht alle Schutzattribute explizit angegeben wurden, wird ein **aktiver benutzerspezifischer** Regelbehälter (z.B. SYS.UDF) herangezogen. Bleiben bestimmte Schutzattribute weiterhin unversorgt, wird ein aktiver pubsetglobaler Regelbehälter (z.B. SYS.PDF) herangezogen. Schutzattribute, für die nach dieser Hierarchiestufe immer noch keine Standardwerte gefunden wurden, werden mit den herkömmlichen System-Standardwerten vorbesetzt.

Schutzattribute

Die folgende Tabelle zeigt, welche Attribute über den Standardschutz voreingestellt werden können. Die Spalten „Attributbereich ...“ geben an, wann diese Attribute wirksam werden. Dabei bedeutet:

– *CREATE-OBJECT: Der Attributsatz wird einer Datei oder Jobvariablen standardmäßig bei der Erstellung zugewiesen (Kommandos /CREATE-FILE, /CREATE-FILE-GROUP oder /CREATE-JV).

– *MODIFY-OBJECT-ATTR: Dieser Attributsatz kann einer bereits eingerichteten Datei zugewiesen werden. Um das zu veranlassen muss das Kommandos /MODIFY-FILE-ATTRIBUTES oder /MODIFY-FILE-GROUP-ATTRIBUTES mit der Angabe PROTECTION-ATTR=*BY-DEF-PROT-OR-STD) aufgerufen werden.

Schutzattribut	DMS-Objekte (Dateien)		JV-Objekte (Jobvariablen)
	Attributbereich *CREATE-OBJECT	Attributbereich *MODIFY-OBJECT-ATTR	Attributbereich *CREATE-OBJECT
ACCESS	+	+	+
USER-ACCESS	+	+	+
BASIC-ACL	+	+	+
GUARDS	+	+	+
WRITE-PASSWORD	+	+	+
READ-PASSWORD	+	+	+
EXEC-PASSWORD	+	+	-
DESTROY-BY-DELETE	+	+	-
SPACE-RELEASE-LOCK	+	+	-
EXPIRATION-DATE	-	+	-
FREE-FOR-DELETION	-	+	-
Bedeutung der Symbole: + wird unterstützt - wird nicht unterstützt			

Temporäre Dateien und Jobvariablen

Für temporäre Dateien werden nur die beiden Dateiattribute DESTROY-BY-DELETE und SPACE-RELEASE-LOCK für den Standardschutz verwendet. Alle anderen Voreinstellungen werden vom DMS ignoriert.
Für temporäre Jobvariablen werden alle Voreinstellungen vom JVS ignoriert.

5.5.1 Anwendungskonzept

Grundlage für die Einführung einer sinnvollen Standardschutz-Einstellung bildet das Anwendungskonzept. Der Anwender ist diejenige Instanz, die sowohl konzeptionell als auch manuell festlegen muss, für welche Dateien welche Schutzattribut-Standardwerte gelten sollen.

Für die Spezifizierung einer benutzerspezifischen Standard-Schutzeinstellung sind zwei Arbeitsschritte notwendig:

– Festlegen der Schutzattribut-Standardwerte in Attributguards (Guardtyp DEFPATTR).

– Verknüpfen der festgelegten Schutzattribut-Standardwerte mit den Objektnamen, für die die Schutzattribut-Standardwerte gelten sollen. Die Verknüpfung muss in Form von Regeln in Guards des Typs DEFAULTP durchgeführt werden. Guards dieses Typs werden Regelbehälter genannt.

Für die Spezifizierung einer pubsetglobalen Standard-Schutzeinstellung durch die Systemverwaltung ist optional ein weiterer Arbeitsschritt notwendig:

– Festlegen von Benutzer- und Gruppenkennungen, die zur Vervollständigung von Objektpfadnamen auf einem Pubset herangezogen werden (Guardtyp DEFPUID). Damit erhält die Systemverwaltung die Möglichkeit, die Standardwertvergabe auf solche Objekte einzuschränken, die unter den angegebenen Kennungen angelegt werden.

  Dieser Arbeitsschritt kann entfallen, wenn die Objekte nicht anhand einer Benutzerkennung im Pfadnamen unterschieden werden müssen.

Beispiele für eine Konzeptgrundlage

Beispiel 1

Ein Anwender möchte für Dateien, die unter seiner Benutzerkennung angelegt werden, folgende Standardschutzattribute vereinbaren:

a) Bei allen Dateien, deren Name mit ’PUBLIC.’ beginnt, soll das Attribut USER-ACCESS standardmäßig auf *ALL-USERS gesetzt werden.

b) Alle Dateien, deren Name mit ’SCRATCH.*’ beginnt, sollen standardmäßig mit einer BACL geschützt werden.

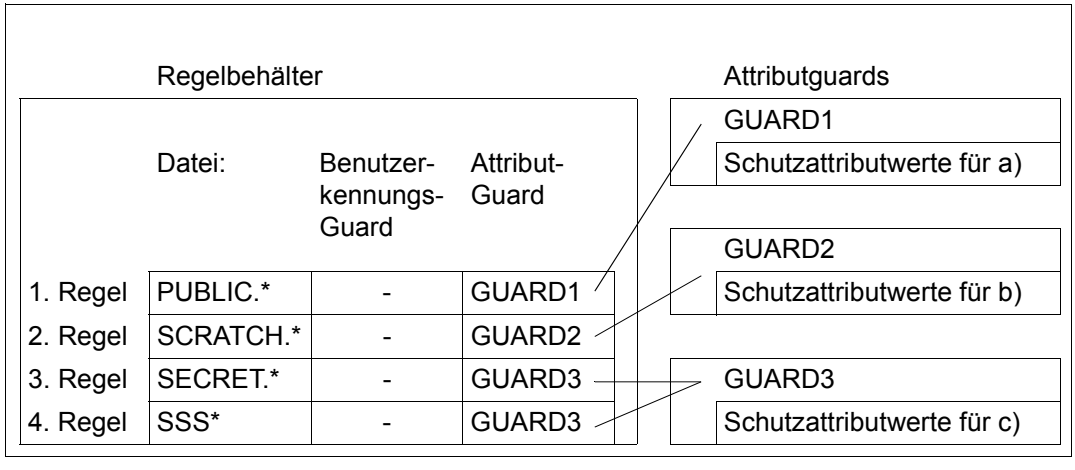
c) Alle Dateien, deren Name mit ’SECRET.’ oder mit ’SSS’ beginnt, sollen standardmäßig mit einem Guard geschützt werden.

Unter diesen Voraussetzungen benötigt der Anwender drei Attributguards, in denen er die unter a) bis c) angegebenen Schutzattribute definiert. Zusätzlich muss er einen Regelbehälter anlegen. Die Regeln in diesem Regelbehälter bestehen aus folgenden Teilen:

1. Name der Datei oder der Dateien, für die Standardschutzattribute gelten sollen.
2. Verweis auf ein Attributguard, das die gewünschten Standardschutzattribute für den genannten Dateinamensraum enthält.
3. Nur für die Systemverwaltung bei einer pubsetweiten Standardschutzmaßnahme

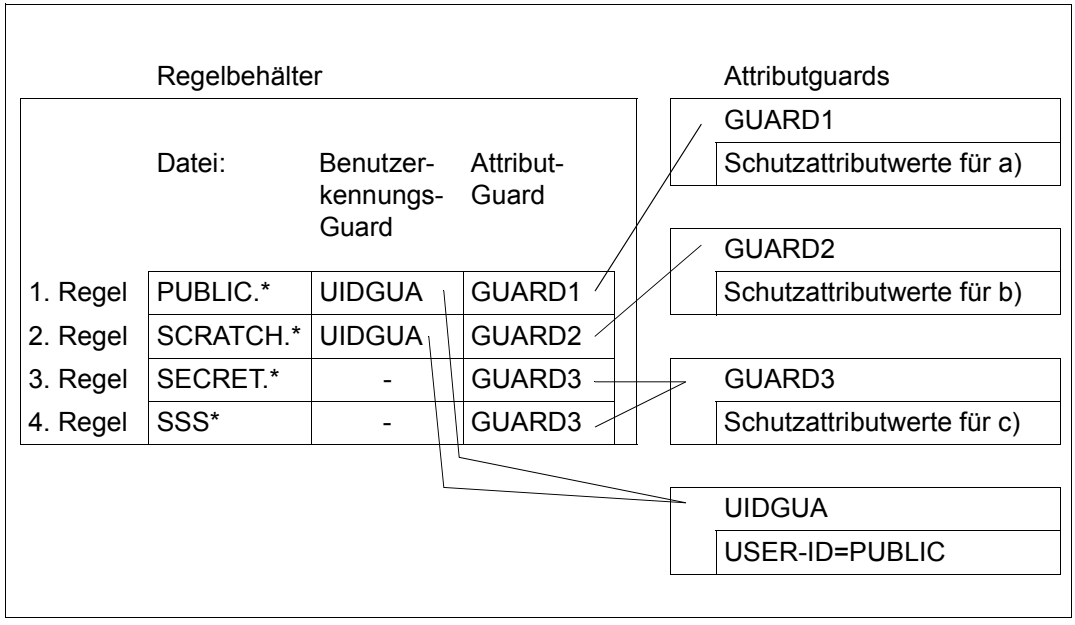
   Verweis auf ein Guard mit einer Liste von Benutzer- oder Gruppenkennungen zur eindeutigen pubsetweiten Identifizierung von Dateinamen.

Die Punkte a) und b) lassen sich jeweils in einer Regel beschreiben, während für Punkt c) zwei Regeln verwendet werden. Insgesamt ergibt sich folgendes Bild:



Beispiel 2 (für die Systemverwaltung)

Die Systemverwaltung möchte pubsetglobal dieselben Vorgaben machen wie der Anwender in Beispiel 1. Allerdings sollen die Schutzattribute aus a) und b) nur dann gelten, wenn die Dateien unter der Benutzerkennung PUBLIC angelegt werden. Der dazu erforderliche Regelbehälter und die benötigten Guards sind in folgender Grafik dargestellt:



5.5.2 Festlegung der Schutzattribut-Standardwerte

Schutzattribut-Standardwerte werden in Attributguards (Guards des Typs DEFPATTR) spezifiziert und sitzungsübergreifend gespeichert.

Die Festlegung der Schutzattribut-Standardwerte erfolgt in zwei Schritten:

1. Einrichten von Guards (siehe Seite 434).
2. Eintragen der Schutzattribut-Standardwerte in die Guards

Ein Anwender kann unter seiner Benutzerkennung beliebig viele Attributguards unterschiedlichen Namens erstellen, die jeweils einen Satz Schutzattribut-Standardwerte enthalten.

Eintragen der Schutzattribut-Standardwerte

Zur Bearbeitung von Attributguards stehen folgende Kommandos zur Verfügung. Diese Kommandos sind nicht RFA-fähig:

ADD-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute eintragen
MODIFY-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute ändern
SHOW-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute anzeigen

Außerdem stehen für die Verwaltung von Attributguards die allgemeinen GUARDS-Verwaltungskommandos zur Verfügung (siehe Seite 434).

Für folgende Schutzattribute können Standardwerte voreingestellt werden:

Schutzattribut:	**Bedeutung:**	**Vorrang hat:**
GUARDS	Zugriffsschutz wird über benennbare Guards des Typs STDAC gesteuert.	
BASIC-ACL	Zugriffsschutz wird über Basic Access-Control-Lists (BACL) gesteuert, für die spezielle Einstellungen möglich sind.	GUARDS
USER-ACCESS	Art der Verfügbarkeit, zum Beispiel nur für den Eigentümer oder für alle Benutzer im System.	GUARDS BASIC-ACL
ACCESS	Art des Zugriffs, zum Beispiel lesend oder schreibend.	GUARDS BASIC-ACL
WRITE-PASSWORD	Festlegung eines Schreib-Kennwortes.	
READ-PASSWORD	Festlegung eines Lese-Kennwortes.	
EXEC-PASSWORD	Festlegung eines Ausführ-Kennwortes.	
DESTROY-BY-DELETE	Daten werden beim Löschen mit binär Null überschrieben.	
SPACE-RELEASE-LOCK	Regelung über die Freigabe von Speicherplatz.	
EXPIRATION-DATE (RETENTION-PERIOD)	Regelung einer Schutzfrist, während der die Datei weder verändert noch gelöscht werden darf.	
FREE-FOR-DELETION	Regelung über das Löschen der Datei ab einem bestimmten Zeitpunkt ohne die Berücksichtigung jeglicher Schutzattribute.	

5.5.3 Festlegung der Standardschutzregeln

Der Standardschutz wird in Form von Regeln festgelegt, die in Regelbehältern (Guards des Typs DEFAULTP) sitzungsübergreifend gespeichert werden.

Ein Anwender kann unter seiner Benutzerkennung beliebig viele Regelbehälter unterschiedlichen Namens erstellen, wobei jeder Regelbehälter mehrere Standardschutzregeln für Dateien seiner Benutzerkennung enthalten kann.

Regelbehälter werden nur dann für die Vergabe von Standardwerten herangezogen, wenn sie einer bestimmten Namenskonvention genügen (siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458). Sie werden dann **aktive** Regelbehälter genannt.

Damit nicht schon während der Einrichtungsphase unerwünschten Standardwerte vergeben werden, empfiehlt es sich, zur Vorbereitung von Regeln einen inaktiven Regelbehälter zu verwenden. Wenn alle Regeln und Attributguards fertiggestellt sind, kann dieser Regelbehälter durch Umbenennung aktiviert werden:

```
/MODIFY-GUARD-ATTRIBUTES ...,NEW-NAME=SYS.UDF
```

Die Festlegung der Standardschutzregeln erfolgt in zwei Schritten:

1. Einrichten von Regelbehältern (Guards, siehe Seite 434)
2. Eintragen der Standardschutzregeln in die Regelbehälter (Guards)

Die Systemverwaltung kann auch Regelbehälter erstellen, die Standardschutzregeln für Dateien eines Pubsets enthalten. Auch für die Aktivierung dieser Regelbehälter muss eine Namenskonvention eingehalten werden (siehe Seite 459).

Eintragen der Standardschutzregeln

Zur Erstellung und Verwaltung von Standardschutzregeln stehen folgende Kommandos zur Verfügung. Diese Kommandos sind nicht RFA-fähig:

ADD-DEFAULT-PROTECTION-RULE	Standardschutzregel hinzufügen
MODIFY-DEFAULT-PROTECTION-RULE	Standardschutzregel ändern
REMOVE-DEFAULT-PROTECTION-RULE	Standardschutzregel entfernen
SHOW-DEFAULT-PROTECTION-RULE	Standardschutzregel anzeigen
SHOW-OBJECT-PROTECTION-DEFAULT	Standardschutzattribute für Objekt anzeigen

Außerdem können die Regelbehälter wie ein Guard mit den allgemeinen GUARDS-Verwaltungskommandos verwaltet werden (siehe Seite 434).

Ein Regelbehälter wird implizit wieder gelöscht, sobald ein letzter Eintrag mit dem Kommando /REMOVE-DEFAULT-PROTECTION-RULE entfernt wird.

Aufbau der Standardschutzregeln

Jede Regel wird durch einen Namen angesprochen und gliedert sich in drei Teile:

1. Regelteil:

   Dieser Teil beinhaltet den Namen einer Datei oder Jobvariablen, für die bestimmte Schutzattribut-Standardwerte verwendet werden sollen. Der Name kann teilqualifiziert oder mit Hilfe von Musterzeichen angegeben werden. Er enthält jedoch keine Angaben über Pubsetid oder Benutzerkennung.

2. Regelteil

   Dieser Teil beinhaltet den Verweis auf ein Guard des Typs DEFPUID, das die Liste von Benutzerkennungen enthält, die die im 1. Regelteil angegebenen Dateien pubsetglobal eindeutig bezeichnen. Dieser Regelteil ist der Systemverwaltung für pubsetglobale Festlegungen vorbehalten und wird für eine benutzerspezifische Standardwertvergabe ignoriert.

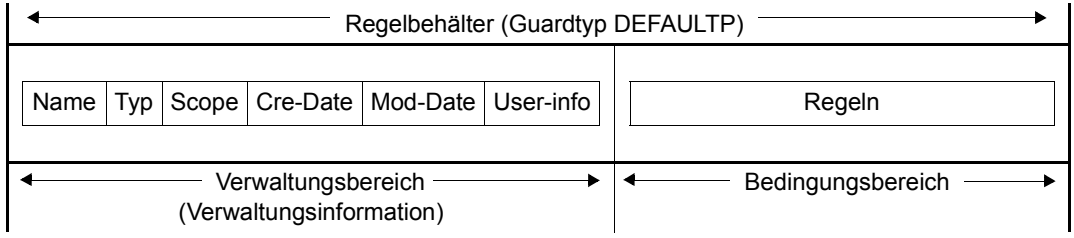
3. Regelteil:

   Dieser Teil beinhaltet den Verweis auf ein Guard des Typs DEFPATTR, das die Schutzattribut-Standardwerte enthält, die für die im 1. Regelteil angegebene Datei gelten sollen.

Die Reihenfolge, in der die Regeln in den Regelbehälter angeordnet sind, spielt eine entscheidende Rolle bei der Auswahl einer gültigen Regel, d. h. bei der Auswahl der einzusetzenden Standardwerte. Die Suche nach einer passenden Regel erfolgt in der Reihenfolge, in der die Regeln im Regelbehälter stehen und wird mit dem ersten Treffer beendet (Näheres hierzu finden Sie im Abschnitt „Überlappung von Objektnamen“ auf Seite 465).

5.5.3.1 Aufbau eines Regelbehälters (Guard Typ DEFAULTP)

Ein Regelbehälter für den Standardschutz hat folgenden Aufbau:



Der Bedingungsbereich eines Regelbehälters ist folgendermaßen aufgebaut:

Regelname	**1. Regelteil (Objektname)**	**2. Regelteil (optional Benutzerkennungsliste, nur pubsetglobal)**	**3. Regelteil (Attributwerte)**
REGEL001	Name (mit Musterzeichen)	Name des Benutzerkennungsguards	Name des Attributguards
REGEL002	Name (mit Musterzeichen)	Name des Benutzerkennungsguards	Name des Attributguards
	...	...	...
REGEL100	Name (mit Musterzeichen)	Name des Benutzerkennungsguards	Name des Attributguards

5.5.3.2 Geltungsbereich der Standardschutzregeln

In Standardschutzregeln werden die Objektnamen ohne Pfad (d. h. ohne Pubset-ID und Benutzerkennung) angegeben. Für die Vergabe von Standardwerten wird der **aktive** benutzerspezifische Regelbehälter verwendet, der auf **demselben Pubset** und unter **derselben Benutzerkennung** eingerichtet ist wie die Datei oder Jobvariable, die Standardwerte erhalten soll.

Können nicht alle Standardwerte aus dem benutzerspezifischen aktiven Regelbehälter ermittelt werden, wird der pubsetglobale aktive Regelbehälter von diesem Pubset herangezogen.

Die Attributguards mit den Standardwerten und (für die Systemverwaltung) die Benutzerkennungsguards mit den Benutzerkennungslisten müssen auf demselben Pubset eingerichtet sein wie der jeweilige Regelbehälter, der zur Auswertung verwendet wird.

5.5.3.3 Aktivierung eines Regelbehälters

Obwohl unter einer Benutzerkennung beliebig viele Regelbehälter eingerichtet werden können, kann nur einer von ihnen **aktiv** sein und bei der Vergabe von Standardwerten berücksichtigt werden. Die Aktivierung eines Regelbehälters wird erreicht, indem man fest vorgeschriebene Namen verwendet (siehe „Namenskonvention“ auf Seite 459). Eine entsprechende Namenskonvention gilt auch für die Aktivierung pubsetglobaler Regelbehälter, die immer unter der Benutzerkennung TSOS erwartet werden.

Soll ein Regelbehälter aktiviert werden, kann er mit Hilfe von GUARDS-Verwaltungskommandos umbenannt oder kopiert werden um den vorgeschriebenen Namen erhalten (siehe „Namenskonvention“ auf Seite 459 und „Umbenennen von Regelbehältern“ auf Seite 460).

Wenn ein aktiver Regelbehälter aus Platzgründen keine weiteren Regeln mehr aufnehmen kann, kann der Anwender sekundäre Fortsetzungsbehälter einrichten. Auf diese Weise bildet sich eine aktive Behältersequenz, bestehend aus einem primären Behälter und bis zu neun Sekundärbehältern, jeweils mit genau vorgeschriebenen Namen.

Die gültige Reihenfolge der Fortsetzungsbehälter ist durch eine laufende Nummer im Namen festgelegt. Zusätzliche Verkettungen gibt es nicht. Das Ende einer Sequenz ist erreicht, sobald die Nummernreihenfolge unterbrochen ist oder der letztmögliche Fortsetzungsbehälter erreicht ist.

Namenskonvention

Der Name eines aktiven Regelbehälters für den Standardschutz muss folgendermaßen aufgebaut sein:

SYS.<Geltungsbereich><Behältertyp><Objekttyp>[<Sekundärkennzeichen>]

Für die einzelnen Bestandteile sind folgende Werte zulässig:

– Geltungsbereich:
  U Benutzerspezifisch (**u**ser specific)
  P Pubsetglobal (**p**ubset global)

– Behältertyp:
  D Standardschutz (**D**efault Protection)

– Objekttyp:
  F Datei (**F**ile)
  J **J**obvariable

– Sekundärkennzeichen:
  1..9 Nummer des Sekundärbehälters

  Ist kein Sekundärkennzeichen angegeben, handelt es sich um einen Primärbehälter. Es können maximal 10 Regelbehälter aktiv sein (1 Primärbehälter und wahlweise bis zu 9 Sekundärbehälter).

Somit sind folgende Namen erlaubt:

SYS.UDF	aktiver benutzerspezifischer Primärbehälter für Dateien
SYS.UDF<n>	aktive benutzerspezifische Sekundärbehälter für Dateien (n=1..9)
SYS.UDJ	aktiver benutzerspezifischer Primärbehälter für Jobvariable
SYS.UDJ<n>	aktiver benutzerspezifischer Sekundärbehälter für Jobvariable (n=1..9)
SYS.PDF	aktiver pubsetglobaler Primärbehälter für Dateien
SYS.PDF<n>	aktive pubsetglobale Sekundärbehälter für Dateien (n=1..9)
SYS.PDJ	aktiver pubsetglobaler Primärbehälter für Jobvariable
SYS.PDJ<n>	aktive pubsetglobale Sekundärbehälter für Jobvariable (n=1..9)

Aktive benutzerspezifische Regelbehälter werden unter der Benutzerkennung erwartet, für deren Objekte der Standardschutz wirksam sein soll. Aktive pubsetglobale Regelbehälter werden unter der Benutzerkennung TSOS erwartet. Alle Regelbehälter müssen auf demselben Pubset wie die betroffenen Objekte stehen.

Beispiel

Für die Benutzerkennung OTTO soll festgelegt werden, dass Dateien, deren Name mit ’SYS.’ oder ’A’ beginnt, bestimmte Standardschutzattribute erhalten. Dazu muss unter der Kennung OTTO ein Regelbehälter $OTTO.SYS.UDF eingerichtet sein, der die entsprechenden Regeln enthält:

Regelbehälter
$OTTO.SYS.UDF

Datei = SYS.	User-Id = -	Attr = GUARD3
...		
Datei = A*	User-Id = -	Attr = GUARD2

Umbenennen von Regelbehältern

Zum Umbenennen von Regelbehältern steht das GUARDS-Verwaltungskommando /MODIFY-GUARD-ATTRIBUTES zur Verfügung.

Ein Umbenennen von Regelbehältern ist insbesondere erforderlich, wenn ein aktiver Regelbehälter deaktiviert oder ein inaktiver Regelbehälter aktiviert werden soll.

Beispiel

Ein wirksamer Standardschutz soll im Guard UDF.BAK sichergestellt und durch Regeln ersetzt werden, die im Regelbehälter UDF.NEU stehen.

```
/modify-guard-attributes guard-name=sys.udf,new-name=udf.bak
/modify-guard-attributes guard-name=udf.neu,new-name=sys.udf
```

5.5.4 Festlegung der Benutzer- und Gruppenkennungen für Pfadnamen (nur für Systemverwaltung)

Standardschutz-Benutzerkennungslisten werden in Benutzerkennungsguards (Typ DEFPUID) spezifiziert und sitzungsübergreifend gespeichert. Mit ihnen können die in den pubsetglobalen Standardschutzregeln festgelegten Objektnamen wahlweise feiner differenziert werden.

Beispiel

Auf einem Pubset :A: sind unter der Benutzerkennung SALARY alle Dateien als sicherheitskritisch eingestuft, deren Namen mit dem Präfix SAVE. beginnen. Sie sollen standardmäßig mit dem Schutzattribut DESTROY=*YES versehen werden. Es ist jedoch nicht ausgeschlossen, dass auf dem selben Pubset auch andere Benutzer unter ihren Kennungen Dateien mit dem Präfix SAVE. einrichten. Für diese Dateien soll jedoch der System-Standardwert DESTROY=*NO gelten.

Legt die Systemverwaltung im pubsetglobalen Regelbehälter eine Standardschutzregel für das Objekt SAVE.* fest, würde diese Regel pubsetweit für alle Dateien mit dem Präfix SAVE. gelten. Weist der Systemverwalter hingegen in dieser Regel zusätzlich ein Benutzerkennungsguard zu, in das er die Benutzerkennung SALARY eingetragen hat, sind nur noch die Dateien mit dem Pfadnamen :A:$SALARY.SAVE.* von dieser Regel betroffen.

Im Benutzerkennungsguard können die Benutzerkennungen und Benutzergruppen in beliebiger Reihenfolge und mit Hilfe von Musterzeichen festgelegt werden. Das heißt, die Benutzerkennung aus dem Pfadnamen eines Objekts, auf das eine Regel zutrifft, wird gegen alle im Benutzerkennungsguard eingetragenen Benutzerkennungen und Gruppen geprüft. (Siehe auch „Überprüfung der Benutzerkennungsliste (Systemverwaltung)“ auf Seite 463).

Die Festlegung der Standardschutz-Benutzerkennungslisten erfolgt in zwei Schritten:

1. Einrichten von Guards (siehe Seite 434).
2. Eintragen der Standardschutz-Benutzerkennungslisten in die Guards

Eintragen der Standardschutz-Benutzerkennungslisten

Zur Bearbeitung von Benutzerkennungsguards stehen der Systemverwaltung folgende Kommandos zur Verfügung. Diese Kommandos sind nicht RFA-fähig:

ADD-DEFAULT-PROTECTION-UID	Benutzerkennung oder Gruppe hinzufügen
REMOVE-DEFAULT-PROTECTION-UID	Benutzerkennung oder Gruppe löschen
SHOW-DEFAULT-PROTECTION-UID	Benutzerkennung oder Gruppe anzeigen

Außerdem stehen für die Verwaltung von Benutzerkennungsguards die allgemeinen GUARDS-Verwaltungskommandos zur Verfügung (siehe Seite 434).

5.5.5 Suchlogik

Die Suche nach passenden Schutzattribut-Standardwerten setzt sich aus zwei Vorgängen zusammen:

– der Suche **nach** den aktiven Regelbehältern

– der Suche **in** den aktiven Regelbehältern

Einen Überblick über die Suchlogik bei der Ermittlung der Schutzattribut-Standardwerte gibt Bild 20 auf Seite 464.

5.5.5.1 Suche nach den aktiven Regelbehältern

Die Suche nach den benutzerspezifischen und pubsetglobalen Regelbehältern erfolgt in zwei Stufen:

Stufe 1: Suche nach benutzerspezifischen Regelbehältern

Der Regelbehälter SYS.UDF oder SYS.UDJ wird unter derselben Katalog- und Benutzerkennung gesucht, unter der sich die Datei oder Jobvariable befindet, für die Standardwerte gesucht werden sollen. Gibt es diesen Regelbehälter, wird geprüft, ob er oder einer seiner Fortsetzungsbehälter eine passende Regel enthält. Ist das der Fall, wird die Suche abgebrochen und die Regel ausgewertet.

Stufe 2: Suche nach pubsetglobalen Regelbehältern

Wird in der 1. Stufe der Suche keine passende Regel gefunden, dann wird unter derselben Katalogkennung ein pubsetglobaler Regelbehälter $TSOS.SYS.PDF oder $TSOS.SYS.PDJ gesucht. Ist dieser vorhanden, dann wird er (und ggf. seine Fortsetzungsbehälter) nach einer passenden Regel durchsucht. Wird eine passende Regel gefunden, dann wird die Suche abgebrochen.

Führt auch die zweite Stufe der Suche zu keinem Ergebnis, werden die herkömmlichen System-Standardwerte eingesetzt.

5.5.5.2 Suche in den aktiven Regelbehältern

Ein Regelbehälter kann mehrere Regeln enthalten, die wiederum jeweils aus mehreren Bedingungen bestehen. Daher muss die Prüfung einer ganz bestimmten Logik folgen.

Suche nach gültigen Regeln

Die Regeln werden in der Reihenfolge geprüft, in der sie im Regelbehälter eingetragen sind. Die Prüfung ermittelt, ob die Regel auf das Objekt (Datei oder Jobvariable) zutrifft, auf das zugegriffen werden soll. Der Name des Zugriffsobjekts wird nacheinander mit dem Objektnamen in der ersten, zweiten, ... n-ten Regel des Regelbehälters verglichen, so lange, bis ein passender Name gefunden wurde oder keine weitere Regel vorhanden ist.

Ist eine passende Regel gefunden, wird die Suche im Regelbehälter abgebrochen. Die entsprechenden Standardwerte werden zugewiesen. Ist für ein Attribut als Standardwert *BY-SYSTEM-STANDARD angegeben, hängt die weitere Suche vom Typ des Regelbehälters ab, in dem die Regel gefunden wurde:

- Handelt es sich um einen benutzerspezifischen Regelbehälter, wird die Suche nach Regelbehältern mit Stufe 2 fortgesetzt.
- Handelt es sich um einen pubsetglobalen Regelbehälter, wird der herkömmliche System-Standardwert zugeordnet.

Wird keine passende Regel gefunden, erhält das Objekt die herkömmlichen System-Standardwerte.

Überprüfung der Benutzerkennungsliste (Systemverwaltung)

Eine Regel in **pubsetglobalen** Regelbehältern kann auf eine Benutzerkennungsliste verweisen (Guard des Typs DEFPUID). Damit eine Regel als passend erkannt wird, müssen in diesem Fall zwei Bedingungen erfüllt sein:

1. Der Objektname der Regel muss zum Namen des betreffenden Objektes passen,

   UND

2. die referenzierte Benutzerkennungsliste muss entweder eine Benutzerkennung enthalten, die mit der Benutzerkennung des betreffenden Objektes übereinstimmt, oder die referenzierte Benutzerkennungsliste muss eine Gruppenkennung enthalten, der die Benutzerkennung dieses Objektes angehört.

Ist die Benutzerkennungsliste nicht zugreifbar, wird die Suche mit Fehler abgebrochen.

Für die Ermittlung der Schutzattribut-Standardwerte gilt:

Ist das in der ermittelten Regel referenzierte Attributguard nicht verfügbar, wird die Suche mit Fehler abgebrochen.

Die folgende Grafik zeigt die Suchstrategie bei der Ermittlung von Standardwerten:

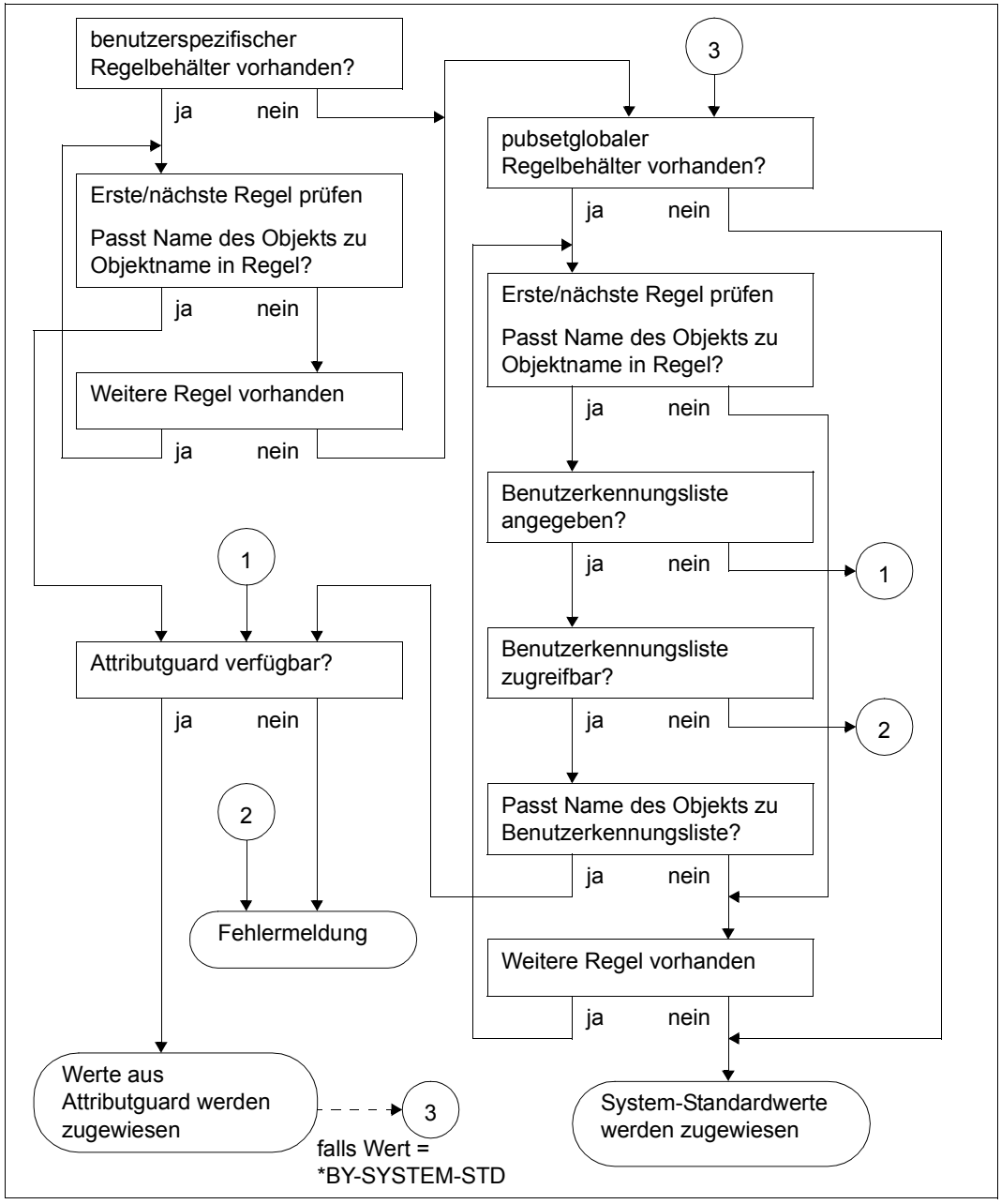
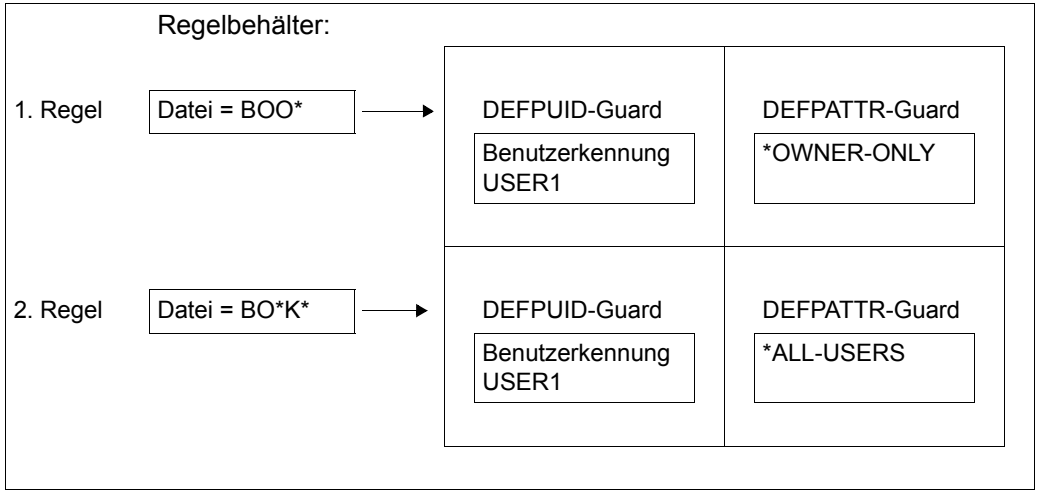


Bild 20: Logik bei der Ermittlung von Standardwerten mit Hilfe des Standardschutzes

5.5.5.3 Überlappung von Objektnamen

Durch die Verwendung von Musterzeichen im Objektnamen ist es möglich, dass auf den Namen eines Objektes mehrere Regeln eines Regelbehälters passen. Die Prüfung erfolgt jedoch grundsätzlich in der Reihenfolge, in der die Regeln im Regelbehälter stehen, und wird beim ersten Treffer beendet.

Die Grafik zeigt den aktiven Regelbehälter (pubsetglobal):



USER1 erstellt die Datei $USER1.BOOK. Bei der Suche nach passenden Standardwerten wird der String BOO* aus der ersten Regel gegen den Dateinamensteil BOOK geprüft. Der Name passt. Nun wird die Benutzerkennung im Pfadnamen der Datei BOOK ($USER1) gegen die spezifizierte Benutzerkennung im DEFPUID-Guard geprüft. Sie stimmt überein und es wird der Standardwert USER-ACCESS=*OWNER-ONLY verwendet. Die 2. Regel wird bei der Suche nicht mehr berücksichtigt.

ACHTUNG!
Die Reihenfolge der Regeln innerhalb eines Regelbehälters und in einer Regelbehältersequenz spielt eine entscheidende Rolle bei der Zuweisung von Schutzattribut-Standardwerten.

5.5.5.4 Reorganisation aktiver Regelbehälter

Die Reorganisation von Regelbehältern kann erforderlich sein, wenn folgende Bedingungen zutreffen:

– Mindestens ein Sekundärbehälter ist vorhanden

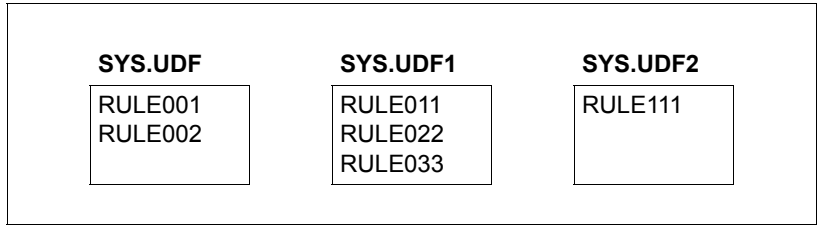
– Der Primärbehälter oder ein Sekundärbehälter, der nicht der letzte in der Behältersequenz ist, ist nicht vollständig gefüllt.

Für die Reorganisation der Namen und Inhalte von Regelbehältern ist der Anwender selbst verantwortlich. Für diesen Vorgang können mehrere Arbeitsschritte erforderlich sein.

Mit den folgenden Beispielen wird eine Vorgehensweise gezeigt, die verhindert, dass während der Reorganisation eine unerwünschte Standardwertvergabe eintritt:

Beispiel 1

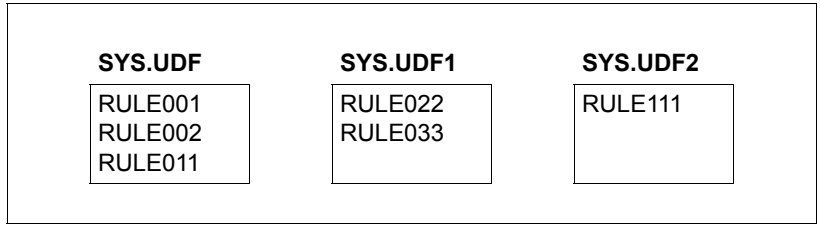
Durch eine günstigere Verteilung der Regeln innerhalb einer aktiven Behältersequenz SYS.UDF - SYS.UDF2 kann ein Fortsetzungsbehälter eingespart werden:



Zunächst wird die erste Regel des ersten sekundären Regelbehälters SYS.UDF1 hinter der letzten Regel des primären Regelbehälters SYS.UDF eingefügt. Anschließend wird sie aus SYS.UDF1 gelöscht.

```
/add-default-protection-rule rule-container-guard=sys.udf, -
/                            protection-rule=rule011, ...
/remove-default-protection-rule rule-container-guard=sys.udf1, -
/                               protection-rule=rule011, ...
```

Dadurch entsteht im Regelbehälter SYS.UDF1 Platz für eine neue Regel.

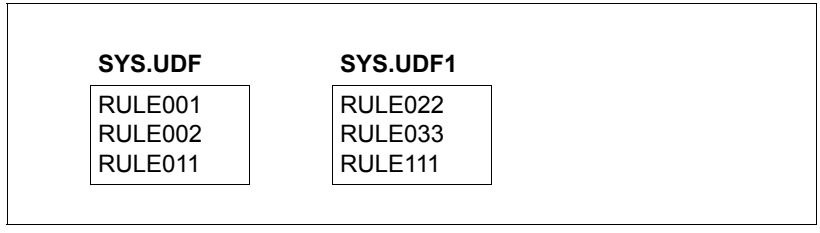


Dieser wird mit der ersten und in diesem Fall einzigen Regel des nächsten sekundären Regelbehälters SYS.UDF2 gefüllt.

```
/add-default-protection-rule rule-container-guard=sys.udf1, -
/                            protection-rule rule111, ...
```

Anschließend wird die Regel aus SYS.UDF2 gelöscht, wobei der Regelbehälter automatisch ebenfalls gelöscht wird, da er keine Regel mehr enthält.

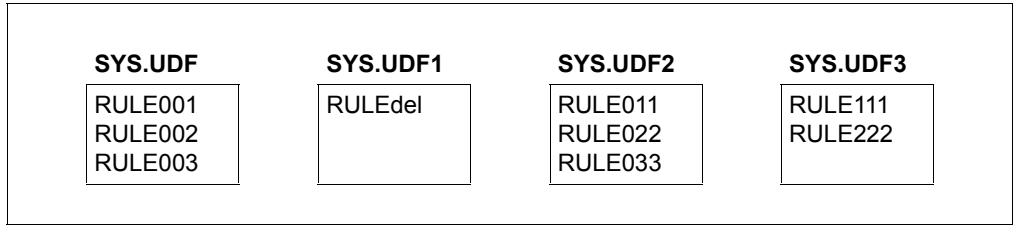
```
/remove-default-protection-rule rule-container-guard = sys.udf2, -
/                               protection-rule= rule111, ...
```



Während des gesamten Reorganisationsvorgangs bleibt die Reihenfolge der Regeln unverändert. Die Tatsache, dass einige Regeln zeitweise doppelt vorhanden waren, spielt bei der Auswertung keine Rolle.

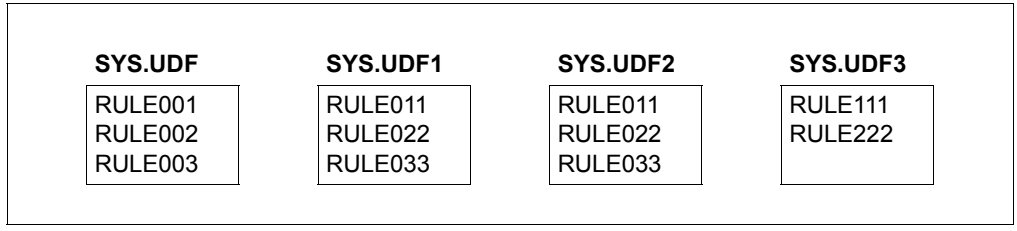
Beispiel 2

In einer aktiven Regelbehältersequenz SYS.UDF - SYS.UDF3 enthält der Sekundärbehälter SYS.UDF1 nur noch eine einzige Regel, die entfernt werden soll. Da beim Löschen einer letzten Regel der ganze Regelbehälter gelöscht wird, muss verhindert werden, dass die Namenskette abreißt, damit auch die Regelbehälter SYS.UDF2 und SYS.UDF3 weiterhin als aktive Fortsetzungsbehälter berücksichtigt werden.



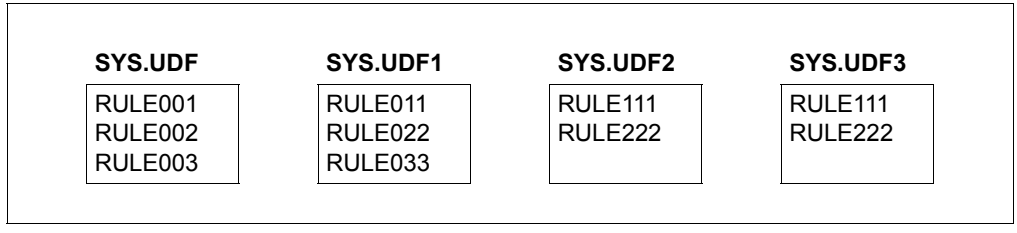
Der Regelbehälter SYS.UDF2, der in der Regelbehältersequenz unmittelbar hinter dem zu löschenden Regelbehälter SYS.UDF1 liegt, wird so kopiert, dass er den zu löschenden Behälter ersetzt.

```
/copy-guard from-guard=sys.udf2,to-guard=sys.udf1,replace-old-guard=*yes
```



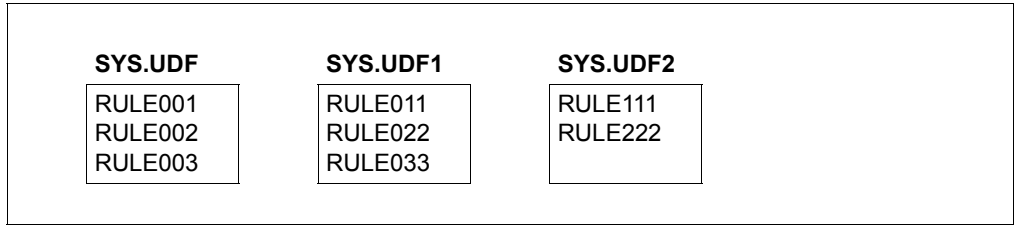
Dadurch wird der Regelbehälter SYS.UDF2 überflüssig. Er wird durch den nächsten Regelbehälter aus der Sequenz ersetzt:

```
/copy-guard from-guard=sys.udf3,to-guard=sys.udf2,replace-old-guard=*yes
```



Damit wird der Regelbehälter SYS.UDF3 überflüssig und kann gelöscht werden, da ihm keine weiteren Behälter in der Sequenz folgen.

```
/delete-guard guard-name=sys.udf3
```



5.5.6 Allgemeine Hinweise zum Einsatz des Standardschutzes

Im Hinblick auf die Ablaufsicherheit des Systems und der installierten Produkte ist beim Einsatz des Standardschutzes (Default-Protection) Folgendes zu beachten:

– Für Dateien, die von Anwendungen oder Systemkomponenten angelegt werden, dürfen keine Standardwerte vergeben werden, die einen Lese- oder Schreibzugriff durch die Produkte selbst verbieten.

– Die aktiven Regelbehälter mit allen referenzierten Attribut- und Benutzerkennungsguards müssen zugreifbar sein. Ansonsten wird die entsprechende Datei- oder Jobvariablenbearbeitung mit Fehlermeldung DMS05B5 bzw. JVS044C abgewiesen.

– Der Standardschutz ist während der Startup- und Shutdown-Phase ausgeschaltet.

– Der Standardschutz ist während eines Pubsetimports oder -exports für das betroffene Pubset ausgeschaltet.

Hinweise für nichtprivilegierte Anwender

Für Dateien mit dem Präfix “S.” bzw. “SYS*” sollten keine Standardschutzregeln festgelegt werden. Falls Schutzattribut-Standardwerte festgelegt werden, die den Zugriff auf diese Dateien verhindern, können folgende Probleme auftreten:

– Es können keine primären SYSOUT-Dateien und keine temporären Spool-Dateien angelegt werden.

– Das Starten von Enter-Aufträgen ist nicht möglich, weil dabei die primäre SYSOUT-Datei “S.OUT.<tsn>” angelegt werden muss.

Hinweise für die Systemverwaltung

Die Hinweise für nichtprivilegierte Anwender gelten auch für die Systemverwaltung und insbesondere bei der Verwendung pubsetglobaler Regelbehälter. Zusätzlich sollten bei der Verwendung dieser Regelbehälter auch keine Standardschutzregeln für Dateien und Jobvariablen mit dem Präfix “SYS*” (z.B. “SYSLOG.”-Dateien) festgelegt werden.

Außerdem ist Folgendes zu beachten:

– In einem Verbund von Rechnern muss die Rechnerumgebung aufeinander abgestimmt sein. Insbesondere wird bei einem Einsatz von SECOS auf einem Rechner im Rechnerverbund dringend empfohlen, auch auf allen anderen beteiligten Rechnern SECOS mit derselben Version einzusetzen.

– Der Entzug von Zugriffsrechten für “S.”-Dateien auf dem Home-Pubset führt insbesondere zum Beenden der Job-Scheduler während des System-Startups.

– Die Kennung SYSSAG sollte von der Vergabe von Standardwerten über den Standardschutz ausgenommen werden, da diese Kennung von IMON bei der Produktinstallation verwendet wird.

Die folgende Tabelle enthält eine Aufstellung besonders kritischer Dateien und Jobvariablen und der betroffenen Produkte:

Produkt/ Komponente	**Typ**	**Objekt**	**Problem**
JobScheduler	Datei	$<userid>.S.OUT.<tsn>*	Beendigung, wenn kein Zugriff auf Primary-Sysout-Files möglich ist
SPOOL	Datei	$<userid>.S.LST.<tsn>*	Kein Anlegen von Spool-Dateien
POSIX	Datei	$TSOS.S.IN.SINPRC.POSINST.<vers>.<tsn>*	Abbruch POSIX-Erstinstallation
	Datei	$SYSROOT. SYSLOG.POSIX-BC.<vers>.INIT	Abbruch POSIX-Start
Memory Management	Datei	:<catid>:$TSOS.SYS.PAGING.<vsn>	Löschen der Paging-Datei nicht möglich (Kdo. DELETE-PAGING-FILE)
SIR	Datei	:<catid>:$TSOS.SIR.TEMPORARY-FILE.<tsn> :<catid>:$TSOS.S.*	Kein Extend-Pubset mit Copy bei SIR
SystemDump	Datei	$SYSDUMP.<modulname>	DumpFile kann nicht erzeugt bzw. schreibend geöffnet werden
MSCF	JV	$TSOS.SYS.PVS.<catid>.MASTER.CONTROL und $TSOS.SYS.MSCF.CONTROL-STATE	Import für Shared Pubset bricht ab
	Datei	$TSOS.SYS.MSCF-TRACE.<datum>	MSCF-Tracedatei kann nicht angelegt werden.
DSSM	Datei	$TSOS.DSSMLOG.<date>.<time>	Kein DSSM-Logging
HSMS	JV	$SYSHSMS.SYS.HSM.MIGRATE.<catid> $SYSHSMS.SYS.HSM.MIGRATE	Migration kann nicht gestartet werden
ARCHIVE	Datei	:<catid>:$TSOS.ARCHIVE*	Kein Schreiben in Archiv wenn für das Schutzattribut GUARDS entsprechende Standardwerte vergeben wurden.
IMON	File	$SYSSAG.*. Mit den Endungen DOC, IA, IC, IE, II, IL, IP, IR, SCI, SCI.GPN	IMON-Installation wird abgebrochen

5.6 Miteigentümerschutz (Co-owner protection)

Über den Miteigentümerschutz legt ein Objekteigentümer fest, für welche seiner Objekte er Miteigentümer benennen will und welche Bedingungen die Miteigentümer bei Verwaltungszugriffen zu erfüllen haben.

Ein Objekteigentümer ist diejenige Benutzerkennung, unter der ein Objekt eingerichtet ist oder eingerichtet wird.

Ein Miteigentümer ist eine Benutzerkennung, die ungleich der Benutzerkennung des Objekteigentümers ist, aber in Bezug auf ein bestimmtes Objekt dieselben Rechte besitzt wie der Objekteigentümer.

Allgemein gilt für Miteigentümer:

Alle Lese-, Schreib- und Ausführungszugriffe auf Dateien und Jobvariablen werden nach Regeln der traditionellen Schutzmechanismen kontrolliert:

– Ist eine Datei oder Jobvariable über SHARE/ACCESS oder über BACL geschützt, hat ein Miteigentümer dieselben Lese-, Schreib- und Ausführungsrechte wie der Eigentümer.

– Ist eine Datei oder Jobvariable durch Guards geschützt, erfolgt die Zugriffsregelung durch Auswertung von Zugriffsbedingungen, die in STDAC-Guards festgelegt sind.

Erzeugt ein Miteigentümer unter fremder Kennung eine Datei oder Jobvariable und schützt diese mit einem STDAC-Guard, so muss er vor einem Zugriff dafür sorgen, dass seiner Kennung ein Zugriffsrecht auf dieses Objekt eingeräumt ist. Umgekehrt muss einem Eigentümer bewusst sein, dass ihm Datenzugriffe durch Miteigentümer untersagt werden können.

Mit dem Kommando /MODIFY-FILE-ATTRIBUTES (bzw. /MODIFY-JV-ATTRIBUTES) können sich jedoch sowohl Dateieigentümer als auch Miteigentümer das Zugriffsrecht jederzeit und uneingeschränkt wieder zurückbeschaffen.

Miteigentümerobjekte sind Dateien und Jobvariablen.

Miteigentümer werden in Form von Regeln mit den entsprechenden Namen der Objekte verknüpft, die sie mitverwalten dürfen. Die Objektmenge kann dabei mit Hilfe von Musterzeichen festgelegt werden.

Die Regeln werden sessionübergreifend in Regelbehältern (Guards des Typs DEFAULTP) gespeichert. Ein Anwender kann unter seiner Kennung beliebig viele solcher Regelbehälter erstellen. Entspricht der Name eines Regelbehälters einer ganz bestimmten Namenskonvention (z.B. SYS.UCF), gilt er als aktiv und wird für die Überprüfung der Miteigentümerzugriffe verwendet (z.B. bei Ausführung des Kommandos /CREATE-FILE FILE-NAME=$FOREIGN.FILE, wenn sich die angegebene Benutzerkennung von der des Kommandogebers unterscheidet). Näheres ist dem Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 479 zu entnehmen.

Miteigentümerschaft von TSOS

Standardmäßig besitzt die Benutzerkennung TSOS systemweit ein uneingeschränktes Mitverwaltungsrecht für Dateien und Jobvariablen. SECOS erlaubt es jedoch, dieses Recht einzuschränken. Das bedeutet:

– Ein Benutzer unter der Benutzerkennung TSOS darf eine festgelegte Menge von Attributen eines fremden Objekts nur dann **nicht verändern**, wenn es ihm der Objekteigentümer über den Miteigentümerschutz **explizit verbietet**.

– Für nichtprivilegierte Benutzer ändert sich durch diese neue Funktion nichts. Sie dürfen Attribute einer fremden Datei oder Jobvariablen nur dann **verändern**, wenn es der Objekteigentümer über den Miteigentümerschutz **explizit erlaubt**.

Die Einschränkung der TSOS-Mitverwaltungsrechte hat folgende Ziele:

– Dem Benutzer unter der Benutzerkennung TSOS soll es verwehrt werden, sich durch Ändern der Schutzattribute fremder Dateien oder Jobvariablen unberechtigten Zugriff auf Daten zu verschaffen.

– Sabotage-Attacken, wie zum Beispiel das Löschen von Objekten, sollen unterbunden werden.

Näheres zu diesem Thema finden Sie im Abschnitt „Einschränkung der TSOS-Miteigentümerschaft“ auf Seite 487.

5.6.1 Anwendungskonzept

Grundlage für die Einführung einer sinnvollen Miteigentümerschaftsregelung bildet das Anwendungskonzept. Der Anwender ist diejenige Instanz, die sowohl konzeptionell als auch manuell festlegen muss, für welche seiner Dateien und Jobvariablen Miteigentümerschaften gestattet werden und unter welchen Bedingungen Miteigentümerschaften gestattet werden. Für die Spezifizierung eines Miteigentümerschutzes sind darum zwei Arbeitsschritte notwendig:

– Festlegen der Miteigentümerbedingungen in Bedingungsguards (Guards des Typs STDAC).

– Verknüpfen dieser spezifizierten Miteigentümerbedingungen mit den Namen der Dateien oder Jobvariablen, die durch Miteigentümer verwaltet werden sollen. Die Verknüpfung muss in Form von Regeln in Guards des Typs COOWNERP durchgeführt werden. Diese Guards werden Regelbehälter genannt.

Beispiel einer Konzeptgrundlage

Ein Anwender möchte für Dateien, die unter seiner Kennung angelegt sind oder noch angelegt werden, folgende Miteigentümerregelungen vereinbaren:

a) Alle Dateien, deren Name mit ’A.’ beginnt, soll die Benutzerkennung USER1 jederzeit mitverwalten dürfen.

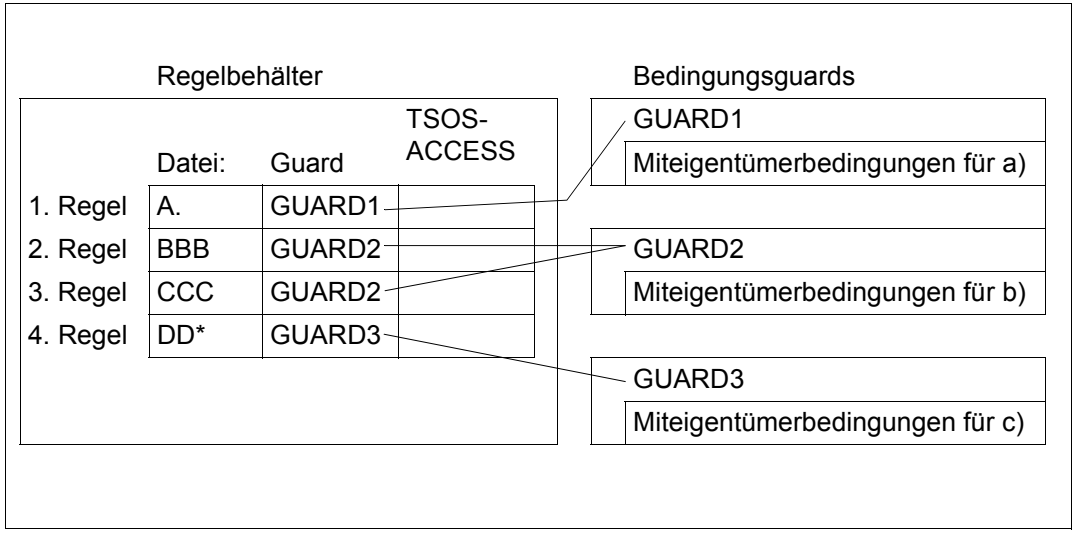
b) Die Dateien BBB und CCC soll die Kennung USER1 nur montags mitverwalten dürfen.

c) Die Dateien, deren Name mit ’DD’ beginnt, soll die Benutzerkennung USER2 mitverwalten dürfen.

Unter diesen Voraussetzungen benötigt der Anwender drei Bedingungsguards (Guardtyp STDAC), in denen er die unter a) bis c) angegebenen Miteigentümerbedingungen definiert. Zusätzlich muss er einen Regelbehälter anlegen. Die Regeln in diesem Regelbehälter bestehen aus folgenden Teilen:

1. Name der Datei oder der Dateien, für die Miteigentümer festgelegt werden sollen.
2. Verweis auf ein Bedingungsguard, das die gewünschten Miteigentümerbedingungen für den genannten Dateinamensraum enthält.
3. Kennzeichen, ob dem Benutzer TSOS das standardmäßige Mitverwaltungsrecht entzogen werden soll. Näheres hierzu finden Sie im Abschnitt „Einschränkung der TSOS-Miteigentümerschaft“ auf Seite 487.

Die Punkte a) und c) lassen sich jeweils in einer Regel beschreiben, während für Punkt b) zwei Regeln verwendet werden. Insgesamt ergibt sich folgendes Bild:



5.6.2 Festlegung der Miteigentümerbedingungen

Die Bedingungen, die ein Benutzer erfüllen muss, um Miteigentümer zu sein, werden in Bedingungsguards (Guardtyp STDAC) festgelegt. Hierzu sind zwei Schritte erforderlich:

1. Einrichten von Guards (siehe Seite 434).
2. Eintragen der Miteigentümerbedingungen in die Guards

Eintragen der Miteigentümerbedingungen

Zum Bearbeiten und Verwalten der Miteigentümerbedingungen stehen folgende Kommandos zur Verfügung:

ADD-ACCESS-CONDITIONS	Miteigentümerbedingungen hinzufügen
MODIFY-ACCESS-CONDITIONS	Miteigentümerbedingungen ändern
REMOVE-ACCESS-CONDITIONS	Miteigentümerbedingungen entfernen
SHOW-ACCESS-ADMISSION	Eigene Miteigentümerbedingungen anzeigen
SHOW-ACCESS-CONDITIONS	Definitionen anzeigen

Außerdem stehen für die Verwaltung von Bedingungsguards die allgemeinen GUARDS-Verwaltungskommandos zur Verfügung (siehe Seite 434).

5.6.3 Festlegung der Miteigentümerschutzregeln

Der Miteigentümerschutz wird in Form von Regeln festgelegt, die in Regelbehältern (Guards des Typs COOWNERP) sitzungsübergreifend gespeichert werden.

Regelbehälter werden nur dann für den Miteigentümerschutz herangezogen, wenn sie einer bestimmten Namenskonvention genügen (siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 479). Sie werden dann **aktive** Regelbehälter genannt.

Damit es nicht schon während der Einrichtungsphase zu unerwünschten Miteigentümerzugriffen kommt, empfiehlt es sich, zur Vorbereitung von Regeln einen inaktiven Regelbehälter zu verwenden. Wenn alle Regeln und Bedingungsguards fertiggestellt sind, kann dieser Regelbehälter durch Umbenennung aktiviert werden:

```
/MODIFY-GUARD-ATTRIBUTES ...,NEW-NAME=SYS.UCF
```

Die Festlegung der Miteigentümerschutzregeln erfolgt in zwei Schritten:

1. Einrichten von Regelbehältern (Guards, Seite 434)
2. Eintragen der Miteigentümerschutzregeln in die Regelbehälter (Guards)

Eintragen der Miteigentümerschutzregeln

Zur Erstellung und Verwaltung von Miteigentümerschutzregeln stehen folgende Kommandos zur Verfügung. Diese Kommandos sind nicht RFA-fähig:

ADD-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel hinzufügen
MODIFY-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel ändern
REMOVE-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel entfernen
SHOW-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel anzeigen
SHOW-COOWNER-ADMISSION-RULE	Miteigentümerberechtigungsregel anzeigen

Außerdem können die Regelbehälter auch mit den allgemeinen GUARDS-Verwaltungskommandos verwaltet werden (siehe Seite 434).

Ein Regelbehälter wird implizit wieder gelöscht, sobald ein letzter Eintrag mit dem Kommando /REMOVE-DEFAULT-PROTECTION-RULE entfernt wird.

Aufbau der Miteigentümerschutzregeln

Jede Regel wird durch einen Namen angesprochen und gliedert sich in drei Teile:

1. Regelteil:

   Dieser Teil enthält den Namen eines Objekts, für das eine Miteigentümerschaft festgelegt werden soll. Der Name kann teilqualifiziert oder mit Hilfe von Musterzeichen angegeben werden. Er enthält jedoch keine Angaben über Pubset-Id oder Benutzerkennung.

2. Regelteil:

   Dieser Teil enthält den Verweis auf ein Guard des Typs STDAC, das die Bedingungen enthält, die ein Benutzer erfüllen muss, um Miteigentümer des im 1. Regelteil angegebene Objekts zu sein.

3. Regelteil:

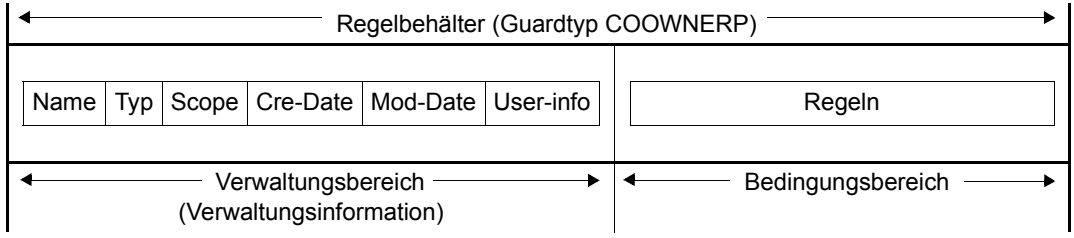
   Dieser Teil legt die Einschränkung der Miteigentümerschaft der Benutzerkennung TSOS fest.

   Näheres hierzu finden Sie im Abschnitt „Einschränkung der TSOS-Miteigentümerschaft“ auf Seite 487.

Die Reihenfolge, in der die Regeln in den Regelbehälter angeordnet sind, spielt eine entscheidende Rolle bei der Auswahl einer gültigen Regel, d. h. bei der Erkennung und Überprüfung eines Miteigentümers. Die Suche nach einer passenden Regel erfolgt in der Reihenfolge, in der die Regeln im Regelbehälter stehen und wird mit dem ersten Treffer beendet (Näheres dazu finden Sie im Abschnitt „Überlappung von Objektnamen“ auf Seite 485).

5.6.3.1 Aufbau eines Regelbehälters (Typ COOWNERP)

Ein Regelbehälter für den Miteigentümerschutz hat folgenden Aufbau:



Der Bedingungsbereich eines Regelbehälters ist folgendermaßen aufgebaut**:**

Regelname	**1. Regelteil (Objektname)**	**2. Regelteil (Zugriffsbedingung)**	**3. Regelteil (TSOS-ACCESS)**
REGEL001	Name (mit Musterzeichen)	Name des Guards mit Miteigentümerbedingungen	SYSTEM-STD oder RESTRICTED
REGEL002	Name (mit Musterzeichen)	Name des Guards mit Miteigentümerbedingungen	SYSTEM-STD oder RESTRICTED
	...	...	
REGEL100	Name (mit Musterzeichen)	Name des Guards mit Miteigentümerbedingungen	SYSTEM-STD oder RESTRICTED

5.6.3.2 Geltungsbereich der Miteigentümerschutzregeln

In Miteigentümerschutzregeln werden die Objektnamen ohne Pfad (d. h. ohne Pubset-ID und Benutzerkennung) angegeben. Bei der Überprüfung einer Miteigentümerschaft wird der **aktive** benutzerspezifische Regelbehälter verwendet, der auf **demselben Pubset** und unter **derselben Benutzerkennung** eingerichtet ist wie die mitzuverwaltende Datei/Bibliothek oder Jobvariable.

Die Guards mit den Miteigentümerbedingungen müssen auf demselben Pubset eingerichtet sein wie der jeweilige Regelbehälter, der zur Auswertung verwendet wird.

5.6.3.3 Aktivierung eines Regelbehälters

Obwohl unter einer Benutzerkennung beliebig viele Regelbehälter eingerichtet werden können, kann nur einer von ihnen **aktiv** sein und bei der Miteigentümerüberprüfung berücksichtigt werden. Die Aktivierung eines Regelbehälters wird erreicht, indem man fest vorgeschriebene Namen verwendet (siehe „Namenskonvention“ auf Seite 480).

Soll ein Regelbehälter aktiviert werden, kann er mit Hilfe von GUARDS-Verwaltungskommandos umbenannt oder kopiert werden um den vorgeschriebenen Namen erhalten (siehe „Namenskonvention“ auf Seite 480 und „Umbenennen von Regelbehältern“ auf Seite 481).

Wenn ein aktiver Regelbehälter aus Platzgründen keine weiteren Regeln mehr aufnehmen kann, kann der Anwender sekundäre Fortsetzungsbehälter einrichten. Auf diese Weise bildet sich eine aktive Behältersequenz, bestehend aus einem primären Behälter und bis zu neun Sekundärbehältern, jeweils mit genau vorgeschriebenen Namen.

Die gültige Reihenfolge der Fortsetzungsbehälter ist durch eine laufende Nummer im Namen festgelegt. Zusätzliche Verkettungen gibt es nicht. Das Ende einer Sequenz ist erreicht, sobald die Nummernreihenfolge unterbrochen ist oder der letztmögliche Fortsetzungsbehälter erreicht ist.

Namenskonvention

Der Name eines aktiven Regelbehälters für den Miteigentümerschutz muss folgendermaßen aufgebaut sein:

SYS.<Geltungsbereich><Behältertyp><Objekttyp>[<Sekundärkennzeichen>]

Für die einzelnen Bestandteile sind folgende Werte zulässig:

– Geltungsbereich:
  U Benutzerspezifisch (**u**ser specific)

– Behältertyp:
  C Miteigentümerschutz (**C**o-owner Protection)

– Objekttyp:
  F Datei (**F**ile)
  J **J**obvariable

– Sekundärkennzeichen:
  1..9 Nummer des Sekundärbehälters

  Ist kein Sekundärkennzeichen angegeben, handelt es sich um einen Primärbehälter. Es können maximal 10 Regelbehälter aktiv sein (1 Primärbehälter und wahlweise bis zu 9 Sekundärbehälter)

Somit sind folgende Namen erlaubt:

SYS.UCF	aktiver benutzerspezifischer Primärbehälter für Dateien
SYS.UCF<n>	aktiver benutzerspezifischer Sekundärbehälter für Dateien (n=1..9)
SYS.UCJ	aktiver benutzerspezifischer Primärbehälter für Jobvariable
SYS.UCJ<n>	aktiver benutzerspezifischer Sekundärbehälter für Jobvariable (n=1..9)

Aktive benutzerspezifische Regelbehälter werden unter der Benutzerkennung erwartet, für deren Objekte Miteigentümer festgelegt werden sollen. Alle Regelbehälter müssen auf demselben Pubset wie die Miteigentümerobjekte stehen.

Beispiel

Für die Dateien einer Benutzerkennung OTTO, deren Name mit 'SYS.' oder 'A' beginnt, ist ein Miteigentümerschutz festgelegt. Die Regeln stehen im primären Regelbehälter für Dateien $OTTO.SYS.UCF.

Regelbehälter $OTTO.SYS.UCF

Dateiname	Zugriffsbedingung	TSOS-ACCESS
SYS.	GUARDZ	
	...	
A*	GUARDZ	

Umbenennen von Regelbehältern

Zum Umbenennen von Regelbehältern steht das GUARDS-Verwaltungskommando /MODIFY-GUARD-ATTRIBUTES zur Verfügung.

Ein Umbenennen von Regelbehältern ist insbesondere erforderlich, wenn ein aktiver Regelbehälter deaktiviert oder ein inaktiver Regelbehälter aktiviert werden soll.

Beispiel

Der wirksame Miteigentümerschutz soll im Guard UCF.BAK sichergestellt und durch Regeln ersetzt werden, die im Regelbehälter UCF.NEW stehen.

```
/modify-guard-attributes guard-name=sys.ucf,new-name=ucf.bak
/modify-guard-attributes guard-name=ucf.new,new-name=sys.ucf
```

5.6.4 Suchlogik

Die Suche nach einer passenden Regel für den Miteigentümerschutz setzt sich aus zwei Vorgängen zusammen:

– der Suche **nach** den aktiven Regelbehältern

– der Suche **in** den aktiven Regelbehältern

Einen Überblick über die Suchlogik bei der Ermittlung von Miteigentümern gibt Bild 21 auf Seite 484.

5.6.4.1 Suche nach den aktiven Regelbehältern

Der Regelbehälter SYS.UCF oder SYS.UCJ wird unter derselben Katalog- und Benutzerkennung gesucht, unter der sich die Datei oder Jobvariable befindet, auf die zugegriffen werden soll.

Gibt es diesen Regelbehälter, so wird er ausgewertet.

Gibt es den Regelbehälter nicht, oder ist er nicht zugreifbar, ist der Zugreifer kein Miteigentümer.

5.6.4.2 Suche in den aktiven Regelbehältern

Ein Regelbehälter kann mehrere Regeln enthalten, die wiederum jeweils aus mehreren Bedingungen bestehen. Daher muss die Prüfung einer ganz bestimmten Logik folgen.

Suche nach gültigen Regeln

Die Regeln werden in der Reihenfolge geprüft, in der sie im Regelbehälter eingetragen sind. Die Prüfung ermittelt, ob die Regel auf das Objekt (Datei oder Jobvariable) zutrifft, auf das zugegriffen werden soll. Der Name des Zugriffsobjekts wird nacheinander mit dem Objektnamen in der ersten, zweiten, ... n-ten Regel des Regelbehälters verglichen, so lange, bis ein passender Name gefunden wurde oder keine weitere Regel vorhanden ist.

Ist eine passende Regel gefunden, wird die Suche im Regelbehälter abgebrochen und die entsprechende Miteigentümerbedingung überprüft.

Wird keine passende Regel gefunden, gilt die Standardregelung des Systems: Die Benutzerkennung TSOS ist der einzige Miteigentümer des Objekts.

	1. Regelteil (Objektname)	**2. Regelteil (Zugriffsbedingung)**	**3. Regelteil (TSOS-Miteigentum)***
1. Regel	Name (mit Musterzeichen)	Guardname	TSOS-ACCESS = Wert
	nein ja → Überprüfen der Zugriffsbedingung ↓		
2. Regel	Name (mit Musterzeichen)	Guardname	TSOS-ACCESS = Wert
	nein ja → Überprüfen der Zugriffsbedingung ↓		
3.Regel	Name (mit Musterzeichen)	Guardname	TSOS-ACCESS = Wert
	nein ja → Überprüfen der Zugriffsbedingung ↓ Kein Miteigentümer		

* Dieser Regelteil betrifft die Überprüfung der Miteigentümerschaft für die Benutzerkennung TSOS, Näheres siehe Abschnitt „Einschränkung der TSOS-Miteigentümerschaft“ auf Seite 487

Überprüfung der Miteigentümerbedingungen

Die Überprüfung der Miteigentümerbedingungen hängt davon ab, ob der Zugreifer das TSOS-Privileg besitzt oder nicht:

– Für nichtprivilegierte Benutzer gilt:

  Die Objektnamen jeder Regel sind mit den Zugriffsbedingungen (STDAC-Guards) verknüpft. Wurde eine Regel mit einem passenden Objektnamen gefunden, liefert die Auswertung des STDAC-Guards das Ergebnis, ob der Zugreifer Miteigentümer des Objekts ist oder nicht.

– Für Benutzer mit TSOS-Privileg liefert die Auswertung des Regelattributs TSOS-ACCESS das Ergebnis, ob der Zugreifer Miteigentümer des Objekts ist oder nicht (siehe Abschnitt „Einschränkung der TSOS-Miteigentümerschaft“ auf Seite 487).

Die folgende Grafik verdeutlicht die gesamte Prüflogik des Miteigentümerschutzes für Benutzer **ohne** TSOS-Privileg. Die Prüflogik, die dabei der Auswertung von STDAC-Guards zugrunde liegt, finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 446.

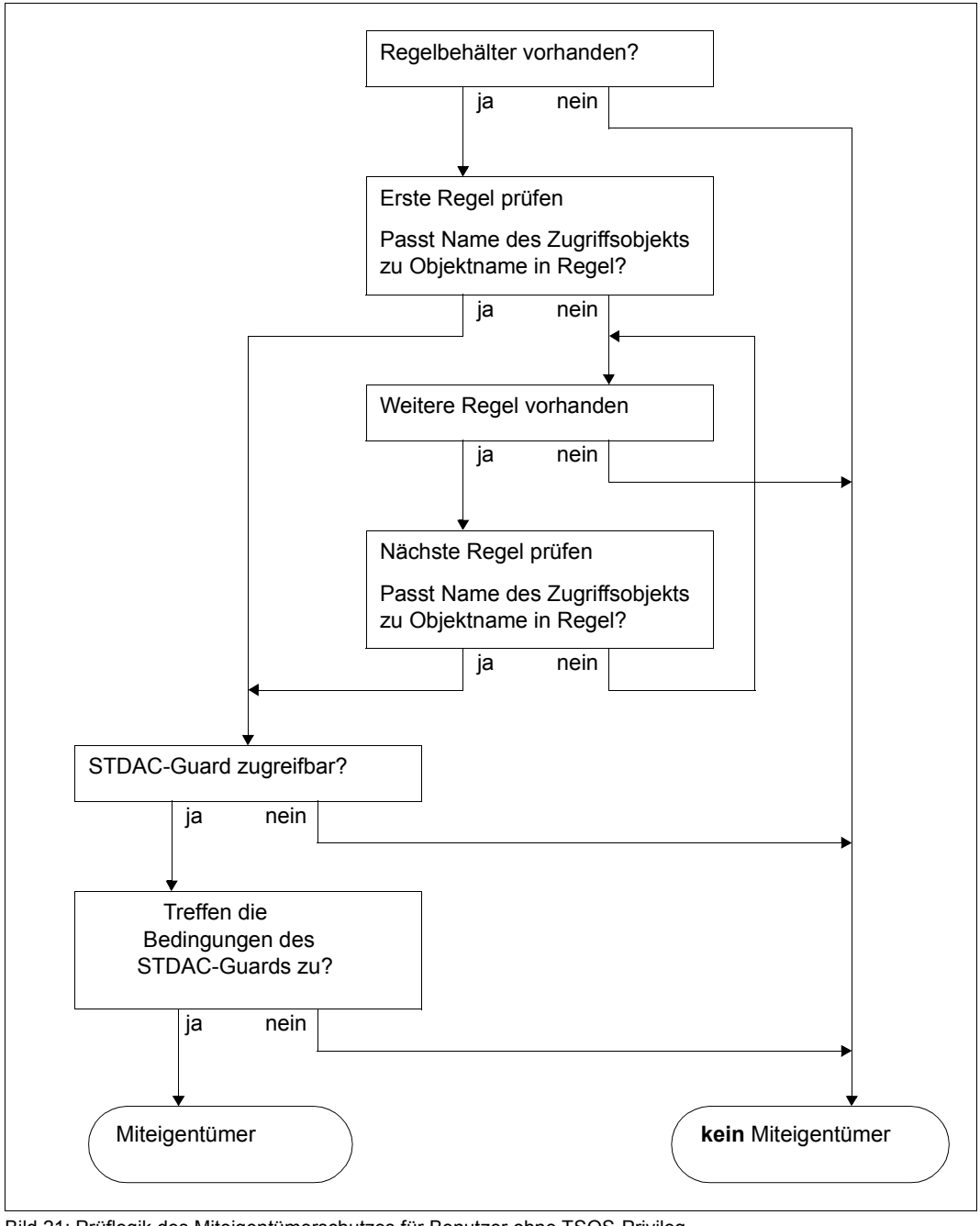
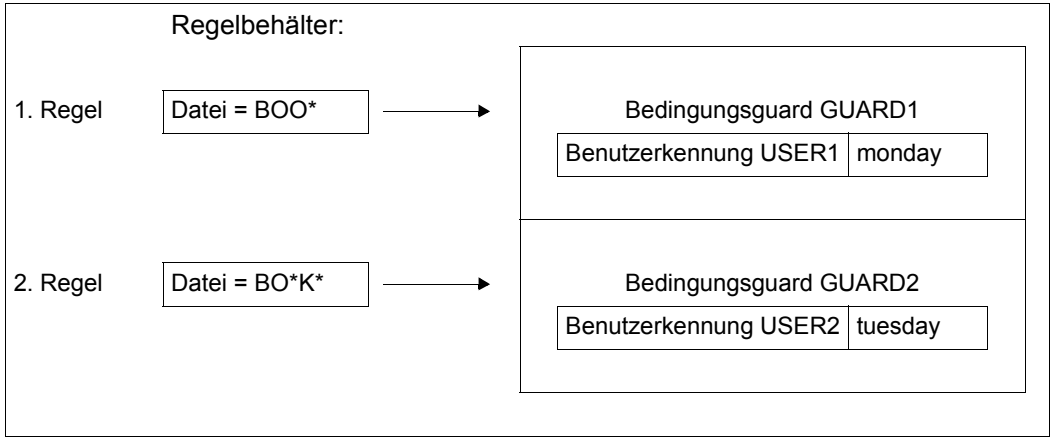


Bild 21: Prüflogik des Miteigentümerschutzes für Benutzer ohne TSOS-Privileg

5.6.4.3 Überlappung von Objektnamen

Durch die Verwendung von Musterzeichen im Objektnamen ist es möglich, dass auf den Namen eines Objektes mehrere Regeln eines Regelbehälters passen. Die Prüfung erfolgt jedoch grundsätzlich in der Reihenfolge, in der die Regeln im Regelbehälter stehen, und wird beim ersten Treffer beendet.

Die Grafik zeigt den aktiven Regelbehälter (ohne Berücksichtigung des Regelattributs TSOS-ACCESS):



– Ein Anwender mit der Benutzerkennung USER1 möchte am Montag die Datei BOOK mitverwalten. Bei der Suche nach einer passenden Regel wird die Zeichenfolge BOO* aus der ersten Regel gegen den Dateinamen BOOK geprüft. Der Name passt, die Suche nach einer weiteren passenden Regel wird beendet, und die Zugriffsbedingung in GUARD1 wird ausgewertet.

  USER1 ist laut Miteigentümerbedingung in GUARD1 Miteigentümer von BOOK.

– Am Dienstag versucht USER2 einen Miteigentümerzugriff auf die Datei BOOK. Wieder wird bei der Miteigentümerüberprüfung der Dateiname BOO* aus der ersten Regel gegen den Dateinamen BOOK geprüft. Der Name passt, die Suche nach einer weiteren passenden Regel wird beendet und die Zugriffsbedingung ausgewertet, die in GUARD1 festgelegt ist.

  USER2 ist laut Miteigentümerbedingung in GUARD1 kein Miteigentümer von BOOK. Die zweite Regel bleibt unberücksichtigt, die USER2 zum Miteigentümer erklärt hätte (GUARD2).

ACHTUNG!
Die Reihenfolge der Regeln innerhalb eines Regelbehälters und in einer Regelbehältersequenz spielt eine entscheidende Rolle bei der Ermittlung der Miteigentümerschaft.

5.6.4.4 Reorganisation aktiver Regelbehälter

Für die Reorganisation der Behälternamen und ihrer Inhalte ist der Anwender selbst verantwortlich.

Ein Beispiel zur Vorgehensweise bei der Reorganisation von Regelbehältern finden Sie im Abschnitt „Reorganisation aktiver Regelbehälter“ auf Seite 466.

5.7 Einschränkung der TSOS-Miteigentümerschaft

Zunehmende Rechnervernetzungen und Rechnerverbünde erlauben es, in immer stärkerem Maße externe RZ-Dienstleistungen (Outsourcing) zu nutzen. Dazu müssen fremden Dienstleistungsunternehmen unter Umständen sicherheitskritische Daten anvertraut werden. Administrationstätigkeiten müssen unter der Benutzerkennung TSOS abgewickelt werden. Ein Benutzer unter der Benutzerkennung TSOS hat aber auf Grund seiner Systemprivilegierung das uneingeschränkte Mitverwaltungsrecht für Dateien und Jobvariablen. Dadurch ist er in der Lage, Schutzmechanismen zu verändern und sich damit Zugriff auf die ihm anvertrauten Daten zu ermöglichen.

Beispiel

Ein DV-Benutzer will seine sicherheitskritische Datei NOT-FOR-TSOS vor Zugriffen durch das fremde RZ-Personal seines Dienstleistungszentrums schützen. Zu diesem Zweck verknüpft er die Datei mit dem Guard GUA. Das Guard verbietet dem Benutzer TSOS alle lesenden, schreibenden und ausführenden Datenzugriffe (siehe Abschnitt „Zugriffs- und Zugangsschutz“ auf Seite 438):

```
/add-access-conditions $customer.gua,subjects=*user(tsos),admission=*no
/modify-file-attributes file-name=$customer.not-for-tsos,         -
/                       protection=(guards=(read=$customer.gua,   -
/                                           write=$customer.gua,  -
/                                           exec=$customer.gua))
```

Auf Grund der systemweiten TSOS-Miteigentümerrechte darf die fremde RZ-Administration unter der Benutzerkennung TSOS die Schutzattribute dieser Datei administrieren und somit auch den Dateischutz entfernen:

```
/modify-file-attributes file-name=$customer.not-for-tsos, -
/                       protection=*par(guards=*none)
```

Ohne Guardsschutz sind dem Benutzer TSOS die Daten der Datei $CUSTOMER.NOT-FOR-TSOS uneingeschränkt zugänglich. Zwar kann eine SAT-Protokollierung Datenzugriffe im Nachhinein sichtbar machen, ein möglicher Schaden kann dadurch aber nicht verhindert werden.

5.7.1 Ziel

Das systemweite Mitverwaltungsrecht des Benutzers TSOS kann eingeschränkt werden. Unter das eingeschränkte Mitverwaltungsrecht fallen Dateien und Jobvariable. Folgende Ziele können dadurch erreicht werden:

– Ein Benutzer unter der Kennung TSOS darf für fremde Kennungen nur noch eine definierbare Menge von Dateien und Jobvariablen administrieren. Die Schutzattribute dieser Menge können nur noch vom Objekteigentümer selber oder den von ihm ernannten Miteigentümern verändert werden.

– Für Dialog- und Batch-Tasks, die unter der Benutzerkennung TSOS ablaufen, wird das TSOS-Mitverwaltungsrecht kontrolliert und gegebenenfalls abgewiesen.

– Für Systemtasks, die mit dem TSOS-Privileg ausgestattet sind, findet keine Überwachung des TSOS-Mitverwaltungsrechtes statt, damit ein normaler Systemablauf aufrecht erhalten bleibt. Deswegen wird im Folgenden von einer **eingeschränkten** TSOS-Miteigentümerschaft gesprochen.

5.7.2 Umfang

Die Einschränkung der TSOS-Miteigentümerschaft wirkt sich auf bestimmte Kommandos und Makros aus, und dort gegebenenfalls nur auf einzelne Operanden. In der folgenden Tabelle sind diese Kommandos und Makros aufgelistet. Eine genaue Auflistung der betroffenen Operanden ist dem Anhang zu entnehmen.

	Kommandos	**Makros**
DVS	MODIFY-FILE-ATTRIBUTES	CATAL (STATE=*UPDATE)
	MODIFY-GENERATION-SUPPORT	CATAL (STATE=*UPDATE)
	MODIFY-FILE-GROUP-ATTRIBUTES	CATAL (STATE=*UPDATE)
	DELETE-FILE	ERASE
	COPY-FILE	COPFILE
JVS	MODIFY-JV-ATTRIBUTES	CATJV (STATE=*UPDATE)
	DELETE-JV	ERAJV

5.7.3 Systemspezifische Einstellungen

Die Wirksamkeit einer eingeschränkten TSOS-Mitverwaltung hängt unter anderem von speziellen Systemschutzeinstellungen ab, die der Sicherheitsbeauftragte (standardmäßig SYSPRIV) vornehmen muss. Denn solange sich ein Benutzer unter der Benutzerkennung TSOS Systemzugang unter fremden Benutzerkennungen verschaffen kann, wäre die Überwachung von TSOS-Miteigentümerzugriffen sinnlos.

Der Sicherheitsbeauftragte muss folgende Privilegienverteilung vornehmen:

– Er muss dem Benutzer TSOS das Recht zur Benutzerverwaltung entziehen. (Privileg USER-ADMINISTRATION)

  Damit wird dem Benutzer TSOS der Zugang zu fremden Benutzerkennungen verwehrt.

– Er muss dem Benutzer TSOS das Recht zur Guard-Administration entziehen. (Privileg GUARD-ADMINISTRATION)

  So kann ein Benutzer TSOS keine fremden Guards administrieren und damit auch keine Schutzeinstellungen in fremden Guards modifizieren.

Genaueres zum Privilegienmanagement ist dem Abschnitt „Privilegien verwalten“ auf Seite 40 zu entnehmen.

5.7.4 Benutzerspezifische Einstellungen

Um ein Objekt (Datei oder Jobvariable) wirksam vor TSOS zu schützen, muss der Objekteigentümer **zwei** benutzerspezifische Schutzeinstellungen vornehmen:

1. Der Objekteigentümer muss dem Benutzer TSOS das **Mitverwaltungsrecht** für seine Objekte entziehen.

   Siehe dazu „Festlegungen für den TSOS-Miteigentümerschutz“ auf Seite 490.

2. Der Objekteigentümer muss dem Benutzer TSOS das **Zugriffsrecht** für seine Objekte entziehen. Hierzu muss der GUARDS-Zugriffsschutz genutzt werden, da nur mit diesem TSOS-Zugriffe unterbunden werden können.

   Diese Einstellung ist aus folgendem Grund erforderlich: Das Entziehen des Mitverwaltungsrechts im 1. Schritt verbietet nur die Modifikation von Schutzattributen. Es verbietet **keine** Datenzugriffe, wie z.B. das Lesen oder Verschlüsseln einer Datei.

   Siehe dazu „Festlegungen für den TSOS-Zugriffsschutz“ auf Seite 492.

Festlegungen für den TSOS-Miteigentümerschutz

Die Einschränkung der TSOS-Miteigentümerschaft basiert auf dem Miteigentümerschutz, das heißt:

– Es muss ein aktiver Regelbehälters mit Namen SYS.UCF (bzw. SYS.UCJ) eingerichtet werden.
(Kommando /CREATE-GUARD)

– Es müssen Miteigentümerregeln definiert werden, aus denen hervorgeht, welche Datei der Benutzer TSOS **nicht** mitverwalten darf.
(Kommando /ADD-COOWNER-PROTECTION-RULE)

In einer Miteigentümerregel kann für ein Objekt sowohl eine Festlegung über Miteigentümerbedingungen für normale Benutzer getroffen werden, als auch eine Festlegung über die Art der TSOS-Miteigentümerschaft. Dazu gliedert sich eine Miteigentümerregel in drei Teile:

1. Regelteil:

   Dieser Regelteil enthält die Angabe, für welche Datei oder Jobvariable eine Miteigentümerschaft festgelegt oder eingeschränkt werden soll.

2. Regelteil

   In diesem Regelteil wird festgelegt, welche Miteigentümerbedingungen **normale Benutzer** erfüllen müssen, um Miteigentümer des im 1. Regelteil genannten Objektes zu sein.

   Die eigentlichen Miteigentümerbedingungen werden dabei in einem eigenen Guard (Typ STDAC) definiert, der 2. Regelteil verweist lediglich auf dieses Guard.

3. Regelteil

   In diesem Regelteil wird festgelegt, ob der **Benutzer TSOS** das volle oder nur ein eingeschränktes Mitverwaltungsrecht für das im 1. Regelteil genannte Objekt besitzt.

   Alternativ sind die beiden Werte *SYSTEM-STD oder *RESTRICTED möglich.

Folgendes ist zu beachten:

– In einer Regel können Angaben für die Miteigentümerschaft nichtprivilegierter Benutzer und des Benutzers unter der Benutzerkennung TSOS alternativ oder gemeinsam festgelegt werden.

– Wird in einer Regel die Miteigentümerschaft für nichtprivilegierte Benutzer festgelegt werden, muss im 2. Regelteil der Verweis auf ein Guard eingetragen sein. Für die TSOS-Miteigentümerschaft sind dieses Guard und die dort festgelegten Miteigentümerbedingungen unbedeutend.

Beispiel

```
/show-coowner-protection-rule rule-container-guard=$customer.sys.ucf

%------------------------------------------------------------------------------
%RULE CONTAINER :2OSC:$CUSTOMER.SYS.UCF              ACTIVE  COOWNER PROTECTION
%------------------------------------------------------------------------------
%RULE1          OBJECT      = COOWNER.*
%               CONDITIONS  = $CUSTOMER.GUA
%               TSOS-ACCESS = SYSTEM-STD    ← von Bedeutung für die
                                              TSOS-Miteigentümerschaft
%------------------------------------------------------------------------------
%RULE CONTAINER SELECTED: 1                                    END OF DISPLAY

/show-access-conditions guard-name=$customer.gua

%:2OSC:$CUSTOMER.GUA
%   User   TSOS         has NO ADMISSION  ← ohne Bedeutung für die
                                            TSOS-Miteigentümerschaft
%------------------------------------------------------------------------------
%Guards selected: 1                                            End of display
```

– Soll in einer Regel **nur die eingeschränkte TSOS-Miteigentümerschaft** festgelegt werden, muss im 2. Regelteil statt eines Guardverweises der Wert *NONE eingetragen werden. Der 3. Regelteil muss auf *RESTRICTED gesetzt werden. Damit wird die Miteigentümerschaft des Benutzer TSOS für das im 1. Regelteil genannte Objekt eingeschränkt.

Beispiel

```
/add-coowner-protection-rule rule-container-guard=sys.ucf, -
/             protection-rule=rule2, -
/             protect-object=*par(name=not-for-tsos, -
/             condition-guard=*none, -
/             tsos-access=*restricted)

/show-coowner-protection-rule rule-container-guard=$customer.sys.ucf

%------------------------------------------------------------------------------
%RULE CONTAINER :2OSC:$CUSTOMER.SYS.UCF              ACTIVE  COOWNER PROTECTION
%------------------------------------------------------------------------------
%RULE1          OBJECT      = COOWNER.*
%               CONDITIONS  = $CUSTOMER.GUA
%               TSOS-ACCESS = SYSTEM-STD
%RULE2          OBJECT      = NOT-FOR-TSOS
%               CONDITIONS   = *NONE
%               TSOS-ACCESS = RESTRICTED
%------------------------------------------------------------------------------
%RULE CONTAINER SELECTED: 1                                    END OF DISPLAY
```

Genaueres zum Miteigentümerschutz finden Sie in Abschnitt „Miteigentümerschutz (Co-owner protection)“ auf Seite 471.

Festlegungen für den TSOS-Zugriffsschutz

Der Schutz vor TSOS-Zugriffen basiert auf dem GUARDS-Zugriffsschutz, das heißt:

– Es muss ein Zugriffsbedingungsguard (Typ STDAC) einrichtet werden.
(Kommando /CREATE-GUARD)

– Darin muss für den Benutzer TSOS (*SUBJECTS) definiert werden, dass er kein Zugriffsrecht besitzen soll.
(Kommando /ADD-ACCESS-CONDITIONS)

– Das Zugriffsbedingungsguard muss mit dem zu schützenden Objekt verknüpft werden.
(Kommando /MODIFY-FILE-ATTRIBUTES)

Genaueres zum GUARDS-Zugriffsschutz finden Sie in Abschnitt „Zugriffs- und Zugangsschutz“ auf Seite 438.

Mit den Schutzmechanismen BACL oder ACCESS/USER-ACCESS können keine TSOS-Zugriffe unterbunden werden.

5.7.5 Überprüfung

Bei Überprüfung der TSOS-Miteigentümerschaft spielen zwei Aspekte eine Rolle:

– Überprüfung der Systemumgebung

– Überprüfung der TSOS-Miteigentümerzugriffe

Überprüfung der Systemumgebung

Für die Auftragsabwicklung werden im System Tasks erzeugt, die zur Erfüllung ihre Aufträge das TSOS-Privileg benutzen (Systemtasks). Auch die unter der Benutzerkennung TSOS ablaufenden Dialog und Batch-Tasks sind mit dem TSOS-Privileg ausgezeichnet. Um den Systemablauf nicht zu gefährden, darf die Überwachung der TSOS-Miteigentümerschaft nur in einer ganz speziellen Systemumgebung vorgenommen werden. Das bedeutet, dass TSOS-Miteigentümerzugriffe nur dann kontrolliert werden, wenn die Task, unter der sie vorgenommen werden, folgende Eigenschaften besitzt:

– sie ist vom Typ DIALOG oder BATCH
und
– sie läuft unter der Benutzerkennung TSOS ab
und
– sie ist mit dem TSOS-Privileg versehen

Für jede andere Task gilt grundsätzlich das uneingeschränktes TSOS-Mitverwaltungsrecht, unabhängig davon, ob eine eingeschränkte TSOS-Miteigentümerschaft festgelegt wurde oder nicht.

Überprüfung der TSOS-Miteigentümerzugriffe

Die Prüflogik des Miteigentümerschutzes für die Benutzerkennung TSOS ist im folgenden Bild dargestellt:

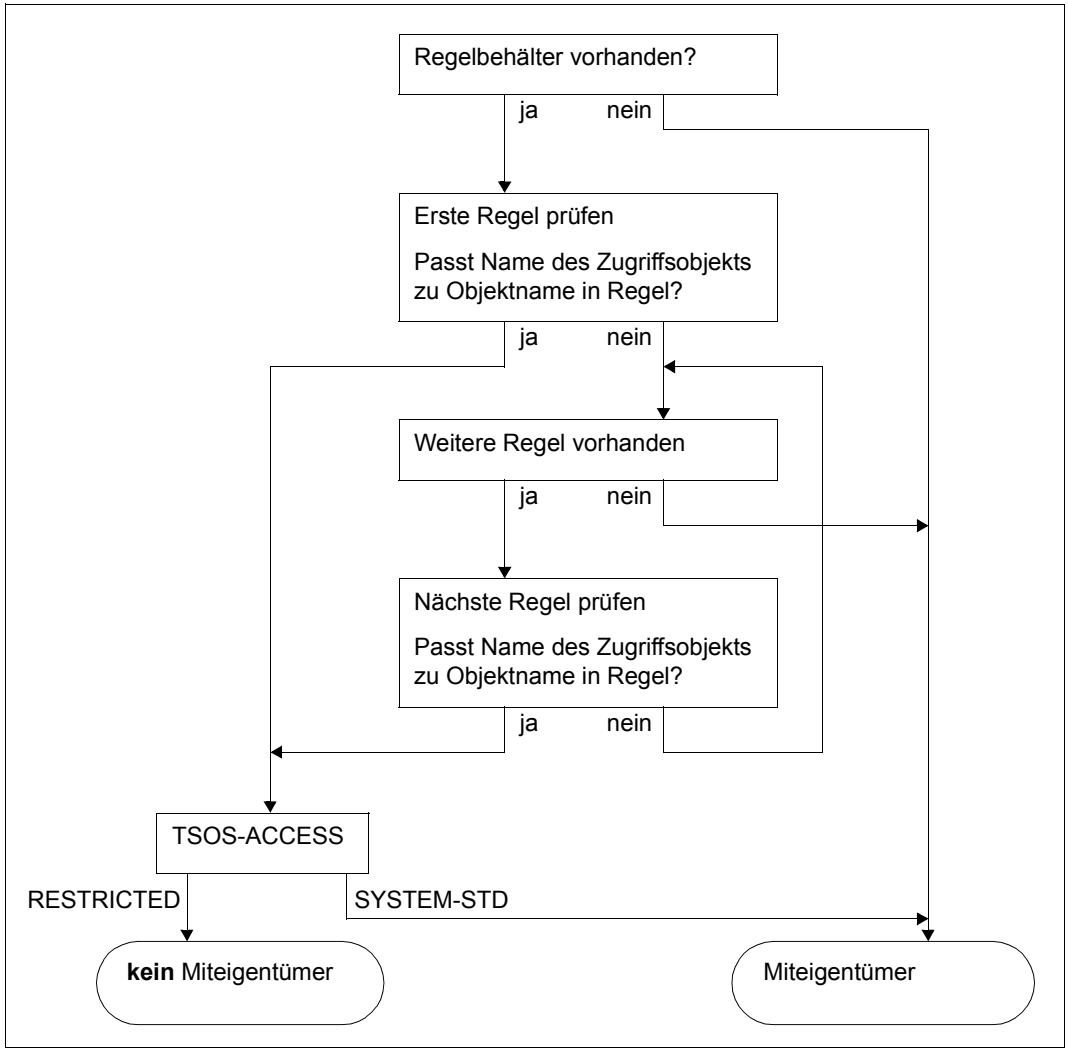


Bild 22: Prüflogik des Miteigentümerschutzes für die Benutzerkennung TSOS

ACHTUNG!
Für die Überprüfung der TSOS-Miteigentümerschaft müssen systemintern aktive Regelbehälter für den Miteigentümerschutz gelesen und ausgewertet werden. Wenn bei einem solchen Lesevorgang ein Systemfehler auftritt, der die notwendige Überprüfung verhindert, behält der Benutzer TSOS sein Mitverwaltungsrecht.

5.7.6 Anwendungsbeispiel

An diesem Beispiel soll demonstriert werden, wie die eingeschränkte TSOS-Miteigentümerschaft festgelegt wird, und wie danach auf TSOS-Zugriffe reagiert wird.

Festlegung der systemspezifischen Einstellungen

Der Sicherheitsbeauftragte (standardmäßig SYSPRIV) entzieht der Benutzerkennung TSOS die beiden Privilegien USER-ADMINISTRATION und GUARD-ADMINISTRATION. Damit kann sich der Benutzer TSOS weder den Zugang zu fremden Benutzerkennungen verschaffen, noch Guards administrieren und damit Guardinhalte verändern:

```
/reset-privilege privilege=(*guard-administration,*user-administration), -
/                user-id=tsos
```

Der Sicherheitsbeauftragte ernennt die Benutzerkennung USERADM zum neuen Benutzerverwalter:

```
/set-privilege privilege=*user-administration, -
/              user-id=useradm
```

Der Sicherheitsbeauftragte ernennt die Benutzerkennung GUARDADM zum neuen Guard-Administrator:

```
/set-privilege privilege=*guard-administration, -
/              user-id=guardadm
```

Festlegung der benutzerspezifischen Einstellungen

– Der Benutzer CUSTOMER gibt sich allein das volle Zugriffsrecht für seine Datei MY-OWN. Die Zugriffsbedingung soll durch das Guard GUA1 geregelt werden.

```
/add-access-conditions guard-name=$customer.gua1,-
/                      subjects=*user(customer), -
/                      admission=*yes
/modify-file-attributes file-name=$customer.my-own, -
/                       protection=*par(guards=(read=$customer.gua1, -
/                                               write=$customer.gua1, -
/                                               exec=$customer.gua1))
```

– Der Benutzer CUSTOMER möchte, dass seine Datei TSOS-ACC-RESTRICTED nur eingeschränkt von TSOS mitverwaltet werden darf.

  Er gibt sich allein das volle Zugriffsrecht für seine Datei TSOS-ACC-RESTRICTED. Die Zugriffsbedingung wird ebenfalls durch das Guard GUA1 geregelt.

```
/add-coowner-protection-rule rule-container-guard=$customer.sys.ucf, -
/                            protection-rule=rule1, -
/                            protect-object=(name=tsos-acc-restricted, -
/                                            condition-guard=*none, -
/                                            tsos-access=*restricted)
/modify-file-attributes file-name=$customer.tsos-acc-restricted, -
/                       protection=*par(guards=(read=gua1, -
/                                               write=gua1, -
/                                               exec=gua1))
```

– Der Benutzer CUSTOMER macht einen Fehler. Er möchte zwar, dass auch seine Datei TSOS-ERROR nur eingeschränkt von TSOS mitverwaltet wird. Er **vergisst** aber, die Datei mit dem Guard GUA1 zu verknüpfen. Deshalb hat TSOS zwar ein eingeschränktes Mitverwaltungsrecht, behält aber das volle Zugriffsrecht für die Datei.

```
/add-coowner-protection-rule $customer.sys.ucf, -
/                             protection-rule=rule2, -
/                             protect-object=(name=tsos-error, -
/                                             condition-guard=*none, -
/                                             tsos-access=*restricted)
```

Zusammenfassung der benutzerspezifischen Einstellungen

Nachdem der Benutzer CUSTOMER die beschriebenen Einstellungen vorgenommen hat, haben seine Dateien die folgenden Schutzattribute:

– Datei $CUSTOMER.MY-OWN

```
/show-file-attributes file-name=$customer.my-own, -
/                     information=(security=*yes)

%00000003 :2OSC:$CUSTOMER.MY-OWN
%  ------------------------------ SECURITY     --------------------------------
%  READ-PASS  = NONE         WRITE-PASS = NONE         EXEC-PASS  = NONE
%  USER-ACC   = OWNER-ONLY   ACCESS     = WRITE        ACL        = NO
%  AUDIT      = NONE         FREE-DEL-D = *NONE        EXPIR-DATE = 2018-03-23
%  DESTROY    = NO           FREE-DEL-T = *NONE        EXPIR-TIME =   00:00:00
%  SP-REL-LOCK= NO
%  GUARD-READ = $CUSTOMER.GUA1
%  GUARD-WRIT = $CUSTOMER.GUA1
%  GUARD-EXEC = $CUSTOMER.GUA1
```

– Datei $CUSTOMER.TSOS-ACC-RESTRICTED

```
/show-file-attributes file-name=$customer.tsos-acc-restricted, -
/                     information=(security=*yes)

%00000003 :2OSC:$CUSTOMER.TSOS-ACC-RESTRICTED
%  ------------------------------ SECURITY     --------------------------------
%  READ-PASS  = NONE         WRITE-PASS = NONE         EXEC-PASS  = NONE
%  USER-ACC   = OWNER-ONLY   ACCESS     = WRITE        ACL        = NO
%  AUDIT      = NONE         FREE-DEL-D = *NONE        EXPIR-DATE = 2018-03-23
%  DESTROY    = NO           FREE-DEL-T = *NONE        EXPIR-TIME =   00:00:00
%  SP-REL-LOCK= NO
%  GUARD-READ = $CUSTOMER.GUA1
%  GUARD-WRIT = $CUSTOMER.GUA1
%  GUARD-EXEC = $CUSTOMER.GUA1
End of display
```

– Datei $CUSTOMER.TSOS-ERROR

```
/show-file-attributes file-name=$customer.tsos.error, -
/                     information=(security=*yes)

%00000003 :2OSC:$CUSTOMER.TSOS-ERROR
%  ------------------------------ SECURITY     --------------------------------
%  READ-PASS  = NONE         WRITE-PASS = NONE         EXEC-PASS  = NONE
%  USER-ACC   = OWNER-ONLY   ACCESS     = WRITE        ACL        = NO
%  AUDIT      = NONE         FREE-DEL-D = *NONE        EXPIR-DATE = 2018-03-23
%  DESTROY    = NO           FREE-DEL-T = *NONE        EXPIR-TIME =   00:00:00
%  SP-REL-LOCK= NO
```

– Guard $CUSTOMER.GUA1
/**show-access-conditions guard-name=$customer.gua1**

```
%:2OSC:$CUSTOMER.GUA1
%   User   CUSTOMER has ADMISSION
%------------------------------------------------------------------------------
%Guards selected: 1
```

– Regelbehälter $CUSTOMER.SYS.UCF
/**show-coowner-protection-rule rule-container-guard=$customer.sys.ucf**

```
%------------------------------------------------------------------------------
%RULE CONTAINER :2OSC:$CUSTOMER.SYS.UCF              ACTIVE  COOWNER PROTECTION
%------------------------------------------------------------------------------
%RULE1         OBJECT      = TSOS-ACC-RESTRICTED
%              CONDITIONS  = *NONE
%              TSOS-ACCESS = RESTRICTED
%RULE2         OBJECT      = TSOS-ERROR
%              CONDITIONS  = *NONE
%              TSOS-ACCESS = RESTRICTED
%------------------------------------------------------------------------------
%RULE CONTAINER SELECTED: 1                                    END OF DISPLAY
```

TSOS-Zugriffe und Reaktionen

Der Benutzer TSOS unternimmt folgende Zugriffsversuche auf die Dateien des Benutzers CUSTOMER:

/**show-file $customer.my-own**

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  SHO0003 'DMS' REPORTED ERROR '0666'. COMMAND NOT PROCESSED
```

Grund:
Die Datei wird durch das Guard $CUSTOMER.GUA1 geschützt, in dem nur für CUSTOMER eine Zugriffsbedingung definiert ist. Für TSOS ist daher der **Daten**zugriff verboten.

/**modify-file-attributes file-name=$customer.my-own,guard=*none**

Ergebnis:
Die Änderung wird **durchgeführt**.

Grund:
Der aktive Miteigentümerregelbehälter unter der Benutzerkennung CUSTOMER enthält keine Regel für die Datei $CUSTOMER.MY-OWN. TSOS besitzt daher standardmäßig die uneingeschränkte Erlaubnis für **Miteigentümer**zugriffe.

```
/show-file file-name=$customer.tsos-acc-restricted
```

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  SHO0003 'DMS' REPORTED ERROR '0666'. COMMAND NOT PROCESSED
```

Grund:
Die Datei wird durch das Guard $CUSTOMER.GUA1 geschützt, in dem nur für CUSTOMER eine Zugriffsbedingung definiert ist. Für TSOS ist daher der **Daten**zugriff verboten.

```
/modify-file-attributes file-name=$customer.tsos-acc-restricted,guards=*none
```

Ergebnis:
Die Änderung wird **abgelehnt**.

```
%  DMS0681 DMS ERROR '05CB' WHEN ACCESSING FILE ':A:$CUSTOMER.TSOS-ACC-RESTRICTED'.
FOR FURTHER INFORMATION: /HELP-MSG DMS05CB
```

Grund:
Der aktive Miteigentümerregelbehälter unter der Benutzerkennung CUSTOMER enthält eine Regel, die das TSOS-Miteigentümerrecht für die Datei einschränkt. Daher ist für TSOS der **Miteigentümer**zugriff verboten.

```
/copy-file from-file=$customer.tsos-acc-restricted,to-file=$tsos.new-file
```

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  DMS0666 REQUESTED ACCESS TO FILE NOT PERMITTED DUE TO EXISTING FILE PROTECTION.
COMMAND NOT PROCESSED
```

Grund:
Die Datei wird durch das Guard $CUSTOMER.GUA1 geschützt, in dem nur für CUSTOMER eine Zugriffsbedingung definiert ist. Für TSOS ist daher der **Daten**zugriff verboten.

```
/copy-file from-file=$customer.tsos-acc-restricted, -
/          to-file=$tsos.new-file, -
/          ignore-protection=*source-file
```

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  DMS0666 REQUESTED ACCESS TO FILE NOT PERMITTED DUE TO EXISTING FILE PROTECTION.
COMMAND NOT PROCESSED
```

Grund:
Die Datei $CUSTOMER.TSOS-ACC-RESTRICTED wird durch das Guard $CUSTOMER.GUA1 geschützt, in dem nur für CUSTOMER eine Zugriffsbedingung definiert ist. Für TSOS ist daher der **Daten**zugriff verboten.
TSOS versucht zwar, diesen Schutz durch Angabe des Operanden IGNORE-PROTECTION zu umgehen, aber der aktive Miteigentümerregelbehälter unter der Benutzerkennung CUSTOMER enthält eine Regel, die das TSOS-Miteigentümerrecht für die Datei einschränkt. Daher ist für TSOS der **Miteigentümer**zugriff, also auch die Verwendung des Operanden IGNORE-PROTECTION, verboten.

```
/delete-file file-name=$customer.tsos-acc-restricted
```

Ergebnis:

Der Zugriff wird **abgelehnt**.

```
%  DMS0801 ERROR WHEN DELETING FILE ':A:$CUSTOMER.TSOS-ACC-RESTRICTED'
%  DMS0666 REQUESTED ACCESS TO FILE NOT PERMITTED DUE TO EXISTING FILE PROTECTION.
COMMAND NOT PROCESSED
```

Grund:
Die Datei wird durch das Guard $CUSTOMER.GUA1 geschützt, in dem nur für CUSTOMER eine Zugriffsbedingung definiert ist. Für TSOS ist daher der **Daten**zugriff verboten.

```
/delete-file file-name=$customer.tsos-acc-restricted, -
/            ignore-protection=*access
```

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  DMS0801 ERROR WHEN DELETING FILE ':A:$CUSTOMER.TSOS-ACC-RESTRICTED'
%  DMS0666 REQUESTED ACCESS TO FILE NOT PERMITTED DUE TO EXISTING FILE PROTECTION.
COMMAND NOT PROCESSED
```

Grund:
Der aktive Miteigentümerregelbehälter unter der Benutzerkennung CUSTOMER enthält eine Regel, die das TSOS-Miteigentümerrecht für die Datei einschränkt. Daher ist für TSOS der **Miteigentümer**zugriff, also auch die Verwendung des Operanden IGNORE-PROTECTION, verboten.

```
/show-file file-name=$customer.tsos-error
```

Ergebnis:

Der Zugriff wird **durchgeführt**, d.h. die Datei wird angezeigt.

Grund:
Es wurde vergessen, die Datei mit einem GUARDS-Zugriffsschutz zu versehen. Deshalb besitzt TSOS die standardmäßig uneingeschränkte Erlaubnis für **Daten**zugriffe.

```
/modify-file-attributes file-name=$customer.tsos-error,guards=*none
```

Ergebnis:
Der Zugriff wird **abgelehnt**.

```
%  DMS0681 DMS ERROR '05CB' WHEN ACCESSING FILE ':A:$CUSTOMER.TSOS-ACC-RESTRICTED'.
FOR FURTHER INFORMATION: /HELP-MSG DMS05CB
```

Grund:
Der aktive Miteigentümerregelbehälter unter der Benutzerkennung CUSTOMER enthält eine Regel, die das TSOS-Miteigentümerrecht für die Datei einschränkt. Daher ist für TSOS der **Miteigentümer**zugriff verboten.

```
/copy-file from-file=$customer.tsos-error,to-file=$tsos.new-file
```

Ergebnis:
Der Zugriff wird **durchgeführt**.

Grund:
Es wurde vergessen, die Datei mit einem GUARDS-Zugriffsschutz zu versehen. Deshalb besitzt TSOS die standardmäßig uneingeschränkte Erlaubnis für **Daten**zugriffe.

```
/copy-file from-file=$customer.tsos-error, -
/          to-file=$tsos.new-file, -
/          ignore-protection=*source-file
```

Ergebnis:
Der Zugriff wird **durchgeführt**, d.h. die Datei wird angezeigt.

Grund:
Es wurde vergessen, die Datei mit einem GUARDS-Zugriffsschutz zu versehen. Deshalb besitzt TSOS die standardmäßig uneingeschränkte Erlaubnis für **Daten**zugriffe. Die Verwendung des Operanden IGNORE-PROTECTION ist hier unbedeutend, denn es kann kein Schutz ignoriert werden, der gar nicht gesetzt ist.

```
/delete-file file-name=$customer.tsos-error
```

Ergebnis:
Der Zugriff wird **durchgeführt**.

Grund:
Es wurde vergessen, die Datei mit einem GUARDS-Zugriffsschutz zu versehen. Deshalb besitzt TSOS die standardmäßig uneingeschränkte Erlaubnis für **Daten**zugriffe.

```
/delete-file file-name=$customer.tsos-error,ignore-protection=*access
```

Ergebnis:
Der Zugriff wird **durchgeführt**.

Grund:
Es wurde vergessen, die Datei mit einem GUARDS-Zugriffsschutz zu versehen. Deshalb besitzt TSOS die standardmäßig uneingeschränkte Erlaubnis für **Daten**zugriffe. Die Verwendung des Operanden IGNORE-PROTECTION ist hier unbedeutend, denn es kann kein Schutz ignoriert werden, der gar nicht gesetzt ist.

5.7.7 Sicherung und Restaurierung von Guards mit GUARDS-SAVE

Für die Sicherung von Guards mit GUARDS-SAVE gilt:

Alle Guards können durch den Benutzer TSOS mit GUARDS-SAVE **vollständig gesichert** werden.

Bei der Restaurierung von Guards mit GUARDS-SAVE gilt für Regelbehälter der Miteigentümerschaft:

5.7.8 Sicherung mit HSMS/ARCHIVE

Systemsicherungen oder Restaurierungen durch den Benutzer TSOS sind möglich.

Das Kriterium zur Einschränkung der TSOS-Miteigentümerschaft ist nicht direkt mit der Datei bzw. Jobvariable verbunden. Es ist in einem aktiven Regelbehälter (Guard) für den Miteigentümerschutz hinterlegt. Es ist zu beachten, dass bei einer HSMS/ARCHIVE-Sicherung keine einzelnen Regelbehälter erfasst werden können, sondern nur der GUARDS-Systemkatalog in seiner Gesamtheit.

5.7.9 Rechnerverbünde

Sicherheitskritische Dateien können nicht zuverlässig vor TSOS-Zugriffen geschützt werden, wenn im Rechnerverbund unterschiedliche SECOS-Versionen eingesetzt sind.

5.8 GUARDS administrieren

5.8.1 Guardskatalog

GUARDS legt Guards in einem Systemkatalog ($TSOS.SYSCAT.GUARDS) ab. GUARDS verwaltet pro Pubset einen solchen Guardskatalog. Der Guardskatalog wird mit Importieren des Pubsets geöffnet und bleibt offen bis zum Exportieren des Pubsets oder bis zum Beenden des Subsystems GUARDS (durch Systemlaufbeendigung).

Wird während des Betriebs von GUARDS ein neues Pubset importiert, auf dem kein Guardskatalog existiert, wird ein neuer, leerer Katalog angelegt.

Falls der Guardskatalog auf dem Pubset mit BLKSIZE=(STD,2) katalogisiert ist, so wird er umkatalogisiert und erhält den Namen SYSCAT.GUARDS.datum.uhrzeit. Dann wird er in einen neuen Guardskatalog mit BLKSIZE=(STD,4) und dem Namen SYSCAT.GUARDS kopiert. Dieser wird so zum aktuellen Guardskatalog.

Fehler, die beim Öffnen des Guardskatalogs auftreten können, sind im Abschnitt „Fehler bei der Initialisierung des Subsystems“, Seite 511ff, beschrieben.

5.8.2 Guardskatalog wechseln

Ein bestehender Guardskatalog kann vom Guard-Administrator mit dem Kommando /CHANGE-GUARD-FILE gegen einen anderen ausgetauscht werden, siehe Seite 558ff.

5.8.3 Guardskatalog wiederherstellen

Ein Guardskatalog, der sich in einem inkonsistenten Zustand befindet, kann vom System- oder Guard-Administrator mit dem Kommando /REPAIR-GUARD-FILE wiederhergestellt werden, siehe Seite 619ff.

5.8.4 Sicherung mit ARCHIVE

ARCHIVE erkennt einen Guardskatalog und sperrt ihn während der Sicherung gegen Schreibzugriffe, damit ein konsistenter Stand gesichert wird. Während der Sicherung sind nur Lesezugriffe möglich.

Eine selektivere Möglichkeit der Sicherung bietet GUARDS-SAVE (siehe Seite 881ff).

Soll ein mit ARCHIVE gesicherter Guardskatalog wieder rekonstruiert werden, so muss er zuerst unter dem Namen SYSCAT.GUARDS.BAK unter der Kennung TSOS rekonstruiert werden, um ihn anschließend mit dem Kommando CHANGE-GUARD-FILE zu aktivieren (siehe Seite 558ff).

5.8.5 GUARDS mit MSCF und SPVS

Mit Ausnahme der Administratorkommandos /CHANGE-GUARD-FILE, /REPAIR-GUARD-FILE, /SHOW-GUARD-MANAGEMENT-STATUS, /SHOW-EVALUATED-CONDITIONS und dem Makro CHKSAC sind alle Kommandos und Makros in einem MSCF-Verbund verwendbar. Ob die im Guard-Namen angegebene Benutzerkennung existiert, kann im MSCF-Verbund nur für Shared-Pubset-Betrieb überprüft werden.

In einem Verbund von Rechnern mit abgestimmter Umgebung wird vorausgesetzt, dass Datum und Uhrzeit in allen Rechnern übereinstimmen.

Verschiedene SECOS-Versionen im MSCF-Verbund

ACHTUNG!
Bei einem Einsatz von SECOS V5.3 auf einem Rechner im Rechnerverbund wird dringend empfohlen, auch auf allen anderen beteiligten Rechnern SECOS V5.3 einzusetzen.

5.8.6 GUARDS und RFA

Folgende Kommandos und Makros sind uneingeschränkt RFA-fähig:

Kommando	**Makro**
CREATE-GUARD	CREGUAD
DELETE-GUARD	DELGUAD
SHOW-GUARD-ATTRIBUTES	
ADD-ACCESS-CONDITIONS	MODSAC
MODIFY-ACCESS-CONDITIONS	MODSAC
REMOVE-ACCESS-CONDITIONS	REMSAC
SHOW-ACCESS-ADMISSION	
SHOW-ACCESS-CONDITIONS	

Die folgenden Kommandos und Makros sind nur unter den angegebenen Bedingungen RFA-fähig:

COPY-GUARD oder Makro COPGUAD
Ziel- und Quell-Guard müssen auf demselben Rechner lokal zugreifbar sein.

MODIFY-GUARD-ATTRIBUTES oder Makro MODGUAD
Soll ein Guard umbenannt werden, so müssen Ziel- und Quell-Guard auf demselben Rechner lokal zugreifbar sein.

Makro SHWGUAD
Die Größe des Ausgabebereichs ist abhängig von RFA (maximal 64KB). Ist der Ausgabebereich größer als die maximale Blockgröße in RFA, wird pro Aufruf der Übertragung nur Information von maximal 64KB übertragen. Die verbliebene Information kann durch wiederholten Aufruf übertragen werden. Auf diese Weise geht keine Information des Makros verloren.

Makro SHWSAC
Die Größe des Ausgabebereichs ist abhängig von RFA (maximal 64KB). Ist der Ausgabebereich größer als die maximale Blockgröße in RFA, wird pro Aufruf der Übertragung nur Information von maximal 64KB übertragen. Die verbliebene Information kann durch wiederholten Aufruf übertragen werden. Auf diese Weise geht keine Information des Makros verloren.

Alle übrigen Kommandos und Makros sind nicht RFA-fähig. Das sind insbesondere alle Kommandos und Makros des Standardschutzes und des Miteigentümerschutzes.

5.8.7 GUARDS und SMS

Im BS2000 gibt es Single-Feature-Pubsets (SF-Pubsets) und System-Managed-Pubsets (SM-Pubsets). SM-Pubsets werden wie SF-Pubsets über ihre Katalogkennung angesprochen.

Ein SF-Pubset besteht aus einer oder mehreren Platten, die in den wesentlichen Eigenschaften (Plattenformat, Allokierungseinheit, Verfügbarkeit) übereinstimmen müssen. Ein SM-Pubset kann im Gegensatz dazu aus mehreren so genannten Volume-Sets mit unterschiedlichen Eigenschaften bestehen. Nur innerhalb eines Volume-Sets müssen die wesentlichen Eigenschaften der Platten übereinstimmen.

Wenn ein Benutzer volume-set-spezifische Eigenschaften für eine Datei auf einem SM-Pubset festlegt, ermittelt das System einen zu diesen Eigenschaften passenden Volume-Set des SM-Pubsets und legt die Datei dort ab. Dadurch ist es insbesondere möglich, eine Datei auf einen unterschiedlich performanten Datenträger innerhalb desselben SM-Pubsets zu verschieben, ohne den Namen der Datei ändern zu müssen.

Zum Generieren von SM-Pubsets steht der Systembetreuung das Dienstprogramm SMPGEN zur Verfügung, mit dem auch mehrere bereits bestehende SF-Pubsets zu einem SM-Pubset zusammengefasst werden können.

Voraussetzung für die Zusammenfassung ist, dass auf den betreffenden SF-Pubsets keine Dateien gleichen Namens existieren. Eine Ausnahme von dieser Bedingung bilden u.a. die Systemkataloge von GUARDS, die die Guards enthalten. Da sie auf jedem SF-Pubset unter demselben Namen eingetragen sind, werden sie bei der Generierung eines SM-Pubsets von SMPGEN zu einem einzigen Systemkatalog zusammengefasst.

Voraussetzung für die Zusammenführung der GUARDS-Kataloge ist, dass in ihnen keine Guards gleichen Namens existieren. Ist diese Voraussetzung nicht erfüllt, müssen die betroffenen Guards zuvor von ihren Eigentümern umbenannt werden.

Bei einer Zusammenführung von SF-Pubsets zu einem SM-Pubset werden in den Guards automatisch die Pfadnamen angepasst, die in den Zugriffsbedingungen PROGRAM definiert sind. Die Anpassung besteht darin, dass die Katalogkennung des SF-Pubsets durch die des SM-Pubsets ersetzt wird. Dabei sind unbedingt die Hinweise zu beachten, die im Handbuch „Dienstprogramme“ [15] bei SMPGEN beschrieben sind.

Zur Erkennung von Namensduplikaten und Konflikten bei der automatischen Korrektur der Pfadnamen bietet SMPGEN die Möglichkeit, vor der tatsächlichen Zusammenführung eine Prüfung mit Protokollierung aller Konfliktsituationen durchzuführen. Diese Prüfung kann sowohl von der Systembetreuung als auch von jedem anderen Benutzer vorgenommen werden.

Nähere Informationen zu SM-Pubsets finden Sie im Handbuch „SMS“ [33].

Informationen zum Dienstprogramm SMPGEN finden Sie in den Handbüchern „Dienstprogramme“ [15] und „SMS“ [33].

5.9 SSINFO-Datei

Die SSINFO-Datei wird beim Importieren eines Pubset gelesen. Über sie kann gesteuert werden, wie viele Pubsets (d. h. wie viele GUARDS-Kataloge) jeweils von einer eigenen GUARDS-Servertask bearbeitet werden sollen. Standardmäßig wird für jedes importierte Pubset eine eigene GUARDS-Servertask zur Bearbeitung des auf dem Pubset angelegten GUARDS-Katalogs aufgebaut.

In der SSINFO-Datei werden die Steuerparameter in Form von ISP-Kommandos angegeben. Die SSINFO-Datei wird mit einem gängigen Editor bearbeitet. Zusätzlich kann die Datei Kommentare enthalten.

Datei- und Verarbeitungseigenschaften

Die SSINFO-Datei ist eine SAM-Datei. Die Datensätze der SSINFO-Datei haben variable Länge. Eine Shared-Update-Verarbeitung ist nicht nötig, da beim Subsystem-Start und beim Importieren nur lesend auf die SSINFO-Datei zugegriffen wird.

Dateieigenschaften:

– Zugriffsmethode ist SAM
– Satzformat ist variable Länge
– Blocklänge ist 2048 Byte

Verarbeitungseigenschaften:

– keine Shared-Update-Verarbeitung

Aufbau der SSINFO-Datei

Die ersten Datensätze der SSINFO-Datei beginnen mit „*“, sind somit als Kommentar gekennzeichnet, und enthalten einen Hilfetext für die Spezifikation der Steuerparameter.

Außer Kommentarzeilen kann die SSINFO-Datei nur noch folgendes Kommando enthalten:

```
SET-TASK-DISTRIBUTION PUBSET = list-poss(16): <catid 1..4> / *HOME
```

Mit diesem Kommando werden die Pubsets zusammengefasst, die von einer GUARDS-Servertask bedient werden sollen. *HOME bezeichnet den Home-Pubset. Bei Angabe von *HOME braucht die SSINFO-Datei nicht angepasst werden, wenn sich der Home-Pubset ändert.

Eine GUARDS-Servertask kann maximal 16 Pubsets verwalten. Der Operand PUBSET hat die maximale Länge von 255 Zeichen.

Mehrere Single-Feature-Pubsets (SF-Pubsets) können zu einem System-Managed-Pubset (SM-Pubset) zusammengefasst werden. In diesem Fall werden die ehemaligen SF-Pubsets nur noch über die Katalogkennung des SM-Pubsets angesprochen.

ACHTUNG!
Wird ein SM-Pubset generiert, so muss die Systembetreuung darauf achten, dass das Kommando SET-TASK-DISTRIBUTION in der SSINFO-Datei entsprechend angepasst wird.

Verhalten bei fehlerhaften Steuerparametern

Falls fehlerhafte Steuerparameter in der SSINFO-Datei eingetragen sind, gilt für die betroffenen Pubsets die Defaultregelung: für jeden Pubset wird eine GUARDS-Servertask erzeugt.

Eine Aktualisierung der SSINFO-Datei bzw. eine Korrektur der fehlerhaften Steuerparameter findet nicht statt. Kann die SSINFO-Datei nicht ausgewertet werden, wird dies mit einer Meldung auf die Konsole protokolliert.

5.10 GUARDS - Installation und Inbetriebnahme

Benötigte Dateien

- Subsystem GUARDS

Datei	Name der Datei
Subsystemkatalog	$TSOS.SYSSSC.GUARDS.nnn
Subsystembibliothek – für SU /390 und S-Server – für SU x86 und SQ-Server	 $TSOS.SYSLNK.GUARDS.nnn $TSOS.SKMLNK.GUARDS.nnn
Makrobibliothek	$TSOS.SYSLIB.GUARDS.nnn
Syntaxdatei	$TSOS.SYSSDF.GUARDS.nnn
Meldungsdatei	$TSOS.SYSMES.GUARDS.nnn
Korrekturdatei	$TSOS.SYSRMS.GUARDS.nnn
IMON-Datei	$TSOS.SYSSII.GUARDS.nnn
SSINFO-Datei	$TSOS.SYSSSI.GUARDS.nnn

Tabelle 11: Installationsdateien für GUARDS (nnn = Version des Subsystems)

- Subsystem GUARDDEF

Datei	Name der Datei
Subsystemkatalog	$TSOS.SYSSSC.GUARDDEF.nnn
Subsystembibliothek – für SU /390 und S-Server – für SU x86 und SQ-Server	 $TSOS.SYSLNK.GUARDDEF.nnn $TSOS.SKMLNK.GUARDDEF.nnn
Makrobibliothek	$TSOS.SYSLIB.GUARDDEF.nnn
Syntaxdatei	$TSOS.SYSSDF.GUARDDEF.nnn
Meldungsdatei	$TSOS.SYSMES.GUARDDEF.nnn
Korrekturdatei	$TSOS.SYSREP.GUARDDEF.nnn
IMON-Datei	$TSOS.SYSSII.GUARDDEF.nnn
SSINFO-Datei	$TSOS.SYSSSI.GUARDDEF.nnn

Tabelle 12: Installationsdateien für GUARDDEF (nnn = Version des Subsystems)

- Subsystem GUARDCOO

Datei	Name der Datei
Subsystemkatalog	$TSOS.SYSSSC.GUARDCOO.nnn
Subsystembibliothek – für SU /390 und S-Server – für SU x86 und SQ-Server	 $TSOS.SYSLNK.GUARDCOO.nnn $TSOS.SKMLNK.GUARDCOO.nnn
Makrobibliothek	$TSOS.SYSLIB.GUARDCOO.nnn
Syntaxdatei	$TSOS.SYSSDF.GUARDCOO.nnn
Meldungsdatei	$TSOS.SYSMES.GUARDCOO.nnn
Korrekturdatei	$TSOS.SYSREP.GUARDCOO.nnn
IMON-Datei	$TSOS.SYSSII.GUARDCOO.nnn
SSINFO-Datei	$TSOS.SYSSSI.GUARDCOO.nnn

Tabelle 13: Installationsdateien für GUARDCOO (nnn = Version des Subsystems)

Für die Generierung wird folgende Datei benötigt:

– Subsystemkatalog
Der Subsystemkatalog enthält die Beschreibung des Subsystems aus der Sicht vom DSSM.

Für die Installation werden folgende Dateien benötigt:

– Subsystembibliothek
In der Subsystembibliothek wird der gebundene Großmodul mit dem Namen GUARDS, GUARDDEF bzw. GUARDCOO hinterlegt. Der Name dieser Bibliothek muss im Subsystemkatalog eingetragen werden.

– SDF-Syntaxdatei
Die Syntaxdatei enthält die Beschreibung der Kommandosyntax des jeweiligen Subsystems.

– Meldungsdatei
Die Meldungsdatei enthält die Meldungen des jeweiligen Subsystems.

– Korrekturdatei (Rep-Datei)
Der Subsystemkatalog soll standardmäßig einen Korrekturdateinamen enthalten, auch wenn keine Korrekturdatei vorhanden ist.

– SSINFO-Datei (optional)
  In der SSINFO-Datei können Angaben gemacht werden, wie viele Pubsets (d. h. wie viele GUARDS-Kataloge) jeweils von einer eigenen GUARDS-Servertask verwaltet werden.
  Einzelheiten über die SSINFO-Datei sind dem Abschnitt „SSINFO-Datei“ auf Seite 507 zu entnehmen.

Anmerkungen

Wird der Name einer SSINFO-Datei im Subsystemkatalog angegeben, muss die Datei beim Subsystemstart auch vorhanden sein. Andernfalls wird der Ladevorgang durch DSSM abgebrochen.

Fehler bei der Initialisierung des Subsystems GUARDS

Fehlerbild: Das Laden des Subsystems wird mit der Fehlermeldung PRO6007 abgebrochen.

Auswirkung: In dieser Sitzung antwortet GUARDS auf alle Anfragen einer Objektverwaltung mit einer negativen Antwort.

Ursachen: In der Meldung PRO6007 wird als Einfügung die Fehlerklasse mit ausgegeben. Die genauere Ursache ist dem SERSLOG-Eintrag zu entnehmen:

01 Fehler beim Anmelden des Task-Locks.

02 Fehler beim Anmelden des Subsystems bei der Task-Verwaltung.

03 Fehler beim Lesen des Home-Pubsets.

04 Fehler bei der Ermittlung der Hardware-Basis, auf der die BS2000-Version abläuft (/390, x86).

05 Fehler bei der Ermittlung der laufenden BS2000-Version

06 Fehler beim Anmelden der Standardbedingungsverwaltung.

Fehler bei der Initialisierung der GUARDS-Verwaltung

Fehlerbild: Die Initialisierung der GUARDS-Verwaltung eines Pubsets wird mit der Fehlermeldung PRO6002 abgebrochen.

Auswirkung: Die Initialisierung der GUARDS-Verwaltung eines Pubsets startet die IMCAT-Verarbeitung. Tritt ein Fehler auf, wird der Operator durch die Meldung PRO6002 benachrichtigt und gefragt, ob die IMCAT-Verarbeitung ohne die GUARDS-Verwaltung fortgesetzt werden soll. Wird die Frage bejaht, antwortet GUARDS in dieser Sitzung auf alle Anfragen einer Objektverwaltung mit einer negativen Antwort.

Ursachen: In der Meldung PRO6002 wird als Einfügung die Fehlerklasse ausgegeben. Die genauere Ursache ist dem SERSLOG-Eintrag zu entnehmen:

01 Der Task-Lock für die Zugriffe auf subsystemspezifische, globale Tabellen konnte nicht belegt bzw. freigegeben werden.

02 Die Pubset-Tabelle konnte nicht angelegt, gefunden oder eingekettet werden.

03 Fehler beim Überprüfen des Guardskatalogs $TSOS.SYSCAT.GUARDS.
- /01: Die Datei ist kein Guardskatalog
- /03: Die Versionsnummer des Guardskatalogs wird nicht unterstützt
- /05: Interner Fehler
- /06: Der GUARDS-Katalog liegt nicht auf dem Control-Volume-Set eines SM-Pubsets
- /DMSxxxx: Der DMS-Fehlercode gibt nähere Auskünfte

04 Fehler bei der Erzeugung der Servertask oder beim Verbindungsaufbau mit der Servertask.
- /01: Parameterfehler
- /02: Fehler beim Task-Lock-Aufruf
- /03: Fehler beim Erzeugen der TSN
- /04: Fehler beim Erzeugen der Task
- /05: Fehler beim Anfordern von Speicherplatz
- /06: Pubset-Tabelle existiert nicht
- /07: Servertask antwortet nicht

05 Fehler beim Öffnen des Guardskatalogs; falls ein DMS-Fehler auftrat, wird der DMS-Fehlercode mit ausgegeben.

06 Interner Fehler beim Verbindungsaufbau.

Maßnahmen: Trat der Fehler während der IMCAT-Verarbeitung auf, ist die Verarbeitung abzubrechen und die IMCAT-Verarbeitung erneut einzuleiten.

Bei der Ursache 03 muss geprüft werden, ob eine Datei mit dem Namen $TSOS.SYSCAT.GUARDS existiert, die kein Guardskatalog ist. Diese Datei ist dann umzubenennen.

Abnormale Terminierung einer GUARDS-Servertask

Auf den Guardskatalog wird über eine Servertask zugegriffen. Fällt eine Servertask aus, werden die globalen Tabellen bereinigt und die GUARDS-Verwaltung der von dieser Servertask bedienten Pubsets abnormal beendet. Dieses Ereignis wird mit der Meldung PRO6006 auf der Konsole dokumentiert.

Fehlerbild: Servertask wird mit der Fehlermeldung PRO6006 abgebrochen.

Auswirkung: In dieser Sitzung antwortet GUARDS auf alle Anfragen einer Objektverwaltung mit einer negativen Antwort.

Ursachen: Die Ursache kann nur nach Analyse der System-Dumps festgestellt werden. Bitte informieren Sie Ihren Systemkundendienst.

Maßnahmen: Es gibt zwei Möglichkeiten:

01 Pubset exportieren und anschließend neu importieren

02 Durch das Administrationskommando /REPAIR-GUARD-FILE die Verwaltung des Guardskatalogs für das Pubset aktivieren.

SERSLOG-Einträge

Wenn ein Schnittstellenaufruf einen unerwarteten Fehlercode liefert oder ein interner Fehler auftritt, wird ein SERSLOG-Eintrag geschrieben.

Die folgenden Einträge werden geschrieben:

– Subsystem GUARDS

PRO0001: Parameterfehler, Schnittstellenfehler

Aufbau des Eintrags:

PARAMETERAREA ERROR. CALLED INTERFACE: 1

PARAMETERAREA: 2

ADDRESS OF CALLER: 3

1: Name der fehlerhaften Schnittstelle (8 bytes)

2: Parameterbereich des Schnittstelle (variabel)

3: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

PRO0002: Interner Fehler

Aufbau des Eintrags:

INTERNAL ERROR IN MODUL: 1 (2).

REASON: 3 4

ADDRESS OF CALLER: 5

1: Name des Moduls (8 bytes)

2: Modulinterne Fehlernummer (2 bytes)

3: Kurze Beschreibung des Fehlers (80 bytes)

4: Datenbereich (variabel)

5: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

Beim Schreiben eines SERSLOG-Eintrags mit der Option DUMP=DIAG wird auch die Meldung PRO6008 auf der Konsole ausgegeben.

– Subsystem GUARDDEF

DEF0001: Parameterfehler, Schnittstellenfehler

Aufbau des Eintrags:

PARAMETERAREA ERROR. CALLED INTERFACE: 1

PARAMETERAREA: 2

ADDRESS OF CALLER: 3

1: Name der fehlerhaften Schnittstelle (8 bytes)

2: Parameterbereich des Schnittstelle (variabel)

3: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

DEF0002: Interner Fehler

Aufbau des Eintrags:

INTERNAL ERROR IN MODUL: 1 (2).

REASON: 3 4

ADDRESS OF CALLER: 5

1: Name des Moduls (8 bytes)

2: Modulinterne Fehlernummer (2 bytes)

3: Kurze Beschreibung des Fehlers (80 bytes)

4: Datenbereich (variabel)

5: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

Beim Schreiben eines SERSLOG-Eintrags mit der Option DUMP=DIAG wird auch die Meldung DEF5002 auf der Konsole ausgegeben.

– Subsystem GUARDCOO

COO0001: Parameterfehler, Schnittstellenfehler

Aufbau des Eintrags:

PARAMETERAREA ERROR. CALLED INTERFACE: 1

PARAMETERAREA: 2

ADDRESS OF CALLER: 3

1: Name der fehlerhaften Schnittstelle (8 bytes)

2: Parameterbereich des Schnittstelle (variabel)

3: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

COO0002: Interner Fehler

Aufbau des Eintrags:

INTERNAL ERROR IN MODUL: 1 (2).

REASON: 3 4

ADDRESS OF CALLER: 5

1: Name des Moduls (8 bytes)

2: Modulinterne Fehlernummer (2 bytes)

3: Kurze Beschreibung des Fehlers (80 bytes)

4: Datenbereich (variabel)

5: Name und Adresse des Aufrufers (abdruckbar) (22 bytes)

Beim Schreiben eines SERSLOG-Eintrags mit der Option DUMP=DIAG wird auch die Meldung COO5002 auf der Konsole ausgegeben.

5.11 GUARDS-Kommandos

In diesem Kapitel werden alle GUARDS-Kommandos in alphabetischer Reihenfolge aufgeführt. Die Beschreibung der Kommandos ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion des Kommandos erklärt, dann folgt das Kommandoformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung folgt der Kommando-Returncode und gegebenenfalls ein Anwendungsbeispiel.

Funktionelle Übersicht

Die Kommandos für GUARDS teilen sich in folgende Gruppen auf:

Kommandos der GUARDS-Verwaltung

COPY-GUARD	Guard kopieren
CREATE-GUARD	Guard einrichten
DELETE-GUARD	Guard löschen
MODIFY-GUARD-ATTRIBUTES	Guard-Attribute ändern
SHOW-GUARD-ATTRIBUTES	Guard-Attribute anzeigen

Kommandos der Standardbedingungsverwaltung

ADD-ACCESS-CONDITIONS	Zugriffsbedingungen hinzufügen
MODIFY-ACCESS-CONDITIONS	Zugriffsbedingungen ändern
REMOVE-ACCESS-CONDITIONS	Zugriffsbedingungen entfernen
SHOW-ACCESS-ADMISSION	Zugriffserlaubnis anzeigen
SHOW-ACCESS-CONDITIONS	Zugriffsbedingungen anzeigen
SHOW-EVALUATED-CONDITIONS	Auszuwertende Zugriffsbedingungen anzeigen

Kommandos der Standardschutzverwaltung

ADD-DEFAULT-PROTECTION-RULE	Standardschutzregel hinzufügen
MODIFY-DEFAULT-PROTECTION-RULE	Standardschutzregel ändern
REMOVE-DEFAULT-PROTECTION-RULE	Standardschutzregel entfernen
SHOW-DEFAULT-PROTECTION-RULE	Standardschutzregel anzeigen
SHOW-OBJECT-PROTECTION-DEFAULT	Standardschutzattribute für Objekt anzeigen

Kommandos der Standardschutz-Attributverwaltung

ADD-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute festlegen
MODIFY-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute ändern
SHOW-DEFAULT-PROTECTION-ATTR	Standardwerte für Schutzattribute anzeigen

Kommandos der Standardschutz-Objektpfadverwaltung (nur für die Systemverwaltung)

ADD-DEFAULT-PROTECTION-UID	Kennungen für Objektpfad hinzufügen
REMOVE-DEFAULT-PROTECTION-UID	Kennungen für Objektpfad entfernen
SHOW-DEFAULT-PROTECTION-UID	Kennungen für Objektpfad anzeigen

Kommandos der Miteigentümerschutzverwaltung

ADD-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel hinzufügen
MODIFY-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel ändern
REMOVE-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel entfernen
SHOW-COOWNER-PROTECTION-RULE	Miteigentümerschutzregel anzeigen
SHOW-COOWNER-ADMISSION-RULE	Miteigentümerberechtigungsregel anzeigen

Kommandos zur Verwaltung der Guardskataloge

CHANGE-GUARD-FILE	Guardskatalog austauschen
REPAIR-GUARD-FILE	Guardskatalog wiederherstellen
SHOW-GUARD-MANAGEMENT-STATUS	GUARDS-Systemeinstellungen anzeigen

ADD-ACCESS-CONDITIONS
Zugriffsbedingungen hinzufügen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Zugriffsbedingungen in ein oder mehrere Guards eingetragen. Die Zugriffsbedingungen können dabei durch wiederholte Kommandoaufrufe nacheinander für jeweils einen der möglichen Subjekttypen *USER, *GROUP, *OTHERS und *ALL-USERS eingetragen werden.

```
ADD-ACCESS-CONDITIONS

 GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,SUBJECTS = *NONE / *OTHERS / *ALL-USERS / *USER(...) / *GROUP(...)
    *USER(...)
    |    USER-IDENTIFICATION = list-poss(20): <name 1..8>
    *GROUP(...)
    |    GROUP-IDENTIFICATION = *UNIVERSAL / list-poss(20): <name 1..8>
,ADMISSION = *YES / *NO / *PARAMETERS(...)
    *PARAMETERS(...)
    |    DATE = *ANY / *EXCEPT(...) / list-poss(4): *INTERVAL(...)
    |      *EXCEPT(...)
    |      |    DATE = list-poss(4): *INTERVAL(...)
    |      |      *INTERVAL(...)
    |      |      |    FROM = <date 8..10 with-compl>
    |      |      |   ,TO = *SAME / <date 8..10 with-compl>
    |      *INTERVAL(...)
    |      |    FROM = <date 8..10 with-compl>
    |      |   ,TO = *SAME / <date 8..10 with-compl>
```

(Teil 1 von 2)

```
,TIME = *ANY / *EXCEPT(...) / list-poss(4): *INTERVAL(...)
    *EXCEPT(...)
        TIME = list-poss(4): *INTERVAL(...)
            *INTERVAL(...)
                FROM = <time 1..8>
                ,TO = <time 1..8>
    *INTERVAL(...)
        FROM = <time 1..8>
        ,TO = <time 1..8>
,WEEKDAY = *ANY / *EXCEPT(...) / list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY /
                *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
    *EXCEPT(...)
        WEEKDAY = list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY /
                        *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
,PRIVILEGE = *ANY / *EXCEPT(...) / list-poss(31): <text>
    *EXCEPT(...)
        PRIVILEGE = list-poss(31): <text>
,PROGRAM = *ANY / list-poss(4): <filename 1..54 without-gen-vers with-wild> /
                *PHASE(...) / *MODULE(...)
    *PHASE(...)
        LIBRARY = <filename 1..54 without-gen-vers with-wild>
        ,ELEMENT = <composed-name 1..64 with-under with-wild>
        ,VERSION = *ANY / <composed-name 1..24 with-under with-wild>
    *MODULE(...)
        LIBRARY = <filename 1..54 without-gen-vers with-wild>
        ,ELEMENT = <composed-name 1..32 with-under with-wild>
        ,VERSION = *ANY / <composed-name 1..24 with-under with-wild>
,DIALOG-CONTROL = *STD / *NO / *GUARD-CHANGE / *USER-ID-CHANGE / *CATALOG-CHANGE
```

(Teil 2 von 2)

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Angabe eines oder mehrerer Guards, in die Zugriffsbedingungen eingetragen werden sollen. Im Namen dürfen Musterzeichen (wildcards) enthalten sein.

Wird der Name ohne Musterzeichen angegeben und das genannte Guard ist noch nicht eingerichtet, wird es neu angelegt und erhält den Guardtyp STDAC.

Wird der Guardname mit Hilfe von Musterzeichen angegeben, werden nur die Guards berücksichtigt, die den Guardtyp STDAC besitzen.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator angeben.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SUBJECTS =
Angabe, für welchen Subjekttyp die einzutragenden Zugriffsbedingungen gelten sollen. Mögliche Subjekttypen sind:
– *USER (Benutzerkennungen),
– *GROUP (Benutzergruppen)
– *OTHERS (alle nicht explizit genannten Benutzerkennungen).

Zusätzlich existiert noch der Pseudo-Subjekttyp *ALL-USERS, mit dem Zusatzbedingungen festgelegt werden können.

Sollen Zugriffsbedingungen für mehrere dieser Subjekttypen festgelegt werden, muss das Kommando entsprechend oft eingegeben werden.

SUBJECTS = *NONE
Es werden keine Zugriffsbedingungen definiert. Mit diesem Operandenwert kann einem Guard des Typs UNDEF der Typ STDAC zugewiesen werden. Dann kann das Guard nur noch Zugriffsbedingungen aufnehmen.

SUBJECTS=*NONE darf nur zusammen mit ADMISSION=*YES angegeben werden.

SUBJECTS = *OTHERS
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für die Benutzer gelten sollen, die keiner der beiden Listen SUBJECTS=*USER oder *GROUP enthalten sind.

SUBJECTS = *ALL-USERS
Angabe, dass es sich bei den mit dem Operanden ADMISSION festgelegten Bedingungen um **Zusatz**bedingungen handelt.

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen, als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

SUBJECTS = *USER(...)
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für bestimmte Benutzerkennungen gelten sollen.

USER-IDENTIFICATION = list-poss(20): <name 1..8>
Angabe von maximal 20 Benutzerkennungen, für die die mit dem Operanden ADMISSION definierten Zugriffsbedingungen gelten sollen. Sollen mehr als 20 Benutzerkennungen aufgezählt werden, muss der Kommandoaufruf entsprechend oft wiederholt werden.

SUBJECTS = *GROUP(...)
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für bestimmte Benutzergruppen gelten sollen.

GROUP-IDENTIFICATION = *UNIVERSAL / list-poss(20): <name 1..8>
Angabe von maximal 20 Gruppenkennungen, für die die mit dem Operand ADMISSION definierten Zugriffsbedingungen gelten sollen. Sollen mehr als 20 Gruppenkennungen aufgezählt werden, muss der Kommandoaufruf entsprechend oft wiederholt werden.

ADMISSION =
Legt die Zugriffsbedingungen für den mit dem Operand SUBJECTS angegebenen Subjekttyp (*USER, *GROUP, *OTHERS) oder Zusatzbedingungen für alle Subjekttypen (*ALL-USERS) fest.

ADMISSION = *YES
Legt fest, dass dem mit dem Operanden SUBJECTS angegebenen Subjekttyp der Zugriff gestattet ist.

Zu beachten ist hierbei das Zusammenspiel der der Bedingungen für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) mit den **Zusatz**bedingungen für den Pseudo-Subjekttyp *ALL-USERS:

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

Bei Angabe von SUBJECTS=*NONE muss ADMISSION=*YES gesetzt sein. Andernfalls wird ein Fehler gemeldet.

ADMISSION = *NO
Legt fest, dass dem mit dem Operanden SUBJECTS angegebenen Subjekttyp oder Pseudo-Subjektyp der Zugriff verboten ist.

Erfolgt diese Angabe für den Pseudo-Subjekttyp *ALL-USERS, ist der Zugriff für alle Subjektypen **generell verboten**. Dies gilt unabhängig von den für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) festgelegten Bedingungen.

ADMISSION = *PARAMETERS(...)
Genauere Spezifizierung der Zugriffsbedingungen, die dem mit dem Operanden SUBJECTS angegebenen Subjekttyp oder Pseudo-Subjektyp gelten sollen.

Zu beachten ist hierbei das Zusammenspiel der der Bedingungen für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) mit den **Zusatz**bedingungen für den Pseudo-Subjekttyp *ALL-USERS:

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

DATE =
Angabe von Kalenderdaten, an denen der Zugriff erlaubt oder untersagt ist. Jahresangaben müssen zwischen 1991 und 2099 liegen. SDF erlaubt die Angabe des Datums sowohl mit vierstelliger als auch mit zweistelliger Jahreszahl. Ein Datum mit zweistelliger Jahreszahl (jj-mm-tt) wird ergänzt zu:

20jj-mm-tt, falls jj < 60 oder
19jj-mm-tt, falls jj ≥ 60.

DATE = *ANY
Es kann jederzeit auf das Objekt zugegriffen werden.

DATE = *EXCEPT(DATE = list-poss(4): *INTERVAL(...))
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff untersagt ist.

FROM = <date 8..10 with-compl>
Gibt den Anfang des Intervalls an.

TO = *SAME
Gibt an, dass das Ende gleich dem Anfang des Intervalls ist. (Bedingung gilt nur an einem Tag).

TO = <date 8..10 with-compl>
Gibt das Ende des Intervalls an.

DATE = list-poss(4): *INTERVAL(...)
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff erlaubt ist.

FROM = <date 8..10 with-compl>
Gibt den Anfang des Intervalls an.

TO = *SAME
Gibt an, dass das Ende gleich dem Anfang des Intervalls ist. (Bedingung gilt nur an einem Tag).

TO = <date 8..10 with-compl>
Gibt das Ende des Intervalls an.

TIME =
Angabe von Tageszeiten, an denen der Zugriff erlaubt oder untersagt ist. Sekundenangaben werden ignoriert. Stunden- und Minutenangaben sind durch Doppelpunkte voneinander zu trennen. Angaben ohne Doppelpunkt werden als Stundenangabe interpretiert.

TIME = *ANY
Es kann jederzeit auf das Objekt zugegriffen werden.

TIME = *EXCEPT(TIME = list-poss(4): *INTERVAL(...))
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff untersagt ist.

FROM = <time 1..8>
Gibt den Anfang des Intervalls an.

TO = <time 1..8>
Gibt das Ende des Intervalls an.

TIME = list-poss(4): *INTERVAL(...)
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff erlaubt ist.

FROM = <time 1..8>
Gibt den Anfang des Intervalls an.

TO = <time 1..8>
Gibt das Ende des Intervalls an.

WEEKDAY =
Legt einen oder mehrere Wochentage fest, an denen der Zugriff erlaubt ist.

WEEKDAY = *ANY
Zugriff ist an jedem Wochentag erlaubt.

WEEKDAY = *EXCEPT(...)
Legt die Tage fest, an denen der Zugriff untersagt ist.

WEEKDAY = list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
Hier wird die Liste der Tage festgelegt, an denen der Zugriff untersagt ist.

WEEKDAY = list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
Zugriff ist nur an den angegebenen Tagen erlaubt.

PRIVILEGE =
Spezifiziert die Privilegien, mit denen der Zugriff erlaubt ist.

PRIVILEGE = *ANY
Es ist kein besonderes Privileg für den Zugriff notwendig.

PRIVILEGE = *EXCEPT(...)

PRIVILEGE = list-poss(31): <text>
Untersagt ist ein Zugriff mit den angegebenen Privilegien. Mögliche Privilegien siehe Seite 128.

PRIVILEGE = list-poss(31): <text>
Nur Benutzer mit den angegebenen Privilegien dürfen zugreifen. Mögliche Privilegien siehe Seite 128.

PROGRAM = *ANY /
list-poss(4): <filename 1..54 without-gen-vers with-wild> / *PHASE(...) / *MODULE(...)
Legt fest, über welches Programm ein Zugriff erfolgen darf. Es können maximal 4 Programmnamen angegeben werden. Die benannten Programme können entweder als gebundene Phase in einer Datei, oder als Objektmodul (OM) bzw. Binderlademodul (LLM) als Bibliothekselement vorliegen.

Hinweise

Um Konflikte bei der Verwendung von Moduln des Typs OM und LLM zu vermeiden, wird empfohlen, die Module in unterschiedlichen Bibliotheken zu führen (siehe auch Handbuch „LMS“ [23]).

Bei Zugriffen über ein Programm wird geprüft, ob das zugreifende Programm geladen und die Kontrolle übernommen hat.

Soll auf ein mit Guards geschütztes Objekt nur über ein Programm zugegriffen werden, ist auf Folgendes zu achten:

Die Datei oder Bibliothek, in der das zum Zugriff berechtigte Programm abgelegt ist, sollte selber so geschützt werden, dass das Programm weder modifiziert noch gelesen werden kann. Es könnte sonst von einem Benutzer (der keinen Zugriff auf das geschützte Objekt hat) unter dessen Benutzerkennung kopiert und mit dem Namen des zum Zugriff berechtigten Programms benannt werden.

PROGRAM = *ANY
Der Zugriff darf über jedes beliebige Programm erfolgen.

PROGRAM = <filename 1..54 without-gen-vers with-wild>
Das Programm ist eine gebundene Phase und liegt als Datei vor. Wird der Dateiname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

PROGRAMM = *PHASE(...)
Das Programm ist eine gebundene Phase und liegt als Bibliothekselement des Typs C vor.

LIBRARY = <filename 1..54 without-gen-vers with-wild>
Name der Bibliothek, in der die gebundene Phase eingetragen ist. Wird der Bibliotheksname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

ELEMENT = <composed-name 1..64 with-under with-wild>
Name des Bibliothekselements.

VERSION = *ANY
Es wird keine spezielle Version für das Bibliothekselement festgelegt.

VERSION = <composed-name 1..24 with-under with-wild>
Version des Bibliothekselements.

PROGRAM = *MODULE(...)
Das Programm ist ein Objektmodul (OM) oder ein Bindelademodul (LLM) und liegt als Bibliothekselement vom Typ R bzw. L vor.

LIBRARY = <filename 1..54 without-gen-vers with-wild>
Name der Bibliothek, in der der Objekt- bzw. Lademodul eingetragen ist. Wird der Bibliotheksname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

ELEMENT = <composed-name 1..32 with-under with-wild>
Name des Bibliothekselements.

VERSION = *ANY
Es wird keine spezielle Version für das Bibliothekselement festgelegt.

VERSION = <composed-name 1..24 with-under with-wild>
Version des Bibliothekselements.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Bedingungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Bedingungsguard mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Bedingungsguard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Bedingungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Bedingungsguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Bedingungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Bedingungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	PRO1011	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1015	Das angegebene Subjekt ist nicht im Guard enthalten
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen.
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1026	Kennung bereits in Bedingung enthalten
	64	PRO1027	Bedingungsbereich voll
	64	PRO1028	Guard hat falschen Typ
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
2	64	PRO1035	Kommando nicht ausgeführt
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt
	128	PRO1038	Guardskatalog durch ARCHIVE gesperrt

Beispiel

Es soll in das Guard eingetragen werden, dass der Benutzer SECOSMAN nur zwischen 7 und 17 Uhr zugreifen darf:

```
/add-access-conditions -
/    guard-name=guardexa,subjects=*user(user-identification=secosman), -
/    admission=*parameters(time=*interval(from=07:00,to=17:00))
```

Die Bedingung kann überprüft werden mit /SHOW-ACCESS-CONDITIONS:

```
/show-access-conditions guard-name=guardexa,information=*all

     Guard name          Scope       Creation Date            Last Mod Date
------------------------------------------------------------------------------
:N:$SECOSMAN.GUARDEXA     SYS     2017-09-29/10:52:28     2017-09-29/11:07:28
                         GUARD FUER DIE GUARD-BEISPIELE
   User   SECOSMAN
    Time      IN ( <07:00,17:00> )
------------------------------------------------------------------------------
Guards selected: 1                                                End of display
```

ADD-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel hinzufügen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando wird eine Miteigentümerschutzregel in einen Regelbehälter (Guard) eingetragen. Handelt es sich dabei um den ersten Regeleintrag, wird der Regelbehälter neu angelegt, wobei er den Guardtyp COOWNERP erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt.

Gibt es den Regelbehälter bereits, bleibt der SCOPE unverändert und die Regel wird an die angegebene Position im Regelbehälter eingefügt.

Es können beliebig viele Regelbehälter beliebigen Namens erstellt werden. Für eine Miteigentümerüberprüfung werden nur Regelbehälter mit den Namen SYS.UCF[<n>] bzw. SYS.UCJ[<n>] herangezogen (aktive Regelbehälter, siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 479).

Ein Anwender kann nur Regelbehälter für seine eigene Benutzerkennung einrichten. Ein Guard-Administrator darf Regelbehälter unter fremden Benutzerkennungen einrichten.

ADD-COOWNER-**PROTECT**ION-**RULE** (**ADD-COO-PRO-R**)

RULE-CONTAINER-**GUARD** = <filename 1..24 without-gen-vers with-wild(40)>

,**PROTECT**ION-**RULE** = <alphanum-name 1..12>

,**RULE-POS**ITION = ***LAST** / ***BEFORE**(...)

***BEFORE**(...)

PROTECTION-**RULE** = <alphanum-name 1..12>

,**PROTECT-OBJ**ECT = ***PAR**AMETERS(...)

***PAR**AMETERS(...)

NAME = <filename 1..41 without-cat-user-gen with-wild(80)>

,**COND**ITION-**GUARD** = ***NONE** / <filename 1..18 without-cat-gen-vers>

,**TSOS-ACCESS** = ***SYS**TEM-**STD** / ***RESTRICTED**

,**GUARD-CHECK** = ***Y**ES / ***NO**

,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***RULE-CONT**AINER-**CHA**NGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ COOWNERP, in den eine erste oder weitere Regel eingetragen werden soll. Der Behälter wird neu eingerichtet sofern es ihn noch nicht gibt.

Der Behältername kann beliebig gewählt werden, für die Zugriffskontrolle wird jedoch ausnahmslos ein Regelbehälter mit fest vorgeschriebenem Namen verwendet.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel durch Absetzen eines einzigen Kommandos in mehrere Behälter eingetragen wird, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE = <alphanumeric name 1..12>
Name der Regel, die eingetragen werden soll. Doppelte Namen in einem Behälter sind nicht erlaubt.

RULE-POSITION =
Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt werden soll. Die Reihenfolge der Regeln ist ausschlaggebend bei der Miteigentümerüberprüfung (siehe Abschnitt „Suchlogik“ auf Seite 482).

RULE-POSITION = *LAST
Die Regel soll an die letzte Position im Regelbehälter gestellt werden.

RULE-POSITION = *BEFORE(...)
Die Regel soll vor eine benannte Regel im Regelbehälter gestellt werden.

PROTECTION-RULE = <alphanumeric name 1..12>
Name einer vorhandenen Regel im Regelbehälter, vor die die einzutragende Regel gestellt werden soll.
Das Kommando wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

PROTECT-OBJECT = *PARAMETERS(...)
Angaben über das Objekt, auf das sich die zu bearbeitende Regel beziehen soll.

NAME =
Dieser Operand bezeichnet den Namen des Objekts, für das die einzutragende Regel gelten soll.

NAME = <filename 1..41 without-cat-gen-user with-wild(80)>
Name des Objektes.
Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten. Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

CONDITION-GUARD =
Name des Guards vom Typ STDAC, das die Zugriffsbedingungen enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

CONDITION-GUARD = *NONE
Es wird kein Guardname angegeben. Der Miteigentümerschutz wird für das Objekt außer Kraft gesetzt, es gibt keine Miteigentümer für das Objekt.

CONDITION-GUARD = <filename 1..18 without-cat-gen-ver>
Name eines Guards des Typs STDAC, das die Zugriffsbedingungen enthält, die ein Miteigentümer erfüllen muss. Der Name darf keine Katalogkennung enthalten. Seine Länge ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

TSOS-ACCESS =
Angabe über die Miteigentümerschaft der Benutzerkennung TSOS.

TSOS-ACCESS = *SYSTEM-STD
Die Benutzerkennung TSOS erhält die volle Miteigentümerschaft für das Objekt.

TSOS-ACCESS = *RESTRICTED
Die Benutzerkennung TSOS erhält eine eingeschränkte Miteigentümerschaft für das Objekt. Die Kommandos und Makros, auf die sich eine Einschränkung der TSOS-Miteigentümerschaft auswirkt, finden Sie im Abschnitt „Wirksamkeit der TSOS-Einschränkung“ auf Seite 939.

GUARD-CHECK =
Bei Kommandodurchführung kann wahlweise die Verfügbarkeit des in der Regel namentlich genannten Guards überprüft werden.

GUARD-CHECK = *YES
Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt es das Guard nicht, oder ist der Eigentümer des gerade bearbeiteten Regelbehälters nicht berechtigt, das Guard zu verwenden, wird das Kommando nicht durchgeführt.

GUARD-CHECK = *NO
Das Kommando wird unabhängig davon durchgeführt, ob das genannte Guard verfügbar ist oder vom Eigentümer des gerade bearbeiteten Regelbehälters verwendet werden darf.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	COO3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen.
2	0	COO3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
	1	COO3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	COO3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	COO3300	Der angegebene Regelbehälter existiert nicht.
	64	COO3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	COO3303	Es passt keine weitere Regel mehr in den Regelbehälter.
	64	COO3304	Es wurde kein Regelbehälter selektiert.
	64	COO3305	Der angegebene Regelname zum Positionieren wurde nicht gefunden.
	64	COO3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	COO3307	Eine einzufügende Regel existiert bereits.
	64	COO3308	Eine Benutzerkennung ist unbekannt.
	64	COO3309	Keine Unterstützung für einen Remote-File-Access.
	64	COO3311	Ein angegebenes Guard für Zugriffsbedingungen ist nicht zugreifbar.
	64	COO3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	COO3314	Fehler im Kommunikationsmittel des MRS.
	64	COO3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	128	COO3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	COO3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	COO3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

ADD-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute festlegen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Schutzattribut-Standardwerte in ein Attributguard eingetragen.

Gibt es das Attributguard noch nicht, wird es implizit angelegt, wobei es den Guardtyp DEFPATTR erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt.

Gibt es das Attributguard bereits, weil es mit dem Kommando /CREATE-GUARD oder dem Makro CREGUA angelegt wurde, bleibt der SCOPE unverändert.

Das Kommando kann nur auf ein noch nicht eingerichtetes oder ein noch undefiniertes Guard angewendet werden. Im anderen Fall wird es abgewiesen. Die Modifikation von Attributen in einem Attributguard muss mit dem Kommando /MODIFY-DEFAULT-PROTECTION-ATTR durchgeführt werden.

Ein Anwender kann nur Attributguards für seine eigene Benutzerkennung einrichten. Ein Guards-Administrator darf Attributguards unter fremden Benutzerkennungen einrichten.

Generell werden die spezifizierten Schutzattributwerte in die Attributbereiche *CREATE-OBJECT und *MODIFY-OBJECT-ATTR eingetragen. Folgende Abweichungen sind dabei zu beachten:

ACCESS
: Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Bereich *CREATE-OBJECT wird der entsprechende Wert auf *SYSTEM-STD gesetzt. Damit wird verhindert, dass ein neu eingerichtetes Objekt standardmäßig mit dem Attribut ACCESS=READ versehen wird, bevor es überhaupt mit Daten versehen werden konnte. Sollte dieses Verhalten jedoch explizit vom Anwender gewünscht sein, muss der Attributwert explizit mit dem Kommando /MODIFY-DEFAULT-PROTECTION-ATTR modifiziert werden.

EXPIRATION-DATE
: Da das Schutzattribut beim Neuanlegen eines Objektes nicht wirkt, wird der spezifizierte Wert nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSTEM-STD gesetzt.

FREE-FOR-DELETION
: Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSTEM-STD gesetzt. So soll verhindert werden, dass durch den Standardwert für FREE-FOR-DELETION ein Kennwortschutz unterlaufen wird, den eine bestehende Anwendung für Dateien vorsieht, die sie neu anlegt.

*Bedeutung des Operandenwertes *SYSTEM-STD*

Der Wert *SYSTEM-STD steht stellvertretend für einen in der hierarchisch höheren Instanz vorgegebenen Attributwert.

Die hierarchisch höhere Instanz ist
– der pubsetglobale Regelbehälter,
  wenn ein Attributguard aus einem benutzerspezifischen Regelbehälter heraus ausgewertet wird oder wenn es keinen benutzerspezifischen Regelbehälter gibt
– die herkömmliche Systemvoreinstellung,
  wenn ein Attributguard aus einem pubsetglobalen Regelbehälter heraus ausgewertet wird oder wenn es keinen pubsetglobalen Regelbehälter gibt.

Die folgende Tabelle zeigt, wie die spezifizierten Werte den beiden Attributbereichen zugeordnet werden:

Attribut	**Attributber4eich**	
	***CREATE-OBJECT**	***MOD-OBJECT-ATTR**
ACCESS	*SYSTEM-STD	spezifizierter Wert
USER-ACCESS	spezifizierter Wert	spezifizierter Wert
BASIC-ACL	spezifizierter Wert	spezifizierter Wert
GUARDS	spezifizierter Wert	spezifizierter Wert
WRITE-PASSWORD	spezifizierter Wert	spezifizierter Wert
READ-PASSWORD	spezifizierter Wert	spezifizierter Wert
EXEC-PASSWORD	spezifizierter Wert	spezifizierter Wert
DESTROY-BY-DELETE	spezifizierter Wert	spezifizierter Wert
SPACE-RELEASE-LOCK	spezifizierter Wert	spezifizierter Wert
EXPIRATION-DATE	*SYSTEM-STD	spezifizierter Wert
FREE-FOR-DELETION	*SYSTEM-STD	spezifizierter Wert

Anmerkungen

– Der Attributbereich *MOD-OBJECT-ATTR ist nur für Dateien relevant, da bei der Modifikation von Jobvariablen-Attributen der Standardschutz nicht unterstützt wird.

– Attribute im Bereich *CREATE-OBJECT, die nur für Dateien relevant sind (z.B. EXEC-PASSWORD oder USER-ACCESS=*SPECIAL), werden für Jobvariablen ohne Meldung ignoriert. Dadurch kann für Dateien und Jobvariablen dergleiche Attributbehälter verwendet werden.

ADD-DEFAULT-PROTECTION-ATTR (**ADD-DEF-PRO-A**)

GUARD-NAME = <filename 1..24 without-gen-vers>
,**ACCESS** = ***SYS**TEM-**STD** / ***WR**ITE / *READ
,**USER-ACCESS** = ***SYS**TEM-**STD** / ***OWNER-ONLY** / ***ALL-USERS** / ***SPECIAL**
,**BASIC-ACL** = ***SYS**TEM-**STD** / ***NONE** / ***PAR**AMETERS(...)
***PAR**AMETERS(...)
OWNER = ***PAR**AMETERS(...)
***PAR**AMETERS(...)
READ = ***NO** / *YES
,**WR**ITE = ***NO** / *YES
,**EXEC** = ***NO** / *YES
,**GR**OUP = ***PAR**AMETERS(...)
***PAR**AMETERS(...)
READ = ***NO** / *YES
,**WR**ITE = ***NO** / *YES
,**EXEC** = ***NO** / *YES
,**OTHERS** = ***PAR**AMETERS(...)
***PAR**AMETERS(...)
READ = ***NO** / *YES
,**WR**ITE = ***NO** / *YES
,**EXEC** = ***NO** / *YES
,**GUARDS** = ***SYS**TEM-**STD** / ***NONE** / ***PAR**AMETERS(...)
***PAR**AMETERS(...)
READ = ***NONE** / <filename 1..18 without-cat-gen-vers>
,**WR**ITE = ***NONE** / <filename 1..18 without-cat-gen-vers>
,**EXEC** = ***NONE** / <filename 1..18 without-cat-gen-vers>

(Teil 1 von 2)

,**READ-PASS**WORD = ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**WR**ITE-**PASS**WORD = ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**EXEC-PASS**WORD = ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**DESTROY**-BY-DELETE = ***SYS**TEM-**STD** / ***NO** / *YES

,**SPACE-RELE**ASE-**LOCK** = ***SYS**TEM-**STD** / ***NO** / *YES

,**EXPIR**ATION-DATE = ***SYS**TEM-**STD** / ***TODAY** / ***TOMORROW** / <date with-compl> / <integer 0..99999>

,**FREE-FOR-DEL**ETION = ***SYS**TEM-**STD** / ***NONE** / <date with-compl> / <integer 0..99999>

(Teil 2 von 2)

GUARD-NAME = <filename 1..24 without-gen-vers>
Dieser Operand bezeichnet den Namen eines Guards, in das Schutzattribut-Standardwerte eingetragen werden sollen. Der Name ist beliebig, seine Länge ohne Katalog- und Benutzerkennung darf jedoch 8 Zeichen nicht überschreiten. Falls das Guard noch nicht existiert, wird es eingerichtet und erhält den Guardtyp DEFPATTR.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

ACCESS =
Gibt an, welche Art von Zugriff auf das Objekt erlaubt ist.

ACCESS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

ACCESS = *WRITE
Lesende, schreibende und ausführende Objektzugriffe sind erlaubt.

Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Bereich *CREATE-OBJECT wird der entsprechende Wert auf *SYSTEM-STD gesetzt.

ACCESS = *READ
Es sind nur lesende und ausführende Objektzugriffe erlaubt.

Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Bereich *CREATE-OBJECT wird der entsprechende Wert auf *SYSTEM-STD gesetzt. Damit wird verhindert, dass ein neu eingerichtetes Objekt standardmäßig mit dem Attribut ACCESS=READ versehen wird, bevor es überhaupt mit Daten versehen werden konnte. Sollte dieses Verhalten jedoch explizit vom Anwender gewünscht sein, muss der Attributwert explizit mit /MODIFY-DEFAULT-PROTECTION-ATTR modifiziert werden.

USER-ACCESS =
Gibt an, ob fremde Benutzerkennungen auf das Objekt zugreifen dürfen.

USER-ACCESS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

USER-ACCESS = *OWNER-ONLY
Der Zugriff auf das Objekt ist nur unter der eigenen Benutzerkennung möglich, aber unter jeder Katalogkennung, unter der die (namentlich) gleiche Benutzerkennung eingerichtet ist (d.h. nicht nur unter der Katalogkennung, unter der das Objekt eingerichtet wurde). Miteigentümer haben ebenfalls Zugriff.

USER-ACCESS = *ALL-USERS
Der Zugriff auf das Objekt ist auch unter fremden Benutzerkennungen möglich.

USER-ACCESS = *SPECIAL
Das Objekt ist für alle Benutzerkennungen einschließlich der Kennungen mit dem Privileg HARDWARE-MAINTENANCE zugänglich. Zugriffe der Wartungskennung sind generell nur möglich, wenn USER-ACCESS=*SPECIAL gilt.

BASIC-ACL =
Aktiviert den Zugriffsschutz über BACL.

BASIC-ACL = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

BASIC-ACL = *NONE
Der Zugriffsschutz über BACL wird nicht aktiviert.

BASIC-ACL = *PARAMETERS(...)
Ein Zugriffsschutz über BACL wird eingetragen. Sofern kein höherer Zugriffsschutz existiert, wird er automatisch aktiv.

OWNER =
Legt die Zugriffsrechte für den Eigentümer und Miteigentümer der Datei fest.

OWNER = *PARAMETERS(...)
Die Zugriffsrechte des Eigentümers werden nachfolgend spezifiziert.

READ = *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

GROUP =
Legt die Zugriffsrechte für Mitglieder der Gruppe des Eigentümers fest.

GROUP = *PARAMETERS(...)
Die Zugriffsrechte für Mitglieder der Benutzergruppe des Eigentümers werden nachfolgend spezifiziert.

READ = *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

OTHERS =
Legt die Zugriffsrechte für alle Benutzer fest, die nicht Mitglieder der Benutzergruppe des Eigentümers sind.

OTHERS = *PARAMETERS(...)
Die Zugriffsrechte für die übrigen Benutzer werden nachfolgend spezifiziert.

READ = *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

GUARDS =
Gibt an, ob die Zugriffskontrolle über GUARDS erfolgt.

GUARDS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

GUARDS = *NONE
Die Zugriffskontrolle erfolgt nicht über GUARDS.

GUARDS = *PARAMETERS(...)
Die Zugriffskontrolle erfolgt über GUARDS.

Der Guard-Name darf maximal 8 Zeichen, mit Angabe einer Benutzerkennung maximal 18 Zeichen lang sein. Eine Katalogkennung kann nicht angegeben werden, denn das Guard muss immer in dem Katalog abgelegt sein, in dem sich auch die Datei befindet!

READ =
Angaben für den Leseschutz.

READ = *NONE
Es wird kein Guardname zugewiesen. Es sind keine Lesezugriffe erlaubt.

READ = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Leseschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

WRITE =
Angaben für den Schreibschutz.

WRITE = *NONE
Es wird kein Guardname zugewiesen. Es sind keine Schreibzugriffe erlaubt.

WRITE = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Schreibschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

EXEC =
Angaben für den Ausführschutz.

EXEC = *NONE
Es wird kein Guardname zugewiesen. Es sind keine Ausführungszugriffe erlaubt.

EXEC = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Ausführungsschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

WRITE-PASSWORD = *SYSTEM-STD / *NONE / *SECRET /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Schreiben. Der Operand WRITE-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

WRITE-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

WRITE-PASSWORD = *NONE
Es wird kein Schreibkennwort vergeben.

WRITE-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Schreibkennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Schreibkennwort zur Verfügung gestellt wird.

READ-PASSWORD = *SYSTEM-STD / *NONE / *SECRET /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Lesen. Der Operand READ-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

READ-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

READ-PASSWORD = *NONE
Es wird kein Lesekennwort vergeben.

READ-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Lesekennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Lesekennwort zur Verfügung gestellt wird.

EXEC-PASSWORD = *SYSTEM-STD / *NONE / *SECRET /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Ausführen. Der Operand EXEC-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

EXEC-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

EXEC-PASSWORD = *NONE
Es wird kein Ausführungskennwort vergeben.

EXEC-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Ausführungskennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Ausführungskennwort zur Verfügung gestellt wird.

DESTROY-BY-DELETE =
Zur Erhöhung des Datenschutzes kann der Benutzer im Katalogeintrag festlegen, dass nicht mehr benötigte Daten mit X’00’ (binär Null) überschrieben werden. Bei Plattendateien wirkt sich das auf Löschoperationen und Speicherplatzfreigabe aus (siehe Kommando /MODIFY-FILE-ATTRIBUTES und /DELETE-FILE). Bei Banddateien wirkt sich das auf das Überschreiben von Restdaten bei EOF- und EOV-Verarbeitung aus (siehe Operand DESTROY-OLD-CONTENTS im Kommando /ADD-FILE-LINK).

DESTROY-BY-DELETE = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

DESTROY-BY-DELETE = *NO
Bei dieser Einstellung wirkt eine im Kommando /DELETE-FILE getroffene Vereinbarung (Operand OPTION).

Bei Plattendateien wird der Speicherplatz unverändert freigegeben, wenn nicht im Kommando /DELETE-FILE der Operand OPTION=DESTROY-ALL angegeben wird.

Bei Banddateien werden die auf dem Band folgenden Restdaten nicht überschrieben, wenn im Kommando /ADD-FILE-LINK für den aktuellen Verarbeitungslauf nicht DESTROY-OLD-CONTENTS=*YES vereinbart wird.

DESTROY-BY-DELETE = *YES
Diese Einstellung wirkt auch, wenn im Kommando /DELETE-FILE, Operand OPTION eine andere Vereinbarung getroffen wird.

Bei Plattendateien wird freigegebener Speicherplatz automatisch mit binär Null (X'00') überschrieben.

Bei Banddateien wird der Bandinhalt nach dem Dateiende mit binär Null (X'00') überschrieben. Im Kommando /ADD-FILE-LINK muss das Löschen der Restdaten für den aktuellen Verarbeitungslauf nicht explizit angegeben werden.

SPACE-RELEASE-LOCK =
Gibt an, ob die Freigabe von Speicherplatz mit dem Kommando /MODIFY-FILE-ATTRIBUTES bzw. FILE-Makro ignoriert werden soll.

SPACE-RELEASE-LOCK = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

SPACE-RELEASE-LOCK = *NO
Speicherplatz kann freigegeben werden.

SPACE-RELEASE-LOCK = *YES
Speicherplatz kann nicht freigegeben werden.

EXPIRATION-DATE =
Schutzfrist der Datei. Bis zu dem angegebenen Datum kann die Datei nicht verändert oder gelöscht werden. Eine Schutzfrist kann nur vergeben werden, wenn die Datei bereits eröffnet wurde, das heißt, ein CREATION-DATE besitzt.

Die Schutzfrist kann, wenn sie nicht über ein Schlüsselwort spezifiziert wird, auf zwei Arten angegeben werden:

– als absolute Datumsangabe
  Datumsangabe in der Form YY-MM-DD oder YYYY-MM-DD
  (YY = Jahr, MM = Monat, DD = Tag).

– als relative Datumsangabe
  Maximal 6-stellig einschließlich Vorzeichen in der Form +n als Distanz zum aktuellen Tagesdatum.

Da das Schutzattribut beim Neuanlegen eines Objektes nicht wirkt, wird der spezifizierte Wert nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSTEM-STD gesetzt.

EXPIRATION-DATE = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

EXPIRATION-DATE = *TODAY
Es wird keine Schutzfrist vergeben, oder eine bestehende Schutzfrist wird aufgehoben, indem sie auf das aktuelle Tagesdatum gesetzt wird.

EXPIRATION-DATE = *TOMORROW
Als Schutzfrist wird das Datum des nächsten Tages vergeben.

EXPIRATION-DATE = <date with-compl>
Die Datei ist bis zum angegebenen Datum (ausschließlich) geschützt.

EXPIRATION-DATE = <integer 0..99999>
Die Datei kann für die angegebene Anzahl von Tagen nicht verändert oder gelöscht werden.

FREE-FOR-DELETION =
Legt fest, ab wann das Objekt ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

Das Lösch-Freigabedatum kann, wenn es nicht über ein Schlüsselwort spezifiziert wird,auf zwei Arten angegeben werden:

– als absolute Datumsangabe
  Datumsangabe in der Form YY-MM-DD oder YYYY-MM-DD
  (YY = Jahr, MM = Monat, DD = Tag).

– als relative Datumsangabe
  Maximal 6-stellig einschließlich Vorzeichen in der Form +n als Distanz zum aktuellen Tagesdatum.

Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSTEM-STD gesetzt. So soll verhindert werden, dass durch den Standardwert für FREE-FOR-DELETION ein Kennwortschutz unterlaufen wird, den eine bestehende Anwendung für Dateien vorsieht, die sie neu anlegt.

FREE-FOR-DELETION = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 536).

FREE-FOR-DELETION = *NONE
Das Objekt kann nur unter Berücksichtigung der Schutzattribute gelöscht werden.

FREE-FOR-DELETION = <date with-compl>
Das Objekt darf ab dem angegebenen Datum ohne Berücksichtigung der Schutzattribute gelöscht werden.

FREE-FOR-DELETION = <integer 0..99999>

Das Objekt kann nach der angegebenen Anzahl von Tagen ohne Berücksichtigung der Schutzattribute gelöscht werden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3350	Ein genanntes Attributguard gibt es bereits.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

ADD-DEFAULT-PROTECTION-RULE
Standardschutzregel hinzufügen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando wird eine Regel für die Standardwertvergabe für Datei- oder Jobvariablen-Schutzattribute in einen Regelbehälter (Guard) eingetragen. Handelt es sich dabei um den ersten Regeleintrag, wird der Regelbehälter neu angelegt, wobei er den Guardtyp DEFAULTP erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt. Gibt es den Regelbehälter bereits, bleibt der SCOPE unverändert und die Regel wird an die angegebene Position im Regelbehälter eingefügt.

Es können beliebig viele Regelbehälter beliebigen Namens erstellt werden. Für die Standardwertvergabe werden nur Regelbehälter mit den Namen SYS.UDF[<n>] bzw. SYS.UDJ[<n>] und $TSOS.SYS.PDF[<n>] bzw. $TSOS.SYS.PDJ[<n>] herangezogen (aktive Regelbehälter, siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458).

Ein Anwender kann nur Regelbehälter unter seiner eigenen Benutzerkennung einrichten. Ein Guards-Administrator kann Regelbehälter unter fremden Benutzerkennungen einrichten.

Ein Regelbehälter für den pubsetglobalen Standardschutz kann nur vom Systemverwalter oder vom Guard-Administrator eingerichtet werden, er muss unter der Benutzerkennung TSOS abgelegt sein.

```
ADD-DEFAULT-PROTECTION-RULE                                    (ADD-DEF-PRO-R)

  RULE-CONTAINER-GUARD = filename 1..24 without-gen-vers with-wild(40)>
,PROTECTION-RULE = <alphanum-name 1..12>
,RULE-POSITION = *LAST / *BEFORE(...)
    *BEFORE(...)
        PROTECTION-RULE = <alphanum-name 1..12>
,PROTECT-OBJECT = *PARAMETERS(...)
    *PARAMETERS(...)
        NAME = *TEMPORARY / <filename 1..41 without-cat-user-gen with-wild(80)>
        ,ATTRIBUTE-GUARD = *NONE / <filename 1..18 without-cat-gen-vers>
        ,USER-ID-GUARD = *ANY-USER-ID / <filename 1..18 without-cat-gen-vers>
,GUARD-CHECK = *YES / *NO
,DIALOG-CONTROL = *STD / *NO / *RULE-CONTAINER-CHANGE / *USER-ID-CHANGE /
                  *CATALOG-CHANGE
```

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ DEFAULTP, in den eine erste oder weitere Regel eingetragen werden soll. Der Behälter wird neu eingerichtet sofern es ihn noch nicht gibt.

Der Behältername kann beliebig gewählt werden. Für die Suche nach passenden Standardwerten werden jedoch in Hierarchie ausnahmslos aktive Regelbehälter verwendet. Diese müssen einen vorgeschriebenen Namen tragen (siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458).

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel durch Absetzen eines einzigen Kommandos in mehrere Behälter eingetragen wird, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE = <alphanumeric name 1..12>
Name der Regel, die eingetragen werden soll. Doppelte Namen in einem Behälter sind nicht erlaubt.

RULE-POSITION =
Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt werden soll. Die Reihenfolge der Regeln ist ausschlaggebend bei der Ermittlung der Schutzattribut-Standardwerte (siehe Abschnitt „Suchlogik“ auf Seite 462).

RULE-POSITION = *LAST
Die Regel soll an die letzte Position im Regelbehälter gestellt werden.

RULE-POSITION = *BEFORE(...)
Die Regel soll vor eine benannte Regel im Regelbehälter gestellt werden.

PROTECTION-RULE = <alphanumeric name 1..12>
Name einer vorhandenen Regel im Regelbehälter, vor die die einzutragende Regel gestellt werden soll. Das Kommando wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

PROTECT-OBJECT = *PARAMETERS(...)
Angaben über das Objekt, auf das sich die zu bearbeitende Regel beziehen soll.

NAME =
Dieser Operand bezeichnet den Namen des Objekts, für das die einzutragende Regel gelten soll.

NAME = *TEMPORARY
Das Objekt ist eine temporäres Objekt. Für alle temporären Objekte kann stellvertretend nur eine einzige Regel angegeben werden.

Hinweis für Dateien

Für temporäre DMS-Dateien werden bei der Standardwertvergabe nur die Schutzattribute DESTROY-BY-DELETE und SPACE-RELEASE-LOCK berücksichtigt. Alle anderen Attribute erhalten die herkömmlichen System-Standardwerte.

Hinweis für Jobvariablen

Für temporäre Jobvariablen werden bei der Standardwertvergabe keine Schutzattribute berücksichtigt. Alle Attribute erhalten die herkömmlichen System-Standardwerte.

NAME = <filename 1..41 without-cat-gen-user with-wild(80)>
Name des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ATTRIBUTE-GUARD =
Angabe eines Guards vom Typ DEFPATTR, das die Standardwerte enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

ATTRIBUTE-GUARD = *NONE
Es wird kein Guardname angegeben. Die Attributstandardwerte werden bei der Standardwertvergabe aus der nächst höheren Hierarchiestufe (pubsetglobal oder herkömmlicher Systemstandard) ermittelt.

ATTRIBUTE-GUARD = <filename 1..18 without-cat-gen-vers>

Name eines Guards des Typs DEFPATTR, das die Schutzattribute enthält, die bei der Standardwertvergabe verwendet werden sollen. Der Name darf keine Katalogkennung enthalten. Seine Länge ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

USER-ID-GUARD =
Name eines Guards vom Typ DEFPUID, das die Benutzerkennungen für die Pfadvervollständigung beim pubsetglobalen Standardschutz enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

Dieser Guardname darf nur vom Systemverwalter oder Guard-Administrator angegeben werden.

USER-ID-GUARD = *ANY-USER-ID
Es wird kein Guard für Benutzerkennungen angegeben. Der Name des Objektes gilt für alle Benutzerkennungen eines Pubsets.

USER-ID-GUARD = <filename 1..18 without-cat-gen-vers>
Name eines Guards des Typs DEFPUID, das die Liste von Benutzerkennungen enthält. Der Name darf keine Katalogkennung enthalten. Seine Länge ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

GUARD-CHECK =
Bei Kommandodurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

GUARD-CHECK = *YES
Es wird geprüft, ob die namentlich angesprochenen Guards verfügbar sind. Gibt es eines der Guards nicht, oder ist der Eigentümer des gerade bearbeiteten Regelbehälters nicht berechtigt, eines der Guards zu verwenden, wird das Kommando nicht durchgeführt.

GUARD-CHECK = *NO
Das Kommando wird unabhängig davon durchgeführt, ob die genannten Guards verfügbar sind oder vom Eigentümer des gerade bearbeiteten Regelbehälters verwendet werden dürfen.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *RULE-CONTAINER-CHANGE
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen.
2	0	DEF3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3300	Der angegebene Regelbehälter existiert nicht.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3303	Es passt keine weitere Regel mehr in den Regelbehälter.
	64	DEF3304	Es wurde kein Regelbehälter selektiert.
	64	DEF3305	Der angegebene Regelname zum Positionieren wurde nicht gefunden.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3307	Eine einzufügende Regel existiert bereits.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3311	Ein angegebenes Guard für Zugriffsbedingungen ist nicht zugreifbar.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3318	Ein Guard mit Benutzerkennungen, das in eine Regel eingetragen werden soll, ist nicht zugreifbar.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

ADD-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad hinzufügen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: GUARD-ADMINISTRATION, TSOS

Mit diesem Kommando kann der Systemverwalter oder ein Guard-Administrator Benutzer- und Gruppenkennungen in ein Benutzerkennungsguard eintragen, die bei der Festlegung von Standardschutzregeln die Objektnamen pubsetweit genauer qualifizieren.

Gibt es das Benutzerkennungsguard noch nicht, wird es implizit angelegt, wobei es den Guardtyp DEFPUID erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt. Gibt es das Benutzerkennungsguard bereits, bleibt der SCOPE unverändert.

Es können beliebig viele Benutzer- und Gruppenkennungen eingetragen werden. Ist der Bedingungsbereich voll, sind keine weiteren Eintragungen möglich.

ADD-DEFAULT-PROTECTION-**UID** (**ADD-DEF-PRO-U**)
GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,**USER-ID**ENTIFICATION = list-poss(20): <name 1..8 with-wild(20)> / ***GR**OUP(...)
***GR**OUP(...)
GROUP-**ID**ENTIFICATION = ***UNIV**ERSAL / <name 1..8 with-wild(20)>
,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***GUARD-CHANGE** / ***USER-ID-CHA**NGE / *CATALOG-CHANGE

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Guards vom Typ DEFPUID, in das Benutzerkennungen und Benutzergruppen eingetragen werden sollen. Der Name kann beliebig sein, seine Länge ohne Musterzeichen, Katalog- und Benutzerkennung darf jedoch 8 Zeichen nicht überschreiten. Das Guard wird neu eingerichtet, falls es noch nicht existiert.

Musterzeichen im Namen des Guards bewirken, dass die Benutzerkennungen durch Absetzen eines einzigen Kommandos in mehrere Guard eingetragen wird.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

USER-IDENTIFICATION = list-poss(20)
Angabe von Benutzer- oder Benutzergruppenkennungen, die in das Guard eingetragen werden.

USER-IDENTIFICATION = list-poss(20): <name 1..8 with-wild(20)>
Namen von Benutzerkennungen

USER-IDENTIFICATION = list-poss(20): *GROUP(...)
Angabe einer Benutzergruppe als Menge von Benutzerkennungen.

GROUP-IDENTIFICATION =
Name einer Benutzergruppe

GROUP-IDENTIFICATION = *UNIVERSAL
Der Name der Benutzergruppe ist *UNIVERSAL.

GROUP-IDENTIFICATION = <name 1..8 with-wild(20)>
Benutzergruppe

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Benutzerkennungsguard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
2	0	DEF3012	Bei der Verarbeitung von Benutzerkennungsguards, die mit Musterzeichen angegeben wurden, konnten nicht alle selektierten Benutzerkennungsguards korrekt bearbeitet werden.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3402	Kein Benutzerkennungsguard entspricht den Auswahlkriterien.
	64	DEF3403	Eine einzufügende Kennung ist bereits im Benutzerkennungsguard enthalten.
	64	DEF3406	Es passt keine weitere Kennung mehr in das Benutzerkennungsguard.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

CHANGE-GUARD-FILE
Guardskatalog austauschen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: GUARD-ADMINISTRATION

Mit diesem Kommando kann der Guardskatalog im laufenden Betrieb gewechselt werden.

Dieses Kommando ist nur für Benutzer mit dem Privileg GUARD-ADMINISTRATION zugelassen. Dieses Kommando ist nicht MSCF- oder RFA-fähig.

Tritt beim Wechsel ein Fehler auf, wird automatisch eine Recovery-Maßnahme eingeleitet, die versucht, den ursprünglichen Zustand wiederherzustellen. Start, Ende und Ergebnis des Katalogaustausches sowie eine eventuell eingeleitete Recovery-Maßnahme werden auf Konsole protokolliert.

Da der aktuelle Guardskatalog im laufenden Betrieb ständig geöffnet ist, kann ein mit ARCHIVE gesicherter Guardskatalog nur als Backup-Katalog eingespielt werden. Das Kommando CHANGE-GUARD-FILE muss verwendet werden, wenn der geöffnete aktuelle Guardskatalog durch den Backup-Katalog ersetzt werden soll.

CHANGE-**GUARD-FILE**
PUBSET = <cat- id 1..4>

PUBSET = <cat-id 1..4>
Angabe des Pubsets, auf dem der Guardskatalog ausgetauscht werden soll.

Folgende Namenskonventionen sind zu beachten:

– SYSCAT.GUARDS

  Aktueller Guardskatalog

  Bedeutung:

  Vor Kommandoausführung: Der **auszutauschende** Guardskatalog
  Nach Kommandoausführung: Der **ausgetauschte** Guardskatalog

SYSCAT.GUARDS.BAK

Guardskatalog, der den aktuellen Guardskatalog ersetzen soll

Bedeutung:

Vor Kommandoausführung: Der Backup-Guardskatalog

Nach Kommandoausführung: Der aktuelle Guardskatalog

– SYSCAT.GUARDS.datum.uhrzeit

  Ehemaliger Guardskatalogs nach dem Austausch.

Der Wechsel des Guardskatalogs findet nur statt, wenn folgende Bedingungen erfüllt sind:

– Das Kommando wird unter der Benutzerkennung eines Guards-Administrators ausgeführt.
– Es existiert eine Datei SYSCAT.GUARDS, sie ist geöffnet und ein gültiger Guardskatalog. D. h. sie muss durch die Guards-Verwaltung eingerichtet worden sein.
– Es existiert eine Datei SYSCAT.GUARDS.BAK, sie ist geschlossen und ein gültiger Guardskatalog. D. h. sie muss durch die Guards-Verwaltung eingerichtet worden sein, z.B. indem ein mit ARCHIVE gesicherter Guardskatalog bei der Rekonstruktion entsprechend umbenannt wurde.
– Falls die bestehende Backup-Datei SYSCAT.GUARDS.BAK mit BLKSIZE=(STD,2) katalogisiert ist, so wird sie umkatalogisiert und erhält den Namen SYSCAT.GUARDS.BAK.datum.uhrzeit. Dann wird sie in eine neue Datei mit BLKSIZE=(STD,4) und dem Namen SYSCAT.GUARDS.BAK kopiert. Diese wird so zur aktuellen Backup-Datei.

Falls sich der Guardskatalog nach der Kommandoausführung auf Grund eines Systemfehlers in einem nicht ordnungsgemäßen Zustand befindet, muss versucht werden, den Fehler mit dem Kommando /REPAIR-GUARD-FILE zu beheben (siehe Seite 619).

Ein leerer Guardskatalog kann durch einen mit ARCHIVE gesicherten Guardskatalog ersetzt werden.

ACHTUNG!
Ein Guardskatalog kann nicht mit dem Kommando COPY-FILE kopiert werden, weil dabei das Kennzeichen verloren geht, dass es sich um einen Guardskatalog handelt. Das Kennzeichen wird von GUARDS beim Einrichten eines leeren Katalogs gesetzt. Beim Umkatalogisieren des Katalogs mit dem Kommando /MODIFY-FILE-ATTRIBUTES bleibt es erhalten.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
32	PRO1008	Der aktuelle oder der Austausch-Guardskatalog existiert nicht
64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
64	PRO1020	Kein Speicher mehr vorhanden
64	PRO1040	Der aktuelle oder der Austausch-Guardskatalog ist kein Guards-katalog
64	PRO1041	Der aktuelle oder der Austausch-Guardskatalog hat die falsche Ver-sion
64	PRO1047	Der Austausch eines Guardskatalogs auf einem fremden Rechner ist nicht möglich
64	PRO1048	Der aktuelle oder der Austausch-Guardskatalog befindet sich nicht auf dem Control-Volume-Set des SM-Pubsets
64	PRO1049	Der Austausch-Guardskatalog ist geöffnet
64	PRO1050	Der aktuelle Guardskatalog ist geschlossen und wird daher für den Austausch nicht akzeptiert
64	PRO1051	Der aktuelle oder der Austausch-Guardskatalog enthält keinen Header-Satz und wird daher als Guardskatalog nicht anerkannt
64	PRO1052	DVS-Fehler beim Prüfen des aktuellen oder des Austausch-Guards-katalogs
64	PRO1053	DVS-Fehler beim Prüfen der Version des Austausch-Guardskatalogs
64	PRO1054	DVS-Fehler beim Schließen und Wiedereröffnen des Guardskatalogs
64	PRO1055	DVS-Fehler beim Umbenennen des Guardskatalogs
128	PRO1037	Guardskatalog wird bereits ausgetauscht
128	PRO1038	Aktueller Guardskatalog ist wegen eines Zugriffs gesperrt
128	PRO1045	Es findet gerade ein Masterwechsel statt
128	PRO1046	Das Pubset steht wegen einer SM-Pubset-Generierung unter der Kontrolle von SMPGEN

COPY-GUARD
Guard kopieren

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando kann ein Guard kopiert werden. Der Eigentümer darf nur seine eigenen Guards kopieren. Benutzer mit dem Privileg GUARD-ADMINISTRATION dürfen fremde Guards in ihre oder unter andere Kennungen kopieren. Alle anderen Benutzer dürfen ein fremdes Guard nur in die eigene Kennung kopieren und das auch nur, wenn dies durch das SCOPE-Attribut (festgelegt bei der Definition der Attribute) gestattet ist.

Dieses Kommando darf unter RFA eingesetzt werden, wenn Quell- und Ziel-Guard auf dem gleichen Rechner lokal zugreifbar sind.

COPY-GUARD
FROM-GUARD = <filename 1..24 without-gen-vers>
,**TO-GUARD** = <filename 1..24 without-gen-vers>
,**REPL**ACE**-OLD-GUARD** = ***NO** / ***Y**ES / ***BY-DIALOG**

FROM-GUARD = <filename 1..24 without-gen-vers>
Namensangabe des Guards, das kopiert werden soll (Quell-Guard).

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

TO-GUARD = <filename 1..24 without-gen-vers>
Namensangabe des Guards, in das kopiert werden soll (Ziel-Guard). Nur Benutzer mit dem Privileg GUARD-ADMINISTRATION dürfen Guards zwischen Benutzerkennungen kopieren.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

REPLACE-OLD-GUARD =
Angabe, wie bei einem bereits existierenden Guard verfahren werden soll.

REPLACE-OLD-GUARD = *NO
Ein existierendes Guard wird nie überschrieben; das Guard wird nicht kopiert.

REPLACE-OLD-GUARD = *YES
Ein bereits existierendes Guard wird ohne Rückfrage überschrieben.

REPLACE-OLD-GUARD = *BY-DIALOG
Im Dialog-Betrieb kann der Anwender bei Angabe dieser Option entscheiden, ob ein bereits existierendes Guard überschrieben werden soll oder nicht. Wird diese Option im Batch-betrieb verwendet, so verhält sich das Kommando wie bei REPLACE-OLD-GUARD = *NO.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	PRO1011	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1006	Das angegebene Guard existiert bereits
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1024	Nutzung des Guards nicht zugelassen
	64	PRO1025	Remote-Copy nicht möglich
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt

Beispiel

Es soll das Guard GUARDEXA in das bereits existierende Guard EXAGUARD kopiert werden. Um das Überschreiben zu bestätigen, wird die Dialog-Kontrolle auf *BY-DIALOG gesetzt:

```
/copy-guard from-guard=guardexa,to-guard=exaguard, -
/           replace-old-guard=*by-dialog
%  PRO1034 GUARD ':N:$SECOSMAN.EXAGUARD' EXISTS ALREADY.
           OVERWRITE/ REPLY (Y=YES; N=NO)? y
```

CREATE-GUARD
Guard einrichten

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando wird ein Guard angelegt und erhält den Typ UNDEF. Nichtprivilegierte Benutzer können Guards nur für die eigene Kennung anlegen. Ein Guard-Administrator kann auch Guards für andere Kennungen anlegen.

Ein mit diesem Kommando erzeugtes Guard enthält noch keinen Schutzmechanismus und kann daher noch keine Schutzfunktion ausüben.

CREATE-GUARD
GUARD-NAME = <filename 1..24 without-gen-vers> ,**SCOPE** = ***USER-ID** / ***USER-GROUP** / ***HOST-SYS**TEM ,**USER-INF**ORMATION = '␣' / <c-string 1..80 with-low>

GUARD-NAME = <filename 1..24 without-gen-vers>
Name des anzulegenden Guards. Die Länge des eigentlichen Namens, ohne catid und userid, beträgt 8 Zeichen.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SCOPE =
Legt fest, wer dieses Guard zum Schutz seiner Objekte verwenden darf. Das Verwaltungsrecht (Löschen, Ändern eines Guards) bleibt beim Eigentümer.

Der Guardadministrator ist berechtigt, seine eigenen Dateien mit fremden Guards zu schützen, ohne dass der Scope dieser Guards auf *HOST-SYSTEM eingestellt sein muss und ohne das bei SCOPE=*USER-GROUP eine Gruppenzugehörigkeit vorliegen muss.

SCOPE = *USER-ID
Nur der Eigentümer darf das Guard verwenden.

SCOPE = *USER-GROUP
Alle Mitglieder der Benutzergruppe des Eigentümers dürfen das Guard verwenden.

SCOPE = *HOST-SYSTEM
Jeder darf das Guard verwenden.

USER-INFORMATION = <c-string 1..80 with-low>
Es kann ein wahlfreier Kommentar-Text hinterlegt werden.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1006	Das angegebene Guard existiert bereits
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	128	PRO1036	Guardskatalog gesperrt

Beispiel

```
/create-guard guard-name=guardexa, -
/             user-information='GUARD FUER DIE GUARD-BEISPIELE'
/show-guard-attributes

     Guard name          Scope   Type      Creation Date       Last Mod Date
------------------------------------------------------------------------------
:N:$SECOSMAN.GUARDEXA     USR  UNDEF   2017-09-29/10:52:28 2017-10-03/10:52:28
                          GUARD FUER DIE GUARD-BEISPIELE
------------------------------------------------------------------------------
Guards selected: 1                                              End of display
```

DELETE-GUARD
Guard löschen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können Guards gelöscht werden.

DELETE-GUARD
GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***GUARD-CHA**NGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Angabe der Guards, die gelöscht werden sollen. Im Namen dürfen Musterzeichen enthalten sein. Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator angeben.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Guard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Guards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	PRO1011	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt

Beispiel

Aus einer Liste von vier Guards sollen zwei gelöscht werden. Dafür wird die Dialog-Option DIALOG-CONTROL=*GUARD-CHANGE verwendet:

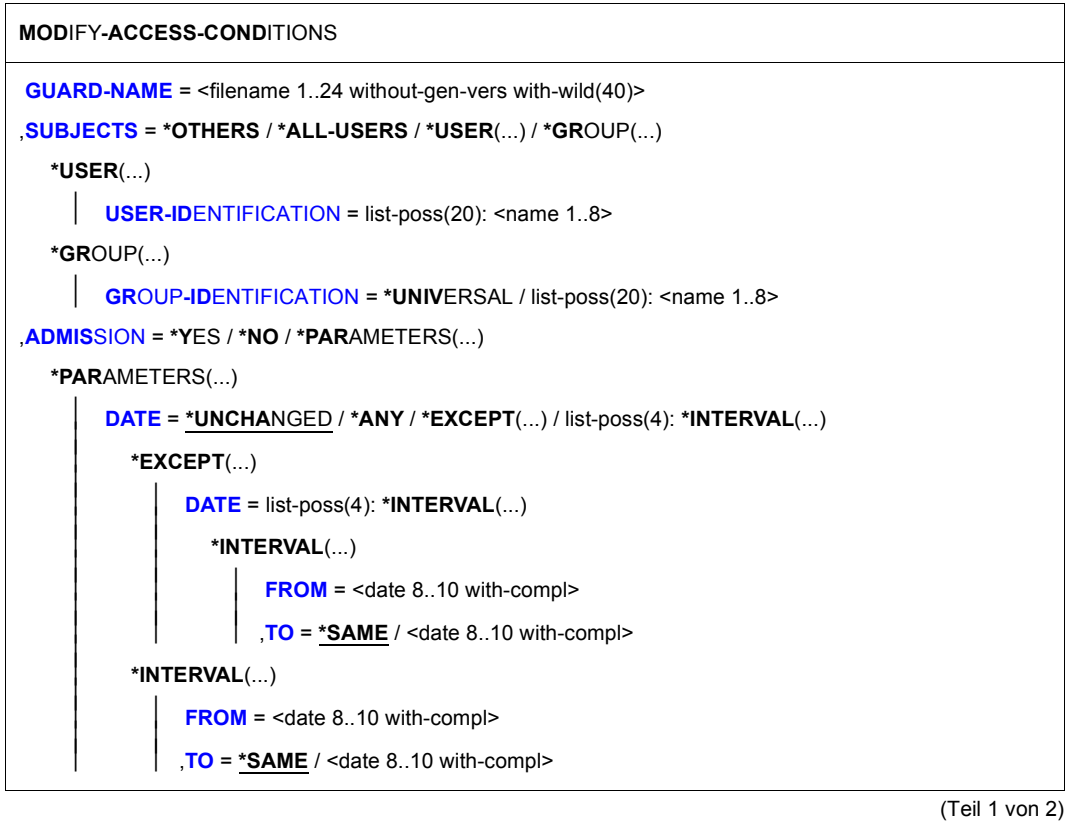
```
/delete-guard guard-name=$secosman.*,dialog-control=*guard-change
% PRO1010 DELETE GUARD(S) ':N:$SECOSMAN.EXAGUARD'? REPLY (Y=YES; N=NO;
T=TERMINATE COMMAND)?n
% PRO1010 DELETE GUARD(S) ':N:$SECOSMAN.GUARDEXA'? REPLY (Y=YES; N=NO;
T=TERMINATE COMMAND)?n
% PRO1010 DELETE GUARD(S) ':N:$SECOSMAN.KALLE'? REPLY (Y=YES; N=NO;
T=TERMINATE COMMAND)?y
% PRO1010 DELETE GUARD(S) ':N:$SECOSMAN.SECGUAD'? REPLY (Y=YES; N=NO;
T=TERMINATE COMMAND)?y
```

MODIFY-ACCESS-CONDITIONS
Zugriffsbedingungen ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Zugriffsbedingungen in einem oder mehreren Guards geändert. Die Änderungen können dabei durch erneute Kommandoaufrufe nacheinander für jeweils einen der möglichen Subjekttypen *USER, *GROUP, *OTHERS und *ALL-USERS angegeben werden.



(Teil 1 von 2)

,**TIME** = ***UNCHA**NGED / ***ANY** / ***EXCEPT**(...) / list-poss(4): ***INTERVAL**(...)

***EXCEPT**(...)

TIME = list-poss(4): ***INTERVAL**(...)

***INTERVAL**(...)

FROM = <time 1..8>

,**TO** = <time 1..8>

***INTERVAL**(...)

FROM = <time 1..8>

,**TO** = <time 1..8>

,**WEEKDAY** = ***UNCHA**NGED / ***ANY** / ***EXCEPT**(...) / list-poss(7): ***MONDAY** / ***TUESDAY** / ***WEDNESDAY** / ***THURSDAY** / ***FRIDAY** / ***SATURDAY** / ***SUNDAY**

***EXCEPT**(...)

WEEKDAY = list-poss(7): ***MONDAY** / ***TUESDAY** / ***WEDNESDAY** / ***THURSDAY** / ***FRIDAY** / ***SATURDAY** / ***SUNDAY**

,**PRIVIL**EGE = ***UNCHA**NGED / ***ANY** / ***EXCEPT**(...) / list-poss(31): <text>

***EXCEPT**(...)

PRIVILEGE = list-poss(31): <text>

,**PROG**RAM = ***UNCHANGED** / ***ANY** / list-poss(4): <filename 1..54 without-gen-vers with-wild> / ***PHASE**(...) / ***MOD**ULE(...)

***PHASE**(...)

LIBRARY = <filename 1..54 without-gen-vers with-wild>

,**ELEM**ENT = <composed-name 1..64 with-under with-wild>

,**VERSION** = ***ANY** / <composed-name 1..24 with-under with-wild>

***MOD**ULE(...)

LIBRARY = <filename 1..54 without-gen-vers with-wild>

,**ELEM**ENT = <composed-name 1..32 with-under with-wild>

,**VERSION** = ***ANY** / <composed-name 1..24 with-under with-wild>

,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***GUARD-CHANGE** / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

(Teil 2 von 2)

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>

Angabe eines oder mehrerer Guards, in denen Zugriffsbedingungen geändert werden sollen. Im Namen dürfen Musterzeichen enthalten sein.

Wird der Guardname mit Hilfe von Musterzeichen angegeben, werden nur die Guards berücksichtigt, die den Guardtyp STDAC besitzen.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator angeben.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SUBJECTS =
Angabe, für welchen Subjekttyp die Zugriffsbedingungen geändert werden sollen.
Mögliche Subjekttypen sind:
– *USER (Benutzerkennungen),
– *GROUP (Benutzergruppen)
– *OTHERS (alle nicht explizit genannten Benutzerkennungen).

Zusätzlich existiert noch der Pseudo-Subjekttyp *ALL-USERS mit dem Zusatzbedingungen festgelegt werden können.

Sollen Zugriffsbedingungen für mehrere dieser Subjekttypen geändert werden, muss das Kommando entsprechend oft eingegeben werden.

SUBJECTS = *OTHERS
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für die Benutzer gelten sollen, die keiner der beiden Listen SUBJECTS=*USER oder *GROUP enthalten sind.

SUBJECTS = *ALL-USERS
Angabe, dass es sich bei den mit dem Operanden ADMISSION festgelegten Bedingungen um **Zusatz**bedingungen handelt.

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen, als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

SUBJECTS = *USER(...)
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für bestimmte Benutzerkennungen gelten sollen.

USER-IDENTIFICATION = list-poss(20): <name 1..8>
Angabe von maximal 20 Benutzerkennungen, für die die mit dem Operanden ADMISSION definierten Zugriffsbedingungen gelten sollen. Sollen mehr als 20 Benutzerkennungen aufgezählt werden, muss der Kommandoaufruf entsprechend oft wiederholt werden.

SUBJECTS = *GROUP(...)
Angabe, dass die mit dem Operanden ADMISSION festgelegten Bedingungen für bestimmte Benutzergruppen gelten sollen.

GROUP-IDENTIFICATION = *UNIVERSAL / list-poss(20): <name 1..8>
Angabe von maximal 20 Gruppenkennungen, für die die mit dem Operand ADMISSION definierten Zugriffsbedingungen gelten sollen. Sollen mehr als 20 Gruppenkennungen aufgezählt werden, muss der Kommandoaufruf entsprechend oft wiederholt werden.

ADMISSION =
Legt die Zugriffsbedingungen für den mit dem Operand SUBJECTS angegebenen Subjekttyp (*USER, *GROUP, *OTHERS) oder Zusatzbedingungen für alle Subjekttypen (*ALL-USERS) fest.

ADMISSION = *YES
Legt fest, dass dem mit dem Operanden SUBJECTS angegebenen Subjekttyp der Zugriff gestattet ist.

Zu beachten ist hierbei das Zusammenspiel der der Bedingungen für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) mit den **Zusatz**bedingungen für den Pseudo-Subjekttyp *ALL-USERS:

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen, als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

ADMISSION = *NO
Legt fest, dass dem mit dem Operanden SUBJECTS angegebenen Subjekttyp oder Pseudo-Subjektyp der Zugriff verboten ist.

Erfolgt diese Angabe für den Pseudo-Subjekttyp *ALL-USERS, ist der Zugriff für alle Subjektypen **generell verboten**. Dies gilt unabhängig von den für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) festgelegten Bedingungen.

ADMISSION = *PARAMETERS(...)
Genauere Spezifizierung der Zugriffsbedingungen, die dem mit dem Operanden SUBJECTS angegebenen Subjekttyp oder Pseudo-Subjektyp gelten sollen.

Zu beachten ist hierbei das Zusammenspiel der der Bedingungen für die einzelnen Subjekttypen (*USER, *GROUP und *OTHERS) mit den **Zusatz**bedingungen für den Pseudo-Subjekttyp *ALL-USERS:

Falls Zusatzbedingungen festgelegt sind, gilt: Ein Subjekttyp erhält nur dann Zugriffserlaubnis, wenn ihm sowohl die für den Subjekttyp selbst festgelegten Bedingungen, als auch die für den Pseudo-Subjekttyp *ALL-USERS festgelegten Bedingungen den Zugriff erlauben.

Weitere Information zur Festlegung und Überprüfung von Zugriffsbedingungen finden Sie im Abschnitt „Zugriffsbedingungen definieren“ auf Seite 443.

DATE = *UNCHANGED / *ANY / *EXCEPT(...) / list-poss(4): *INTERVAL(...)
Angabe von Kalenderdaten, an denen der Zugriff erlaubt oder untersagt ist. Jahresangaben müssen zwischen 1991 und 2099 liegen. SDF erlaubt die Angabe des Datums sowohl mit vierstelliger als auch mit zweistelliger Jahreszahl. Ein Datum mit zweistelliger Jahreszahl (jj-mm-tt) wird ergänzt zu:

20jj-mm-tt, falls jj < 60 oder
19jj-mm-tt, falls jj ≥ 60.

DATE = *ANY
Es kann jederzeit auf das Objekt zugegriffen werden.

DATE = *EXCEPT(DATE = list-poss(4): *INTERVAL(...))
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff untersagt ist.

FROM = <date 8..10 with-compl>
Gibt den Anfang des Intervalls an.

TO = *SAME
Gibt an, dass das Ende gleich dem Anfang des Intervalls ist. (Bedingung gilt nur an einem Tag).

TO = <date 8..10 with-compl>
Gibt das Ende des Intervalls an.

DATE = list-poss(4): *INTERVAL(...)
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff erlaubt ist.

FROM = <date 8..10 with-compl>
Gibt den Anfang des Intervalls an.

TO = *SAME
Gibt an, dass das Ende gleich dem Anfang des Intervalls ist. (Bedingung gilt nur an einem Tag).

TO = <date 8..10 with-compl>
Gibt das Ende des Intervalls an.

TIME = *UNCHANGED / *ANY / *EXCEPT(...) / list-poss(4): *INTERVAL(...)
Angabe von Tageszeiten, an denen der Zugriff erlaubt oder untersagt ist. Sekundenangaben werden ignoriert. Stunden- und Minutenangaben sind durch Doppelpunkte voneinander zu trennen. Angaben ohne Doppelpunkt werden als Stundenangabe interpretiert.

TIME = *ANY
Es kann jederzeit auf das Objekt zugegriffen werden.

TIME = *EXCEPT(TIME = list-poss(4): *INTERVAL(...))
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff untersagt ist.

FROM = <time 1..8>
Gibt den Anfang des Intervalls an.

TO = <time 1..8>
Gibt das Ende des Intervalls an.

TIME = list-poss(4): *INTERVAL(...)
Es können maximal 4 Intervalle definiert werden, in denen der Zugriff erlaubt ist.

FROM = <time 1..8>
Gibt den Anfang des Intervalls an.

TO = <time 1..8>
Gibt das Ende des Intervalls an.

WEEKDAY = *UNCHANGED / *ANY / *EXCEPT(...) / list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
Legt einen oder mehrere Wochentage fest, an denen der Zugriff erlaubt ist.

WEEKDAY = *ANY
Zugriff ist an jedem Wochentag erlaubt.

WEEKDAY = *EXCEPT(...)
Legt die Tage fest, an denen der Zugriff untersagt ist.

WEEKDAY = list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
Hier wird die Liste der Tage festgelegt, an denen der Zugriff untersagt ist.

WEEKDAY = list-poss(7): *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY / *SUNDAY
Zugriff ist nur an den angegebenen Tagen erlaubt.

PRIVILEGE = *UNCHANGED / *ANY / *EXCEPT(...) / list-poss(31): <text>
Spezifiziert die Privilegien, mit denen der Zugriff erlaubt ist.

PRIVILEGE = *ANY
Es ist kein besonderes Privileg für den Zugriff notwendig.

PRIVILEGE = *EXCEPT(...)

PRIVILEGE = list-poss(31): <text>
Untersagt ist ein Zugriff mit den angegebenen Privilegien. Mögliche Privilegien siehe Seite 128.

PRIVILEGE = list-poss(31): <text>
Nur Benutzer mit den angegebenen Privilegien dürfen zugreifen. Mögliche Privilegien siehe Seite 128.

PROGRAM = *UNCHANCHED / *ANY / list-poss(4): <filename 1..54 without-gen-vers with-wild> / *PHASE(...) / *MODULE(...)
Legt fest, über welches Programm ein Zugriff erfolgen darf. Es können maximal 4 Programmnamen angegeben werden. Die benannten Programme können entweder als gebundene Phase in einer Datei, oder als Objektmodul (OM) bzw. Binderlademodul (LLM) als Bibliothekselement vorliegen.

Hinweise

Um Konflikte bei der Verwendung von Moduln des Typs OM und LLM zu vermeiden, wird empfohlen, die Module in unterschiedlichen Bibliotheken zu führen (siehe auch Handbuch „LMS“ [23]).

Bei Zugriffen über ein Programm wird geprüft, ob das zugreifende Programm geladen und die Kontrolle übernommen hat.

Soll auf ein mit Guards geschütztes Objekt nur über ein Programm zugegriffen werden, ist auf Folgendes zu achten:

Die Datei oder Bibliothek, in der das zum Zugriff berechtigte Programm abgelegt ist, sollte selber so geschützt werden, dass das Programm weder modifiziert noch gelesen werden kann. Es könnte sonst von einem Benutzer (der keinen Zugriff auf das geschützte Objekt hat) unter dessen Benutzerkennung kopiert und mit dem Namen des zum Zugriff berechtigten Programms benannt werden.

PROGRAM = *ANY
Der Zugriff darf über jedes beliebige Programm erfolgen.

PROGRAM = <filename 1..54 without-gen-vers with-wild>
Das Programm ist eine gebundene Phase und liegt als Datei vor. Wird der Dateiname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

PROGRAMM = *PHASE(...)
Das Programm ist eine gebundene Phase und liegt als Bibliothekselement des Typs C vor.

LIBRARY = <filename 1..54 without-gen-vers with-wild>
Name der Bibliothek, in der die gebundene Phase eingetragen ist. Wird der Bibliotheksname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

ELEMENT = <composed-name 1..64 with-under with-wild>
Name des Bibliothekselements.

VERSION = *ANY
Es wird keine spezielle Version für das Bibliothekselement festgelegt.

VERSION = <composed-name 1..24 with-under with-wild>
Version des Bibliothekselements.

PROGRAM = *MODULE(...)
Das Programm ist ein Objektmodul (OM) oder ein Bindelademodul (LLM) und liegt als Bibliothekselement vom Typ R bzw. L vor.

LIBRARY = <filename 1..54 without-gen-vers with-wild>
Name der Bibliothek, in der der Objekt- bzw. Lademodul eingetragen ist. Wird der Bibliotheksname ohne Pfad angegeben, wird er mit der Default-Pubset-ID und der Benutzerkennung des Kommandogebers vervollständigt.

ELEMENT = <composed-name 1..32 with-under with-wild>
Name des Bibliothekselements.

VERSION = *ANY
Es wird keine spezielle Version für das Bibliothekselement festgelegt.

VERSION = <composed-name 1..24 with-under with-wild>
Version des Bibliothekselements.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Guard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Guards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	PRO1011	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1015	Das angegebene Subjekt ist nicht im Guard enthalten
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1026	Kennung bereits in Bedingung enthalten
	64	PRO1027	Bedingungsbereich voll
	64	PRO1028	Guard hat falschen Typ
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	64	PRO1042	Nutzer nicht registriert
2	64	PRO1035	Kommando nicht ausgeführt
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt
	128	PRO1038	Guardskatalog durch ARCHIVE gesperrt

MODIFY-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando wird eine Miteigentümerschutzregel in einem Regelbehälter (Guard des Typs COOWNERP) modifiziert.

Ein Anwender kann nur Regelbehälter unter seiner eigenen Benutzerkennung modifizieren. Ein Guard-Administrator darf Regelbehälter fremder Benutzerkennungen modifizieren.

MODIFY-**COOW**NER-**PROTECT**ION-**RULE** (**MOD-COO-PRO-R**)
RULE-CONTAINER-**GUARD** = <filename 1..24 without-gen-vers with-wild(40)> ,**PROTECT**ION-**RULE** = <alphanum-name 1..12> ,**NEW-NAME** = ***SAME** / <alphanum-name 1..12> ,**RULE-POS**ITION = ***UNCHA**NGED / ***LAST** / ***BEFORE**(...) ***BEFORE**(...) **PROTECT**ION-**RULE** = <alphanum-name 1..12> ,**PROTECT-OBJ**ECT = ***PAR**AMETERS(...) ***PAR**AMETERS(...) **NAME** = ***UNCHA**NGED / <filename 1..41 without-cat-user-gen with-wild(80)> ,**COND**ITION-**GUARD** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers> ,**TSOS-ACCESS** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***RESTRICTED** ,**GUARD-CHECK** = ***Y**ES / *NO ,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***RULE-CONT**AINER-**CHA**NGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ COOWNERP, in dem eine Regel modifiziert werden soll.

Der Behältername kann zwar beliebig gewählt werden, für die Zugriffskontrolle werden jedoch ausnahmslos Regelbehälter mit fest vorgeschriebenen Namen verwendet (aktive Regelbehälter, siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 479).

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel durch Absetzen eines einzigen Kommandos in mehreren Behältern modifiziert wird, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE = <alphanumeric name 1..12>
Name der Regel, die modifiziert werden soll. Doppelte Namen in einem Behälter sind nicht erlaubt.

NEW-NAME =
Mit diesem Operand kann die zu bearbeitende Regel umbenannt werden.

NEW-NAME = *SAME
Der Name bleibt unverändert.

NEW-NAME = <alphanumeric name 1..12>
Neuer Name, den die Regel erhalten soll.

RULE-POSITION =
Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt werden soll. Die Reihenfolge der Regeln ist ausschlaggebend bei der Miteigentümerüberprüfung (siehe Abschnitt „Suchlogik“ auf Seite 462).

RULE-POSITION = *UNCHANGED
Die Regelposition bleibt unverändert.

RULE-POSITION = *LAST
Die Regel soll an die letzte Position im Regelbehälter gestellt werden.

RULE-POSITION = *BEFORE(...)
Die Regel soll vor eine benannte Regel im Regelbehälter gestellt werden.

PROTECTION-RULE = <alphanumeric name 1..12>
Name einer vorhandenen Regel im Regelbehälter, vor die die zu modifizierende Regel gestellt werden soll. Das Kommando wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

PROTECT-OBJECT = *PARAMETERS(...)
Angaben über das Objekt, auf das sich die zu bearbeitende Regel beziehen soll.

NAME =
Dieser Operand bezeichnet den Namen des Objekts, für das die zu modifizierende Regel gelten soll.

NAME = *UNCHANGED
Der Objektname bleibt unverändert.

NAME = <filename 1..41 without-cat-gen-user with-wild(80)>
Name des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

CONDITION-GUARD =
Name des Guards vom Typ STDAC, das die Zugriffsbedingungen enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

CONDITION-GUARD = *UNCHANGED
Der Guardname bleibt unverändert.

CONDITION-GUARD = *NONE
Es wird kein Guardname angegeben. Der Miteigentümerschutz ist für das Objekt außer Kraft gesetzt. Es gibt keine Miteigentümer für das Objekt.

CONDITION-GUARD = <filename 1..18 without-cat-gen-ver>
Name eines Guards des Typs STDAC, das die Zugriffsbedingungen enthält, die ein Miteigentümer erfüllen muss. Der Name darf keine Katalogkennung enthalten. Seine Länge ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.
Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

TSOS-ACCESS =
Angabe über die Miteigentümerschaft der Benutzerkennung TSOS.

TSOS-ACCESS = *UNCHANGED
Die Miteigentümerschaft von TSOS für das Objekt bleibt unverändert.

TSOS-ACCESS = *SYSTEM-STD
Die Benutzerkennung TSOS erhält die volle Miteigentümerschaft für das Objekt.

TSOS-ACCESS = *RESTRICTED
Die Benutzerkennung TSOS erhält eine eingeschränkte Miteigentümerschaft für das Objekt. Die Kommandos und Makros, auf die sich eine Einschränkung der TSOS-Miteigentümerschaft auswirkt, finden Sie im Abschnitt „Wirksamkeit der TSOS-Einschränkung“ auf Seite 939.

GUARD-CHECK =
Bei Kommandodurchführung kann wahlweise die Verfügbarkeit des in der Regel namentlich genannten Guards überprüft werden.

GUARD-CHECK = *YES
Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt es das Guard nicht, oder ist der Eigentümer des gerade bearbeiteten Regelbehälters nicht berechtigt, das Guard zu verwenden, wird das Kommando nicht durchgeführt.

GUARD-CHECK = *NO
Das Kommando wird unabhängig davon durchgeführt, ob das genannte Guard verfügbar ist oder vom Eigentümer des gerade bearbeiteten Regelbehälters verwendet werden darf.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *RULE-CONTAINER-CHANGE
Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	COO3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
2	0	COO3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
	1	COO3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	COO3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	COO3300	Der angegebene Regelbehälter existiert nicht.
	64	COO3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	COO3303	Es passt keine weitere Regel mehr in den Regelbehälter.
	64	COO3304	Es wurde kein Regelbehälter selektiert.
	64	COO3305	Der angegebene Regelname zum Positionieren wurde nicht gefunden.
	64	COO3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	COO3307	Eine einzufügende Regel existiert bereits.
	64	COO3308	Eine Benutzerkennung ist unbekannt.
	64	COO3309	Keine Unterstützung für einen Remote-File-Access.
	64	COO3310	Eine Regel wurde im Regelbehälter nicht gefunden.
	64	COO3311	Ein angegebenes Guard für Zugriffsbedingungen ist nicht zugreifbar
	64	COO3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	COO3314	Fehler im Kommunikationsmittel des MRS.
	64	COO3315	Ein angegebenes Public Volume Set ist der lokalen Guards-Verwaltung nicht bekannt
	128	COO3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	COO3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	COO3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

MODIFY-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können Schutzattribut-Standardwerte in einem Attributguard geändert werden.

Ein Anwender kann nur Attributguards seiner eigenen Benutzerkennung ändern. Ein Guard-Administrator darf Attributguards fremder Benutzerkennungen ändern

Die Attributmodifikationen werden bei einem Aufruf des Kommandos immer nur für einen der Attributbereiche *CREATE-OBJECT oder *MODIFY-OBJECT-ATTR durchgeführt.

*Bedeutung des Operandenwertes *SYSTEM-STD*

Der Wert *SYSTEM-STD steht stellvertretend für einen in der hierarchisch höheren Instanz vorgegebenen Attributwert.

Die hierarchisch höhere Instanz ist
– der pubsetglobale Regelbehälter,
  wenn ein Attributguard aus einem benutzerspezifischen Regelbehälter heraus ausgewertet wird oder wenn es keinen benutzerspezifischen Regelbehälter gibt
– die herkömmliche Systemvoreinstellung,
  wenn ein Attributguard aus einem pubsetglobalen Regelbehälter heraus ausgewertet wird oder wenn es keinen pubsetglobalen Regelbehälter gibt.

MODIFY-**DEFAULT-PROTECT**ION-**ATTR** (**MOD-DEF-PRO-A**)

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,**ATTR-SCOPE** = ***CRE**ATE-**OBJ**ECT / ***MOD**IFY-**OBJ**ECT-**ATTR**
,**ACCESS** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***WR**ITE / *READ
,**USER-ACCESS** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***OWNER-ONLY** / ***ALL-USERS** / ***SPECIAL**
,**BASIC-ACL** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / ***PAR**AMETERS(...)
*PAR**AMETERS(...)
OWNER = ***UNCHA**NGED / ***PAR**AMETERS(...)
*PAR**AMETERS(...)
READ = ***UNCHA**NGED / ***NO** / *YES
,**WR**ITE = ***UNCHA**NGED / ***NO** / *YES
,**EXEC** = ***UNCHA**NGED / ***NO** / *YES
,**GR**OUP = ***UNCHA**NGED / ***PAR**AMETERS(...)
*PAR**AMETERS(...)
READ = ***UNCHA**NGED / ***NO** / *YES
,**WR**ITE = ***UNCHA**NGED / ***NO** / *YES
,**EXEC** = ***UNCHA**NGED / ***NO** / *YES
,**OTHERS** = ***UNCHA**NGED / ***PAR**AMETERS(...)
*PAR**AMETERS(...)
READ = ***UNCHA**NGED / ***NO** / *YES
,**WR**ITE = ***UNCHA**NGED / ***NO** / *YES
,**EXEC** = ***UNCHA**NGED / ***NO** / *YES
,**GUARDS** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / ***PAR**AMETERS(...)
*PAR**AMETERS(...)
READ = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>
,**WR**ITE = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>
,**EXEC** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>

(Teil 1 von 2)

,**READ-PASS**WORD = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**WR**ITE-**PASS**WORD = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**EXEC-PASS**WORD = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / ***SECRET** /
<c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>

,**DESTROY**-BY-DELETE = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NO** / *YES

,**SPACE-RELE**ASE-**LOCK** = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NO** / *YES

,**EXPIR**ATION-DATE = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***TODAY** / ***TOMORROW** / <date with-compl> /
<integer 0..99999>

,**FREE-FOR-DEL**ETION = ***UNCHA**NGED / ***SYS**TEM-**STD** / ***NONE** / <date with-compl> / <integer 0..99999>

,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***GUARD-CHANGE** / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

(Teil 2 von 2)

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Guards vom Typ DEFPATTR, in dem Schutzattribut-Standardwerte modifiziert werden sollen. Der Guardname darf Musterzeichen enthalten, seine Länge ohne Katalog- und Benutzerkennung darf jedoch 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

ATTR-SCOPE =
In einem Attributguard werden zwei Bereiche von Attributen geführt:

1. Schutzattribute, die zukünftig beim Neueinrichten eines Objektes (zum Beispiel mit /CREATE-FILE) zum Einsatz gelangen sollen, und
2. Schutzattribute, die zukünftig beim Modifizieren von Objektattributen eines bereits angelegten Objektes (zum Beispiel mit /MODIFY-FILE-ATTRIBUTES) zum Einsatz gelangen sollen.

ATTR-SCOPE = *CREATE-OBJECT
Es wird der Attributbereich modifiziert, der zukünftig beim Neueinrichten eines Objektes für die Standardwertvergabe verwendet wird.

ATTR-SCOPE = *MODIFY-OBJECT-ATTR
Es wird der Attributbereich modifiziert, der zukünftig beim Modifizieren von Objektattributen eines bereits angelegten Objektes für die Standardwertvergabe verwendet wird.

ACCESS = *UNCHANGED / *SYSTEM-STD / *WRITE / *READ
Gibt an, welche Art von Zugriff auf das Objekt erlaubt ist.

ACCESS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

ACCESS = *WRITE
Lesende, schreibende und ausführende Objektzugriffe sind erlaubt.

ACCESS = *READ
Es sind nur lesende und ausführende Objektzugriffe erlaubt.

USER-ACCESS = *UNCHANGED / *SYSTEM-STD / *OWNER-ONLY / *ALL-USERS / *SPECIAL
Gibt an, ob fremde Benutzerkennungen auf das Objekt zugreifen dürfen.

USER-ACCESS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

USER-ACCESS = *OWNER-ONLY
Der Zugriff auf das Objekt ist nur unter der eigenen Benutzerkennung möglich, aber unter jeder Katalogkennung, unter der die (namentlich) gleiche Benutzerkennung eingerichtet ist (d.h. nicht nur unter der Katalogkennung, unter der das Objekt eingerichtet wurde). Miteigentümer haben ebenfalls Zugriff.

USER-ACCESS = *ALL-USERS
Der Zugriff auf das Objekt ist auch unter fremden Benutzerkennungen möglich.

USER-ACCESS = *SPECIAL
Das Objekt ist für alle Benutzerkennungen einschließlich der Kennungen mit dem Privileg HARDWARE-MAINTENANCE zugänglich. Zugriffe der Wartungskennung sind generell nur möglich, wenn USER-ACCESS=*SPECIAL gilt.

BASIC-ACL = *UNCHANGED / *SYSTEM-STD / *NONE / *PARAMETERS(...)
Aktiviert den Zugriffsschutz über BACL.

BASIC-ACL = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

BASIC-ACL = *NONE
Der Zugriffsschutz über BACL wird nicht aktiviert.

BASIC-ACL = *PARAMETERS(...)
Der Zugriffsschutz über BACL wird durch explizite Angaben aktiviert, sofern kein höherer Zugriffsschutz aktiv ist.

OWNER = *UNCHANGED / *PARAMETERS(...)
Legt die Zugriffsrechte für den Eigentümer und Miteigentümer der Datei fest.

OWNER = *PARAMETERS(...)
Die Zugriffsrechte des Eigentümers werden nachfolgend spezifiziert.

READ = *UNCHANGED / *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *UNCHANGED / *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *UNCHANGED / *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

GROUP = *UNCHANGED / *PARAMETERS(...)
Legt die Zugriffsrechte für Mitglieder der Gruppe des Eigentümers fest.

GROUP = *PARAMETERS(...)
Die Zugriffsrechte für Mitglieder der Benutzergruppe des Eigentümers werden nachfolgend spezifiziert.

READ = *UNCHANGED / *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *UNCHANGED / *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *UNCHANGED / *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

OTHERS = *UNCHANGED / *PARAMETERS(...)
Legt die Zugriffsrechte für alle Benutzer fest, die nicht Mitglieder der Benutzergruppe des Eigentümers sind.

OTHERS = *PARAMETERS(...)
Die Zugriffsrechte für die übrigen Benutzer werden nachfolgend spezifiziert.

READ = *UNCHANGED / *NO / *YES
Gibt an, ob Leseberechtigung gesetzt wird.

WRITE = *UNCHANGED / *NO / *YES
Gibt an, ob Schreibberechtigung gesetzt wird.

EXEC = *UNCHANGED / *NO / *YES
Gibt an, ob Ausführberechtigung gesetzt wird.

GUARDS = *UNCHANGED / *SYSTEM-STD / *NONE / *PARAMETERS(...)
Gibt an, ob die Zugriffskontrolle über GUARDS erfolgt.

GUARDS = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

GUARDS = *NONE
Die Zugriffskontrolle erfolgt nicht über GUARDS.

GUARDS = *PARAMETERS(...)
Die Zugriffskontrolle erfolgt über GUARDS. Der Guard-Name darf maximal 8 Zeichen, mit Angabe einer Benutzerkennung maximal 18 Zeichen lang sein. Eine Katalogkennung kann nicht angegeben werden, denn das Guard muss immer in dem Katalog abgelegt sein, in dem sich auch die Datei befindet!

READ =
Angaben für den Leseschutz.

READ = *UNCHANGED
Der Wert bleibt unverändert.

READ = *NONE
Es wird kein Guardname zugewiesen. Es sind keine Lesezugriffe erlaubt.

READ = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Leseschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

WRITE =
Angaben für den Schreibschutz.

WRITE = *UNCHANGED
Der Wert bleibt unverändert.

WRITE =*NONE
Es wird kein Guardname zugewiesen. Es sind keine Schreibzugriffe erlaubt.

WRITE = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Schreibschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

EXEC =
Angaben für den Ausführschutz.

EXEC = *UNCHANGED
Der Wert bleibt unverändert.

EXEC = *NONE
Es wird kein Guardname zugewiesen. Es sind keine Ausführungszugriffe erlaubt.

EXEC = <filename 1..18 without-cat-gen-vers>
Name eines Guards, das den Ausführungsschutz regelt. Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

WRITE-PASSWORD = *UNCHANGED / *SYSTEM-STD / *NONE / *SECRET / <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Schreiben. Der Operand WRITE-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

WRITE-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

WRITE-PASSWORD = *NONE
Es wird kein Schreibkennwort vergeben.

WRITE-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Schreibkennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Schreibkennwort zur Verfügung gestellt wird.

READ-PASSWORD = *UNCHANGED / *SYSTEM-STD / *NONE / *SECRET / <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Lesen. Der Operand READ-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

READ-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

READ-PASSWORD = *NONE
Es wird kein Lesekennwort vergeben.

READ-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Lesekennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Lesekennwort zur Verfügung gestellt wird.

EXEC-PASSWORD = *UNCHANGED / *SYSTEM-STD / *NONE / *SECRET / <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Kennwort zum Schutz vor unberechtigtem Ausführen. Der Operand EXEC-PASSWORD ist als "geheim" definiert. Das Eingabefeld wird im geführten Dialog dunkelgesteuert, und der eingegebene Wert wird nicht protokolliert.

EXEC-PASSWORD = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

EXEC-PASSWORD = *NONE
Es wird kein Ausführungskennwort vergeben.

EXEC-PASSWORD = *SECRET
Diese Angabe ist nur im ungeführten Dialog zulässig und ermöglicht die verdeckte Eingabe des gewünschten Ausführungskennwortes. Hierfür erfolgt eine spezielle Eingabeaufforderung, wobei ein dunkel gesteuertes Feld für das "geheime" Ausführungskennwort zur Verfügung gestellt wird.

DESTROY-BY-DELETE = *UNCHANGED / *SYSTEM-STD / *NO / *YES
Zur Erhöhung des Datenschutzes kann der Benutzer im Katalogeintrag festlegen, dass nicht mehr benötigte Daten mit X’00’ (binär Null) überschrieben werden. Bei Plattendateien wirkt sich das auf Löschoperationen und Speicherplatzfreigabe aus (siehe Kommando /MODIFY-FILE-ATTRIBUTES und /DELETE-FILE). Bei Banddateien wirkt sich das auf das Überschreiben von Restdaten bei EOF- und EOV-Verarbeitung aus (siehe Operand DESTROY-OLD-CONTENTS im Kommando /ADD-FILE-LINK).

DESTROY-BY-DELETE = *SYSTEM-STD
Als Standardwert wird der Attributwert verwendet, den die hierarchisch höhere Instanz vorsieht. Das ist der pubsetglobale Regelbehälter, wenn ein Attributguard aus einem benutzerspezifischen Regelbehälter heraus ausgewertet wird. Das sind die herkömmlichen Systemvoreinstellungen, wenn es einen pubsetglobalen Regelbehälter nicht gibt, oder wenn ein Attributguard aus einem pubsetglobalen Regelbehälter heraus ausgewertet wird.

DESTROY-BY-DELETE = *NO
Bei dieser Einstellung wirkt eine im Kommando /DELETE-FILE getroffene Vereinbarung (Operand OPTION).

Bei Plattendateien wird der Speicherplatz unverändert freigegeben, wenn nicht im Kommando /DELETE-FILE der Operand OPTION=DESTROY-ALL angegeben wird.

Bei Banddateien werden die auf dem Band folgenden Restdaten nicht überschrieben, wenn im Kommando /ADD-FILE-LINK für den aktuellen Verarbeitungslauf nicht DESTROY-OLD-CONTENTS=*YES vereinbart wird.

DESTROY-BY-DELETE = *YES
Diese Einstellung wirkt auch, wenn im Kommando /DELETE-FILE über den Operand OPTION eine andere Vereinbarung getroffen wird.

Bei Plattendateien wird freigegebener Speicherplatz automatisch mit X'00' (binär Null) überschrieben.

Bei Banddateien wird der Bandinhalt nach dem Dateiende mit X'00' (binär Null) überschrieben. Im Kommando /ADD-FILE-LINK muss das Löschen der Restdaten für den aktuellen Verarbeitungslauf nicht explizit angegeben werden.

SPACE-RELEASE-LOCK = *UNCHANGED / *SYSTEM-STD / *NO / *YES
Gibt an, ob die Freigabe von Speicherplatz mit dem Kommando /MODIFY-FILE-ATTRIBUTES bzw. FILE-Makro ignoriert werden soll.

SPACE-RELEASE-LOCK = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

SPACE-RELEASE-LOCK = *NO
Speicherplatz kann freigegeben werden.

SPACE-RELEASE-LOCK = *YES
Speicherplatz kann nicht freigegeben werden.

EXPIRATION-DATE = *UNCHANGED / *SYSTEM-STD / *TODAY / <date with-compl> / <integer 0..99999>
Schutzfrist der Datei. Bis zu dem angegebenen Datum kann die Datei nicht verändert oder gelöscht werden. Eine Schutzfrist kann nur vergeben werden, wenn die Datei bereits eröffnet wurde, das heisst, ein CREATION-DATE besitzt.

Die Schutzfrist kann, wenn sie nicht über ein Schlüsselwort spezifiziert wird, auf zwei Arten angegeben werden:

– als absolute Datumsangabe
  Datumsangabe in der Form YY-MM-DD oder YYYY-MM-DD
  (YY = Jahr, MM = Monat, DD = Tag).

– als relative Datumsangabe
  Maximal 6-stellig einschließlich Vorzeichen in der Form +n als Distanz zum aktuellen Tagesdatum.

EXPIRATION-DATE = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

EXPIRATION-DATE = *TODAY
Es wird keine Schutzfrist vergeben werden, oder eine bestehende Schutzfrist wird aufgehoben, indem sie auf das aktuelle Tagesdatum gesetzt wird.

EXPIRATION-DATE = *TOMORROW
Als Schutzfrist wird das Datum des nächsten Tages vergeben.

EXPIRATION-DATE = <date with-compl>
Die Datei ist bis zum angegebenen Datum (ausschließlich) geschützt.

EXPIRATION-DATE = <integer 0..99999>
Die Datei kann für die angegebene Anzahl von Tagen nicht verändert oder gelöscht werden.

FREE-FOR-DELETION = *UNCHANGED / *SYSTEM-STD / *NONE / <date with-compl> / integer 0..99999>
Legt fest, ab wann das Objekt ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

Das Lösch-Freigabedatum kann, wenn es nicht über ein Schlüsselwort spezifiziert wird, auf zwei Arten angegeben werden:

– als absolute Datumsangabe
Datumsangabe in der Form YY-MM-DD oder YYYY-MM-DD
(YY = Jahr, MM = Monat, DD = Tag).

– als relative Datumsangabe
Maximal 6-stellig einschließlich Vorzeichen in der Form +n als Distanz zum aktuellen Tagesdatum.

FREE-FOR-DELETION = *SYSTEM-STD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSTEM-STD“ auf Seite 584).

FREE-FOR-DELETION = *NONE
Das Objekt kann nur unter Berücksichtigung der Schutzattribute gelöscht werden.

FREE-FOR-DELETION = <date with-compl>
Das Objekt darf ab dem angegebenen Datum ohne Berücksichtigung der Schutzattribute gelöscht werden.

FREE-FOR-DELETION = <integer 0..99999>
Das Objekt kann nach der angegebenen Anzahl von Tagen ohne Berücksichtigung der Schutzattribute gelöscht werden.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Attributguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Attributguard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Attributguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Attributguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
2	0	DEF3003	Bei der Verarbeitung von Attributguards, die mit Musterzeichen angegeben wurden, konnten nicht alle selektierten Attributguards korrekt bearbeitet werden.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3351	Ein genanntes Attributguard gibt es noch nicht.
	64	DEF3352	Es wurde kein Attributguard selektiert.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

MODIFY-DEFAULT-PROTECTION-RULE
Standardschutzregel ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando wird eine Regel innerhalb eines benannten Regelbehälters (Guard) modifiziert.

Es können beliebig viele Regelbehälter beliebigen Namens modifiziert werden. Für die Standardwertvergabe werden jedoch nur aktive Regelbehälter berücksichtigt (siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458).

Ein Anwender kann nur Regelbehälter für seine Benutzerkennung modifizieren. Ein Guard-Administrator kann auch Regelbehälter unter fremden Benutzerkennungen modifizieren.

Ein Regelbehälter SYS.PDF kann nur vom Systemverwalter oder Guard-Administrator modifiziert werden, er wird unter der Benutzerkennung TSOS erwartet und enthält die Regeln für pubsetglobale Standardwerte.

MODIFY-**DEFAULT-PROTECT**ION-**RULE** (**MOD-DEF-PRO-R**)

RULE-CONTAINER-**GUARD** = <filename 1..24 without-gen-vers with-wild(40)>

,**PROTECT**ION-**RULE** = <alphanum-name 1..12>

,**NEW-NAME** = ***SAME** / <alphanum-name 1..12>

,**RULE-POS**ITION = ***UNCHA**NGED / ***LAST** / ***BEFORE**(...)

***BEFORE**(...)

PROTECTION-**RULE** = <alphanum-name 1..12>

,**PROTECT-OBJ**ECT = ***PAR**AMETERS(...)

***PAR**AMETERS(...)

NAME = ***UNCHA**NGED / ***TEMP**ORARY /

<filename 1..41 without-cat-user-gen with-wild(80)>

,**ATTR**IBUTE-**GUARD** = ***UNCHA**NGED / ***NONE** / <filename 1..18 without-cat-gen-vers>

,**USER-ID-GUARD** = ***UNCHA**NGED / ***ANY-USER-ID** / <filename 1..18 without-cat-gen-vers>

,**GUARD-CHECK** = ***Y**ES / ***NO**

,**DIALOG-CONTR**OL = ***STD** / ***NO** / *RULE-CONTAINER-CHANGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ DEFAULTP, in dem eine Regel modifiziert werden soll.

Der Behältername kann zwar beliebig gewählt werden, für die Suche nach passenden Standardwerten werden jedoch in Hierarchie ausnahmslos aktive Regelbehälter berücksichtigt (siehe Abschnitt „Aktivierung eines Regelbehälters“ auf Seite 458).

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel durch Absetzen eines einzigen Kommandos in mehreren Behältern modifiziert wird, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE = <alphanumeric name 1..12>
Name der Regel, die modifiziert werden soll. Doppelte Namen in einem Behälter sind nicht erlaubt.

NEW-NAME =
Mit diesem Operand kann die zu bearbeitende Regel umbenannt werden.

NEW-NAME = *SAME
Der Name soll unverändert bleiben.

NEW-NAME = <alphanumeric name 1..12>
Neuer Name, den die zu bearbeitende Regel erhalten soll.

RULE-POSITION =
Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt werden soll. Die Reihenfolge der Regeln ist ausschlaggebend bei der Ermittlung der Schutzattribut-Standardwerte (siehe Abschnitt „Suchlogik“ auf Seite 462).

RULE-POSITION = *UNCHANGED
Die Regelposition bleibt unverändert.

RULE-POSITION = *LAST
Die Regel soll an die letzte Position im Regelbehälter gestellt werden.

RULE-POSITION = *BEFORE(...)
Die Regel soll vor eine benannte Regel im Regelbehälter gestellt werden.

PROTECTION-RULE = <alphanumeric name 1..12>
Name einer vorhandenen Regel im Regelbehälter, vor die die zu modifizierende Regel gestellt werden soll. Das Kommando wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

PROTECT-OBJECT = *PARAMETERS(...)
Angaben über das Objekt, auf das sich die zu bearbeitende Regel beziehen soll.

NAME =
Dieser Operand bezeichnet den Namen des Objekts, für das die zu modifizierende Regel gelten soll.

NAME = *UNCHANGED
Der Objektname bleibt unverändert.

NAME = *TEMPORARY
Das Objekt ist eine temporäres Objekt. Für alle temporären Objekte kann stellvertretend nur eine einzige Regel angegeben werden.

Hinweis für Dateien

Für temporäre DMS-Dateien werden bei der Standardwertvergabe nur die Schutzattribute DESTROY-BY-DELETE und SPACE-RELEASE-LOCK berücksichtigt. Alle anderen Attribute erhalten die herkömmlichen System-Standardwerte.

Hinweis für Jobvariablen

Für temporäre Jobvariablen werden bei der Standardwertvergabe keine Schutzattribute berücksichtigt. Alle Attribute erhalten die herkömmlichen System-Standardwerte.

NAME = <filename 1..41 without-cat-user-gen with-wild(80)>
Name des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ATTRIBUTE-GUARD =
Angabe eines Attributguards (Typ DEFPATTR), das die Standardwerte enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

ATTRIBUTE-GUARD = *UNCHANGED
Der Guardname bleibt unverändert.

ATTRIBUTE-GUARD = *NONE
Es wird kein Guardname angegeben. Die Attributstandardwerte werden bei der Standardwertvergabe aus der nächst höheren Hierarchiestufe (pubsetglobal oder herkömmlicher Systemstandard) ermittelt.

ATTRIBUTE-GUARD = <filename 1..18 without-cat-gen-vers>
Name eines Guards des Typs DEFPATTR, das die Schutzattribute enthält, die bei der Standardwertvergabe verwendet werden sollen. Der Name darf keine Katalogkennung enthalten. Seine Länge ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

USER-ID-GUARD =
Name eines Guards vom Typ DEFPUID, das die Benutzer- oder Gruppenkennungen für die Pfadvervollständigung beim pubsetglobalen Standardschutz enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt der Kommandoeingabe nicht zugreifbar, hängt das Ergebnis der Kommandoverarbeitung vom Operanden GUARD-CHECK ab.

ACHTUNG!
Dieser Guardname darf nur vom Systemverwalter oder Guard-Administrator angegeben werden.

USER-ID-GUARD = *UNCHANGED
Der Guardname bleibt unverändert.

USER-ID-GUARD = *ANY-USER-ID
Es wird kein Guard für Benutzerkennungen angegeben. Der Name des Objektes gilt für alle Benutzerkennungen eines Pubsets.

USER-ID-GUARD = <filename 1..18 without-cat-gen-vers>
Name eines Guards des Typs DEFPUID, das die Liste von Benutzerkennungen enthält.

Die Länge des Namens ohne Benutzerkennung darf 8 Zeichen nicht überschreiten.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

GUARD-CHECK =
Bei Kommandodurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

GUARD-CHECK = *YES
Es wird geprüft, ob die namentlich angesprochenen Guards verfügbar sind. Existiert eines der Guards nicht, oder ist der Eigentümer des gerade bearbeiteten Regelbehälters nicht berechtigt, eines der Guards zu verwenden, wird das Kommando nicht durchgeführt.

GUARD-CHECK = *NO
Das Kommando wird unabhängig davon durchgeführt, ob die genannten Guards verfügbar sind oder vom Eigentümer des gerade bearbeiteten Regelbehälters verwendet werden dürfen.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *RULE-CONTAINER-CHANGE
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen.
2	0	DEF3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3300	Der angegebene Regelbehälter existiert nicht.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3303	Es passt keine weitere Regel mehr in den Regelbehälter.
	64	DEF3304	Es wurde kein Regelbehälter selektiert.
	64	DEF3305	Der angegebene Regelname zum Positionieren wurde nicht gefunden.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3307	Eine einzufügende Regel existiert bereits.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3310	Eine Regel wurde im Regelbehälter nicht gefunden.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3318	Ein Guard mit Benutzerkennungen, das in eine Regel eingetragen werden soll, ist nicht zugreifbar.
	64	DEF3319	Die Verwendung eines Benutzerkennungsguards in einer Regel ist nicht erlaubt.
	64	DEF3320	Ein angegebenes Attributguard ist nicht zugreifbar.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

MODIFY-GUARD-ATTRIBUTES
Guard-Attribute ändern

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können die Attribute bestehender Guards verändert werden. Ist beim Operanden NEW-NAME ein Name angegeben, wird das Guard umbenannt. Der Eigentümer darf nur seine eigenen Guards ändern. Benutzer mit dem Privileg TSOS dürfen auch fremde Guards verändern.

Dieses Kommando darf unter RFA eingesetzt werden, wenn Quell- und Ziel-Guard auf dem gleichen Rechner lokal zugreifbar sind.

Bei Angabe des Operandenwertes *UNCHANGED gelten weiterhin die Einstellungen, wie sie vor Aufruf des Kommandos festgelegt waren.

MODIFY-**GUARD-ATTR**IBUTES
GUARD-NAME = <filename 1..24 without-gen-vers>
,**NEW-NAME** = ***SAME** / <filename 1..24 without-gen-vers>
,**SCOPE** = ***UNCHA**NGED / ***USER-ID** / ***USER-GROUP** / ***HOST-SYS**TEM
,**USER-INF**ORMATION = ***UNCHA**NGED / <c-string 1..80 with-low>

GUARD-NAME = <filename 1..24 without-gen-vers>
Name des zu ändernden Guards. Die Länge des eigentlichen Namens, ohne catid und userid, ist 8 Zeichen.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

NEW-NAME = *SAME / <filename 1..24 without-gen-vers>
Neuer Name des Guards. Die Länge des eigentlichen Namen, ohne catid und userid, ist 8 Zeichen. *SAME ändert den Namen nicht.

Nur ein Guard-Administrator darf beim Umbenennen eines Guards eine andere Kennung angeben.

SCOPE =
Legt fest, wer dieses Guard zum Schutz seiner Objekte verwenden darf. Das Verwaltungsrecht (Löschen, Ändern eines Guards) bleibt beim Eigentümer.

Der Guardadministrator ist berechtigt, seine eigenen Dateien mit fremden Guards zu schützen, ohne dass der Scope dieser Guards auf *HOST-SYSTEM eingestellt sein muss und ohne das bei SCOPE=*USER-GROUP eine Gruppenzugehörigkeit vorliegen muss.

SCOPE = *USER-ID
Nur der Eigentümer darf das Guard verwenden.

SCOPE = *USER-GROUP
Alle Mitglieder der Benutzergruppe des Eigentümers dürfen das Guard verwenden.

SCOPE = *HOST-SYSTEM
Das Guard darf jeder verwenden.

USER-INFORMATION = <c-string 1..80 with-low>
Es kann ein wahlfreier Text zur Kommentierung hinterlegt werden.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
64	PRO1002	Der Guard-Name ist syntaktisch falsch
64	PRO1006	Das angegebene Guard existiert bereits
64	PRO1007	Das angegebene Guard existiert nicht
64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
64	PRO1016	Fehler im Kommunikationsmittel des MRS
64	PRO1017	Unbekannte Benutzerkennung
64	PRO1018	Fernes System nicht verfügbar
64	PRO1020	Kein Speicher mehr vorhanden
64	PRO1021	BCAM-Verbindungsfehler
64	PRO1022	BCAM-Verbindung unterbrochen
64	PRO1025	Remote-Copy nicht möglich
64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
128	PRO1036	Guardskatalog gesperrt

Beispiel

Das bestehende Guard GUARDEXA soll für alle Benutzer freigegeben werden:

```
/modify-guard-attributes guard-name=guardexa,scope=*host-system
```

Zur Überprüfung werden die Attribute angezeigt:

```
/show-guard-attributes guard-name=guardexa

     Guard name          Scope   Type      Creation Date       Last Mod Date
------------------------------------------------------------------------------
:N:$SECOSMAN.GUARDEXA    SYS  STDAC   2017-09-29/10:52:28 2017-10-03/10:55:10
                         GUARD FUER DIE GUARD-BEISPIELE
------------------------------------------------------------------------------
Guards selected: 1                                              End of display
```

REMOVE-ACCESS-CONDITIONS
Zugriffsbedingungen entfernen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Zugriffsbedingungen aus einem oder mehreren Guards entfernt. Die Zugriffsbedingungen können nacheinander durch erneute Kommandoaufrufe für die Subjekte *USER, *GROUP, *OTHERS und *ALL-USERS entfernt werden.

```
REMOVE-ACCESS-CONDITIONS

 GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,SUBJECTS = *ALL / *OTHERS / *ALL-USERS / *USER(...) / *GROUP(...)
    *USER(...)
      | USER-IDENTIFICATION = *ALL / list-poss(20): <name 1..8>
    *GROUP(...)
      | GROUP-IDENTIFICATION = *ALL / *UNIVERSAL / list-poss(20): <name 1..8>
,DIALOG-CONTROL = *STD / *NO / *GUARD-CHANGE / *USER-ID-CHANGE / *CATALOG-CHANGE
```

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Angabe des Guards, in dem Zugriffsbedingungen gelöscht werden sollen. Im Namen dürfen Musterzeichen enthalten sein.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SUBJECTS =
Es wird spezifiziert, wessen Zugriffsdefinition gelöscht werden soll. Es ist immer nur ein Subjekttyp explizit anzugeben. Sollen verschiedene Subjekttypen gelöscht werden, müssen diese Zugriffsbedingung nacheinander durch wiederholten Aufruf gelöscht werden.

SUBJECTS = *ALL
Es werden alle Definitionen für alle Subjekte und die Namen aller Subjekte gelöscht. Das Guard ist dann leer, das Ergebnis der Auswertung lautet von nun an bis neue Bedingungen definiert wurden „Bedingungen nicht erfüllt“.

SUBJECTS = *OTHERS
Es sollen die Definitionen für *OTHERS gelöscht werden.

SUBJECTS = *ALL-USERS
Es sollen die Definitionen für *ALL-USERS gelöscht werden.

SUBJECTS = *USER(...)
Angabe der Benutzerkennungen, deren Definitionen gelöscht werden sollen.

USER-IDENTIFICATION = *ALL
Es werden alle Einträge für *USER gelöscht.

USER-IDENTIFICATION = list-poss(20): <name 1..8>
Es können bis zu 20 Benutzerkennungen explizit gelöscht werden. Sollen mehr Kennungen aus diesem Guard gelöscht werden, muss das Kommando entsprechend mehrmals aufgerufen werden.

SUBJECTS = *GROUP(...)
Angabe der Benutzergruppe, deren Definitionen gelöscht werden sollen.

GROUP-IDENTIFICATION = *ALL / *UNIVERSAL / list-poss(20): <name 1..8>
Es können alle oder bis zu 20 Einträge für Gruppen explizit gelöscht werden. Sollen mehr Gruppen aus diesem Guard gelöscht werden, muss das Kommando entsprechend mehrmals aufgerufen werden. *UNIVERSAL ist der Name der Gruppenwurzel.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Guard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Guard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Guards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Guards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	PRO1011	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1015	Das angegebene Subjekt ist nicht im Guard enthalten
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1028	Guard hat falschen Typ
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
2	64	PRO1035	Kommando nicht ausgeführt
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt
	128	PRO1038	Guardskatalog durch ARCHIVE gesperrt

REMOVE-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel entfernen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Miteigentümerschutzregeln aus einem Regelbehälter (Guard des Typ COOWNERP) entfernt. Ein Anwender darf nur Regeln aus seinen eigenen Regelbehältern entfernen. Ein Guard-Administrator darf Regeln aus Regelbehältern fremder Benutzerkennungen entfernen. Verbleibt keine weitere Regel mehr im Behälter, wird der gesamte Behälter gelöscht.

REMOVE-**COOW**NER-**PROTECT**ION-**RULE** (**REM-COO-PRO-R**)
RULE-CONTAINER-**GUARD** = <filename 1..24 without-gen-vers with-wild(40)> ,**PROTECT**ION-**RULE** = ***ALL** / <alphanum-name 1..12 with-wild(20)> ,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***RULE-CONT**AINER-**CHA**NGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ COOWNERP, aus dem Regeln gelöscht werden sollen.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regeln durch Absetzen eines einzigen Kommandos in mehreren Behältern gelöscht werden, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE =
Angaben über die zu löschenden Regeln.

PROTECTION-RULE = *ALL
Alle Regeln im Behälter sollen gelöscht werden. Das bewirkt, dass der gesamte Regelbehälter gelöscht wird.

PROTECTION-RULE = <alphanumeric name 1..12 with-wild(20)>
Angabe des Namens der Regel, die gelöscht werden soll. Der Name darf Musterzeichen enthalten.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *RULE-CONTAINER-CHANGE
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	COO3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen.
2	0	COO3001	Ein Regelbehälter wurde gelöscht, weil er keine Regeln mehr enthielt.
2	0	COO3002	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten alle selektierten Regelbehälter korrekt bearbeitet werden, es sind ein oder mehrere Regelbehälter komplett gelöscht worden
2	0	COO3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
2	0	COO3004	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden, und es wurden ein oder mehrere Regelbehälter gelöscht
	1	COO3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	COO3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	COO3300	Der angegebene Regelbehälter existiert nicht.
	64	COO3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	COO3304	Es wurde kein Regelbehälter selektiert.
	64	COO3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	COO3308	Eine Benutzerkennung ist unbekannt.
	64	COO3309	Keine Unterstützung für einen Remote-File-Access.
	64	COO3310	Eine Regel wurde im Regelbehälter nicht gefunden.
	64	COO3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	COO3314	Fehler im Kommunikationsmittel des MRS.
	64	COO3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	128	COO3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	COO3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	COO3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

REMOVE-DEFAULT-PROTECTION-RULE
Standardschutzregel entfernen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden Standardschutzregeln aus einem Regelbehälter (Guard des Typs DEFAULTP) entfernt. Ein Anwender darf nur Regeln aus seinen eigenen Regelbehältern entfernen. Ein Guard-Administrator darf Regeln aus Regelbehältern fremder Benutzerkennungen entfernen. Verbleibt keine Regel mehr im Behälter, wird der gesamte Behälter gelöscht.

REMOVE-**DEFAULT-PROTECT**ION-**RULE** (**REM-DEF-PRO-R**)
RULE-CONTAINER-**GUARD** = <filename 1..24 without-gen-vers with-wild(40)> ,**PROTECT**ION-**RULE** = ***ALL** / <alphanum-name 1..12 with-wild(20)> ,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***RULE-CONT**AINER-**CHA**NGE / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ DEFAULTP, aus dem Regeln gelöscht werden sollen.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regeln durch Absetzen eines einzigen Kommandos in mehreren Behältern gelöscht werden, sofern diese zugreifbar sind.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

PROTECTION-RULE =
Angaben über die zu löschenden Regeln.

PROTECTION-RULE = *ALL
Alle Regeln im Behälter sollen gelöscht werden. Das bewirkt, dass der gesamte Regelbehälter gelöscht wird.

PROTECTION-RULE = <alphanumeric name 1..12 with-wild(20)>
Angabe des Namens der Regel, die gelöscht werden soll. Der Name darf Musterzeichen enthalten.

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jeden ausgewählten Regelbehälter angewendet.

DIALOG-CONTROL = *RULE-CONTAINER-CHANGE
Der Anwender kann für jeden ausgewählten Regelbehälter im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen.
2	0	DEF3001	Der gesamte Regelbehälter wurde gelöscht, weil nach dem Löschen einer Regel keine weiteren Regeln mehr verblieben sind.
2	0	DEF3002	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten alle selektierten Regelbehälter korrekt bearbeitet werden, es sind einer oder mehrere Regelbehälter komplett gelöscht worden.
2	0	DEF3003	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden.
2	0	DEF3004	Bei der Verarbeitung von Regelbehältern, die mit Musterzeichen spezifiziert wurden, konnten nicht alle selektierten Regelbehälter korrekt bearbeitet werden und es wurden einer oder mehrere Regelbehälter gelöscht.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3300	Der angegebene Regelbehälter existiert nicht.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3304	Es wurde kein Regelbehälter selektiert.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3310	Eine Regel wurde im Regelbehälter nicht gefunden.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

REMOVE-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad entfernen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: GUARD-ADMINISTRATION, TSOS

Mit dieser Funktion werden Benutzer- oder Gruppenkennungen aus einem Benutzerkennungsguard entfernt.

Verbleibt keine weitere Kennung mehr im Benutzerkennungsguard, wird das gesamte Guard gelöscht.

REMOVE-**DEFAULT-PROTECT**ION-**UID** (**REM-DEF-PRO-U**)

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>

,**USER-ID**ENTIFICATION = list-poss(20): <name 1..8 with-wild(20)> / ***GR**OUP(...)

***GR**OUP(...)

GROUP-**ID**ENTIFICATION =

***UNIV**ERSAL / <name 1..8 with-wild(20)>

,**DIALOG-CONTR**OL = ***STD** / ***NO** / ***GUARD-CHANGE** / ***USER-ID-CHA**NGE / ***CAT**ALOG-**CHA**NGE

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>

Dieser Operand bezeichnet den Namen des Guards vom Typ DEFPUID, aus dem Benutzerkennungen oder Benutzergruppen entfernt werden sollen. Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Musterzeichen im Namen des Guards bewirken, dass Benutzerkennungen oder Benutzergruppen durch Absetzen eines einzigen Kommandos aus mehreren Guards gelöscht werden.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

USER-IDENTIFICATION = list-poss(20)
Angabe von Benutzer- oder Benutzergruppenkennungen, die aus dem Guard ausgetragen werden sollen.

USER-IDENTIFICATION = list-poss(20): <name 1..8 with-wild(20)>
Namen von Benutzerkennungen

Die Angabe von Musterzeichen bedeutet nicht, dass alle Kennungen aus dem Guard entfernt werden, die dem Muster entsprechen. Es werden nur die Kennungseinträge entfernt, die mit derselben Musterzeichenangabe eingetragen wurden.

Beispiel

```
/add-default-protection-uid ...,user-id=(a*,abc,ax)
/remove-default-protection-uid ...,user-id=a*
```

Die Einträge USER-ID=(ABC,AX) bleiben erhalten.

USER-IDENTIFICATION = list-poss(20): *GROUP(...)
Angabe einer Benutzergruppe als Menge von Benutzerkennungen.

GROUP-IDENTIFICATION =
Name einer Benutzergruppe

GROUP-IDENTIFICATION = *UNIVERSAL
Der Name der Benutzergruppe ist *UNIVERSAL.

GROUP-IDENTIFICATION = <name 1..8 with-wild(20)>
Benutzergruppe

DIALOG-CONTROL =
Der Anwender kann das Kommando mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

DIALOG-CONTROL = *STD
Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *NO
Das Kommando wird ohne Rückfrage auf jedes ausgewählte Benutzerkennungsguard angewendet.

DIALOG-CONTROL = *GUARD-CHANGE
Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *USER-ID-CHANGE
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

DIALOG-CONTROL = *CATALOG-CHANGE

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob das Kommando angewendet werden soll oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
2	0	DEF3000	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
2	0	DEF3010	Das Benutzerkennungsguard wurde gelöscht, weil keine Kennungen mehr eingetragen waren.
2	0	DEF3011	Bei der Verarbeitung von Benutzerkennungsguards wurden ein oder mehrere Benutzerkennungsguards gelöscht, weil keine Kennungen mehr eingetragen waren.
2	0	DEF3012	Bei der Verarbeitung von Benutzerkennungsguards, die mit Musterzeichen angegeben wurden, konnten nicht alle selektierten Benutzerkennungsguards korrekt bearbeitet werden.
2	0	DEF3013	Bei der Verarbeitung von Benutzerkennungsguards, die mit Musterzeichen angegeben wurden, konnten nicht alle selektierten Benutzerkennungsguards korrekt bearbeitet werden und es wurden ein oder mehrere Benutzerkennungsguards gelöscht, weil keine Kennungen mehr eingetragen waren.
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3400	Das spezifizierte Benutzerkennungsguard existiert nicht.
	64	DEF3402	Kein Benutzerkennungsguard entspricht den angegebenen Auswahlktriterien.
	64	DEF3404	Die spezifizierte Kennung wurde im Benutzerkennungsguard nicht gefunden.
	128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.

REPAIR-GUARD-FILE
Guardskatalog wiederherstellen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: GUARD-ADMINISTRATION, TSOS

Mit diesem Kommando kann ein Pubset im laufenden Betrieb wieder in die GUARDS-Verwaltung aufgenommen werden, wenn es sich nicht mehr unter der Kontrolle von GUARDS befindet. Dieser Zustand kann durch ein unerwartetes Systemverhalten nach dem Systemstart oder nach einem Pubset-Import eintreten.

Außerdem kann der Guardskatalog nach einem misslungenen Austauschversuch (siehe Kommando /CHANGE-GUARD-FILE auf Seite 558) mit diesem Kommando wiederhergestellt werden, falls die Fehlersituation es zulässt. Dabei wird neben weiteren Systemaktionen der Guardskatalog neu eingerichtet und/oder geöffnet, falls sein Zustand es erfordert.

Falls die Durchführung des Kommandos /REPAIR-GUARD-FILE misslingt, führen Sie folgende Aktionen zur Behebung der Fehlersituation in der angegebenen Reihenfolge aus:

1. Umkatalogisieren oder Löschen des aktuellen Guardskatalogs $TSOS.SYSCAT.GUARDS

   Gegebenfalls muss zuvor das Schließen des Guardskatalogs mit dem Kommando REPAIR-DISK-FILES erzwungen werden.

2. Exportieren des betroffenen Pubsets

3. Importieren des betroffenen Pubsets
   Hierbei wird ein neuer Guardskatalog $TSOS.SYSCAT.GUARDS eingerichtet, da der defekte Katalog zuvor gelöscht wurde.

4. Sicherung einspielen

   Diese Aktion kann entfallen, wenn sichergestellt ist, dass der defekte Guardskatalog keine Guards enthielt.

   Abhängig von der Art der Sicherung ist Folgendes zu beachten:

   a) Sicherung mit GUARDS-SAVE
   Die gesicherten Guards werden direkt in den neu eingerichteten Guardskatalog eingespielt. Damit ist die Rekonstruktion abgeschlossen.

   oder

   b) Sicherung mit ARCHIVE
   Der gesicherte Guardskatalog muss unter dem Namen $TSOS.SYSCAT.GUARDS.BAK eingespielt werden. Anschließend muss mit dem Kommando /CHANGE-GUARD-FILE der Austausch des Guardskatalogs veranlasst werden.

Dieses Kommando ist nur für Benutzer mit dem Privileg TSOS oder GUARD-ADMINISTRATION zugelassen. Dieses Kommando ist nicht MSCF- oder RFA-fähig.

ACHTUNG!
Dieses Kommando darf nicht während einer ARCHIVE-Sicherung oder während eines Katalogaustauschs (/CHANGE-GUARD-FILE, Seite 558) ausgeführt werden.

Grund:
Während der Sicherung oder während eines Katalogaustauchs wird eine Katalogsperre gesetzt, um anderen Tasks den Zugriff zu dieser Zeit zu verwehren. Das Kommando /REPAIR-GUARD-FILE bewirkt jedoch eine Aufhebung der Katalogsperre. Dies kann während eines Sicherungslaufs zu erheblichen Konflikten führen.

Nach der fehlerhaften Beendigung eines Katalogwechsels muss es jedoch ausgeführt werden, um die Sperren aufzuheben.

REPAIR-**GUARD-FILE**
PUBSET = <cat- id 1..4>

PUBSET = <cat-id 1..4>
Angabe des Pubsets, auf dem der Guardskatalog wiederhergestellt werden soll.

Es sind folgende Namenskonventionen zu beachten:

SYSCAT.GUARDS	Standardname des Guardskatalogs, der in einen ordnungsgemäßen Zustand versetzt werden soll.

Das Wiederherstellen des Guardskatalogs umfasst folgende Maßnahmen:

– Das Pubset wird wieder unter die Kontrolle von GUARDS gestellt. Bei Zugriffen auf den Guardskatalog sollte die Meldung PRO1013 somit nicht mehr auftreten.

– Falls notwendig, wird eine neue GUARDS-Server-Task (PRnn) eingerichtet, die das Pubset bedient.

– Eventuelle Katalogsperren, die bei einem ARCHIVE-Lauf oder Katalogwechsel gesetzt wurden, werden aufgehoben.

– Falls der Guardskatalog geschlossen ist, wird er geöffnet.

– Falls kein Guardskatalog existiert, wird einer erstellt.

– Falls der Guardskatalog auf dem Pubset mit BLKSIZE=(STD,2) katalogisiert ist, so wird er umkatalogisiert und erhält den Namen SYSCAT.GUARDS.datum.uhrzeit. Dann wird er in einen neuen Guardskatalog mit BLKSIZE=(STD,4) und dem Namen SYSCAT.GUARDS kopiert. Dieser wird so zum aktuellen Guardskatalog.

Das Kommando wird abgewiesen, wenn es sich bei der Datei SYSCAT.GUARDS um keinen GUARDS-Katalog handelt oder die Version des GUARDS-Katalogs nicht zur eingesetzten SECOS-Version passt.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
64	PRO1020	Kein Speicher mehr vorhanden
64	PRO1040	Der Guardskatalog ist kein Guardskatalog
64	PRO1041	Der Guardskatalog hat eine falsche Version
64	PRO1047	Das Wiederherstellen eines Guardskatalogs auf einem fremden Rechner ist nicht möglich
64	PRO1048	Der Guardskatalog befindet sich nicht auf dem Control-Volume-Set des SM-Pubsets
64	PRO1051	Der Guardskatalog enthält keinen Heade-Satz und wird daher als Guardskatalog nicht anerkannt
64	PRO1052	DVS-Fehler beim Prüfen des Guardskatalogs
64	PRO1053	DVS-Fehler beim Prüfen der Version des Guardskatalogs
64	PRO1054	DVS-Fehler beim Schließen und Wiedereröffnen des Guardskatalogs
64	PRO1056	DVS-Fehler beim Anlegen des Guardskatalogs
128	PRO1045	Es findet gerade ein Masterwechsel statt
128	PRO1046	Das Pubset steht wegen einer SM-Pubset-Generierung unter der Kontrolle von SMPGEN

SHOW-ACCESS-ADMISSION
Zugriffserlaubnis anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Dieses Kommando zeigt die für den Aufrufer gültigen Zugriffsbedingungen des benannten Guards an. Das Guard muss nicht ein eigenes, sondern kann auch ein fremdes sein.

Bei der Anzeige werden nur die Bedingungsdefinitionen bewertet, nicht jedoch, ob die Bedingung im Augenblick zutrifft. Es werden nur die für den Aufrufer gültigen Bedingungen angezeigt, nicht aber, welche weiteren Bedingungen für andere Subjekte in dem Guard abgelegt sind. Beispielsweise erhält ein Aufrufer die Information, dass ihm der Zugriff montags erlaubt ist, unabhängig vom Wochentag, an dem die Ausgabe erfolgt. Der SCOPE des Guards wird nicht berücksichtigt.

Der komplette Guard-Inhalt kann mit dem Kommando /SHOW-ACCESS-CONDITIONS angezeigt werden, sofern der SCOPE des Guards dies zulässt.

Der Aufrufer erhält keinen Hinweis darauf, auf Grund welcher Subjekt-Definition das Ergebnis der Auswertung zustande kommt (ob aus der USER-, GROUP-, OTHERS- oder ALL-USERS-Definition).

SHOW-ACCESS-ADMISSION
GUARD-NAME = <filename 1..24 without-gen-vers> ,**OUTPUT** = list-poss(2): ***SYSOUT** / ***SYSLST**

GUARD-NAME = <filename 1..24 without-gen-vers >
Angabe des Guards, dessen Zugriffsbedingungen angezeigt werden sollen.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

OUTPUT =
Bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Ausgabe auf Datensichtstation, sofern das Kommando im Dialog gegeben wurde.
Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST
Ausgabe auf SYSLST.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1024	Nutzung des Guards nicht zugelassen
	64	PRO1028	Guard hat falschen Typ
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	64	PRO1030	Benutzer-Bedingung im Guard nicht erfüllbar
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Beispiel

Unter der Benutzerkennung SECOS1 wurden ein Guard GUARDEXA zwei Zugriffsbedingungen eingetragen:

```
/add-access-conditions guardexa,subjects=*user(secos1),admission=*yes
/add-access-conditions guardexa,subjects=*user(user1),admission=*no
```

Abhängig von der Benutzerkennung, unter der das Kommando /SHOW-ACCESS-ADMISSION aufgerufen wird, erhält man unterschiedliche Ausgaben:

– Unter der Benutzerkennung SECOS1

```
/show-access-admission guardexa
:N:$SECOS1.GUARDEXA
  User ALWAYS has access admission
------------------------------------------------------------------------------
                                                                  End of display
```

– Unter der Benutzerkennung USER1

```
/show-access-admission $secos1.guardexa
PRO1030 NO USER ACCESS TO OBJECT PROTECTED BY THIS GUARD
```

Das Kommando /SHOW-ACCESS-CONDITIONS liefert im Gegensatz dazu folgende Ausgaben:

– Unter der Benutzerkennung SECOS1

```
/show-access-conditions guardexa
:N:$SECOS1.GUARDEXA
   User   SECOS1   has ADMISSION
   User   USER1    has NO ADMISSION
------------------------------------------------------------------------------
Guards selected: 1                                            End of display
```

– Unter der Benutzerkennung USER1

```
/show-access-conditions $secos1.guardexa
PRO1024 NO AUTHORIZATION FOR GUARD ':2OSG:$QM212.GUARDEXA'. FUNCTION NOT
PROCESSED
```

Das Format der Ausgabe wird nicht garantiert.

Erläuterung der Ausgabe siehe Kommando /SHOW-ACCESS-CONDITIONS, Seite 635.

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Guards, dessen Zugriffsbedingungen angezeigt werden.	var(*LIST).GUARD-NAME	S	'' <filename 1..40>	
Subjekttyp USER : Bedingungen, die explizit für einen Benutzer gelten				
Zugriffserlaubnis für den Benutzer *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).USER.ADMIS	S	'' *NO *PAR *YES	
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).USER.DATE(*LIST).FROM	S	'' <yyyy-mm-dd>	
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).USER.DATE(*LIST).TO	S	'' <yyyy-mm-dd>	
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER.DATE-KIND	S	'' *ANY *EXCEPT *INTERVAL	

(Teil 1 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg des Benutzers	var(*LIST).USER.PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).USER.PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).USER.PROG(*LIST).F	S	'' <filename 1..54>	
Name des Bibliothekelements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).USER.PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..32>	

(Teil 2 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).USER.PROG(*LIST).MODULE.LIB	S	'' <filename 1..54>	
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).USER.PROG(*LIST).MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	
Name des Bibliothekelements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).USER.PROG(*LIST).PHASE.ELEM	S	'' <comp.-name 1..64>	
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).USER.PROG(*LIST).PHASE.LIB	S	'' <filename 1..54>	
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).USER.PROG(*LIST).PHASE.VERSION	S	'' *ANY <comp.-name 1..24>	
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).USER.PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).USER.PROG-CONTR	S	'' *ANY *LIST	
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).USER.TIME(*LIST).FROM	S	'' <hh:mm>	
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).USER.TIME(*LIST).TO	S	'' <hh:mm>	
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER.TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	

(Teil 3 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).USER.WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER.WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	
WHEN: Zusätzliche, maßgebende Bedingungen, die im Pseudosubjekt ALL-USERS hinterlegt sind				
Zugriffserlaubnis für den Benutzer *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).WHEN.ADMIS	S	'' *NO *PAR *YES	
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).WHEN.DATE(*LIST).FROM	S	'' <yyyy-mm-dd>	
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).WHEN.DATE(*LIST).TO	S	'' <yyyy-mm-dd>	
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).WHEN.DATE-KIND	S	'' *ANY *EXCEPT *INTERVAL	

(Teil 4 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg	var(*LIST).WHEN.PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).WHEN.PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).WHEN.PROG(*LIST).F	S	'' <filename 1..54>	
Name des Bibliothekelements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).WHEN.PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..32>	

(Teil 5 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).WHEN.PROG(*LIST).MODULE.LIB	S	'' <filename 1..54>	
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).WHEN.PROG(*LIST).MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	
Name des Bibliothekelements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).WHEN.PROG(*LIST).PHASE.ELEM	S	'' comp.-name 1..64>	
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).WHEN.PROG(*LIST).PHASE.LIB	S	'' <filename 1..54>	
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).WHEN.PROG(*LIST).PHASE.VERSION	S	'' *ANY <comp.-name 1..24>	
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).WHEN.PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).WHEN.PROG-CONTR	S	'' *ANY *LIST	
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).WHEN.TIME(*LIST).FROM	S	'' <hh:mm>	
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).WHEN.TIME(*LIST).TO	S	'' <hh:mm>	
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).WHEN.TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	

(Teil 6 von 7)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).WHEN.WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).WHEN.WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	

(Teil 7 von 7)

SHOW-ACCESS-CONDITIONS
Zugriffsbedingungen anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können einzelne oder alle in einem Guard bestehenden Zugriffsbedingungen und die Guard-Attribute angezeigt werden, sofern für den Abfrager die Verwendung des Guards zugelassen ist (SCOPE-Attribut).

Informationen über die für den Aufrufer geltenden Bedingungen zeigt das Kommando /SHOW-ACCESS-ADMISSION.

```
SHOW-ACCESS-CONDITIONS

        GUARD-NAME = * / <filename 1..24 without-gen-vers with-wild(40)>
,SELECT = *ALL / *BY-ATTRIBUTES(...)
    *BY-ATTRIBUTES(...)
        SUBJECTS = *ALL / *OTHERS / *ALL-USERS / *USER(...) / *GROUP(...)
            *USER(...)
                USER-IDENTIFICATION = *ALL / list-poss(20): <name 1..8>
            *GROUP(...)
                GROUP-IDENTIFICATION = *ALL / *UNIVERSAL / list-poss(20): <name 1..8>
,INFORMATION = *ADMISSIONS / *ALL / *NAMES-ONLY / *ATTRIBUTES
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
```

GUARD-NAME = * / <filename 1..24 without-gen-vers with-wild(40)>
Angabe des anzuzeigenden Guard. Im Namen dürfen Musterzeichen enthalten sein. Sind im Namen Musterzeichen enthalten, werden alle Guards angezeigt, die in das Muster passen.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

GUARD-NAME = *
Es werden alle Guards angezeigt.

SELECT =
Auswahl, welche Bedingungen angezeigt werden sollen.

SELECT = *ALL
Es werden alle Informationen über alle Guards ausgegeben, die mit dem Operanden GUARD-NAME ausgewählt wurden.

SELECT = *BY-ATTRIBUTES(...)
Selektiert die anzuzeigenden Bedingungen.

SUBJECTS =
Spezifiziert die Subjekte, über die Informationen ausgegeben werden sollen.

SUBJECTS = *ALL
Es wird über alle Subjekte Auskunft gegeben.

SUBJECTS = *USER(...)

USER-IDENTIFICATION = *ALL
Es wird über alle USER Auskunft gegeben.

USER-IDENTIFICATION = list-poss(20): <name 1..8>
Es wird über die angegebenen USER Auskunft gegeben.

SUBJECTS = GROUP(...)

GROUP-IDENTIFICATION = *ALL
Es wird über alle GROUPs Auskunft gegeben.

GROUP-IDENTIFICATION = list-poss(20): <name 1..8>
Es wird über die angegebenen GROUPs Auskunft gegeben.

GROUP-IDENTIFICATION = *UNIVERSAL
Es wird über die GROUP *UNIVERSAL Auskunft gegeben.

INFORMATION =
Umfang der Informationsausgabe pro Guard.

INFORMATION = *ADMISSIONS
Es werden nur die Zugriffsbedingungen angezeigt.

INFORMATION = *ALL
Es werden die Guard-Attribute und die Zugriffsbedingungen angezeigt.

INFORMATION = *NAMES-ONLY
Es werden nur die Namen der Guards angezeigt.

INFORMATION = *ATTRIBUTES
Es werde nur die Guard-Attribute angezeigt.

OUTPUT =
Bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Ausgabe auf Datensichtstation, sofern das Kommando im Dialog gegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST
Ausgabe auf SYSLST.

Ausgabelayout für INFORMATION=*ADMISSIONS

```
/show-access-conditions guard-name=guardexa,information=*admissions

:PUB1:$GUARDS.DOCS
 User    GUARDUSE has ADMISSION
 Group   SECOS
   Time       IN ( <08:00,11:15> , <12:00,15:15> ,
                   <15:45,17:00> )
   Date       IN ( <2017-05-04,2017-10-24> , <2017-09-01,2017-10-01> ,
                   <2017-11-11,2017-11-11> )
   Week-Day   EX ( SA, SU )
   Privilege  IN ( TSOS    , NET-ADM  )
   Program
     File   = $RZTOOL.DAMP.V10A00
     Phase
       Lib  = $MAYDAY.TOOLS.LIB
       Elem = DAMP.V10A02
       Vers = 22
     Module
       Lib  = $MAYDAY.TOOLS.LIB
       Elem = DAMP.V10A02
       Vers = *ANY
```

Ausgabelayout für INFORMATION=*ATTRIBUTES

```
/show-access-conditions guard-name=guardexa,information=*attributes

 Guard name          Scope       Creation Date            Last Mod Date
------------------------------------------------------------------------------
:N:$GUARDDOC.GUARDEXA     SYS     2017-04-29/10:52:28     2017-05-29/11:07:28
                        GUARD FUER DIE GUARD-BEISPIELE
------------------------------------------------------------------------------
Guards selected: 1                                              End of display
```

Ausgabelayout für INFORMATION=*NAMES-ONLY

```
/show-access-conditions guard-name=*,information=*names-only

:N:$GUARDDOC.EXAGUARD
:N:$GUARDDOC.GUARDEXA
:N:$GUARDDOC.SECGUARD
------------------------------------------------------------------------------
Guards selected: 3                                              End of display
```

Erläuterung der Ausgabe

Das Format der Ausgabe wird nicht garantiert.
Bedingungen, die mit IN beginnen, führen zum Ergebnis WAHR, wenn die Bedingung erfüllt ist (im Beispiel TIME IN (<08:00>, <11:15>).
Bedingungen, die mit EX beginnen, führen zum Ergebnis WAHR, wenn die Bedingung **nicht** erfüllt ist (im Beispiel Week-Day EX (SA, SU)).
Privilegien werden abgekürzt ausgegeben, siehe „Tabelle der Privilegien“ auf Seite 128.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guards-katalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1024	Nutzung des Guards nicht zugelassen
	64	PRO1028	Guard hat falschen Typ
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	64	PRO1030	Benutzer-Bedingung im Guard nicht erfüllbar
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = ADMISSIONS	1
INFORMATION = ALL	2
INFORMATION = ATTRIBUTES	3
INFORMATION = NAMES-ONLY	4

Bitte beachten Sie, dass in dieser Tabelle von der sonst üblichen alphabetischen Reihenfolge der S-Variablennamen abgewichen wird. Um einen besseren Überblick zu erhalten, sind die allgemeinen Attribute des Guards vorgezogen, und im Anschluss daran die Bedingungen für die Subjekttypen ALL-USERS, GROUP, OTHERS und USER beschrieben.

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Allgemeinen Attribute des Guards				
Erstellungsdatum des Guards	var(*LIST).CRE-DATE	S	'' <yyyy-mm-dd>	2,3
Erstellungszeit des Guards	var(*LIST).CRE-TIME	S	'' <hh:mm:ss>	2,3
Name des Guards	var(*LIST).GUARD-NAME	S	'' <filename 1..40>	1,2,3,4
		S	'' <part.-filename 2..40>	2,3,4
Datum der letzten Änderung	var(*LIST).LAST-MOD-DATE	S	'' <yyyy-mm-dd>	2,3
Tageszeit der letzten Änderung	var(*LIST).LAST-MOD-TIME	S	'' <hh:mm:ss>	2,3
Nutzungsberechtigung für Guard: *HOST-SYS: Jeder darf das Guard benutzen *USER-GROUP: Mitglieder der Benutzergruppe des Eigentümers dürfen Guard benutzen *USER-ID: Nur der Eigentümer darf Guard benutzen	var(*LIST).SCOPE	S	'' *HOST-SYS *USER-GROUP *USER-ID	2,3
Kommentartext zum Guard	var(*LIST).USER-INFO	S	<c-string1..80>	2

(Teil 1 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Pseudosubjekt ALL-USERS				
Zugriffserlaubnis *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).ALL-USER.ADMIS	S	” *NO *PAR *YES	1,2
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).ALL-USER.DATE(*LIST).FROM	S	” <yyyy-mm-dd>	1,2
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).ALL-USER.DATE(*LIST).TO	S	<yyyy-mm-dd>	1,2
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).ALL-USER.DATE-KIND	S	” *ANY *EXCEPT *INTERVAL	1,2

(Teil 2 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg	var(*LIST).ALL-USER.PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *HARDWARE-MAINT *HSMS-ADM *GUA-ADM *NET-ADM *NOTIF-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *T-KEY-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1,2
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).ALL-USER.PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).ALL-USER.PROG(*LIST).F	S	'' <filename 1..54>	1,2
Name des Bibliothekelements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).ALL-USER.PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..32>	1,2

(Teil 3 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).ALL-USER.PROG(*LIST). MODULE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).ALL-USER.PROG(*LIST). MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Name des Bibliothekelements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).ALL-USER.PROG(*LIST). PHASE.ELEM	S	'' <comp.-name 1..64>	1,2
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).ALL-USER.PROG(*LIST).PHASE. LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).ALL-USER.PROG(*LIST).PHASE. VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).ALL-USER. PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).ALL-USER.PROG-CONTR	S	'' *ANY *LIST	1,2
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).ALL-USER.TIME(*LIST).FROM	S	'' <hh:mm>	1,2
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).ALL-USER.TIME(*LIST).TO	S	'' <hh:mm>	1,2
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).ALL-USER.TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 4 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).ALL-USER.WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1,2
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).ALL-USER.WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Subjekttyp GROUP				
Zugriffserlaubnis für den Benutzer *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).GROUP(*LIST).ADMIS	S	'' *NO *PAR *YES	1,2
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).GROUP(*LIST).DATE(*LIST).FROM	S	'' <yyyy-mm-dd>	1,2
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).GROUP(*LIST).DATE(*LIST).TO	S	'' <yyyy-mm-dd>	1,2
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).GROUP(*LIST).DATE-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Gruppenkennung	var(*LIST).GROUP(*LIST).GROUP-ID	S	'' <name 1..8>	1,2

(Teil 5 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg	var(*LIST).GROUP(*LIST).PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *HARDWARE-MAINT *HSMS-ADM *GUA-ADM *NET-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1,2
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).GROUP(*LIST).PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).GROUP(*LIST).PROG(*LIST).F	S	'' <filename 1..54>	1,2
Name des Bibliothekelements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).GROUP(*LIST).PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..64>	1,2

(Teil 6 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).GROUP(*LIST).PROG(*LIST).MODULE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).GROUP(*LIST).PROG(*LIST).MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Name des Bibliothekselements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).GROUP(*LIST).PROG(*LIST).PHASE.ELEM	S	'' <comp.-name 1..64>	1,2
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).GROUP(*LIST).PROG(*LIST).PHASE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).GROUP(*LIST).PROG(*LIST).PHASE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).GROUP.PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).GROUP(*LIST).PROG-CONTR	S	'' *ANY *LIST	1,2
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).GROUP(*LIST).TIME(*LIST).FROM	S	'' <hh:mm>	1,2
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).GROUP(*LIST).TIME(*LIST).TO	S	'' <hh:mm>	1,2
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).GROUP(*LIST).TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 7 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).GROUP(*LIST).WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1,2
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).GROUP(*LIST).WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Subjekttyp OTHERS				
Zugriffserlaubnis *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).OTHERS.ADMIS	S	'' *NO *PAR *YES	1,2
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).OTHERS.DATE(*LIST).FROM	S	'' <yyyy-mm-dd>	1,2
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).OTHERS.DATE(*LIST).TO	S	'' <yyyy-mm-dd>	1,2
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).OTHERS.DATE-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 8 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg	var(*LIST).OTHERS.PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1,2
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).OTHERS.PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).OTHERS.PROG(*LIST).F	S	'' <filename 1..54>	1,2
Name des Bibliothekelements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).OTHERS.PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..32>	1,2

(Teil 9 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).OTHERS.PROG(*LIST). MODULE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).OTHERS.PROG(*LIST). MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Name des Bibliothekelements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).OTHERS.PROG(*LIST).PHASE. ELEM	S	'' <comp.-name 1..64>	1,2
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).OTHERS.PROG(*LIST).PHASE. LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).OTHERS.PROG(*LIST).PHASE. VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).OTHERS. PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).OTHERS.PROG-CONTR	S	'' *ANY *LIST	1,2
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).OTHERS.TIME(*LIST).FROM	S	'' <hh:mm>	1,2
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).OTHERS.TIME(*LIST).TO	S	'' <hh:mm>	1,2
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).OTHERS.TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 10 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).OTHERS.WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1,2
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).OTHERS.WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Subjekttyp USER				
Zugriffserlaubnis *NO: Kein Zugriff *PAR: Zugriff durch bestimmte Parameter eingeschränkt *YES: Zugriff erlaubt	var(*LIST).USER(*LIST).ADMIS	S	'' *NO *PAR *YES	1,2
Kalendardatum, ab dem der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).USER(*LIST).DATE(*LIST).FROM	S	'' <yyyy-mm-dd>	1,2
Kalendardatum, an dem der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).USER(*LIST).DATE(*LIST).TO	S	'' <yyyy-mm-dd>	1,2
Wie wird der Zugriff über die Kalendardaten geregelt? *ANY: Jederzeit ist der Zugriff auf das Objekt möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER(*LIST).DATE-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 11 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Privileg	var(*LIST).USER(*LIST).PRIVIL(*LIST)	S	'' *ACS-ADM *CUST-PRIV-1 ... *CUST-PRIV-8 *FT-ADM *FTAC-ADM *GUA-ADM *HARDWARE-MAINT *HSMS-ADM *NET-ADM *OPER *POSIX-ADM *PRINT-SERVICE-ADM *PROP-ADM *SAT-F-EVALUATION *SAT-F-MANAGE *SEC-ADM *STD-PROCESS *SUBSYS-MANAGE *SOFTWARE-MONITOR-ADM *TAPE-ADM *TSOS *USER-ADM *VIRT-MACHINE-ADM *VM2000-ADM	1,2
Wie wird der Zugriff über Privilegien geregelt? *ANY: Kein besonderes Privileg für den Zugriff notwendig *EXCEPT: Zugriff bei den angegebenen Privilegien untersagt *INTERVAL: Zugriff bei den angegebenen Privilegien erlaubt	var(*LIST).USER(*LIST).PRIVIL-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Name des Programms, über welches auf das Objekt zugegriffen wird	var(*LIST).USER(*LIST).PROG(*LIST).F	S	'' <filename1..54>	1,2
Name des Bibliothekselements, in welchem sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).USER(*LIST).PROG(*LIST).MODULE.ELEM	S	'' <comp.-name 1..32>	1,2

(Teil 12 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name der Bibliothek, in welcher sich das Modul befindet, über das auf das Objekt zugegriffen wird	var(*LIST).USER(*LIST).PROG(*LIST).MODULE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich das Modul befindet? *ANY : Keine besondere Version	var(*LIST).USER(*LIST).PROG(*LIST).MODULE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Name des Bibliothekelements, in welchem sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).USER(*LIST).PROG(*LIST).PHASE.ELEM	S	'' <comp.-name1..64>	1,2
Name der Bibliothek, in welcher sich die Phase befindet, über die auf das Objekt zugegriffen wird	var(*LIST).USER(*LIST).PROG(*LIST).PHASE.LIB	S	'' <filename 1..54>	1,2
Welche Version muss das Bibliothekselement haben, in dem sich die Phase befindet? *ANY : Keine besondere Version	var(*LIST).USER(*LIST).PROG(*LIST).PHASE.VERSION	S	'' *ANY <comp.-name 1..24>	1,2
Mit welchen Werten sind die Elemente der Listenvariable var(*LIST).USER.PROG(*LIST) versorgt? *ANY: Elemente der Listenvariable mit Default-Wert '' versorgt *LIST: Elemente der Listenvariable mit aktuellen Werten versorgt	var(*LIST).USER(*LIST).PROG-CONTR	S	'' *ANY *LIST	1,2
Tageszeit, ab der der Zugriff auf das durch das Guard geschützte Objekt beginnt	var(*LIST).USER(*LIST).TIME(*LIST).FROM	S	'' <hh:mm>	1,2
Tageszeit, bei der der Zugriff auf das durch das Guard geschützte Objekt endet	var(*LIST).USER(*LIST).TIME(*LIST).TO	S	'' <hh:mm>	1,2
Wie wird der Zugriff über die Tageszeiten geregelt? *ANY: Der Zugriff auf das Objekt ist jederzeit möglich *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER(*LIST).TIME-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2
Benutzerkennung	var(*LIST).USER(*LIST).USER-ID	S	'' <name 1..8>	1,2

(Teil 13 von 14)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Wochentag, an dem der Zugriff auf das durch das Guard geschützte Objekt erlaubt ist	var(*LIST).USER(*LIST).WEEKDAY(*LIST)	S	'' *MONDAY *TUESDAY *WEDNESDAY *THURSDAY *FRIDAY *SATURDAY *SUNDAY	1,2
Wie wird der Zugriff über die Wochentage geregelt? *ANY: An jedem Wochentag ist der Zugriff erlaubt *EXCEPT: In dem bezeichneten Intervall ist der Zugriff untersagt *INTERVAL: In dem bezeichneten Interval ist der Zugriff erlaubt	var(*LIST).USER(*LIST).WEEKDAY-KIND	S	'' *ANY *EXCEPT *INTERVAL	1,2

(Teil 14 von 14)

SHOW-COOWNER-ADMISSION-RULE
Miteigentümerberechtigungsregel anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando kann sich ein Anwender für einen spezifizierten Objektnamen anzeigen lassen, ob er Miteigentümer ist und in welchen Regeln das Miteigentum für ihn beschrieben ist.

Regeln für das Miteigentum können sowohl für Dateinamen als auch für Jobvariablen spezifiziert und in einem jeweils separaten, aktiven Regelbehälter eingetragen sein. Darum wird über den Operanden RULE-CONTAINER-TYPE gesteuert, ob Auskunft über das Miteigentum von Dateien oder über Jobvariablen gewünscht wird.

Die Anzeige der zu erfüllenden Zugriffsbedingungen muss in einem gesonderten Schritt erfolgen. Die in den angezeigten Regeln benannten Condition-Guards können mit dem Kommando /SHOW-ACCESS-ADMISSION angezeigt werden.

Näheres über das Anzeigeverhalten einer Zugriffserlaubnis ist der Beschreibung des Kommandos /SHOW-ACCESS-ADMISSION zu entnehmen.

Die Ausgabe der Miteigentümererlaubnis entspricht der Ausgabe des Kommandos /SHOW-COOWNER-PROTECTION-RULE. Sie unterscheidet sich darin, dass nur die Untermenge von Regeln ausgegeben wird, die für die angegebene Benutzerkennung von Bedeutung ist.

ACHTUNG!
Nicht angezeigt werden Regeln, die eine Miteigentümerschaft verweigern.

Mit diesem Kommando werden nur die für den Aufrufer relevanten Regeln angezeigt. Ob ein Miteigentümerzugriff möglich ist, hängt jedoch von weiteren Kriterien ab.

SHOW-COOWNER-**ADMIS**SION-**RULE**	(**SHO-COO-ADMIS-R**)
OBJECT-**NAME** = <filename 1..54 without-gen with-wild>	
,**RULE-CONT**AINER-**TYP**E = ***FILE** / ***JV** / ***CAPRI**	
,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)	
***SYSLST**(...)	
SYSLST-NUMBER = ***STD** / <integer 1..99>	

OBJECT-NAME = <filename 1..54 without-gen-with-wild>
Name des Objektes, über das sich ein Benutzer bezüglich seiner Miteigentümerschaft informieren will.

Bei der Verwendung von Musterzeichen sind nur folgende Angaben erlaubt:
– :<catid>:$<userid>.*
– $<userid>.* oder
– *

Musterzeichen in der Katalog- oder Benutzerkennung sind nicht erlaubt.

Ist der Objektname vollqualifiziert angegeben, wird die erste für den Benutzer relevante Regel angezeigt. Das ist die Regel, die auch für die Miteigentümerprüfung herangezogen wird.

Bei Angabe des Musterzeichens „*“ im Namensteil des Objektnamens werden alle für den Benutzer relevanten Regeln angezeigt. Damit erhält der Benutzer die Information, welche Namenskonventionen und Zugriffsbedingungen er einhalten muss, um Miteigentümer von Dateien einer fremden Kennung zu sein.

RULE-CONTAINER-TYPE =
Typ der aktiven Regelbehälter, in denen nach einer passenden Miteigentümerregel gesucht werden soll.

RULE-CONTAINER-TYPE = *FILE
Es soll in den aktiven Regelbehältern gesucht werden, in denen Regeln für das Miteigentum von Dateien spezifiziert sind (SYS.UCF[<n>]).

RULE-CONTAINER-TYPE = *JV
Es soll in den aktiven Regelbehältern gesucht werden, in denen Regeln für das Miteigentum von Jobvariablen spezifiziert sind (SYS.UCJ[<n>]).

RULE-CONTAINER-TYPE = *CAPRI
Es soll in aktiven Regelbehälter gesucht werden, in denen Regeln für das Miteigentum von CAPRI spezifiziert sind (SYS.UCC[<n>]).
Siehe auch die Dokumentation zu CAPRI unter *http://manuals.ts.fujitsu.com*.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (Admission Rules)

Beispiel 1

Ein Benutzer LUZIFER informiert sich, welche Regel ihm den Miteigentümer-Zugriff auf die Datei PARADISE der Benutzerkennung $GUABRIEL erlaubt.

Der Benutzer gibt folgendes Kommando:

```
/show-coowner-admission-rule object-name=:abcd:$guabriel.paradise
```

```
------------------------------------------------------------------------------
COOWNER RULES FOR FILE :ABCD:$GUABRIEL.PARADISE
------------------------------------------------------------------------------
RULENAME001    OBJECT     = PARADISE
               CONDITIONS = $GUABRIEL.GUA-ALL
------------------------------------------------------------------------------
RULES SELECTED: 1                                          END OF DISPLAY
```

Beispiel 2

Ein Benutzer LUZIFER informiert sich, welche Regeln ihm ihm den Miteigentümer-Zugriff auf Dateien der Benutzerkennung $GUABRIEL erlauben.

Der Benutzer gibt folgendes Kommando:

```
/show-coowner-admission-rule object-name=:abcd:$guabriel.*
```

```
------------------------------------------------------------------------------
COOWNER RULES FOR FILE :ABCD:$GUABRIEL.PARADISE
------------------------------------------------------------------------------
RULENAME001    OBJECT     = PARADISE
               CONDITIONS = $GUABRIEL.GUA-ALL
RULENAME004    OBJECT     = HEAVEN
               CONDITIONS = $GUABRIEL.GUA-ALL
RULENAME006    OBJECT     = APPLE*
               CONDITIONS = $GUABRIEL.GUA-LUZ
------------------------------------------------------------------------------
RULES SELECTED: 3                                          END OF DISPLAY
```

Das Format der Ausgabe wird nicht garantiert.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
1	COO3100	Es wurde ein fehlerhafter Operandenwert erkannt.
32	COO3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
64	COO3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
64	COO3308	Eine Benutzerkennung ist unbekannt.
64	COO3309	Keine Unterstützung für einen Remote-File-Access
64	COO3312	Es wurde keine Zugriffsregel für ein angegebenes Zugriffsobjekt gefunden.
64	COO3314	Fehler im Kommunikationsmittel des MRS.
64	COO3316	Ein Miteigentümerzugriff ist nicht erlaubt.
64	COO3321	Der aktive Regelbehälter ist nicht zugreifbar.
128	COO3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Objekts	VAR(*LIST).OBJECT-NAME	S	<filename 1..54 without-gen with-wild(80)>	
Typ der aktiven Regelbehälter	VAR(*LIST).CONTAIN-TYPE	S	*FILE *JV	
Name der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). RULE-NAME	S	<alphanumeric name 1..12>	
Objektname der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). OBJECT-NAME	S	<filename 1..41 without-cat-gen-user with-wild(80)>	
Name des Bedingungsguards in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). CONDITION-GUARD	S	*NONE <filename 1..18 without-cat-gen-ver>	
Miteigentümerschaft von TSOS	VAR(*LIST). PROTECTION-RULE(*LIST). TSOS-ACCESS	S	*SYSTEM-STD *RESTRICTED ''	1

SHOW-COOWNER-PROTECTION-RULE
Miteigentümerschutzregel anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können Regeln des Miteigentümerschutzes angezeigt werden, die in einem oder mehreren Regelbehältern (Guards des Typs COOWNERP) eingetragen sind.

SHOW-COOWNER-**PROTECT**ION-**RULE** (**SHO-COO-PRO-R**)
RULE-CONTAINER-**GUARD** = ***** / <filename 1..24 without-gen-vers with-wild(40)>
,**SEL**ECT = ***ALL** / ***BY-RULES**(...)
***BY-RULES**(...)
PROTECTION-**RULE** = <alphanum-name 1..12 with-wild(20)>
,**INF**ORMATION = ***RULES** / ***CONT**AINER-**GUARD-NAM**ES-**ON**LY
,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)
***SYSLST**(...)
SYSLST-NUMBER = ***STD** / <integer 1..99>

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters (Guard des Typs COOWNERP), dessen Regeln angezeigt werden sollen.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regeln mehrerer Behälter durch Absetzen eines einzigen Kommandos angezeigt werden.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SELECT=
Mit diesem Operanden wird das Selektionskriterium festgelegt.

SELECT = *ALL
Es sollen alle Regeln angezeigt werden.

Das bedeutet für INFORMATION=*RULES:
Es wird der Name des Regelbehälters und alle darin enthaltenen Regeln angezeigt.

Das bedeutet für INFORMATION=*CONTAINER-GUARD-NAMES-ONLY:
Es wird nur der Name des Regelbehälters angezeigt.

SELECT = *BY-RULES(...)
Es wird eine genau spezifizierte Regel angezeigt.

Das bedeutet für INFORMATION=*RULES:
Es wird der Name des Regelbehälters und die selektierten Regeln angezeigt.

Das bedeutet für INFORMATION=*CONTAINER-GUARD-NAMES-ONLY:
Es wird der Name des Regelbehälters angezeigt.

PROTECTION-RULE = name 1..12 with-wild(20)>
Name der Regel, die angezeigt wird. Der Name kann mit Musterzeichen spezifiziert werden.

INFORMATION=
Legt den Umfang der Information fest, die ausgegeben wird.

INFORMATION = *RULES
Es werden sowohl der Name des Regelbehälters als auch die enthaltenen Regeln angezeigt.

INFORMATION = *CONTAINER-GUARD-NAMES-ONLY
Es werden nur die Namen der Behälter angezeigt.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (Rules)

Beispiel

Ein Benutzer hat unter seiner Benutzerkennung GUABRIEL einen benutzerspezifischen Regelbehälter angelegt. Bevor er ihn modifiziert hat, hat er sich eine Sicherungskopie erstellt.

Der Benutzer gibt folgendes Kommando:

```
/show-coowner-protection-rule rule-container-guard=*,information=*rules
```

```
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$GUABRIEL.UCF.BAK                    COOWNER PROTECTION
------------------------------------------------------------------------------
REGELNAME001  OBJECT      = PARADISE.*
              CONDITIONS  = $GUABRIEL.GUA-USR
              TSOS-ACCESS = SYSTEM-STD
REGELNAME002  OBJECT      = CLOUD
              CONDITIONS  = *NONE
              TSOS-ACCESS = RESTRICTED
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$GUABRIEL.SYS.UCF              ACTIVE  COOWNER PROTECTION
------------------------------------------------------------------------------
REGELNAME001  OBJECT      = PARADISE.*
              CONDITIONS  = $GUABRIEL.GUA-USR
              TSOS-ACCESS = SYSTEM-STD
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 2                                   END OF DISPLAY
```

Ausgabelayout (Container Names only)

Der Benutzer gibt folgendes Kommando:

```
/show-coowner-protection-rule rule-container-guard=*, -
/                             information=*container-guard-names-only
```

```
------------------------------------------------------------------------------
LIST OF RULE CONTAINER NAMES                              COOWNER PROTECTION
------------------------------------------------------------------------------
:ABCD:$TSOS.SYS.UCF                                                   ACTIVE
:ABCD:$TSOS.UCF.BAK
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 2                                   END OF DISPLAY
```

Das Format der Ausgabe wird nicht garantiert.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
1	COO3100	Es wurde ein fehlerhafter Operandenwert erkannt.
32	COO3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
64	COO3300	Der angegebene Regelbehälter existiert nicht.
64	COO3301	Es wurde keine Regel gefunden, die den angegebenen Auswahlkriterien entspricht.
64	COO3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
64	COO3304	Es wurde kein Regelbehälter selektiert.
64	COO3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
64	COO3308	Eine Benutzerkennung ist unbekannt.
64	COO3309	Keine Unterstützung für einen Remote-File-Access.
64	COO3310	Eine Regel wurde im Regelbehälter nicht gefunden.
64	COO3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
64	COO3314	Fehler im Kommunikationsmittel des MRS.
64	COO3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
128	COO3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
128	COO3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
128	COO3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.
128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	Bedingung in Tabelle
INFORMATION = *RULES INFORMATION = *CONTAINER-GUARD-NAMES-ONLY	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Regelbehälters	VAR(*LIST).RULE-CONTAIN-GUARD	S	<filename 1..24>	1, 2
Angabe, ob der Regelbehälter aktiv ist	VAR(*LIST).CONTAIN-CONDITION	S	ACTIVE ''	1
Name der Regel	VAR(*LIST). PROTECTION-RULE(*LIST).RULE-NAME	S	<alphanumeric name 1..12>	1
Objektname in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). OBJECT-NAME	S	<filename 1..41 without-cat-gen-user with-wild(80)>	1
Name des Bedingungsguards in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). CONDITION-GUARD	S	*NONE <filename 1..18 without-cat-gen-ver>	1
Miteigentümerschaft von TSOS	VAR(*LIST). PROTECTION-RULE(*LIST). TSOS-ACCESS	S	*SYSTEM-STD *RESTRICTED ''	1

SHOW-DEFAULT-PROTECTION-ATTR
Standardwerte für Schutzattribute anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können Schutzattribut-Standardwerte angezeigt werden.

Ein Anwender, der weder Eigentümer des anzuzeigenden Attributguards noch Guard-Administrator ist, erhält die Attribute nur dann angezeigt, wenn er die entsprechende Berechtigung hat, auf das Attributguard zuzugreifen (SCOPE=*USER-GROUP oder *HOST-SYSTEM).

SHOW-DEFAULT-PROTECTION-**ATTR** (**SHO-DEF-PRO-A**)
GUARD-NAME = ***** / <filename 1..24 without-gen-vers with-wild(40)>
,**INF**ORMATION = ***ATTR**IBUTES / ***GUARD-NAM**ES-**ON**LY
,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)
***SYSLST**(...)
SYSLST-NUMBER = ***STD** / <integer 1..99>

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Guards vom Typ DEFPATTR, das angezeigt wird.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Seine Länge ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

INFORMATION =
Legt den Umfang der Information fest, die für jedes Guard ausgegeben wird.

INFORMATION = *ATTRIBUTES
Es werden die Attribute des Guards angezeigt

INFORMATION = *GUARD-NAMES-ONLY
Es werden nur die Namen der Guards angezeigt

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (INFORMATION = *ATTRIBUTES)

```
------------------------------------------------------------------------------
GUARD :ABCD:$GUABRIEL.STD.ATTR                  DEFAULT PROTECTION ATTRIBUTES
------------------------------------------------------------------------------
                  % SCOPE: CREATE-OBJECT        % SCOPE: MODIFY-OBJECT-ATTR
                  % ----------------------------- % ----------------------------
ACCESS            % *WRITE                      % *READ
USER-ACCESS       % *OWNER-ONLY                 % *OWNER-ONLY
BASIC-ACL         % *NONE                       % OWNER  = R W X
                  %                            % GROUP  = R - -
                  %                            % OTHERS = - - -
GUARDS            % *NONE                       % READ   = $AAAAAAAA.BBBBBBBB
                  %                            % WRITE  = $AAAAAAAA.BBBBBBBB
                  %                            % EXEC   = $AAAAAAAA.BBBBBBBB
READ-PASSWORD     % *NONE                       % *NONE
WRITE-PASSWORD    % *NONE                       % *YES
EXEC-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
DESTROY-BY-DELETE % *NO                        % *YES
SPACE-RELEASE-LOCK % *NO                       % *YES
EXPIRATION-DATE   % yyyy-mm-dd                 % yyyy-mm-dd
FREE-FOR-DELETION % yyyy-mm-dd                 % yyyy-mm-dd
------------------------------------------------------------------------------
GUARDS SELECTED: 1                                          END OF DISPLAY
```

Ausgabelayout (INFORMATION = *GUARD-NAMES-ONLY)

```
------------------------------------------------------------------------------
LIST OF ATTRIBUTE GUARDS                        DEFAULT PROTECTION ATTRIBUTES
------------------------------------------------------------------------------
GUARD :ABCD:$GUABRIEL.STD.ATTR
GUARD :ABCD:$GUABRIEL.ATTR-BAK
------------------------------------------------------------------------------
GUARDS SELECTED: 2                                          END OF DISPLAY
```

Das Format der Ausgabe wird nicht garantiert.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
	32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
	64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
	64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
	64	DEF3308	Eine Benutzerkennung ist unbekannt.
	64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
	64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
	64	DEF3314	Fehler im Kommunikationsmittel des MRS.
	64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
	64	DEF3351	Ein genanntes Attributguard gibt es noch nicht.
	64	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
	128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
	128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.
	128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	gekürzte Schreibweise in Tabelle
INFORMATION = *ATTRIBUTES	1
INFORMATION = *GUARD-NAMES-ONLY	2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Attributguards	VAR(*LIST).GUARD-NAME	S	<filename 1.24>	1, 2
Attributbereich	VAR(*LIST).SCOPE(*LIST).SCOPE	S	*CREATE-OBJECT *MODIFY-OBJECT-ATTR	1
Zugriffsart	VAR(*LIST).SCOPE(*LIST).ACCESS	S	*SYSTEM-STD *READ *WRITE	1

(Teil 1 von 3)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Benutzerkreis des Objekts	VAR(*LIST).SCOPE(*LIST).USER-ACCESS	S	*SYSTEM-STD *OWNER-ONLY *ALL-USERS *SPECIAL	1
Schutz durch BASIC-ACL	VAR(*LIST).SCOPE(*LIST).B-ACL.ACTIVE	S	*SYSTEM-STD *NONE *BY-VALUE	1
Leseberechtigung für OWNER (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OWNER.READ	S	*YES *NO ''	1
Schreibberechtigung für OWNER (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OWNER.WRITE	S	*YES *NO ''	1
Ausführberechtigung für OWNER (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OWNER.EXEC	S	*YES *NO ''	1
Leseberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.GROUP.READ	S	*YES *NO ''	1
Schreibberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.GROUP.WRITE	S	*YES *NO ''	1
Ausführberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.GROUP.EXEC	S	*YES *NO ''	1
Leseberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OTHERS.READ	S	*YES *NO ''	1
Schreibberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OTHERS.WRITE	S	*YES *NO ''	1
Ausführberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). B-ACL.OTHERS.EXEC	S	*YES *NO ''	1
Schutz durch GUARDS	VAR(*LIST).SCOPE(*LIST). GUARDS.ACTIVE	S	*SYSTEM-STD *NONE *BY-VALUE	1
Name des Guards, über das lesende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST).GUARDS.READ	S	<guard-name> ''	1
Name des Guards, über das schreibende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST).GUARDS.WRITE	S	<guard-name> ''	1

(Teil 2 von 3)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Guards, über das ausführende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST).GUARDS.EXEC	S	<guard-name> ''	1
Lesekennwort	VAR(*LIST).SCOPE(*LIST).READ-PASS	S	*SYSTEM-STD *NONE *YES	1
Schreibkennwort	VAR(*LIST).SCOPE(*LIST).WRITE-PASS	S	*SYSTEM-STD *NONE *YES	1
Ausführungskennwort	VAR(*LIST).SCOPE(*LIST).EXEC-PASS	S	*SYSTEM-STD *NONE *YES	1
Datenzerstörung beim Löschen	VAR(*LIST).SCOPE(*LIST).DESTROY	S	*SYSTEM-STD *YES *NO	1
Freigabe von Speicherplatz	VAR(*LIST).SCOPE(*LIST). SPACE-RELE-LOCK	S	*SYSTEM-STD *YES *NO	1
Freigabedatum	VAR(*LIST).SCOPE(*LIST).EXPIR-DATE	S I	*SYSTEM-STD *TODAY *TOMORROW <yyyy-mm-dd> <integer 1.99999>	1
Löschungsdatum des Objekts	VAR(*LIST).SCOPE(*LIST).DEL-DATE	S I	*SYSTEM-STD *NONE <yyyy-mm-dd> <integer 1.99999>	1

(Teil 3 von 3)

SHOW-DEFAULT-PROTECTION-RULE
Standardschutzregel anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando können Regeln für die Standardwertvergabe angezeigt werden, die in einem oder mehreren Regelbehältern (Guards des Typs DEFAULTP) eingetragen sind.

SHOW-DEFAULT-PROTECTION-RULE	(**SHO-DEF-PRO-R**)

RULE-CONTAINER-GUARD = ***** / <filename 1..24 without-gen-vers with-wild(40)>

,**SELECT** = ***ALL** / ***BY-RULES**(...)

***BY-RULES**(...)

PROTECTION-RULE = <alphanum-name 1..12 with-wild(20)>

,**INFORMATION** = ***RULES** / ***CONTAINER-GUARD-NAMES-ONLY**

,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)

***SYSLST**(...)

SYSLST-NUMBER = ***STD** / <integer 1..99>

RULE-CONTAINER-GUARD = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Regelbehälters vom Typ DEFAULTP, dessen Regeln angezeigt werden sollen.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regeln mehrerer Behälter durch Absetzen eines einzigen Kommandos angezeigt werden.

Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Behälternamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SELECT=
Mit diesem Operanden wird das Selektionskriterium festgelegt.

SELECT = *ALL
Es werden alle Regeln angezeigt.

Das bedeutet für INFORMATION=*RULES:
Es wird der Name des Regelbehälters und alle darin enthaltenen Regeln angezeigt.

Das bedeutet für INFORMATION=*CONTAINER-GUARD-NAMES-ONLY:
Es wird nur der Name des Regelbehälters angezeigt.

SELECT = *BY-RULES(...)
Es wird eine genau spezifizierte Regel angezeigt.

Das bedeutet für INFORMATION=*RULES:
Es werden der Name des Regelbehälters und die selektierte Regel angezeigt.

Das bedeutet für INFORMATION=*CONTAINER-GUARD-NAMES-ONLY:
Es wird der Name des Regelbehälters angezeigt.

PROTECTION-RULE = name 1..12 with-wild(20)>
Name der Regel, die angezeigt wird. Der Name kann mit Musterzeichen spezifiziert werden.

INFORMATION=
Legt den Umfang der Information fest, die ausgegeben wird.

INFORMATION = *RULES
Der Name des Regelbehälters und die enthaltenen Regeln werden angezeigt.

INFORMATION = *CONTAINER-GUARD-NAMES-ONLY
Nur die Namen der Behälter werden angezeigt.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (INFORMATION = *RULES)

Beispiel

Ein Guard-Administrator hat unter der Benutzerkennung TSOS einen benutzerspezifischen und einen pubsetspezifischen Regelbehälter angelegt. Bevor er beide modifiziert hat, hat er sich eine Sicherungskopie erstellt.

Der Guard-Administrator gibt folgendes Kommando:

```
/show-default-protection-rule rule-container-guard=*,information=*rules
```

```
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$TSOS.PDF.BAK                          DEFAULT PROTECTION
------------------------------------------------------------------------------
REGELNAME001   OBJECT     = PARADIES.*
               ATTRIBUTES = $GUABRIEL.GUA-ATTR
               USER-IDS   = $GUABRIEL.GUA-UIDS
REGELNAME002   OBJECT     = ADAM.*
               ATTRIBUTES = $GUABRIEL.GRP-ATTR
               USER-IDS   = $GUABRIEL.GRP-UIDS
REGELNAME003   FOR ALL TEMPORARY OBJECTS
               ATTRIBUTES = $GUABRIEL.GUA-ATTR
               USER-IDS   = *NONE
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$TSOS.UDF.BAK                          DEFAULT PROTECTION
------------------------------------------------------------------------------
REGELNAME00X   OBJECT     = SYS.*
               ATTRIBUTES = $TSOS.OWN-ATTR
               USER-IDS   = $TSOS.OWN-UIDS
REGELNAME00Y   OBJECT     = *.SYS
               ATTRIBUTES = $TSOS.ALL-ATTR
               USER-IDS   = $TSOS.ALL-UIDS
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$TSOS.SYS.PDF              PVS ACTIVE  DEFAULT PROTECTION
------------------------------------------------------------------------------
REGELNAME001   OBJECT     = PARADIES.*
               ATTRIBUTES = $GUABRIEL.GUA-ATTR
               USER-IDS   = $GUABRIEL.GUA-UIDS
REGELNAME002   OBJECT     = ADAM.*
               ATTRIBUTES = $GUABRIEL.GRP-ATTR
               USER-IDS   = $GUABRIEL.GRP-UIDS
REGELNAME003   FOR ALL TEMPORARY OBJECTS
               ATTRIBUTES = $GUABRIEL.GUA-ATTR
               USER-IDS   = *NONE
------------------------------------------------------------------------------
RULE CONTAINER :ABCD:$TSOS.SYS.UDF              USR ACTIVE  DEFAULT PROTECTION
------------------------------------------------------------------------------
REGELNAME00X   OBJECT     = SYS.*
               ATTRIBUTES = $TSOS.OWN-ATTR
               USER-IDS   = $TSOS.OWN-UIDS
REGELNAME00Y   OBJECT     = *.SYS
               ATTRIBUTES = $TSOS.ALL-ATTR
               USER-IDS   = *ANY-USER-ID
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 4                                  END OF DISPLAY
```

Ausgabelayout (INFORMATION = *CONTAINER-GUARD-NAMES-ONLY)

Der Guard-Administrator gibt folgendes Kommando:

```
/show-default-protection-rule rule-container-guard=*, -
/              information=*container-guard-names-only
```

```
_____________________________________________________________________________
LIST OF RULE CONTAINER NAMES                              DEFAULT PROTECTION
_____________________________________________________________________________
:ABCD:$TSOS.SYS.PDF                                                PVS ACTIVE
:ABCD:$TSOS.SYS.UDF                                                USR ACTIVE
:ABCD:$TSOS.UDF.BAK
_____________________________________________________________________________
RULE CONTAINER SELECTED: 4                                  END OF DISPLAY
```

Das Format der Ausgabe wird nicht garantiert.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
64	DEF3300	Der angegebene Regelbehälter existiert nicht.
64	DEF3301	Es wurde keine Regel gefunden, die den angegebenen Auswahlkriterien entspricht.
64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
64	DEF3304	Es wurde kein Regelbehälter gefunden, der den angegebenen Auswahlkriterien entspricht.
64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
64	DEF3308	Eine Benutzerkennung ist unbekannt.
64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
64	DEF3310	Eine Regel wurde im Regelbehälter nicht gefunden.
64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
64	DEF3314	Fehler im Kommunikationsmittel des MRS.
64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.
128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	gekürzte Schreibweise in Tabelle
INFORMATION = *RULES INFORMATION = *RULE-CONTAINER-GUARD-NAMES	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Regelbehälters	VAR(*LIST).RULE-CONTAIN-GUARD	S	<filename 1..24>	1, 2
Angabe, ob der Regelbehälter aktiv ist	VAR(*LIST).CONTAIN-CONDITION	S	PVS ACTIVE USR ACTIVE ''	1
Name der Regel	VAR(*LIST). PROTECTION-RULE(*LIST).RULE-NAME	S	<alphanumeric name 1..12>	1
Objektname in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). OBJECT-NAME	S	<filename 1..41 without-cat-gen-user with-wild(80)> FOR ALL TEMPORARY OBJECTS	1
Name des Attributguards in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). ATTRIBUTE-GUARD	S	*NONE <filename 1..18 without-cat-gen-vers>	1
Name des Benutzerkennungsguards in der Regel	VAR(*LIST). PROTECTION-RULE(*LIST). USER-ID-GUARD	S	*NONE <filename 1..18 without-cat-gen-vers>	1

SHOW-DEFAULT-PROTECTION-UID
Kennungen für Objektpfad anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: GUARD-ADMINISTRATION, TSOS

Mit dieser Funktion kann sich der Systemverwalter oder ein Guard-Administrator Benutzer- und Gruppenkennungen aus einem Benutzerkennungsguard anzeigen lassen.

SHOW-DEFAULT-PROTECTION-**UID**	(**SHO-DEF-PRO-U**)
GUARD-NAME = ***** / <filename 1..24 without-gen-vers with-wild(40)>	
,**INF**ORMATION = ***USER-ID-LIST** / ***GUARD-NAM**ES-**ON**LY	
,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)	
***SYSLST**(...)	
SYSLST-NUMBER = ***STD** / <integer 1..99>	

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Dieser Operand bezeichnet den Namen des Guards vom Typ DEFPUID, dessen Benutzerkennungen und Benutzergruppen angezeigt werden sollen. Die Länge des Namens ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.

Musterzeichen im Namen des Guards bewirken, dass durch Absetzen eines einzigen Kommandos mehrere Guards angezeigt werden.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

INFORMATION=
Legt den Umfang der Information fest, die für jedes Guard ausgegeben wird.

INFORMATION = *USER-ID-LIST
Es werden die Benutzerkennungen und Benutzergruppen angezeigt.

INFORMATION = *GUARD-NAMES-ONLY
Es werden nur die Namen der Guards angezeigt.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (INFORMATION = *USER-ID-LIST)

```
------------------------------------------------------------------------------
GUARD :ABCD:$TSOS.SYS.LIST                              DEFAULT PROTECTION UID
------------------------------------------------------------------------------
USER      DUSR
          NUSR
          SUSR
GROUP     GRP1
          SYSTEM
------------------------------------------------------------------------------
GUARD :ABCD:$TSOS.USR.LIST                              DEFAULT PROTECTION UID
------------------------------------------------------------------------------
USER      AUSR
          BUSR
------------------------------------------------------------------------------
GUARDS SELECTED: 2                                              END OF DISPLAY
```

Ausgabelayout (INFORMATION = *GUARD-NAMES-ONLY)

```
------------------------------------------------------------------------------
LIST OF USER ID GUARDS                                  DEFAULT PROTECTION UID
------------------------------------------------------------------------------
:ABCD:$TSOS.SYS.LIST
:ABCD:$TSOS.USR.LIST
------------------------------------------------------------------------------
GUARDS SELECTED: 2                                              END OF DISPLAY
```

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
64	DEF3308	Eine Benutzerkennung ist unbekannt.
64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
64	DEF3314	Fehler im Kommunikationsmittel des MRS.
64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
64	DEF3400	Das angegebene Benutzerkennungsguard existiert nicht.
64	DEF3401	Keine Benutzerkennung entspricht den Auswahlkriterien.
64	DEF3402	Kein Benutzerkennungsguard entspricht den Auswahlkriterien.
128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.
128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	gekürzte Schreibweise in Tabelle
INFORMATION = *USER-ID-LIST INFORMATION = *NAMES-ONLY	1 2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Benutzerkennungs-guards	VAR(*LIST).GUARD-NAME	S	<filename 1.24>	1, 2
Angabe, ob die Kennung eine Benutzer- oder Gruppenkennung ist	VAR(*LIST).ID(*LIST).TYPE	S	*USER *GROUP	1
Kennung	VAR(*LIST).ID(*LIST).ID	S	*UNIVERS <name 1.8>	1

SHOW-EVALUATED-CONDITIONS
Auszuwertende Zugriffsbedingungen anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Dieses Kommando zeigt an, welche in einem Guard definierten Bedingungen für welchen Objekttyp ausgewertet wird.

Ein Guard kann gleichzeitig zum Schutz mehrerer unterschiedlicher Objekte herangezogen werden. Nicht jede in einem Guard definierbare Bedingung (Datum, Uhrzeit, Wochentag, Privileg und Programm) ist jedoch für jeden Objekttyp relevant. So spielt beispielsweise die Zugriffsbedingung PROGRAM bei der Zugriffskontrolle für DVS-Dateien eine Rolle, aber bei der Dialog-Zugangskontrolle nicht.

Jede Objektverwaltung, die für ihre Objekte einen Guardsschutz anbietet, legt daher fest, welche Zugriffsbedingungen für ihre Objekte ausgewertet werden müssen. Diese Systeminformation wird mit dem Kommando /SHOW-EVALUATED-CONDITIONS angezeigt. Die Ausgabe enthält dabei jedoch nur diejenigen Objekttypen angezeigt, die GUARDS zum Zeitpunkt der Kommandoeingabe bekannt sind. Wäre zum Beispiel die Objektverwaltung JVS nicht aktiv, würde der Objekttyp JV nicht angezeigt.

Dieses Kommando ist nicht SPVS-, MSCF- oder RFA-fähig.

SHOW-EVALUATED-CONDITIONS
OBJECT-TYPE = ***ALL** / list-poss(20): <composed-name 1..8> ,**OUTPUT** = list-poss(2): ***SYSOUT** / ***SYSLST**

OBJECT-TYPE = *ALL
Es werden die Bedingungen für alle Objekttypen ausgegeben, deren Objektverwaltung zum Zeitpunkt der Kommandoeingabe aktiv ist.

OBJECT-TYPE = list-poss(20): <name 1..8>
Die Bedingungen für den angegebenen Objekttyp werden ausgeben, sofern seine Objektverwaltung zum Zeitpunkt der Kommandoeingabe aktiv ist.
Als Name des Objekttyps muss der systeminterne Objekttypname gemäß folgender Tabelle angegeben werden.

Systeminterner Objektypname	Bedeutung:
DMS	Datei
FITC	FITC-Port
PLAM	Bibliothekslement
JV	Jobvariable
STOR-CLS	Storage-Klasse
MGMT-CLS	HSMS-Management-Klasse
SRPM-GPR	Gruppenzuordnung
SRPM-LDI	Dialog-Zugang, Netzdialog-Zugang, Terminal-Set
SRPM-LBA	Batch-Zugang
SRPM-PRL	POSIX-Rlogin-Zugang
SRPM-PRE	POSIX-Remote-Zugang

OUTPUT =
Bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Ausgabe auf Datensichtstation, sofern das Kommando im Dialog gegeben wurde.

OUTPUT = *SYSLST
Ausgabe auf SYSLST.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
64	PRO1042	Nutzer nicht registriert
64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Beispiel

```
/show-evaluated-conditions

%Objecttype     Time      Date     Weekday  Privilege  Program
%-------------------------------------------------------------
%DMS             YES       YES       YES       YES       YES
%FITC            YES       YES       YES       YES       YES
%PLAM            YES       YES       YES       YES       YES
%JV              YES       YES       YES       YES       YES
%STOR-CLS        YES       YES       YES       YES       NO
%MGMT-CLS        YES       YES       YES       YES       NO
%SRPM-GPR        YES       YES       YES       YES       YES
%SRPM-LDI        YES       YES       YES       NO        NO
%SRPM-LBA        YES       YES       YES       YES       YES
%SRPM-PRL        YES       YES       YES       NO        NO
%SRPM-PRE        YES       YES       YES       NO        NO
```

YES: Die Bedingung wird für den Objekttyp ausgewertet.

NO: Die Bedingung wird für den Objekttyp nicht ausgewertet.

Das Format der Ausgabe wird nicht garantiert.

Die Spalte *Objecttype* enthält den systeminternen Namen des Objektyps. Eine Übersicht über die Bedeutung der systeminternen Objekttypnamen finden Sie bei der Beschreibung der Operanden OBJECT-TYPE auf Seite 674.

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Objekttyps	var(*LIST).OBJECT-TYPE	S	<name1..8>	
Tageszeit als Zugriffsbedingung	var(*LIST).TIME	S	*NO *YES	
Datum als Zugriffsbedingung	var(*LIST).DATE	S	*NO *YES	
Wochentag als Zugriffsbedingung	var(*LIST).WEEKDAY	S	*NO *YES	
Privileg als Zugriffsbedingung	var(*LIST).PRIVIL	S	*NO *YES	
Programm als Zugriffsbedingung	var(*LIST).PROG	S	*NO *YES	

SHOW-GUARD-ATTRIBUTES
Guard-Attribute anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando werden die folgenden Informationen ausgegeben:

– Name des Guards
– SCOPE-Attribut des Guards (USR, GRP oder SYS)
– Typ des Guards
– Erstellungsdatum
– Datum der letzten Änderung
– Kommentar

Ein Guard wird nur berechtigten Anwendern angezeigt. Dies sind immer der Eigentümer und ein Guard-Administrator. Da ein Guard-Administrator Eigentümer aller Guards ist, kann er sich auch alle Guards anzeigen lassen. Andere Benutzer bekommen ein Guard nur angezeigt, wenn dies durch die SCOPE-Angabe bei der Definition des Guards zugelassen wurde.

```
SHOW-GUARD-ATTRIBUTES

 GUARD-NAME = * / <filename 1..24 without-gen-vers with-wild(40)>
,SELECT = *ALL / *BY-ATTRIBUTES(...)
    *BY-ATTRIBUTES(...)
        SCOPE = *ANY / list-poss(3): *USER-ID / *USER-GROUP / *HOST-SYSTEM
        ,TYPE = *ANY / <c-string 1..8>
,INFORMATION = *ALL / *NAMES-ONLY
,OUTPUT = list-poss(2): *SYSOUT / *SYSLST
```

GUARD-NAME = * / <filename 1..24 without-gen-vers with-wild(40)>
Angabe des Guards, dessen Attribute angezeigt werden. Im Namen dürfen Musterzeichen enthalten sein. Seine Länge ohne Musterzeichen, Katalog- und Benutzerkennung darf 8 Zeichen nicht überschreiten.
Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator verwenden.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SELECT =
Bestimmt, welche Guards angezeigt werden.

SELECT = *ALL
Es werden alle Guards angezeigt, die durch die Angabe von GUARD-NAME in diesem Kommando ausgewählt wurden. Wenn ein teilqualifizierter Guard-Name oder ein Guard-Name mit Musterzeichen angegeben wurde, können mehrere Guards der Auswahl entsprechen.

SELECT = *BY-ATTRIBUTES(...)
Die Ausgabe wird auf die folgenden Kriterien eingeschränkt.

SCOPE =
Die Auswahl erfolgt anhand des Attributs SCOPE.

SCOPE = *ANY
Keine einschränkende Wirkung auf die Ausgabe.

SCOPE = list-poss(3): *USER-ID / *USER-GROUP / *HOST-SYSTEM
Wählt Guards mit dem angegebenen SCOPE aus. SCOPE wurde bei der Definition festgelegt. Der SCOPE-Selektionsoperand wird nur ausgewertet, wenn der Aufrufer der Eigentümer oder Guard-Administrator ist.

TYPE =
Die Auswahl erfolgt anhand des Guardtyps.

TYPE = *ANY
Keine einschränkende Wirkung auf die Ausgabe.

TYPE = <c-string 1..8>
Es werden nur Guards mit dem angegebenen Typ ausgegeben. Die selektive Ausgabe von Guards des Typs UNDEF wird nicht unterstützt.

INFORMATION =
Legt den Umfang der auszugebenden Information fest.

INFORMATION = *ALL
Es werden alle Attribute des Guards angezeigt.

INFORMATION = *NAMES-ONLY
Es wird nur der Name des Guards angezeigt.

OUTPUT =
Bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Ausgabe auf Datensichtstation, sofern das Kommando im Dialog gegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST
Ausgabe auf SYSLST.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1002	Der Guard-Name ist syntaktisch falsch
	64	PRO1007	Das angegebene Guard existiert nicht
	64	PRO1012	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	64	PRO1013	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	64	PRO1016	Fehler im Kommunikationsmittel des MRS
	64	PRO1017	Unbekannte Benutzerkennung
	64	PRO1018	Fernes System nicht verfügbar
	64	PRO1020	Kein Speicher mehr vorhanden
	64	PRO1021	BCAM-Verbindungsfehler
	64	PRO1022	BCAM-Verbindung unterbrochen
	64	PRO1023	Kein Guard entspricht den Auswahlkriterien
	64	PRO1024	Nutzung des Guards nicht zugelassen
	64	PRO1029	GUARDS auf dem fernen Rechner nicht verfügbar
	128	PRO1009	Das angegebene Guard ist von einer anderen Task gesperrt
	128	PRO1036	Guardskatalog gesperrt
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Beispiel

```
/show-guard-attributes
```

```
Guard name          Scope   Type      Creation Date       LastMod Date
-------------------------------------------------------------------------------
:N:$GUARDDOC.EXAGUARD     USR  STDAC    2017-04-29/13:11:21 2017-05-13/13:24:39
:N:$GUARDDOC.GUARDEXA     GRP  STDAC    2017-04-29/10:52:28 2017-04-29/11:07:06
                          GUARD FOR ACCESS CONTROL OF ALL GROUP MEMBERS
:N:$GUARDDOC.SECGUARD     SYS  STDAC    2017-04-27/11:32:38 2017-04-27/13:35:04
                          EXAMPLE GUARD
:N:$GUARDDOC.XYZGUARD     SYS  UNDEF    2017-04-28/13:42:19 2017-04-02/09:16:51
-------------------------------------------------------------------------------
Guards selected: 4                                              End of display
```

Das Format der Ausgabe wird nicht garantiert.

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Erstellungsdatum des Guards	var(*LIST).CRE-DATE	S	<yyyy-mm-dd>	INF=*ALL
Erstellungs-Uhrzeit des Guards	var(*LIST).CRE-TIME	S	<hh:mm:ss>	INF=*ALL
Name des Guards	var(*LIST).GUARD-NAME	S	<filename 1..40> <part.-filename 2..40>	INF=*ALL/ *NAMES-ONLY
Datum der letzten Änderung	var(*LIST).LAST-MOD-DATE	S	<yyyy-mm-dd>	INF=*ALL
Uhrzeit der letzten Änderung	var(*LIST).LAST-MOD-TIME	S	<hh:mm:ss>	INF=*ALL
Benutzergruppe, die das Guard zum Schutz ihrere Objekte verwenden darf *HOST-SYS: Jeder darf das Guard benutzen *USER-GROUP: Mitglieder der Benutzergruppe des Eigentümers dürfen Guard benutzen *USER-ID: Nur der Eigentümer darf Guard benutzen	var(*LIST).SCOPE	S	*HOST-SYS *USER-GROUP *USER-ID	INF=*ALL
Typ des Guards	var(*LIST).TYPE	S	*COOWNERP *DEFAULTP *DEFPATTR *DEFPUID *STDAC *UNDEF	INF=*ALL
Kommentartext zum Guard	var(*LIST).USER-INFO	S	<c-string1..80>	INF=*ALL

SHOW-GUARD-MANAGEMENT-STATUS
GUARDS-Systemeinstellungen anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: TSOS, GUARD-ADMINISTRATION

Dieses Kommando gibt die folgenden Informationen zum Zustand der GUARDS-Verwaltung aus:

– Name des Guardskatalogs

– Name der SSINFO-Datei

– Anzahl der Servertasks

– Anzahl der von GUARDS verwalteten Pubsets

– Pubsets pro Servertask

– pro Pubset: zugehörige Servertask
Status des Pubsets - mögliche Anzeigen sind:

NOT INITIALIZED	Guardskatalog auf dem Pubset ist nicht initialisiert
INITIALIZED	Guardskatalog auf dem Pubset ist initialisiert
IN INITIALIZATION	Guardskatalog auf dem Pubset wird initialisiert
IN TERMINATION	GUARDS für das Pubset wird beendet
LOCKED BY ARCHIVE	Guardskatalog auf dem Pubset von ARCHIVE gesperrt

Dieses Kommando ist nicht MSCF- oder RFA-fähig.

SHOW-GUARD-MANAGEMENT-**STA**TUS
OUTPUT = list-poss(2): ***SYSOUT** / ***SYSLST**

OUTPUT =
Bestimmt das Ziel der Ausgabe. Bei Angabe beider Schlüsselwörter wird die Information sowohl auf die Datensichtstation als auch auf SYSLST ausgegeben. Im Batchbetrieb ist die Angabe von *SYSOUT unwirksam.

Kommando-Returncode

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	Kommando erfolgreich ausgeführt
	32	PRO1001	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	64	PRO1014	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	64	PRO1020	Kein Speicher mehr vorhanden
	64	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
	130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
	32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Beispiel

```
/show-guard-management-status

 Status Information for  G U A R D S
                        ___________________________________
GUARD Catalog name    : $TSOS.SYSCAT.GUARDS
INFO File name        : $TSOS.SYSSSI.GUARDS.055
Number of server tasks: 1               Number of served pubsets: 1

Task serves pubsets
PRO1                    11

Pubset served by task                   Status
11                      PRO1            INITIALIZED
                                                          End of display
```

Ausgabe in S-Variablen

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Guardkatalogs	var(*LIST).GUARD-CAT-NAME	S	<filename 1..40>	
Anzahl der von GUARDS verwalteten Pubsets	var(*LIST).NUM-OF-SERVED-PUBSET	I	<integer 1..16>	
Anzahl der Server-Tasks	var(*LIST).NUM-OF-SERVER-TASK	I	<integer 1..32767>	
Katalogkennung des Pubsets	var(*LIST).PUBSET(*LIST).PUBSET	S	<cat-id 1..4>	
Status des Pubsets *IN-INIT: Guardskatalog wird auf Pubset initialisiert *IN-TERM: GUARDS wird für dieses Pubset beendet *INIT: Guardskatalog ist auf dem Pubset initialisiert *LOCK-BY-ARCHIVE: Guardskatalog auf diesem Pubset ist von ARCHIVE zur Sicherung gesperrt *NOT-INIT: Guardskatalog ist auf dem Pubset nicht initialisiert	var(*LIST).PUBSET(*LIST).STA	S	*IN-INIT *IN-TERM *INIT *LOCK-BY-ARCHIVE *NOT-INIT	
TSN der Servertask	var(*LIST).PUBSET(*LIST).TSN	S	<name 1..4>	
Katalogkennung des Pubsets	var(*LIST).SERVER(*LIST).PUBSET(*LIST)	S	<cat-id 1..4>	
TSN der Servertask	var(*LIST).SERVER(*LIST).TSN	S	<name 1..4>	
Name der SSINFO-Datei	var(*LIST).SSINFO-F-NAME	S	<filename 1..40>	

SHOW-OBJECT-PROTECTION-DEFAULT
Standardschutzattribute für Objekt anzeigen

Anwendungsbereich: SECURITY-ADMINISTRATION

Privilegierung: STD-PROCESSING, GUARD-ADMINISTRATION

Mit diesem Kommando kann sich ein Anwender für einen spezifizierten Objektnamen anzeigen lassen, welche Standardschutzwerte festgelegt sind und in welchen Regeln diese Standardschutzwerte beschrieben sind. Die Standardschutzattribute werden jedoch nur für eigene Objekte des Kommandoaufrufers oder für Objekte mit entsprechender Miteigentümerberechtigung angezeigt.

Regeln für den Standardschutz können sowohl für Dateinamen als auch für Jobvariablen spezifiziert und in einem jeweils separaten, aktiven Regelbehälter eingetragen sein. Darum wird über den Operand RULE-CONTAINER-TYPE gesteuert, ob Auskunft über Standardschutzattribute von Dateien oder von Jobvariablen gewünscht wird.

Es wird immer nur ein gesamtmögliches Attribut-Set angezeigt, unabhängig davon, ob einzelne Attribute für Jobvariablen verwertbar sind oder nicht.

SHOW-OBJECT-**PROTECT**ION-**DEFAULT**	(**SHO-OBJ-PRO-DEF**)

OBJECT-**NAM**E = <filename 1..54 without-gen>

,**RULE-CONT**AINER-**TYP**E = ***FILE** / ***JV**

,**INF**ORMATION = ***ATTR**IBUTE-**VAL**UES / ***ATTR**IBUTE-**ORIGIN**

,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)

***SYSLST**(...)

SYSLST-NUMBER = ***STD** / <integer 1..99>

OBJECT-NAME =

Name des Objektes, über das sich der Aufrufer bezüglich der Standardschutzattribute informieren will.

ACHTUNG!
Der Name darf keine Musterzeichen enthalten.

RULE-CONTAINER-TYPE =
Typ des aktiven Regelbehälters, in dem nach Regeln für die Standardattributfestlegung gesucht wird.

RULE-CONTAINER-TYPE = *FILE
Es wird in aktiven Regelbehältern gesucht, in denen Regeln für den Standardschutz von Dateien spezifiziert sind (SYS.UDF[<n>]).

RULE-CONTAINER-TYPE = *JV
Es wird in aktiven Regelbehältern gesucht, in denen Regeln für den Standardschutz von Jobvariablen spezifiziert sind (SYS.UDJ[<n>]).

INFORMATION =
Legt den Umfang der Information fest, die ausgegeben wird.

INFORMATION = *ATTRIBUTE-VALUES
Es werden die aus den entsprechenden Regelbehältern und Regeln ermittelten Werte der Standardschutzattribute ausgegeben.

INFORMATION = *ATTRIBUTE-ORIGIN
Es werden zusätzlich zu den Attributwerten pro Standardschutzattribut diejenigen Regelbehälternamen und Regeln angezeigt, in denen der jeweilige Attributwert festgelegt ist.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Ausgabelayout (Attribute Values)

Beispiel

Der Miteigentümer LUZIFER informiert sich, welche Standardschutzattribute eine Datei mit Namen $GUABRIEL.PARADIES erhalten würde, wenn er die Datei neu einrichten oder die Attribute mit /MODIFY-FILE-ATTRIBUTES PROTECTION-ATTR=*BY-DEF-PROT-OR-STD ändern würde.

Der Benutzer gibt folgendes Kommando:

```
/show-object-protection-default object-name=:abcd:$guabriel.paradies -
/                               information=*attribute-values
```

```
------------------------------------------------------------------------------
DEFAULTS FOR FILE  :ABCD:$GUABRIEL.PARADIES
------------------------------------------------------------------------------
                   % SCOPE: CREATE-OBJECT        % SCOPE: MODIFY-OBJECT-ATTR
                   % ---------------------------- % --------------------------
ACCESS             % *SYSTEM-STD                 % *READ
USER-ACCESS        % *SYSTEM-STD                 % *OWNER-ONLY
BASIC-ACL          % *SYSTEM-STD                 % *NONE
GUARDS             % *SYSTEM-STD                 % READ   = $GUABRIEL.REAGUARD
                   %                            % WRITE  = $GUABRIEL.WRIGUARD
                   %                            % EXEC   = $GUABRIEL.EXEGUARD
READ-PASSWORD      % *SYSTEM-STD                 % *YES
WRITE-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
EXEC-PASSWORD      % *SYSTEM-STD                 % *SYSTEM-STD
DESTROY-BY-DELETE  % *SYSTEM-STD                 % *YES
SPACE-RELEASE-LOCK % *SYSTEM-STD                 % *YES
EXPIRATION-DATE    % *SYSTEM-STD                 % *SYSTEM-STD
FREE-FOR-DELETION  % *SYSTEM-STD                 % *SYSTEM-STD
------------------------------------------------------------------------------
                                                                END OF DISPLAY
```

Ausgabelayout (Attribute Origin)

Beispiel

Der Miteigentümer LUZIFER informiert sich, woher die Standardschutzattribute für eine Datei mit Namen $GUABRIEL.PARADIES genommen werden, wenn er die Datei neu einrichten oder die Attribute mit /MODIFY-FILE-ATTRIBUTES PROTECTION-ATTR=*BY-DEF-PROT-OR-STD ändern würde.

Der Benutzer gibt folgendes Kommando:

```
/show-object-protection-default object-name=:abcd:$guabriel.paradise -
/                               information=*attribute-origin

------------------------------------------------------------------------------
DEFAULT ORIGIN FOR FILE :ABCD:$GUABRIEL.PARADISE
------------------------------------------------------------------------------
ACCESS               SCOPE           % CREATE-OBJECT
                     VALUE           % *SYSTEM-STD
                     CONTAINER GUARD % $GUABRIEL.SYS.UDF         USR ACTIVE
                     RULE            % RULE00000001
                     USERID GUARD    %                           IGNORED
                     ATTRIBUTE GUARD % $GUABRIEL.MYATTRIB
------------------------------------------------------------------------------
ACCESS               SCOPE           % MODIFY-OBJECT-ATTR
                     VALUE           % *SYSTEM-STD
                     CONTAINER GUARD % $GUABRIEL.SYS.UDF         USR ACTIVE
                     RULE            % RULE00000001
                     USERID GUARD    %                           IGNORED
                     ATTRIBUTE GUARD % $GUABRIEL.MYATTRIB
------------------------------------------------------------------------------

USER-ACCESS
BASIC-ACL
GUARDS
READ-PASSWORD
WRITE-PASSWORD
EXEC-PASSWORD
DESTROY-BY-DELETE
SPACE-RELEASE-LOCK
EXPIRATION-DATE

------------------------------------------------------------------------------
FREE-FOR-DELETION    SCOPE          : CREATE-OBJECT
                     VALUE           % *SYSTEM-STD
                     CONTAINER GUARD: $TSOS.SYS.PDF              PVS ACTIVE
                     RULE           : 2
                     USERID GUARD   :                            *ANY-USER-ID
                     ATTRIBUTE GUARD: $TSOS.SYSATTR
------------------------------------------------------------------------------
FREE-FOR-DELETION    SCOPE          : MODIFY-OBJECT-ATTR
                     VALUE           % *SYSTEM-STD
                     CONTAINER GUARD: $TSOS.SYS.PDF              PVS ACTIVE
                     RULE           : 2
                     USERID GUARD   :                            *ANY-USER-ID
                     ATTRIBUTE GUARD: $TSOS.SYSATTR
------------------------------------------------------------------------------
                                                                 END OF DISPLAY
```

(Auf die Ausgabe für diese Attribute wird aus Platzgründen verzichtet, das Format der Ausgabe ist wie bei den Attributen ACCESS und FREE-FOR-DELETION)

Das Format der Ausgabe wird nicht garantiert.

Kommando-Returncode

(SC2) SC1	Maincode	Bedeutung
0	CMD0001	Kommando erfolgreich ausgeführt
1	DEF3100	Es wurde ein fehlerhafter Operandenwert erkannt.
32	DEF3200	Es ist ein interner Fehler aufgetreten. Für eine genaue Analyse wurde ein SERSLOG-Eintrag erzeugt.
64	DEF3300	Der angegebene Regelbehälter existiert nicht.
64	DEF3302	Der Benutzer ist nicht autorisiert, die Funktion auszuführen.
64	DEF3306	Ein angegebenes Guard ist nicht vom erforderlichen Guardtyp.
64	DEF3308	Eine Benutzerkennung ist unbekannt.
64	DEF3309	Keine Unterstützung für einen Remote-File-Access.
64	DEF3312	Es wurde keine Standardschutzregel für ein genanntes Objekt gefunden.
64	DEF3313	Ein angegebenes Public Volume Set ist nicht verfügbar.
64	DEF3314	Fehler im Kommunikationsmittel des MRS.
64	DEF3315	Ein angegebenes Public Volume Set ist der lokalen GUARDS-Verwaltung nicht bekannt.
64	DEF3316	Der Standardschutz ist nicht aktiv, da kein aktiver Regelbehälter gefunden wurde.
64	DEF3318	Ein Guard mit Benutzerkennungen, das in eine Regel eingetragen werden soll, ist nicht zugreifbar.
64	DEF3320	Ein angegebenes Attributguard ist nicht zugreifbar.
64	DEF3321	Ein benötigter benutzerspezifischer Regelbehälter ist nicht zugreifbar.
64	DEF3322	Ein benötigter pubsetspezifischer Regelbehälter ist nicht zugreifbar.
128	DEF3900	Es steht nicht mehr genügend Systemspeicher zur Verfügung.
128	DEF3901	Ein zu bearbeitendes Guard ist von einer anderen Task gesperrt und kann zur Zeit nicht bearbeitet werden.
128	DEF3902	Ein Guard ist vorübergehend nicht zugreifbar, weil der GUARDS-Katalog gewechselt wird, oder ein Master-Wechsel im Rechnerverbund stattfindet.
128	OPS0002	Ausgabe der S-Variablen wurde unterbrochen
130	OPS0001	Ausgabe der S-Variablen konnte nicht durchgeführt werden
32	CMD2009	Systemfehler bei Ausgabe der S-Variablen

Ausgabe in S-Variablen

Mit dem Operanden INFORMATION des Kommandos wird festgelegt, welche S-Variablen mit Werten versorgt werden. Folgende Angaben sind für INFORMATION möglich:

Schreibweise im Kommando	gekürzte Schreibweise in Tabelle
INFORMATION = *ATTRIBUTE-VALUES	1
INFORMATION = *ATTRIBUTE-ORIGIN	2

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Name des Objekts	VAR(*LIST).OBJECT-NAME	S	<filename 1..54>	1, 2
Typ des aktiven Regelbehälters	VAR(*LIST).RULE-CONTAIN-TYPE	S	*FILE *JV	1, 2
Attributbereich	VAR(*LIST).SCOPE(*LIST).SCOPE	S	*CREATE-OBJECT *MODIFY-OBJECT-ATTR	1, 2
Zugriffsart	VAR(*LIST).SCOPE(*LIST).ATTR-ACCESS	S	*SYSTEM-STD *READ *WRITE	1, 2
Benutzerkreis des Objekts	VAR(*LIST).SCOPE(*LIST).ATTR-USER-ACCESS	S	*SYSTEM-STD *OWNER-ONLY *ALL-USERS *SPECIAL	1, 2
Schutz durch BASIC-ACL	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.ACTIVE	S	*SYSTEM-STD *NONE *BY-VALUE	1, 2
Leseberechtigung für OWNER (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.OWNER.READ	S	*YES *NO ''	1, 2
Ausführberechtigung für OWNER (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.OWNER.WRITE	S	*YES *NO ''	1, 2
Schreibberechtigung für OWNER (Basic ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.OWNER.EXEC	S	*YES *NO ''	1, 2
Leseberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.GROUP.READ	S	*YES *NO ''	1, 2
Ausführberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.GROUP.WRITE	S	*YES *NO ''	1, 2
Schreibberechtigung für GROUP (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST).ATTR-B-ACL.GROUP.EXEC	S	*YES *NO ''	1, 2

(Teil 1 von 3)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Leseberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). ATTR-B-ACL.OTHERS.READ	S	*YES *NO ''	1, 2
Ausführberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). ATTR-B-ACL.OTHERS.WRITE	S	*YES *NO ''	1, 2
Schreibberechtigung für OTHERS (BASIC-ACL)	VAR(*LIST).SCOPE(*LIST). ATTR-B-ACL.OTHERS.EXEC	S	*YES *NO ''	1, 2
Schutz durch GUARDS	VAR(*LIST).SCOPE(*LIST). ATTR-GUARDS.ACTIVE	S	*SYSTEM-STD *NONE *BY-VALUE	1, 2
Name des Guards, über das lesende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST). ATTR-GUARDS.READ	S	<guard-name> *NONE ''	1, 2
Name des Guards, über das schreibende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST). ATTR-GUARDS.WRITE	S	<guard-name> *NONE ''	1, 2
Name des Guards, über das ausführende Zugriffe kontrolliert werden	VAR(*LIST).SCOPE(*LIST). ATTR-GUARDS.EXEC	S	<guard-name> *NONE ''	1, 2
Lesekennwort	VAR(*LIST).SCOPE(*LIST). ATTR-READ-PASS	S	*SYSTEM-STD *NONE *YES	1, 2
Schreibkennwort	VAR(*LIST).SCOPE(*LIST). ATTR-WRITE-PASS	S	*SYSTEM-STD *NONE *YES	1, 2
Ausführungskennwort	VAR(*LIST).SCOPE(*LIST). ATTR-EXEC-PASS	S	*SYSTEM-STD *NONE *YES	1, 2
Datenzerstörung beim Löschen	VAR(*LIST).SCOPE(*LIST). ATTR-DESTROY	S	*SYSTEM-STD *YES *NO	1, 2
Freigabe von Speicherplatz	VAR(*LIST).SCOPE(*LIST). ATTR-SPACE-RELE-LOCK	S	*SYSTEM-STD *YES *NO	1, 2
Freigabedatum	VAR(*LIST).SCOPE(*LIST). ATTR-EXPIR-DATE	S I	*SYSTEM-STD *TODAY *TOMORROW <yyyy-mm-dd> <integer 1..99999>	1, 2

(Teil 2 von 3)

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Löschungsdatum des Objekts	VAR(*LIST).SCOPE(*LIST). ATTR-DEL-DATE	S I	*SYSTEM-STD *NONE <yyyy-mm-dd> <integer 1..99999>	1, 2
Regel, mit der die Zugriffsart festgelegt wird	VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der der Benutzerkreis des Objekts festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-USER-ACCESS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der der Schutz durch BASIC-ACL festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-B-ACL	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der der Schutz durch GUARDS festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-GUARDS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der das Lesekennwort festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-READ-PASS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der das Schreibkennwort festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-WRITE-PASS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der das Ausführungskennwort festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-EXEC-PASS	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der die Datenzerstörung beim Löschen festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-DESTROY	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der die Freigabe von Speicherplatz festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-SPACE-RELE-LOCK	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der das Freigabedatum festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-EXPIR-DATE	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1
Regel, mit der das Löschungsdatum des Objekts festgelegt wird	VAR(*LIST).SCOPE(*LIST). ORIG-DEL-DATE	Unterstruktur (Aufbau siehe Anmerkung am Ende dieser Tabelle)		1

(Teil 3 von 3)

Anmerkung

Die Unterstrukturen ORIG-ACCESS, ORIG-USER-ACCESS, ORIG-B-ACL, ORIG-GUARDS, ORIG-READ-PASS, ORIG-WRITE-PASS, ORIG-EXEC-PASS, ORIG-DESTROY, ORIG-SPACE-RELE-LOCK, ORIG-EXPIR-DATE und ORIG-DEL-DATE bestehen aus folgenden Einzelvariablen:

Ausgabe-Information	Name der S-Variablen	T	Inhalt	Bedingung
Regelbehälter, in dem der Wert des Attributs festgelegt ist	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.RULE-CONTAIN-GUARD	S	<filename 1..24>	1
Angabe, ob es ein pubsetglobaler oder ein benutzerspezifischer Regelbehälter ist	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.RULE-CONTAIN-CONDITION	S	USR ACTIVE PVS ACTIVE	1
Name der Regel, durch die der Wert des Attributs festgelegt ist	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.RULE-NAME	S	<alphanumeric name 1..12>	1
Name des Attributguards, das in der Regel eingetragen ist	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.ATTRIBUTE-GUARD	S	<filename 1..24>	1
Name des Benutzerkennungsguards, das in der Regel eingetragen ist	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.USER-ID-GUARD	S	<filename 1..24>	1
Angabe, ob ein Benutzerkennungsguard in der Regel eingetragen ist bzw ob das Benutzerkennungsguard ausgewertet wird	VAR(*LIST).SCOPE(*LIST).ORIG-xxx.USER-ID-GUARD-IND	S	IGNORED *ANY-USER-ID ”	1

Beispiel

Die Unterstruktur VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS besteht aus folgenden Variablen:

– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.RULE-CONTAIN-GUARD
– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.RULE-CONTAIN-CONDITION
– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.RULE-NAME
– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.ATTRIBUTE-GUARD
– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.USER-ID-GUARD und
– VAR(*LIST).SCOPE(*LIST).ORIG-ACCESS.USER-ID-GUARD-IND

5.11.1 Beispiele zu GUARDS-Kommandos

Die folgenden Beispiele zeigen die Anwendung der GUARDS-Kommandos zur Definition von Guards. Guard und Objekt werden über die Schnittstellen der jeweiligen Objektverwaltung einander zugeordnet. Dies wird exemplarisch für eine Datei am Ende des Beispiels gezeigt.

Beispiel 1: Einrichten eines Zugriffsschutzes

Aufgabenstellung

Der Zugriff auf Dateien des Projektes GUARDS soll durch das Guard GUARDPRO kontrolliert werden.

Das Team besteht aus vier Mitarbeitern mit den Benutzerkennungen GUARDS1, GUARDS2, GUARDS3 und GUARDS4.

Die Arbeitszeit aller Mitarbeiter geht an den Tagen Montag bis Freitag von 07:00 Uhr bis 19:00.

Der Mitarbeiter mit der Benutzerkennung GUARDS3 arbeitet als Teilzeitkraft an den Tagen Montag, Mittwoch und Donnerstag.

Der Mitarbeiter mit der Benutzerkennung GUARDS4 ist ein Mitarbeiter, dessen Vertrag am 1. Juli 2017 beginnt und am 30. September 2017 ausläuft.

Für Reviews sollen die Benutzergruppen ONE und TWO kurzfristig Zugriff erhalten. Der Review findet am 23./24. August 2017 und 2./3. September 2017 von 9:00 Uhr bis 15:00 Uhr statt.

Lösung

Es werden Zugriffsbedingungen für die Kennungen GUARDS1 und GUARDS2 in ein Guard mit dem Namen GUARDPRO eingetragen. Dieses Guard wird dabei automatisch erzeugt.

```
/add-access-conditions guard-name=guardpro, -
/           subjects=*user(user-identification=guards1)
/add-access-conditions guard-name=guardpro, -
/           subjects=*user(user-identification=guards2)
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1  has ADMISSION
   User   GUARDS2  has ADMISSION
------------------------------------------------------------------------------
Guards selected: 1                                          End of display
```

Es werden die Zugriffsbedingungen für die Teilzeitkraft eingetragen:

```
/add-access-conditions guard-name=guardpro, -
/            subjects=*user(user-identification=guards3), -
/             admission=*parameters(weekday=(*monday, *wednesday,*thursday))
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1  has ADMISSION
   User   GUARDS2  has ADMISSION
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
------------------------------------------------------------------------------
Guards selected: 1                                            End of display
```

Es werden die Zugriffsbedingungen für den Mitarbeiter mit der Kennung GUARDS4 eingetragen, dessen Vertrag ausläuft:

```
/add-access-conditions guard-name=guardpro, -
/            subjects=*user(user-identification=guards4), -
/            admission=*parameters( -
/                        date=*interval(from=2017-07-01,to=2017-09-30))
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1  has ADMISSION
   User   GUARDS2  has ADMISSION
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
   User   GUARDS4
    Date      IN ( <2017-07-01,2017-09-30> )
------------------------------------------------------------------------------
Guards selected: 1                                            End of display
```

Für alle Mitarbeiter wird die Arbeitszeit festgelegt:

```
/add-access-conditions guard-name=guardpro,subjects=*all-users, -
/            admission=*parameters(time=*interval(from=7,to=19),  -
/            weekday=*except(weekday=(*saturday,*sunday)))
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1  has ADMISSION
   User   GUARDS2  has ADMISSION
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
   User   GUARDS4
    Date      IN ( <2017-07-01,2017-09-30> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
------------------------------------------------------------------------------
Guards selected: 1                                            End of display
```

Festlegen der Zugriffsbedingungen für die Gruppen ONE und TWO

```
/add-access-conditions guard-name=guardpro, -
/    subjects=*group(group-identification=(one,two)), -
/    admission=*parameters( -
/                date=(*interval(from=2017-08-23,to=2017-08-24), -
/                      *interval(from=2017-09-02,to=2017-09-03)), -
/                time=*interval(from=9,to=15))
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1  has ADMISSION
   User   GUARDS2  has ADMISSION
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
   User   GUARDS4
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  ONE
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-02,2017-09-03> )
   Group  TWO
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-02,2017-09-03> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
--------------------------------------------------------------------------------
Guards selected: 1                                              End of display
```

Beispiel 2: Modifizieren der Zugriffsbedingungen

Aufgabenstellung

Der Mitarbeiter mit der Benutzerkennung GUARDS1 geht von 15. Oktober 2017 bis 15. November 2017 in Urlaub.

Der Mitarbeiter mit der Benutzerkennung GUARDS3 arbeitet statt Montag, Mittwoch und Donnerstag jetzt Montag, Dienstag und Mittwoch.

Das Review am 2./3. September wird verschoben. Es findet am 9./10. September statt.

Lösung

```
/modify-access-conditions guard-name=guardpro, -
/       subjects=*user(user-identification=guards1), -
/       admission=*parameters(date= -
/             *except(date=*interval(from=17-10-15,to=17-11-15)))
/modify-access-conditions guard-name=guardpro, -
/       subjects=*user(user-identification=guards3), -
/       admission=*parameters(weekday=(*monday,*tuesday,*wednesday))
/modify-access-conditions guard-name=guardpro, -
/       subjects=*group(group-identification=(one,two)), -
/       admission=*parameters(date=( -
/                            *interval(from=17-08-23,to=17-08-24), -
/                            *interval(from=17-09-09,to=17-09-10)))
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1
    Date      EX ( <2017-10-15,2017-11-15> )
   User   GUARDS2  has ADMISSION
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
   User   GUARDS4
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  ONE
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-09,2017-09-10> )
   Group  TWO
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-09,2017-09-10> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
------------------------------------------------------------------------------
Guards selected: 1                                          End of display
```

Beispiel 3: Löschen einer Zugriffsbedingung

Aufgabenstellung

Der Mitarbeiter mit der Benutzerkennung GUARDS2 wechselt die Firma. Seine Benutzerkennung soll aus dem Guard entfernt werden.

Lösung

```
/remove-access-conditions guard-name=guardpro, -
/       subjects=*user(user-identification=guards2)
/show-access-conditions guard-name=guardpro

:N:$SECOSMAN.GUARDPRO
   User   GUARDS1
    Date      EX ( <2017-10-15,2017-11-15> )
   User   GUARDS3
    Weekday   IN ( MO, WE, TH )
   User   GUARDS4
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  ONE
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-09,2017-09-10> )
   Group  TWO
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> , <2017-09-09,2017-09-10> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
------------------------------------------------------------------------------
Guards selected: 1                                              End of display
```

Beispiel 4: Verknüpfung einer Datei mit dem Guard GUARDPRO

Aufgabenstellung

Die Datei SECOS soll mit dem Guard GUARDPRO verknüpft werden, damit für Zugriffe die Zugriffsbedingungen des Guards gelten.

Lösung

```
/modify-file-attributes file-name=secos, -
/    protection=*parameters(guards=*parameters(read=guardpro,write=guardpro))
/show-file-attributes file-name=secos,information=*parameters(security=yes)

00001266 :N:$SECOSMAN.SECOS
  ------------------------------ SECURITY     ------------------------------
  READ-PASS  = NONE        WRITE-PASS = NONE        EXEC-PASS  = NONE
  USER-ACC   = OWNER-ONLY  ACCESS     = WRITE       ACL        = NO
  AUDIT      = NONE        DESTROY    = YES         EXPIR-DATE = 2017-11-17
  SP-REL-LOCK= NO                                  EXPIR-TIME =   00:00:00
  GUARD-READ = $SECOSMAN.GUARDPRO
  GUARD-WRIT = $SECOSMAN.GUARDPRO
  GUARD-EXEC = NONE
:N:    PUBLIC:      1 FILE  RES=     1266  FREE=        2  REL=       0 PAGES
```

Beispiel 5: Lösen der Verknüpfung Guard - Datei

Aufgabenstellung

Die Datei SECOS soll nicht mehr mit den Zugriffsbedingungen des Guards GUARDPRO geschützt werden. Dazu wird die Verknüpfung gelöst. Nachdem der GUARDS-Schutz entfernt wurde, gelten die in der Hierarchie niedrigeren Zugriffsschutzmechanismen.

Lösung

```
/modify-file-attributes file-name=secos,protection=*parameters(guards=*none)
/show-file-attributes file-name=secos,information=*parameters(security=*yes)

00001266 :N:$SECOSMAN.SECOS
  ------------------------------ SECURITY     ------------------------------
  READ-PASS  = NONE        WRITE-PASS = NONE        EXEC-PASS  = NONE
  USER-ACC   = OWNER-ONLY  ACCESS     = WRITE       ACL        = NO
  AUDIT      = NONE        DESTROY    = YES         EXPIR-DATE = 2017-11-17
  SP-REL-LOCK= NO                                  EXPIR-TIME =   00:00:00
:N:    PUBLIC:      1 FILE  RES=     1266  FREE=        2  REL=       0 PAGES
```

Beispiel 6: Einrichtung eines benutzerspezifischen Standardschutzes

Aufgabenstellung

Der Benutzer USER1 möchte, dass alle Dateien, deren Namen mit ’FILE‘ beginnen, so angelegt werden, dass der Benutzer USER2 Schreibzugriff darauf hat.

Es ist kein pubsetglobaler Standardschutz aktiv.

Lösung

USER 1 richtet ein Bedingungsguard WRGUA1 mit den Zugriffsbedingungen für USER2 ein:

```
/create-guard wrgua1,user-inf=?Guardschutz zum Schreiben?
/add-access-conditions guard-name=wrgua1, -
/                      subjects=*user(user-identification=user2)
```

Anschließend legt er ein Attributguard ATTR1 an, in dem er als Standardschutzattribut festlegt, dass das Schreibrecht über das Bedingungsguard WRGUA gesteuert werden soll:

```
/create-guard attr1,user-inf=?Guard fuer die Standardschutzattribute?
/add-default-protection-attr guard-name=attr1,-
/                            guards=*parameters(write=wrgua1)
```

Schließlich definiert er einen Regelbehälter DEF1 für Default Protection mit einer Standardschutzregel. Diese Regel besagt, dass die Standardschutzattribute für alle Dateien, die mit ’FILE’ beginnen, im Attributguard ATTR1 festgelegt sind:

```
/create-guard def1,user-inf='Default-Protection-Regelbehaelter'
/add-default-protection-rule rule-container-guard=def1,-
/            protection-rule=rule1, -
/            protect-object=*parameters(name=file*,attribute-guard=attr1)
```

Zur Kontolle gibt USER1 Informationen über alle Guards und den Regelbehälter DEF1 aus. Voraussetzung: Zu Beginn dieser Beispielsitzung waren keine Guards unter der Kennung USER1 vorhanden.

```
/show-guard-attributes
```

```
     Guard name          Scope   Type      Creation Date       LastMod Date
------------------------------------------------------------------------------
:DEL1:$USER1.ATTR1        USR  DEFPATTR 2017-04-20/07:48:09 2017-04-20/08:04:01
                          Guard fuer die Standardschutzattribute
:DEL1:$USER1.DEF1         USR  DEFAULTP 2017-04-20/07:52:36 2017-04-20/08:11:11
                          Default-Protection-Regelbehaelter
:DEL1:$USER1.WRGUA1       USR  STDAC    2017-04-20/07:48:46 2017-04-20/07:49:17
                          Guardschutz zum Schreiben
------------------------------------------------------------------------------
Guards selected: 3                                              End of display
```

```
/show-default-protection-rule rule-container-guard=def1

------------------------------------------------------------------------------
RULE CONTAINER :DEL1:$USER1.DEF1                            DEFAULT PROTECTION
------------------------------------------------------------------------------
RULE1          OBJECT     = FILE*
               ATTRIBUTES = $USER1.ATTR1
               USER-IDS   = *ANY-USER-ID
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                    END OF DISPLAY
```

Da der Name des Regelbehälters nicht den Namenskonventionen für aktive Regelbehälter entspricht, dient er nur zur Vorbereitung der Standardschutzregel. Für eine Datei mit dem Namen FILE1 (entspricht dem Muster FILE*) ist noch kein Standardschutz aktiv, wie folgendes Kommando zeigt:

```
/show-object-protection-default file1
DEF3316 NO DEFAULT PROTECTION ACTIVE
```

Um den Standardschutz zu aktivieren, benennt USER1 den inaktiven Regelbehälter DEF1 um:

```
/mod-guard-attr guard-name=def1,new-name=sys.udf
/show-guard-attributes

     Guard name          Scope   Type      Creation Date       LastMod Date
------------------------------------------------------------------------------
:DEL1:$USER1.ATTR1        USR  DEFPATTR 2017-04-20/07:48:09 2017-04-20/08:04:01
                          Guard fuer die Standardschutzattribute
:DEL1:$USER1.SYS.UDF      USR  DEFAULTP 2017-04-20/07:52:36 2017-04-20/08:17:27
                          Default-Protection-Regelbehaelter
:DEL1:$USER1.WRGUA1       USR  STDAC    2017-04-20/07:48:46 2017-04-20/07:49:17
                          Guardschutz zum Schreiben
------------------------------------------------------------------------------
Guards selected: 3                                              End of display
```

USER1 lässt sich den Inhalt des jetzt aktiven Regelbehälters anzeigen:

```
/show-default-protection-rule rule-container-guard=sys.udf

------------------------------------------------------------------------------
RULE CONTAINER :DEL1:$USER1.SYS.UDF             USR ACTIVE  DEFAULT PROTECTION
------------------------------------------------------------------------------
RULE1          OBJECT     = FILE*
               ATTRIBUTES = $USER1.ATTR1
               USER-IDS   = *ANY-USER-ID
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                    END OF DISPLAY
```

Anschließend überprüft USER1 noch einmal, welche Schutzattribute die Datei FILE1 beim Anlegen erhalten würde:

```
/show-object-protection-default object-name=file1
/                               information=*attribute-values

------------------------------------------------------------------------------
DEFAULTS FOR FILE  :DEL1:$USER1.FILE1
------------------------------------------------------------------------------
                  % SCOPE: CREATE-OBJECT        % SCOPE: MODIFY-OBJECT-ATTR
                  % --------------------------- % -------------------------
ACCESS            % *SYSTEM-STD                 % *SYSTEM-STD
USER-ACCESS       % *SYSTEM-STD                 % *SYSTEM-STD
BASIC-ACL         % *SYSTEM-STD                 % *SYSTEM-STD
GUARDS            % READ   =                    % READ   =
                  % WRITE  = $USER1.WRGUA1      % WRITE  = $USER1.WRGUA1
                  % EXEC   =                    % EXEC   =
READ-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
WRITE-PASSWORD    % *SYSTEM-STD                 % *SYSTEM-STD
EXEC-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
DESTROY-BY-DELETE % *SYSTEM-STD                 % *SYSTEM-STD
SPACE-RELEASE-LOCK % *SYSTEM-STD                % *SYSTEM-STD
EXPIRATION-DATE   % *SYSTEM-STD                 % *SYSTEM-STD
FREE-FOR-DELETION % *SYSTEM-STD                 % *SYSTEM-STD
------------------------------------------------------------------------------
                                                                END OF DISPLAY
```

Der gewünschte Standardschutz ist aktiv. USER1 legt die Datei FILE1 an

```
/create-file file1
/show-file-attributes file1,security=*yes

00000003 :DEL1:$USER1.FILE1
  ------------------------------ SECURITY     --------------------------------
  READ-PASS  = NONE        WRITE-PASS = NONE        EXEC-PASS  = NONE
  USER-ACC   = OWNER-ONLY  ACCESS     = WRITE       ACL        = NO
  AUDIT      = NONE        FREE-DEL-D = *NONE       EXPIR-DATE = NONE
  DESTROY    = NO          FREE-DEL-T = *NONE       EXPIR-TIME = NONE
  SP-REL-LOCK= NO
  GUARD-READ = NONE
  GUARD-WRIT = $USER1.WRGUA1
  GUARD-EXEC = NONE
:DEL1: PUBLIC:      1 FILE RES=         3  FREE=        3  REL=        3 PAGES
```

Wie die Ausgabe des Kommandos /SHOW-FILE-ATTRIBUTES zeigt, wurde das Schutzattribut für GUARD-WRIT aus dem Attributguard ATTR1 übernommen.

Anschließend möchte USER1 eine Datei FILE2 erzeugen. Auch dieser Name entspricht dem Muster in der Standardschutzregel:

```
/show-object-protection-default object-name=file2
/                               information=*attribute-values

------------------------------------------------------------------------------
DEFAULTS FOR FILE  :DEL1:$USER1.FILE2
------------------------------------------------------------------------------
                  % SCOPE: CREATE-OBJECT        % SCOPE: MODIFY-OBJECT-ATTR
                  % --------------------------- % -------------------------
ACCESS            % *SYSTEM-STD                 % *SYSTEM-STD
USER-ACCESS       % *SYSTEM-STD                 % *SYSTEM-STD
BASIC-ACL         % *SYSTEM-STD                 % *SYSTEM-STD
GUARDS            % READ   =                    % READ   =
                  % WRITE  = $USER1.WRGUA1      % WRITE  = $USER1.WRGUA1
                  % EXEC   =                    % EXEC   =
READ-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
WRITE-PASSWORD    % *SYSTEM-STD                 % *SYSTEM-STD
EXEC-PASSWORD     % *SYSTEM-STD                 % *SYSTEM-STD
DESTROY-BY-DELETE % *SYSTEM-STD                 % *SYSTEM-STD
SPACE-RELEASE-LOCK % *SYSTEM-STD                % *SYSTEM-STD
EXPIRATION-DATE   % *SYSTEM-STD                 % *SYSTEM-STD
FREE-FOR-DELETION % *SYSTEM-STD                 % *SYSTEM-STD
------------------------------------------------------------------------------
                                                                END OF DISPLAY
```

USER1 möchte diese Datei jedoch mit den herkömmlichen Standardschutz-Attributen einrichten:

```
/create-file file2, protection=*parameters(protection-attr=*std)
/show-file-att file2,security=*yes

00000003 :DEL1:$USER1.FILE2
  ------------------------------ SECURITY     --------------------------------
  READ-PASS  = NONE        WRITE-PASS = NONE        EXEC-PASS  = NONE
  USER-ACC   = OWNER-ONLY  ACCESS     = WRITE       ACL        = NO
  AUDIT      = NONE        FREE-DEL-D = *NONE       EXPIR-DATE = NONE
  DESTROY    = NO          FREE-DEL-T = *NONE       EXPIR-TIME = NONE
  SP-REL-LOCK= NO
:DEL1: PUBLIC:      1 FILE RES=         3  FREE=        3  REL=        3 PAGES
```

Alle Schutzattribute haben Systemstandard.

Beispiel 7: Festlegen von Miteigentümern

Aufgabenstellung

USER1 möchte, dass USER2 das Recht hat, unter seiner Kennung (USER1) Dateien anzulegen und zu verwalten, wenn deren Name die Zeichenfolge 'TEST' enthält.

Lösung

USER1 definiert ein Bedingungsguard COND1, das USER2 zeitlich unbegrenzten Zugriff gewährt:

```
/create-guard cond1,user-inf='Zugriffsbedingungen fuer Coowner'
/add-access-conditions guard-name=cond1, -
/                      subjects=*user(user-identification=user2)
```

Dann definiert USER1 einen Regelbehälter COO1 mit einer Miteigentümerregel. Diese gibt an, dass die Zugriffsbedingungen für Miteigentümer der Dateien, deren Name dem Muster '*TEST*' entspricht, im Bedingungsguard COND1 festgelegt sind:

```
/create-guard coo1,user-inf='Coowner-Regelbehaelter'
/add-coowner-protection-rule rule-container-guard=coo1, -
/            protection-rule=rule1, -
/            protect-object=*parameters(name=*test*,-
/                                       condition-guard=cond1)
```

Zur Kontolle gibt USER1 Informationen über alle Guards und den Regelbehälter COO1 aus. Voraussetzung: Zu Beginn dieser Beispielsitzung waren keine Guards unter der Kennung USER1 vorhanden.

```
/show-guard-attributes

     Guard name          Scope   Type      Creation Date       LastMod Date
-------------------------------------------------------------------------------
:DEL1:$USER1.COND1        USR  STDAC    2017-04-19/10:35:47 2017-04-19/10:36:33
                          Zugriffsbedingungen fuer Coowner
:DEL1:$USER1.COO1         USR  COOWNERP 2017-04-19/10:37:26 2017-04-19/10:38:53
                          Coowner-Regelbehaelter
-------------------------------------------------------------------------------
Guards selected: 2                                                End of display
```

```
/show-coowner-protection-rule coo1

-------------------------------------------------------------------------------
RULE CONTAINER :DEL1:$USER1.COO1                          COOWNER PROTECTION
-------------------------------------------------------------------------------
RULE1         OBJECT      = *TEST*
              CONDITIONS  = $USER1.COND1
              TSOS-ACCESS = SYSTEM-STD
-------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                    END OF DISPLAY
```

Da der Name des Regelbehälters nicht den Namenskonventionen für aktive Regelbehälter entspricht, dient er nur zur Vorbereitung der Standardschutzregel. USER2 hat noch keine Miteigentümerberechtigung für Dateien unter der Kennung USER1, wie der Aufruf des folgenden Kommandos unter der Kennung USER2 zeigt:

```
/show-coowner-admission-rule $user1.*
COO3316 NO COOWNER PROTECTION ACTIVE
```

Um den Miteigentümerschutz zu aktivieren, benennt USER1 den inaktiven Regelbehälter COO1 um:

```
/mod-guard-attr guard-name=coo1,new-name=sys.ucf
/show-guard-attributes

     Guard name          Scope   Type      Creation Date       LastMod Date
------------------------------------------------------------------------------
:DEL1:$USER1.COND1        USR  STDAC    2017-04-19/10:35:47 2017-04-19/10:36:33
                          Zugriffsbedingungen fuer Coowner
:DEL1:$USER1.SYS.UCF      USR  COOWNERP 2017-04-19/10:37:26 2017-04-19/11:29:53
                          Coowner-Regelbehaelter
------------------------------------------------------------------------------
Guards selected: 2                                                End of display
```

USER1 lässt sich den Inhalt des jetzt aktiven Regelbehälters anzeigen:

```
/show-coowner-protection-rule

------------------------------------------------------------------------------
RULE CONTAINER :DEL1:$USER1.SYS.UCF                 ACTIVE COOWNER PROTECTION
------------------------------------------------------------------------------
RULE1         OBJECT      = *TEST*
              CONDITIONS  = $USER1.COND1
              TSOS-ACCESS = SYSTEM-STD
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                        END OF DISPLAY
```

USER2 überprüft, welche Regeln ihn zum Miteigentümer von Dateien der Kennung USER1 machen:

```
/show-coowner-admission-rule $user1.*

------------------------------------------------------------------------------
COOWNER RULES FOR FILE  :DEL1:$USER1.*
------------------------------------------------------------------------------
RULE1          OBJECT     = *TEST*
               CONDITIONS = $USER1.COND1
------------------------------------------------------------------------------
RULES SELECTED: 1                                                 END OF DISPLAY
```

Jetzt kann USER2 die Datei TESTTEST unter $USER1 anlegen:

```
/create-file $user1.testtest
/show-file-att $user1.testtest

0000003 :DEL1:$USER1.TESTTEST
:DEL1: PUBLIC:    1 FILE    RES=    3  FREE=    3  REL=    3 PAGES
```

5.12 GUARDS-Makros

In diesem Kapitel werden alle GUARDS-Makros in alphabetischer Reihenfolge aufgeführt. Die Beschreibung der Makros ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion des Makros erklärt, dann folgt das Makroformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Im Anschluss an die Operandenbeschreibung werden die Returncodes erklärt. Der Beschreibung der GUARDS-Makros folgen Anwendungsbeispiele zu den Makros MODSAC, REMSAC und SHWSAC und die Makro-Syntax der GUARDS-Makros.

Funktionelle Übersicht

Die Makros für GUARDS teilen sich in folgende Gruppen auf:

Makros der GUARDS-Verwaltung

COPGUAD	Guard kopieren
CREGUAD	Guard einrichten
DELGUAD	Guard löschen
MODGUAD	Guard-Attribute ändern
SHWGUAD	Guard-Attribute anzeigen

Makros der Standardbedingungsverwaltung

MODSAC	Zugriffsbedingungen hinzufügen (ACTION=*ADD) oder ändern (ACTION=*MODIFY)
REMSAC	Zugriffsbedingungen entfernen
SHWSAC	Zugriffserlaubnis (VIEW=*ADMISSIONS) oder Zugriffsbedingungen anzeigen VIEW=*CONDITIONS
CHKSAC	Zugriffsbedingungen auswerten
MSGGUAD	Meldungen und Return-Codes ausgeben
SACMGMT	Globale Konstanten definieren

Makros der Standardschutzverwaltung

ADDDEF	Standardschutzregel hinzufügen
MODDEF	Standardschutzregel ändern
REMDEF	Standardschutzregel entfernen
SHWDEF	Standardschutzregel anzeigen
SHWOBJ	Standardschutzattribute für Objekt anzeigen

Makros der Standardschutz-Attributverwaltung

ADDATTR	Standardwerte für Schutzattribute festlegen
MODATTR	Standardwerte für Schutzattribute ändern
SHWATTR	Standardwerte für Schutzattribute anzeigen

Makros der Standardschutz-Objektpfadverwaltung (nur für die Systemverwaltung)

ADDUID	Kennungen für Objektpfad hinzufügen
REMUID	Kennungen für Objektpfad entfernen
SHWUID	Kennungen für Objektpfad anzeigen

Makros der Miteigentümerschutzverwaltung

ADDCOO	Miteigentümerschutzregel hinzufügen
MODCOO	Miteigentümerschutzregel ändern
REMCOO	Miteigentümerschutzregel entfernen
SHWCOO	Miteigentümerschutzregel anzeigen
SHWACOO	Miteigentümerberechtigungsregel anzeigen

ADDATTR
Standardwerte für Schutzattribute festlegen

Mit dieser Funktion werden Schutzattribut-Standardwerte in ein Attributguard eingetragen. Gibt es das Attributguard noch nicht, wird es implizit angelegt, wobei es den Guardtyp DEFPATTR erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt.

Gibt es das Attributguard bereits, weil es mit dem Kommando /CREATE-GUARD oder dem Makro CREGUA angelegt wurde, bleibt der SCOPE unverändert.

Die Funktion kann nur auf ein nicht vorhandenes oder leeres Attributguard angewendet werden. Im anderen Fall wird sie abgewiesen. Die Modifikation von Attributen in einem Attributguard muss mit der Funktion MODATTR durchgeführt werden.

Ein Anwender kann nur Attributguards für seine eigene Benutzerkennung einrichten. Ein Guard-Administrator darf Attributguards unter fremden Benutzerkennungen einrichten.

Generell gelten die spezifizierten Schutzattributwerte sowohl für den Attributbereich *CREATE-OBJECT als auch für *MODIFY-OBJECT-ATTR. Folgende Abweichungen sind dabei zu beachten:

ACCESS
: Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Bereich *CREATE-OBJECT wird der entsprechende Wert auf *SYSSTD gesetzt. Damit wird verhindert, dass ein neu eingerichtetes Objekt standardmäßig mit dem Attribut ACCESS=READ versehen wird, bevor es überhaupt mit Daten versehen werden konnte. Sollte dieses Verhalten jedoch explizit vom Anwender gewünscht sein, muss der Attributwert explizit mit dem Kommando /MODIFY-DEFAULT-PROTECTION-ATTR modifiziert werden.

EXPIRATION-DATE
: Da das Schutzattribut beim Neuanlegen eines Objektes nicht wirkt, wird der spezifizierte Wert nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSSTD gesetzt.

FREE-FOR-DELETION
: Der spezifizierte Wert wird nur in den Attributbereich *MODIFY-OBJECT-ATTR eingetragen. Im Attributbereich *CREATE-OBJECT wird der Wert auf *SYSSTD gesetzt. So soll verhindert werden, dass durch den Standardwert für FREE-FOR-DELETION ein Kennwortschutz unterlaufen wird, den eine bestehende Anwendung für Dateien vorsieht, die sie neu anlegt.

*Bedeutung des Operandenwertes *SYSSTD*

Der Wert *SYSSTD steht stellvertretend für einen in der hierarchisch höheren Instanz vorgegebenen Attributwert.

Die hierarchisch höhere Instanz ist
– der pubsetglobale Regelbehälter,
  wenn ein Attributguard aus einem benutzerspezifischen Regelbehälter heraus ausgewertet wird
– die herkömmliche Systemvoreinstellung,
  wenn ein Attributguard aus einem pubsetglobalen Regelbehälter heraus ausgewertet wird oder wenn es keinen pubsetglobalen Regelbehälter gibt.

Die folgende Tabelle zeigt, wie die spezifizierten Werte den beiden Attributbereichen zugeordnet werden:

Attribut	**Attributbereich**	
	***CREATE-OBJECT**	***MOD-OBJECT-ATTR**
ACCESS	*SYSTEM-STD	spezifizierter Wert
USER-ACCESS	spezifizierter Wert	spezifizierter Wert
BASIC-ACL	spezifizierter Wert	spezifizierter Wert
GUARDS	spezifizierter Wert	spezifizierter Wert
WRITE-PASSWORD	spezifizierter Wert	spezifizierter Wert
READ-PASSWORD	spezifizierter Wert	spezifizierter Wert
EXEC-PASSWORD	spezifizierter Wert	spezifizierter Wert
DESTROY-BY-DELETE	spezifizierter Wert	spezifizierter Wert
SPACE-RELEASE-LOCK	spezifizierter Wert	spezifizierter Wert
EXPIRATION-DATE	*SYSTEM-STD	spezifizierter Wert
FREE-FOR-DELETION	*SYSTEM-STD	spezifizierter Wert

Anmerkung

Der Attributbereich *MOD-OBJECT-ATTR ist nur für Dateien relevant, da die Objektverwaltung für Jobvariablen (JVS) bei der Modifikation von JV-Attributen keinen Standardschutz unterstützt.

Makro	Operanden	
ADDATTR	MF =	C / D / L / M / E
	,PREFIX =	D / <name 1>
	,MACID =	EFJ / <name 3>
	,PARAM =	<name 1..8>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,ATTRGUA	’␣’ / <c-string 1..24: filename 1..24 without-gen-vers> / <var: char:24> /
	,ACCESS =	*SYSSTD / *READ / *WRITE / <var: enum-of _access_s:1>
	,SHARE =	*SYSSTD / *OWNER / *ALL / *SPECIAL / <var: enum-of _user_access_s:1>
	,DESTROY =	*SYSSTD / *NO / *YES / <var: enum-of _destroy_s:1>
	,SPRLOCK =	*SYSSTD / *NO / *YES / <var: enum-of _relspace_lock_s:1>
	,DELDATE =	structure(3): (1) valtype: *SYSSTD / *NONE / *DATEABS / *DATEREL / <var: enum-of _free_for_deletion_s:1> (2) dateabs: ’␣’ / <c-string 8..10> / <var: char:10> (3) daterel: 0 / <integer 0..99999> / <var: int:4>
	,EXDATE =	structure(3): (1) valtype: *SYSSTD / *TODAY / *TOMORROW / *DATEABS / *DATEREL / <var: enum-of _expiration_date_s:1> (2) dateabs: ’␣’ / <c-string 8..10> / <var: char:10> (3) daterel: 0 / <integer 0..99999> / <var: int:4>
	,WRPASS=	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _write_pwd_s:1> (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>

(Teil 1 von 2)

Makro	Operanden	
ADDATTR	,RDPASS=	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _read_pwd_s:1> / (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>
	,EXPASS	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _exec_pwd_s:1> (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>
	,BASACL =	structure(10): (1) valtype: *SYSSTD / *NONE / *BASVAL / <var: enum-of _basic_acl_s:1> (2) ownerr: *NO / *YES / <var: bit:1> (3) ownerw: *NO / *YES / <var: bit:1> (4) ownerx: *NO / *YES / <var: bit:1> (5) groupr: *NO / *YES / <var: bit:1> (6) groupw: *NO / *YES / <var: bit:1> (7) groupx: *NO / *YES / <var: bit:1> (8) otherr: *NO / *YES / <var: bit:1> (9) otherw: *NO / *YES / <var: bit:1> (10) otherx: *NO / *YES / <var: bit:1>
	,GUARDS =	structure(4): (1) valtype: *SYSSTD / *NONE / *GUAVAL / <var: enum-of _guards_s:1> (2) readgua:'␣' / <c-string 1..18> / <var: char:18> (3) writgua:'␣' / <c-string 1..18> / <var: char:18> (4) execgua:'␣' / <c-string 1..18> / <var: char:18>

(Teil 2 von 2)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

ATTRGUA Name des Attributguards

Dieser Operand bezeichnet den Namen des Attributguards vom Typ DEFPATTR, in dem Standardwerte für Schutzattribute spezifiziert werden. Das Guard wird neu eingerichtet, sofern es noch nicht erzeugt worden ist.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

ACCESS Zugriffsart

Gibt an, welche Art von Zugriff auf das Objekt erlaubt ist.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

=*READ Es sind nur lesende und ausführende Objektzugriffe erlaubt.

Der spezifizierte Wert gilt nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Bereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSTEM-STD. Damit wird verhindert, dass neu einzurichtende Objekte standardmäßig mit einem Schreibschutz versehen werden, bevor sie erstmalig mit Daten versehen wurden. Ist dieses Verhalten jedoch explizit vom Anwender gewünscht, muss der Attributwert explizit mit der Funktion MODATTR modifiziert werden.

=*WRITE Lesende, schreibende und ausführende Objektzugriffe sind erlaubt.

Der spezifizierte Wert gilt nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Bereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSSTD.

SHARE Mehrbenutzbarkeit

Gibt an, ob fremde Benutzerkennungen auf das Objekt zugreifen dürfen.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

=*OWNER Der Zugriff auf das Objekt ist nur unter der eigenen Benutzerkennung möglich, aber unter jeder Katalogkennung, unter der die (namentlich) gleiche Benutzerkennung eingerichtet ist (d.h. nicht nur unter der Katalogkennung, unter der das Objekt eingerichtet wurde). Miteigentümer haben ebenfalls Zugriff.

=*ALL Der Zugriff auf das Objekt ist auch unter fremden Benutzerkennungen möglich.

=*SPECIAL

Das Objekt ist für alle Benutzerkennungen einschließlich der Kennungen mit dem Privileg HARDWARE-MAINTENANCE zugänglich. Zugriffe der Wartungskennung sind generell nur möglich, wenn SHARE=*SPECIAL gilt.

DESTROY Durchlöschen nicht mehr benötigter Daten (nur für Dateien)

Zur Erhöhung des Datenschutzes kann der Benutzer im Katalogeintrag festlegen, dass nicht mehr benötigte Daten mit X'00' (binär Null) überschrieben werden.

Bei Plattendateien wirkt sich das auf Löschoperationen und Speicherplatzfreigabe aus (siehe Kommando /MODIFY-FILE-ATTRIBUTES und /DELETE-FILE).

Bei Banddateien wirkt sich das auf das Überschreiben von Restdaten bei EOF-\und\EOV-Verarbeitung aus (siehe Operand DESTROY-OLD-CONTENTS im Kommando /ADD-FILE-LINK).

=*SYSSTD

Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

=*YES Diese Einstellung wirkt auch, wenn im Kommando /DELETE-FILE, Operand OPTION eine andere Vereinbarung getroffen wird.

Bei Plattendateien wird freigegebener Speicherplatz automatisch mit binär Null (X'00') überschrieben.

Bei Banddateien wird der Bandinhalt nach dem Dateiende mit binär Null (X'00') überschrieben. Im Kommando /ADD-FILE-LINK muss das Löschen der Restdaten für den aktuellen Verarbeitungslauf nicht explizit angegeben werden.

=*NO Bei dieser Einstellung wirkt eine im Kommando /DELETE-FILE getroffene Vereinbarung (Operand OPTION).

Bei Plattendateien wird der Speicherplatz unverändert freigegeben, wenn nicht im Kommando /DELETE-FILE der Operand OPTION=DESTROY-ALL angegeben wird.

Bei Banddateien werden die auf dem Band folgenden Restdaten nicht überschrieben, wenn im Kommando /ADD-FILE-LINK für den aktuellen Verarbeitungslauf nicht DESTROY-OLD-CONTENTS=*YES vereinbart wird.

SPRLOCK Speicherplatzfreigabe (nur für Dateien)

Gibt an, ob die Freigabe von Speicherplatz mit dem Kommando /MODIFY-FILE-ATTRIBUTES bzw. FILE-Makro ignoriert werden soll.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

=*NO Speicherplatz kann freigegeben werden.

=*YES Speicherplatz kann nicht freigegeben werden.

DELDATE Freigabedatum

Legt fest, ab wann das Objekt ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE
Löschen nur unter Berücksichtigung der Schutzattribute möglich.

*DATEABS
Absolute Datumsangabe in Form einer Zeichenkette, ab wann ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

*DATEREL
Relative Datumsangabe in Form einer Integerzahl, ab wann ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

dateabs: Datum

Die Schutzfrist wird in Form eines absoluten Datums angegeben. Das Objekt kann ab dem angegebenen Datum ohne Berücksichtigung der Schutzattribute gelöscht werden.

daterel: Anzahl von Tagen

Die Schutzfrist wird in Form eines relativen Datums angegeben. Das Objekt kann nach der angegebenen Anzahl von Tagen ohne Berücksichtigung der Schutzattribute gelöscht werden.

EXDATE Schutzfrist (nur für Dateien)

Bis zu dem angegebenen Datum kann die Datei nicht verändert oder gelöscht werden. Eine Schutzfrist kann nur vergeben werden, wenn die Datei bereits eröffnet wurde, das heißt, ein CREATION-DATE besitzt. Da das Schutzattribut beim Anlegen einer Datei nicht wirkt, gilt der spezifizierte Wert auch nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Attributbereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSSTD

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*TODAY
Es wird keine Schutzfrist vergeben bzw. eine bestehende Schutzfrist wird aufgehoben, indem sie auf das aktuelle Tagesdatum gesetzt wird.

*TOMORROW

Als Schutzfrist wird das Datum des nächsten Tages vergeben.

*DATEABS

Absolute Datumsangabe in Form einer Zeichenkette

*DATEREL

Relative Datumsangabe in Form einer Integerzahl

dateabs: Datum

Die Schutzfrist wird in Form eines absoluten Datums angegeben. Das Objekt bleibt bis zum angegebenen Datum (ausschließlich) geschützt.

daterel: Anzahl von Tagen

Die Schutzfrist wird in Form eines relativen Datums angegeben. Die Datei bleibt für die angegebene Anzahl von Tagen geschützt.

WRPASS Schreibkennwort

Kennwort zum Schutz vor unberechtigtem Schreiben.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE
Es wird kein Schreibkennwort vergeben.

*VALCODE
Es ist ein Schreibkennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

RDPASS Lesekennwort

Kennwort zum Schutz vor unberechtigtem Lesen.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE

Es wird kein Lesekennwort vergeben.

*VALCODE

Es ist ein Lesekennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

EXPASS Ausführkennwort

Kennwort zum Schutz vor unberechtigtem Ausführen.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE
Es wird kein Ausführkennwort vergeben.

*VALCODE
Es ist ein Ausführkennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

BASACL BASIC-ACL-Schutz

Aktiviert den Zugriffsschutz über BASIC-ACL.

valtype: Indikator

Der Indikator zeigt an, wie der BASIC-ACL-Schutz spezifiziert ist.

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE
Es wird kein BASIC-ACL-Schutz verwendet.

*BASVAL
Es wird ein BASIC-ACL-Schutz aktiviert.

ownerr: Leseberechtigung für den Eigentümer.

*NO Eigentümer hat keine Leseberechtigung.

*YES Eigentümer hat Leseberechtigung.

ownerw: Schreibberechtigung für den Eigentümer.

*NO Eigentümer hat keine Schreibberechtigung.

*YES Eigentümer hat Schreibberechtigung.

ownerx: Ausführberechtigung für den Eigentümer.

*NO Eigentümer hat keine Ausführberechtigung.

*YES Eigentümer hat Ausführberechtigung.

groupr: Leseberechtigung für Gruppenmitglieder.

*NO Gruppenmitglieder haben keine Leseberechtigung.

*YES Gruppenmitglieder haben Leseberechtigung.

groupw: Schreibberechtigung für Gruppenmitglieder.

*NO Gruppenmitglieder haben keine Schreibberechtigung.

*YES Gruppenmitglieder haben Schreibberechtigung.

groupx: Ausführberechtigung für Gruppenmitglieder.

*NO Gruppenmitglieder haben keine Ausführberechtigung.

*YES Gruppenmitglieder haben Ausführberechtigung.

otherr: Leseberechtigung für alle anderen.

*NO Alle anderen haben keine Leseberechtigung.

*YES Alle anderen haben Leseberechtigung.

otherw: Schreibberechtigung für alle anderen.

*NO Alle anderen haben keine Schreibberechtigung.

*YES Alle anderen haben Schreibberechtigung.

otherx: Ausführberechtigung für alle anderen.

*NO Alle anderen haben keine Ausführberechtigung.

*YES Alle anderen haben Ausführberechtigung.

GUARDS Guards-Schutz

Aktiviert den Zugriffsschutz über GUARDS.

valtype: Indikator

Der Indikator zeigt an, wie der GUARDS-Schutz spezifiziert ist.

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 707).

*NONE
Es wird kein GUARDS-Schutz verwendet.

*GUAVAL
Es wird ein GUARDS-Schutz verwendet.

readgua: Leseguard

Name des Guards für den Leseschutz.

writgua: Schreibguard

Name des Guards für den Schreibschutz.

execgua: Ausführguard

Name des Guards für den Ausführschutz.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X’00’	X’00’	X’0000’	class A: CMD0001
X’00’ X’01’ X’02’ X’03’ X’04’ X’05’ X’06’ X’07’ X’08’ X’09’ X’0A’ X’0B’ X’0C’ X’0D’ X’0E’ X’0F’ X’10’	X’01’	X’3100’	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: ATTRGUA ungültiger Operand: ACCESS ungültiger Operand: SHARE ungültiger Operand: DESTROY ungültiger Operand: SPRLOCK ungültiger Operand: DELDATE ungültiger Operand: EXDATE ungültiger Operand: WRPASS ungültiger Operand: RDPASS ungültiger Operand: EXPASS ungültiger Operand: BASACL ungültiger Operand: GUARDS ungültiger Operand: READGUA ungültiger Operand: WRITGUA ungültiger Operand: EXECGUA ungültiger Wert im reservierten Feld
X’00’	X’20’	X’3200’	class C: DEF3200
X’00’	X’40’	X’3302’	class D: DEF3302
X’00’	X’40’	X’3306’	class D: DEF3306
X’00’	X’40’	X’3308’	class D: DEF3308
X’00’	X’40’	X’3309’	class D: DEF3309
X’00’	X’40’	X’3313’	class D: DEF3313
X’00’	X’40’	X’3314’	class D: DEF3314
X’00’	X’40’	X’3315’	class D: DEF3315
X’00’	X’40’	X’3350’	class D: DEF3350
X’00’	X’80’	X’3900’	class E: DEF3900
X’00’	X’80’	X’3901’	class E: DEF3901
X’00’	X’80’	X’3902’	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

ADDCOO
Miteigentümerschutzregel hinzufügen

Mit dieser Funktion wird eine Miteigentümerschutzregel in einen Regelbehälter (Guard) eingetragen. Handelt es sich dabei um den ersten Regeleintrag, wird der Regelbehälter neu angelegt, wobei im Guard-Verwaltungsteil der SCOPE auf *USER-ID gesetzt wird.

Gibt es den Regelbehälter bereits, bleibt der SCOPE unverändert und die Regel wird an die angegebene Position im Regelbehälter eingefügt.

Ein Anwender kann nur Regelbehälter unter seiner eigenen Benutzerkennung einrichten. Ein Guard-Administrator kann Regelbehälter unter fremden Benutzerkennungen einrichten.

Makro	**Operanden**	
ADDCOO	MF =	C / D / L / M / E
	,PREFIX =	C / <name 1>
	,MACID =	OOA / <name 3>
	,PARAM =	<name 1..8>
	,DIALOG =	*STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,COGUARD =	’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,RULENAM =	’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,RULEPOS =	structure(2): (1) target: *LAST / *BEFORE / <var: enum-of _target_s:1> (2) posnam: ’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,OBJECT =	structure(2): (1) objnam: ’␣’ / <c-string 1..80: filename 1..41 without-cat-gen-user-vers with-wild(80)> / <var: char:80> (2) objtype: *FILE / <var: enum-of _object_type_s:1>
	,CONDGUA =	*NONE / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,TSOSACC =	*SYSSTD / *RESTRICTED / <var: enum-of _tsos_access_s:1>
	,GUACHK =	*YES / *NO / <var: enum-of _guard_check_s:1>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD

Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, in den eine erste oder weitere Regeln eingetragen werden. Der Behälter wird neu eingerichtet sofern es ihn noch nicht gibt.

Der Behältername kann zwar beliebig gewählt werden, für die Miteigentümerzugriffskontrolle wird jedoch ausnahmslos Regelbehälter mit fest vorgeschriebenen Namen verwendet.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel in mehrere Behälter eingetragen wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu bearbeitenden Regel. Doppelte Namen in einem Behälter sind nicht erlaubt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULEPOS Position

Dieser Operand bezeichnet die Position innerhalb eines Regelbehälter, an die die zu bearbeitende Regel gestellt wird. Die Reihenfolge der Regeln ist ausschlaggebend bei der Zugriffsüberprüfung der Miteigentümer.

target Angabe zur Zielposition im Regelbehälter.

*LAST Die Regel wird an die letzte Position im Regelbehälter gestellt.

*BEFORE
Die Regel wird vor die durch den Operand RULENAM benannte Regel gestellt .

posnam Name der Regel zur Positionsangabe

Dieser Operand bezeichnet eine im Regelbehälter eingetragene Regel, vor die die zu bearbeitende Regel gestellt wird, wenn die Angabe target des Operanden RULEPOS den Wert *BEFORE hat. Die Funktion wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden, wenn die Teilangabe target des Operanden RULEPOS den Wert *BEFORE hat. Es dürfen nur Großbuchstaben verwendet werden!

OBJECT Objekt

Dieser Operand bezeichnet das Objekt, für das die zu bearbeitende Regel gilt.

objnam Objektname

Angaben über den Namen des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

objtype Typ des Objektnamens entsprechend der SDF-Syntaxbeschreibung (siehe Handbuch „Kommandos“ [4]).

Angaben über den SDF-Namenstyp des Objektes. Zur Zeit wird nur der SDF-Namenstyp <filename> (*FILE) unterstützt, der sowohl für Dateinamen als auch für Jobvariablennamen gibt.

*FILE Der Objektname hat den SDF-Datentyp <filename>.

CONDGUA Zugriffsbedingungen

Dieser Operand bezeichnet den Namen eines Guards vom Typ STDAC, das die Zugriffsbedingungen enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*NONE Es werden keine Zugriffsbedingungen festgelegt. Der Miteigentümerschutz ist für das Objekt außer Kraft gesetzt, und ein Miteigentümerzugriff wird abgelehnt.

TSOSACC Angabe über die Miteigentümerschaft der Benutzerkennung TSOS.

= *SYSSTD
Die Benutzerkennung TSOS erhält die uneingeschränkte Miteigentümerschaft für das Objekt.

= *RESTRICTED
Die Benutzerkennung TSOS erhält eine eingeschränkte Miteigentümerschaft für das Objekt.

GUACHK Guardprüfung

Bei der Funktionsdurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

=*YES Die Guardprüfung wird eingeschaltet. Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt das Guard nicht, oder ist der Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht berechtigt, das Guard zu verwenden, bricht die Funktion mit einem entsprechenden Returncode ab.

Es ist zu beachten, dass die Prüfung nur eine „Momentaufnahme“ sein kann, die unmittelbar nach Funktionsdurchführung von anderen Tasks durch entsprechende Guardmodifikationen verändert sein kann.

=*NO Die Guardprüfung wird ausgeschaltet.

Die Funktion wird durchgeführt, unabhängig davon, dass ein genanntes Guard nicht verfügbar ist oder vom Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht verwendet werden darf.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: COO3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3003'	class A: COO3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X'00' X'01' X'02' X'03' X'04' X'05' X'06' X'07' X'08' X'09' X'0A' X'0B'	X'01'	X'3100'	class B: COO3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM Operand RULEPOS: ungültige Teilangabe target Operand RULEPOS: ungültige Teilangabe posnam Operand OBJECT: ungültige Teilangabe objnam Operand OBJECT: ungültige Teilangabe objtype ungültiger Operand: CONDGUA ungültiger Guardtyp des Bedingungsguards ungültiger Operand: GUACHK ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: COO3200
X'00'	X'40'	X'3300'	class D: COO3300
X'00'	X'40'	X'3302'	class D: COO3302
X'00'	X'40'	X'3303'	class D: COO3303
X'00'	X'40'	X'3304'	class D: COO3304
X'00'	X'40'	X'3305'	class D: COO3305
X'00'	X'40'	X'3306'	class D: COO3306
X'00'	X'40'	X'3307'	class D: COO3307
X'00'	X'40'	X'3308'	class D: COO3308
X'00'	X'40'	X'3309'	class D: COO3309
X'00'	X'40'	X'3311'	class D: COO3311
X'00'	X'40'	X'3313'	class D: COO3313

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3314'	class D: COO3314
X'00'	X'40'	X'3315'	class D: COO3315
X'00'	X'80'	X'3900'	class E: COO3900
X'00'	X'80'	X'3901'	class E: COO3901
X'00'	X'80'	X'3902'	class E: COO3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG COO3902`.

ADDDEF
Standardschutzregel hinzufügen

Mit dieser Funktion wird eine Regel für die Standardwertvergabe für Datei- oder Jobvariablen-Schutzattributen in einen Regelbehälter (Guard) eingetragen. Handelt es sich dabei um den ersten Regeleintrag, wird der Regelbehälter neu angelegt, wobei im Guard-Verwaltungsteil der SCOPE auf *USER-ID gesetzt wird.

Gibt es den Regelbehälter bereits, bleibt der SCOPE unverändert und die Regel wird an die angegebene Position im Regelbehälter eingefügt.

Ein Anwender kann nur Regelbehälter unter seiner eigenen Benutzerkennung einrichten. Ein Guard-Administrator kann Regelbehälter unter fremden Benutzerkennungen einrichten.

Ein Regelbehälter für den pubsetglobalen Standardschutz kann nur von TSOS oder von einem Guard-Administrator eingerichtet werden, er muss unter der Benutzerkennung TSOS abgelegt sein

.

Makro	**Operanden**	
ADDDEF	MF =	C / D / L / M / E
	,PREFIX =	D / <name 1>
	,MACID =	EFA / <name 3>
	,PARAM =	<name 1..8>
	,DIALOG =	*STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,COGUARD =	’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,RULENAM =	’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,RULEPOS =	structure(2): (1) target: *LAST / *BEFORE / <var: enum-of _target_s:1> (2) posnam: ’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,OBJECT =	structure(2): (1) objnam: ’␣’ / *TEMP / <c-string 1..80: filename 1..41 without-cat-gen-user-vers with-wild(80)> / <var: char:80> (2) objtype: *FILE / <var: enum-of _object_type_s:1>
	,ATTRGUA =	*NONE / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,UIDGUA =	*ANYUID / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,GUACHK =	*YES / *NO / <var: enum-of _guard_check_s:1>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD

Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, in den eine erste oder weitere Regeln eingetragen werden. Der Behälter wird neu eingerichtet, falls er noch nicht existiert.

Der Behältername kann zwar beliebig gewählt werden, für die Suche nach passenden Standardwerten werden jedoch in Hierarchie ausnahmslos Regelbehälter mit fest vorgeschriebenen Namen verwendet.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel in mehrere Behälter eingetragen wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu bearbeitenden Regel. Doppelte Namen in einem Behälter sind nicht erlaubt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULEPOS Position

Dieser Operand bezeichnet die Position innerhalb eines Regelbehälter, an die die zu bearbeitende Regel gestellt wird. Die Reihenfolge der Regeln ist ausschlaggebend bei der Ermittlung der Schutzattribut-Standardwerte.

target Angabe zur Zielposition im Regelbehälter.

*LAST
Die Regel wird an die letzte Position im Regelbehälter gestellt.

*BEFORE
Die Regel wird vor die durch den Operand RULENAM benannte Regel gestellt.

posnam Name der Regel zur Positionsangabe

Dieser Operand bezeichnet eine im Regelbehälter eingetragene Regel, vor die die zu bearbeitende Regel gestellt wird, wenn die Angabe target des Operanden RULEPOS den Wert *BEFORE hat. Die Funktion wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden, wenn die Teilangabe target des Operanden RULEPOS den Wert *BEFORE hat. Es dürfen nur Großbuchstaben verwendet werden!

OBJECT Objekt

Dieser Operand bezeichnet das Objekt, für das die zu bearbeitende Regel gilt.

objnam Objektname

Angaben über den Namen des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

*TEMP Die Regel gilt für alle temporären Objekte.

objtype Typ des Objektnamens entsprechend der SDF-Syntaxbeschreibung (siehe Handbuch „Kommandos“ [4]).

Angaben über den SDF-Namenstyp des Objektes. Zur Zeit wird nur der SDF-Namenstyp <filename> (*FILE) unterstützt, der sowohl für Dateinamen als auch für Jobvariablennamen gibt.

ATTRGUA Attribute

Dieser Operand bezeichnet den Namen eines Guards vom Typ STDAC, das die Attribute enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*NONE Es werden keine Attribute in dieser Regel festgelegt. Die Attributstandardwerte werden bei der Standardwertvergabe aus der nächst höheren Hierarchiestufe (pubsetglobal oder herkömmlicher Systemstandard) ermittelt.

UIDGUA Benutzerkennungen

Name des Guards vom Typ DEFPUID, das die Benutzerkennungen für die Pfadvervollständigung beim pubsetglobalen Standardschutz enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Dieser Operand darf nur von TSOS oder von einem Guard-Administrator angegeben werden. Es dürfen nur Großbuchstaben verwendet werden!

=*ANYUID

Es wird kein Guard für Benutzerkennungen angegeben. Der Name des Objektes gilt für alle Benutzerkennungen eines Pubsets.

GUACHK Guardprüfung

Bei der Funktionsdurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

=*YES Die Guardprüfung wird eingeschaltet. Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt das Guard nicht, oder ist der Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht berechtigt, das Guard zu verwenden, bricht die Funktion mit einem entsprechenden Returncode ab.

Es ist zu beachten, dass die Prüfung nur eine „Momentaufnahme“ sein kann, die unmittelbar nach Funktionsdurchführung von anderen Tasks durch entsprechende Guardmodifikationen verändert sein kann.

=*NO Die Guardprüfung wird ausgeschaltet.

Die Funktion wird durchgeführt, unabhängig davon, dass ein genanntes Guard nicht verfügbar ist oder vom Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht verwendet werden darf.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3003'	class A: DEF3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X'00' X'01' X'02' X'03' X'04' X'05' X'06' X'07' X'08' X'09' X'0A' X'0B' X'0C' X'0D'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM Operand RULEPOS: ungültige Teilangabe target Operand RULEPOS: ungültige Teilangabe posnam Operand OBJECT: ungültige Teilangabe objnam Operand OBJECT: ungültige Teilangabe objtype ungültiger Operand: ATTRGUA ungültiger Guardtyp des Attributguards ungültiger Operand: ATTRGUA ungültiger Guardtyp des Useridguards ungültiger Operand: GUACHK ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3300'	class D: DEF3300
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3303'	class D: DEF3303
X'00'	X'40'	X'3304'	class D: DEF3304
X'00'	X'40'	X'3305'	class D: DEF3305
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3307'	class D: DEF3307
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3313'	class D: DEF3313
X'00	X'40	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3318'	class D: DEF3318
X'00	X'40	X'3319'	class D: DEF3319
X'00'	X'40'	X'3320'	class D: DEF3320
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

ADDUID
Kennungen für Objektpfad hinzufügen

Mit dieser Funktion kann ein Benutzer der Kennung TSOS oder ein Guard-Administrator Benutzer- und Gruppenkennungen in ein Benutzerkennungsguard eintragen, die bei der Festlegung von Standardschutzregeln die Objektnamen pubsetweit genauer qualifizieren.

Gibt es das Benutzerkennungsguard noch nicht, wird es implizit angelegt, wobei es den Guardtyp DEFPUID erhält. Im Guard-Verwaltungsteil wird der SCOPE auf *USER-ID gesetzt. Gibt es das Benutzerkennungsguard bereits, bleibt der SCOPE unverändert.

Es können beliebig viele Benutzer- und Gruppenkennungen eingetragen werden. Ist der Bedingungsbereich voll, sind keine weiteren Eintragungen möglich.

Makro	**Operanden**	
ADDUID	MF = ,PREFIX = ,MACID = ,PARAM = ,DIALOG = ,ERRMSG = ,UIDGUA = ,IDTYPES = ,IDS =	C / D / L / M / E D / <name 1> EFB / <name 3> <name 1..8> *STD / *NO / *UIDGUA / *USERID / *CATALOG / <var: enum-of _dialog_s:1> *NO / *YES / <var: bit:1> ’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40> array(20): *UID / *GRP / <var: enum-of _type_s:1> array(20): ’␣’ / <c-string 1..20: name 1..8 with-wild(20)> / *UNIVERS / <var: char:20>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*NO Die Funktion wird ohne Rückfrage auf jedes Benutzerkennungsguard angewendet.

=*UIDGUA

Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Der Anwender kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*STD Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine angegebene Benutzerkennung bereits eingetragen ist und die Funktion aus diesem Grund auf das Guard nicht angewendet wird.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

UIDGUA Name des Benutzerkennungsguards

Dieser Operand bezeichnet den Namen des Benutzerkennungsguards vom Typ DEFPUID, in das Kennungen eingetragen werden.

Musterzeichen im Namen des Benutzerkennungsguards bewirken, dass die Benutzer- und Gruppenkennungen in mehrere Guards eingetragen wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

IDTYPES Typliste

Über diesen Operanden können in Form eines Arrays die Typen der Kennungen angegeben werden, die über den Operanden IDS spezifiziert werden.

*UID Es handelt sich um eine Benutzerkennung.

*GRP Es handelt sich um eine Gruppenkennung.

IDS Liste der Kennungen

Über diesen Operanden können in Form eines Arrays die Kennungen (ohne $) angegeben werden, deren Typ über den Operanden TYPE spezifiziert werden muss. Die Kennungen dürfen Musterzeichen enthalten.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

*UNIVERS

Benutzergruppe *UNIVERSAL

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3012'	class A: DEF3012 Warnung: Bei Wildcardverarbeitung konnten nicht alle Benutzerkennungsguards korrekt bearbeitet werden
X'00' X'01' X'02' X'03' X'04' X'05'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: UIDGUA ungültiger Operand: IDTYPES ungültiger Operand: IDS ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3303'	class D: DEF3303
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3400'	class D: DEF3400
X'00'	X'40'	X'3402'	class D: DEF3402
X'00'	X'40'	X'3403'	class D: DEF3403
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

CHKSAC
Zugriffsbedingungen auswerten

Mit diesem Makro wird GUARDS aus einem Programm heraus aufgerufen, um eine Bedingungsauswertung durchzuführen. Das Programm wird damit zu einer Objektverwaltung. GUARDS kann dann zum Schutz der Objekte des Programms eingesetzt werden.

Makro	Operanden	
CHKSAC	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROV / <name 3>
	,PARAM =	<name 1..8>
	,GUARD =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,OBJOWN =	*OWN / <c-string: name 1..8> / <var: char(8)> / (<reg: A(char(8))>)
	,ACCTSN =	*OWN / <c-string: name 1..4> / <var: char(4)> / (<reg: A(char(4))>)
	,ACCUID =	*OWN / <c-string: name 1..8> / <var: char(8)> / (<reg: A(char(8))>)
*	,EVAL =	*ACCESS / *SHOW / <var: enum EVAL> / (<reg: enum EVAL>)
	,TIME =	*NO / *YES
	,DATE =	*NO / *YES
	,WEEKDAY =	*NO / *YES
	,PRIV =	*NO / *YES
	,PROG =	*NO / *YES

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Operanden, die mit „*“ gekennzeichnet sind, sind Pflichtoperanden bei MF=L.

GUARD — Name des Guards, mit dem die Bedingung geprüft wird. Der Name darf nur aus Großbuchstaben bestehen.

OBJOWN — Eigentümer des Objekts, das durch das Guard geschützt ist. Mit *OWN ist die eigene Benutzerkennung voreingestellt.

Die beiden folgenden Operanden ACCTSN und ACCUID können nur alternativ angegeben werden.

ACCTSN TSN der Task, die den Zugriff durchführt. Mit *OWN ist die eigene TSN voreingestellt.

ACCUID Benutzerkennung, für die eine Zugriffsüberprüfung durchgeführt wird. Die Kennung muss existieren. Diese Angabe ist nur aus Programmen erlaubt, die unter einer Task mit TSOS-Privileg laufen. Mit *OWN ist die eigene Benutzerkennung voreingestellt.

EVAL Legt fest, wie überprüft wird. Dieser Operand ist bei MF=L Pflichtoperand.

=*ACCESS
Es wird überprüft, ob ein Zugriff auf das durch GUARDS zu schützende Objekt zugelassen ist.

=*SHOW Es wird überprüft, ob der Benutzer das Guard sehen darf. Zu schützende Objekte sind hiervon unberührt. Es wird überprüft, ob der Zugriff immer oder nur unter bestimmten Umständen erlaubt ist.
*SHOW führt dazu, dass die folgenden Parameter dieses Makros nicht ausgewertet werden.

TIME Festlegung, ob eine Zeitbedingung ignoriert wird:

=*NO Zeitbedingung nicht ignorieren

=*YES Zeitbedingung ignorieren

DATE Festlegung, ob eine Datumsbedingung ignoriert wird:

=*NO Datumsbedingung nicht ignorieren

=*YES Datumsbedingung ignorieren

WEEKDAY Festlegung, ob eine Wochentagsbedingung ignoriert wird:

=*NO Wochentagsbedingung nicht ignorieren

=*YES Wochentagsbedingung ignorieren

PRIV Festlegung, ob eine Privilegsbedingung ignoriert wird:

=*NO Privilegsbedingung nicht ignorieren

=*YES Privilegsbedingung ignorieren

PROG Festlegung, ob eine Programmbedingung ignoriert wird:

=*NO Programmbedingung nicht ignorieren

=*YES Programmbedingung ignorieren

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X’01’	X’1000’	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X’20’	X’1001’	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X’40’	X’1002’	Der Guard-Name ist syntaktisch falsch
	X’40’	X’1003’	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X’40’	X’1007’	Das angegebene Guard existiert nicht
	X’40’	X’1012’	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X’40’	X’1013’	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X’40’	X’1014’	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X’40’	X’1019’	Zugreifende Benutzerkennung unbekannt
	X’40’	X’1020’	Kein Speicher mehr vorhanden
	X’40’	X’1024’	Nutzung des Guards nicht zugelassen

Beispiel

Dieses Beispiel zeigt, wie ein Programmteil mit GUARDS geschützt werden kann.

Im Programm sind Teile enthalten, die nur bestimmten Programmbenutzern zugänglich sein sollen. Im Programm muss hinterlegt werden, welche Programmteile durch welche Guards geschützt werden sollen.

Für den Schutz der Programmteile müssen die entsprechenden Guards erstellt werden, um dann vor der Ausführung des Programmteils durch den CHKSAC-Aufruf geprüft werden zu können.

So wird ermittelt, ob die im Guard definierten Bedingungen für den Benutzer erfüllt sind oder nicht.

Beispiel für den Schutz eines Programmteils mit Hilfe von GUARDS über den Makro CHKSAC

```
BSPL     CSECT
R10      EQU   10
         BALR  R10,0
         USING *,R10
*        ************************************************
*                                                       *
*        DER PARAMETERBEREICH WIRD VOR JEDEM MF=E-AUFRUF  *
*        WIEDER MIT DEM ANFANGSINHALT VERSORGT:          *
*                                                       *
         MVC   PARAMFC(PROV#),PARAMFL
*                                                       *
*        UND FALLS ERFORDERLICH GEAENDERT:               *
*                                                       *
         CHKSAC MF=M,GUARD=GUARDNAM
*                                                       *
*        ************************************************
*                                                       *
*        AUSFUEHRUNG DES MACRO:
*                                                       *
         CHKSAC MF=E,PARAM=PARAMFC
*                                                       *
*        ************************************************
*                                                       *
*        ABFRAGE DES RETURNCODES:                        *
*                                                       *
         CLC   PROVMRET,=Y(PRMTSUCC)
         BNE   RCNOTOK
*                                                       *
*        ************************************************
*                                                       *
*        ABFRAGE DES ERGEBNISSES:                        *
*                                                       *
         CLI   PROVCHKR,PROVCYES
         BNE   BSPLNO
*                                                       *
*        ************************************************
*        DIESER TEIL DES PROGRAMS IST GESCHUETZT UND WIRD  *
*        NUR DANN AUSGEFUEHRT, WENN ES DURCH DAS GUARD     *
*        MYGUARD ERLAUBT WIRD                            *
*                                                       *
         MVC   TEXT,OKTEXT
         B     ENDE
*                                                       *
*        ************************************************
BSPLNO   EQU   *
```

```
*        WENN GUARD MYGUARD DIE AUSFUEHRUNG DES GESCHUETZTEN
*        PROGRAMTEILS NICHT ERLAUBT, WIRD DIESER TEIL      *
*        DURCHGEFUEHRT                                     *
*                                                          *
         B     ENDE
*                                                          *
*        ******************************************************
*                                                          *
RCNOTOK  EQU   *
*        FEHLERBEHANDLUNG DES FEHLERHAFTEN RETURNCODE      *
*        WIE SOLL FORTGESETZT WERDEN, HAENGT VON DER       *
*        AUFGABE AB.                                       *
*        FALLS WEITERGEMACHT WERDEN SOLL                   *
*        (DAS KANN Z.B. BEI 1007 SINNVOLL SEIN),           *
*        SO SOLLTE DER GESCHUETZTE PROGRAMTEIL NICHT       *
*        DURCHLAUFEN WERDEN                                *
         MVC   TEXT,RCTEXT
         B     ENDE
*                                                          *
*        ******************************************************
*                                                          *
ENDE     EQU   *
         WROUT MELDUNG,WRFEHL
WRFEHL   EQU   *
         TERM
*                                                          *
*        ******************************************************
*                                                          *
*        DER PARAMETERBEREICH (BEIM MACROAUFRUF IST        *
*        DIE ADRESSE PARAMFC IM REGISTER 1 :               *
PARAMFC  DS    OF
         CHKSAC MF=C
*                                                          *
*        ******************************************************
*                                                          *
*        DER BEREICH PARAMFL BLEIBT UNVERAENDERT WAEHREND  *
*        DES GANZEN PROGRAMLAUFS (IM NORMALFALL) UND WIRD  *
*        VOR JEDEM MF=E-AUFRUF DES MACROS IN DEN PARAMETER-*
*        BEREICH (PARAMFC) UEBERTRAGEN (S. MVC OBEN)       *
*                                                          *
PARAMFL  DS    OF
         CHKSAC EVAL=*ACCESS,MF=L
*                                                          *
*        ******************************************************
*                                                          *
*        DER WERT EINES ZU MODIFIZIERENDEN PARAMETERS:     *
*                                                          *
GUARDNAM DC    CL24'MYGUARD'
```

```
*                                                               *
*       ***************************************************     *
*                                                               *
MELDUNG  DC    Y(MELDENDE-MELDUNG)
         DS    CL2
         DC    X'01'
TEXT     DC   'ZUGRIFFSBEDINGUNGEN IN MYGUARD: ZUGRIFF NICHT GESTATTET'
MELDENDE EQU   *
OKTEXT   DC    'ZUGRIFFSBEDINGUNGEN IN MYGUARD: ZUGRIFF GESTATTET'
RCTEXT   DC    '.....  RETURN CODE UNGLEICH 0000   .....             '
*                                                               *
*       ***************************************************     *
*                                                               *
*       DIE NAMEN (EQUATES) FUER RETURN CODE WERTE  SIND  *
*       IN DER FOLGENDEN DSECT VORHANDEN                        *
*                                                               *
         MSGGUAD MF=D
*                                                               *
*       FALLS NOETIG KOENNEN DIE NAMEN IM PARAMETERBEREICH
*       ALS DSECT GENERIERT WERDEN, JEDOCH WEGEN DER      *
*       GLEICHZEITIGEN BENUTZUNG VON MF=C, MUESSEN DIE    *
*       NAMEN EINEN ANDEREN PREFIX HABEN                  *
*                                                               *
         CHKSAC MF=D,PREFIX=X
*                                                               *
*       ***************************************************     *
         END
```

Prozedur zum Aufruf des Beispielprogramms

```
/PROC A,(&BIBL),SUBDTA=
/REMARK DAS BEISPIELPROGRAM BSPL IST IN DER BIBLIOTHEK BIBL
/DELETE-GUARD MYGUARD
/STEP
/ADD-ACCESS-CONDITION MYGUARD,SUBJECT=USER(($SYSJV.USERID)), ADM=NO
/START-PROGRAM *P(&BIBL.,BSPL)
/REMARK FOLGENDER TEXT WURDE VOM BSPL AUSGEGEBEN:
/REMARK ZUGRIFFSBEDINGUNGEN IN MYGUARD: ZUGRIFF NICHT GESTATTET
/MOD-ACCESS-CONDITION MYGUARD,SUBJECT=USER( ($SYSJV.USERID)),ADM=YES ?
/START-PROGRAM *P(&BIBL.,BSPL)
/REMARK FOLGENDER TEXT WURDE VOM BSPL AUSGEGEBEN:
/REMARK ZUGRIFFSBEDINGUNGEN IN MYGUARD: ZUGRIFF GESTATTET
/ENDP
```

COPGUAD
Guard kopieren

Dieser Makro kopiert ein Guard.

Der Eigentümer darf seine eigenen Guards kopieren. Benutzer mit dem Privileg GUARD-ADMINISTRATION dürfen fremde Guards in ihre oder unter andere Kennungen kopieren. Andere Benutzer dürfen ein fremdes Guard nur kopieren, wenn das SCOPE-Attribut (CREGUAD oder MODGUAD) dies gestattet.

RFA kann nur verwendet werden, wenn beide Guards (Quell- und Ziel-Guard) auf dem gleichen Rechner lokal zugreifbar sind.

Makro	**Operanden**	
COPGUAD	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROO / <name 3>
	,PARAM =	<name 1..8>
	,FRNAME =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,TONAME =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,REPLACE =	*NO / *YES / *DIALOG / <var: enum REPLACE> / (<reg: enum REPLACE>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

FRNAME vollqualifizierter Name des Guards, das kopiert wird. Es dürfen nur Großbuchstaben verwendet werden.

TONAME vollqualifizierter neuer Name des Guards. Es dürfen nur Großbuchstaben verwendet werden.

Es darf nur in die eigene Benutzerkennung kopiert werden.Ein Benutzer mit dem Privileg GUARD-ADMINISTRATION darf in jede Kennung kopieren, da er Eigentümer aller Kennungen ist).

REPLACE regelt, ob ein existierendes Guard überschrieben werden darf oder nicht.

=*NO wenn das Ziel-Guard bereits existiert, wird es nicht überschrieben.

=*YES es wird überschrieben, falls ein Guard gleichen Namens bereits existiert.

=*DIALOG Diese Angabe ist nur im Dialogbetrieb wirksam. Im Batchbetrieb gilt die Einstellung *NO. Sofern ein Ziel-Guard bereits existiert, wird ein Dialog begonnen, in dem der Aufrufer festlegen kann, ob das Guard überschrieben werden soll.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1006'	Das angegebene Guard existiert bereits
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1014'	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1024'	Nutzung des Guards nicht zugelassen
	X'40'	X'1025'	Kopieren vom/zum fernen System nicht möglich
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
	X'80'	X'1036'	Guardskatalog gesperrt

CREGUAD
Guard einrichten

Mit diesem Makro wird ein Guard angelegt und mit Attributen versehen. Nicht-privilegierte Benutzer können Guards nur für die eigene Kennung anlegen. Der Guard-Administrator kann auch Guards für andere Kennungen anlegen.

Makro	Operanden	
CREGUAD	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROK / <name 3>
	,PARAM =	<name 1..8>
	,NAME =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,COMMENT =	<c-string: text 1..80> / <var: char(80)> / (<reg: A(char(80))>)
	,SCOPE =	*USERID / *USER_GROUP / *HOST_SYSTEM / <var: enum SCOPE> / (<reg: enum SCOPE>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

NAME vollqualifizierter Name des Guards, das erzeugt wird. Es dürfen nur Großbuchstaben verwendet werden. Der Name soll nicht mit der Zeichenfolge „SYS“ beginnen. Dieser Namensraum ist für Guards reserviert, die von der BS2000-Entwicklung festgelegt werden.

COMMENT Text, der als Kommentar für dieses Guard hinterlegt wird.

SCOPE Legt fest, wer dieses Guard für den Schutz seiner Objekte verwenden darf:

=*USERID Nur der Eigentümer darf das Guard verwenden oder der Objekteigentümer mit dem Privileg TSOS.

=*USER_GROUP
Der Eigentümer und die Benutzergruppe, der der Eigentümer angehört, dürfen das Guard verwenden.

=*HOST_SYSTEM
Das Guard darf von allen verwendet werden.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X’01’	X’1000’	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X’20’	X’1001’	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X’40’	X’1002’	Der Guard-Name ist syntaktisch falsch
	X’40’	X’1003’	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X’40’	X’1006’	Das angegebene Guard existiert bereits
	X’40’	X’1012’	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X’40’	X’1013’	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X’40’	X’1014’	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X’40’	X’1016’	Fehler im Kommunikationsmittel des MRS
	X’40’	X’1017’	Unbekannte Benutzerkennung
	X’40’	X’1018’	Fernes System nicht verfügbar
	X’40’	X’1020’	Kein Speicher mehr vorhanden
	X’40’	X’1021’	BCAM-Verbindungsfehler
	X’40’	X’1022’	BCAM-Verbindung unterbrochen
	X’40’	X’1029’	GUARDS auf dem fernen Rechner nicht verfügbar
	X’80’	X’1036’	Guardskatalog gesperrt

DELGUAD
Guard löschen

Mit diesem Makro werden Guards gelöscht. Nicht-privilegierte Benutzer können nur Guards der eigenen Kennung löschen. Der Guard-Administrator kann auch Guards anderer Kennungen löschen.

Makro	Operanden	
DELGUAD	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROM / <name 3>
	,PARAM =	<name 1..8>
	,NAME =	<c-string: filename 1..40 without-gen-vers with-wild> / <c-string: partial-filename 2..40 with-wild> / <var: char(40)> / (<reg: A(char(40))>)
	,DIALOG =	*STD / *NO / *GUARD / *USERID / *CATALOG / <var: enum DIALOG> / (<reg: enum DIALOG>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

NAME Name des Guards, das gelöscht wird. Der Name darf Musterzeichen enthalten. Er darf aber nur aus Großbuchstaben bestehen.

DIALOG legt die Art der Dialogführung fest.

=*STD Es gelten folgende Einstellungen:

Im Batchbetrieb: *NO

Im Dialogbetrieb: *GUARD, wenn NAME Musterzeichen enthält

*NO, wenn NAME keine Musterzeichen enthält

=*NO Die Funktion wird ohne Rückfrage auf die passenden Guards ausgeführt

=*GUARD Der Aufrufer kann für jedes Guard mit *NO / *YES entscheiden, ob die Funktion ausgeführt wird. Die Antwort TERMINATE beendet die Kommandoausführung, auch wenn noch nicht alle passenden Guards behandelt wurden.

=*USERID Diese Angabe ist nur für Guard-Administratoren zugelassen. Wenn die Benutzerkennung Musterzeichen enthält, wird bei einem Wechsel der Kennung gefragt, ob die Funktion auf die genannte Kennung auch angewandt wird. Die Antwortmöglichkeiten entsprechen *GUARD.

=*CATALOG

Wenn die Katalogkennung Musterzeichen enthält, wird bei einem Wechsel des Katalogs gefragt, ob die Funktion auf den genannten Katalog auch angewandt wird. Die Antwortmöglichkeiten entsprechen *GUARD.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
X'02'	CMD	X'1011'	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1014'	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1023'	Kein Guard entspricht den Auswahlkriterien
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
	X'80'	X'1036'	Guardskatalog gesperrt

MODATTR
Standardwerte für Schutzattribute ändern

Mit dieser Funktion können Schutzattribut-Standardwerte in einem Attributguard geändert werden.

Ein Anwender kann nur Attributguards seiner eigenen Benutzerkennung ändern. Ein Guard-Administrator darf Attributguards fremder Benutzerkennungen ändern.

Die Attributmodifikationen werden bei einem Aufruf des Makros immer nur für einen der Attributbereiche *CREATE-OBJECT oder *MODIFY-OBJECT-ATTR durchgeführt.

*Bedeutung des Operandenwertes *SYSSTD*

Der Wert *SYSSTD steht stellvertretend für einen in der hierarchisch höheren Instanz vorgegebenen Attributwert.

Die hierarchisch höhere Instanz ist
– der pubsetglobale Regelbehälter,
  wenn ein Attributguard aus einem benutzerspezifischen Regelbehälter heraus ausgewertet wird
– die herkömmliche Systemvoreinstellung,
  wenn ein Attributguard aus einem pubsetglobalen Regelbehälter heraus ausgewertet wird oder wenn es keinen pubsetglobalen Regelbehälter gibt.

Makro	Operanden	
MODATTR	MF =	C / D / L / M / E
	,PREFIX =	D / <name 1>
	,MACID =	EFK / <name 3>
	,PARAM =	<name 1..8>
	,DIALOG =	*STD / *NO / *ATTRGUA / *USERID / *CATALOG / <var: enum-of _dialog_s:1>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,ATTRGUA =	’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,ATTRSCP =	*CRE / *MOD / <var: enum-of _attr_scope_s:1>
	,ACCESS =	*SYSSTD / *READ / *WRITE / <var: enum-of _access_s:1>
	,SHARE =	*SYSSTD / *OWNER / *ALL / *SPECIAL / <var: enum-of _user_access_s:1>
	,DESTROY =	*SYSSTD / *NO / *YES / <var: enum-of _destroy_s:1>
	,SPRLOCK =	*SYSSTD / *NO / *YES / <var: enum-of _relspace_lock_s:1>
	,DELDATE =	structure(3): (1) valtype: *SYSSTD / *NONE / *DATEABS / *DATEREL / <var: enum-of _free_for_deletion_s:1> (2) dateabs: ’␣’ / <c-string 8..10> / <var: char:10> (3) daterel: 0 / <integer 0..99999> / <var: int:4>
	,EXDATE =	structure(3): (1) valtype: *SYSSTD / *TODAY / *TOMORROW / *DATEABS / *DATEREL / <var: enum-of _expiration_date_s:1> (2) dateabs: ’␣’ / <c-string 8..10> / <var: char:10> (3) daterel: 0 / <integer 0..99999> / <var: int:4>
	,WRPASS=	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _write_pwd_s:1> (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>

(Teil 1 von 2)

Makro	Operanden	
MODATTR	,RDPASS=	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _read_pwd_s:1> / default: _read_pwd_s.system_std (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>
	,EXPASS	structure(2): (1) valtype: *SYSSTD / *NONE / *VALCODE / <var: enum-of _exec_pwd_s:1> (2) code: 0 / <integer -2147483648..2147483647> / <var: int:4>
	,BASACL =	structure(10): (1) valtype: *SYSSTD / *NONE / *BASVAL / <var: enum-of _basic_acl_s:1> (2) ownerr: *NO / *YES / <var: bit:1> (3) ownerw: *NO / *YES / <var: bit:1> (4) ownerx: *NO / *YES / <var: bit:1> (5) groupr: *NO / *YES / <var: bit:1> (6) groupw: *NO / *YES / <var: bit:1> (7) groupx: *NO / *YES / <var: bit:1> (8) otherr: *NO / *YES / <var: bit:1> (9) otherw: *NO / *YES / <var: bit:1> (10) otherx: *NO / *YES / <var: bit:1>
	,GUARDS =	structure(4): (1) valtype: *SYSSTD / *NONE / *GUAVAL / <var: enum-of _guards_s:1> (2) readgua: ’␣’ / <c-string 1..18> / <var: char:18> (3) writgua: ’␣’ / <c-string 1..18> / <var: char:18> (4) execgua :’␣’ / <c-string 1..18> / <var: char:18>

(Teil 2 von 2)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*NO Die Funktion wird ohne Rückfrage auf jedes Attributguard angewendet.

=*ATTRGUA
Der Anwender kann für jedes ausgewählte Attributguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Attributguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Der Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*STD Der Anwender kann für jedes ausgewählte Attributguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Attributguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel ein Attributguard nicht vorhanden ist und die Bearbeitung beim nächsten Attributguard fortsetzt.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

ATTRGUA Name des Attributguards

Dieser Operand bezeichnet den Namen des Attributguards vom Typ DEFPATTR, in dem Standardwerte für Schutzattribute modifiziert werden.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

ATTRSCP Attributbereich

Gibt an, ob die spezifizierten Attribute beim Erzeugen eines Objektes als Standardwerte verwendet werden, oder beim Modifizieren eines bestehenden Objektes.

*CRE Die spezifizierten Attribute werden beim Erzeugen eines Objektes als Standardwerte verwendet.

*MOD Die spezifizierten Attribute werden beim Modifizieren eines Objektes als Standardwerte verwendet.

ACCESS Zugriffsart

Gibt an, welche Art von Zugriff auf das Objekt erlaubt ist.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

=*READ Es sind nur lesende Objektzugriffe erlaubt.

Der spezifizierte Wert gilt nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Bereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSTEM-STD. Damit wird verhindert, dass neu einzurichtende Objekte standardmäßig mit einem Schreibschutz versehen werden, bevor sie erstmalig mit Daten versehen wurden. Ist dieses Verhalten jedoch explizit vom Anwender gewünscht, muss der Attributwert explizit mit der Funktion MODATTR modifiziert werden.

=*WRITE Lesende, schreibende und ausführende Objektzugriffe sind erlaubt.

Der spezifizierte Wert gilt nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Bereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSSTD.

SHARE Mehrbenutzbarkeit

Gibt an, ob fremde Benutzerkennungen auf das Objekt zugreifen dürfen.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

=*OWNER Der Zugriff auf das Objekt ist nur unter der eigenen Benutzerkennung möglich, aber unter jeder Katalogkennung, unter der die (namentlich) gleiche Benutzerkennung eingerichtet ist (d.h. nicht nur unter der Katalogkennung, unter der das Objekt eingerichtet wurde). Miteigentümer haben ebenfalls Zugriff.

=*ALL Der Zugriff auf das Objekt ist auch unter fremden Benutzerkennungen möglich.

=*SPECIAL
Das Objekt ist für alle Benutzerkennungen einschließlich der Kennungen mit dem Privileg HARDWARE-MAINTENANCE zugänglich. Zugriffe der Wartungskennung sind generell nur möglich, wenn SHARE=*SPECIAL gilt.

DESTROY Durchlöschen nicht mehr benötigter Daten (nur für Dateien)

Zur Erhöhung des Datenschutzes kann der Benutzer im Katalogeintrag festlegen, dass nicht mehr benötigte Daten mit X’00’ (binär Null) überschrieben werden.

Bei Plattendateien wirkt sich das auf Löschoperationen und Speicherplatzfreigabe aus (siehe Kommando /MODIFY-FILE-ATTRIBUTES und /DELETE-FILE).

Bei Banddateien wirkt sich das auf das Überschreiben von Restdaten bei EOF-\und\EOV-Verarbeitung aus (siehe Operand DESTROY-OLD-CONTENTS im Kommando /ADD-FILE-LINK).

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

=*YES Diese Einstellung wirkt auch, wenn im Kommando /DELETE-FILE, Operand OPTION eine andere Vereinbarung getroffen wird.

Bei Plattendateien wird freigegebener Speicherplatz automatisch mit binär Null (X’00’) überschrieben.

Bei Banddateien wird der Bandinhalt nach dem Dateiende mit binär Null (X'00') überschrieben. Im Kommando /ADD-FILE-LINK muss das Löschen der Restdaten für den aktuellen Verarbeitungslauf nicht explizit angegeben werden.

=*NO Bei dieser Einstellung wirkt eine im Kommando /DELETE-FILE getroffene Vereinbarung (Operand OPTION).

Bei Plattendateien wird der Speicherplatz unverändert freigegeben, wenn nicht im Kommando /DELETE-FILE der Operand OPTION=DESTROY-ALL angegeben wird.

Bei Banddateien werden die auf dem Band folgenden Restdaten nicht überschrieben, wenn im Kommando /ADD-FILE-LINK für den aktuellen Verarbeitungslauf nicht DESTROY-OLD-CONTENTS=*YES vereinbart wird.

SPRLOCK Speicherplatzfreigabe (nur für Dateien)

Gibt an, ob die Freigabe von Speicherplatz mit dem Kommando /MODIFY-FILE-ATTRIBUTES bzw. FILE-Makro ignoriert wird.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

=*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

=*NO Speicherplatz kann freigegeben werden.

=*YES Speicherplatz kann nicht freigegeben werden.

DELDATE Freigabedatum

Legt fest, ab wann das Objekt ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Löschen nur unter Berücksichtigung der Schutzattribute möglich.

*DATEABS
Absolute Datumsangabe in Form einer Zeichenkette, ab wann ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

*DATEREL
Relative Datumsangabe in Form einer Integerzahl, ab wann ohne Berücksichtigung der Schutzattribute gelöscht werden darf.

dateabs: Datum

Die Schutzfrist wird in Form eines absoluten Datums angegeben. Das Objekt kann ab dem angegebenen Datum ohne Berücksichtigung der Schutzattribute gelöscht werden.

daterel: Anzahl von Tagen

Die Schutzfrist wird in Form eines relativen Datums angegeben. Das Objekt kann nach der angegebenen Anzahl von Tagen ohne Berücksichtigung der Schutzattribute gelöscht werden.

EXDATE Schutzfrist (nur für Dateien)

Bis zu dem angegebenen Datum kann die Datei nicht verändert oder gelöscht werden. Eine Schutzfrist kann nur vergeben werden, wenn die Datei bereits eröffnet wurde, das heißt, ein CREATION-DATE besitzt. Da das Schutzattribut beim Anlegen einer Datei nicht wirkt, gilt der spezifizierte Wert auch nur für den Attributbereich *MODIFY-OBJECT-ATTR. Für den Attributbereich *CREATE-OBJECT gilt grundsätzlich die Voreinstellung *SYSTEM-STD.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*TODAY
Es wird keine Schutzfrist vergeben werden bzw. eine bestehende Schutzfrist wird aufgehoben, indem sie auf das aktuelle Tagesdatum gesetzt wird.

*TOMORROW
Als Schutzfrist wird das Datum des nächsten Tages vergeben.

*DATEABS
Absolute Datumsangabe in Form einer Zeichenkette

*DATEREL
Relative Datumsangabe in Form einer Integerzahl

dateabs: Datum

Die Schutzfrist wird in Form eines absoluten Datums angegeben. Das Objekt bleibt bis zum angegebenen Datum (ausschließlich) geschützt.

daterel: Anzahl von Tagen

Die Schutzfrist wird in Form eines relativen Datums angegeben. Das Objekt bleibt für die angegebene Anzahl von Tagen geschützt bleibt.

WRPASS Schreibkennwort

Kennwort zum Schutz vor unberechtigtem Schreiben.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Es wird kein Schreibkennwort vergeben.

*VALCODE
Es ist ein Schreibkennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

RDPASS Lesekennwort

Kennwort zum Schutz vor unberechtigtem Lesen.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Es wird kein Lesekennwort vergeben.

*VALCODE
Es ist ein Lesekennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

EXPASS Ausführkennwort

Kennwort zum Schutz vor unberechtigtem Ausführen.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Spezifikationstyp

Angabe, wie der Attributwert spezifiziert ist

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Es wird kein Ausführkennwort vergeben.

*VALCODE
Es ist ein Ausführkennwort spezifiziert.

code: Kennwort

Angabe des Kennwortes in Form einer Zahl.

BASACL BASIC-ACL-Schutz

Aktiviert den Zugriffsschutz über BASIC-ACL.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Indikator

Der Indikator zeigt an, wie der BASIC-ACL-Schutz spezifiziert ist.

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Es wird kein BASIC-ACL-Schutz verwendet.

*BASVAL
Es wird ein BASIC-ACL-Schutz aktiviert.

ownerr: Leseberechtigung für den Eigentümer.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Eigentümer hat keine Leseberechtigung.

*YES Eigentümer hat Leseberechtigung.

ownerw: Schreibberechtigung für den Eigentümer.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Eigentümer hat keine Schreibberechtigung.

*YES Eigentümer hat Schreibberechtigung.

ownerx: Ausführberechtigung für den Eigentümer.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Eigentümer hat keine Ausführberechtigung.

*YES Eigentümer hat Ausführberechtigung.

groupr: Leseberechtigung für Gruppenmitglieder.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Gruppenmitglieder haben keine Leseberechtigung.

*YES Gruppenmitglieder haben Leseberechtigung.

groupw: Schreibberechtigung für Gruppenmitglieder.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Gruppenmitglieder haben keine Schreibberechtigung.

*YES Gruppenmitglieder haben Schreibberechtigung.

groupx: Ausführberechtigung für Gruppenmitglieder.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Gruppenmitglieder haben keine Ausführberechtigung.

*YES Gruppenmitglieder haben Ausführberechtigung.

otherr: Leseberechtigung für alle anderen.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Alle anderen haben keine Leseberechtigung.

*YES Alle anderen haben Leseberechtigung.

otherw: Schreibberechtigung für alle anderen.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Alle anderen haben keine Schreibberechtigung.

*YES Alle anderen haben Schreibberechtigung.

otherx: Ausführberechtigung für alle anderen.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

*NO Alle anderen haben keine Ausführberechtigung.

*YES Alle anderen haben Ausführberechtigung.

GUARDS Guards-Schutz

Aktiviert den Zugriffsschutz über GUARDS.

Wird der Operand nicht angegeben, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

valtype: Indikator

Der Indikator zeigt an, wie der GUARDS-Schutz spezifiziert ist.

*SYSSTD
Der Attributwert wird durch die hierarchisch höhere Instanz festgelegt (siehe „Bedeutung des Operandenwertes *SYSSTD“ auf Seite 750).

*NONE
Es wird kein GUARDS-Schutz verwendet.

*GUAVAL
Es wird ein GUARDS-Schutz verwendet.

readgua: Leseguard

Name des Guards für den Leseschutz.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

writgua: Schreibguard

Name des Guards für den Schreibschutz.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

execgua: Ausführguard

Name des Guards für den Ausführschutz.

Wird keine Angabe gemacht, bleibt der bisherige Wert im angegebenen Attributbereich des Attributguards unverändert.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3003'	class A: DEF3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X'00' X'01' X'02' X'03' X'04' X'05' X'06' X'07' X'08' X'09' X'0A' X'0B' X'0C' X'0D' X'0E' X'0F' X'10' X'11'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: ATTRGUA ungültiger Operand: ATTRSCP ungültiger Operand: ACCESS ungültiger Operand: SHARE ungültiger Operand: DESTROY ungültiger Operand: SPRLOCK ungültiger Operand: DELDATE ungültiger Operand: EXDATE ungültiger Operand: WRPASS ungültiger Operand: RDPASS ungültiger Operand: EXPASS ungültiger Operand: BASACL ungültiger Operand: GUARDS ungültiger Operand: READGUA ungültiger Operand: WRITGUA ungültiger Operand: EXECGUA ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3351'	class D: DEF3351
X'00'	X'40'	X'3352'	class D: DEF3352
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

MODCOO
Miteigentümerschutzregel ändern

Mit dieser Funktion wird eine Miteigentümerschutzregel in einem Regelbehälter (Guard) modifiziert.

Welcher Regelteil modifiziert oder unverändert bleiben soll, hängt davon ab, ob bei Schnittstellenaufruf der jeweilige Operand angegeben wird oder nicht. Wird der Operand nicht angegeben, bedeutet das, dass der durch den Operand repräsentierte Wert unverändert (UNCHANGED) bleibt. Wird der Operand angegeben, bedeutet das, dass der durch den Operand repräsentierte Wert für die Modifikation verwendet wird.

Ein Anwender kann nur seine eigenen Regelbehälter modifizieren. Ein Guard-Administrator kann Regelbehälter fremder Kennungen modifizieren.

Makro	Operanden	
MODCOO	MF =	C / D / L / M / E
	,PREFIX =	C / <name 1>
	,MACID =	OOM / <name 3>
	,PARAM =	<name 1..8>
	,DIALOG =	*STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,COGUARD =	’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,RULENAM =	’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,NEWNAM =	*SAME / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,RULEPOS =	structure(2): (1) target: *LAST / *BEFORE / <var: enum-of _target_s:1> (2) posnam: ’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,OBJECT =	structure(2): (1) objnam: ’␣’ / *TEMP / <c-string 1..80: filename 1..41 without-cat-gen-user-vers with-wild(80)> / <var: char:80> (2) objtype: *FILE / <var: enum-of _object_type_s:1>
	,CONDGUA =	*NONE / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,TSOSACC =	*SYSSTD / *RESTRICTED / <var: enum-of _tsos_access_s:1>
	,GUACHK =	*YES / *NO / <var: enum-of _guard_check_s:1>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD

Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, in dem eine Regel modifiziert wird.

Der Behältername kann zwar beliebig gewählt werden, für die Miteigentümerzugriffskontrolle wird jedoch ausnahmslos Regelbehälter mit fest vorgeschriebenen Namen verwendet.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel in mehreren Behältern modifiziert wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu bearbeitenden Regel.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

NEWNAM Neuer Regelname

Mit diesem Operanden kann die zu bearbeitende Regel umbenannt werden.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*SAME Der Name bleibt unverändert

RULEPOS Position

Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt wird. Die Reihenfolge der Regeln ist ausschlaggebend bei der Zugriffsüberprüfung der Miteigentümer.

target Angabe zur Zielposition im Regelbehälter.

*LAST
Die Regel wird an die letzte Position im Regelbehälter gestellt.

*BEFORE
Die Regel wird vor die durch den Operand NAME benannte Regel gestellt.

posnam Name der Regel zur Positionsangabe

Dieser Operand bezeichnet eine im Regelbehälter eingetragene Regel, vor die die zu bearbeitende Regel gestellt wird, wenn die Angabe target des Operanden RULEPOS den Wert *BEFORE hat. Die Funktion wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden, wenn die Teilangabe target des Operanden RULEPOS den Wert *BEFORE hat. Es dürfen nur Großbuchstaben verwendet werden!

OBJECT Objekt

Dieser Operand bezeichnet das Objekt, für das die zu bearbeitende Regel gilt.

objnam Objektname

Angaben über den Namen des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

objtype Typ des Objektnamens entsprechend der SDF-Syntaxbeschreibung (siehe Handbuch „Kommandos“ [4]).

Angaben über den SDF-Namenstyp des Objektes. Zur Zeit wird nur der SDF-Namenstyp <filename> (*FILE) unterstützt, der sowohl für Dateinamen als auch für Jobvariablennamen gibt.

*FILE Der Objektname hat den SDF-Datentyp <filename>.

CONDGUA Zugriffsbedingungen

Dieser Operand bezeichnet den Namen eines Guards vom Typ STDAC, das die Zugriffsbedingungen enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*NONE Es werden keine Zugriffsbedingungen festgelegt. Der Miteigentümerschutz wird für das Objekt außer Kraft gesetzt, und ein Miteigentümerzugriff wird abgelehnt.

TSOSACC Angabe über die Miteigentümerschaft der Benutzerkennung TSOS.

= *SYSSTD
Die Benutzerkennung TSOS erhält die uneingeschränkte Miteigentümerschaft für das Objekt.

= *RESTRICTED
Die Benutzerkennung TSOS erhält eine eingeschränkte Miteigentümerschaft für das Objekt.

GUACHK Guardprüfung

Bei der Funktionsdurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

=*YES Die Guardprüfung wird eingeschaltet. Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt es das Guard nicht, oder ist der Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht berechtigt, das Guard zu verwenden, bricht die Funktion mit einem entsprechenden Returncode ab.

Es ist zu beachten, dass die Prüfung nur eine „Momentaufnahme“ sein kann, die unmittelbar nach Funktionsdurchführung von anderen Tasks durch entsprechende Guardmodifikationen verändert sein kann.

=*NO Die Guardprüfung wird ausgeschaltet.

Die Funktion wird durchgeführt, unabhängig davon, dass ein genanntes Guard nicht verfügbar ist oder vom Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht verwendet werden darf.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X’00’	X’00’	X’0000’	class A: CMD0001
X’02’	X’00’	X’3000’	class A: COO3000 Warnung: Die Dialog-Kontrollabfrage wurde mit ’Terminate’ beantwortet und die Funktionsdurchführung dadurch abgebrochen
X’02’	X’00’	X’3003’	class A: COO3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden

SC2	SC1	Maincode	Erläuterung
X'00' X'01' X'02' X'03' X'04' X'05' X'06' X'07' X'08' X'09' X'0A' X'0B' X'0C'	X'01'	X'3100'	class B: COO3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Operand: NEWNAM Operand RULEPOS: ungültige Teilangabe target Operand RULEPOS: ungültige Teilangabe posnam Operand OBJECT: ungültige Teilangabe objnam Operand OBJECT: ungültige Teilangabe objtype ungültiger Operand: CONDGUA ungültiger Guardtyp des Bedingungsguards ungültiger Operand: GUACHK ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: COO3200
X'00'	X'40'	X'3300'	class D: COO3300
X'00'	X'40'	X'3302'	class D: COO3302
X'00'	X'40'	X'3303'	class D: COO3303
X'00'	X'40'	X'3304'	class D: COO3304
X'00'	X'40'	X'3305'	class D: COO3305
X'00'	X'40'	X'3306'	class D: COO3306
X'00'	X'40'	X'3307'	class D: COO3307
X'00'	X'40'	X'3308'	class D: COO3308
X'00'	X'40'	X'3309'	class D: COO3309
X'00'	X'40'	X'3310'	class D: COO3310
X'00'	X'40'	X'3311'	class D: COO3311
X'00'	X'40'	X'3313'	class D: COO3313
X'00	X'40	X'3314'	class D: COO3314
X'00'	X'40'	X'3315'	class D: COO3315
X'00'	X'80'	X'3900'	class E: COO3900
X'00'	X'80'	X'3901'	class E: COO3901
X'00'	X'80'	X'3902'	class E: COO3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG COO3902`.

MODDEF
Standardschutzregel ändern

Mit dieser Funktion wird eine Regel für die Standardwertvergabe für Datei- oder Jobvariablen-Schutzattribute in einem Regelbehälter (Guard) modifiziert.

Welcher Regelteil modifiziert oder unverändert bleiben soll, hängt davon ab, ob bei Schnittstellenaufruf der jeweilige Operand angegeben wird oder nicht. Wird der Operand nicht angegeben, bedeutet das, dass der durch den Operand repräsentierte Wert unverändert (UNCHANGED) bleibt. Wird der Operand angegeben, bedeutet das, dass der durch den Operand repräsentierte Wert für die Modifikation verwendet wird.

Ein Anwender kann nur seine eigenen Regelbehälter modifizieren. Ein Guard-Administrator kann Regelbehälter fremder Kennungen modifizieren.

Ein Regelbehälter für den pubsetglobalen Standardschutz kann nur vom Systemverwalter oder von einem Guard-Administrator modifiziert werden.

Makro	Operanden	
MODDEF	MF =	C / D / L / M / E
	,PREFIX =	D / <name 1>
	,MACID =	EFM / <name 3>
	,PARAM =	<name 1..8>
	,DIALOG =	*STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1>
	,ERRMSG =	*NO / *YES / <var: bit:1>
	,COGUARD =	’␣’ / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,RULENAM =	’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,NEWNAM =	*SAME / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,RULEPOS =	structure(2): (1) target: *LAST / *BEFORE / <var: enum-of _target_s:1> (2) posnam: ’␣’ / <c-string 1..12: alphanumeric name 1..12> / <var: char:12>
	,OBJECT =	structure(2): (1) objnam: ’␣’ / *TEMP / <c-string 1..80: filename 1..41 without-cat-gen-user-vers with-wild(80)> / <var: char:80> (2) objtype: *FILE / <var: enum-of _object_type_s:1>
	,ATTRGUA =	*NONE / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,UIDGUA =	*ANYUID / <c-string 1..18: filename 1..18 without-cat-gen-vers> / <var: char:18>
	,GUACHK =	*YES / *NO / <var: enum-of _guard_check_s:1>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD
Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Ein Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG
Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, in dem eine Regel modifiziert wird. Der Behälter wird neu eingerichtet sofern es ihn noch nicht gibt.

Der Behältername kann zwar beliebig gewählt werden, für die Suche nach passenden Standardwerten werden jedoch in Hierarchie ausnahmslos Regelbehälter mit fest vorgeschriebenen Namen verwendet.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel in mehreren Behältern modifiziert wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu bearbeitenden Regel. Doppelte Namen in einem Behälter sind nicht erlaubt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

NEWNAM Neuer Regelname

Mit diesem Operanden kann die zu bearbeitende Regel umbenannt werden.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*SAME Der Name bleibt unverändert

RULEPOS Position

Dieser Operand bezeichnet die Position innerhalb eines Regelbehälters, an die die zu bearbeitende Regel gestellt wird. Die Reihenfolge der Regeln ist ausschlaggebend bei der Ermittlung der Schutzattribut-Standardwerte.

target Angabe zur Zielposition im Regelbehälter.

*LAST
Die Regel wird an die letzte Position im Regelbehälter gestellt.

*BEFORE
Die Regel wird vor die durch den Operand RULENAM benannte Regel gestellt.

posnam Name der Regel zur Positionsangabe

Dieser Operand bezeichnet eine im Regelbehälter eingetragene Regel, vor die die zu bearbeitende Regel gestellt wird, wenn die Angabe target des Operanden RULEPOS den Wert *BEFORE hat. Die Funktion wird abgewiesen, wenn es eine Regel dieses Namens nicht gibt.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden, wenn die Teilangabe target des Operanden RULEPOS den Wert *BEFORE hat. Es dürfen nur Großbuchstaben verwendet werden!

OBJECT Objekt

Dieser Operand bezeichnet das Objekt, für das die zu bearbeitende Regel gelten wird.

objnam Objektname

Angaben über den Namen des Objektes.

Der Name kann Musterzeichen enthalten oder teilqualifiziert angegeben werden. Er darf keine Katalog- und Benutzerkennung enthalten.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

*TEMP
Die Regel gilt für alle temporären Objekte.

objtype Typ des Objektnamens entsprechend der SDF-Syntaxbeschreibung (siehe Handbuch „Kommandos“ [4]).

Angaben über den SDF-Namenstyp des Objektes. Zur Zeit wird nur der SDF-Namenstyp <filename> (*FILE) unterstützt, der sowohl für Dateinamen als auch für Jobvariablennamen gibt.

*FILE Der Objektname hat den SDF-Datentyp <filename>.

ATTRGUA Attribute

Dieser Operand bezeichnet den Namen eines Guards vom Typ STDAC, das die Attribute enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*NONE Es werden keine Attribute in dieser Regel festgelegt. Die Attributstandardwerte werden bei der Standardwertvergabe aus der nächst höheren Hierarchiestufe (pubsetglobal oder herkömmlicher Systemstandard) ermittelt werden.

UIDGUA Benutzerkennungen

Name des Guards vom Typ DEFPUID, das die Benutzerkennungen für die Pfadvervollständigung beim pubsetglobalen Standardschutz enthält. Der Name darf keine Katalogkennung enthalten. Ist das genannte Guard zum Zeitpunkt des Funktionsaufrufes nicht zugreifbar, weil es noch nicht eingerichtet ist, oder der SCOPE die Verwendung des Guards untersagt, bricht die Funktion mit Fehler ab.

ACHTUNG!
Dieser Operand darf nur von einem Systemverwalter oder von einem Guard-Administrator angegeben werden. Es dürfen nur Großbuchstaben verwendet werden!

=*ANYUID

Es wird kein Guard für Benutzerkennungen angegeben. Der Name des Objektes gilt für alle Benutzerkennungen eines Pubsets.

GUACHK Guardprüfung

Bei der Funktionsdurchführung kann wahlweise die Verfügbarkeit der in der Regel namentlich genannten Guards überprüft werden.

=*YES Die Guardprüfung wird eingeschaltet. Es wird geprüft, ob das namentlich angesprochene Guard verfügbar ist. Gibt das Guard nicht, oder ist der Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht berechtigt, das Guard zu verwenden, bricht die Funktion mit einem entsprechenden Returncode ab.

Es ist zu beachten, dass die Prüfung nur eine „Momentaufnahme“ sein kann, die unmittelbar nach Funktionsdurchführung von anderen Tasks durch entsprechende Guardmodifikationen verändert sein kann.

=*NO Die Guardprüfung wird ausgeschaltet.

Die Funktion wird durchgeführt, unabhängig davon, dass ein genanntes Guard nicht verfügbar ist oder vom Eigentümer des unter dem Operanden COGUARD angegebenen Regelbehälters nicht verwendet werden darf.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X’00’	X’00’	X’0000’	class A: CMD0001
X’02’	X’00’	X’3000’	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit ’Terminate’ beantwortet und die Funktionsdurchführung dadurch abgebrochen
X’02’	X’00’	X’3003’	class A: DEF3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X’00’ X’01’ X’02’ X’03’ X’04’ X’05’ X’06’ X’07’ X’08’ X’09’ X’0A’ X’0B’ X’0C’ X’0D’ X’0E’	X’01’	X’3100’	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Operand: NEWNAM Operand RULEPOS: ungültige Teilangabe target Operand RULEPOS: ungültige Teilangabe posnam Operand OBJECT: ungültige Teilangabe objnam Operand OBJECT: ungültige Teilangabe objtype ungültiger Operand: ATTRGUA ungültiger Guardtyp des Attributguards ungültiger Operand: ATTRGUA ungültiger Guardtyp des Useridguards ungültiger Operand: GUACHK ungültiger Wert im reservierten Feld
X’00’	X’20’	X’3200’	class C: DEF3200
X’00’	X’40’	X’3300’	class D: DEF3300

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3303'	class D: DEF3303
X'00'	X'40'	X'3304'	class D: DEF3304
X'00'	X'40'	X'3305'	class D: DEF3305
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3307'	class D: DEF3307
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3310'	class D: DEF3310
X'00'	X'40'	X'3313'	class D: DEF3313
X'00	X'40	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3318'	class D: DEF3318
X'00	X'40	X'3319'	class D: DEF3319
X'00'	X'40'	X'3320'	class D: DEF3320
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

MODGUAD
Guard-Attribute ändern

Mit diesem Makro werden die Attribute eines Guards geändert. Nicht-privilegierte Benutzer können nur Guards der eigenen Kennung ändern. Der Guard-Administrator kann auch Guards anderer Kennungen ändern.

RFA kann nur verwendet werden, wenn beide Guards (Quell- und Ziel-Guard) auf dem gleichen Rechner lokal zugreifbar sind.

Makro	**Operanden**	
MODGUAD	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROL / <name 3>
	,PARAM =	<name 1..8>
	,NAME =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,NEWNAME =	<c-string: filename 1..24 without-gen-vers> / <var: char(24)> / (<reg: A(char(24))>)
	,COMMENT =	<c-string: text 1..80> / <var: char(80)> / (<reg: A(char(80))>)
	,SCOPE =	*UNCHANGED / *USERID / *USER_GROUP / *HOST_SYSTEM / <var: enum SCOPE> / (<reg: enum SCOPE>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

NAME vollqualifizierter Name des Guards, das umbenannt oder geändert wird. Es dürfen nur Großbuchstaben verwendet werden.

NEWNAME vollqualifizierter neuer Name des Guards. Es dürfen nur Großbuchstaben verwendet werden.

COMMENT Text, der als Kommentar für dieses Guard hinterlegt wird.

SCOPE Legt fest, wer dieses Guard für den Schutz seiner Objekte verwenden darf:

=*USERID Nur der Eigentümer darf das Guard verwenden.

=*USER_GROUP
Der Eigentümer und die Benutzergruppe, der der Eigentümer angehört, dürfen das Guard verwenden.

=*HOST_SYSTEM
Das Guard darf von allen verwendet werden.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1006'	Das angegebene Guard existiert bereits
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1014'	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1025'	Kopieren vom/zum fernen System nicht möglich
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
	X'80'	X'1036'	Guardskatalog gesperrt

MODSAC
Zugriffsbedingungen hinzufügen oder ändern

Mit diesem Makro werden, je nach Angabe des Operanden ACTION, neue Bedingungsdefinitionen einem Guard hinzugefügt oder bestehende Bedingungsdefinitionen geändert.

Makro	Operanden	
MODSAC	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROY / <name 3>
	,MGMTPRE =	P / <name 1>
	,MGMTMAC =	ROZ / <name 3>
	,PARAM =	<name 1..8>
*	,ACTION =	*ADD / *MODIFY
	,DIALOG =	*STD / *NO / *GUARD / *USERID / *CATALOG / <var: enum DIALOG> / (<reg: enum DIALOG>)
	,ERRMSG =	*NO / *YES
*	,GUARD	<c-string: filename 1..40 without-gen-vers with-wild> / <c-string: partial-filename 2..40 with-wild> / <var: char(40)> / (<reg: A(char(40))>)
	,SUBTYPE =	*NONE / *USER / *GROUP / *OTHER / *ALLUSER / <var: enum SUBTYPE> / (<reg: enum SUBTYPE>)
	,SUBIDS =	array(20): <c-string: name 1..8> / <var: char(8)> / (<reg: A(char(8))>)
	,ADMISS =	*YES / *NO / *PARAMS / <var: enum ADMISS> / (<reg: enum ADMISS>)
	,CKTIME =	*NO / *ADMISSION / *EXCLUSION / <var: enum COND_KIND> / (<reg: enum COND_KIND>)
	,TIMEN =	<integer 1..4> / <var: integer(1)> / (<reg: A(integer(1))>)
	,TIME#1 =	structure(2): (1) low: <c-string: time 5> / <var: char(5)> / (<reg: A(char(5))>) (2) high: <c-string: time 5> / <var: char(5)> / (<reg: A(char(5))>)
	,TIME#2 =	siehe TIME#1
	,TIME#3 =	siehe TIME#1
	,TIME#4 =	siehe TIME#1

(Teil 1 von 3)

Makro	Operanden	
MODSAC	,CKDATE =	*NO / *ADMISSION / *EXCLUSION / <var: enum COND_KIND> / (<reg: enum COND_KIND>)
	,DATEN =	<integer 1..4> / <var: integer(1)> / (<reg: A(integer(1))>)
	,DATE#1 =	structure(2): (1) low: <c-string: date 10> / <var: char(10)> / (<reg: A(char(10))>) (2) high: <c-string: date 10> / <var: char(10)> / (<reg: A(char(10))>)
	,DATE#2 =	siehe DATE#1
	,DATE#3 =	siehe DATE#1
	,DATE#4 =	siehe DATE#1
	,CKWEEK =	*NO / *ADMISSION / *EXCLUSION / <var: enum COND_KIND> / (<reg: enum COND_KIND>)
	,MO =	*NO / *YES
	,TU =	*NO / *YES
	,WE =	*NO / *YES
	,TH =	*NO / *YES
	,FR =	*NO / *YES
	,SA =	*NO / *YES
	,SU =	*NO / *YES
	,CKPRIV =	*NO / *ADMISSION / *EXCLUSION / <var: enum COND_KIND> / (<reg: enum COND_KIND>)
	,ACSADM =	*NO / *YES
	,CUPRV001 =	*NO / *YES
	,CUPRV002 =	*NO / *YES
	,CUPRV003 =	*NO / *YES
	,CUPRV004 =	*NO / *YES
	,CUPRV005 =	*NO / *YES
	,CUPRV006 =	*NO / *YES
	,CUPRV007 =	*NO / *YES
	,CUPRV008 =	*NO / *YES
	,FTADM =	*NO / *YES
	,FTACADM =	*NO / *YES
	,HWMAINT =	*NO / *YES
	,HSMSADM =	*NO / *YES
	,NETADM =	*NO / *YES
	,NOTIFADM =	*NO / *YES
	,OPERATG =	*NO / *YES
	,POSXADM =	*NO / *YES
	,PRSVADM =	*NO / *YES

(Teil 2 von 3)

Makro	Operanden	
MODSAC	,PROPADM =	*NO / *YES
	,SATFEVA =	*NO / *YES
	,SATFMGM =	*NO / *YES
	,SECADM =	*NO / *YES
	,STDPROC =	*NO / *YES
	,SUBSMGM =	*NO / *YES
	,SWMONAD =	*NO / *YES
	,TAPEADM =	*NO / *YES
	,TAPEKEYADM =	*NO / *YES
	,TSOS =	*NO / *YES
	,USERADM =	*NO / *YES
	,VMPRIV =	*NO / *YES
	,VM2ADM =	*NO / *YES
	,CKPROG =	*NO / *ADMISSION / *EXCLUSION / <var: enum COND_KIND> / (<reg: enum COND_KIND>)
	,PHASEN =	<integer 1..4> / <var: integer(1)> / (<reg: A(integer(1))>)
	,PHASE#1 =	structure(4): (1) type: *FILE / *PHASE / *MODULE / <var: enum PROG_TYPE> / (<reg: enum PROG_TYPE>) (2) library: <c-string: filename 1..54> / <var: char(54)> / (<reg: A(char(54))>) (3) element: <c-string: composed-name 1..54> / <var: char(54)> / (<reg: A(char(54))>) (4) version: *ANY / <c-string: composed-name 1..24> / <var: char(24)> / (<reg: A(char(24))>)
	,PHASE#2 =	siehe PHASE#1
	,PHASE#3 =	siehe PHASE#1
	,PHASE#4 =	siehe PHASE#1

(Teil 3 von 3)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Operanden, die mit „*“ gekennzeichnet sind, sind Pflichtoperanden bei MF=L.

Unterstrichene Operandenwerte sind nur bei ACTION=*ADD die voreingestellten Werte. Für ACTION=*MODIFY werden nur die explizit angegebenen Werte geändert; alle anderen bleiben unverändert.

Die Angaben COND_KIND, PROG_TYPE, DIALOG, SUBTYPE und ADMISSION verweisen auf die DSECT des Makros SACMGMT.

MGMTPRE und MGMTMAC
Legen den Präfix fest, der den globalen DSECTS, Konstanten und Gleichsetzungen vorangestellt wird. Dieses Präfix besteht aus den beiden Operanden MGMTPRE und MGMTMAC, die in dieser Reihenfolge zusammengesetzt werden.

Wenn ein Präfix verwendet wird, muss dieser mit dem bei SACMGMT im Operanden PREFIX übereinstimmen, da sonst Übersetzungsfehler auftreten.

ACTION legt die auszuführende Aktion fest. Dieser Operand muss bei MF=L angegeben werden. Wird nur ein Parameterbereich verwendet, so muss dieser bei einem Wechsel von *ADD nach *MODIFY oder umgekehrt neu initialisiert werden.

=*ADD Die Zugriffsbedingung wird hinzugefügt. Dies entspricht dem Kommando /ADD-ACCESS-CONDITIONS. Existiert das angegebene Guard nicht, wird es durch einen impliziten CREGUAD-Aufruf mit den Standardwerten angelegt.

=*MODIFY
Eine bestehende Zugriffsbedingung wird geändert. Dies entspricht dem SDF-Kommando /MODIFY-ACCESS-CONDITIONS

DIALOG Im Dialogbetrieb kann der Anwender die Funktion mit Kontrolldialog nutzen. Im Batchbetrieb wird immer DIALOG=*NO angenommen, auch wenn andere Angaben gemacht wurden.

=*STD Im Dialogbetrieb: *GUARD (siehe dort)
Im Batchbetrieb: *NO

=*NO Die Funktion wird ohne Rückfrage auf jedes der Auswahl entsprechende Guard ausgeführt.

=*GUARD Der Anwender kann für jedes der Auswahl entsprechende Guard im Dialog entscheiden, wie weiterzuverfahren ist:
NO: Funktion nicht ausführen
YES: Funktion ausführen
TERMINATE: Funktion abbrechen, auch wenn noch weitere Guards bearbeitet werden könnten.

=*USERID
Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Wurden in der Benutzerkennung Musterzeichen verwendet, wird bei jedem Wechsel einer Benutzerkennung ein Dialog eröffnet, in dem bestimmt werden kann, ob die der Auswahl entsprechende Benutzerkennung bearbeitet wird. Der Dialog kann wie bei *GUARD gesteuert werden.

=*CATALOG
Wurden in der Katalogkennung Musterzeichen verwendet, wird bei jedem Wechsel einer Katalogkennung ein Dialog eröffnet, in dem bestimmt werden kann, ob die der Auswahl entsprechende Katalogkennung bearbeitet wird. Der Dialog kann wie bei *GUARD gesteuert werden.

ERRMSG gibt an, ob Fehlermeldungen am Terminal (*SYSOUT) angezeigt werden.

=*NO Keine Fehlermeldungsausgabe am Terminal

=*YES Fehlermeldungsausgabe am Terminal

GUARD Name des zu bearbeitenden Guard. Der Name darf Musterzeichen enthalten. Es dürfen nur Großbuchstaben verwendet werden. Musterzeichen in der Benutzerkennung sind nur dem Guard-Administrator erlaubt. Dieser Operand muss bei MF=L angegeben werden.

SUBTYPE Legt den Typ der zu ändernden Subjekte fest.

=*NONE Es werden keine speziellen Zugriffsbedingungen definiert. Es wird ein Guard vom Typ STDACC eingerichtet.

=*USER Angabe der Benutzerkennungen, für die die nachfolgende Definition gilt.

=*GROUP Angabe der Benutzergruppe, für die die nachfolgende Definition gilt.

=*OTHER Angabe, wie mit allen anderen Benutzern, die weder in der *USER-Liste noch einer der explizit genannten Benutzergruppen enthalten sind, verfahren werden soll.

=*ALLUSER
Einträge bei *ALLUSER werden als letzte ausgewertet, wenn die bis dahin ausgewerteten Bedingungen das Ergebnis „Bedingungen erfüllt“ geben. Bei der Auswertung werden die Zugriffsbedingungen für *USER, *GROUP und *OTHERS mit der von *ALL-USERS über das logische UND verknüpft.

SUBIDS Bis zu je 20 Einträgen für *USER und *GROUP können explizit mit einem Aufruf eingetragen werden. Sollen Subjekte von diesem Guard verwaltet werden, muss überlegt werden, ob die Zusammenfassung über Gruppen zusammen mit der Definition der Zugriffsbedingung bei *ALLUSER diese Liste soweit verkürzt, dass nur die wirklichen Sonderfälle einzeln eingetragen werden müssen.

ADMISS Regelt, wie auf das durch das Guard geschützte Objekt zugegriffen werden darf. Ist für *ALLUSER ADMISS=*NO gegeben worden, lautet das Ergebnis der Auswertung immer, dass die Bedingungen nicht erfüllt sind, selbst wenn für einen Benutzer ADMISS=*YES eingetragen ist.

=*YES ein Zugriff ist immer erlaubt (sofern durch *ALLUSER überhaupt zugelassen)

=*NO ein Zugriff ist nie erlaubt

=*PARAMS
Ein Zugriff ist unter bestimmten Bedingungen gestattet, die im folgenden definiert werden

CKTIME legt fest, wie eine zeitliche Begrenzung in Stunden und Minuten zu werten ist:

=*NO Die Zeit-Bedingung wird nicht bewertet.

=*ADMISSION
Während der angegebenen Zeit ist der Zugriff erlaubt.

=*EXCLUSION
Während der angegebenen Zeit ist der Zugriff verboten.

TIMEN Gibt an, wie viele Zeitintervalle definiert werden. Es sind maximal 4 Zeitintervalle möglich.

TIME#1 - TIME#4
Definition je eines Zeitintervalls in Stunden und Minuten. Die Zeit ist in Form von HH:MM immer fünfstellig anzugeben.

CKDATE legt fest, wie eine zeitliche Begrenzung in Form eines Datums zu werten ist:

=*NO Die Datumsbedingung wird nicht bewertet.

=*ADMISSION
Während der angegebenen Zeit ist der Zugriff erlaubt.

=*EXCLUSION
Während der angegebenen Zeit ist der Zugriff verboten.

DATEN Gibt an, wie viele Datumsintervalle definiert werden. Es sind maximal 4 Datumsintervalle möglich.

DATE#1 - DATE#4
Definition je eines Datumsintervalls. Das Datum ist in Form von JJJJ-MM-DD immer zehnstellig anzugeben. Wird bei einem Datums-Intervall die obere Grenze weggelassen, wird sie mit der unteren gleichgesetzt.

CKWEEK legt fest, wie eine zeitliche Begrenzung in Form eines Wochentags zu werten ist:

=*NO Die Wochentagsbedingung wird nicht bewertet.

=*ADMISSION
Während der angegebenen Zeit ist der Zugriff erlaubt.

=*EXCLUSION
Während der angegebenen Zeit ist der Zugriff verboten.

MO, ..., SU Angabe der Wochentage, an denen die mit CKWEEK festgelegte Zugriffsbedingung gilt:

Die Operandennamen haben folgende Bedeutung:

Operand	Wochentag
MO	MOnday (Montag)
TU	TUesday (Dienstag)
WE	WEdnesday (Mittwoch)
TH	THursday (Donnerstag)
FR	FRiday (Freitag)
SA	SAturday (Samstag)
SU	SUnday (Sonntag)

=*NO Der Wochentag hat keinen Einfluss auf eine Zugriffsbedingung.

=*YES Die Zugriffsbedingung gilt an diesem Wochentag.

CKPRIV legt fest, wie die Angabe eines Privilegs zu werten ist:

=*NO Die Privileg-Angabe wird nicht bewertet.

=*ADMISSION
Dem angegebenen Privileg ist der Zugriff erlaubt.

=*EXCLUSION
Dem angegebenen Privileg ist der Zugriff verboten.

ACSADM, ..., VM2ADM
Angabe der Privilegien, an denen die mit CKPRIV festgelegte Zugriffsbedingung gilt:

Die Operandennamen haben folgende Bedeutung:

Operand	Privileg
ACSADM	ACS-ADMINISTRATION
CUPRV001 ... 008	CUSTOMER-PRIVILEGE-1 ... 8
FTADM	FT-ADMINISTRATION
FTACADM	FTAC-ADMINISTRATION
GUAADM	GUARD-ADMINISTRATION
HWMAINT	HARDWARE-MAINTENANCE
HSMSADM	HSMS-ADMINISTRATION
NETADM	NET-ADMINISTRATION
NOTIFADM	NOTIFICATION-ADMINISTRATION
OPERATG	OPERATING
POSXADM	POSIX-ADMINISTRATION
PRSVADM	PRINT-SERVICE-ADMINISTRATION
PROPADM	PROP-ADMINISTRATION
SATFEVA	SAT-FILE-EVALUATION
SATFMGM	SAT-FILE-MANAGEMENT
SECADM	SECURITY-ADMINISTRATION
STDPROC	STD-PROCESSING
SUBSMGM	SUBSYSTEM-MANAGEMENT
SWMONAD	SW-MONITOR-ADMINISTRATION
TAPEADM	TAPE-ADMINISTRATION
TAPEKEYADM	TAPE-KEY-ADMINISTRATION
TSOS	TSOS
USERADM	USER-ADMINISTRATION
VMPRIV	VIRTUAL-MACHINE-ADMINISTRATION
VM2ADM	VM2000-ADMINISTRATION

=*NO Das Privileg hat keinen Einfluss auf eine Zugriffsbedingung.

=*YES Die Zugriffsbedingung gilt für dieses Privileg.

PHASEN Gibt an, wie viele Programmdefinition folgen. Es sind maximal 4 Programmdefinitionen möglich. Bei Programmen ist darauf zu achten, dass sie wirksam gegen Änderungen geschützt sind (also nur das Ausführungsrecht für den Benutzer besitzen).
Um Konflikte bei der Verwendung von Modulen des Typs OM oder LLM zu vermeiden, wird empfohlen, die Module in unterschiedlichen Bibliotheken zu halten (siehe auch Handbuch „LMS“ [23]).

PHASE#1 - PHASE#4

Nummerierte Definition für je ein Programm. Jede Programmdefinition kann wie folgt spezifiziert werden:

type Gibt den Typ des Programmbehälters an

=*FILE

Das Programm ist eine gebundene Phase, die in einer Datei abgelegt ist. Die Operanden element und version werden nicht berücksichtigt.

=*PHASE

Das Programm ist eine gebundene Phase, die in einem Bibliothekselement vom Typ C abgelegt ist.

=*MODULE

Das Programm ist ein Modul oder LLM, das in einem Bibliothekselement vom Typ R oder L abgelegt ist.

library Name der Bibliothek oder der Datei, die das Programm enthält.

element Name des Bibliothekselements, das das Programm enthält.

version Version des Bibliothekselements, das das Programm enthält.

=*ANY

Die Version kann einen beliebigen Wert haben.

Hinweise zur Anwendung

Mit diesem Makro werden Zugriffsbedingungen als ganzes verändert. Jede Zugriffsbedingung besteht aus:

– Art der Zugriffsbedingung (Operand beginnt mit CK...)

– eine oder mehrere Bedingungen

Werden nicht alle Operanden einer Zugriffsbedingung angegeben, ist zu beachten:

– Wird ein Operand, beginnend mit CK..., nicht angegeben, so wird der Standardwert *NO angenommen und alle übrigen Operanden der Zugriffsbedingung nicht berücksichtigt oder, falls vorhanden, auf die Standardwerte (ebenfalls *NO) gesetzt.

– Wird beim Operanden CK... der Wert *NO explizit angegeben, werden alle übrigen Operanden der Zugriffsbedingung nicht berücksichtigt oder, falls vorhanden, auf die Standardwerte (ebenfalls *NO) gesetzt.

– Alle nicht angegebenen Operanden, die zu einer Bedingung (Operand beginnt mit CK...) gehören, werden mit den Standardwerten belegt.

– Wurde als Operandenwert *ADMISSION oder *EXCLUSION angegeben, muss mindestens ein Intervall oder Programm oder Privileg definiert werden.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
X'02'	CMD	X'1011'	Kommando wurde auf Wunsch des Benutzers abgebrochen
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1014'	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X'40'	X'1015'	Das angegebene Subjekt ist nicht im Guard enthalten
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1023'	Kein Guard entspricht den Auswahlkriterien
	X'40'	X'1026'	Kennung bereits in Bedingung enthalten
	X'40'	X'1027'	Bedingungsbereich voll
	X'40'	X'1028'	Guard hat falschen Typ
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
X'02'	X'40'	X'1035'	Kommando nicht ausgeführt
	X'80'	X'1036'	Guardskatalog gesperrt
	X'80'	X'1038'	Guardskatalog durch ARCHIVE gesperrt

MSGGUAD
Meldungen und Return-Codes ausgeben

Dieser Makro enthält Definitionen für die Meldungen und Fehlercodes der GUARDS- und Standardbedingungsverwaltung.

Makro	Operanden	
MSGGUAD	MF =	D
	,PREFIX =	P / <name 1>
	,MACID =	ROP / <name 3>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

REMCOO
Miteigentümerschutzregel entfernen

Mit dieser Funktion werden Miteigentümerschutzregeln aus einem Regelbehälter (Guard) gelöscht.

Ein Anwender kann nur Regeln aus Regelbehältern seiner eigenen Benutzerkennung löschen. Ein Guard-Administrator darf Regeln aus Regelbehältern fremder Benutzerkennungen löschen. Verbleibt keine weitere Regel mehr im Behälter, wird der gesamte Behälter gelöscht.

Makro	**Operanden**	
REMCOO	MF = ,PREFIX = ,MACID = ,PARAM = ,DIALOG = ,ERRMSG = ,COGUARD = ,RULENAM =	C / D / L / M / E C / <name 1> OOR / <name 3> <name 1..8> *STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1> *NO / *YES / <var: bit:1> ' ␣ ' / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40> ' ␣ ' / <c-string 1..20: alphanumeric name 1..12 with-wild(20)> / <var: char:20> / *ALL

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD

Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Der Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, aus dem Regeln gelöscht werden.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regeln aus mehreren Behälter gelöscht werden, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu löschenden Regel. Musterzeichen im Namen sind erlaubt. Verbleibt keine Regel mehr im Regelbehälter, wird er gelöscht.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

=*ALL Es werden alle Regeln und damit auch der Regelbehälter gelöscht.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: COO3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3001'	class A: COO3001 Warnung: Ein Regelbehälter wurde gelöscht, weil er keine Regeln mehr enthielt
X'02'	X'00'	X'3002'	class A: COO3002 Warnung: Bei Wildcardverarbeitung wurden ein oder mehrere Regelbehälter gelöscht, weil keine Regeln mehr eingetragen waren
X'02'	X'00'	X'3003'	class A: COO3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X'02'	X'00'	X'3004'	class A: COO3004 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden und es wurden ein oder mehrere Regelbehälter gelöscht, weil keine Regeln mehr eingetragen waren
X'00' X'01' X'02' X'03' X'04'	X'01'	X'3100'	class B: COO3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: COO3200
X'00'	X'40'	X'3300'	class D: COO3300
X'00'	X'40'	X'3302'	class D: COO3302
X'00'	X'40'	X'3304'	class D: COO3304
X'00'	X'40'	X'3306'	class D: COO3306

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3308'	class D: COO3308
X'00'	X'40'	X'3309'	class D: COO3309
X'00'	X'40'	X'3310'	class D: COO3310
X'00'	X'40'	X'3313'	class D: COO3313
X'00	X'40	X'3314'	class D: COO3314
X'00'	X'40'	X'3315'	class D: COO3315
X'00'	X'80'	X'3900'	class E: COO3900
X'00'	X'80'	X'3901'	class E: COO3901
X'00'	X'80'	X'3902'	class E: COO3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG COO3902`.

REMDEF
Standardschutzregel entfernen

Mit dieser Funktion werden Standardschutzregeln aus einem Regelbehälter (Guard) gelöscht. Ein Anwender kann nur Regeln aus Regelbehältern seiner eigenen Benutzerkennung löschen. Ein Guard-Administrator darf Regeln aus Regelbehältern fremder Benutzerkennungen löschen. Verbleibt keine weitere Regel mehr im Behälter, wird der gesamte Behälter gelöscht.

Makro	**Operanden**	
REMDEF	MF = ,PREFIX = ,MACID = ,PARAM = ,DIALOG = ,ERRMSG = ,COGUARD = ,RULENAM =	C / D / L / M / E D / <name 1> EFR / <name 3> <name 1..8> *STD / *NO / *COGUARD / *USERID / *CATALOG / <var: enum-of _dialog_s:1> *NO / *YES / <var: bit:1> ' ␣ ' / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40> ' ␣ ' / <c-string 1..20: alphanumeric name 1..12 with-wild(20)> / <var: char:20> / *ALL

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*STD Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob das Kommando angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

=*NO Die Funktion wird ohne Rückfrage auf jeden Regelbehälter angewendet.

=*COGUARD

Der Anwender kann für jeden ausgewählten Behälter im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Der Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Regelbehälters mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt werden. Das kann erwünscht sein, wenn zum Beispiel eine Positionsregel nicht vorhanden ist und eine Bearbeitung darum nicht möglich war.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

COGUARD Name des Regelbehälters

Dieser Operand bezeichnet den Namen des Regelbehälters, aus dem Regeln gelöscht werden.

Musterzeichen im Namen des Regelbehälters bewirken, dass die Regel in mehreren Behältern gelöscht wird, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der zu löschenden Regel. Musterzeichen im Namen sind erlaubt. Verbleibt keine Regel mehr im Regelbehälter, wird er gelöscht.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

=*ALL Es werden alle Regeln und damit auch der Regelbehälter gelöscht.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3001'	class A: DEF3001 Warnung: Ein Regelbehälter wurde gelöscht, weil er keine Regeln mehr enthielt
X'02'	X'00'	X'3002'	class A: DEF3002 Warnung: Bei Wildcardverarbeitung wurden ein oder mehrere Regelbehälter gelöscht, weil keine Regeln mehr eingetragen waren
X'02'	X'00'	X'3003'	class A: DEF3003 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden
X'02'	X'00'	X'3004'	class A: DEF3004 Warnung: Bei Wildcardverarbeitung konnten nicht alle Regelbehälter korrekt bearbeitet werden und es wurden ein oder mehrere Regelbehälter gelöscht, weil keine Regeln mehr eingetragen waren
X'00' X'01' X'02' X'03' X'04'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3300'	class D: DEF3300
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3304'	class D: DEF3304
X'00'	X'40'	X'3306'	class D: DEF3306

SC2	SC1	Maincode	Erläuterung
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3310'	class D: DEF3310
X'00'	X'40'	X'3313'	class D: DEF3313
X'00	X'40	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902.`

REMSAC
Zugriffsbedingungen entfernen

Dieser Makro löscht Zugriffsbedingungen.

Makro	Operanden	
REMSAC	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROX / <name 3>
	,MGMTPRE =	P / <name 1>
	,MGMTMAC =	ROZ / <name 3>
	,PARAM =	<name 1..8>
*	,GUARD =	<c-string: filename 1..40 without-gen-vers with-wild> / <c-string: partial-filename 2..40 with-wild> / <var: char(40)> / (<reg: A(char(40))>)
*	,SUBTYPE =	*ALL / *USER / *GROUP / *OTHER / *ALLUSER / <var: enum SUBTYPE> / (<reg: enum SUBTYPE>)
	,SUBIDS =	*NO / *ALL / array(20): <c-string: name 1..8> / <var: char(8)> / (<reg: A(char(8))>)
	,DIALOG =	*STD / *NO / *GUARD / *USERID / *CATALOG / <var: enum DIALOG> / (<reg: enum DIALOG>)
	,ERRMSG =	*NO / *YES

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Operanden, die mit „*“ gekennzeichnet sind, sind Pflichtoperanden bei MF=L. Die Angaben zu SUBTYPE und DIALOG verweisen auf die DSECT des Makros SACMGMT.

MGMTPRE und MGMTMAC

Legen das Präfix fest, das den globalen DSECTS, Konstanten und Gleichsetzungen vorangestellt wird. Dieses Präfix besteht aus den beiden Operanden MGMTPRE und MGMTMAC, die in dieser Reihenfolge zusammengesetzt werden.

Wenn ein Präfix verwendet wird, muss es mit dem bei SACMGMT im Operanden PREFIX übereinstimmen, da sonst Übersetzungsfehler auftreten.

GUARD

Name des zu bearbeitenden Guard. Der Name darf Musterzeichen enthalten. Es dürfen nur Großbuchstaben verwendet werden. Musterzeichen in der Benutzerkennung sind nur dem Guard-Administrator erlaubt. Dieser Operand muss bei MF=L angegeben werden.

SUBTYPE Legt den Typ der zu löschenden Subjekte fest. Dieser Operand muss bei MF=L angegeben werden.

=*ALL Es werden alle Zugriffsbedingungen gelöscht.

=*USER Angabe der Benutzerkennungen, deren Zugriffsbedingungen gelöscht werden.

=*GROUP Angabe der Benutzergruppe, deren Zugriffsbedingungen gelöscht werden.

=*OTHER Die Zugriffsbedingungen für alle anderen Benutzer werden gelöscht.

=*ALLUSER
Die Zugriffsbedingungen für *ALLUSER werden gelöscht.

SUBIDS Bestimmt, welche der bei SUBTYPE =*GROUP oder SUBTYPE=*USER vorhandenen Einzeleinträge gelöscht werden. Da für SUBTYPE=*ALLUSER und SUBTYPE=*OTHER jeweils nur ein Eintrag vorhanden ist, können für diese beiden SUBTYPES keine SUBIDS angegeben werden.

=*NO Es werden keine Zugriffsbedingungen gelöscht.

=*ALL Es werden alle Zugriffsbedingungen für den angegebenen SUBTYPE gelöscht.

=array(20) Wie bei der Definition der Zugriffsbedingung können bis zu 20 Einzeldefinitionen angegeben werden, die gelöscht werden.

DIALOG Im Dialogbetrieb kann der Anwender die Funktion mit Kontrolldialog nutzen. Im Batchbetrieb wird immer DIALOG=*NO angenommen, auch wenn andere Angaben gemacht wurden.

=*STD Im Dialogbetrieb: *GUARD (siehe unten)
Im Batchbetrieb: *NO

=*NO Die Funktion wird ohne Rückfrage auf jedes der Auswahl entsprechende Guard ausgeführt.

=*GUARD Der Anwender kann für jedes der Auswahl entsprechende Guard im Dialog entscheiden, wie weiterzuverfahren ist:

NO:	Funktion nicht ausführen
YES:	Funktion ausführen
TERMINATE:	Funktion abbrechen, auch wenn noch weitere Guards bearbeitet werden könnten.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.

Wurden in der Benutzerkennung Musterzeichen verwendet, wird bei jedem Wechsel einer Benutzerkennung ein Dialog eröffnet, in dem bestimmt werden kann, ob die der Auswahl entsprechende Benutzerkennung bearbeitet wird. Der Dialog kann wie bei *GUARD gesteuert werden.

=*CATALOG

Wurden in der Katalogkennung Musterzeichen verwendet, wird bei jedem Wechsel einer Katalogkennung ein Dialog eröffnet, in dem bestimmt werden kann, ob die der Auswahl entsprechende Katalogkennung bearbeitet wird. Der Dialog kann wie bei *GUARD gesteuert werden.

ERRMSG gibt an, ob Fehlermeldungen am Terminal angezeigt werden.

=*NO Keine Fehlermeldungsausgabe am Terminal

=*YES Fehlermeldungsausgabe am Terminal

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
X'02'	CMD	X'1011'	Das Kommando wurde auf Wunsch des Benutzers abgebrochen
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1014'	Der Benutzer ist nicht autorisiert, die Funktion auszuführen
	X'40'	X'1015'	Das angegebene Subjekt ist nicht im Guard enthalten
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1023'	Kein Guard entspricht den Auswahlkriterien
	X'40'	X'1028'	Guard hat falschen Typ
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
X'02'	X'40'	X'1035'	Kommando nicht ausgeführt
	X'80'	X'1036'	Guardskatalog gesperrt
	X'80'	X'1038'	Guardskatalog durch ARCHIVE gesperrt

REMUID
Kennungen für Objektpfad entfernen

Mit dieser Funktion werden Kennungen aus einem Benutzerkennungsguard gelöscht.

Verbleibt keine weitere Kennung mehr im Benutzerkennungsguard, wird das gesamte Guard gelöscht.

Makro	**Operanden**	
REMUID	MF = ,PREFIX = ,MACID = ,PARAM = ,DIALOG = ,ERRMSG = ,UIDGUA = ,IDTYPES = ,IDS =	C / D / L / M / E D / <name 1> EFH / <name 3> <name 1..8> *STD / *NO / *UIDGUA / *USERID / *CATALOG / <var: enum-of _dialog_s:1> *NO / *YES / <var: bit:1> ' ␣ ' / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40> array(20): *UID / *GRP / <var: enum-of _type_s:1> array(20): ' ␣ ' / <c-string 1..20: name 1..8 with-wild(20)> / *UNIVERS / <var: char:20>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

DIALOG Dialogführung

Der Anwender kann die Schnittstelle mit Kontrolldialog benutzen, wobei die Art der Dialogführung steuerbar ist. Die Dialogführung ist im Batchbetrieb wirkungslos, was der Angabe DIALOG-CONTROL=*NO entspricht.

=*NO Die Funktion wird ohne Rückfrage auf jedes Benutzerkennungsguard angewendet.

=*UIDGUA

Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt unabhängig davon, ob der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist oder nicht.

Ein Funktionsabbruch ist möglich.

=*USERID

Diesen Kontrolldialog kann nur ein Guard-Administrator verwenden.
Der Guard-Administrator kann für jede ausgewählte Benutzerkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Benutzerkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*CATALOG

Der Anwender kann für jede ausgewählte Katalogkennung im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn die Katalogkennung im Namen des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Funktionsabbruch ist möglich.

=*STD Der Anwender kann für jedes ausgewählte Benutzerkennungsguard im Dialog entscheiden, ob die Funktion angewendet wird oder nicht. Die Dialogführung erfolgt jedoch nur dann, wenn der Name des Benutzerkennungsguards mit Hilfe von Musterzeichen spezifiziert ist.

Ein Kommandoabbruch ist möglich.

ERRMSG Meldungsausgabe

Der Anwender kann angeben, ob aufgetretene Fehler als Meldung angezeigt wird. Das kann erwünscht sein, wenn zum Beispiel eine angegebene Benutzerkennung nicht eingetragen ist und die Funktion aus diesem Grund auf das Guard nicht angewendet wird.

=*NO Es werden keine Meldungen ausgegeben.

=*YES Es werden Meldungen ausgegeben.

UIDGUA Name des Benutzerkennungsguards

Dieser Operand bezeichnet den Namen des Benutzerkennungsguards vom Typ DEFPUID, aus dem Kennungen gelöscht werden.

Musterzeichen im Namen des Benutzerkennungsguards bewirken, dass die Benutzer- und Gruppenkennungen aus mehreren Guards gelöscht werden, sofern diese zugreifbar sind.

Musterzeichen in der Benutzerkennung darf nur ein Guard-Administrator spezifizieren.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

IDTYPES Typliste

Über diesen Operanden können in Form eines Arrays die Typen der Kennungen angegeben werden, die über den Operanden IDS spezifiziert werden.

=*UID Es handelt sich um eine Benutzerkennung.

=*GRP Es handelt sich um eine Gruppenkennung.

IDS Liste der Kennungen

Über diesen Operanden können in Form eines Arrays die Kennungen (ohne $) angegeben werden, deren Typ über den Operanden TYPE spezifiziert werden muss. Die Kennungen dürfen Musterzeichen enthalten.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*UNIVERS
Benutzergruppe *UNIVERSAL

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'02'	X'00'	X'3000'	class A: DEF3000 Warnung: Die Dialog-Kontrollabfrage wurde mit 'Terminate' beantwortet und die Funktionsdurchführung dadurch abgebrochen
X'02'	X'00'	X'3010'	class A: DEF3010 Warnung: Ein Benutzerkennungsguard wurde gelöscht, weil es keine Kennungen mehr enthielt
X'02'	X'00'	X'3011'	class A: DEF3011 Warnung: Bei Wildcardverarbeitung wurden ein oder mehrere Benutzerkennungsguards gelöscht, weil keine Kennungen mehr eingetragen waren
X'02'	X'00'	X'3012'	class A: DEF3012 Warnung: Bei Wildcardverarbeitung konnten nicht alle Benutzerkennungsguards korrekt bearbeitet werden
X'02'	X'00'	X'3013'	class A: DEF3013 Warnung: Bei Wildcardverarbeitung konnten nicht alle Benutzerkennungsguards korrekt bearbeitet werden und es wurden ein oder mehrere Benutzerkennungsguards gelöscht, weil keine Kennungen mehr eingetragen waren

SC2	SC1	Maincode	Erläuterung
X'00' X'01' X'02' X'03' X'04' X'05'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: DIALOG ungültiger Operand: UIDGUA ungültiger Operand: IDTYPES ungültiger Operand: IDS ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3400'	class D: DEF3400
X'00'	X'40'	X'3402'	class D: DEF3402
X'00'	X'40'	X'3404'	class D: DEF3404
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

SACMGMT
Globale Konstanten definieren

Der Makro enthält globale Konstanten und Deklarationen für die Standardbedingungsverwaltung. Der Makro muss vor den Makros CHKSAC, MODSAC, REMSAC und SHWSAC aufgerufen werden.

Makro	Operanden	
SACMGMT	MF =	D / L / C
	,PREFIX =	P / <name 1>
	,MACID =	ROZ / <name 3>
	,XPAND =	ALL / PARAM / ACOND

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND Der Umfang der expandierten DSECTS und Gleichsetzungen (EQUATES) kann gesteuert werden.

=ALL Es wird alles expandiert.

=PARAM Es werden die Gleichsetzungen (EQUATES) für den Subjekttyp, die möglichen Werte von DIALOG, WEEKDAYS und PRIVILEGES generiert.

=ACOND Es werden die Gleichsetzungen (EQUATES) und DSECTS für die Vereinbarung einer Zugriffsbedingung (ACOND) generiert.

SHWACOO
Miteigentümerberechtigungsregel anzeigen

Mit dieser Funktion kann sich ein Anwender für einen spezifizierten Objektnamen anzeigen lassen, ob er Miteigentümer ist und in welchen Regeln das Miteigentum für ihn beschrieben ist.

Die Anzeige der zu erfüllenden Zugriffsbedingungen muss in einem gesonderten Schritt erfolgen. Die in den angezeigten Regeln benannten Condition-Guards können mit dem Kommando /SHOW-ACCESS-ADMISSION oder mit der Programmschnittstelle SHWSAC aufgelistet werden. Näheres über das Anzeigeverhalten einer Zugriffserlaubnis ist der Beschreibung des Kommandos /SHOW-ACCESS-ADMISSION zu entnehmen.

Die Ausgabe der Miteigentümererlaubnis entspricht der Ausgabe des Kommandos /SHOW-COOWNER-PROTECTION-RULE. Sie unterscheidet sich darin, dass nur die Untermenge von Regeln ausgegeben wird, die bedeutend für die angegebene Benutzerkennung ist. Nicht angezeigt werden Regeln, die einen Zugriff verweigern.

Makro	**Operanden**	
SHWACOO	MF = XPAND = OBJECT = COTYPE = OUTAREA =	C / D / L / M / E PARAM / OUTPUT structure(2): (1) objnam: <u>' '</u> / <c-string 1..54: filename 1..54 without-gen-vers> / <var: char:54> (2) objtype: <u>*FILE</u> / <var: enum-of _object_type_s:1> <u>*FILE</u> / *JV / <var: enum-of _container_type_s:1> structure(2): (1) address: <u>NULL</u> / <var: pointer> (2) len: <u>0</u> / *ONERULE / *SUGRULES / <integer 144..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=<u>PARAM</u> Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

OBJECT Objekt

Name des Objektes, über das sich der Aufrufer bezüglich seiner Miteigentümerschaft informieren will.

objnam: Miteigentümerobjektname

Angaben über den Namen des Miteigentümerobjektes.

Aliasnamen und vereinbarte Präfixe sind nicht erlaubt, der spezifizierte Objektname wird unverändert verwendet.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

objtype Typ des Objektnamens entsprechend der SDF-Syntaxbeschreibung (siehe Handbuch „Kommandos“ [4]).

Angaben über den SDF-Namenstyp des Objektes. Zur Zeit wird nur der SDF-Namenstyp <filename> (*FILE) unterstützt, der sowohl für Dateinamen als auch für Jobvariablennamen gibt.

*FILE Der Objektname hat den SDF-Datentyp <filename>.

COTYPE Typ des aktiven Regelbehälters

Regeln für das Miteigentum können sowohl für Dateinamen als auch für Jobvariablen spezifiziert und in einem jeweils separaten, aktiven Regelbehälter eingetragen sein. Mit diesem Operand kann darum gesteuert werden, ob eine Miteigentümerregel für Datei- oder Jobvariablen-Miteigentümerschaft ermittelt wird.

=*FILE Es wird in einem aktiven Regelbehälter gesucht, der Miteigentümerregeln für Dateien enthält.

=*JV Es wird in einem aktiven Regelbehälter gesucht, der Miteigentümerregeln für Jobvariablen enthält.

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passen nicht alle selektierten Regeln in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen grösseren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Die Länge muss mindestens 144 Bytes betragen.

*ONERULE

Ausgabelänge für eine Regel.

*SUGRULES

Vorgeschlagene Ausgabelänge für mehrere Regeln.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X’00’	X’00’	X’0000’	class A: CMD0001
X’00’ X’01’ X’02’ X’03’ X’04’	X’01’	X’3100’	class B: COO3100 ungültige Parameteradresse ungültiger Operand: COTYPE Operand OBJECT: ungültige Teilangabe objnam Operand OBJECT: ungültige Teilangabe objtype ungültiger Operand: OUTAREA
X’00’	X’20’	X’3200’	class C: COO3200
X’00’	X’40’	X’3300’	class D: COO3300
X’00’	X’40’	X’3302’	class D: COO3302
X’00’	X’40’	X’3306’	class D: COO3306
X’00’	X’40’	X’3308’	class D: COO3308
X’00’	X’40’	X’3309’	class D: COO3309
X’00’	X’40’	X’3312’	class D: COO3312
X’00’	X’40’	X’3313’	class D: COO3313
X’00’	X’40’	X’3314’	class D: COO3314
X’00’	X’40’	X’3315’	class D: COO3315
X’00’	X’40’	X’3316’	class D: COO3316
X’00’	X’40’	X’3317’	class D: Ausgabebereich ist nicht groß genug
X’00’	X’80’	X’3900’	class E: COO3900
X’00’	X’80’	X’3901’	class E: COO3901
X’00’	X’80’	X’3902’	class E: COO3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG COO3902`.

SHWATTR
Standardwerte für Schutzattribute anzeigen

Mit dieser Funktion können Schutzattribut-Standardwerte angezeigt werden.

Ein Anwender, der weder Eigentümer des anzuzeigenden Attributguards noch Guard-Administrator ist, erhält die Attribute nur dann angezeigt, wenn er die entsprechende Berechtigung hat, auf das Attributguard zuzugreifen (SCOPE=*USER-GROUP oder *HOST-SYSTEM).

Makro	**Operanden**	
SHWATTR	MF = ,PREFIX = ,MACID = ,PARAM = ,XPAND = ,ATTRGUA ,OUTAREA=	C / D / L / M / E D / <name 1> EFL / <name 3> <name 1..8> PARAM / OUTPUT ' ␣ ' / <c-string 1..24: filename 1..24 without-gen-vers> / <var: char:24> / structure(2): (1) address: NULL / <var: pointer> (2) len: 0 / *SUGLEN / <integer 164..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

ATTRGUA Name des Attributguards

Dieser Operand bezeichnet den Namen des Attributguards vom Typ DEFPATTR, dessen Standardwerte für Schutzattribute angezeigt werden.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passt die Ausgabe nicht in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen größeren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss mindestens 224 Bytes betragen.

*SUGLEN

Vorgeschlagene Ausgabelänge für beide Attributbereiche.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'00' X'01' X'02'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: ATTRGUA ungültiger Operand: OUTAREA
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3317'	class D: Ausgabebereich ist nicht groß genug
X'00'	X'40'	X'3351'	class D: DEF3351
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG CO03902`.

SHWCOO
Miteigentümerschutzregel anzeigen

Mit dieser Funktion können Regeln des Miteigentümerschutzes aus einem Regelbehälter (Guard) angezeigt werden.

Ein Anwender, der weder Eigentümer des anzuzeigenden Behälters noch Guard-Administrator ist, erhält die Regeln nur dann angezeigt, wenn er die entsprechende Berechtigung hat, auf den Behälter zuzugreifen (SCOPE=*USER-GROUP oder *HOST-SYSTEM).

Makro	**Operanden**	
SHWCOO	MF =	C / D / L / M / E
	,PREFIX =	C / <name 1>
	,MACID =	OOS / <name 3>
	,PARAM =	<name 1..8>
	,XPAND =	PARAM / OUTPUT
	,COGUARD =	' ␣ ' / <c-string 1..40: filename 1..40 without-gen-vers> / <var: char:40>
	,RULENAM =	*ALL / <c-string 1..20: alphanumeric name 1..12 with-wild(20)> / <var: char:20>
	,OUTAREA =	structure(2): (1) address: NULL / <var: pointer> (2) len: 0 / *ONERULE / *SUGRULES / <integer 144..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

COGUARD Name des Regelbehälters
Dieser Operand bezeichnet den Namen des Regelbehälters, aus dem eine oder alle Regeln angezeigt werden.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden! Es dürfen keine Musterzeichen verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der anzuzeigenden Regel. Musterzeichen im Namen sind erlaubt.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*ALL Es werden alle Regeln angezeigt.

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passen nicht alle selektierten Regeln in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen grösseren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss mindestens 144 Bytes betragen.

*ONERULE
Ausgabelänge für eine Regel.

*SUGRULES
Vorgeschlagene Ausgabelänge für mehrere Regeln.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'00' X'01' X'02' X'03'	X'01'	X'3100'	class B: COO3100 ungültige Parameteradresse ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Operand: OUTAREA
X'00'	X'20'	X'3200'	class C: COO3200
X'00'	X'40'	X'3300'	class D: COO3300
X'00'	X'40'	X'3301'	class D: COO3301
X'00'	X'40'	X'3302'	class D: COO3302
X'00'	X'40'	X'3306'	class D: COO3306
X'00'	X'40'	X'3308'	class D: COO3308
X'00'	X'40'	X'3309'	class D: COO3309
X'00'	X'40'	X'3310'	class D: COO3310
X'00'	X'40'	X'3313'	class D: COO3313
X'00'	X'40'	X'3314'	class D: COO3314
X'00'	X'40'	X'3315'	class D: COO3315
X'00'	X'40'	X'3317'	class D: Ausgabebereich ist nicht groß genug
X'00'	X'80'	X'3900'	class E: COO3900
X'00'	X'80'	X'3901'	class E: COO3901
X'00'	X'80'	X'3902'	class E: COO3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG COO3902`.

SHWDEF
Standardschutzregel anzeigen

Mit dieser Funktion können Regeln des Standardschutzes aus einem Regelbehälter (Guard) angezeigt werden.

Ein Anwender, der weder Eigentümer des anzuzeigenden Behälters noch Guard-Administrator ist, erhält die Regeln nur dann angezeigt, wenn er die entsprechende Berechtigung hat, auf den Behälter zuzugreifen (SCOPE=*USER-GROUP oder *HOST-SYSTEM).

Makro	**Operanden**	
SHWDEF	MF =	C / D / L / M / E
	,PREFIX =	D / <name 1>
	,MACID =	EFS / <name 3>
	,PARAM =	<name 1..8>
	,XPAND =	PARAM / OUTPUT
	,COGUARD =	' ␣ ' / <c-string 1..40: filename 1..24 without-gen-vers with-wild(40)> / <var: char:40>
	,RULENAM =	*ALL / <c-string 1..20: alphanumeric name 1..12 with-wild(20)> / <var: char:20>
	,OUTAREA =	structure(2): (1) address: NULL / <var: pointer> (2) len: 0 / *ONERULE / *SUGRULES / <integer 164..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

COGUARD Name des Regelbehälters
Dieser Operand bezeichnet den Namen des Regelbehälters, aus dem eine oder alle Regeln angezeigt werden.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden! Es dürfen keine Musterzeichen verwendet werden!

RULENAM Name der Regel

Dieser Operand bezeichnet den Namen der anzuzeigenden Regel. Musterzeichen im Namen sind erlaubt.

ACHTUNG!
Es dürfen nur Großbuchstaben verwendet werden!

=*ALL Es werden alle Regeln angezeigt.

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passen nicht alle selektierten Regeln in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen grösseren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss mindestens 164 Bytes betragen.

*ONERULE
Ausgabelänge für eine Regel.

*SUGRULES
Vorgeschlagene Ausgabelänge für mehrere Regeln.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'00' X'01' X'02' X'03'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: COGUARD ungültiger Operand: RULENAM ungültiger Operand: OUTAREA
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3300'	class D: DEF3300
X'00'	X'40'	X'3301'	class D: DEF3301
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3310'	class D: DEF3310
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3317'	class D: Ausgabebereich ist nicht groß genug
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

SHWGUAD
Guard-Attribute anzeigen

Dieser Makro zeigt die Attribute von Guards an.

Makro	Operanden	
SHWGUAD	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	RON / <name 3>
	,PARAM =	<name 1..8>
	,XPAND =	PARAM / OUTPUT
	,NAME =	<c-string: filename 1..40 without-gen-vers with-wild> / <c-string: partial-filename 2..40 with-wild> / <var: char(40)> / (<reg: A(char(40))>)
	,SCOPE =	*ANY / list-poss(3): *USER_GROUP/*USERID/*HOST_SYSTEM
	,INFORM =	*ALL / *NAME / <var: enum INFORM> / (<reg: enum INFORM>)
	,OUTAREA =	structure(2): (1) address: <label> / (<reg: pointer>) (2) length: <integer 4..2^{31}-1> / <var: integer(4)> / (<reg: integer(4)>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

NAME Name des anzuzeigenden Guard. Es dürfen nur Großbuchstaben verwendet werden. Der NAME darf Musterzeichen enthalten. Musterzeichen in der Benutzerkennung sind nur für einen Guard-Administrator zulässig.

SCOPE Auswahl nach dem SCOPE-Attribut (wurde bei CREATE-GUARD oder CREGUAD vergeben). Jede Angabe außer *ANY zeigt nur die Guards des angegebenen SCOPE an. Eine Selektion nach dem SCOPE-Attribut ist nur für den Eigentümer und den Guard-Administrator möglich.

INFORM Auswahl der auszugebenden Information.

=*ALL Es werden alle verfügbaren Informationen zu dem Guard ausgegeben.

=*NAME Es werden nur die Namen der Guards ausgegeben. Diese Angabe ist nicht sinnvoll, wenn NAME keine Musterzeichen enthält (es wird nur der Guard-Name angezeigt, den man bei NAME bereits angegeben hat!).

OUTAREA Adresse und Länge des Ausgabebereichs.

Hinweise zur Anwendung

1. Der Eigentümer und ein Guard-Administrator können sich immer alle Informationen eines Guards anzeigen lassen. Andere Benutzer dürfen dies nur, wenn es über das SCOPE-Attribut zugelassen ist.
2. Liegen Guards auf einem Pubset, das über RFA zugreifbar ist, wird nur ein Ausgabebereich bis max. 64 KByte unterstützt, d.h. auch bei Angabe eines größeren Bereichs (> 64KByte) werden nur 64 KByte Ausgabeinformation in den Ausgabebereich übertragen. Ist der zu übertragende Block größer als 64 KByte, muss der Aufruf der Schnittstelle entsprechend oft wiederholt werden, um alle Daten zu übertragen.
3. Im Parameterbereich kann beim Indikator prefix.RONOMOR abgelesen werden, ob noch Guards das Auswahlkriterium erfüllen, aber keinen Platz im Ausgabebereich gefunden haben. Diese Guards können durch einen erneuten Aufruf der Prozedur gelesen werden, wobei jedoch zu beachten ist, dass der Parameterblock nicht verändert werden darf.
4. Das Feld prefix.RONOUS# gibt die in den Ausgabebereich übertragene Größe der Information an.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1004'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht beschreibbar
	X'40'	X'1005'	Der Ausgabebereich ist zu klein
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1023'	Kein Guard entspricht den Auswahlkriterien
	X'40'	X'1024'	Nutzung des Guards nicht zugelassen
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
	X'80'	X'1036'	Guardskatalog gesperrt

SHWOBJ
Standardschutzattribute für Objekt anzeigen

Mit dieser Funktion kann sich ein Anwender für einen spezifizierten Objektnamen anzeigen lassen, welche Standardschutzwerte festgelegt sind und in welchen Regeln diese Standardschutzwerte beschrieben sind. Die Standardschutzattribute werden jedoch nur für eigene Objekte des Kommandoaufrufers oder für Objekte mit entsprechender Miteigentümerberechtigung angezeigt.

Regeln für den Standardschutz können sowohl für Dateinamen als auch für Jobvariablen spezifiziert und in einem jeweils separaten, aktiven Regelbehälter eingetragen sein. Darum muss über den Operand COTYPE gesteuert werden, ob Auskunft über Standardschutzattribute von Dateien oder von Jobvariablen gewünscht wird. Dabei ist zu beachten, dass immer nur ein gesamtmögliches Attribut-Set angezeigt wird, unabhängig davon, ob einzelne Attribute für Jobvariablen verwertbar sind oder nicht.

Makro	**Operanden**	
SHWOBJ	MF = ,PREFIX = ,MACID = ,PARAM = ,XPAND = ,OBJNAM = ,COTYPE = ,OUTAREA =	C / D / L / M / E D / <name 1> EFD / <name 3> <name 1..8> PARAM / OUTPUT ’␣’ / <c-string 1..54: filename 1..54 without-gen-vers> / <var: char:54> *FILE / *JV / <var: enum-of _container_type_s:1> structure(2): (1) address: NULL / <var: pointer> (2) len: *MAXLEN / <integer 144..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

OBJNAM Objekt

Name des Objektes, über das sich der Aufrufer bezüglich der Standardwertvergabe informieren will.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

COTYPE Typ des aktiven Regelbehälters

Regeln für den Standardschutz können sowohl für Dateinamen als auch für Jobvariablen spezifiziert und in einem jeweils separaten, aktiven Regelbehälter eingetragen sein. Mit diesem Operand kann daher gesteuert werden, ob eine Regel für den Standardschutz von Dateien oder Jobvariablen ermittelt wird.

=*FILE Es wird in einem aktiven Regelbehälter gesucht, der Standardschutzregeln für Dateien enthält.

=*JV Es wird in einem aktiven Regelbehälter gesucht, der Standardschutzregeln für Jobvariablen enthält.

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passen nicht alle selektierten Regeln in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen grösseren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss mindestens 164 Bytes betragen.

*MAXLEN
Maximale Länge für die Ausgabe.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'00' X'01' X'02' X'03'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: COTYPE ungültiger Operand: OBJNAM ungültiger Operand: OUTAREA
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3300'	class D: DEF3300
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3312'	class D: DEF3312
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3316'	class D: DEF3316
X'00'	X'40'	X'3317'	class D: Ausgabebereich ist nicht groß genug
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

SHWSAC
Zugriffserlaubnis oder Zugriffsbedingungen anzeigen

Dieser Makro zeigt die Definition der Zugriffsbedingungen an.

Makro	Operanden	
SHWSAC	MF =	D / L / C / M / E
	,PREFIX =	P / <name 1>
	,MACID =	ROW / <name 3>
	,MGMTPRE =	P / <name 1>
	,MGMTMAC =	ROZ / <name 3>
	,XPAND =	PARAM / OUTPUT
	,PARAM =	<name 1..8>
*	,GUARD =	<c-string: filename 1..40 without-gen-vers with-wild> / <c-string: partial-filename 2..40 with-wild> / <var: char(40)> / (<reg: A(char(40))>)
	,SUBTYPE =	*ALL / *USER / *GROUP / *OTHER / *ALLUSER / <var: enum SUBTYPE> / (<reg: enum SUBTYPE>)
	,SUBIDS =	*ALL / array(20): <c-string: name 1..8> / <var: char(8)> / (<reg: A(char(8))>)
	,VIEW =	*CONDITIONS / *ADMISSION <var: enum VIEW> / (<reg: enum VIEW>)
	,INFORM =	*ADM / *ATTR / *ALL / *NAME / <var: enum INFORM> / (<reg: enum INFORM>)
	,OUTAREA =	structure(2): (1) address: <label> / (<reg: pointer>) (2) length: <integer 136..2^{31}-1> / <var: integer(4)> / (<reg: integer(4)>)

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

Operanden, die mit „*“ gekennzeichnet sind, sind Pflichtoperanden bei MF=L. Die Angaben zu SUBTYPE verweisen auf die DSECT des Makros SACMGMT.

MGMTPRE und MGMTMAC

Legen das Präfix fest, das den globalen DSECTS, Konstanten und Gleichsetzungen vorangestellt wird. Dieses Präfix besteht aus den beiden Operanden MGMTPRE und MGMTMAC, die in dieser Reihenfolge zusammengesetzt werden.

Wenn ein Präfix verwendet wird, muss dieses mit dem bei SACMGMT im Operanden PREFIX übereinstimmen, da sonst Übersetzungsfehler auftreten.

XPAND gibt die zu expandierenden Deklarationen an. Dieser Operand gilt nur bei MF=D.

=PARAM Das Modell des Parameterbereichs.

=OUTPUT Die Modelle der Teilbereiche der Ausgabe.

GUARD Name des anzuzeigenden Guard. Es dürfen nur Großbuchstaben verwendet werden. Der Name darf Musterzeichen enthalten (Einschränkung siehe Operand *ADMISSION in diesem Makro). Dieser Operand muss bei MF=L angegeben werden.

SUBTYPE, SUBIDS und INFORM werden nur bei VIEW=*CONDITIONS ausgewertet.

SUBTYPE Legt den Typ mit der VIEW=*CONDITIONS anzuzeigenden Subjekte fest.

=*ALL Es werden alle Zugriffsbedingungen angezeigt.

=*USER Angabe der Benutzerkennungen, deren Zugriffsbedingungen angezeigt werden.

=*GROUP Angabe der Benutzergruppe, deren Zugriffsbedingungen angezeigt werden.

=*OTHER Die Zugriffsbedingungen für alle anderen Benutzer werden angezeigt.

=*ALLUSER

Die Zugriffsbedingungen für *ALLUSER werden angezeigt.

SUBIDS Bestimmt, welche der bei SUBTYPE =*GROUP oder SUBTYPE=*USER vorhandenen Einzeleinträge angezeigt werden. Da für SUBTYPE=*ALLUSER und SUBTYPE=*OTHER jeweils nur ein Eintrag vorhanden ist, können für diese beiden SUBTYPES keine SUBIDS angegeben werden.

=*ALL es werden alle Zugriffsbedingungen für den angegebenen SUBTYPE angezeigt.

=array(20) Wie bei der Definition der Zugriffsbedingung können bis zu 20 Subjekte angegeben werden, die angezeigt werden.

VIEW Es können die auszugebenden Informationen eingeschränkt werden:

=*CONDITIONS
Es werden Zugriffsbedingungen des Guards angezeigt, die der Aufrufer des Makros zum Schutz seiner Objekte verwenden kann. Dies wird vom SCOPE-Attribut bestimmt.
Die Verwendung des Makros mit diesem Operandenwert entspricht dem Funktionsumfang von /SHOW-ACCESS-CONDITIONS.

=*ADMISSION
Es wird angezeigt, welche Bedingungen der Aufrufer erfüllen muss, um über dieses Guard auf ein Objekt zugreifen zu können. Der Aufrufer bekommt keine Auskunft darüber, durch welches Attribut der Zugriff gestattet ist. Die Verwendung des Makros mit diesem Operandenwert entspricht dem Funktionsumfang von /SHOW-ACCESS-ADMISSION.

Es werden nur die Bedingungen für den Aufrufer ausgewertet. Das SCOPE-Attribut wird nicht berücksichtigt - sollte sich aus einer illegalen Nutzung eines Guards das Ergebnis „Bedingung nicht erfüllt“ ergeben, wird dies über diese Option nicht angezeigt. Hierzu muss VIEW=*CONDITIONS gegeben werden.

Der Guard-Name darf bei Angabe von *ADMISSION keine Musterzeichen enthalten.

INFORM Legt fest, welche Informationen für jedes Guard ausgegeben werden.

=*ADM Es werden die Zugriffsbedingungen des Guards angezeigt.

=*ATTR Es werden die Attribute des Guards angezeigt.

=*ALL Es werden die Attribute und die Zugriffsbedingungen des Guards angezeigt.

=*NAME Es wird nur der Name des Guards angezeigt.

OUTAREA Adresse und Länge des Ausgabebereichs.

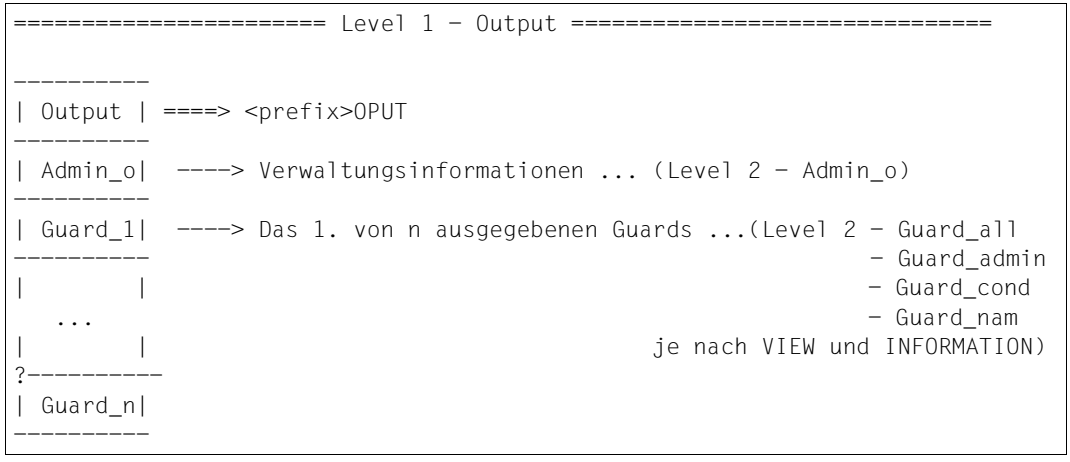
Layout der Ausgabebereiche von SHWSAC

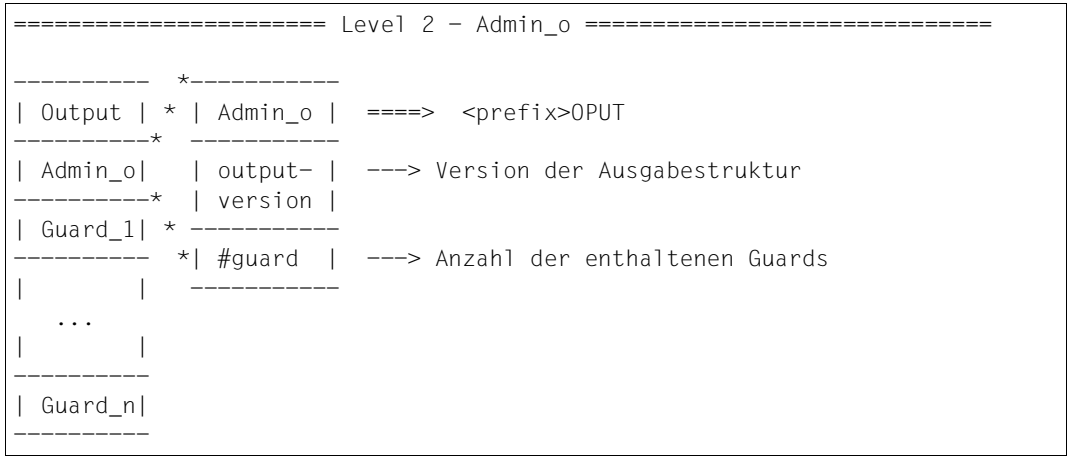
Der Ausgabebereich enthält eine komprimierte Darstellung der Zugriffsbedingungen und somit variable Teile; dadurch ist es nicht möglich, den Ausgabebereich durch eine einzelne DSECT zu beschreiben.

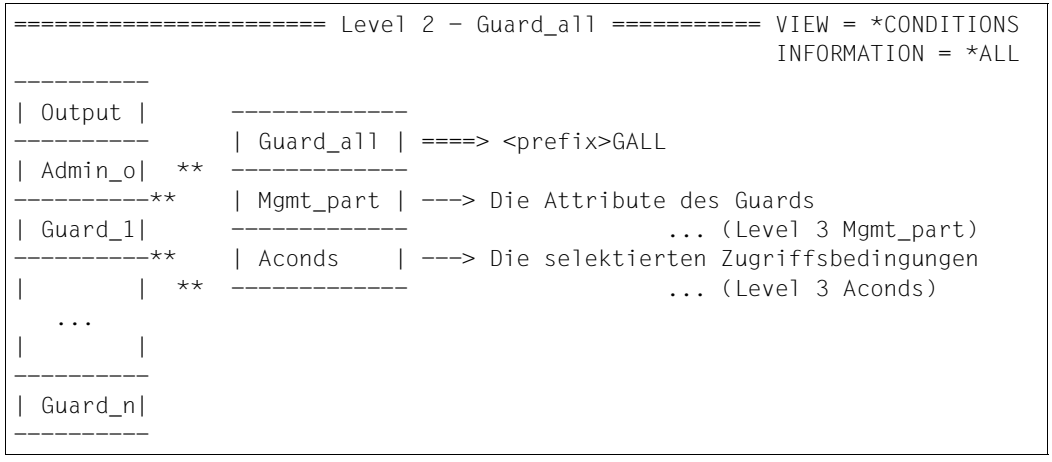
Der Aufrufer muss deshalb die einzelnen Einträge im Ausgabebereich selbst adressieren. Die dafür notwendigen DSECTS sind im folgenden Abschnitt genau beschrieben.

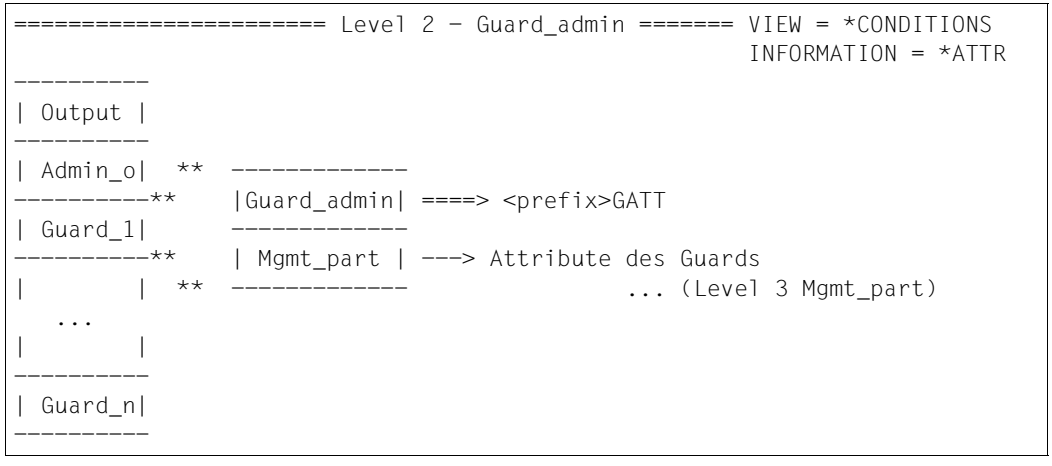
Da die Menge der ausgegebenen Information von den Aufruf-Parametern abhängt, wird folgendes Ausgabemodell verwendet:

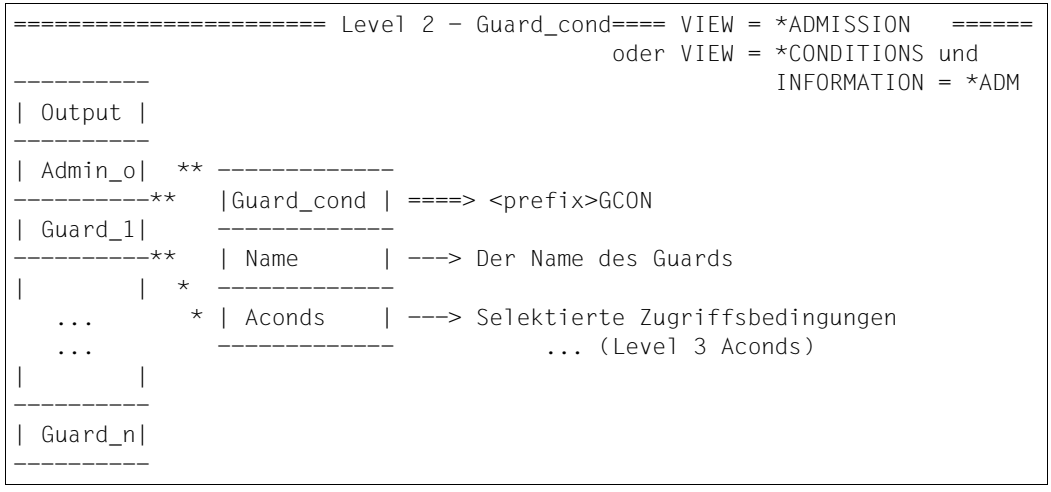
--->	Semantische Bedeutung des Feldes
===>	Verweis auf die entsprechende DSECT. <prefix> ist das bei SHWSAC angegebene PREFIX verkettet mit MACID. <mgmtpref> ist das bei SACMGMT angegebene Prefix von MGMTPRE verkettet mit MGMTMAC.
...	kennzeichnet, dass dieser Ausgabebereich in der angegebenen, weiteren Detaillierungsstufe (Level) beschrieben ist.

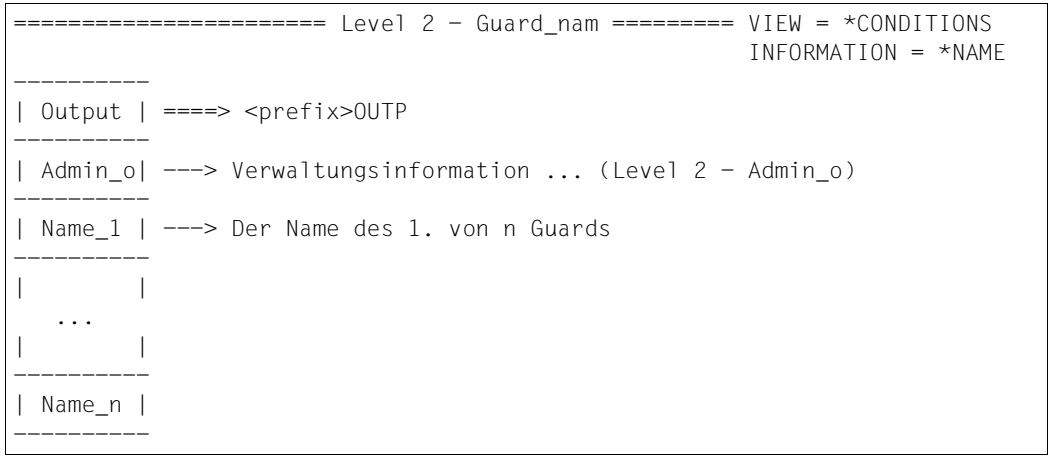

========== Level 1 - Output ==========
Output
====> <prefix>OPUT
Admin_o
----> Verwaltungsinformationen ... (Level 2 - Admin_o)
Guard_1
----> Das 1. von n ausgegebenen Guards ...(Level 2 - Guard_all
- Guard_admin
- Guard_cond
- Guard_nam
je nach VIEW und INFORMATION)
Guard_n

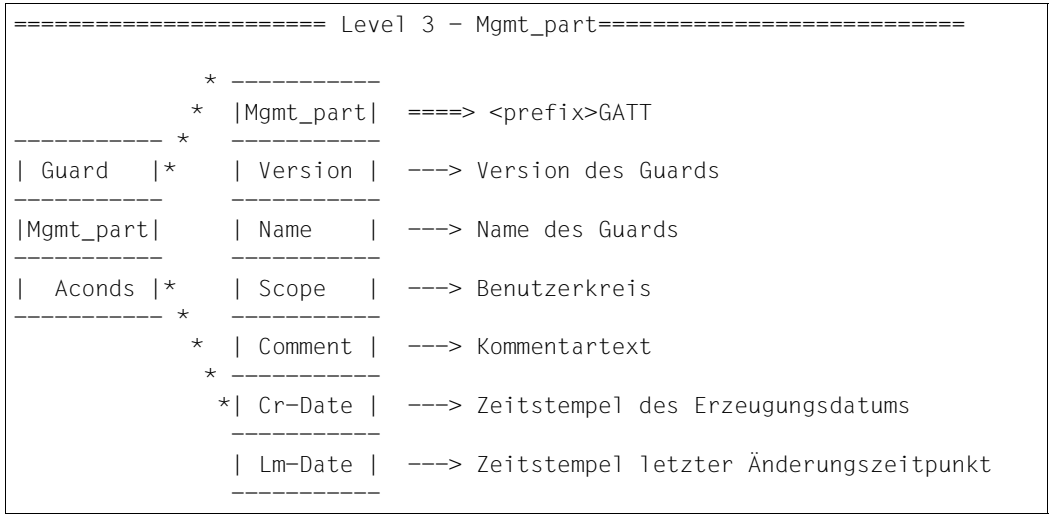

========== Level 2 - Admin_o ==========
Output
Admin_o
====> <prefix>OPUT
output- version
---> Version der Ausgabestruktur
Guard_1
#guard
---> Anzahl der enthaltenen Guards
Guard_n

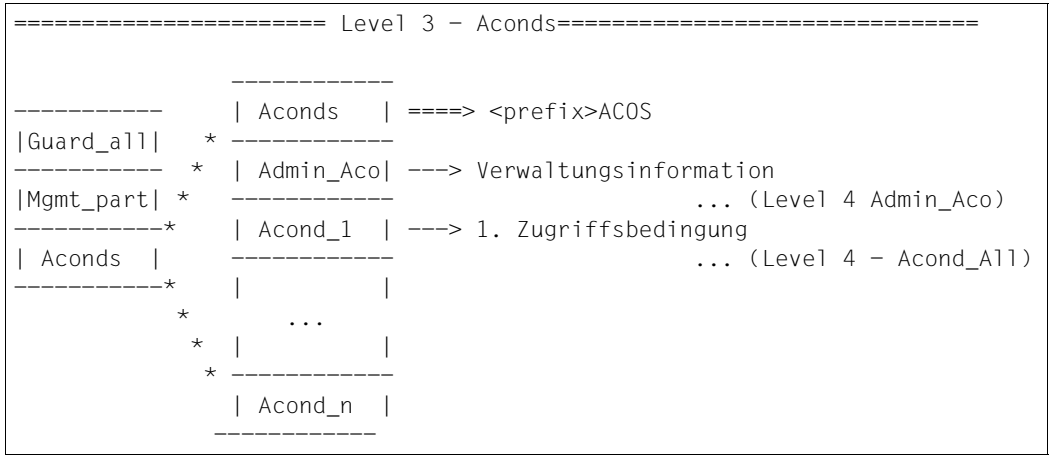

Level 2 - Guard_all
VIEW = *CONDITIONS
INFORMATION = *ALL
Output
Admin_o
Guard_1
Guard_n
Guard_all
<prefix>GALL
Mgmt_part
---> Die Attribute des Guards
... (Level 3 Mgmt_part)
Aconds
---> Die selektierten Zugriffsbedingungen
... (Level 3 Aconds)

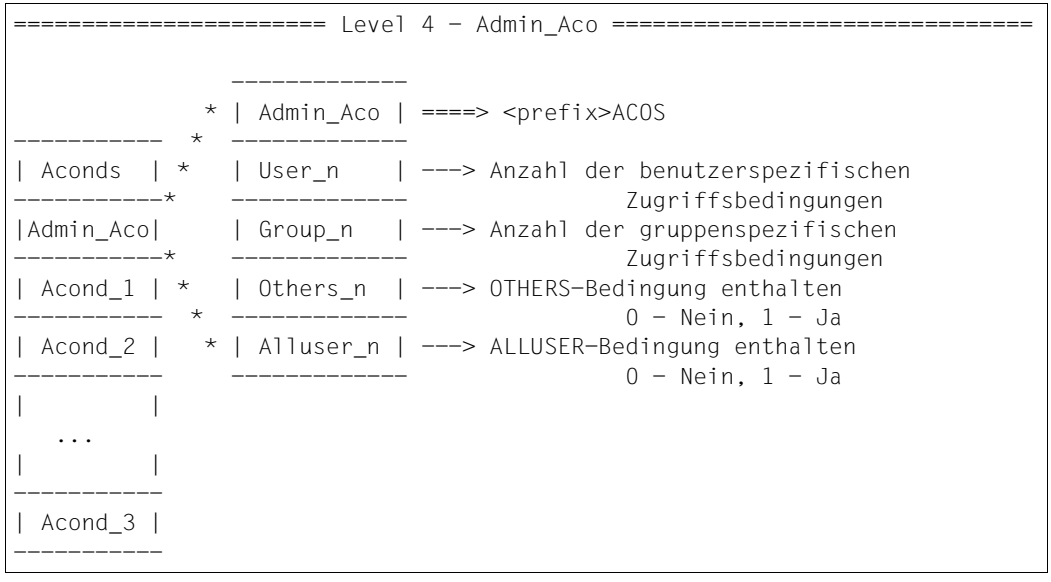

Level 2 - Guard_admin
VIEW = *CONDITIONS
INFORMATION = *ATTR
Output
Admin_o
Guard_1
Guard_n
Guard_admin
<prefix>GATT
Mgmt_part
---> Attribute des Guards
... (Level 3 Mgmt_part)

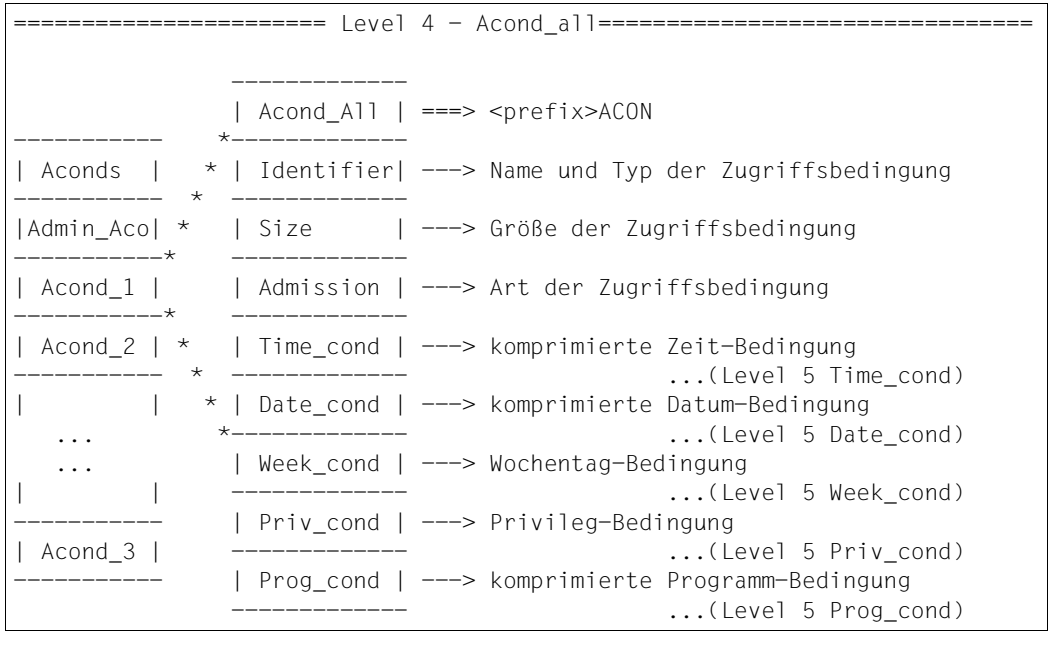

Level 2 - Guard_cond
VIEW = *ADMISSION
oder VIEW = *CONDITIONS und
INFORMATION = *ADM
Output
Admin_o
Guard_1
Guard_n
Guard_cond
Name
Aconds
<prefix>GCON
Der Name des Guards
Selektierte Zugriffsbedingungen
... (Level 3 Aconds)

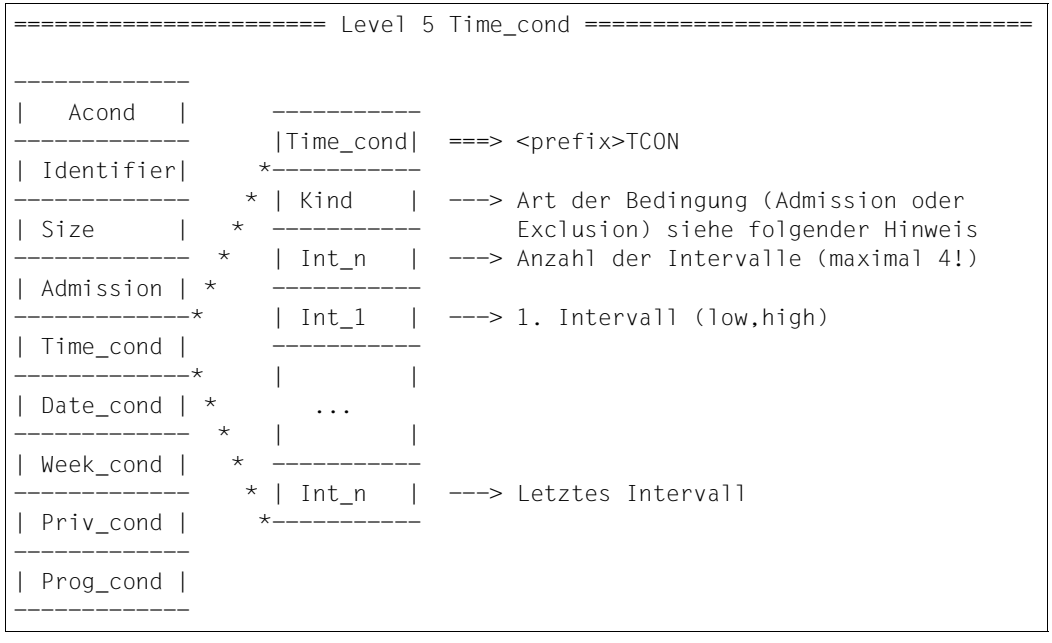

Level 2 - Guard_nam
VIEW = *CONDITIONS
INFORMATION = *NAME
Output
<prefix>OUTP
Admin_o
Verwaltungsinformation ... (Level 2 - Admin_o)
Name_1
Der Name des 1. von n Guards
Name_n

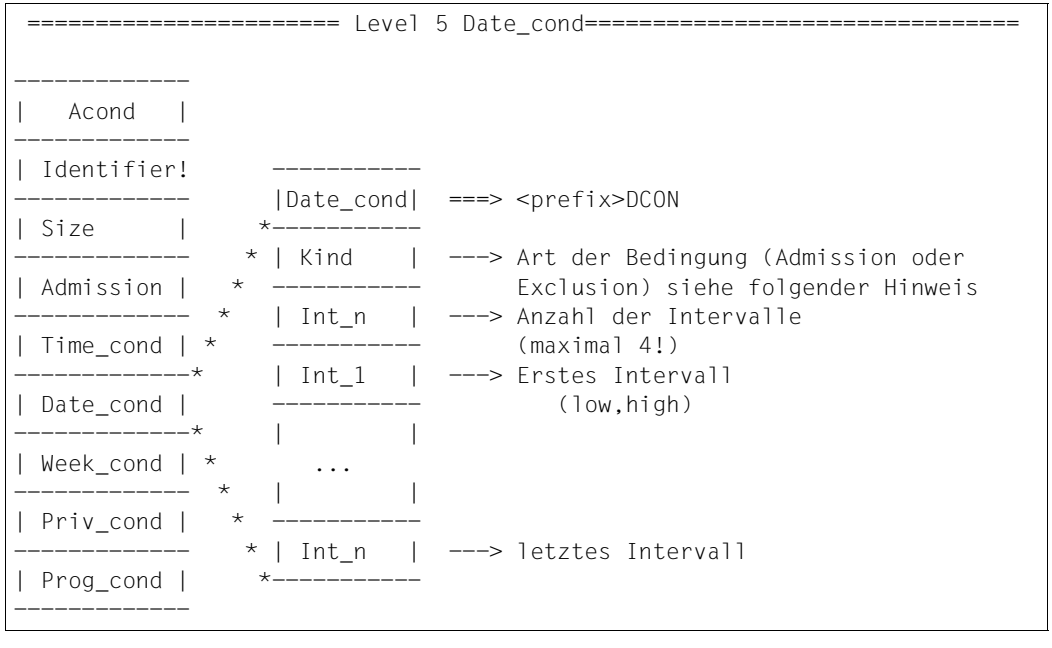

Level 3 - Mgmt_part
Mgmt_part
<prefix>GATT
Guard
Version
---> Version des Guards
Mgmt_part
Name
---> Name des Guards
Aconds
Scope
---> Benutzerkreis
Comment
---> Kommentartext
Cr-Date
---> Zeitstempel des Erzeugungsdatums
Lm-Date
---> Zeitstempel letzter Änderungszeitpunkt

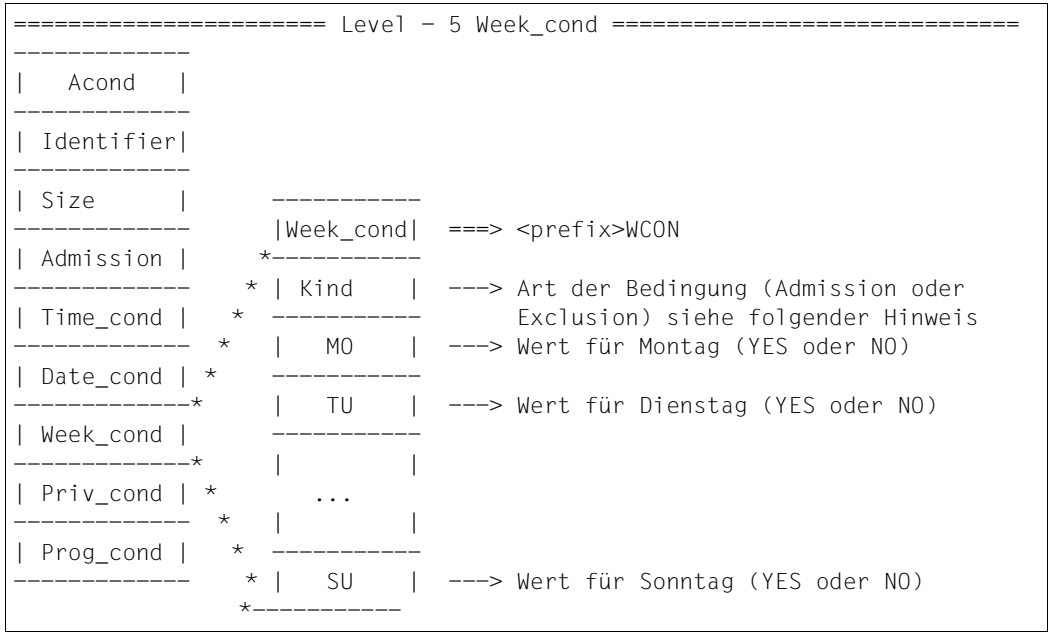

Level 3 - Aconds
Aconds
<prefix>ACOS
Guard_all
Admin_Aco
---> Verwaltungsinformation
... (Level 4 Admin_Aco)
Mgmt_part
Acond_1
---> 1. Zugriffsbedingung
... (Level 4 - Acond_All)
Aconds
...
Acond_n

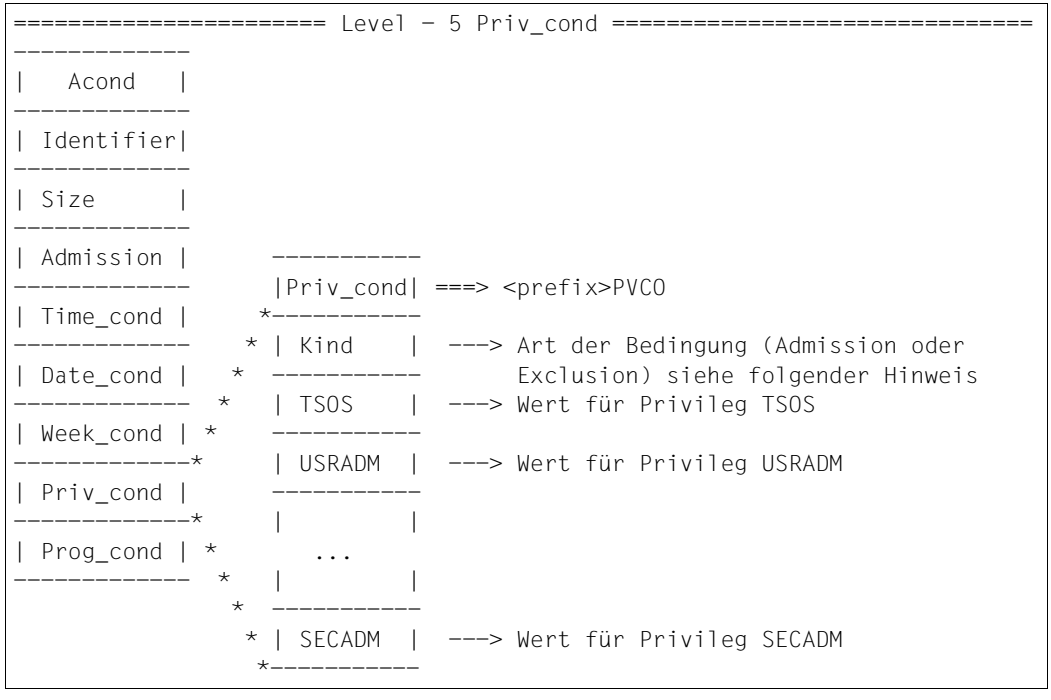

Level 4 - Admin_Aco
Admin_Aco
<prefix>ACOS
Aconds
Admin_Aco
Acond_1
Acond_2
Acond_3
User_n
Group_n
Others_n
Alluser_n
---> Anzahl der benutzerspezifischen Zugriffsbedingungen
---> Anzahl der gruppenspezifischen Zugriffsbedingungen
---> OTHERS-Bedingung enthalten
0 - Nein, 1 - Ja
---> ALLUSER-Bedingung enthalten
0 - Nein, 1 - Ja

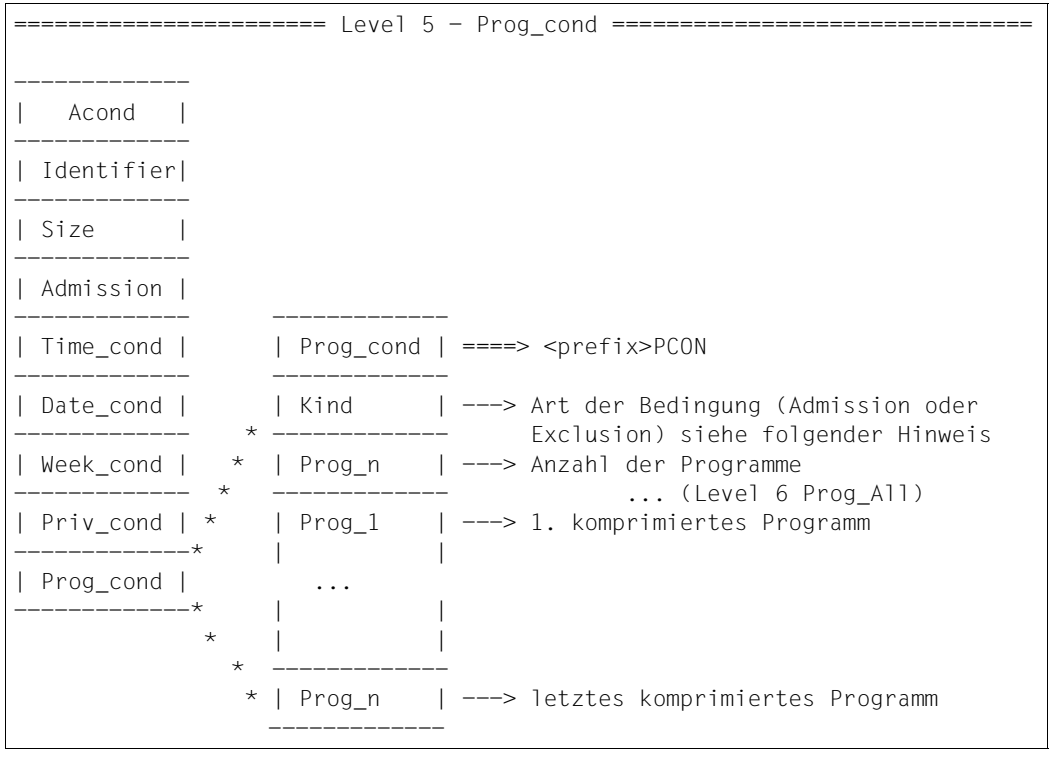

Level 4 - Acond_all
Acond_All
<prefix>ACON
Aconds
Admin_Aco
Acond_1
Acond_2
Acond_3
Identifier
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
---> Name und Typ der Zugriffsbedingung
---> Größe der Zugriffsbedingung
---> Art der Zugriffsbedingung
---> komprimierte Zeit-Bedingung
...(Level 5 Time_cond)
---> komprimierte Datum-Bedingung
...(Level 5 Date_cond)
---> Wochentag-Bedingung
...(Level 5 Week_cond)
---> Privileg-Bedingung
...(Level 5 Priv_cond)
---> komprimierte Programm-Bedingung
...(Level 5 Prog_cond)

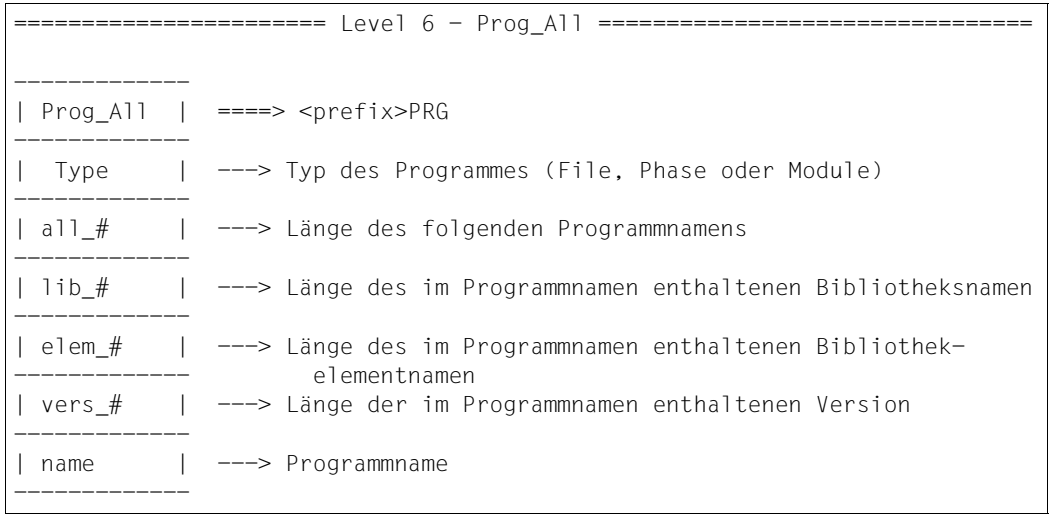

Level 5 Time_cond
Acond
Identifier
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
Time_cond
Kind
Int_n
Int_1
Int_n
===> <prefix>TCON
---> Art der Bedingung (Admission oder Exclusion) siehe folgender Hinweis
---> Anzahl der Intervalle (maximal 4!)
---> 1. Intervall (low,high)
---> Letztes Intervall


Level 5 Date_cond
Acond
Identifier!
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
Date_cond
Kind
Int_n
Int_1
Int_n
===> <prefix>DCON
---> Art der Bedingung (Admission oder Exclusion) siehe folgender Hinweis
---> Anzahl der Intervalle (maximal 4!)
---> Erstes Intervall (low,high)
---> letztes Intervall


Level - 5 Week_cond
Acond
Identifier
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
Week_cond
<prefix>WCON
Kind
Art der Bedingung (Admission oder Exclusion) siehe folgender Hinweis
MO
Wert für Montag (YES oder NO)
TU
Wert für Dienstag (YES oder NO)
SU
Wert für Sonntag (YES oder NO)


Level - 5 Priv_cond
Acond
Identifier
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
Priv_cond
<prefix>PVCO
Kind
Art der Bedingung (Admission oder Exclusion) siehe folgender Hinweis
TSOS
Wert für Privileg TSOS
USRADM
Wert für Privileg USRADM
SECADM
Wert für Privileg SECADM


====================== Level 5 - Prog_cond ==============================
Acond
Identifier
Size
Admission
Time_cond
Date_cond
Week_cond
Priv_cond
Prog_cond
Prog_cond
Kind
Prog_n
Prog_1
...
Prog_n
====> <prefix>PCON
---> Art der Bedingung (Admission oder
Exclusion) siehe folgender Hinweis
---> Anzahl der Programme
... (Level 6 Prog_All)
---> 1. komprimiertes Programm
---> letztes komprimiertes Programm


====================== Level 6 - Prog_All ==============================
Prog_All
====> <prefix>PRG
Type
---> Typ des Programmes (File, Phase oder Module)
all_#
---> Länge des folgenden Programmnamens
lib_#
---> Länge des im Programmnamen enthaltenen Bibliotheksnamen
elem_#
---> Länge des im Programmnamen enthaltenen Bibliothek-
elementnamen
vers_#
---> Länge der im Programmnamen enthaltenen Version
name
---> Programmname

Hinweise zur Auswertung des Ausgabebereichs von Bedingungen

Bei der Auswertung von Bedingungen ist zu beachten:

Die oben dargestellte Struktur einer Bedingung ist nur dann gültig, wenn die Art der Bedingung 'Kind' ungleich dem Wert *NO für CONDITION_KIND ist. (CONDITION_KIND wird im Makro SACMGMT definiert)

Im Fall *NO für CONDITION_KIND wird nur die Art der Bedingung in der Ausgabe hinterlegt.

Analog zu CONDITION_KIND gilt dieses Verhalten auch für Time_cond, Date_cond, Week_cond, Priv_cond und Prog_cond.

So kann die Ausgabestruktur einer Zugriffsbedingung folgendes Aussehen haben (Auszug aus der gesamten Ausgabe).

```
====================== Level 4 - Acond_All ==============================

_________________________
| Acond_All             |
_________________________
| Identifier            |
_________________________
| Size                  |
_________________________
| Admission             |
_________________________
| Time_cond: Kind       |   ---> mit Wert NO belegt
_________________________
| Date_cond: Kind       |   ---> mit Wert NO belegt
_________________________
| Week_cond: Kind       |   ---> mit Wert NO belegt
_________________________
| Priv_cond: Kind       |   ---> mit Wert NO belegt
_________________________
| Prog_cond: Kind       |   ---> mit Wert NO belegt
_________________________
```

Hinweise zur Anwendung

1. Ist im Parameterbereich der Indikator prefix.RONOMOR gesetzt, gibt es noch Guards, die das Auswahlkriterium erfüllen, aber im Ausgabebereich nicht mehr Platz gefunden haben.

   Diese Guards können durch einen erneuten Aufruf der Prozedur gelesen werden, wobei jedoch zu beachten ist, dass der Parameterblock nicht verändert werden darf.

2. Das Feld prefix.RONOUS# in der Unterstruktur prefix.ROWOPUT des Parameterbereichs gibt die in den Ausgabebereich übertragene Größe an.

3. Liegen Guards auf einem Pubset, das über RFA zugreifbar ist, wird nur ein Ausgabebereich bis max. 64 KByte unterstützt, d.h. auch bei Angabe eines größeren Bereichs (> 64KByte) werden nur 64 KByte Ausgabeinformation in den Ausgabebereich übertragen. Ist der zu übertragende Block größer als 64 KByte, muss der Aufruf entsprechend oft wiederholt werden, um alle Daten zu übertragen.

4. Das Feld prefix.ROWOUTV der Verwaltungsinformation zeigt die Version der Ausgabestruktur an. Diese Information ist jedoch erst von Bedeutung, wenn mehrere Versionen von SHWSAC mit unterschiedlicher Ausgabestruktur vorhanden sein können.

5. Wird SHWSAC mit VIEW=*ADMISSION aufgerufen, wird nur dann die gefundene Zugriffsbedingung zurückgegeben, wenn der Wert des Felds prefix.ROWAADM ungleich *NO ist.

   Ist das Feld prefix.ROWAADM der Zugriffsbedingung mit *NO belegt oder wird keine passende Zugriffsbedingung gefunden, wird der Returncode (X'1030', siehe DSECT von Makro MSGGUAD) zurückgegeben.

6. Wird SHWSAC mit VIEW=*ADMISSION aufgerufen, hat die Ausgabe dieselbe Struktur wie bei einem Aufruf mit VIEW=*CONDITIONS, INFORM=*ADM
   (siehe Level 2 - Guards_Cond).

7. Wurde in einem der Kommandos /ADD-ACCESS-CONDITIONS bzw. /MODIFY-ACCESS-CONDITIONS oder mit dem Makro MODSAC bei der PROGRAM-Bedingung der Operand VERSION mit *ANY versorgt, enthält die Version bei der Ausgabe ebenfalls die Zeichenkette *ANY.

8. Die Zeitstempel für CREATION-DATE und LAST-MODIFICATION-DATE werden in UNIVERSAL-TIME-COORDINATE (UTC) in Deutsch ausgegeben.

9. Die Schnittstelle MODSAC erlaubt nur die Eingabe von Großbuchstaben. Beim Operanden SUBIDS ist deshalb darauf zu achten, dass die Bezeichner nur Großbuchstaben enthalten.

   Werden trotzdem Kleinbuchstaben angegeben, führt das zwar zu keinem Fehler, es werden dann aber keine Zugriffsbedingungen selektiert und zurückgegeben.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
	X'01'	X'1000'	Der angegebene Wert des Operanden liegt nicht im erlaubten Bereich. Der fehlerhafte Operand steht als symbolischer Wert im SC2
	X'20'	X'1001'	Ein interner Fehler trat auf. Für eine genauere Analyse wurde ein SERSLOG-Eintrag geschrieben
	X'40'	X'1002'	Der Guard-Name ist syntaktisch falsch
	X'40'	X'1003'	Speicher für den Ausgabebereich nicht in der benötigten Länge allokiert oder nicht zugreifbar
	X'40'	X'1004'	Speicher für den Parameterbereich nicht in der benötigten Länge allokiert oder nicht beschreibbar
	X'40'	X'1005'	Der Ausgabebereich ist zu klein
	X'40'	X'1007'	Das angegebene Guard existiert nicht
	X'80'	X'1009'	Das angegebene Guard ist von einer anderen Task gesperrt
	X'40'	X'1012'	Der angegebene Katalog ist nicht definiert oder nicht zugreifbar
	X'40'	X'1013'	Das Pubset ist bei der GUARDS-Verwaltung unbekannt (Guardskatalog wurde wahrscheinlich bei IMPORT-PUBSET nicht geöffnet)
	X'40'	X'1016'	Fehler im Kommunikationsmittel des MRS
	X'40'	X'1017'	Unbekannte Benutzerkennung
	X'40'	X'1018'	Fernes System nicht verfügbar
	X'40'	X'1020'	Kein Speicher mehr vorhanden
	X'40'	X'1021'	BCAM-Verbindungsfehler
	X'40'	X'1022'	BCAM-Verbindung unterbrochen
	X'40'	X'1023'	Kein Guard entspricht den Auswahlkriterien
	X'40'	X'1024'	Nutzung des Guards nicht zugelassen
	X'40'	X'1028'	Guard hat falschen Typ
	X'40'	X'1029'	GUARDS auf dem fernen Rechner nicht verfügbar
	X'40'	X'1030'	Benutzer-Bedingung im Guard nicht erfüllbar

SHWUID
Kennungen für Objektpfad anzeigen

Mit dieser Funktion kann sich ein Systemverwalter oder ein Guard-Administrator Benutzer- und Gruppenkennungen aus einem Benutzerkennungsguard angezeigen lassen.

Makro	**Operanden**	
SHWUID	MF = ,PREFIX = ,MACID = ,PARAM = ,UIDGUA = ,OUTAREA=	C / D / L / M / E D / <name 1> EFI / <name 3> <name 1..8> ' ␣ ' / <c-string 1..24: filename 1..24 without-gen-vers> / <var: char:24> structure(2): (1) address: NULL / <var: pointer> (2) len: 0 / *ONEID / *MAXIDS / <integer 52..268435455> / <var: int:4>

Die Beschreibung der Parameter MF, PREFIX, MACID, PARAM siehe Handbuch „Makroaufrufe an den Ablaufteil“ [16].

UIDGUA Name des Benutzerkennungsguards

Dieser Operand bezeichnet den Namen des Benutzerkennungsguards vom Typ DEFPUID, das die Kennungen enthält, die angezeigt werden.

ACHTUNG!
Der Operand muss mit einem Wert versehen werden. Es dürfen nur Großbuchstaben verwendet werden!

OUTAREA Ausgabebereich

Dieser Operand bezeichnet Adresse und Länge des Adressraumes, in den die ermittelte Ausgabeinformation eingetragen wird. Passen nicht alle selektierten Kennungen in den Ausgabebereich, wird ein Fehler gemeldet und der Aufrufer muss einen größeren Ausgabebereich zur Verfügung stellen.

address: Adresse

Angabe der Adresse des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss an Wortgrenze stehen.

len: Länge

Angabe über die Länge des Ausgabebereiches.

ACHTUNG!
Der Ausgabebereich muss mindestens 52 Bytes betragen.

*ONEID
Ausgabelänge für eine Regel.

*MAXIDS
Vorgeschlagene Ausgabelänge für mehrere Regeln.

Makro-Returncode

SC2	SC1	Maincode	Erläuterung
X'00'	X'00'	X'0000'	class A: CMD0001
X'00' X'01' X'02' X'03'	X'01'	X'3100'	class B: DEF3100 ungültige Parameteradresse ungültiger Operand: UIDGUA ungültiger Operand: OUTAREA ungültiger Wert im reservierten Feld
X'00'	X'20'	X'3200'	class C: DEF3200
X'00'	X'40'	X'3302'	class D: DEF3302
X'00'	X'40'	X'3306'	class D: DEF3306
X'00'	X'40'	X'3308'	class D: DEF3308
X'00'	X'40'	X'3309'	class D: DEF3309
X'00'	X'40'	X'3313'	class D: DEF3313
X'00'	X'40'	X'3314'	class D: DEF3314
X'00'	X'40'	X'3315'	class D: DEF3315
X'00'	X'40'	X'3317'	class D: Ausgabebereich ist nicht groß genug
X'00'	X'40'	X'3400'	class D: DEF3400
X'00'	X'40'	X'3401'	class D: DEF3401
X'00'	X'40'	X'3402'	class D: DEF3402
X'00'	X'80'	X'3900'	class E: DEF3900
X'00'	X'80'	X'3901'	class E: DEF3901
X'00'	X'80'	X'3902'	class E: DEF3902

Die genaue Fehlerursache kann durch Aufruf des Kommandos /HELP-MSG mit der in der Tabelle angegebenen Fehlernummer ermittelt werden, z.B. `/HELP-MSG DEF3902`.

5.12.1 Beispiele zu GUARDS-Makros

Die Anwendung der Schnittstellen MODSAC, REMSAC und SHWSAC wird durch ein größeres Beispiel beschrieben. Dabei werden mehrere Aufgabenstellungen und deren Lösung aufgezeigt.

Beispiel 1: Zugriffsbedingungen hinzufügen

In einem Guard mit Namen TEST-GUA, das bisher noch nicht existiert, sollen folgende Dateizugriffe für ein Arbeitsteam festgelegt werden:

1. Den Mitarbeitern ANNE und JOHN sollen Dateizugriffe ohne spezielle Einschränkungen erlaubt sein.
2. Mitarbeiterin MARY ist Teilzeitkraft. Darum sind für sie Dateizugriffe nur an ihren Arbeitstagen Montag, Mittwoch und Donnerstag erlaubt.
3. Der externe Mitarbeiter PAUL steht vom 1. Juli 2017 bis 30. September 2017 unter Vertrag. Während dieser Zeit ist auch er zugriffsberechtigt.

Die Mitarbeiter ANNE, JOHN, MARY und PAUL sind von der Systemadministration zur Benutzergruppe WORKTEAM zusammengefasst, der noch weitere Gruppenmitglieder angehören. Die Benutzergruppe REVIEWER umfasst ein Team, das Reviewarbeiten durchführen soll.

4. Für die Zeitdauer eines gemeinsamen Reviews ist es notwendig, dass die gesamte Gruppe TEAMWORK und die Gruppe REVIEWER Zugriffsrecht erhalten.

   Für die Reviews sind folgende Termine angesetzt:

   – 23./24. August 2017 von 09:00 bis 15:00 Uhr

   – 02./03. September 2017 von 09:00 bis 15:00 Uhr

5. Für alle Zugriffsberechtigten gilt die Zusatzregelung, dass ein Dateizugriff außerhalb der offiziellen Arbeitszeit (Montags bis Freitags von 07:00 bis 19:00) generell nicht gestattet ist.

Lösung

```
*        ************************************************************
*        * ---------------------------------------------------------- *
*        *                                                            *
*        * Makro MODSAC: Zugriffsbedingungen hinzufuegen             *
*        * ============================================               *
*        *                                                            *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
GUA1     CSECT
*
*        ************************************************************
*        * ---------------------------------------------------------- *
*        * Makro MOVE                                                 *
*        * ==========                                                 *
*        * Aufgabe: Move Parameterbereich PARMACL nach PARMACC.       *
*        * Zweck:   Mit diesem Makro wird vor jedem Aufruf des        *
*        *          Makros MODSAC der in Register 1 zu uebergebende  *
*        *          Parameterbereich PARMACC neu initialisiert.      *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
         MACRO
         MOVE

         LA    R@TO,PARMACC
         LA    R@TOL,PROY#
         LA    R@FR,PARMACL
         LA    R@FRL,PROY#
         ICM   R@FRL,8,=C' '
         MVCL  R@TO,R@FR
         MEND
*
*        ************************************************************
*
R@TO     EQU   6               Zieladresse
R@TOL    EQU   7               Zielfeldlaenge
R@FR     EQU   8               Quelladresse
R@FRL    EQU   9               Quellfeldlaenge / Fuellzeichen
R@BASE   EQU   10              Basisregister
         BALR  R@BASE,0
         USING *,R@BASE
*
```

```
*       ***************************************************************
*       * 1. Den Mitarbeitern ANNE und JOHN sollen Dateizugriffe     *
*       *    ohne spezielle Einschraenkungen erlaubt sein.          *
*       ***************************************************************
*
        MOVE                                    Parameterinitialisierung
        MODSAC MF=M,                                                   -
              ACTION=*ADD,                                             -
              GUARD='TEST-GUA',                                        -
              SUBTYPE=*USER,                                           -
              SUBIDS=('ANNE    ','JOHN    '),                          -
              ADMISS=*YES
        MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
*       ***************************************************************
*       * 2. Mitarbeiterin MARY ist Teilzeitkraft. Darum sind fuer   *
*       *    sie Dateizugriffe nur an ihren Arbeitstagen            *
*       *    Montag, Mittwoch und Donnerstag erlaubt.               *
*       ***************************************************************
*
        MOVE                                    Parameterinitialisierung
        MODSAC MF=M,                                                   -
              ACTION=*ADD,                                             -
              GUARD='TEST-GUA',                                        -
              SUBTYPE=*USER,                                           -
              SUBIDS='MARY    ',                                       -
              ADMISS=*PARAMS,                                          -
              CKWEEK=*ADMISSION,                                       -
              MO=*YES,                                                 -
              WE=*YES,                                                 -
              TH=*YES
        MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
```

```
*       ************************************************************
*       * 3. Der externe Mitarbeiter PAUL steht vom 1. Juli 2017    *
*       *    bis 30. September 2017 unter Vertrag. Waehrend dieser  *
*       *    Zeit ist auch er zugriffsberechtigt.                   *
*       ************************************************************
*
        MOVE                                  Parameterinitialisierung
        MODSAC MF=M,                                                  -
              ACTION=*ADD,                                            -
              GUARD='TEST-GUA',                                       -
              SUBTYPE=*USER,                                          -
              SUBIDS='PAUL    ',                                      -
              ADMISS=*PARAMS,                                         -
              CKDATE=*ADMISSION,                                      -
              DATEN=1,                                                -
              DATE#1=('2017-07-01','2017-09-30')
       MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
*       ************************************************************
*       * 4. Fuer die Zeitdauer eines gemeinsamer Reviews ist es    *
*       *    notwendig, dass die gesamte Gruppe TEAMWORK und die    *
*       *    Gruppe REVIEWER Zugriffsrecht erhalten.                *
*       *    Fuer die Reviews sind folgende Termine angesetzt:      *
*       *    23./24. August    2017 von 09:00 bis 15:00 Uhr         *
*       *    02./03. September 2017 von 09:00 bis 15:00 Uhr         *
*       ************************************************************
*
        MOVE                                  Parameterinitialisierung
        MODSAC MF=M,                                                  -
              ACTION=*ADD,                                            -
              GUARD='TEST-GUA',                                       -
              SUBTYPE=*GROUP,                                         -
              SUBIDS=('TEAMWORK','REVIEWER'),                         -
              ADMISS=*PARAMS,                                         -
              CKTIME=*ADMISSION,                                      -
              TIMEN=1,                                                -
              TIME#1=('09:00','15:00'),                               -
              CKDATE=*ADMISSION,                                      -
              DATEN=2,                                                -
              DATE#1=('2017-08-23','2017-08-24'),                     -
              DATE#2=('2017-09-02','2017-09-03')
       MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
```

```
*       ************************************************************
*       * 5. Fuer alle Zugriffsberechtigten gilt die Zusatzregelung, *
*       *    dass ein Dateizugriff ausserhalb der offiziellen       *
*       *    Arbeitszeit (Montags bis Freitags von 07:00 bis 19:00)  *
*       *    generell nicht gestattet ist.                           *
*       ************************************************************
*
        MOVE                                    Parameterinitialisierung
        MODSAC MF=M,                                                   -
              ACTION=*ADD,                                             -
              GUARD='TEST-GUA',                                        -
              SUBTYPE=*ALLUSER,                                        -
              ADMISS=*PARAMS,                                          -
              CKTIME=*ADMISSION,                                       -
              TIMEN=1,                                                 -
              TIME#1=('07:00','19:00'),                                -
              CKWEEK=*EXCLUSION,                                       -
              SA=*YES,                                                 -
              SU=*YES
        MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
        BE    ENDE
*
*       ************************************************************
*       * Fehlerbehandlung
*       ************************************************************
*
RCNOTOK EQU   *
*       Die moeglichen Returncode-Werte sind im Makro MSGGUAD
*       aufgelistet
        B     ENDE
*
ENDE    EQU   *
        TERM
*
```

```
*        ************************************************************
*        *----------------------------------------------------------*
*        * Parameterdeklarationen                                   *
*        *----------------------------------------------------------*
*        ************************************************************
*
*        Dieser Parameterbereichs wird bei Aufruf des Makros MODSAC
*        im Register 1 uebergeben.
*
PARMACC  DS    OF
         MODSAC MF=C
*
*        Dieser Parameterbereich wird vor Aufruf des Makros MODSAC
*        verwendet, um den Parameterbereich PARMACC neu zu
*        initialisieren.
*
PARMACL  DS    OF
         MODSAC MF=L,                                              -
               ACTION=*ADD,                                        -
               GUARD='                                    '
*
*        ************************************************************
*        *----------------------------------------------------------*
*        * Deklarationen der Returncodes                           *
*        *----------------------------------------------------------*
*        ************************************************************
*
         MSGGUAD MF=D
*
*        ************************************************************
*        *----------------------------------------------------------*
*        * Deklarationen globaler Variablen                         *
*        *----------------------------------------------------------*
*        ************************************************************
*
         SACMGMT MF=D,XPAND=PARAM
*
         END
```

Ergebnis

Nach Ablauf des Programms hat das erzeugte Guard TEST-GUA folgenden Inhalt:

```
:PUB1:$TESTUID.TEST-GUA
   User   ANNE     has ADMISSION
   User   JOHN     has ADMISSION
   User   MARY
    Weekday   IN ( MO, WE, TH )
   User   PAUL
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  REVIEWER
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-02,2017-09-03> )
   Group  TEAMWORK
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-02,2017-09-03> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
```

Beispiel 2: Zugriffsbedingungen ändern

Die Voraussetzungen von Beispiel 1 haben sich folgendermaßen geändert.

1. Die Mitarbeiterin ANNE hat Urlaub vom 15. Oktober bis 15. November 2017. Während dieser Zeit wird ihr der Dateizugriff verboten.
2. Die Teilzeitmitarbeiterin MARY verlagert ihre Arbeitszeit auf Montag, Dienstag und Mittwoch.
3. Der für den 3./4. September vorgesehene Review wird auf den 07./08. September verschoben.

Das in Beispiel 1 erzeugte Guard TEST-GUA soll nun an die neuen Gegebenheiten angepasst werden.

Lösung

```
*         ************************************************************
*         * ---------------------------------------------------------- *
*         *                                                            *
*         * Makro MODSAC: Zugriffsbedingungen aendern                 *
*         * ========================================                   *
*         *                                                            *
*         * ---------------------------------------------------------- *
*         ************************************************************
*
```

```
GUA2     CSECT
*
*        ************************************************************
*        * ---------------------------------------------------------- *
*        * Makro MOVE                                                 *
*        * ==========                                                 *
*        * Aufgabe: Move Parameterbereich PARMACL nach PARMACC.       *
*        * Zweck:   Mit diesem Makro wird vor jedem Aufruf des        *
*        *          Makros MODSAC der in Register 1 zu uebergebende  *
*        *          Parameterbereich PARMACC neu initialisiert.      *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
MACRO
         MOVE

         LA    R@TO,PARMACC
         LA    R@TOL,PROY#
         LA    R@FR,PARMACL
         LA    R@FRL,PROY#
         ICM   R@FRL,8,=C' '
         MVCL  R@TO,R@FR
         MEND
*
*        ************************************************************
*
R@TO     EQU   6               Zieladresse
R@TOL    EQU   7               Zielfeldlaenge
R@FR     EQU   8               Quelladresse
R@FRL    EQU   9               Quellfeldlaenge / Fuellzeichen
R@BASE   EQU   10              Basisregister
         BALR  R@BASE,0
         USING *,R@BASE
*
```

```
*       ************************************************************
*       * 1. Die Mitarbeiterin ANNE hat Urlaub vom                 *
*       *    15. Oktober bis 15. November 2017. Waehrend dieser Zeit *
*       *    wird ihr der Dateizugriff verboten.                   *
*       ************************************************************
*
        MOVE                                  Parameterinitialisierung
        MODSAC MF=M,                                                  -
              ACTION=*MODIFY,                                         -
              GUARD='TEST-GUA',                                       -
              SUBTYPE=*USER,                                          -
              SUBIDS=('ANNE    '),                                    -
              ADMISS=*PARAMS,                                         -
              CKDATE=*EXCLUSION,                                      -
              DATEN=1,                                                -
              DATE#1=('2017-10-15','2017-11-15')
       MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
*       ************************************************************
*       * 2. Die Teilzeitmitarbeiterin MARY verlagert ihre         *
*       *    Arbeitszeit auf Montag, Dienstag und Mittwoch.       *
*       ************************************************************
*
        MOVE                                  Parameterinitialisierung
        MODSAC MF=M,                                                  -
              ACTION=*MODIFY,                                         -
              GUARD='TEST-GUA',                                       -
              SUBTYPE=*USER,                                          -
              SUBIDS='MARY    ',                                      -
              ADMISS=*PARAMS,                                         -
              CKWEEK=*ADMISSION,                                      -
              MO=*YES,                                                -
              TU=*YES,                                                -
              WE=*YES
       MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
```

```
*       ************************************************************
*       * 3. Der fuer den 2./3. September vorgesehene Review wird    *
*       *    auf den 09./10. September verschoben.                   *
*       *                                                            *
*       * Hinweis:                                                   *
*       * Der Wert fuer DATE#1 muss angegeben werden, weil die       *
*       * Zugriffsbedingungen DATE nur als Ganzes geaendert werden   *
*       * kann. Das Aendern einzelner Datumsintervalle ist nicht     *
*       * moeglich.                                                  *
*       ************************************************************
*
        MOVE                                  Parameterinitialisierung
        MODSAC MF=M,                                                  -
              ACTION=*MODIFY,                                         -
              GUARD='TEST-GUA',                                       -
              SUBTYPE=*GROUP,                                         -
              SUBIDS=('TEAMWORK','REVIEWER'),                         -
              ADMISS=*PARAMS,                                         -
              CKDATE=*ADMISSION,                                      -
              DATEN=2,                                                -
              DATE#1=('2017-08-23','2017-08-24'),                     -
              DATE#2=('2017-09-09','2017-09-10')
       MODSAC MF=E,PARAM=PARMACC
        CLC   PROYMRET,=Y(PROPSUCC)
        BNE   RCNOTOK
*
        BE    ENDE
*
*       ************************************************************
*       * Fehlerbehandlung
*       ************************************************************
*
RCNOTOK EQU   *
*       Die moeglichen Returncode-Werte sind im Makro MSGGUAD
*       aufgelistet
        B     ENDE
*
ENDE    EQU   *
        TERM
*
*
*
```

```
*       ************************************************************
*       *------------------------------------------------------------*
*       * Parameterdeklarationen                                    *
*       *------------------------------------------------------------*
*       ************************************************************
*
*       Dieser Parameterbereichs wird bei Aufruf des Makros MODSAC
*       im Register 1 uebergeben.
*
PARMACC  DS    OF
         MODSAC MF=C
*
*       Dieser Parameterbereich wird vor Aufruf des Makros MODSAC
*       verwendet, um den Parameterbereich PARMACC neu zu
*       initialisieren.
*
PARMACL  DS    OF
         MODSAC MF=L,                                              -
               ACTION=*MODIFY,                                     -
               GUARD='                                    '
*
*       ************************************************************
*       *------------------------------------------------------------*
*       * Deklarationen der Returncodes                            *
*       *------------------------------------------------------------*
*       ************************************************************
*
         MSGGUAD MF=D
*
*       ************************************************************
*       *------------------------------------------------------------*
*       * Deklarationen globaler Variablen                          *
*       *------------------------------------------------------------*
*       ************************************************************
*
         SACMGMT MF=D,XPAND=PARAM
*
         END
```

Ergebnis

Nach Ablauf des Programms hat das geänderte Guard TEST-GUA folgenden Inhalt:

```
:PUB1:$TESTUID.TEST-GUA
   User   ANNE
    Date      EX ( <2017-10-15,2017-11-15> )
   User   JOHN     has ADMISSION
   User   MARY
    Weekday   IN ( MO, TU, WE )
   User   PAUL
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  REVIEWER
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-09,2017-09-10> )
   Group  TEAMWORK
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-09,2017-09-10> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
```

Beispiel 3: Zugriffsbedingung löschen

Das im Beispiel 1 erzeugte und in Beispiel 2 geänderte Guard TEST-GUA muss ein weiteres Mal geändert werden:

– Der Mitarbeiter JOHN verlässt die Firma. Seine Zugriffsbedingungen sollen aus dem Guard entfernt werden.

Lösung

```
*        ************************************************************
*        * ---------------------------------------------------------- *
*        *                                                            *
*        * Makro REMSAC: Zugriffsbedingungen entfernen               *
*        * ==========================================                 *
*        *                                                            *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
GUA3     CSECT
*
*        ************************************************************
*        * ---------------------------------------------------------- *
*        * Makro MOVE                                                 *
*        * ==========                                                 *
*        * Aufgabe: Move Parameterbereich PARRACL nach PARRACC.       *
*        * Zweck:   Mit diesem Makro wird vor jedem Aufruf des        *
*        *          Makros REMSAC der in Register 1 zu uebergebende   *
*        *          Parameterbereich PARRACC neu initialisiert.       *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
         MACRO
         MOVE

         LA    R@TO,PARRACC
         LA    R@TOL,PROX#
         LA    R@FR,PARRACL
         LA    R@FRL,PROX#
         ICM   R@FRL,8,=C' '
         MVCL  R@TO,R@FR
         MEND
*
*        ************************************************************
```

```
*
R@TO     EQU   6               Zieladresse
R@TOL    EQU   7               Zielfeldlaenge
R@FR     EQU   8               Quelladresse
R@FRL    EQU   9               Quellfeldlaenge / Fuellzeichen
R@BASE   EQU   10              Basisregister
         BALR  R@BASE,0
         USING *,R@BASE
*
*        ***************************************************************
*        * 1. Der Mitarbeiter JOHN verlaesst die Firma. Seine         *
*        *    Zugriffsbedingungen werden aus dem Guard entfernt.      *
*        ***************************************************************
*
         MOVE                                  Parameterinitialisierung
         REMSAC MF=M,                                                  -
               GUARD='TEST-GUA',                                       -
               SUBTYPE=*USER,                                          -
               SUBIDS=('JOHN    ')
         REMSAC MF=E,PARAM=PARRACC
         CLC   PROXMRET,=Y(PROPSUCC)
         BNE   RCNOTOK
*
         BE    ENDE
*
*        ***************************************************************
*        * Fehlerbehandlung
*        ***************************************************************
*
RCNOTOK  EQU   *
*        Die moeglichen Returncode-Werte sind im Makro MSGGUAD
*        aufgelistet
         B     ENDE
*
ENDE     EQU   *
         TERM
*
*
*
```

```
*       ************************************************************
*       *----------------------------------------------------------*
*       * Parameterdeklarationen                                  *
*       *----------------------------------------------------------*
*       ************************************************************
*
*       Dieser Parameterbereichs wird bei Aufruf des Makros REMSAC
*       im Register 1 uebergeben.
*
PARRACC  DS    OF
         REMSAC MF=C
*
*       Dieser Parameterbereich wird vor Aufruf des Makros REMSAC
*       verwendet, um den Parameterbereich PARRACC neu zu
*       initialisieren.
*
PARRACL  DS    OF
         REMSAC MF=L,                                              -
               SUBTYPE=*USER,                                      -
               GUARD='                                  '
*
*       ************************************************************
*       *----------------------------------------------------------*
*       * Deklarationen der Returncodes                           *
*       *----------------------------------------------------------*
*       ************************************************************
*
         MSGGUAD MF=D
*
*       ************************************************************
*       *----------------------------------------------------------*
*       * Deklarationen globaler Variablen                        *
*       *----------------------------------------------------------*
*       ************************************************************
*
         SACMGMT MF=D,XPAND=PARAM
*
         END
```

Ergebnis

Nach Ablauf des Programms hat das geänderte Guard TEST-GUA folgenden Inhalt:

```
:PUB1:$TESTUID.TEST-GUA
   User   ANNE
    Date      EX ( <2017-10-15,2017-11-15> )
   User   MARY
    Weekday   IN ( MO, TU, WE )
   User   PAUL
    Date      IN ( <2017-07-01,2017-09-30> )
   Group  REVIEWER
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-09,2017-09-10> )
   Group  TEAMWORK
    Time      IN ( <09:00,15:00> )
    Date      IN ( <2017-08-23,2017-08-24> ,
                   <2017-09-09,2017-09-10> )
   Alluser
    Time      IN ( <07:00,19:00> )
    Weekday   EX ( SA, SU )
```

Beispiel 4: Zugriffsbedingungen anzeigen

Die Zugriffsbedingungen im Guard TEST-GUA, das im Beispiel 1 erstellt und in den Beispielen 2 und 3 geändert wurde, sollen mit dem Makro SHWSAC gelesen, aufbereitet und nach SYSOUT ausgegeben werden.

Lösung

```
*        ************************************************************
*        * ---------------------------------------------------------- *
*        *                                                            *
*        * Makro SHWSAC: Zugriffsbedingungen anzeigen                 *
*        * ==========================================                 *
*        *                                                            *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
GUA4     CSECT
*
*        ************************************************************
*        * ---------------------------------------------------------- *
*        * Makro WRITE                                                *
*        * ===========                                                *
*        * Aufgabe: Ausgabe des Datensatzes WROBER nach WROUT und     *
*        *          den Bereich WROBER wieder mit Blanks              *
*        *          initialisieren.                                   *
*        * ---------------------------------------------------------- *
*        ************************************************************
*
         MACRO
         WRITE

         BAL   R@BACK,OUTOUT
         MEND
*
*        ************************************************************
*
R@WEEK   EQU   2              fuer Weekday-Bearbeitung
R@PRGNAM EQU   2              fuer Program-Bearbeitung
R@USED   EQU   2              fuer Vergleich bereich mit R@OUT
R@I      EQU   3              Schleifenzaehler
R@CON    EQU   4              Basisregister fuer Condition
R@OUT    EQU   5              Basisregister fuer Ausgabebereich
R@BASE   EQU   10             Basisregister
R@GUA    EQU   11             Subjekt-Zaehler
R@BACK   EQU   14             Ruecksprungadresse
*
```

```
BALR  R@BASE,0
         USING *,R@BASE
*
*        ***************************************************************
*        * Initialisierung                                             *
*        ***************************************************************
         MVC   WROGNAM(WROTEXL),SPACES         Ausgabebereich loeschen
         MVC   PARSACC(PROW#),PARSACL          Parameterinitialisierung
         SHWSAC MF=M,                                                  -
               GUARD='TEST-GUA',                                       -
               SUBTYPE=*ALL,                                           -
               INFORM=*ADM,                                            -
               OUTAREA=(OUTBER,OUTBERLG)
*
*        ***************************************************************
*        * Zugriffsbedingungen ermitteln, bis keine weiteren Guards   *
*        * mehr angezeigt werden. In diesem Beispiel wird jedoch      *
*        * nur das eine Guard TEST-GUA angefordert.                   *
*        ***************************************************************
MORE1    EQU   *
         SHWSAC MF=E,PARAM=PARSACC
         CLC   PROWMRET,=Y(PROPSUCC)
         BNE   RCNOTOK
*
*        ***************************************************************
*        * Ausgabebereich abarbeiten                                   *
*        ***************************************************************
         L     R@OUT,PROWOADR       Laden SHWSAC-Ausgabebereiches
         USING PROWOPUT,R@OUT
*
         LA    R@OUT,PROWOSGC       Positionieren auf (erstes) Guard
         USING PROWGCON,R@OUT
*
ONEGUARD EQU   *
         MVC   WROGNAM,PROWGCNA     Guardname -> WROUT-Bereich
         LA    R@OUT,PROWGCSA       Positionieren auf 1. Subjekttyp
         USING PROWACOS,R@OUT
*
```

```
*       ***************************************************************
*       * Schleife ueber Subjekttyp *USER, *GROUP, *OTHERS, *ALLUSER *
*       ***************************************************************
        SR    R@GUA,R@GUA
        LH    R@GUA,PROWAAUN       *USER
        AH    R@GUA,PROWAAGN       *GROUP
        AH    R@GUA,PROWAAON       *OTHERS
        AH    R@GUA,PROWAAAN       *ALLUSER
*
        LA    R@OUT,PROWACS        Positionieren auf erstes Subjekt
        USING PROWACON,R@OUT
*
*       ***************************************************************
*       * Fuer jedes Subjekt die Zugriffsbedingungen aus dem          *
*       * Ausgabebereich lesen                                       *
*       * Loop-Beginn                                                *
*       ***************************************************************
MORE2   EQU   *
*
*       ***************************************************************
*       * Subjekt und Subjekttyp in den WROUT-Bereich schreiben
*       ***************************************************************
        CLI   PROWAITY,PROZSUSR
        BNE   SBJGRP
        MVC   WROSTYP,=C'USER    ' Type USER    -> WROUT-Bereich
        MVC   WROSNAM,PROWAINA     Subject      -> WROUT-Bereich
        B     SBJEND
SBJGRP  CLI   PROWAITY,PROZSGRP
        BNE   SBJOTH
        MVC   WROSTYP,=C'GROUP   ' Type GROUP   -> WROUT-Bereich
        MVC   WROSNAM,PROWAINA     Subject      -> WROUT-Bereich
        B     SBJEND
SBJOTH  CLI   PROWAITY,PROZSOTH
        BNE   SBJALL
        MVC   WROSTYP,=C'OTHERS  ' Type OTHERS  -> WROUT-Bereich
        B     SBJEND
SBJALL  MVC   WROSTYP,=C'ALLUSERS' Type ALLUSER -> WROUT-Bereich
SBJEND  EQU   *
*
```

```
*        ***************************************************************
*        * Im Testguard sind fuer alle Subjekte spezielle             *
*        * Zugriffsbedingungen mit ADMISSION=*PARAMS                  *
*        * (d.h. mit PROWAADM=PROZAPAR)spezifiziert                   *
*        * Der Fall ADMISSION=*YES/*NO                                *
*        * (d.h. mit PROWAADM=PROZAYES/PROZANO) wird nicht behandelt. *
*        ***************************************************************
         LA    R@OUT,PROWSTCO       Positionieren auf Time Condition
*
*        ***************************************************************
*        * TIME Condition                                             *
*        ***************************************************************
         USING PROWTCON,R@OUT
         CLI   PROWTKD,PROZCNO      Kind of Time EQ *ANY?
         BNE   TIMCYCLA
         LA    R@OUT,PROWT#IN       Positionieren auf Interval
         B     TIMEND
TIMCYCLA EQU   *
         CLI   PROWTKD,PROZCEXC     Kind of Time EXCEPT(TIME=?)
         BNE   TIMCYCLB
         MVC   WROINEX,=C'EX '      EX -> WROUT-Bereich
TIMCYCLB EQU   *
         MVC   WROINEX,=C'IN '      IN -> WROUT-Bereich
         SR    R@I,R@I
         IC    R@I,PROWT#IN
         LA    R@OUT,PROWTINS
         USING PROWTINT,R@OUT
TIMCYCL  EQU   *
         MVC   WROTIML,PROWTILB     Time Lower Bound -> WROUT-Bereich
         MVC   WROTIMU,PROWTIUB     Time Upper Bound -> WROUT-Bereich
         LA    R@OUT,PROWTIN#(R@OUT)
*
*        * Time Condition nach WROUT schreiben
         WRITE
*
         BCT   R@I,TIMCYCL          Naechstes Zeitinterval
TIMEND   EQU   *
*
```

```
*        ************************************************************
*        * DATE Condition                                           *
*        ************************************************************
         USING PROWDCON,R@OUT
         CLI   PROWDKD,PROZCNO      Kind of Date EQ *ANY?
         BNE   DATCYCLA
         LA    R@OUT,PROWD#IN       Positionieren auf Interval
         B     DATEND
DATCYCLA EQU   *
         CLI   PROWDKD,PROZCEXC     Kind of Date EXCEPT(TIME=?)
         BNE   DATCYCLB
         MVC   WROINEX,=C'EX '      EX -> WROUT-Bereich
DATCYCLB EQU   *
         MVC   WROINEX,=C'IN '      IN -> WROUT-Bereich
         SR    R@I,R@I
         IC    R@I,PROWD#IN
         LA    R@OUT,PROWDINS
         USING PROWDINT,R@OUT
DATCYCL  EQU   *
         MVC   WRODATL,PROWDILB     Date Lower Bound -> WROUT-Bereich
         MVC   WRODATU,PROWDIUB     Date Upper Bound -> WROUT-Bereich
         LA    R@OUT,PROWDIN#(R@OUT)
*
*        * Date Condition nach WROUT schreiben
         WRITE
*
         BCT   R@I,DATCYCL          Naechstes Zeitinterval
DATEND   EQU   *
*
```

```
*        ************************************************************
*        * WEEKDAY Condition                                        *
*        ************************************************************
         USING PROWWCON,R@OUT
         CLI   PROWWKD,PROZCNO      Kind of Weekday EQ *ANY?
         BNE   WEKCYCLA
         LA    R@OUT,PROWWDYS       Positionieren auf Weekdays
         B     WEKEND
WEKCYCLA EQU   *
         CLI   PROWWKD,PROZCEXC     Kind of Wekday EXCEPT(WEEKDAY=?)
         BNE   WEKCYCLB
         MVC   WROINEX,=C'EX '      EX -> WROUT-Bereich
WEKCYCLB EQU   *
*
*        Alle Wochentage im Ausgabefeld vorbesetzen
*        In einer Schleife die vorbesetzen Wochentage mit Blank
*        ueberschreiben, wenn sie nicht in der Zugriffsbedingung
*        enthalten sind
*
         MVC   WROWEEK,=C'MO TU WE TH FR SA SU '
         IC    R@I,=X'08'
         ICM   R@CON,B'1000',PROWWDYS
         LA    R@WEEK,WROWEEK
         USING WEKDSEC,R@WEEK
WEKCYCL  EQU   *
         BM    WEKCYCLC
         MVC   WEEKDAY,SPACES
WEKCYCLC EQU   *
         LA    R@WEEK,WEEKDAY#
         SLL   R@CON,1
         LTR   R@CON,R@CON
         BCT   R@I,WEKCYCL
         LA    R@OUT,PROWW#(R@OUT)
*
*        * Weekday Condition nach WROUT schreiben
         WRITE
*
WEKEND   EQU   *
*
```

```
*        ************************************************************
*        * PRIVILEGE Condition                                       *
*        * Die Behandlung der einzelnen Privilegien wird im Beispiel  *
*        * nicht ausfuehrlich behandelt, sondern es wird gleich weiter*
*        * auf die Zugriffsbedingungen PROGRAM ppositioniert.        *
*        ************************************************************
         USING PROWPVCO,R@OUT
         CLI   PROWPKD,PROZCNO      Kind of Privilege EQ *ANY?
         BNE   PRVCYCLA
         LA    R@OUT,PROWPRV        Positionieren auf Privilegien
         B     PRVEND
PRVCYCLA EQU   *
         LA    R@OUT,PROWP#(R@OUT)  -> Zugriffsbedingung Typ PROGRAM
PRVEND   EQU   *
*
```

```
*        ************************************************************
*        * PROGRAM Condition                                        *
*        ************************************************************
         USING PROWPCON,R@OUT
         CLI   PROWPCKD,PROZCNO     Kind of Program EQ *ANY?
         BNE   PRGCYCLA
         LA    R@OUT,PROWPCNP       Positionieren auf Anzahl Programs
*        LA    R@OUT,PROWPCPS       Positionieren auf Programs
         B     PRGEND
PRGCYCLA EQU   *
         SR    R@I,R@I
         IC    R@I,PROWPCNP         Anzahl Programmnamen
         LA    R@OUT,PROWPCPS       Programmname
         USING PROWPRG,R@OUT
PRGCYCL  EQU   *
*
*        Im Beispiel wird nur der Fall FILENAME behandelt
*        Bibliotheksangaben werden nicht beruecksichtigt
*
         SR    R@PRGNAM,R@PRGNAM
         IC    R@PRGNAM,PROWPAL#    size of whole program name
         SH    R@PRGNAM,=H'1'    -1 fuer MVC-Laenge
         N     R@PRGNAM,=F'63'      Name auf 64 begrenzt
         EX    R@PRGNAM,PRGEXMVC    Programname ->WROUT-Bereich
         AH    R@PRGNAM,=H'1'    +1 fuer echte Laenge
*
*        * Program Condition nach WROUT schreiben
         WRITE
*
         LA    R@OUT,PROWPCNS       Start of Programs
         AR    R@OUT,R@PRGNAM
         BCT   R@I,PRGCYCL
PRGEND   EQU   *
*
*        ************************************************************
*        * Alle Zugriffsbedingungen fuer ein Subjekt sind abgearbeitet*
*        * Auf Wortgrenze Positionieren                             *
*        ************************************************************
         AH    R@OUT,=H'3'
         N     R@OUT,=F'-4'         X'FFFFFFFC'
*
```

```
*        ***************************************************************
*        * Fuer jedes Subjekt die Zugriffsbedingungen aus dem          *
*        * Ausgabebereich lesen                                        *
*        * Loop-Ende                                                   *
*        ***************************************************************
         BCT   R@GUA,MORE2
         B     GUAFRTG
*
*        ***************************************************************
*        * Ein Guard wurde komplett abgearbeitet. Pruefen, ob es       *
*        * im SHWSAC-Ausgabebereich weitere Guardeintraege  gibt.      *
*        * In diesem Beispiel gibt es keine.                           *
*        ***************************************************************
GUAFRTG  EQU   *
         L     R@USED,PROWOADR
         A     R@USED,PROWOUS#
         CR    R@USED,R@OUT
         BP    ONEGUARD
*
*        ***************************************************************
*        * Pruefen, ob SHWSAC gemeldet hat, dass weitere Guards        *
*        * zur Anzeige anstehen, die im Ausgabebereich keinen Platz    *
*        * mehr gefunden haben.                                        *
*        ***************************************************************
         CLC   PROWOMOR,=Y(PROWMNO)
         BNE   MORE1
         B     ENDE
*
*        ***************************************************************
*        * Aufruf von WROUT                                            *
*        ***************************************************************
OUTOUT   EQU   *
         WROUT WROBER,WROFEHL
         MVC   WROGNAM(WROTEXL),SPACES
         BR    R@BACK
WROFEHL  EQU   *
         B     ENDE
*
*        ***************************************************************
*        * Fehlerbehandlung                                            *
*        ***************************************************************
RCNOTOK  EQU   *
*        Die moeglichen Returncode-Werte sind im Makro MSGGUAD
*        aufgelistet
         B     ENDE
*
```

```
*        ***************************************************************
*        * Uebertragen Programmname in den WROUT-Ausgabebereich       *
*        ***************************************************************
PRGEXMVC MVC   WROPRGNA(1),PROWPCNS   Start of Programs
*
*        ***************************************************************
*        * Programmende von Beispielprogramm GUA4                      *
*        ***************************************************************
ENDE     EQU   *
         TERM
*
*
*
*        ***************************************************************
*        *-------------------------------------------------------------*
*        * Parameterdeklarationen                                      *
*        *-------------------------------------------------------------*
*        ***************************************************************
*
*        Dieser Parameterbereichs wird bei Aufruf des Makros SHWSAC
*        im Register 1 uebergeben.
*
PARSACC  DS    OF
         SHWSAC MF=C
*
*        Dieser Parameterbereich wird vor Aufruf des Makros SHWSAC
*        verwendet, um den Parameterbereich PARRACC neu zu
*        initialisieren.
*
PARSACL  DS    OF
         SHWSAC MF=L,                                                  -
               GUARD='                                    '            -
               OUTAREA=(OUTBER,OUTBERLG)
*
OUTBERLG DC    A(OUTBERL)
*
```

```
*        ************************************************************
*        *----------------------------------------------------------*
*        * WROUT-Bereich                                            *
*        *----------------------------------------------------------*
*        ************************************************************
*
SPACES   DC   CL256' '
WROBER   EQU   *
         DC    Y(WROBERL)
         DC    X'0000'
         DC    X'00'
WROGNAM  DS    CL24                          Guardname
         DS    XL1
WROSTYP  DS    CL8                           Subjekttyp
         DS    XL1
WROSNAM  DS    CL8                           Subjekt
         DS    XL1
WROINEX  DS    CL3                           INTERVAL oder EXCEPT
         DS    XL1
WROTIML  DS    CL5                           Time Lower Bound
         DS    XL1
WROTIMU  DS    CL5                           Time Upper Bound
         ORG   WROTIML
WRODATL  DS    CL10                          Date Lower Bound
         DS    XL1
WRODATU  DS    CL10                          Date Upper Bound
         ORG   WROTIML
WROWEEK  DS    CL21                          Weekday
         ORG   WROTIML
WROPRGNA DS    CL64                          Programmname
         ORG
WROTEXL  EQU   *-WROGNAM
WROBERL  EQU   *-WROBER
*
```

```
*        ************************************************************
*        *----------------------------------------------------------*
*        * Ausgabebereich fur SHWSAC                               *
*        *----------------------------------------------------------*
*        ************************************************************
*
OUTBER   EQU   *
         DS    XL256
         DS    XL256
         DS    XL256
         DS    XL256
         DS    XL256
         DS    XL256
         DS    XL256
         DS    XL256
OUTBERL  EQU   *-OUTBER
*
*        ************************************************************
*        *----------------------------------------------------------*
*        * Deklarationen globaler Variablen                        *
*        *----------------------------------------------------------*
*        ************************************************************
*
         SACMGMT MF=D,XPAND=PARAM
*
*        ************************************************************
*        *----------------------------------------------------------*
*        * Deklarationen des Ausgabebereiches von SHWSAC           *
*        *----------------------------------------------------------*
*        ************************************************************
*
         SHWSAC MF=D,XPAND=OUTPUT
*
*        ************************************************************
*        *----------------------------------------------------------*
*        * Deklarationen der Returncodes                           *
*        *----------------------------------------------------------*
*        ************************************************************
*
         MSGGUAD MF=D
*
WEKDSEC  DSECT  OX     Weekday-Dsect
WEEKDAY  DS    CL3
WEEKDAY# EQU   *
*
         END
```

Ergebnis

Das Programm gibt die Zugriffsbedingungen in folgender Form nach SYSOUT aus:

```
:PUB1:$TESTUID.TEST-GUA  USER     ANNE     IN  2017-10-15 2017-11-15
                         USER     MARY         MO TU WE
                         USER     PAUL     IN  2017-07-01 2017-09-30
                         GROUP    REVIEWER IN  09:00 15:00
                                           IN  2017-08-23 2017-08-24
                                               2017-09-09 2017-09-10
                         GROUP    TEAMWORK IN  09:00 15:00
                                           IN  2017-08-23 2017-08-24
                                               2017-09-09 2017-09-10
                         ALLUSERS           IN  07:00 19:00
                                            EX                SA SU
```

5.12.2 Makro-Syntax für GUARDS-Makros

Die Makro-Operanden können in zwei Gruppen eingeteilt werden:

– Formatoperanden, die die Form und die Generierung des Makros festlegen; Formatoperanden sind im Handbuch „Makroaufrufe an den Ablaufteil“ [16] beschrieben. Ihre Metasyntax entspricht der üblichen von BS2000-Makro-Formatoperanden.

– Funktionsoperanden, die schnittstellenspezifisch den Inhalt des Parameterbereichs festlegen.

Die Metasyntax der Funktionsoperanden und deren Werte sind in diesem Abschnitt beschrieben.

Beschreibung eines Funktionsoperanden

Die Beschreibung eines Funktionsoperanden hat die folgende Form:

operandenname = operandenwerte

Operanden mit Standardwerten sind optional. Operanden, die keinen Standardwert besitzen, sind für die Form MF=L Pflichtoperanden. Ausnahmen finden sich bei der Beschreibung der Operanden.

Operandenwerte können direkt oder indirekt angegeben werden. Bei der direkten Angabe wird der Wert als Literal oder als Schlüsselwort angegeben. Bei der indirekten Angabe wird der Wert über eine Variable oder in einem Register übergeben.

Direkte Angabe

Die Datentypen der Operandenwerte werden in spitzen Klammern eingeschlossen:

operandenname = <datentyp n..m>

operandenname = <c-string: sdf-datentyp n..m>

Der Zusatz n..m zu Datentypen ermöglicht die Angabe eines zulässigen Wertebereichs oder einer zulässigen Länge. Wenn für den Datentyp ein Wertebereich angegeben ist, gilt dieser auch für die Variablen- oder Registerangabe und wird dort nicht erneut angegeben.

Beispiel

im Syntaxdiagramm:	TYPE=<integer 0..255>
bei der Eingabe:	TYPE=100
im Syntaxdiagramm:	NAME=<c-string: filename 1..40>
bei der Eingabe:	NAME='MYGUARD'

Variable Angabe

Wenn als Operandenwert auch eine Variable angegeben werden kann, wird der Typ der Variablen in spitze Klammern eingeschlossen und mit „var:“ eingeleitet. Dies bedeutet, dass der Inhalt der Variable dem angegebenen Typ entsprechen muss. Bei der Eingabe ist nur der Variablenname (Bezeichner) anzugeben.

operandenname = <var: variablentyp(n)>

Beispiel

im Syntaxdiagramm: NAME=<var: char(24)>

bei der Eingabe: NAME=MYGUARD

Dabei ist MYGUARD der Bezeichner für das Datenfeld der Länge 24, in dem der Name abgelegt ist.

Der Zusatz n in runden Klammern bezeichnet die Länge des Datenfelds.

Registerangabe

Wenn als Wert eines Operanden auch eine (in Klammern stehende) Registerangabe möglich ist, müssen zwei Fälle unterschieden werden:

Das Register enthält den Wert direkt:

operandenname = (<reg: variablentyp(n)>)

Beispiel

im Syntaxdiagramm: TYPE=(<reg: integer(1)>)

bei der Eingabe: TYPE=(9)
Dabei enthält Register 9 die entsprechende Zahl

Das Register enthält die Adresse, die auf das Datenfeld zeigt, in dem der Wert zu finden ist:

operandenname = (<reg: A(variablentyp(n))>)

Beispiel

Im Syntaxdiagramm: IOAREA=(reg: A(<char(8)>))

bei der Eingabe: IOAREA=(9)
wobei Register 9 die Adresse des Bereichs enthält.

Elemente der Metasyntax

Kennzeichen	Beschreibung
GROSSBUCHSTABEN	Großbuchstaben bezeichnen Schlüsselwörter oder Konstanten, die in dieser Form vom Benutzer angegeben werden müssen. Schlüsselwörter beginnen mit *. Beispiel: DIALOG=*STD
Kleinbuchstaben	Kleinbuchstaben bezeichnen Typen der Werte oder Variablen, die vom Benutzer angegeben werden können. Beispiel: NAME=<var:char(40)>
Unterstreichung	Der Unterstrich kennzeichnet den Standardwert eines Operanden für MF=L. Beispiel: DIALOG=*STD
Gleichheitszeichen =	Das Gleichheitszeichen „=“ trennt den Operanden vom Operandenwert.
Schrägstrich /	Der Schrägstrich trennt einfache alternative Operandenwerte. Beispiel: DIALOG=*STD / *NO
< >	Spitze Klammern kennzeichnen den Datentyp des Operanden. Beispiel: <var:char(40)>
list-poss(n):	Aus den Operandenwerten, die list-poss folgen, kann eine Liste gebildet werden. n beschreibt die maximale Anzahl Elemente in der Liste. Die Liste muss in runde Klammern eingeschlossen werden, falls mehr als ein Element angegeben wird. Beispiel: list-poss(3): *YOU / *HE / *US
structure(n):	Der Operandenwert besteht aus einer Liste von n Werten unterschiedlicher Bedeutung (vergl. array). Die Bedeutung der Werte ist von ihrer Stellung in der Liste abhängig. Der Datentyp der einzelnen Elemente wird unter „(m) elementbezeichner:“ beschrieben. Die Liste muss in runden Klammern eingeschlossen sein. Beispiel: CHKPROC=structure(2):
(m) elementbezeichner:	Beschreibt das m-te Element einer „structure“-Liste. „elementbezeichner“ beschreibt die Bedeutung des Elements in der structure-Liste. Beispiel: (1) name: <c-string 32> (2) address: A(<name>) name und address sind hier die Elementbezeichner.
array(n):	Der Operandenwert besteht aus einer Liste von maximal n gleichartigen Elementen. Die Liste muss in runde Klammern eingeschlossen sein, falls sie mehr als ein Element hat.

Datentypen der Operandenwerte

Datentyp	Zeichenvorrat	Besonderheiten
c-string	EBCDIC-Zeichen	ist in Hochkommata einzuschließen und ohne einleitendes „C“ anzugeben. Hochkommata in der Zeichenkette sind doppelt anzugeben. Eine inhaltliche Bedeutung der Angabe wird anschließend in SDF-Schreibweise angegeben, abgetrennt durch Doppelpunkt. Der Zusatz n..m beschreibt die Eingabelänge. Beispiel: im Syntaxdiagramm: GUARD=<c-string: filename 1..54> bei der Eingabe: GUARD='GUARDEXA'
x-string	Sedezimal 00..FF	Ist in Hochkommata einzuschließen, der Buchstabe X muss vorangestellt werden: X'xxxx'. Der Zusatz n..m beschreibt die maximale Eingabelänge in Bytes Beispiel: im Syntaxdiagramm: PASSWORD=<x-string 1..10> bei der Eingabe: PASSWORD=X'FF00AA1122
name	A..Z, 0..9, $, #, @	Bezeichner. Das Format ist der jeweiligen Operandenbeschreibung zu entnehmen. Beispiel: im Syntaxdiagramm: PARAM=<name 1..8> bei der Eingabe: PARAM=MYPARAM
label	A..Z 0..9 $,#,@	Kennzeichnet eine Marke. Beispiel: OUTAREA=structure (2): (1) address: <label>
integer	0..9,+,-	„+“ bzw. „-“ kann nur erstes Zeichen sein. Der Zusatz n..m beschreibt den zulässigen Wertebereich. Beispiel: im Syntaxdiagramm: TIMEN=<integer 1..4> bei der Eingabe: TIMEN=1
var:		Leitet eine variable Angabe ein. Nach dem Doppelpunkt folgt der Datentyp der Variablen. Beispiel: im Syntaxdiagramm: GUARD=<var: char(40)> bei der Eingabe: GUARD=GUARDVAR
reg:		Leitet eine Register-Angabe ein. Nach dem Doppelpunkt folgt der Datentyp des Registerinhalts. Bei der Eingabe kann ein Register oder ein Register-EQUATE verwendet werden.

Datentypen der Variablen und Registerinhalte

Datentyp	Bedeutung
char(n)	Kennzeichnet eine Zeichenkette der Länge n. Fehlt die Längenangabe, wird n=1 angenommen.
integer (n)	Kennzeichnet eine Ganzzahl, die n byte belegt, wobei n<=4 gilt. Fehlt die Längenangabe, wird n=1 angenommen.
enum NAME(n)	Kennzeichnet eine Aufzählung, die n byte belegt, wobei n<=4 gilt. Fehlt die Längenangabe, wird n=1 angenommen.
A(variablentyp(n))	Adresse des Datenfeldes.
pointer	Zeiger (die Adresse wird übergeben).

5.13 Dienstprogramm GUARDS-SAVE

Guards werden pro Pubset in jeweils einem Guardskatalog mit dem Namen $TSOS.SYSCAT.GUARDS verwaltet.

Solange ein Pubset importiert ist, ist der entsprechende Katalog geöffnet, kann aber trotzdem von einem Systemverwalter mit HSMS/ARCHIVE gesichert und von einem Guards-Administrator mit dem Kommando /CHANGE-GUARD-FILE restauriert werden. Eine derartige Sicherung und Restaurierung erfasst jedoch den Guardskatalog immer nur in seiner Gesamtheit. Einzelne Guards können damit nicht gesichert und restauriert werden.

Das Dienstprogramm GUARDS-SAVE erlaubt es im Gegensatz dazu, die im Guardskatalog verwalteten Guards selektiv zu sichern oder zu restaurieren. Die Funktionalität von GUARDS-SAVE steht auch nichtprivilegierten Benutzern zur Verfügung.

Sichern einer auswählbaren Menge von Guards

Ein Anwender kann für jeweils ein Pubset bestimmen, welche Guards in eine benutzereigene Sicherungsdatei gesichert werden sollen. Der Guards-Administrator kann Guards aus dem gesamten Guardbestand für die Sicherung auswählen, jeder andere Benutzer kann nur seine eigenen Guards sichern.

Restaurieren einer auswählbaren Menge von Guards aus einer Sicherungsdatei

Ein Anwender kann festlegen, welche Guards aus einer Sicherungsdatei ins System zurück übertragen werden sollen. Der Guards-Administrator kann diese Guards aus dem gesamten Guardbestand der Sicherungsdatei auswählen, jeder andere Benutzer kann nur seine eigenen Guards restaurieren.

Der Restaurierungsvorgang kann auf zwei Arten ablaufen:

1. Die Guards werden von GUARDS-SAVE unmittelbar und ohne Rückfragen aus dem gesicherten Guardbestand restauriert. Der Anwender hat dabei keinen Einfluss auf den Ablauf des Restaurierungsvorganges.
2. GUARDS-SAVE generiert aus dem gesicherten Guardbestand Kommandos und schreibt diese in eine vom Anwender benannte Prozedurdatei. Der eigentliche Restaurierungsvorgang muss vom Anwender durchgeführt werden, indem er die generierte Prozedurdatei startet. Dadurch besteht die Möglichkeit, den Restaurierungsablauf vorab einzusehen und gegebenenfalls manuell abzuändern.

Anzeigen einer auswählbaren Menge gesicherter Guards

Der Anwender kann sich Guardnamen oder Guardattribute eines mit GUARDS-SAVE gesicherten Guardbestandes anzeigen lassen. Der Guards-Administrator kann für die Anzeige Guards aus dem gesamten Guardbestand der Sicherungsdatei auswählen, jeder andere Benutzer kann sich nur seine eigenen Guards anzeigen lassen.

5.13.1 Berechtigungskonzept

Ein nichtprivilegierter Benutzer darf mit GUARDS-SAVE jeweils nur seine eigenen Guards sichern, restaurieren oder aus einer Sicherungsdatei anzeigen lassen. Ein Guards-Administrator hat Befugnisse über den gesamten Guardbestand im System.

Guards, die aufgrund ihres Attributs `SCOPE=*HOST-SYSTEM` systemweit von allen Benutzern verwendet werden dürfen, werden von GUARDS-SAVE nur dann bearbeitet, wenn der Anwender der Guardeigentümer oder ein Guards-Administrator ist. Diese Berechtigungseinschränkung ist besonders zu beachten, wenn zum Beispiel in Regelbehältern auf Guards (Referenzguards) verwiesen wird, deren Eigentümer sich von denen der Regelbehälter unterscheiden.

Beispiel

Der nichtprivilegierte Benutzer `PETER` kann zwar seine Guards `$PETER.SYS.UCF` und `$PETER.P-ACCESS` sichern, jedoch nicht das Guard `$MARY.M-ACCESS`, obwohl er es in seiner Miteigentümerregel ganz regulär verwenden darf. Die Guards-Administratorin `MARY` hingegen darf alle drei Guards bearbeiten.

```
/show-access-conditions $*.*
%     Guard Name          Scope   Type      Creation Date       LastMod Date
%-------------------------------------------------------------------------------
%:XXXX:$MARY.M-ACCESS     SYS  STDAC    2017-12-10/12:14:02 2017-12-10/12:16:10
%:XXXX:$PETER.P-ACCESS    USR  STDAC    2017-12-10/12:14:07 2017-12-10/12:17:18
%:XXXX:$PETER.SYS.UCF     USR  COOWNERP 2017-12-10/12:14:12 2017-12-10/12:17:43
%-------------------------------------------------------------------------------

/show-coowner-protection-rule $*.*
%-------------------------------------------------------------------------------
%RULE CONTAINER :XXXX:$PETER.SYS.UCF                        COOWNER PROTECTION
%-------------------------------------------------------------------------------
%RULE1          OBJECT      = PETER.*
%               CONDITIONS  = $PETER.P-ACCESS
%               TSOS-ACCESS = SYSTEM-STD
%RULE2          OBJECT      = MARY.*
%               CONDITIONS  = $MARY.M-ACCESS
%               TSOS-ACCESS = SYSTEM-STD
%-------------------------------------------------------------------------------
```

5.13.2 Auswahl der zu bearbeitenden Guards

Guards unterscheiden sich durch ihren Namen und ihren Typ. Der Guardname bewirkt die Eindeutigkeit der Guards auf einem Pubset, der Guardtyp gibt Auskunft über die Art der Daten, die ein Guard enthält. Zum Beispiel sind in Guards des Typs STDAC Zugriffsbedingungen und in Guards des Typs DEFPATTR Standardschutzwerte enthalten.

Bestimmte Guardtypen können Verweise auf weitere Guards (Referenzguards) enthalten. So sind zum Beispiel in Regeln für den Standardschutz (Default protection) die Namen derjenigen Guards aufgeführt, die die erforderlichen Definitionen der Schutzattribut-Defaultwerten enthalten.

GUARDS-SAVE berücksichtigt beim Ermitteln einer Guardmenge mehrere Auswahlkriterien, die der Anwender bestimmen kann:

1. Guardname

   Mit dem Operanden GUARD-NAME wählt der Anwender den Namen eines Guards aus, das bearbeitet werden soll. Wenn der Guardname Musterzeichen enthält, wählt GUARDS-SAVE alle Guards aus, die dem angegebenen Muster entsprechen.

2. Guardtyp

   Mit der Angabe `SELECT=*BY-ATTRIBUTES(TYPE=)` kann der Anwender die mit dem Operanden GUARD-NAME getroffene Auswahl auf bestimmte Guardtypen einschränken. GUARDS-SAVE wählt aus der im ersten Selektionsschritt ermittelten Guardmenge die Guards vom gesuchten Typ aus.

3. Guardreferenzen

   Mit der Angabe `SELECT=*BY-ATTRIBUTES(RESOLVE=*YES)` gibt der Anwender an, ob die in den ersten beiden Selektionsschritte ermittelte Guardmenge nach Referenzguards durchsucht und um die so gefundenen Guards ergänzt werden soll.

   Hierbei werden alle gefundenen Referenzguards wiederum nach Referenzen durchsucht. Eine semantische Prüfung auf Zulässigkeit der Referenzen wird von GUARDS-SAVE jedoch nicht durchgeführt, darum können sowohl zulässige als auch unzulässige Guardreferenzen selektiert werden.

Zulässig sind folgende Guardreferenzen:

Guardzweck	Guardtyp	Referenzzweck	Referenztyp
Regelbehälter für den Standardschutz (Default protection)	DEFAULTP	Spezifikationen der Attribut-Defaultwerte	DEFPATTR
		Spezifikationen der Benutzerkennungen und Benutzergruppen für pubsetglobale Defaultierungen	DEFPUID
Spezifikationen der Attribut-Defaultwerte	DEFPATTR	Lese-, Schreib- Ausführ-Guard, die für den Defaultwert des Schutzattributs GUARDS spezifiziert sind	STDAC
Regelbehälter für den Miteigentümerschutz (Co-owner protection)	COOWNERP	Spezifikationen der Zugriffsbedingungen für die Miteigentümer	STDAC

Die Standardeinstellungen der GUARDS-SAVE-Anweisungen sind so festgelegt, dass die Suche nach Referenzguards durchgeführt wird.

Die implizite Berücksichtigung von Referenzguards sollte bei Sicherungs- und Restaurierungsläufen sinnvollerweise auch dann eingeschaltet bleiben, wenn dabei durch die Angabe `GUARD-NAME=*, SELECT=(TYPE=*ANY)` der komplette Guardbestand ausgewählt wird. Dadurch werden in den Ergebnisprotokollen werden auch Referenzguards aufgelistet, die nicht gefunden wurden. Wird die Suche nach Referenzguards ausgeschaltet `(SELECT=(RESOLVE=*NO))`, werden gegebenenfalls fehlende Guards nicht erkannt.

Folgende Beispiele sollen das in diesem Abschnitt erläuterte Auswahlverfahren verdeutlichen:

Beispiel 1

Es sollen alle Regelbehälter für den Standardschutz gesichert werden, wobei auch die Referenzguards berücksichtigt werden sollen.

Der Anwender macht für die Auswahl der Guards folgende Angaben:

```
GUARD-NAME=SYS.UD*, SELECT=(TYPE=DEFAULTP, RESOLVE=*YES)
```

GUARDS-SAVE führt folgende Selektionsschritte durch:

1. Ermittlung aller Guards, deren Namen mit der Zeichenfolge SYS.UD beginnen.
2. Selektion derjenigen Guards aus der durch Schritt 1 ermittelten Guardmenge, die vom Typ DEFAULTP sind.
3. Rekursives Durchsuchen der in Schritt 1 und 2 ermittelten Guardmenge nach Referenzguards. Die gefundenen Referenzguards werden **zusätzlich** selektiert.

Als Ergebnis dieser Selektion bearbeitet GUARDS-SAVE die Menge aller Guards, deren Namen mit der Zeichenfolge SYS.UD beginnen und vom Guardtyp DEFAULTP sind. Zusätzlich dazu werden aber auch alle Guards gesichert, die von der durch Schritt 1 und Schritt 2 ermittelten Guardmenge referenziert werden und zwar **unabhängig** davon, aus welcher Zeichenfolge sich ihr Name zusammensetzt und welchen Guardtyp sie besitzen. Es gehören zu der selektierten Guardmenge also auch solche Guards, deren Name nicht mit der Zeichenfolge SYS.UD beginnen und deren Guardtyp nicht DEFAULTP ist.

Aus einem Protokoll kann der Anwender ersehen, welche Guards aufgrund ihres Namens und Typs gesichert wurden, welche Guards aufgrund einer Referenz gesichert wurden und welche Guards aufgrund ihrer Referenz gesichert werden müssten, aber nicht gesichert werden konnten.

Beispiel 2

Es sollen alle Regelbehälter für den Miteigentümerschutz gesichert werden; die Referenzguards sollen dabei nicht mit erfasst werden.

Der Anwender macht für die Auswahl der Guards folgende Angaben:

```
GUARD-NAME=SYS.UC*, SELECT=(TYPE=COOWNERP, RESOLVE=*NO)
```

GUARDS-SAVE führt folgende Selektionsschritte durch:

1. Ermitlung aller Guards, deren Namen mit der Zeichenfolge SYS.UC beginnen.
2. Selektion derjenigen Guards aus der durch Schritt 1 ermittelten Guardmenge, die vom Typ COOWNERP sind.

Als Ergebnis dieser Selektion bearbeitet GUARDS-SAVE die Menge aller Guards, deren Namen mit der Zeichenfolge SYS.UC beginnen und vom Guardtyp COOWNERP sind. Mögliche referenzierte Guards vom Typ STDAC bleiben unberücksichtigt.

Aus einem Protokoll kann der Anwender ersehen, welche Guards aufgrund ihres Namens und Typs gesichert wurden. Er kann daraus nicht ersehen, welche Guards referenziert werden.

5.13.3 Bearbeitungsreihenfolge der Guards

Im Guardskatalog und in einer von GUARDS-SAVE erstellten Sicherungsdatei sind die Guardnamen alphabetisch geordnet.

Für einen Sicherungslauf ist es unbedeutend, in welcher Reihenfolge die Guards in die Sicherungsdatei kopiert werden, denn sie verbleiben in vollständiger Anzahl im realen System und können somit ihre Schutzfunktion erwartungsgemäß ausüben.

Im Gegensatz dazu ist jedoch die zeitliche Reihenfolge, in der Guards restauriert werden, von Bedeutung. Werden zum Beispiel aktive Regelbehälter zeitlich vor den von ihnen referenzierten Guards eingespielt, könnte eine Zugriffskontrolle oder Defaultierung so lange zu unerwünschten Ergebnissen führen, bis auch die benötigten Referenzguards eingespielt sind.

ACHTUNG!
GUARDS-SAVE restauriert Guards in alphabetischer Reihenfolge. Befinden sich in der Menge der zu restaurierenden Guards aktive Regelbehälter (erkennbar am vorgeschriebenen Namen wie zum Beispiel SYS.UCF), ist es möglich, dass diese aufgrund der alphabetischen Reihenfolge zeitlich vor den von ihnen referenzierten Guards eingespielt werden. Besteht die Gefahr, dass bereits während eines Restaurierungslaufs Miteigentümerzugriffe oder Standard-Defaultierungen erfolgen, sollte eine prozedurgesteuerte Restaurierung durchgeführt werden und die generierte Kommandoreihenfolge mit einem Texteditor entsprechend umgestellt werden (siehe Abschnitt „Prozedurgesteuerte Restaurierung“ auf Seite 901).

5.13.4 Umbenennung der Guards beim Restaurieren

Guardpfadnamen können bei einer Restaurierung geändert werden. Die entsprechenden Angaben für die Pfadänderungen werden mit dem Operanden NEW-PATH festgelegt.

5.13.4.1 Austausch der Guardpfadnamen

Eine Änderung der Guardpfadnamen wirkt sich aus auf:

1. Die Namen der zu restaurierenden Guards selbst
2. Die Namen der in diesen Guards eingetragenen Referenzguards.

Für jeden Pfadteil (Katalogkennung, Benutzerkennung, Guardnamensteil) kann ein neuer Wert vergeben werden. Ob jedoch eine Umbenennung möglich ist, hängt davon ab, wie der mit dem Operanden GUARD-NAME angegebene Name spezifiziert ist. Jeder Pfadteil kann nur umbenannt werden, wenn er ohne Musterzeichen spezifiziert ist.

Beispiel 1

Mit folgenden Vorgaben kann die Benutzerkennung MARY durch LUZIFER ersetzt werden:

```
GUARD-NAME=:XXXX:$MARY.*, NEW-PATH=(USER-ID=LUZIFER)
```

Beispiel 2

Mit folgenden Vorgaben wird eine Umbenennung abgewiesen, weil die Benutzerkennung mit Musterzeichen spezifiziert ist:

```
GUARD-NAME=:XXXX:$*.*, NEW-PATH=(USER-ID=LUZIFER)
```

In der folgenden Tabelle ist zusammengestellt, welche Voraussetzungen die Angaben im Operand GUARD-NAME und NEW-PATH für eine Umbenennung erfüllen müssen:

Musterzeichen beim Operanden GUARD-NAME in		**Angaben im Operanden NEW-PATH**		**Ergebnis**
Benutzer-kennung	**Guard-namens-teil**	**USER-ID=**	**GUARD-NAME=**	
ja	ja	*SAME	*SAME	keine Umbenennung
		*SAME	<filename 1..8>	nicht erlaubt
		<name 1..8>	*SAME	nicht erlaubt
		<name 1..8>	<filename 1..8>	nicht erlaubt
ja	**nein**	*SAME	*SAME	keine Umbenennung
		*SAME	<filename 1..8>	Guardnamensteil wird umbenannt
		<name 1..8>	*SAME	nicht erlaubt
		<name 1..8>	<filename 1..8>	nicht erlaubt
nein	ja	*SAME	*SAME	keine Umbenennung
		*SAME	<filename 1..8>	nicht erlaubt
		<name 1..8>	*SAME	Benutzerkennung wird umbenannt
		<name 1..8>	<filename 1..8>	nicht erlaubt
nein	**nein**	*SAME	*SAME	keine Umbenennung
		*SAME	<filename 1..8>	Guardnamensteil wird umbenannt
		<name 1..8>	*SAME	Benutzerkennung wird umbenannt
		<name 1..8>	<filename 1..8>	Benutzerkennung und Guard-namensteil werden umbenannt

5.13.4.2 Austausch der Katalogkennung in Zugriffsbedingungen des Typs PROGRAM

In Guards des Typs STDAC können Zugriffsbedingungen festgelegt sein, die einen Zugriff nur über ein bestimmtes Programm erlauben (Angabe `ADMISSION=(PROGRAM=)` in den Kommandos `/ADD-ACCESS-CONDITIONS` oder `/MODIFY-ACCESS-CONDITIONS`). Der Programmname (Datei- oder Bibliothekname) ist dabei inklusive Katalogkennung abgelegt, wobei die Katalogkennung Musterzeichen enthalten kann.

Diese Katalogkennung kann bei einem GUARDS-SAVE-Restaurierungslauf mit der Angabe `NEW-PATH(PROG-PUBSET-ID=...)` geändert werden. Die Umbenennung der Katalogkennung wird unabhängig davon durchgeführt, ob sie im gesicherten Guard mit oder ohne Musterzeichen eingetragen ist.

Beispiel

Zugriffsbedingung vor der Restaurierung

```
/show-access-conditions *
%:XXXX:$MARY.STDAC
%   Others
%    Program
%       File   = :*AA*:$MARY.PROG
```

Zugriffsbedingung nach einer Restaurierung mit folgenden Vorgaben zur Umbenennung:

```
   GUARD-NAME=:XXXX:$MARY.STDAC,NEW-PATH=(PROG-PUBSET-ID=XXXX)
```

```
/show-access-conditions *
%:XXXX:$MARY.STDAC
%   Others
%    Program
%       File   = :XXXX:$MARY.PROG
```

5.13.5 Ergebnisprotokoll

Bei jedem GUARDS-SAVE-Lauf werden Vorgänge und Ereignisse auf SYSOUT/SYSLST ausgegeben. Die Protokolle gliedern sich dabei wie folgt:

- Kopfzeilen
- Rahmenbedingungen
- Liste der bearbeiteten Guards
- Querverweisliste
  Dieser Protokollteil entfällt, wenn die Suche nach Referenzen ausgeschaltet ist (Angabe `SELECT=*BY-ATTRIBUTES(RESOLVE=*NO)`).
- Fußzeilen

Kopfzeilen

Die Kopfzeilen markieren den Beginn des Protokolls und informieren darüber, welche GUARDS-SAVE-Funktion das Protokoll erzeugt hat und welcher Benutzer die Funktion zu welchem Zeitpunkt angefordert hat.

Beispiel

```
%*****************************************************************************
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  MARY       2017-12-07/14:11:58
%                               ------------------------
&                               ***  Begin of Output  ***
%*****************************************************************************
```

Liste der allgemeinen Rahmenbedingungen

Abhängig von der gewählten GUARDS-SAVE-Funktion hat dieser Protokollabschnitt folgenden Inhalt:

- **Sicherungslauf** (//BACKUP-GUARDS)

  Es werden die Basisdaten des Sicherungslaufs protokolliert, mit denen das Sicherungsergebnis auch zu einem späteren Zeitpunkt noch nachvollzogen werden kann.

  Basisdaten sind
  – Name der Sicherungsdatei
  – Zeitpunkt der Sicherung
  – Vorgaben, mit denen der Benutzer die zu sichernden Guards ausgewählt hat (Pubset, Guardname, Guardtyp und Referenz-Suche)

Beispiel

```
%*****************************************************************************
%Backup File     : :XXXX:$MARY.BACKUP-FILE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%
%Backup Guard    : :XXXX:$MARY.*
%Backup Type     : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Backup Resolve  : *YES
%*****************************************************************************
%Saved  Guards   : 6
%Faulty Guards   : 1
%*****************************************************************************
```

- **Restaurierungslauf** (//RESTORE-GUARDS)

  Im ersten Teil werden Basisdaten des **Sicherungs**laufs protokolliert, durch den die Sicherungsdatei erzeugt wurde. Diese Angaben werden aus der Sicherungsdatei ermittelt. Sie entsprechen im Wesentlichen dem Protokoll des Sicherungslaufs.

  Der zweite Teil enthält die Angaben, mit denen der Benutzer die zu restaurierenden Guards ausgewählt hat und die Art der Restaurierung.

  Im dritten Teil werden die Vorgaben für die bei der Restaurierung durchgeführten Umbenennungen protokolliert.

  Beispiel

```
%*****************************************************************************
%Backup File     : :XXXX:$MARY.BACKUP-FILE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 6
%
%Restore Guard   : :XXXX:$MARY.*
%Restore Type    : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Restore Resolve : *YES
%Restore Replace : *YES
%Restore Target  : *SYSTEM
%
%New Pubset-Id   : *SAME
%New User-Id     : *SAME
%New Name        : *SAME
%New Prog Pvs-Id : *SAME
%*****************************************************************************
%Restored Guards : 6
%Faulty Guards   : 1
%*****************************************************************************
```

- **Anzeigelauf** (//SHOW-BACKUP-FILE)

  Im ersten Teil werden Basisdaten des **Sicherungs**laufs protokolliert, durch den die Sicherungsdatei erzeugt wurde. Diese Angaben werden aus der Sicherungsdatei ermittelt. Sie entsprechen im Wesentlichen dem Protokoll des Sicherungslaufs.

  Der zweite Teil enthält die Angaben, mit denen der Benutzer die anzuzeigenden Guards ausgewählt hat.

  Beispiel

```
%*****************************************************************************
%Backup File     : :XXXX:$MARY.BACKUP-FILE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 6
%
%Show Guard      : :XXXX:$MARY.*
%Show Type       : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Show Resolve    : *YES
%*****************************************************************************
%Selected Guards : 6
%Faulty Guards   : 1
%*****************************************************************************
```

Liste der bearbeiteten Guards

Für jedes selektierte Guard wird protokolliert, ob und in welcher Form es bearbeitet wurde bzw. warum es nicht bearbeitet werden konnte.

Zunächst werden in alphabetischer Reihenfolge die Namen der fehlerfrei bearbeiteten Guards aufgelistet.

Gegebenenfalls schließt sich getrennt durch eine gestrichelte Linie eine alphabetische Auflistung der fehlerhaft oder nicht bearbeiteten Guards an.

Die Einträge haben folgenden Aufbau:

- Guardname (Guard Name)

  In jedem GUARDS-SAVE-Protokoll werden die bearbeiteten Guards **immer** mit dem Namen und dem Pfad aufgelistet, der zum **Zeitpunkt der Sicherung** in die Sicherungsdatei eingetragen wurde.

  Dies gilt auch für Restaurierungsläufe, bei denen Umbenennungen durchgeführt werden! Angaben über vorgenommene Umbenennungen gehen **nur** aus den dokumentierten Rahmenbedingungen hervor (siehe „Liste der allgemeinen Rahmenbedingungen“ auf Seite 890).

- Guardtyp (Guard Type)
- Fehlerursache (Error)

  Tritt bei der Bearbeitung eines Guards ein Fehler auf, wird ein entsprechender Fehlercode in Form einer Meldungsnummer mit Präfix protokolliert. Mit dem Kommando /HELP kann sich der Anwender den zugehörigen Fehlertext anzeigen lassen.

- Status

  Abhängig von der gewählten GUARDS-SAVE-Funktion wird der Status eines Guards folgendermaßen angezeigt:

  – Sicherung (//BACKUP-GUARDS):

Status:	**Erläuterung:**
saved	Das Guard wurde gesichert.
only selected	Das Guard wurde nur ausgewählt aber nicht gesichert.
only referenced	Das Guard wurde nur referenziert aber nicht gesichert.
undefined ?????	Beim Auftreten diesen beiden Statusmeldungen sollte der Systemverwalter benachrichtigt werden, denn der Status konnte von GUARDS-SAVE nicht vorschriftsmäßig gesetzt werden.

– Restaurierung (//RESTORE-GUARDS)

Status:	**Erläuterung:**
restored	Das Guard wurde programmgesteuert restauriert.
restored and path changed	Das Guard wurde programmgesteuert mit geändertem Pfadnamen restauriert.
generated	Die Kommandos zur Restaurierung des Guards wurden generiert.
generated and path changed	Die Kommandos zur Restaurierung des Guards wurden mit geändertem Pfadnamen generiert.
only selected	Das Guard wurde nur ausgewählt aber nicht restauriert.
only referenced	Das Guard wurde nur referenziert aber nicht restauriert.
not deleted	Das Guard konnte nicht gelöscht und darum auch nicht restauriert werden. (bei: REPLACE-GUARD=*YES).
deleted and not restored	Das Guard wurde für die Restaurierung gelöscht, danach aber nicht restauriert. (bei: REPLACE-GUARD=*YES).
not restored or overwritten	Das zu restaurierende Guards ist vorhanden und darf darum nicht restauriert werden. (bei: REPLACE-GUARD=*NO). Das Guard kann aus anderen Gründen nicht restauriert werden.
incompletely restored	Das Guard wurde nicht vollständig restauriert.
undefined ?????	Beim Auftreten diesen beiden Statusmeldungen sollte der Systemverwalter benachrichtigt werden, denn der Status konnte von GUARDS-SAVE nicht vorschriftsmäßig gesetzt werden.

– Anzeige (//SHOW-BACKUP-FILE)

Status:	**Erläuterung:**
only selected	Das Guard wurde nur ausgewählt aber die Attribute nicht angezeigt.
only referenced	Das Guard wurde nur referenziert aber die Attribute nicht angezeigt.
undefined ?????	Beim Auftreten diesen beiden Statusmeldungen sollte der Systemverwalter benachrichtigt werden, denn der Status konnte von GUARDS-SAVE nicht vorschriftsmäßig gesetzt werden.

Beispiel

```
%
%                    Alphabetical List of Saved and Faulty Guards
%
%================================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$MARY.COOWNERP      COOWNERP                 saved
%:XXXX:$MARY.DEFAULTP      DEFAULTP                 saved
%:XXXX:$MARY.DEFPATTR      DEFPATTR                 saved
%:XXXX:$MARY.DEFPUID       DEFPUID                  saved
%:XXXX:$MARY.STDAC         STDAC                    saved
%:XXXX:$MARY.UNDEF         UNDEF                    saved
%--------------------------------------------------------------------------------
%:XXXX:$LUZIFER.DEFPATTR  -undefined-      PRO1007  only referenced
%================================================================================
```

Liste mit den Querverweisen

Es wird protokolliert, wie sich die Guards untereinander referenzieren.

Dieser Protokollteil entfällt, wenn die Suche nach Referenzen ausgeschaltet ist (Angabe `SELECT=*BY-ATTRIBUTES(RESOLVE=*NO)`).

Im ersten Abschnitt wird in alphabetischer Reihenfolge jedes Guard aufgelistet, das weitere Guards referenziert, zusammen mit den Namen dieser Referenzguards.

Im zweiten Abschnitt wird in alphabetischer Reihenfolge jedes einzelne Referenzguard aufgeführt, zusammen mit den Namen der Guards, die es referenzieren.

Falls keine Referenzen auftreten, zum Beispiel weil nur Guards des Typs STDAC bearbeitet wurden, wird ein entsprechender Hinweis ausgegeben

Beispiel

```
%
%                   Alphabetical List of Cross References
%
%================================================================================
%:XXXX:$MARY.COOWNERP      COOWNERP    ->  :XXXX:$MARY.STDAC         STDAC
%:XXXX:$MARY.DEFAULT       DEFAULTP    ->  :XXXX:$LUZIFER.DEFPATTR  -undefined-
%                                      ->  :XXXX:$MARY.DEFPUID       DEFPUID
%:XXXX:$MARY.DEFPATTR      DEFPATTR    ->  :XXXX:$MARY.STDAC         STDAC
%--------------------------------------------------------------------------------
%:XXXX:$LUZIFER.DEFPATTR  -undefined-  <-  :XXXX:$MARY.DEFAULTP      DEFAULTP
%:XXXX:$MARY.DEFPUID       DEFPUID     <-  :XXXX:$MARY.DEFAULTP      DEFAULTP
%:XXXX:$MARY.STDAC         STDAC       <-  :XXXX:$MARY.COOWNERP      COOWNERP
%                                      <-  :XXXX:$MARY.DEFPATTR      DEFPATTR
%================================================================================
```

Falls keine Referenzen auftreten, sieht die Liste folgendermaßen aus:

```
%
%                  Alphabetical List of Cross References
%
%================================================================================
%All guards without references
%================================================================================
```

Fußzeilen

Die Kopfzeilen markieren das Ende des Protokolls und informieren darüber, welche GUARDS-SAVE-Funktion das Protokoll erzeugt hat und welcher Benutzer die Funktion zu welchem Zeitpunkt angefordert hat.

Beispiel

```
%********************************************************************************
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  MARY       2017-12-07/14:11:58
%                               -------------------------
&                               ***   End of Output   ***
%********************************************************************************
```

5.13.6 Zeitstempel und Uhrzeiten

In einer von GUARDS-SAVE erstellten Sicherungsdatei und in den gesicherten Guards sind folgende Zeitstempel eingetragen:

– Erstellungsdatum der Sicherungsdatei

  GUARDS-SAVE trägt bei Erstellung einer Sicherungsdatei in einen speziellen Datensatz unter anderem auch Datum und Uhrzeit der Sicherung ein. Die Uhrzeit wird dabei im UTC-Format (Weltzeit) gespeichert. Vor jeder Anzeige, zum Beispiel in GUARDS-SAVE-Protokollen, wird die Uhrzeit in lokale Zeit umgewandelt.

– Erstellungs- und letztes Änderungsdatum in den Guards

  Jedes Guard enthält zwei Zeitstempel, aus denen Datum und Uhrzeit der Erstellung und der letzen Änderung hervorgehen. Die Zeitstempel werden unverändert im UTC-Format (Weltzeit) gesichert. Vor jeder Anzeige wird die Uhrzeit in lokale Zeit umgewandelt. Bei einer programmgesteuerten Restaurierung erhalten die restaurierten Guards ein neues aktuelles Erstellungs- und Modifikationsdatum. Das Erstellungsdatum ergibt sich durch das bei der Restaurierung notwendige Neueinrichten eines Guards. Das Modifikationsdatum entsteht bei der Restaurierung des Guardinhalts.

– In Zugriffsbedingungen definierte Uhrzeiten (Guardtyp STDAC)

  Uhrzeiten, die in Zugriffsbedingungen TIME= definiert werden, beziehen sich immer auf die lokale Zeit, ohne dass dabei die Saison (Sommer- und Normalzeit) berücksichtigt wird. Diese Zeiten werden von GUARDS-SAVE unverändert gesichert und restauriert.

5.13.7 Guards sichern

Mit **einer** GUARDS-SAVE Sicherungs-Anweisung können Guards von jeweils **einem** importierten Pubset gesichert werden. Soll eine Sicherung für mehrere Pubsets durchgeführt werden, müssen entsprechend viele Sicherungs-Anweisungen mit je einer eigenen Sicherungsdatei eingegeben werden.

Beispiel für die Kommando- und Anweisungsfolge eines Sicherungslaufs

```
/start-guards-save
//backup-guards ...
//show-backup-file ... ————————————————————————————————————————— (1)
//end
```

(1) optionale Anweisung zur Kontrolle

5.13.7.1 Die Sicherungsdatei

Die Sicherungsdatei wird bei jedem Sicherungslauf neu eingerichtet, sofern sie noch nicht existiert. Ist sie vorhanden, kann sie auf Wunsch des Anwenders unter Beibehaltung ihrer Dateischutzattribute überschrieben werden. Ein Fortschreiben in eine bestehende Sicherungsdatei über mehrere Sicherungsläufe hinweg ist nicht möglich. Sicherungsdateien können wie normale Datei mit HSMS/ARCHIVE gesichert und mit Schutzattributen versehen werden.

Ein Guards-Administrator kann eine Sicherungsdatei, die den kompletten Guardbestand eines Pubsets enthält, jedem Systemteilnehmer zugänglich machen, da nichtprivilegierte Benutzer nur auf ihren eigenen Guardbestand zugreifen können. Es wird jedoch empfohlen, die Sicherungsdatei in diesem Fall mit einem zusätzlichen Zugriffsschutz zu versehen. Auch sollten Sicherungsdateien, die turnusmäßig für neue Sicherungsstände verwendet werden, mit dem Schutzattribut DESTROY-BY-DELETE belegt werden, damit bei jedem neuen Sicherungslauf die alten Daten zerstört werden.

Das folgende Beispiel zeigt, wie ein empfehlenswerter Schutz für eine systemweit zur Verfügung gestellte Sicherungsdatei eingerichtet werden kann:

```
/CREATE-GUARD GSAVE-R ————————————————————————————————————————  (1)
/ADD-ACCESS-CONDITIONS GSAVE-R -
/   ,SUBJECT=*USER(TSOS),ADMISSION=*YES ————————————————————————  (2)
/ADD-ACCESS-CONDITIONS GSAVE-R -
/   ,SUBJECT=*OTHERS,ADMISSION=*PARAMETERS -
/    (PROGRAM=*MODULE(LIBRARY=$TSOS.SYSLNK.GUARDS-SAVE.040 - ————————  (3)
/                     ,ELEMENT=SAVELLM -
/                     ,VERSION=*ANY))
/CREATE-GUARD GSAVE-W ————————————————————————————————————————  (4)
/ADD-ACCESS-CONDITIONS GSAVE-W -
/   ,SUBJECT=*USER(TSOS),ADMISSION=*YES ————————————————————————  (5)
/ADD-ACCESS-CONDITIONS GSAVE-W -
/    ,SUBJECT=*OTHERS,ADMISSION=*NO ————————————————————————————  (6)
/MOD-FILE-ATTRIBUTES GUARDS-SAVE.BACKUP - ——————————————————————  (7)
/   ,PROTECTION=*PARAMETERS -
/     (GUARDS=*PARAMETERS -
/     (READ=GSAVE-R  -
/     ,WRITE=GSAVE-W -
/     ,EXEC=*NONE) -
/    ,DESTROY-BY-DELETE=*YES)
```

(1) Einrichten eines Guards zum Festlegen der **Lese**-Zugriffsbedingungen.

(2) TSOS soll unbeschränkten Lese-Zugriff erhalten. Alternativ kann dieser Zugriff auch Benutzerkennung des Guard-Administrators ermöglicht werden.

(3) Allen anderen Benutzerkennungen soll der Lese-Zugriff auf die Sicherungsdatei nur mit dem Programm GUARDS-SAVE erlaubt werden.

(4) Einrichten eines Guards zum Festlegen der **Schreib**-Zugriffsbedingungen.

(5) TSOS soll unbeschränkten Schreib-Zugriff erhalten. Alternativ kann dieser Zugriff auch der Benutzerkennung des Guard-Administrators ermöglicht werden.

(6) Allen anderen Benutzerkennungen soll der Schreib-Zugriff auf die Sicherungsdatei verboten werden.

(7) Sicherungsdatei mit Schutzattributen versehen
Die eingerichteten Guards werden zum Schutz der Sicherungsdatei aktiviert.

5.13.7.2 Backup-Katalogkennung

Die Katalogkennung des Pubsets, für das ein Sicherungslauf durchgeführt werden soll, leitet sich vom Guardpfadnamen ab, den der Anwender für den Lauf angegeben hat. Ist im Pfadnamen keine Katalogkennung angegeben, wird als Backup-Pubset das Default-Pubsets des Aufrufers angenommen und in der Sicherungsdatei vermerkt. Gibt ein Guards-Administrator im Guardnamen keine Katalogkennung an und verwendet er gleichzeitig in der Benutzerkennung Musterzeichen, wird als Backup-Pubset der Home-Pubset verwendet und in der Sicherungsdatei vermerkt.

5.13.8 Guards restaurieren

Mit **einer** Restaurierungsanweisung können Guards aus einer von GUARDS-SAVE erstellten Sicherungsdatei auf **ein** importiertes Pubset zurück übertragen werden. Soll eine Restaurierung für mehrere Pubsets durchgeführt werden, müssen entsprechend viele Restaurierungsanweisungen eingegeben werden. Ein Restaurierungsvorgang kann auf folgende Art und Weise durchgeführt werden:

- Programmgesteuert

  Die Guards werden unmittelbar ins laufende System eingespielt

- Prozedurgesteuert

  Für die Restaurierung wird eine Ablaufprozedur generiert

Beispiel für die Kommando- und Anweisungsfolge eines Restaurierungslaufs

```
/start-guards-save
//show-backup-file  ... ————————————————————————————————————————— (1)
//restore-guards ...
//end
/call-procedure ... ————————————————————————————————————————————— (2)
```

(1) optionale Anweisung für Kontrolle

(2) bei prozedurgesteuerter Restaurierung

5.13.8.1 Programmgesteuerte Restaurierung

Bei dieser Art der Restaurierung werden die gesicherten Guards unmittelbar in alphabetischer Reihenfolge ins System eingespielt (siehe Abschnitt „Bearbeitungsreihenfolge der Guards“ auf Seite 886.

ACHTUNG!

Sollen u. a. aktive Regelbehälter (erkennbar am vorgeschriebenen Namen wie zum Beispiel SYS.UCF) restauriert werden, ist es möglich, dass diese aufgrund der alphabetischen Reihenfolge zeitlich vor den von ihnen referenzierten Guards eingespielt werden. Besteht die Gefahr, dass bereits während eines Restaurierungslaufs Miteigentümerzugriffe oder Standard-Defaultierungen erfolgen, sollte in diesem Fall eine prozedurgesteuerte Restaurierung mit manueller Umbenennung der aktiven Regelbehälter bevorzugt werden (siehe Abschnitt „Prozedurgesteuerte Restaurierung“ auf Seite 901).

In den Guards des Typs DEFPATTR, in denen Schutzattribute für den Standardschutz definiert werden können, können auch Schreib-, Lese- und Ausführkennwörter festgelegt werden. Im Gegensatz zur prozedurgesteuerten Restaurierung (siehe Abschnitt „Prozedurgesteuerte Restaurierung“ auf Seite 901) können diese Kennwörter bei einer programmgesteuerten Restaurierung wieder hergestellt werden.

5.13.8.2 Prozedurgesteuerte Restaurierung

Aus den gesicherten Guardinformationen werden Prozedurkommandos abgeleitet und in eine vom Anwender festgelegte Prozedurdatei geschrieben. Diese Prozedurdatei hat das Dateiformat SAM und kann mit einem Texteditor, z.B. EDT, modifiziert werden.

Die Prozedur enthält in Form von Kommentarzeilen dieselben Informationen wie ein GUARDS-SAVE-Protokoll: die Kopf- und Fußzeilen, die Rahmenbedingungen und (am Prozedurende) eine zusammenfassende Liste mit den Namen aller durch die Prozedur restaurierten Guards.

Die Prozedur ist so strukturiert, dass die Guards in alphabetischer Reihenfolge restauriert werden. Vor den Kommandos zum Restaurieren eines Guards werden in Form von Prozedurkommentaren folgende Informationen eingetragen:

– der Pfadname, wie er aus der Sicherungsdatei gelesen wurde

– der Pfadname, wie er sich durch Umbenennungen neu zusammensetzt (falls vorhanden)

– die in dem Guard auftretenden Referenzguards mit ihrem altem und ggf. neuen Pfadnamen

Zur Behandlung von Fehlersituationen werden Sprungmarken generiert, deren Name sich aus einem Buchstaben und einer siebenstelligen Nummer zusammensetzt. Die Nummer der Sprungmarke für das erste zu restaurierende Guard ist 0000001, und sie erhöht sich für jedes weitere um 1. Übersteigt die Anzahl der Sprungmarken die Zahl 9999999, wird ein Fehler gemeldet und der Prozedur-Generierungsprozess abgebrochen. In diesem Fall wird empfohlen, die Restaurierung in mehrere Läufe aufzuteilen, z.B. durch die Erzeugung von je einer eigenen Restaurierungsprozedur pro Guardtyp.

Abhängig vom Operanden REPLACE beim Restaurierungslauf werden bei der Prozedurerstellung folgende Aktionen durchgeführt:

– REPLACE=*YES

/DELETE-GUARD	Mit dem Kommando wird ein gegebenenfalls existierendes Guard gelöscht. Durch entsprechende Sprungmarken wird die Situation abgefangen, dass das zu löschende Guard nicht vorhanden ist.
/CREATE-GUARD	Das Guard wird neu erzeugt und die Guardattribute restauriert.
/ADD-... oder /MODIFY-...	Der Guardinhalt wird restauriert.

– REPLACE=*NO

/CREATE-GUARD	Es wird versucht, das Guard neu zu erzeugen und die Guardattribute zu restaurieren. Gibt es das Guard bereits, protokolliert die Prozedur eine entsprechende Textmeldung und fährt mit dem nächsten Guard fort. Gibt es das Guard nicht, wird mit seiner Restaurierung fortgefahren.
/ADD-... oder /MODIFY-...	Der Guardinhalt wird restauriert.

In den Guards des Typs DEFPATTR, in denen Schutzattribute für den Standardschutz definiert werden können, können auch Schreib-, Lese- und Ausführkennwörter festgelegt werden. Diese Kennwörter werden bei einer Restaurierung per Prozedur nicht restauriert. Stattdessen wird in der Prozeur eine entsprechender Hinweis eingetragen. Soll das Kennwort nicht manuell in die Prozedur eingetragen werden, sondern genauso restauriert werden, wie es gesichert wurde, müssen die Guards des Typs DEFPATTR programmgesteuert restauriert werden (siehe Abschnitt „Programmgesteuerte Restaurierung“ auf Seite 900).

Beispiel

Im folgenden Beispiel wird eine von GUARDS-SAVE generierte Prozedur dargestellt, mit der die beiden Guards $TSOS.SYS.DEFPATTR und $TSOS.SYS.PDF unter gleichzeitigem Austausch von Katalog- und Benutzerkennung restauriert werden können.

Das referenzierte Benutzerkennungsguard $LUZIFER.DEFPUID wurde zuvor nicht gesichert und wird darum bei der Prozedurgenerierung in der Sicherungsdatei nicht gefunden.

Die Schreibkennwörter werden nicht restauriert, stattdessen wird ein entsprechender Hinweis in die Prozeur eingetragen.

```
/ BEGIN-PROCEDURE LOGGING=*NO
/
/ REMARK MOD-JOB-OPT LOGGING=(LISTING=*YES)
/ STEP
/ ASSIGN-SYSLST TO=#RESTORE.LST.2017-12-15.170512
/ STEP
/
/ WRI-TEXT '************************************************************'
/ WRI-TEXT 'GUARDS-SAVE                                  RESTORE-GUARDS'
/ WRI-TEXT 'Proc Generated by User  TSOS      at  2017-12-15/17:05:12'
/ WRI-TEXT '************************************************************'
/ WRI-TEXT '                  ***  Begin  ***                            '
/          "************************************************************"
/          "Backup File     : :XXXX:$TSOS.BACKUP-GUARD                  "
/          "Backup Date     : 2017-12-07/14:11:58                       "
/          "Backup Pubset   : XXXX                                      "
/          "                                                            "
/          "Restore Guard   : :XXXX:$TSOS.*                             "
/          "Restore Type    : COOWNERP, DEFAULTP, DEFPATTR,             "
/          "                  DEFPUID , STDAC   , UNDEF                 "
/          "Restore Resolve : *YES                                      "
/          "Restore Replace : *YES                                      "
/          "                                                            "
/          "New Pubset-Id   : 2OSC                                      "
/          "New User-Id     : MARY                                      "
/          "New Name        : *SAME                                     "
/          "New Prog Pvs-Id : *SAME                                     "
/          "************************************************************"
/
/          "** ================================================ **"
/          "**                                                  **"
/          "** Guard    :XXXX:$TSOS.DEFPATTR      DEFPATTR 0000001 **"    -- alter Pfad
/          "** -->      :2OSC:$MARY.DEFPATTR                      **"    -- neuer Pfad
/          "**                                                  **"
/          "** ================================================ **"
/           DEL-GUARD :2OSC:$MARY.DEFPATTR                          -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  deleted         **'
/           SKIP .C0000001
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  delete  *error* **'
/           SKIP .C0000001
/
/           .C0000001
/           CRE-GUARD :2OSC:$MARY.DEFPATTR                            -
/              ,SCOPE=*USER-ID                                        -
/              ,USER-INFO='                                          '
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  created         **'
/           SKIP .R0000001
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  create  *error* **'
/           SKIP .E0000001
/
```

```
/           .R0000001
/           ADD-DEFAULT-PROTECTION-ATTR :2OSC:$MARY.DEFPATTR
/           MOD-DEFAULT-PROTECTION-ATTR :2OSC:$MARY.DEFPATTR           -
/              ,ATTR-SCOPE=*CREATE-OBJECT                              -
/              ,ACCESS=*SYSTEM-STD                                     -
/              ,USER-ACCESS=*SYSTEM-STD                                -
/              ,BASIC-ACL=*SYSTEM-STD                                  -
/              ,GUARDS=*SYSTEM-STD                                     -
/              ,READ-PASSWORD=*SYSTEM-STD                              -
/              ,WRITE-PASSWORD=*NONE                                   -  -- kein Passwd
/              ,EXEC-PASSWORD=*SYSTEM-STD                              -
/              ,DESTROY-BY-DELETE=*SYSTEM-STD                          -
/              ,SPACE-RELEASE-LOCK=*SYSTEM-STD                         -
/              ,EXPIRATION-DATE=*SYSTEM-STD                            -
/              ,FREE-FOR-DELETION=*SYSTEM-STD                          -
/              ,DIALOG-CONTROL=*NO
/           MOD-DEFAULT-PROTECTION-ATTR :2OSC:$MARY.DEFPATTR           -
/              ,ATTR-SCOPE=*MODIFY-OBJECT-ATTR                         -
/              ,ACCESS=*SYSTEM-STD                                     -
/              ,USER-ACCESS=*SYSTEM-STD                                -
/              ,BASIC-ACL=*SYSTEM-STD                                  -
/              ,GUARDS=*SYSTEM-STD                                     -
/              ,READ-PASSWORD=*SYSTEM-STD                              -
/              ,WRITE-PASSWORD=*NONE                                   -  -- kein Passwd
/              ,EXEC-PASSWORD=*SYSTEM-STD                              -
/              ,DESTROY-BY-DELETE=*SYSTEM-STD                          -
/              ,SPACE-RELEASE-LOCK=*SYSTEM-STD                         -
/              ,EXPIRATION-DATE=*SYSTEM-STD                            -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '**                                                      **'
/ WRI-TEXT '** Warning:                                             **'
/ WRI-TEXT '** -------                                              **'
/ WRI-TEXT '** WRITE-PASSWORD=*NONE restored for ATTR-SCOPE=*CRE    **'    -- Warnung
/ WRI-TEXT '** WRITE-PASSWORD=*NONE restored for ATTR-SCOPE=*MOD    **'    -- Warnung
/ WRI-TEXT '**                                                      **'
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  restored         **'
/           SKIP .E0000001
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.DEFPATTR      DEFPATTR  restore *error* **'
/           SKIP .E0000001
/           .E0000001
/
/          "** ================================================ **"
/          "**                                                  **"
/          "** Guard    :XXXX:$TSOS.SYS.PDF       DEFAULTP 0000002 **"    -- alter Pfad
/          "** -->      :2OSC:$MARY.SYS.PDF                      **"    -- neuer Pfad
/          "**      Ref       $LUZIFER.DEFPUID                    **"
/          "**      Ref       $TSOS.DEFPATTR                      **"    -- alter Pfad
/          "**      -->       $MARY.DEFPATTR                      **"    -- neuer Pfad
/          "**                                                  **"
/          "** ================================================ **"
/ WRI-TEXT '** ------------------------------------------------ **'
/           DEL-GUARD :2OSC:$MARY.SYS.PDF                             -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  deleted          **'
/           SKIP .C0000002
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  delete  *error* **'
/           SKIP .C0000002
/
```

```
/           .C0000002
/           CRE-GUARD :2OSC:$MARY.SYS.PDF                                -
/              ,SCOPE=*USER-ID                                           -
/              ,USER-INFO='                                             '
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  created         **'
/           SKIP .R0000002
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  create  *error* **'
/           SKIP .E0000002
/           .R0000002
/           ADD-DEFAULT-PROTECTION-RULE :2OSC:$MARY.SYS.PDF              -
/              ,PROTECTION-RULE=RULE1                                    -
/              ,RULE-POSITION=*LAST                                      -
/              ,PROTECT-OBJECT=*PARAMETERS                               -
/                (NAME=A                                                 -
/                ,ATTRIBUTE-GUARD=$MARY.DEFPATTR                         -
/                ,USER-ID-GUARD=$LUZIFER.DEFPUID  )                      -  -- fehlt
/              ,GUARD-CHECK=*NO                                          -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  restored        **'
/           SKIP .E0000002
/           STEP
/ WRI-TEXT '** :2OSC:$MARY.SYS.PDF       DEFAULTP  restore *error* **'
/           SKIP .E0000002
/           .E0000002
/
/          "*********************************************************"
/          "Guard Name               Guard Type Error   Status      "
/          "----------               ---------- -----   ------      "
/          ":XXXX:$TSOS.DEFPATTR     DEFPATTR           generated   "    -- alter Pfad
/          ":XXXX:$TSOS.SYS.PDF      DEFAULTP           generated   "    -- alter Pfad
/          "                                                       "
/          ":XXXX:$LUZIFER.DEFPUID   -undefined- DMSOAA8 referenced  "    -- fehlt
/          "-------------------------------------------------------"
/          "Generated Guards: 2                                    "
/          "Faulty Guards   : 1                                    "
/          "*********************************************************"
/
/ WRI-TEXT '*********************************************************'
/ WRI-TEXT '                  ***   End   ***                        '
/          "*********************************************************"
/ WRI-TEXT 'GUARDS-SAVE                                RESTORE-GUARDS'
/ WRI-TEXT 'Proc Generated by User  TSOS      at  2017-12-15/17:05:12'
/ WRI-TEXT '*********************************************************'
/
/ STEP
/ ASSIGN-SYSLST TO=*PRIMARY
/ STEP
/
/ END-PROCEDURE
```

5.13.8.3 Restore-Katalogkennung

Bei einem Restaurierungslauf kann im Guardpfadnamen keine Katalogkennung angegeben werden, weil für eine Restaurierung standardmäßig immer das Pubset verwendet wird, von dem die Sicherung erstellt worden ist. Soll die Katalogkennung bei einer Restaurierung durch eine andere ersetzt werden, muss die neue Katalogkennung mit der Angabe `NEW-PATH(PUBSET-ID=)` festgelegt werden.

5.13.9 Gesicherte Guards anzeigen

Mit **einer** GUARDS-SAVE Anzeige-Anweisung können Guards von jeweils **einem** gesicherten Pubset angezeigt werden. Nichtprivilegierten Benutzern wird nur der eigene Guardbestand aus der Sicherungsdatei angezeigt, ein Guard-Administrator kann sich den gesamten Guardbestand anzeigen lassen.

Beispiel für die Kommando- und Anweisungsfolge eines Anzeigelaufs

```
/start-guards-save
//show-backup-file  ...
//end
```

Es können drei Arten von Informationen angezeigt werden:

- Guardattribute

  Bei dieser Ausgabe werden neben den Guardnamen auch die Guardattribute (Type, Scope, Erstellungs- und Modifikationsdatum und Benutzerinformation) ausgegeben. Fehlerhafte Guards wie zum Beispiel Referenzguards, die nicht gesichert werden konnten, werden nach einer gestrichelten Linie alphabetisch aufgelistet.

```
%
%                  Alphabetical List of Selected and Faulty Guards
%
%================================================================================
%Guard Name               Scope Type    Creation Date       Last Modification
%----------               ----- ----    -------------       -----------------
%:XXXX:$MARY.COOWNERP     USR  COOWNERP 2017-12-11/15:43:05 2017-12-11/15:54:30
%                         Regelbehaelter fuer den Miteigentuemerschutz
%--------------------------------------------------------------------------------
%:XXXX:$LUZIFER.STDAC     -undefined-      DMSOAA8  only referenced
%================================================================================
```

- Guardnamen

  Bei dieser Ausgabe werden lediglich die Guardnamen und ihr Typ aufgelistet. Fehlerhafte Guards wie zum Beispiel Referenzguards, die nicht gesichert werden konnten, werden nach einer gestrichelten Linie alphabetisch aufgelistet.

```
%
%                  Alphabetical List of Selected and Faulty Guards
%
%================================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$MARY.COOWNERP      COOWNERP
%--------------------------------------------------------------------------------
%:XXXX:$LUZIFER.STDAC     -undefined-      DMSOAA8  only referenced
%================================================================================
```

- Kurzinformation

  Bei dieser Ausgabe werden lediglich die Rahmenbedingungen dokumentiert, die dem Sicherungslauf als Basis gedient haben. Des Weiteren wird angezeigt, wie viele Guards aufgrund des durch den Operanden GUARD-NAME angegebenen Guardnamens selektiert wurden, es werden jedoch keinerlei Guardnamen aufgelistet.

```
%*****************************************************************************
%Backup File     : :XXXX:$MARY.BACKUP-FILE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 1
%
%Show Guard      : :XXXX:$MARY.*
%Show Type       : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Show Resolve    : *YES
%*****************************************************************************
%Selected Guards : 1
%Faulty Guards   : 1
%*****************************************************************************
```

5.13.10 GUARDS-SAVE starten

Für die Durchführung einer Guards-Sicherung oder -Restaurierung muss das Dienstprogramm GUARDS-SAVE mit dem Kommando /START-GUARDS-SAVE gestartet werden. Nach dem Ladevorgang wechselt das Programm in einen Eingabemodus, in dem der Anwender Sicherungs-, Restaurierungs- und Anzeigeanweisungen eingeben kann. Mit der Anweisung //END wird das Programm beendet.

START-GUARDS-SAVE
Starten des Programms GUARDS-SAVE

Anwendungsbereich: UTILITIES, SECURITY-ADMINISTRATION

Privilegierung: alle außer: OPERATING, HARDWARE-MAINTENANCE

START-GUARDS-**SAV**E
MONJV = ***NONE** / <filename 1..54 without-gen-vers> ,**CPU**-LIMIT = ***JOB-RE**ST / <integer 1..32767>

MONJV = *NONE / <filename 1..54>
Angabe einer Monitor-Jobvariablen zur Überwachung von GUARDS-SAVE.

MONJV = *NONE
Es wird keine Monitor-Jobvariable verwendet.

MONJV = <filename 1..54 without-gen-vers>
Name der zu verwendenden Monitor-Jobvariablen.

CPU-LIMIT = *JOB-REST / <integer 1..32767>
Angabe der CPU-Zeit, die GUARDS-SAVE beim Ablauf verbrauchen darf. Wird diese Zeitgrenze überschritten, so wird der Benutzer im Dialog vom System benachrichtigt; im Batchbetrieb wird der GUARDS-SAVE-Lauf abgebrochen.

CPU-LIMIT = *JOB-REST
Es soll die verbleibende CPU-Zeit für die Task verwendet werden.

CPU-LIMIT = <integer 1..32767>
Es soll nur die angegebene Zeit verwendet werden.

5.13.11 GUARDS-SAVE-Anweisungen

In diesem Abschnitt werden alle GUARDS-SAVE-Anweisungen in alphabetischer Reihenfolge aufgeführt. Die Beschreibung der Anweisungen ist so aufgebaut, dass zuerst ein allgemeiner Text die Funktion der Anweisung erklärt, dann folgt das Anweisungsformat und im Anschluss die Operandenbeschreibung, in der jeder Operand mit seinen zugehörigen Werten beschrieben wird. Ein Anwendungsbeispiel finden Sie auf Seite 929.

Die Metasyntax zu den Anweisungen finden Sie im Handbuch „Kommandos“ [4].

Funktionelle Übersicht

//BACKUP-GUARDS	Guards in eine Sicherungsdatei kopieren
//RESTORE-GUARDS	Guards restaurieren
//SHOW-BACKUP-FILE	Inhalt einer Sicherungsdatei anzeigen

Die Standardanweisungen von SDF können zusätzlich angegeben werden. Die Beschreibung dieser Anweisungen finden Sie im Handbuch „Dialogschnittstelle SDF“ [20].

BACKUP-GUARDS
Guards in Sicherungsdatei kopieren

Mit dieser Anweisung werden ein oder mehrere Guards in eine Sicherungsdatei kopiert. Die Sicherungsdatei hat ISAM-Format und kann mit den gängigen Sicherungsprogrammen (zum Beispiel HSMS/ARCHIVE) gesichert werden. Die Menge der für die Sicherung auszuwählenden Guards kann durch Musterzeichen festgelegt werden. Ein nichtprivilegierter Benutzer darf nur die Guards seiner eigenen Kennung, ein Guards-Administrator die Guards aller Kennungen sichern.

Mit einer Anweisung können jeweils nur die Guards von einem einzelnen Pubset in eine benannte Sicherungsdatei kopiert werden. Sollen mehrere Pubsets gesichert werden, muss pro Pubset ein Sicherungslauf mit einer eigenen Sicherungsdatei durchgeführt werden.

Guards können weitere Guards referenzieren. Zum Beispiel können in Regeln für den Miteigentümerschutz Verweise auf Guards des Typs STDAC auftreten. Mit dem Operanden RESOLVE kann gesteuert werden, ob referenzierte Guards automatisch mit gesichert werden sollen. In diesem Fall werden alle referenzierten Guards unabhängig von ihrem Namen und ihrem Typ für die Sicherung ausgewählt. Das heißt, für sie haben die Angaben der Operanden GUARD-NAME und GUARD-TYPE keine Bedeutung. Es wird eine Querverweisliste erzeugt und nach SYSOUT/ SYSLST ausgegeben. Kann auf ein Referenzguard nicht zugegriffen werden, z.B. weil es dem (nichtprivilegierten) Aufrufer nicht gehört, wird es in der Liste der referenzierten Guards mit einem entsprechenden Fehlercode aufgelistet.

```
BACKUP-GUARDS

 GUARD-NAME = * / <filename 1..24 without-gen-vers with-wild(40)>
,SELECT = *ALL / *BY-ATTRIBUTES(...)
    *BY-ATTRIBUTES(...)
        TYPE = *ANY / list-poss(6): <name 1..8>
        ,RESOLVE = *YES / *NO
,BACKUP-FILE-NAME = <filename 1..54 without-gen-vers>
,REPLACE-BACKUP-FILE = *NO / *YES
,OUTPUT = *SYSOUT / list-poss(2): *SYSOUT / *SYSLST(...)
    *SYSLST(...)
        SYSLST-NUMBER = *STD / <integer 1..99>
```

GUARD-NAME =
Angabe des oder der zu sichernden Guards.

Abhängigkeit zum Operanden SELECT

– Mit der Angabe von `SELECT=*BY-ATTRIBUTES(TYPE=...)` kann eine typabhängige Einschränkung der benannten Guardmenge erzielt werden.

– Bei Angabe von `SELECT=*BY-ATTRIBUTES(RESOLVE=YES)` werden auch referenzierte Guards gesichert und zwar unabhängig von ihrem Namen und Typ.

GUARD-NAME = *
Bei der Selektion für die Sicherung soll jeder Guardname berücksichtigt werden.

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Teil- oder vollqualifizierter Name der zu sichernden Guards. Guardnamen dürfen Musterzeichen enthalten, Musterzeichen in der Benutzerkennung darf nur ein Guards-Administrator angeben.

Musterzeichen in der Katalogkennung sind nicht erlaubt, denn eine Sicherungsdatei kann nur die Guards eines einzelnen Pubsets aufnehmen.

Die Katalogkennung bestimmt, welches Pubset gesichert wird. Ist keine Katalogkennung angegeben, gilt Folgendes:

– Wenn der Aufrufer nichtprivilegiert ist, wird das Default-Pubset des Aufrufers gesichert

– Wenn der Aufrufer Guards-Administrator ist und die Benutzerkennung mit Musterzeichen definiert ist, wird der Home-Pubset gesichert

– Wenn der Aufrufer Guards-Administrator ist und die Benutzerkennung ohne Musterzeichen definiert ist, wird das Default-Pubset dieser Benutzerkennung gesichert

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SELECT =
Angabe der Kriterien, die zusätzlich zum Operanden GUARD-NAME für die Auswahl der zu sichernden Guards herangezogen werden sollen.

SELECT = *ALL
Es werden alle Guardtypen und alle referenzierten Guards ausgewählt. Die Referenzguards werden dabei unabhängig von ihrem Namen ausgewählt.

SELECT = *BY-ATTRIBUTES(...)
Die Menge der mit dem Operanden GUARD-NAME ausgewählten Guards wird durch weitere Kriterien modifiziert.

TYPE =
Angabe des Guardtyps, auf den die Auswahl beschränkt werden soll.

TYPE = *ANY
Die Guards werden unabhängig von ihrem Typ ausgewählt.

TYPE = list-poss(6): <name 1..8>
Nur Guards des angegeben Typs bzw. der angegebenen Typen werden ausgewählt. Folgende Angaben sind erlaubt:

Guardtyp	Bedeutung
COOWNERP	Regelbehälter für den Miteigentümerschutz
DEFAULTP	Regelbehälter für den Standardschutz
DEFPATTR	Attributguards (Standardschutz)
DEFPUID	Benutzerkennungsguards (Standardschutz)
STDAC	Zugriffsbedingungsguards
UNDEF	Guards undefiniertenTyps

RESOLVE =
Angabe, ob die ausgewählten Guards nach referenzierten Guards durchsucht werden sollen.

RESOLVE = *YES
Ausgewählte Guards werden nach referenzierten Guards durchsucht. Die so gefundenen Referenzguards werden zusätzlich unabhängig von ihrem Namen und Typ ausgewählt.

Guardtyp	Referenzguards
COOWNERP	In den Regeln spezifizierte Zugriffsbedingungsguards
DEFAULTP	In den Regeln spezifizierte Attribut- und Benutzerkennungsguards
DEFPATTR	In den Schutzattributen spezifizierte Guards
DEFPUID	keine
STDAC	keine
UNDEF	keine

RESOLVE = *NO
Die Guards werden nicht nach referenzierten Guards durchsucht. Gesichert werden ausschließlich die aufgrund ihres Namens (Operand GUARD-NAME) und Typs (Operand TYPE) ausgewählten Guards.

BACKUP-FILE-NAME = <filename 1..54 without-gen-vers>
Name der Sicherungsdatei, in die die Guards gesichert werden sollen. Der Name ist frei wählbar. Existiert bereits eine Datei gleichen Namens, wird abhängig vom Operanden REPLACE-BACKUP-FILE entweder die Datei überschrieben oder die Anweisung mit einer entsprechenden Fehlermeldung abgewiesen. Die Angabe der System-Standardkennung im Dateinamen, wie zum Beispiel $<filename> oder $.<filename> ist erlaubt.

REPLACE-BACKUP-FILE =
Angabe, ob eine gegebenenfalls schon vorhandene Sicherungsdatei überschrieben werden soll oder nicht.

REPLACE-BACKUP-FILE = *NO
Eine gegebenenfalls schon vorhandene Sicherungsdatei wird nicht überschrieben.

REPLACE-BACKUP-FILE = *YES
Eine gegebenenfalls schon vorhandene Sicherungsdatei wird überschrieben. Die eingestellten Dateischutzattribute bleiben erhalten.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe einer Ergebnisprotokollierung.

OUTPUT = *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern das Kommando im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Beispiel: Ausgabe nach einem Sicherungslauf

```
//backup-guards guard-name=*,backup-file-name=g-save
%  PRO7014 '2' GUARDS ARE SAVED IN BACKUP FILE ':XXXX:$MARY.G-SAVE'<
%*****************************************************************************<
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  MARY       2017-12-07/14:11:58<
%                               -------------------------                     <
%                               ***  Begin of Output  ***                     <
%*****************************************************************************<
%Backup File     : :XXXX:$MARY.G-SAVE                                         <
%Backup Date     : 2017-12-07/14:11:58                                        <
%Backup Pubset   : XXXX                                                       <
%                                                                             <
%Backup Guard    : :XXXX:$MARY.*                                              <
%Backup Type     : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF    <
%Backup Resolve  : *YES                                                       <
%*****************************************************************************<
%Saved  Guards   : 2                                                          <
%Faulty Guards   : 0                                                          <
%*****************************************************************************<
%                                                                             <
%                  Alphabetical List of Saved and Faulty Guards               <
%                                                                             <
%=============================================================================<
%Guard Name                Guard Type      Error    Status                    <
%----------                ----------      -----    ------                    <
%:XXXX:$MARY.STDAC         STDAC                    saved                     <
%:XXXX:$MARY.SYS.UCF       COOWNERP                 saved                     <
%=============================================================================<
%                                                                             <
%                  Alphabetical List of Cross References                      <
%                                                                             <
%=============================================================================<
%:XXXX:$MARY.SYS.UCF       COOWNERP    ->  :XXXX:$MARY.STDAC         STDAC     <
%-----------------------------------------------------------------------------<
%:XXXX:$MARY.STDAC         STDAC       <-  :XXXX:$MARY.SYS.UCF       COOWNERP  <
%=============================================================================<
%                                                                             <
%*****************************************************************************<
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  MARY       2017-12-07/14:11:58<
%                               -------------------------                     <
%                               ***   End of Output   ***                     <
%*****************************************************************************<
%//
```

RESTORE-GUARDS
Guards aus einer Sicherungsdatei restaurieren

Mit dieser Anweisung können ein oder mehrere gesicherte Guards restauriert werden. Die Menge der für die Restaurierung auszuwählenden Guards kann durch Musterzeichen festgelegt werden. Ein nichtprivilegierter Benutzer darf nur die Guards seiner eigenen Kennung, ein Guards-Administrator die Guards aller Kennungen für die Restaurierung verwenden.

Es kann zwischen zwei Arten der Restaurierung gewählt werden:

– Unmittelbare Restaurierung durch GUARDS-SAVE

– Erstellung einer Prozedurdatei mit allen notwendigen Kommandos, um die gewünschten Guards ins System einzuspielen.
  In diesem Fall muss die erzeugte Kommandoprozedur vom Anwender zum Ablauf gebracht werden. Bei Bedarf kann die Prozedur mit einem Texteditor wie zum Beispiel dem EDT eingesehen und abgeändert werden.

Mit einer Anweisung können jeweils nur die Guards eines einzelnen Pubsets restauriert werden. Sollen mehrere Pubsets bearbeitet werden, muss pro Pubset ein Restaurierungslauf durchgeführt werden.

Guards können weitere Guards referenzieren. Zum Beispiel können in Regeln für den Miteigentümerschutz Verweise auf Guards des Typs STDAC auftreten. Mit dem Operanden RESOLVE kann gesteuert werden, ob referenzierte Guards automatisch mit restauriert werden sollen. In diesem Fall werden alle referenzierten Guards unabhängig von ihrem Namen und ihrem Typ für die Restaurierung ausgewählt. Das heißt, für sie haben die Angaben der den Operanden GUARD-NAME und GUARD-TYPE keine Bedeutung. Es wird eine Querverweisliste erzeugt und nach SYSOUT/ SYSLST ausgegeben. Kann auf ein Referenzguard nicht zugegriffen werden, z.B. weil es dem (nichtprivilegierten) Aufrufer nicht gehört, wird es in der Liste der referenzierten Guards mit einem entsprechenden Fehlercode aufgelistet.

Guards des Typs STDAC enthalten Zugriffsbedingungen, die sich auf bestimmte Subjekte wie zum Beispiel Benutzerkennungen oder Benutzergruppen beziehen. Bei einer Restaurierung wird **nicht** geprüft, ob die in den Zugriffsbedingungen festgelegten Benutzerkennungen oder Benutzergruppen in der Restaurierungsumgebung vorhanden sind. Der Anwender sollte darum nach einer erfolgreichen Restaurierung kontrollieren, ob die in den restaurierten Guards des Typs STDAC enthaltenen Zugriffsbedingungen weiterhin ihre Gültigkeit haben und die Umgebung gegebenenfalls manuell anpassen.

```
RESTORE-GUARDS

 GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
,SELECT = *ALL / *BY-ATTRIBUTES(...)
    *BY-ATTRIBUTES(...)
        TYPE = *ANY / list-poss(6): <name 1..8>
        ,RESOLVE = *YES / *NO
,BACKUP-FILE-NAME = <filename 1..54 without-gen-vers>
,NEW-PATH = *SAME / *BY-RULE(...)
    *BY-RULE(...)
        PUBSET-ID = *SAME / <cat-id 1..4>
        ,USER-ID = *SAME / <name 1..8>
        ,GUARD-NAME = *SAME / <name 1..8 without-cat-user-gen-vers>
        ,PROG-PUBSET-ID = *SAME / <catid 1..4>
,TARGET = *SYSTEM / *PROCEDURE(...)
    *PROCEDURE(...)
        PROC-FILE-NAME = <filename 1..54 without-gen-vers>
        ,REPLACE-PROC-FILE = *NO / *YES
,REPLACE-GUARD = *NO / *YES
,OUTPUT = *SYSOUT / list-poss(2): *SYSOUT / *SYSLST(...)
    *SYSLST(...)
        SYSLST-NUMBER = *STD / <integer 1..99>
```

GUARD-NAME = <filename 1..24 without-cat-gen-vers with-wild(40)>
Name des oder der Guards in einer Sicherungsdatei, die restauriert werden sollen. Guardnamen dürfen Musterzeichen enthalten, Musterzeichen in der Benutzerkennung darf nur ein Guards-Administrator angeben.

Eine Katalogkennung darf im Pfadnamen nicht angegeben werden, es wird auf dem Pubset restauriert, dessen Katalogkennung zum Zeitpunkt der Sicherung in der Sicherungsdatei vermerkt wurde. Soll die Katalogkennung umbenannt werden, muss der Operand NEW-PATH verwendet werden.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

Abhängigkeit zum Operanden SELECT

– Mit der Angabe von `SELECT=*BY-ATTRIBUTES(TYPE=...)` kann eine typabhängige Einschränkung der benannten Guardmenge erzielt werden.

– Bei Angabe von `SELECT=*BY-ATTRIBUTES(RESOLVE=YES)` werden auch referenzierte Guards restauriert und zwar unabhängig von ihrem Namen und Typ.

SELECT =
Angabe der Kriterien, die zusätzlich zum Operanden GUARD-NAME für die Auswahl der zu restaurierenden Guards herangezogen werden sollen.

SELECT = *ALL
Es werden alle Guardtypen und alle referenzierten Guards ausgewählt. Die Referenzguards werden dabei unabhängig von ihrem Namen ausgewählt.

SELECT = *BY-ATTRIBUTES(...)
Die Menge der mit dem Operanden GUARD-NAME ausgewählten Guards wird durch weitere Kriterien modifiziert.

TYPE =
Angabe des Guardtyps, auf den die Auswahl beschränkt werden soll.

TYPE = *ANY
Die Guards werden unabhängig von ihrem Typ ausgewählt.

TYPE = list-poss(6): <name 1..8>
Nur Guards des angegeben Typs bzw. der angegebenen Typen werden ausgewählt. Folgende Angaben sind erlaubt:

Guardtyp	Bedeutung
COOWNERP	Regelbehälter für den Miteigentümerschutz
DEFAULTP	Regelbehälter für den Standardschutz
DEFPATTR	Attributguards (Standardschutz)
DEFPUID	Benutzerkennungsguards (Standardschutz)
STDAC	Zugriffsbedingungsguards
UNDEF	Guards undefiniertenTyps

RESOLVE =
Angabe, ob die ausgewählten Guards nach referenzierten Guards durchsucht werden sollen.

RESOLVE = *YES
Ausgewählte Guards werden nach referenzierten Guards durchsucht. Die so gefundenen Referenzguards werden zusätzlich unabhängig von ihrem Namen und Typ ausgewählt.

Guardtyp	Referenzguards
COOWNERP	In den Regeln spezifizierte Zugriffsbedingungsguards
DEFAULTP	In den Regeln spezifizierte Attribut- und Benutzerkennungsguards
DEFPATTR	In den Schutzattributen spezifizierte Guards
DEFPUID	keine
STDAC	keine
UNDEF	keine

RESOLVE = *NO
Die Guards werden nicht nach referenzierten Guards durchsucht. Restauriert werden ausschließlich die aufgrund ihres Namens (Operand GUARD-NAME) und Typs (Operand TYPE) ausgewählten Guards.

BACKUP-FILE-NAME = <filename 1..54 without-gen-vers>
Name der Sicherungsdatei, aus der die gesicherten Guards restauriert werden sollen. Die Angabe der System-Standardkennung im Dateinamen, wie zum Beispiel $<filename> oder $.<filename> ist erlaubt.

NEW-PATH =
Gibt an, ob bei der Restaurierung die Katalogkennung, die Benutzerkennung oder der Guardname geändert werden soll. Außerdem kann angegeben werden, ob die Katalogkennung geändert werden soll, die in einer Zugriffsbedingung des Typs PROGRAM in einem gesicherten STDAC-Guard hinterlegt ist (siehe Operand ADMISSION=(PROGRAM) der Kommandos /ADD-ACCESS-CONDITIONS auf Seite 526 bzw. /MODIFY-ACCESS-CONDITIONS auf Seite 574).

NEW-PATH = *SAME
Bei der Restauration sollen keine Veränderungen an den Pfadnamen vorgenommen werden.

NEW-PATH = *BY-RULE(...)
Bei der Restaurierung sollen Veränderungen im Guardpfadnamen und/oder in Zugriffsbedingungen des Typs PROGRAM durchgeführt werden.

PUBSET-ID = *SAME
Die Katalogkennung der restaurierten Guards soll unverändert aus der Sicherungsdatei übernommen werden.

PUBSET-ID = <catid 1..4>
Neue Katalogkennung, die bei der Restaurierung eines Guards verwendet werden soll.

USERID-ID = *SAME
Die Benutzerkennung der restaurierten Guards soll unverändert aus der Sicherungsdatei übernommen werden.

USER-ID = <name 1..8>
Neue Benutzerkennung, die bei der Restaurierung eines Guards verwendet werden soll. Bei dieser Angabe darf die im Operanden GUARD-NAME angegebene Benutzerkennung keine Musterzeichen enthalten. Die Angabe der System-Standardkennung, wie zum Beispiel $ wird nicht unterstützt.

GUARD-NAME = *SAME
Der Name der restaurierten Guards soll unverändert aus der Sicherungsdatei übernommen werden.

GUARD-NAME = <name 1..8 without-cat-user-gen-vers>
Neuer Guardname, der bei der Restaurierung eines Guards verwendet werden soll. Bei dieser Angabe darf der im Operanden GUARD-NAME angegebene Guardname keine Musterzeichen enthalten.

PROG-PUBSET-ID =
Angabe, ob die Katalogkennung geändert werden soll, die in einer Zugriffsbedingung des Typs PROGRAM in einem gesicherten STDAC-Guard hinterlegt ist (siehe Operand ADMISSION=(PROGRAM) der Kommandos /ADD--ACCESS-CONDITIONS auf Seite 526 bzw. /MODIFY-ACCESS-CONDITIONS auf Seite 574).

PROG-PUBSET-ID = *SAME
Die Katalogkennung im Pfadnamen einer Zugriffsbedingung des Typs PROGRAM soll unverändert aus der Sicherungsdatei übernommen werden.

PROG-PUBSET-ID =
Neue Katalogkennung, die bei der Restaurierung eines Guards in der Zugriffsbedingung des Typs PROGRAM in den Dateinamen eingesetzt werden soll.

TARGET =
Angabe, auf welcher Art und Weise die Guards restauriert werden sollen.

TARGET = *SYSTEM
Die Guards werden von GUARDS-SAVE unmittelbar im laufenden System restauriert. Der Anwender hat dabei keinen Einfluß auf den Restaurierungsablauf.

TARGET = *PROCEDURE(...)
GUARDS-SAVE erzeugt eine Prozedurdatei mit Kommandos, die die gesicherten Guards restaurieren sollen. Die eigentliche Restaurierung muss der Anwender selbst durchführen, indem er die erzeugte Prozedur zum Ablauf bringt. Zuvor kann er sie bei Bedarf mit einem Texteditor wie zum Beispiel dem EDT bearbeiten.

PROC-FILE-NAME = <filename 1..54 without-gen-vers>
Name einer Datei, in die alle die für eine Restaurierung notwendigen Prozedurkommandos geschrieben werden sollen. Der Name ist frei wählbar. Existiert bereits eine Datei gleichen Namens, wird abhängig vom Operanden REPLACE-BACKUP-FILE entweder die Datei überschrieben oder die Anweisung mit einer entsprechenden Fehlermeldung abgewiesen.

REPLACE-PROC-FILE =
Angabe, ob eine gegebenenfalls schon vorhandene Prozedurdatei überschrieben werden soll oder nicht.

REPLACE-PROC-FILE = *NO
Eine gegebenenfalls schon vorhandene Prozedurdatei wird nicht überschrieben.

REPLACE-PROC-FILE = *YES
Eine gegebenenfalls schon vorhandene Prozedurdatei wird überschrieben. Die eingestellten Dateischutzattribute bleiben erhalten.

REPLACE-GUARD =
Dieser Operand bezeichnet, ob ein gegebenenfalls schon vorhandenes Guard durch eine Restaurierung überschrieben werden soll.

REPLACE-GUARD = *NO
Ein gegebenenfalls schon vorhandenes Guard wird nicht überschrieben.

REPLACE-GUARD = *YES
Ein gegebenenfalls schon vorhandenes Guard wird überschrieben.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe einer Ergebnisprotokollierung.

OUTPUT= *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern die Anweisung im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Beispiel: Ausgabe nach einem einer programmgesteuerten Restaurierungslauf

```
//restore-guards guard-name=*,backup-file-name=g-save
%  PRO7021 '2' GUARDS ARE RESTORED OUT OF BACKUP FILE ':XXXX:$MARY.G-SAVE<
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  MARY       2017-12-07/17:31:15
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$MARY.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Restore Guard   : :XXXX:$MARY.*
%Restore Type    : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Restore Resolve : *YES
%Restore Replace : *NO
%Restore Target  : *SYSTEM
%
%New Pubset-Id   : *SAME
%New User-Id     : *SAME
%New Name        : *SAME
%New Prog Pvs-Id : *SAME
%*****************************************************************************
%Restored Guards : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                  Alphabetical List of Restored and Faulty Guards
%
%=============================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$MARY.STDAC         STDAC                    restored
%:XXXX:$MARY.SYS.UCF       COOWNERP                 restored
%=============================================================================
%
%                  Alphabetical List of Cross References
%
%=============================================================================
%:XXXX:$MARY.SYS.UCF       COOWNERP    ->  :XXXX:$MARY.STDAC         STDAC
%-----------------------------------------------------------------------------
%:XXXX:$MARY.STDAC         STDAC       <-  :XXXX:$MARY.SYS.UCF       COOWNERP
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  MARY       2017-12-07/17:31:15
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
%//
```

Eine generierte Prozedur ist im Abschnitt „Prozedurgesteuerte Restaurierung“ auf Seite 901 abgebildet.

SHOW-BACKUP-FILE
Inhalt einer Sicherungsdatei anzeigen

Mit dieser Anweisung können unterschiedliche Angaben über Guards angezeigt werden, die in einer Sicherungdatei gesichert worden sind. Die Menge der für die Anzeige auszuwählenden Guards kann durch Musterzeichen festgelegt werden. Ein nichtprivilegierter Benutzer sich darf nur die Guards seiner eigenen Kennung, ein Guards-Administrator darf sich die Guards aller Kennungen aus der Sicherungsdatei anzeigen lassen.

Neben dem Datum der Sicherung können wahlweise die Namen der gesicherten Guards, deren Attribute, oder eine Querverweisliste der gesicherten Referenzguards angezeigt werden.

Guards können weitere Guards referenzieren. Zum Beispiel können in Regeln für den Miteigentümerschutz Verweise auf Guards des Typs STDAC auftreten. Mit dem Operanden RESOLVE kann gesteuert werden, ob referenzierte Guards automatisch mit angezeigt werden sollen. In diesem Fall werden alle referenzierten Guards unabhängig von ihrem Namen und ihrem Typ für die Sicherung ausgewählt. Das heißt, für sie haben die Angaben der Operanden GUARD-NAME und GUARD-TYPE keine Bedeutung. Es wird eine Querverweisliste erzeugt und nach SYSOUT/ SYSLST ausgegeben. Kann auf ein Referenzguard nicht zugegriffen werden, z.B. weil es dem (nichtprivilegierten) Aufrufer nicht gehört, wird es in der Liste der referenzierten Guards mit einem entsprechenden Fehlercode aufgelistet.

SHOW-BACKUP-**FI**LE

GUARD-NAME = ***** / <filename 1..24 without-gen-vers with-wild(40)>

,**SEL**ECT = ***ALL** / ***BY-ATTR**IBUTES(...)

***BY-ATTR**IBUTES(...)

TYPE = ***ANY** / list-poss(6): <name 1..8>

,**RES**OLVE = ***YES** / ***NO**

,**BACK**UP-**FILE-NAME** = <filename 1..54 without-gen-vers>

,**INF**ORMATION = ***ATTR**IBUTES / ***NAM**ES-**ON**LY / ***SUM**MARY

,**OUTPUT** = ***SYSOUT** / list-poss(2): ***SYSOUT** / ***SYSLST**(...)

***SYSLST**(...)

SYSLST-NUMBER = ***STD** / <integer 1..99>

GUARD-NAME =
Angabe des oder der Guards, die angezeigt werden sollen.

Abhängigkeit zum Operanden SELECT

– Mit der Angabe von `SELECT=*BY-ATTRIBUTES(TYPE=...)` kann eine typabhängige Einschränkung der benannten Guardmenge erzielt werden.

– Bei Angabe von `SELECT=*BY-ATTRIBUTES(RESOLVE=YES)` werden auch referenzierte Guards angezeigt und zwar unabhängig von ihrem Namen und Typ.

GUARD-NAME = *
Bei der Selektion für die Anzeige soll jeder Guardname berücksichtigt werden.

GUARD-NAME = <filename 1..24 without-gen-vers with-wild(40)>
Teil- oder vollqualifizierter Name der Guards, die angezeigt werden sollen. Guardnamen dürfen Musterzeichen enthalten, Musterzeichen in der Benutzerkennung darf nur ein Guards-Administrator angeben.

Eine Katalogkennung darf im Pfadnamen nicht angegeben werden, denn eine Sicherungsdatei kann nur die Guards eines einzelnen Pubsets aufnehmen.

Die Angabe der System-Standardkennung im Guardnamen, wie zum Beispiel $<filename> oder $.<filename>, wird nicht unterstützt.

SELECT =
Angabe der Kriterien, die zusätzlich zum Operanden GUARD-NAME für die Auswahl der anzuzeigenden Guards herangezogen werden sollen.

SELECT = *ALL
Es werden alle Guardtypen und alle referenzierten Guards ausgewählt. Die Referenzguards werden dabei unabhängig von ihrem Namen ausgewählt.

SELECT = *BY-ATTRIBUTES(...)
Die Menge der mit dem Operanden GUARD-NAME ausgewählten Guards wird durch weitere Kriterien modifiziert.

TYPE =
Angabe des Guardtyps, auf den die Auswahl beschränkt werden soll.

TYPE = *ANY
Die Guards werden unabhängig von ihrem Typ ausgewählt.

TYPE = list-poss(6): <name 1..8>
Nur Guards des angegeben Typs bzw. der angegebenen Typen werden ausgewählt. Folgende Angaben sind erlaubt:

Guardtyp	Bedeutung
COOWNERP	Regelbehälter für den Miteigentümerschutz
DEFAULTP	Regelbehälter für den Standardschutz
DEFPATTR	Attributguards (Standardschutz)
DEFPUID	Benutzerkennungsguards (Standardschutz)
STDAC	Zugriffsbedingungsguards
UNDEF	Guards undefiniertenTyps

RESOLVE =
Angabe, ob die ausgewählten Guards nach referenzierten Guards durchsucht werden sollen.

RESOLVE = *YES
Ausgewählte Guards werden nach referenzierten Guards durchsucht. Die so gefundenen Referenzguards werden zusätzlich unabhängig von ihrem Namen und Typ ausgewählt.

Guardtyp	Referenzguards
COOWNERP	In den Regeln spezifizierte Zugriffsbedingungsguards
DEFAULTP	In den Regeln spezifizierte Attribut- und Benutzerkennungsguards
DEFPATTR	In den Schutzattributen spezifizierte Guards
DEFPUID	keine
STDAC	keine
UNDEF	keine

RESOLVE = *NO
Die Guards werden nicht nach referenzierten Guards durchsucht. Angezeigt werden ausschließlich die aufgrund ihres Namens (Operand GUARD-NAME) und Typs (Operand TYPE) ausgewählten Guards.

BACKUP-FILE-NAME = <filename 1..54 without-gen-vers>
Name der Sicherungsdatei, aus der die anzuzeigenden Guards ermittelt werden sollen. Die Angabe der System-Standardkennung im Dateinamen, wie zum Beispiel $<filename> oder $.<filename> ist erlaubt.

INFORMATION =
Legt den Umfang der Anzeige fest.

INFORMATION = *ATTRIBUTES
Es werden die Guardattribute der gesicherten Guards angezeigt.

INFORMATION = *NAMES-ONLY
Es werden nur die Namen der gesicherten Guards angezeigt.

INFORMATION = *SUMMARY
Es werden nur zusammenfassende Informationen aus der Sicherungsdatei angezeigt, jedoch keine Listen mit Guardnamen. Aus dieser Kurzinformation ist zum Beispiel ersichtlich, für welches Pubset und an welchem Datum die Sicherung durchgeführt wurde und wie viele Guards selektiert wurden.

OUTPUT = list-poss(2):
Dieser Operand bestimmt das Ziel der Ausgabe einer Ergebnisprotokollierung.

OUTPUT= *SYSOUT
Die Ausgabe erfolgt auf die Datensichtstation, sofern die Anweisung im Dialog angegeben wurde. Im Batchbetrieb hängt das Ausgabeziel von den Angaben im Job ab.

OUTPUT = *SYSLST(...)
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = *STD
Die Ausgabe erfolgt auf die Systemdatei SYSLST.

SYSLST-NUMBER = <integer 1..99>
Zweistellige Zahl nn, die zur Bildung des Dateinamens SYSLSTnn verwendet wird.

Beispiele für die Ausgabe nach einem Anzeigelauf

Ausgabe der Guardattribute

```
//show-backup-file guard-name=*,             -
                   backup-file-name=g-save, -
                   information=*ATTRIBUTES
%  PRO7019 '2' GUARDS SELECTED OUT OF BACKUP FILE ':XXXX:$MARY.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$MARY.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Show Guard      : :XXXX:$MARY.*
%Show Type       : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Show Resolve    : *YES
%*****************************************************************************
%Selected Guards : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                   Alphabetical List of Selected and Faulty Guards
%
%=============================================================================
%Guard Name               Scope Type    Creation Date       Last Modification
%----------               ----- ----    -------------       -----------------
%:XXXX:$MARY.STDAC        USR  STDAC    2017-12-06/10:12:07 2017-12-06/10:12:12
%                         Referenzguard fur Miteigentuemerschutz
%:XXXX:$MARY.SYS.UCF      USR  COOWNERP 2017-12-06/10:13:54 2017-12-06/10:20:08
%                         Regelbehaelter fuer Miteigentuemerschutz
%=============================================================================
%
%                   Alphabetical List of Cross References
%
%=============================================================================
%:XXXX:$MARY.SYS.UCF       COOWNERP    ->  :XXXX:$MARY.STDAC         STDAC
%-----------------------------------------------------------------------------
%:XXXX:$MARY.STDAC         STDAC       <-  :XXXX:$MARY.SYS.UCF       COOWNERP
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
%//
```

Ausgabe der Guardnamen

```
//show-backup-file guard-name=*,            -
                   backup-file-name=g-save, -
                   information=*NAMES-ONLY
%  PRO7019 '2' GUARDS SELECTED OUT OF BACKUP FILE ':XXXX:$MARY.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$MARY.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Show Guard      : :XXXX:$MARY.*
%Show Type       : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Show Resolve    : *YES
%*****************************************************************************
%Selected Guards : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                   Alphabetical List of Selected and Faulty Guards
%
%=============================================================================
%Guard Name                 Guard Type      Error    Status
%----------                 ----------      -----    ------
%:XXXX:$MARY.STDAC          STDAC
%:XXXX:$MARY.SYS.UCF        COOWNERP
%=============================================================================
%
%                   Alphabetical List of Cross References
%
%=============================================================================
%:XXXX:$MARY.SYS.UCF        COOWNERP    ->  :XXXX:$MARY.STDAC          STDAC
%-----------------------------------------------------------------------------
%:XXXX:$MARY.STDAC          STDAC       <-  :XXXX:$MARY.SYS.UCF        COOWNERP
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
%//
```

Ausgabe einer zusammenfassenden Information

```
//show-backup-file guard-name=*,            -
                   backup-file-name=g-save, -
                   information=*SUMMARY
%  PRO7019 '2' GUARDS SELECTED OUT OF BACKUP FILE ':XXXX:$MARY.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$MARY.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Show Guard      : :XXXX:$MARY.*
%Show Type       : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Show Resolve    : *YES
%*****************************************************************************
%Selected Guards : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%*****************************************************************************
%GUARDS-SAVE  SHOW-BACKUP-FILE  Started by User  MARY       2017-12-07/18:01:00
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
%//
```

5.13.12 Beispiele zu GUARDS-SAVE

Der Anwender PAUL hat auf seiner Kennung PAUL folgende Guards eingerichtet:

```
/show-guard-attributes

     Guard name          Scope   Type      Creation Date       LastMod Date
------------------------------------------------------------------------------
:XXXX:$PAUL.STDAC         SYS  STDAC    2017-12-07/10:08:09 2017-12-07/10:09:25
                          Pauls Coowner Access Condition Guard
:XXXX:$PAUL.SYS.UCF       SYS  COOWNERP 2017-12-07/10:08:54 2017-12-07/10:10:36
                          Pauls Coowner Rule Container Guard
------------------------------------------------------------------------------
Guards selected: 2                                              End of display

/show-access-conditions

:XXXX:$PAUL.STDAC
   User   SUSI     has ADMISSION
------------------------------------------------------------------------------
Guards selected: 1                                              End of display

/show-coowner-protection-rule

------------------------------------------------------------------------------
RULE CONTAINER :XXXX:$PAUL.SYS.UCF                  ACTIVE  COOWNER PROTECTION
------------------------------------------------------------------------------
RULE1          OBJECT      = *
               CONDITIONS  = $PAUL.STDAC
               TSOS-ACCESS = SYSTEM-STD
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                      END OF DISPLAY
```

Der Anwender PAUL startet eine GUARDS-SAVE-Sitzung:

```
/start-guards-save

%  PROLOAD Program 'SAVELLM', Version 'O55' of '2018-03-01' loaded from file
 ':4V08:$TSOS.SYSLNK.GUARDS-SAVE.O55'
 %  PROCOPY Copyright (C) 'Fujitsu Technology Solutions' '2018' All Rights Reserved
```

Der Anwender PAUL möchte seinen gesamten Guardbestand in eine Sicherungsdatei übertragen:

```
//backup-guards guard-name=*,backup-file-name=g-save
```

```
%  PRO7014 '2' GUARDS SAVED IN BACKUP FILE ':XXXX:$PAUL.G-SAVE'
%*****************************************************************************
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  PAUL       2017-12-07/14:11:58
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$PAUL.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%
%Backup Guard    : :XXXX:$PAUL.*
%Backup Type     : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Backup Resolve  : *YES
%*****************************************************************************
%Saved  Guards   : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                  Alphabetical List of Saved and Faulty Guards
%
%=============================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$PAUL.STDAC         STDAC                    saved
%:XXXX:$PAUL.SYS.UCF       COOWNERP                 saved
%=============================================================================
%
%                  Alphabetical List of Cross References
%
%=============================================================================================
%:XXXX:$PAUL.SYS.UCF       COOWNERP    ->  :XXXX:$PAUL.STDAC         STDAC
%---------------------------------------------------------------------------------------------
%:XXXX:$PAUL.STDAC         STDAC       <-  :XXXX:$PAUL.SYS.UCF       COOWNERP
%=============================================================================================
%
%*****************************************************************************
%GUARDS-SAVE  BACKUP-GUARDS     Started by User  PAUL       2017-12-07/14:11:58
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
```

Anhand des Protokolls hat sich der Anwender PAUL überzeugt, dass die Sicherung fehlerfrei durchgeführt wurde. Die XREF-Liste zeigt ihm, das in seinem Guardbestand keine Referenzen zu fremden Guards auftreten, die den Sicherungsstand damit unter Umständen unvollständig gemacht hätten.

Anmerkung

Um das Protokoll zu verkürzen, wird in den folgenden Beispielen auf ein RESOLVE verzichtet. In der Praxis sollte ein RESOLVE nur nur dann ausgeschaltet werden, wenn zum Beispiel nur Regelbehälter ohne die von ihnen referenzierten Guards bearbeitet werden sollen.

Der Anwender PAUL startet nun einen programmgesteuerten Restaurierungslauf, mit dem er alle seine gesicherten Guards wieder ins System übertragen will:

```
//restore-guards guard-name=*,select=(resolve=*no),backup-file-name=g-save

%  PRO7021 'O' GUARDS RESTORED OUT OF BACKUP FILE ':XXXX:$PAUL.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:31:15
%                               -------------------------
%                                ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$PAUL.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Restore Guard   : :XXXX:$PAUL.*
%Restore Type    : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Restore Resolve : *NO
%Restore Replace : *NO
%Restore Target  : *SYSTEM
%
%New Pubset-Id   : *SAME
%New User-Id     : *SAME
%New Name        : *SAME
%New Prog Pvs-Id : *SAME
%*****************************************************************************
%Restored Guards : 0
%Faulty Guards   : 2
%*****************************************************************************
%
%                  Alphabetical List of Restored and Faulty Guards
%
%=============================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$PAUL.STDAC         STDAC           PRO1006  not restored or overwritten
%:XXXX:$PAUL.SYS.UCF       COOWNERP        PRO1006  not restored or overwritten
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:31:15
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
```

Der programmgesteuerte Restaurierungslauf ist fehlgeschlagen. Um zu erfahren, warum keine Guards restauriert wurden, gibt der Anwender PAUL ein /HELP-Kommando auf die Meldungsnummer PRO1006:

```
//execute help pro1006

%  PRO1006 GUARD '(&OO)' ALREADY EXISTS. FUNCTION NOT PROCESSED
```

Nun startet der Anwender PAUL den Lauf noch einmal und gibt an, dass die im System vorhandenen Guards bei der Restaurierung überschrieben werden sollen:

```
//restore-guards guard-name=*, -
//                select=(resolve=*no), -
//                backup-file-name=g-save, -
//                replace-guard=*yes
```

```
%  PRO7021 '2' GUARDS RESTORED OUT OF BACKUP FILE ':XXXX:$PAUL.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:35:06
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$PAUL.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Restore Guard   : :XXXX:$PAUL.*
%Restore Type    : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Restore Resolve : *NO
%Restore Replace : *YES
%Restore Target  : *SYSTEM
%
%New Pubset-Id   : *SAME
%New User-Id     : *SAME
%New Name        : *SAME
%New Prog Pvs-Id : *SAME
%*****************************************************************************
%Restored Guards : 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                  Alphabetical List of Restored and Faulty Guards
%
%=============================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$PAUL.STDAC         STDAC                    restored
%:XXXX:$PAUL.SYS.UCF       COOWNERP                 restored
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:35:06
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
```

Der Anwender PAUL möchte seinen Guardbestand auch seiner nichtprivilegierten Kollegin MARY zur Verfügung stellen, die auf dem Pubset ZZZZ arbeitet. Der Anwender PAUL erstellt für sie eine Kommandoprozedur und lässt dabei das Pubset XXXX in ZZZZ umbenennen und die Benutzerkennung PAUL in MARY. Die Prozedurkommandos sollen so generiert werden, dass bei der Anwenderin MARY keine vorhandenen Guards überschrieben werden.

```
//restore-guards guard-name=*, -
//                select=(resolve=*no), -
//                backup-file-name=g-save, -
//                new-path=(pubset-id=zzzz,user-id=mary), -
//                target=(proc-file-name=prc.mary,replace-proc-file=*yes)

%  PRO7021 '2' GUARDS RESTORED OUT OF BACKUP FILE ':XXXX:$PAUL.G-SAVE
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:40:45
%                               -------------------------
%                               ***  Begin of Output  ***
%*****************************************************************************
%Backup File     : :XXXX:$PAUL.G-SAVE
%Backup Date     : 2017-12-07/14:11:58
%Backup Pubset   : XXXX
%Backup Guards   : 2
%
%Restore Guard   : :XXXX:$PAUL.*
%Restore Type    : COOWNERP, DEFAULTP, DEFPATTR, DEFPUID , STDAC   , UNDEF
%Restore Resolve : *NO
%Restore Replace : *NO
%Restore Target  : $PAUL.PRC.MARY
%
%New Pubset-Id   : ZZZZ
%New User-Id     : MARY
%New Name        : *SAME
%New Prog Pvs-Id : *SAME
%*****************************************************************************
%Generated Guards: 2
%Faulty Guards   : 0
%*****************************************************************************
%
%                  Alphabetical List of Restored and Faulty Guards
%
%=============================================================================
%Guard Name                Guard Type      Error    Status
%----------                ----------      -----    ------
%:XXXX:$PAUL.STDAC         STDAC                    generated and path changed
%:XXXX:$PAUL.SYS.UCF       COOWNERP                 generated and path changed
%=============================================================================
%
%*****************************************************************************
%GUARDS-SAVE  RESTORE-GUARDS    Started by User  PAUL       2017-12-07/17:40:45
%                               -------------------------
%                               ***   End of Output   ***
%*****************************************************************************
```

Der Anwender PAUL ist fertig und kann die GUARDS-SAVE-Sitzung beenden. Danach lässt er sich die erzeugte Prozedur anzeigen:

```
//end
/show-file PRC.MARY

/ BEGIN-PROCEDURE LOGGING=*NO
/
/ REMARK MOD-JOB-OPT LOGGING=(LISTING=*YES)
/ STEP
/ ASSIGN-SYSLST TO=#RESTORE.LST.2017-12-07.174045
/ STEP
/
/ WRI-TEXT '*********************************************************'
/ WRI-TEXT 'GUARDS-SAVE                                  RESTORE-GUARDS'
/ WRI-TEXT 'Proc Generated by User  PAUL      at  2017-12-07/17:40:45'
/ WRI-TEXT '*********************************************************'
/ WRI-TEXT '                  ***  Begin  ***                         '
/          "*********************************************************"
/          "Backup File     : :XXXX:$PAUL.G-SAVE                     "
/          "Backup Date     : 2017-12-07/14:11:58                    "
/          "Backup Pubset   : XXXX                                   "
/          "                                                         "
/          "Restore Guard   : :XXXX:$PAUL.*                          "
/          "Restore Type    : COOWNERP, DEFAULTP, DEFPATTR,          "
/          "                  DEFPUID , STDAC   , UNDEF              "
/          "Restore Resolve : *NO                                    "
/          "Restore Replace : *NO                                    "
/          "                                                         "
/          "New Pubset-Id   : ZZZZ                                   "
/          "New User-Id     : MARY                                   "
/          "New Name        : *SAME                                  "
/          "New Prog Pvs-Id : *SAME                                  "
/          "*********************************************************"
/          "** ================================================= **"
/          "**                                                     **"
/          "** Guard    :XXXX:$PAUL.STDAC         STDAC    0000001 **"
/          "** -->      :ZZZZ:$MARY.STDAC                        **"
/          "**                                                     **"
/          "** ================================================= **"
/           CRE-GUARD :ZZZZ:$MARY.STDAC                              -
/              ,SCOPE=*HOST-SYSTEM                                   -
/              ,USER-INFO='Pauls Coowner Access Condition Guard      '
/ WRI-TEXT '** :ZZZZ:$MARY.STDAC         STDAC     created         **'
/           SKIP .R0000001
/           STEP
/ WRI-TEXT '** :ZZZZ:$MARY.STDAC         STDAC     create  *error* **'
/           SKIP .E0000001
/
/           .R0000001
/           ADD-ACCESS-CONDITIONS :ZZZZ:$MARY.STDAC                  -
/              ,SUBJECTS=*USER(USER-IDENTIFICATION=SUSI    )         -
/              ,ADMISSION=*YES                                       -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '** :ZZZZ:$MARY.STDAC         STDAC     restored        **'
/           SKIP .E0000001
/           STEP
/ WRI-TEXT '** :ZZZZ:$MARY.STDAC         STDAC     restore *error* **'
/           SKIP .E0000001
/           .E0000001
/
```

```
/          "** ================================================ **"
/          "**                                                  **"
/          "** Guard    :XXXX:$PAUL.SYS.UCF       COOWNERP 0000002 **"
/          "** -->      :ZZZZ:$MARY.SYS.UCF                     **"
/          "**                                                  **"
/          "** ================================================ **"
/           CRE-GUARD :ZZZZ:$MARY.SYS.UCF                          -
/              ,SCOPE=*HOST-SYSTEM                                 -
/              ,USER-INFO='Pauls Coowner Rule Container Guard     '
/ WRI-TEXT '** :ZZZZ:$MARY.SYS.UCF       COOWNERP  created       **'
/           SKIP .R0000002
/           STEP
/ WRI-TEXT '** :ZZZZ:$MARY.SYS.UCF       COOWNERP  create  *error* **'
/           SKIP .E0000002
/
/           .R0000002
/           ADD-COOWNER-PROTECTION-RULE :ZZZZ:$MARY.SYS.UCF        -
/              ,PROTECTION-RULE=RULE1                              -
/              ,RULE-POSITION=*LAST                                -
/              ,PROTECT-OBJECT=*PARAMETERS                         -
/                (NAME=*                                           -
/                ,CONDITION-GUARD=$MARY.STDAC                      -
/                ,TSOS-ACCESS=*SYSTEM-STD)                         -
/              ,GUARD-CHECK=*NO                                    -
/              ,DIALOG-CONTROL=*NO
/ WRI-TEXT '** :ZZZZ:$MARY.SYS.UCF       COOWNERP  restored      **'
/           SKIP .E0000002
/           STEP
/ WRI-TEXT '** :ZZZZ:$MARY.SYS.UCF       COOWNERP  restore *error* **'
/           SKIP .E0000002
/
/           .E0000002
/          "************************************************************"
/          "Guard Name                Guard Type Error   Status       "
/          "----------                ---------- -----   ------       "
/          ":XXXX:$PAUL.STDAC         STDAC              generated    "
/          ":XXXX:$PAUL.SYS.UCF       COOWNERP           generated    "
/          "------------------------------------------------------------"
/          "Generated Guards: 2                                        "
/          "Faulty Guards   : 0                                        "
/          "************************************************************"
/
/ WRI-TEXT '************************************************************'
/ WRI-TEXT '                    ***  End  ***                           '
/ WRI-TEXT '************************************************************'
/ WRI-TEXT 'GUARDS-SAVE                                  RESTORE-GUARDS'
/ WRI-TEXT 'Proc Generated by User  PAUL      at  2017-12-07/17:40:45'
/ WRI-TEXT '************************************************************'
/
/ STEP
/ ASSIGN-SYSLST TO=*PRIMARY
/ STEP
/
/ END-PROCEDURE
```

Am nächsten Tag lässt die Anwenderin MARY die vom Anwender PAUL generierte Prozedur unter ihrer Kennung ablaufen:

```
/call-procedure $paul.prc.mary
```

```
************************************************************
GUARDS-SAVE                                  RESTORE-GUARDS
Proc Generated by User  PAUL      at  2017-12-07/17:40:45
************************************************************
                  ***  Begin  ***
************************************************************
** :ZZZZ:$MARY.STDAC          STDAC     created          **
** :ZZZZ:$MARY.STDAC          STDAC     restored         **
** ------------------------------------------------------ **
** :ZZZZ:$MARY.SYS.UCF        COOWNERP  created          **
** :ZZZZ:$MARY.SYS.UCF        COOWNERP  restored         **
************************************************************
                  ***   End   ***
************************************************************
GUARDS-SAVE                                  RESTORE-GUARDS
Proc Generated by User  PAUL      at  2017-12-07/17:40:45
************************************************************
```

Unter der Benutzerkennung der Anwenderin MARY sind nun folgende Guards eingerichtet:

```
/show-guard-attributes
```

```
     Guard name          Scope   Type      Creation Date       LastMod Date
------------------------------------------------------------------------------
:ZZZZ:$MARY.STDAC         SYS  STDAC    2017-12-08/08:28:09 2017-12-08/08:28:25
                          Pauls Coowner Access Condition Guard
:ZZZZ:$MARY.SYS.UCF       SYS  COOWNERP 2017-12-08/08:28:54 2017-12-08/08:29:36
                          Pauls Coowner Rule Container Guard
------------------------------------------------------------------------------
Guards selected: 2                                          End of display
```

```
/show-access-conditions
```

```
:ZZZZ:$MARY.STDAC
   User   SUSI     has ADMISSION
------------------------------------------------------------------------------
Guards selected: 1                                          End of display
```

```
/show-coowner-protection-rule
```

```
------------------------------------------------------------------------------
RULE CONTAINER :XXXX:$MARY.SYS.UCF                  ACTIVE  COOWNER PROTECTION
------------------------------------------------------------------------------
RULE1         OBJECT      = *
CONDITIONS  = $MARY.STDAC
              TSOS-ACCESS = SYSTEM-STD
------------------------------------------------------------------------------
RULE CONTAINER SELECTED: 1                                  END OF DISPLAY
```

5.13.13 Verhalten von GUARDS-SAVE im Fehlerfall

Beim Auftreten von Systemfehlern während eines GUARDS-SAVE-Laufs gibt GUARDS-SAVE die Meldung PRO7012 aus. Der Fehlertext und Fehlercode dieser Meldung sollten dem Systemverwalter für eine Diagnose bekannt gegeben werden.

Nach der Ausgabe der Fehlermeldung PRO7012 bricht GUARDS-SAVE die Verarbeitung der aktuellen Anweisung ab und erwartet die Eingabe weiterer Anweisungen.

5.13.14 GUARDS-SAVE - Installation und Inbetriebnahme

Benötigte Dateien

Datei	Name der Datei
Modulbibliothek (notwendig für den Aufruf mit START-GUARDS-SAVE)	SYSLNK.GUARDS-SAVE.nnn
Ausführbares Programm (notwendig für den Aufruf mit START-EXECUTABLE-PROGRAM bzw. START-PROGRAM)	SYSPRG.GUARDS-SAVE.nnn
SDF-Syntaxdatei	SYSSDF.GUARDS-SAVE.nnn
IMON-Installationsdatei	SYSSII.GUARDS-SAVE.nnn

Die Angabe nnn bezeichnet die Versionsangabe von GUARDS-SAVE, siehe Freigabemitteilung.

Die Meldungen für GUARDS-SAVE sind in der Meldungsdatei von GUARDS enthalten.

Voraussetzungen

– Subsysteme GUARDS, GUARDDEF, GUARDCOO

6 Anhang

Dieses Kapitel enthält eine Liste der Kommando- und Makro-Operanden, auf die sich die Einschränkung der TSOS-Miteigentümerschaft auswirkt.

6.1 Wirksamkeit der TSOS-Einschränkung

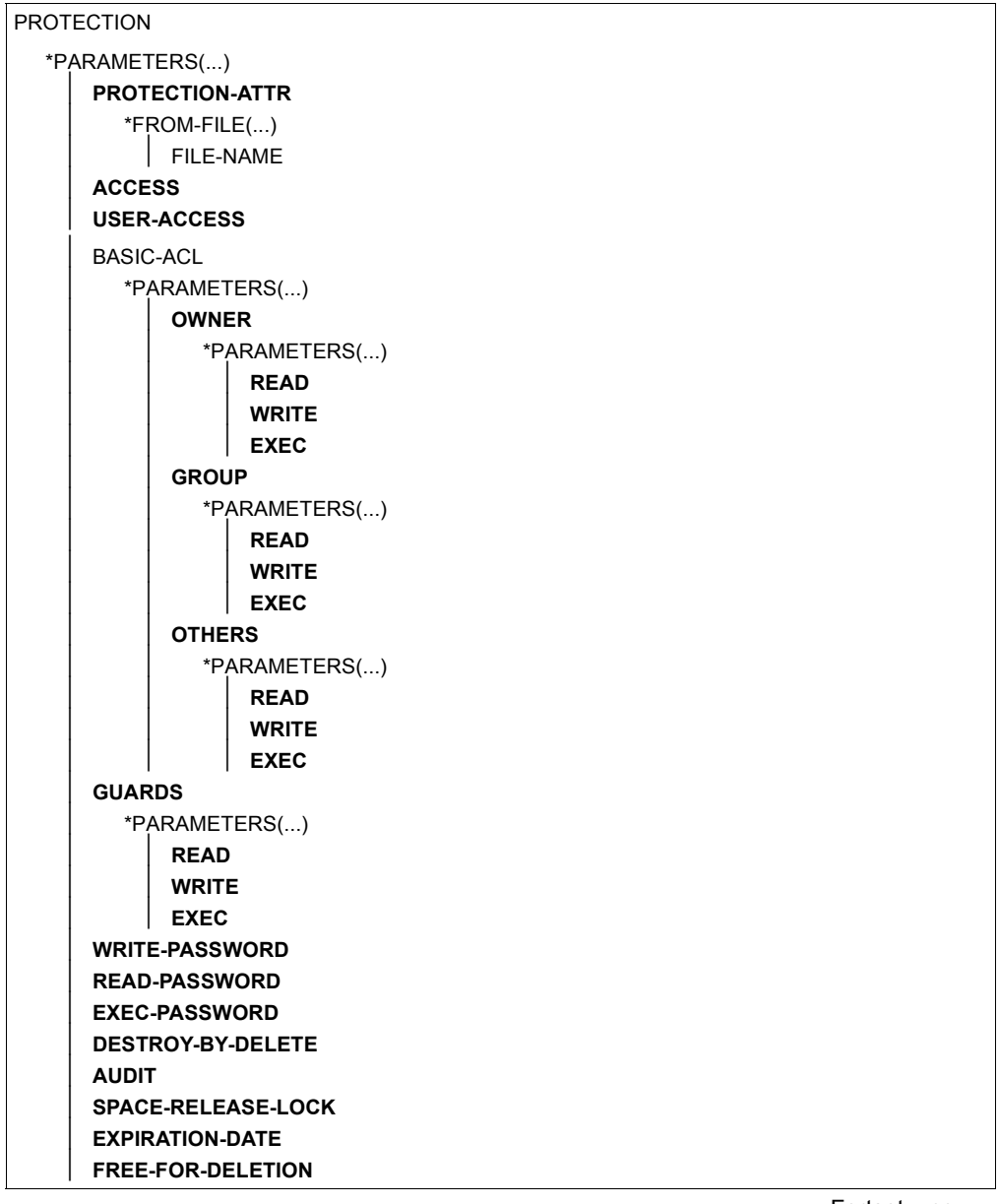
Um durch durch die Einschränkung der TSOS-Miteigentümerschaft den allgemeinen Systemablauf nicht zu gefährden, darf diese nicht generell wirksam sein. Sie wirkt sich deshalb lediglich auf ganz bestimmte Systemfunktionen in einer ganz bestimmten Ablaufumgebung aus.

Die Einschränkung des TSOS-Mitverwaltungsrechts gilt nur für Dialog- oder Batchtasks unter der Benutzerkennung TSOS und hat Auswirkungen auf die Nutzung folgende Funktionen:

- Beim Kommando **/MODIFY-FILE-ATTRIBUTES** wirkt sich die Einschränkung des Mitverwaltungsrechts von TSOS auf die in folgender Übersicht **halbfett** dargestellten Operanden aus:

```
FILE-NAME
NEW-NAME
SUPPORT
  *PUBLIC-DISK(...)
    | STORAGE-CLASS
    |   *NONE(...)
    |     | WORK-FILE
    |     | IO_ATTRIBUTES
    |     | *PARAMETERS(...)
    |     |     | PERFORMANCE
    |     |     | USAGE
    |     | DISK-WRITE
    |     | AVAILABILITY
    |     | FILE-PREFORMAT
    |     | VOLUME-SET
    |     | VOLUME
    |     | DEVICE-TYPE
    |     | SO-MIGRATION
    | SPACE
    |   *RELATIVE(...)
    |     | PRIMARY-ALLOCATION
    |     | SECONDARY-ALLOCATION
    |   *ABSOLUTE(...)
    |     | FIRST-PAGE
    |     | SIZE
    |   *RELEASE(...)
    |     | NUMBER-OF-PAGES
    |     | KEEP-MIN-ALLOCATION
    | MANAGEMENT-CLASS
    | USER-INFORMATION
    | ADM-INFORMATION
  *PRIVATE-DISK(...)
    | ...
  *ANY-DISK(...)
    | ...
  *TAPE(...)
    | ...
```

Fortsetzung ➠



Fortsetzung ➟

```
SAVE
    *PARAMETERS(...)
        BACKUP-CLASS
        SAVED-PAGES
MIGRATE
CODED-CHARACTER-SET
DIALOG-CONTROL
OUTPUT
```

- Beim Kommando **/MODIFY-GENERATION-SUPPORT** wirkt sich die Einschränkung des Mitverwaltungsrechts von TSOS auf die nachfolgend **halbfett** dargestellten Operanden aus:

```
GENERATION-NAME
SUPPORT
    *PUBLIC-DISK(...)
        STORAGE-CLASS
            *NONE(...)
                IO_ATTRIBUTES
                *PARAMETERS(...)
                    PERFORMANCE
                    USAGE
                DISK-WRITE
                AVAILABILITY
                FILE-PREFORMAT
                VOLUME-SET
                VOLUME
                DEVICE-TYPE
                SO-MIGRATION
        SPACE
            *RELATIVE(...)
                PRIMARY-ALLOCATION
                SECONDARY-ALLOCATION
            *ABSOLUTE(...)
                FIRST-PAGE
                SIZE
            *RELEASE(...)
                NUMBER-OF-PAGES
                KEEP-MIN-ALLOCATION
```

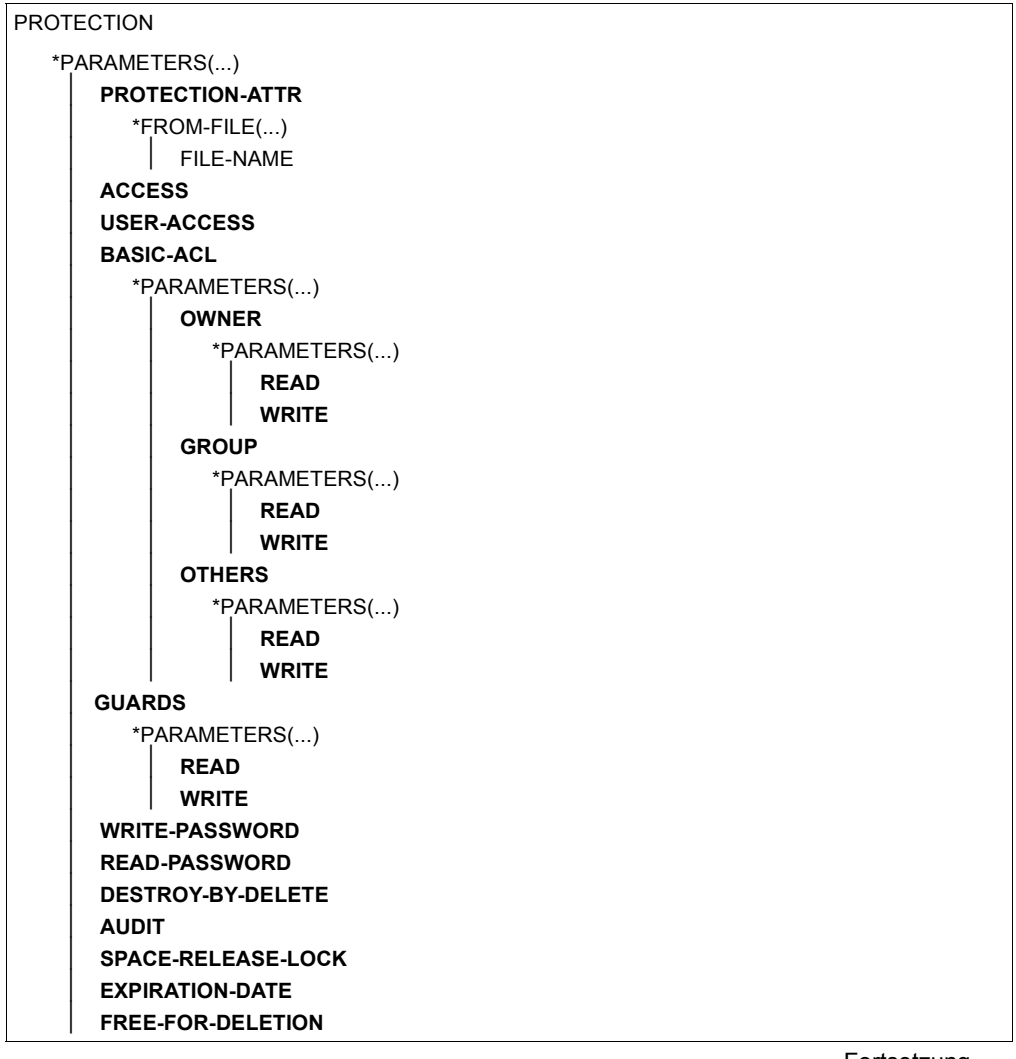
Fortsetzung ➟

```
        USER-INFORMATION
        ADM-INFORMATION
    *PRIVATE-DISK(...)
        ...
    *ANY-DISK(...)
        ...
    *TAPE(...)
        ...
DIALOG-CONTROL
OUTPUT
```

- Beim Kommando **/MODIFY-FILE-GROUP-ATTRIBUTES** betrifft die Einschränkung des Mitverwaltungsrechts von TSOS die in folgender Übersicht **halbfett** dargestellten Operanden:

```
GROUP-NAME
NEW-NAME
GENERATION-PARAMETER
    *GENERATION-PARAMETER(...)
        MAXIMUM
        OVERFLOW-OPTION
        BASE-NUMBER
        *ABSOLUTE(...)
            NUMBER
        *RELATIVE-TO-LAST-GENERATION(..)
            NUMBER
```

Fortsetzung ➠



Fortsetzung ➟

SAVE

*PARAMETERS(...)

BACKUP-CLASS

SAVED-PAGES

MANAGEMENT-CLASS

MIGRATE

CODED-CHARACTER-SET

USER-INFORMATION

ADM-INFORMATION

STOR-CLASS-DEFAULT

DIALOG-CONTROL

OUTPUT

- Beim Makro **CATAL** in Verbindung mit **STATE=*UPDATE** sind die folgenden Operanden von der Einschränkung der TSOS-Miteigentümerschaft betroffen:

  ACCESS
  ADMINFO
  AUDIT
  AVAIL
  BACKUP
  BASACL
  BASE
  DELDATE
  DESTROY
  DISKWR
  DISP
  EXDATE
  EXPASS
  GEN
  GROUPAR (READ, WRITE, EXEC)
  GUARDS (READ, WRITE, EXEC)
  IOPERF
  IOUSAGE
  LARGE
  MANCLAS
  MIGRATE
  NEWNAME
  OTHERAR (READ, WRITE, EXEC)
  OWNERAR (READ, WRITE, EXEC)
  PROTECT
  RDPASS
  RELSPAC
  SHARE
  S0MIGR
  STOCLAS
  USRINFO
  WRPASS

- Beim Kommando **/DELETE-FILE** bezieht sich die Einschränkung nur auf die Angabe **IGNORE-PROTECTION=*ACCESS**, und zwar in folgender Weise:
  - Will der Benutzer TSOS eine fremde Datei löschen, für die das TSOS-Mitverwaltungsrecht eingeschränkt ist, bleibt die Angabe IGNORE-PROTECTION= *ACCESS unberücksichtigt. Damit hängt es von den Schutzmerkmalen der Datei ab, ob TSOS die Datei löschen darf.
  - Will TSOS eine Datei unter der Kennung TSOS löschen, dann wird die Angabe IGNORE-PROTECTION=*ACCESS auch dann berücksichtigt, wenn – unsinnigerweise – das TSOS-Mitverwaltungsrecht eingeschränkt ist. Das Löschen einer **eigenen** Datei kann somit unabhängig von den Schutzmerkmalen der Datei durchgeführt werden.
- Für den Makro-Aufruf **ERASE** mit **IGNORE=ACCESS** gelten die Erläuterungen zum Kommando DELETE-FILE in entsprechender Weise.
- Beim Kommando **/COPY-FILE** wirkt sich die Einschränkung folgendermaßen auf die Angabe des Operanden **IGNORE-PROTECTION** aus:
  - Will TSOS Dateien kopieren und verwendet dabei die Angabe IGNORE-PROTECTION=*SOURCE-FILE oder IGNORE-PROTECTION=*TARGET-FILE in Bezug auf eine Datei unter einer fremden Benutzerkennung, so wird die jeweilige Angabe nicht berücksichtigt. TSOS kann die Datei dann nur kopieren, wenn es die Zugriffsrechte der Ursprungs- und/oder Zieldatei erlauben.
  - Im Zusammenhang mit **eigenen** Dateien werden die Angaben IGNORE-PROTECTION=*SOURCE-FILE oder IGNORE-PROTECTION=*TARGET-FILE berücksichtigt, selbst wenn – unsinnigerweise – das TSOS-Mitverwaltungsrecht eingeschränkt ist. Damit kann TSOS eigene Dateien immer unabhängig von deren Zugriffsrechten kopieren.
- Für den Makro-Aufruf **COPFILE** mit **IGNORE=*SOURCE/*TARGET** gelten die Erläuterungen zum Kommando COPY-FILE in entsprechender Weise.

- Beim Kommando **/MODIFY-JV-ATTRIBUTES** hat die Einschränkung des Mitverwaltungsrechts von TSOS auf die in folgender Übersicht **halbfett** dargestellten Operanden:

```
JV-NAME
NEW-NAME
PROTECTION(...)
    ACCESS
    USER-ACCESS
    BASIC-ACL
      *PARAMETERS(...)
        OWNER
          *PARAMETERS(...)
            READ
            WRITE
        GROUP
          *PARAMETERS(...)
            READ
            WRITE
        OTHERS
          *PARAMETERS(...)
            READ
            WRITE
    GUARDS
      *PARAMETERS(...)
        READ
        WRITE
    WRITE-PASSWORD
    READ-PASSWORD
    RETENTION-PERIOD
    MONJV-PROTECTION
    MANAGEMENT-CLASS
```

- Beim Makro **CATJV** in Verbindung mit **STATE=*UPDATE** sind die folgenden Operanden von der Einschränkung der TSOS-Miteigentümerschaft betroffen:

  jvname2
  ACCESS
  BASACL
  GROUPAR (READ, WRITE)
  GUARDS (READ, WRITE)
  MANCLAS
  MONJV
  OTHERAR (READ, WRITE)
  OWNERAR (READ, WRITE)
  RDPASS
  RETPD
  SHARE
  WRPASS

- Beim Kommando **/DELETE-JV** bezieht sich die Einschränkung nur auf die Angabe **IGNORE-PROTECTION=*ACCESS**, und zwar in folgender Weise:

  – Will der Benutzer TSOS eine fremde Jobvariable löschen, für die das TSOS-Mitverwaltungsrecht eingeschränkt ist, bleibt die Angabe IGNORE-PROTECTION= *ACCESS unberücksichtigt. Damit hängt es von den Schutzmerkmalen der Jobvariablen ab, ob TSOS die Jobvariable löschen darf.

  – Will TSOS eine Jobvariable unter der Kennung TSOS löschen, dann wird die Angabe IGNORE-PROTECTION=*ACCESS auch dann berücksichtigt, wenn – unsinnigerweise – das TSOS-Mitverwaltungsrecht eingeschränkt ist. Das Löschen einer **eigenen** Jobvariablen kann somit unabhängig von den Schutzmerkmalen der Jobvariablen durchgeführt werden.

- Für den Makro-Aufruf **ERAJV** mit **IGNORE=ACCESS** gelten die Erläuterungen zum Kommando DELETE-JV in entsprechender Weise.

Fachwörter

Die folgende Übersicht enthält Definitionen bzw. Erläuterungen zu Begriffen, die in diesem Handbuch im Zusammenhang mit den Funktionseinheiten verwendet werden.

Abrechnungsnummer
Account Number

Sie bezeichnet ein Abrechnungskonto für die zugehörige Benutzerkennung. Eine Abrechnungsnummer kann mehreren Benutzerkennungen zugewiesen werden; eine Benutzerkennung kann über mehrere (bis zu 60) Abrechnungsnummern verfügen. Die Abrechnungsnummer wird bei SET-LOGON-PARAMETERS (bzw. LOGON) und ENTER-JOB ausgewertet.

Ämterhäufung
Function Accumulation

Soll eine Benutzerkennung auf einem Pubset als Gruppenverwalter bestimmt werden (ADD/MODIFY-USER-GROUP), so wird das Kommando zurückgewiesen, wenn die Benutzerkennung das Recht „systemglobale Benutzerverwaltung“ auf diesem Pubset oder auf dem Home-Pubset besitzt.
Soll einer Benutzerkennung auf einem Pubset das Recht „systemglobale Benutzerverwaltung“ zugewiesen werden (SET-PRIVILEGE), so wird dies zurückgewiesen, wenn die Benutzerkennung auf diesem Pubset Verwalter einer Benutzergruppe ist.

Attributguard
Attribute Guard

Spezielles *Guard*, in dem Standardwerte für Schutzattribute von Objekte festgelegt werden.

Authentisierung
Authentication

Nachweis einer angegebenen Identität.

BACL

siehe *Einfache Zugriffskontrollliste*

Benutzer
User

Er wird von einer Benutzerkennung repräsentiert. Der Begriff Benutzer ist ein Synonym für Personen, Anwendungen, Verfahren etc., die über eine Benutzerkennung Zugang zum Betriebssystem erhalten können.

Benutzerattribute
User Attribute

Alle Merkmale einer Benutzerkennung, die im Benutzerkatalog hinterlegt sind.

Benutzergruppe
User Group

Eine Benutzergruppe ist die Zusammenfassung einzelner Benutzer und hat einen Namen (Benutzergruppenkennung).

Benutzergruppeneintrag
Group Entry

Sätze im Benutzerkennungskatalog (ehemals $TSOS.TSOSJOIN, neuer Name siehe *Benutzerkennungskatalog*), die die Daten für eine Benutzergruppe enthalten.

Benutzergruppenkennung
Group Identificaton

Name einer Benutzergruppe, der beim Einrichten der Benutzergruppe vergeben wird. Über die Benutzergruppenkennung wird die Benutzergruppe angesprochen.

Benutzerkatalog

siehe *Benutzerkennungskatalog*

Benutzerkennung (USER-ID)
User Identification

Ist ein maximal acht Zeichen langer Name und wird im Benutzerkatalog eingetragen.
Anhand der Benutzerkennung wird der Benutzer beim Systemzugang identifiziert. Alle Dateien und Jobvariablen werden unter einer Benutzerkennung eingerichtet. Die Namen der Dateien und Jobvariablen werden mit der Benutzerkennung im Dateikatalog hinterlegt.

Benutzerkennungskatalog
User ID catalog

Datei $TSOS.SYSSRPM, die die Benutzerattribute aller Benutzerkennungen eines Pubsets enthält.
Synonym: Benutzerkatalog

Benutzerkommando
User Command
: Kommandos, die unter einer beliebigen Benutzerkennung im Systemmodus (/) oder auch im Programm-Modus mit CMD-Makros gegeben werden können.

Benutzerorganisation
User organization
: Die Zusammenfassung von Benutzerkennungen zu Benutzergruppen. Hierdurch wird die Nachbildung bestehender Organisationsformen ebenso gestattet wie die projektorientierte Zusammenfassung von Benutzern.

Benutzerrechte
User Privilege
: Alle an eine Benutzerkennung vergebenen und im Benutzerkennungskatalog hinterlegten Attribute, die Rechte darstellen.

Benutzerverwaltung
User Administration
: siehe *Systemglobale Benutzerverwaltung*

Beweissicherung
Audit
: Grundfunktion eines sicheren Systems; Protokollierung von Abläufen und Aufbereitung der protokollierten Daten.

CONSLOG-Datei
CONSLOG file
: Protokolldatei, in der der gesamte Nachrichtenverkehr zwischen Bedienstationen, berechtigten Benutzerprogrammen und dem System aufgezeichnet wird.

Co-owner Protection
: siehe *Miteigentümerschutz*

Dateikatalog
File Directory
: Datei, die auf jedem Pubset vorhanden ist (in SM-Pubsets auf jedem Volumeset). Jede Datei und jede Jobvariable eines Pubsets sind im entsprechenden Dateikatalog eingetragen. Dateien von Privatplatten und Bändern können im Dateikatalog eingetragen sein.
Ein Katalogeintrag enthält alle Attribute (Schutzattribute, Lage der verwalteten Daten usw.) einer Datei bzw. einer Jobvariablen.

Datenschutz
Data Protection

Im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, durch den Schutz der personenbezogenen Daten vor Mißbrauch bei der Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

Im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Mißbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

– Datenschutz wird im Unternehmen realisiert durch
– Einhaltung von Unternehmensgrundsätzen und Unternehmensrichtlinien,
– Einhaltung von gesetzlichen Vorschriften,
– problembewußtes Handeln,
– zweckentsprechende Anwendung der Datensicherung.

Datensicherung
Data Security

Technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten; d.h. insbesondere zu erreichen, dass
– der Zugriff zu Daten nur Berechtigten möglich ist,
– keine unerwünschte bzw. unberechtigte Verarbeitung von Daten erfolgt,
– die Daten bei der Verarbeitung nicht verfälscht werden,
– die Daten reproduzierbar sind.

Diese Aufgabe wird gelöst durch
– in Hardware und Software enthaltene technische und organisatorische Vorkehrungen und Maßnahmen,
– übrige organisatorische sowie bauliche und personelle Vorkehrungen und Maßnahmen.

Datensichtstation
Terminal

E/A-Gerät, bestehend aus Tastatur und Bildschirm, das über Netzsoftware dem Verarbeitungsrechner (VAR) angeschlossen ist.
Die Datensichtstation kann dem VAR direkt (über MSN) angeschlossen sein oder sie kann eine Komponente eines Kommunikationsrechners sein (Adressierung über Stations- bzw. Transportsystemadresse).

Default Protection

siehe *Standardschutz*

Eigentümer
Owner
: Benutzerkennung, unter der ein *Objekt* eingerichtet ist

Einfache Zugriffskontrollliste BACL
Basic Access Control List BACL
: Einträge im Dateikatalog, die die Zugriffsrechte auf Dateien und Jobvariable für den Eigentümer, die Benutzergruppe und alle anderen Benutzerkennungen für Lesen, Schreiben und Ausführen regeln.

Filter
: Mechanismus zur Verfeinerung der Preselection von SAT

First-Start
: Beim First-Start werden Systemdateien neu eingerichtet. Vom System werden eine Reihe von Benutzerkennungen vergeben (z.B. TSOS, SYSPRIV, SYSDUMP, SERVICE, SYSGEN, SYSNAC, SYSHSMS, SYSUSER, SYSSNAP, SYSSPOOL, SYSAUDIT). Beim First-Start wird immer der Benutzerkennungskatalog angelegt.
Beim First-Start für einzelne Pubsets sind zwei Varianten möglich: Entweder Systemstart mit diesem Pubset oder IMCAT-Processing (logisches Hinzufügen eines weiteren Pubsets).

Frist
: siehe *Schutzfrist*

Funktionalitätsklasse
Functionality Class
: Klasse, die bestimmte Mindestanforderungen bezüglich der Funktionalität der Sicherheitsfunktionen an ein System der Informationstechnik stellt.
Die Funktionalitätsklassen sind definiert innerhalb der „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)“, 1. Fassung vom 11. Januar 1989, herausgegeben von der Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung.

Gemeinschaftlicher Datenspeicherbereich
Public Space
: Benannter Plattenspeicherbereich, der für eine definierte Anzahl von Benutzerkennungen des Betriebssystems verfügbar ist. Dieser Speicherbereich kann sich über einen oder mehrere Pubsets erstrecken.

Gruppenkennung
: siehe *Benutzergruppenkennung*

Gruppenmitglied
Group Member
Benutzerkennung, die einer Benutzergruppe zugeordnet ist. Der Gruppenverwalter kann einem Gruppenmitglied im Rahmen des Gruppenpotentials Betriebsmittel zuweisen.

Gruppenpotential
Enthält alle Betriebsmittel und Rechte, die an eine Benutzergruppe gebunden sind und an die Gruppenmitglieder der Benutzergruppe bzw. an hierarchisch untergeordnete Benutzergruppen vergeben werden können.

Gruppenverwalter
Group Administrator
Ein Benutzer, der Gruppenpotentiale, Gruppenmitglieder und die untergeordnete Gruppenstruktur verwalten kann. Die Benutzerkennung, unter der diese Tätigkeiten ausgeführt werden dürfen, ist im Gruppenpotential der jeweiligen Benutzergruppe hinterlegt.
Benutzerkennung, die mit dem Gruppenverwalterrecht ausgestattet ist.

Gruppenverwalterrecht
Group Administrator Privilege
Berechtigt eine Benutzerkennung zur Verwaltung von
– den Benutzerkennungen der eigenen Benutzergruppe und
– hierarchisch untergeordneten Benutzerkennungen sowie
– hierarchisch untergeordneten Benutzergruppen.
Das Gruppenverwalterrecht kann in drei Ausprägungen vergeben werden, die den Umfang der erlaubten Tätigkeiten festlegen, diese sind:
– Manage Resources
– Manage Members
– Manage Groups.

Guard
Schutzprofil, das mit dem Schutzmechanismus *GUARDS* erstellt und verwaltet werden kann.

GUARDS
Generally Usable Access Control Administration System
Universeller Schutzmechanismus für Objekte im BS2000.

Identifizierung
Identification
Verfahren zur Erkennung einer Person oder eines *Objekts*.

Installation

Vorgang des Bereitstellens von Gerätetechnik und Software
Bei einem Benutzer vorhandene Gerätetechnik und Software.

IT-Sicherheitskriterien

siehe *Sicherheitskriterien*

Katalogkennung

Catalog Identification CATID

Kennzeichnet einen Pubset durch maximal 4 Zeichen <cat-id 1...4>.

Kennwort

Password

Folge von Zeichen, die der Benutzer eingeben muss, um den Zugriff zu einer Benutzerkennung, einer Datei, einer Jobvariablen, einem Netzknoten oder einer Anwendung zu erhalten.
Das Benutzerkennungs-Kennwort dient zur Authentifizierung des Benutzers. Es dient dem Zugangsschutz. Das Datei-Kennwort dient zur Überprüfung der Zugriffsberechtigung beim Zugriff auf eine Datei (Jobvariable). Es dient dem Zugriffsschutz.
Synonym: Passwort

Kommandoprofil

Command Profile

siehe *Profile*

Miteigentümer

Co-owner

Benutzerkennung, die vom *Eigentümer* eines *Objekts* berechtigt wird, sein *Objekt* mitzuverwalten.

Miteigentümerschaft

Co-ownership

Berechtigung, fremde *Objekte* mitzuverwalten

Miteigentümerschutz

Co-owner Protection

Spezieller Zugriffsschutz für *Objekte*, die von fremden Benutzerkennungen mitverwaltet werden dürfen

Miteigentümerschutzregel

Co-Owner Protection Rule

Regel, die für ein oder mehrere *Objekte* bestimmt, welche Bedingungen eine Benutzerkennung erfüllen muss, um *Miteigentümer* dieser *Objekte* zu sein.

Objekt
Object

Passives Element eines DV-Systems, das Daten enthält oder aufnimmt und auf das eine Operation wie Lesen, Schreiben, Ausführen u.ä. angewendet werden kann.
Beispiele: Dateien, Jobvariablen, Benutzerkennungen, *Terminal-Sets*

offline-Betrieb

Arbeitsweise einer funktionellen Einheit, wenn sie nicht unter der direkten Steuerung eines Rechners steht.
Weder gesteuert noch verbunden mit einem Rechner (Gegensatz zu online-Betrieb).

online-Betrieb

Arbeitsweise einer funktionellen Einheit, wenn sie unter der direkten Steuerung eines Rechners steht.
Fähigkeit eines Benutzers zur interaktiven Arbeit mit einem Rechner.
Benutzerzugriff zu einem Rechner über eine Datensichtstation.
Gesteuert von oder verbunden mit einem Rechner (Gegensatz zu offline-Betrieb)

Operator-Role

Zusammenfassung einer Menge von Routing-Codes unter einem Namen.
Es sind beliebige Kombinationen der 40 Routing-Codes möglich.

Personenbezogene Beweissicherung
Personal Audit for Individual Accountibility

Nachvollziehbarkeit des Umgangs mit einem System.
Identifikation entweder in Form: eine Benutzerkennung entspricht einem Benutzer oder ein Benutzer darf ausschließlich eine Bedienstation benutzen.

persönliche Identifizierung

Für eine Benutzerkennung können andere Benutzerkennungen als zusätzlich zugangsberechtigt festgelegt werden. Während der Dialogzugangsprüfung wird eine personenspezifische Identifizierung/Authentisierung veranlasst. Die Benutzerkennung, die mit der personenbezogenen Identifizierung angegeben wurde, wird in die SAT-Einträge übernommen. Somit ist es möglich, Personen als Urheber einzelner Aktionen auch nachträglich zu ermitteln.

Privilegienverwalter

siehe *Sicherheitsbeauftragter*

Privileg
Privilege

Systemglobales Recht, das zur Ausführung bestimmter Kommandos und zum Aufruf bestimmter Programmschnittstellen berechtigt (z.B. SECURITY-ADMINISTRATION)

Profil
Profile

Ein einer Benutzerkennung zugeordneter Kommando-Vorrat, dessen Zulässigkeit über Syntax-Dateien sichergestellt wird.

Pubset
Pubset

Durch eine Katalogkennung (Catid) definierte Menge von gemeinschaftlichen Plattenspeicher-Einheiten.
Man unterscheidet Single-Feature-Pubsets (SF-Pubsets) und System-Managed-Pubset (SM-Pubset).
Ein SF-Pubset besteht aus einer oder mehreren Platten, die in den wesentlichen Eigenschaften (Plattenformat, Allokierungseinheit, Verfügbarkeit) übereinstimmen müssen.
Ein SM-Pubset kann im Gegensatz dazu aus mehreren so genannten Volume-Sets mit unterschiedlichen Eigenschaften bestehen. Nur innerhalb eines Volume-Sets müssen die wesentlichen Eigenschaften der Platten übereinstimmen.

Qualitätsstufe
Assurance Level

Hierarchische Unterteilung bezüglich der Qualität eines Systems der Informationstechnik (IT-Systems). Bei der Evaluation wird die Qualität eines IT-Systems bewertet. Anhand dieser Bewertung erfolgt eine Einstufung in eine der Qualitätsstufen Q0 bis Q7.

Regel
Rule

Eintrag in einem *Regelbehälter.*
Abhängig von ihrem Zweck unterscheidet man *Miteigentümerschutzregeln* und *Standardschutzregeln*.

Regelbehälter
Rule Container

Spezielles Guard zur Aufnahme von *Miteigentümerschutzregeln* oder den *Standardschutzregeln*.

Rolle
Role
Gruppierung von Attributen, die einem Subjekt zugeordnet werden können, z.B. Sicherheitsbeauftragter.

Sammelprivileg
Privilege-Set
Zusammenfassung systemglobaler Privilegien zu einer Gruppe, die mit einem selbstgewählten Namen bezeichnet wird.

SAT
Security Audit Trail
Protokollierung sicherheitsrelevanter Ereignisse

SATLOG-Datei
SATLOG file
SAT-Protokolldatei, in der SATCP sicherheitsrelevante Ereignisse aufzeichnet.

Schutzattribute
Security Attributes
Sicherheitsrelevante Eigenschaften eines Objekts, die Art und potenzielle Möglichkeit des Zugriffs auf dieses Objekt festlegen.
Für Dateien gibt es folgende Schutzattribute: ACCESS/USER-ACCESS, SERVICE-bit, AUDIT-Attribut (NONE/SUCCESS/FAILURE/ALL), RDPASS, WRPASS, EXPASS, RETPD, BACL und GUARD.

Schutzfrist
Retention Period
Zeitintervall, in dem ein Objekt (Datei) nicht verändert oder gelöscht werden kann.

SF-Pubset
Single-Feature-Pubset siehe *Pubset*

SHUTDOWN
Vorgang der geordneten Systembeendigung (einschließlich des Sicherns spezieller Systemdateien).

Sichere Hardware-Konfiguration
Installierte Gerätetechnik (einschließlich Datenfernübertragungstechnik und Netz), die keinen Sicherheitseinschränkungen unterliegt.

Sicheres BS2000

BS2000, das aktiv entsprechend der F2/Q3-Sicherheitsanforderungen konfiguriert wurde.
Synonyme Begriffe dazu sind: „F2/Q3-System“ oder „evaluiertes System“. Das Gegenteil eines „sicheren BS2000“ ist nicht ein „unsicheres BS2000“, sondern ein System, das beispielsweise nicht-bewertete Teile enthält oder das nicht den Kriterien F2/Q3 entspricht bzw. ein System, das nicht gemäß der empfohlenen Konfiguration betrieben wird.

Sicherheitsbeauftragter

Security Administrator, Security Officer

Sicherheitsbeauftragter im herkömmlichen Sinne: Organisatorisch-administrative Institution.
Die Kennung des Sicherheitsbeauftragten kann mit Hilfe des STARTUP-PARAMETER-SERVICE festgelegt werden. Bei Auslieferung ist die Kennung des Sicherheitsbeauftragten SYSPRIV. Der Sicherheitsbeauftragte hat das Recht, systemglobale Privilegien an Benutzerkennungen zu vergeben und zu entziehen. Er hat das Recht, die SAT-Protokollierung aus- und einzuschalten, Operator-Roles zu verwalten sowie Benutzerkennungen und Ereignisse für die Protokollierung auszuwählen.

Sicherheitskriterien

Security Criteria

Dienen der Bewertung der Sicherheit von Systemen der Informationstechnik. Sie bestehen aus Funktionalitätsklassen und Qualitätsstufen.
Dies wird in Form von Fx/Qy (Funktionalitätsklasse x und Qualitätsstufe y) dargestellt; Beispiel: F2/Q3 bedeutet Funktionalitätsklasse 2 und Qualitätsstufe 3.

Sicherheitsverwalter

siehe *Sicherheitsbeauftragter*

Single Sign On

Mechanismus, der es ermöglicht nach einmaliger Identifizierung/Authentisierung Zugang zu verschiedenen Rechnern und Anwendungen zu erhalten. Dieser Zugang wird über Zertifikate gesteuert.

Single-Feature-Pubset

siehe *Pubset*

SM-Pubset

System-Managed-Pubset siehe *Pubset*

SMS
System-Managed-Storage
Konzept für die Pubset-Verwaltung.

SRPM
System Resources and Privileges Management
Betriebsmittel und Privilegien werden im BS2000 gewöhnlich von der Kennung TSOS verwaltet. SRPM erlaubt, diese Aufgaben auch für andere Benutzerkennungen zuzulassen, die Aufgaben also zu verteilen.

Standardschutz
Default Protection
Schutzmechanismus, mit dem Standardwertvorgaben für Schutzattribute vorgenommen werden können.

Standardschutzregel
Default Protection Rule
Regel, die für ein oder mehrere *Objekte* bestimmt, welche Schutzattribute diese *Objekte* standardmäßig erhalten.

Subjekt
Subject
Aktives Element eines DV-Systems, von dem eine Operation wie Lesen, Schreiben, Ausführen u.ä. ausgehen kann, die einen Informationsfluss bewirkt oder den Systemzustand ändert, z.B. Kennung, Programm, Programmteil.

System-Managed-Pubset
siehe *Pubset*

Systemeinleitung
STARTUP
Laden der Betriebssystem-Software. Es wird unterschieden in:
– DIALOG-STARTUP
– FAST-STARTUP
– AUTOMATIC-STARTUP
Die Varianten der Systemeinleitung unterscheiden sich durch unterschiedlichen Automatisierungsgrad.

Systemglobale Benutzerverwaltung
User Administration

Sie umfasst die Verwaltung von Benutzerkennungen und Benutzergruppen bezüglich Betriebsmitteln und Benutzerrechten, das Neueinrichten, Modifizieren und Löschen von Benutzerkennungen und Benutzergruppen.

Systemglobale Privilegien

Alle mit dem Kommando /SET-PRIVILEGE vergebbaren Rechte sowie das Recht des Sicherheitsbeauftragten und das Recht der Kennung TSOS. Diese sind im Einzelnen im Abschnitt „Privilegien der Systemverwaltung“ aufgezählt. *Systemglobale Privilegien* und *Systemverwalterrechte* sind identisch.

Systemlauf
Session

Vorgänge/Aktivitäten zwischen Systemeinleitung und Systembeendigung.

Systemressourcen
System Resource

Ein Betriebsmittel eines Rechnersystems, das von einem Job oder einer Task angefordert bzw. freigegeben werden kann.

Systemverwalterrechte

siehe *Systemglobale Privilegien*

Systemverwaltung
System Administration

Struktureinheit im Rechenzentrum
Personenkreis, der Benutzerkennungen verwendet, an die systemglobale Rechte gebunden sind.

Terminal-Set

Terminal-Sets haben den Zweck, die Menge der Datensichtstationen, über die der Dialogzugang zu einer Benutzerkennung möglich ist, effektiv verwalten zu können. In einem Terminal-Set wird eine Liste von voll- oder teilqualifizierten Datensichtstationsnamen zusammengefasst.

Zugangsklasse
Access Class

Es werden in SECOS folgende Zugangsklassen unterschieden:

DIALOG-ACCESS	(Zugang vom Teilnehmersystem)
NET-DIALOG-ACCESS	(Dialog-Zugang aus dem Netz)
BATCH-ACCESS	(Zugang für Batchaufträge vom gleichen Rechner)
OPERATOR-ACCESS-TERM	(Operating-Betrieb)
OPERATOR-ACCESS-PROG	(Operating-Betrieb für programmierte Operatoren)
OPERATOR-ACCESS-CONS	(Konsol-Zugang)
POSIX-RLOGIN-ACCESS	(POSIX-Remote-Login)
POSIX-REMOTE-ACCESS	(POSIX-Remote-Kommando-Zugang)

Zugangsschutz

Beinhaltet alle Methoden zum Schutz eines DV-Systems vor unberechtigtem Systemzugang.

Zugriffsberechtigter
Authorized User

Subjekt, das auf ein Objekt zugreifen darf, z.B. Benutzerkennung auf Datei.

Zugriffsberechtigung
Access Admission

Legt fest, welches Subjekt auf welche Weise auf ein Objekt zugreifen darf.

Zugriffsrecht
Access Right

Recht eines Subjekts, auf ein Objekt mit einem vorgegebenen Zugriffsrecht zugreifen zu dürfen.

Zugriffsschutz

Zugriffsschutz bezeichnet die Regeln, nach denen in einem DV-System Subjekte auf Objekte zugreifen können und die Methoden, mit denen die Einhaltung dieser Regeln sichergestellt werden kann.

Zugriffstyp
Access Type

Allgemein: Legt fest, wie auf ein Objekt zugegriffen werden kann.
Die Zugriffstypen für Dateien sind Lesen, Schreiben und Ausführen.
Die Zugriffstypen für Jobvariablen sind Lesen und Schreiben.
Der Zugriffstyp für Memory Pools ist das Anschließen an den Memory Pool (ENAMP).
Der Zugriffstyp für die Serialization ist das Anschließen an die Serialisierungskennung (ENASI).
Der Zugriffstyp für die Ereignissteuerung ist das Anschließen an die ereignisgesteuerte Verarbeitung (ENAEI).
Synonym: Zugriffsart

Literatur

Die Handbücher finden Sie im Internet unter *http://manuals.ts.fujitsu.com*. Handbücher, die mit einer Bestellnummer angezeigt werden, können Sie auch in gedruckter Form bestellen.

[1] **SECOS**
Security Control System - Beweissicherung
Benutzerhandbuch

[2] **BS2000 OSD/BC**
Einführung in die Systembetreuung
Benutzerhandbuch

[3] **BS2000 OSD/BC**
Systeminstallation
Benutzerhandbuch

[4] **BS2000 OSD/BC**
Kommandos
Benutzerhandbuch

[5] **ARCHIVE** (BS2000)
Benutzerhandbuch

[6] **BS2000 OSD/BC**
Einführung in das DVS
Benutzerhandbuch

[7] **BS2000 OSD/BC**
DVS-Makros
Benutzerhandbuch

[8] **EDT** (BS2000)
Anweisungen
Benutzerhandbuch

[9] **FDDRL** (BS2000)
Benutzerhandbuch

[10] **openFT** (BS2000)
Konzepte und Funktionen
Benutzerhandbuch

[11] **openFT** (BS2000)
Installation und Betrieb
Systemverwalterhandbuch

[12] **openFT** (BS2000)
Kommandoschnittstelle
Benutzerhandbuch

[13] **HSMS** (BS2000)
Hierarchisches Speicher Management System
Band 1: Funktionen, Verwaltung und Installation
Benutzerhandbuch

[14] **HSMS** (BS2000)
Hierarchisches Speicher Management System
Band 2: Anweisungen
Benutzerhandbuch

[15] **BS2000 OSD/BC**
Dienstprogramme
Benutzerhandbuch

[16] **BS2000 OSD/BC**
Makroaufrufe an den Ablaufteil
Benutzerhandbuch

[17] **MAREN** (BS2000)
Bandverwaltung in BS2000
Benutzerhandbuch

[18] **openUTM** (BS2000, UNIX, Windows)
Anwendungen generieren
Benutzerhandbuch

[19] **BS2000 OSD/BC**
System Exits
User Guide

[20] **SDF** (BS2000)
Dialogschnittstelle SDF
Benutzerhandbuch

[21] **openSM2** (BS2000)
Software Monitor
Band 1: Verwaltung und Bedienung

[22] **VM2000**
Virtuelles Maschinensystem
Benutzerhandbuch

[23] **LMS** (BS2000)
SDF-Format
Benutzerhandbuch

[24] **SDF-P** (BS2000)
Programmieren in der Kommandosprache
Benutzerhandbuch

[25] **POSIX** (BS2000)
Grundlagen für Anwender und Systemverwalter
Benutzerhandbuch

[26] **POSIX** (BS2000)
Kommandos
Benutzerhandbuch

[27] **C-Bibliotheksfunktionen** (BS2000)
für POSIX-Anwendungen
Referenzhandbuch

[28] **SPOOL** (BS2000)
Teil 1, Benutzerhandbuch

[29] **SPOOL** (BS2000)
Teil 2, Dienstprogramme
Benutzerhandbuch

[30] **BS2000 OSD/BC**
Migration Guide
Benutzerhandbuch

[31] **PROP-XT** (BS2000)
Programmiertes Operating mit komfortablen Sprachmitteln von SDF-P
Produkthandbuch

[32] **JV** (BS2000)
Jobvariablen
Benutzerhandbuch

[33] **BS2000 OSD/BC**
System Managed Storage
Benutzerhandbuch

[34] **SESAM/SQL-Server** (BS2000)
Datenbankbetrieb
Benutzerhandbuch

Sonstige Literatur

Diese Literatur kann nicht über Fujitsu Technology Systems bezogen werden.

[35] **IT-Sicherheitskriterien:** Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)

Herausgegeben von der ZSI, Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung, 1. Fassung vom 11. Januar 1989. - Köln: Bundesanzeiger, 1989
ISBN 3-88784-192-1

Stichwörter

*UNIVERSAL
  Benutzergruppe 71
  Gruppenverwalter 71, 80
  Gruppenverwalterrecht 71

A

Abrechnung
  Account Number 951
  Nummer 951
absetzen
  Gruppenverwalter 72
  systemglobaler Benutzerverwalter 67
Access
  Admission 964
  Class 964
  Right 964
  Type 965
ACS-ADMINISTRATION, Privileg 49
ADD-ACCESS-CONDITIONS (GUARDS-Kommando) 519
ADD-COOWNER-PROTECTION-RULE (GUARDCOO-Kommando) 530
ADD-DEFAULT-PROTECTION-ATTR (GUARDDEF-Kommando) 535
ADD-DEFAULT-PROTECTION-RULE (GUARDDEF-Kommando) 548
ADD-DEFAULT-PROTECTION-UID (GUARDDEF-Kommando) 555
ADD-KEYTAB-ENTRY (SRPM-Kommando) 129, 163, 232, 270
ADD-USER-GROUP (SRPM-Kommando) 132
ADDATTR (GUARDDEF-Makro) 706
ADDCOO (GUARDCOO-Makro) 719
ADDDEF (GUARDDEF-Makro) 726
ADDUID (GUARDDEF-Makro) 734
Admission
  Access 964
Alarm
  Einführung 14
Ämterhäufung 951
ändern
  Gruppenpotential 74
anzeigen
  Benutzergruppeneintrag 324
  persönliche Benutzerkennung 295
  Schutzattribute 277
  systemglobale Privilegien 301
  Terminal-Set 314
ARCHIVE, Guardskatalog 558
Assurance Level 959
Audit 953
AUDIT-Modus
  Recht zum Einschalten vergeben 141
AUDIT-Steuerung 332
Aufbau, Benutzergruppenstruktur 75
Aufgaben
  Systembedienung 31
  Systemverwaltung 30, 31
Aufgabenbereich
  Teilnehmer 30
  Teilnehmerbetrieb 30
ausgeben
  Gruppeninformation 345
ausprobieren, Kennwort 92
Austausch Home-Pubset 74
Authentication 951
Authentisierung 35, 951
  Kennwortschutz 91
Authorized User 964

B
BACKUP-GUARDS (GUARDS-SAVE-Anweisung) 910
BACL 425, 955
Basic Access Control List 420
Wirkung 426
Zugriffsrecht 426
Bandverwaltung 59
MAREN 59
Privileg 59
Basic Access Control List (BACL) 955
Bedrohung
allgemeine 26
DV-System 28
begrenzen, Betriebsmittel 88, 91
Beispiele
Benutzergruppe 81
Benutzerverwaltung 366
GUARDS-Makros 845
Benutzer 952
Katalog 68
Teilnehmerbetrieb 30
Benutzeradressraum
Größe festlegen 142
Benutzerattribute 952
Benutzergruppe 68, 952
*UNIVERSAL 71
Beispiele 81
Benutzerkatalog löschen 234
Benutzerkennung hinzufügen 217
Daten hinterlegen 68
definieren 68
einrichten, Gruppenverwalter 383
einrichten, systemglobaler Benutzerverwalter 384
Gruppenbeschreibungsdaten 68
Gruppenpotential 68
Gruppenpotential vergrößern 389
Gruppenpotential verkleinern 394
Gruppenverwalter 80, 403
hinzufügen 217
in den Benutzerkatalog eintragen 132
löschen 413
löschen, Voraussetzungen 234
maximale Anzahl von Benutzerkennungen festlegen 136
maximale Anzahl von Untergruppen festlegen 137
überordnen 134
umhängen 215, 367, 368, 403
umhängen, Gruppenverwalter 367
verwalten 72
Benutzergruppeneintrag 952
anzeigen 324
Benutzerkatalog 324
SRPM 212
Benutzergruppenkennung 952
Benutzergruppenkonzept 68
Benutzergruppenstruktur
Aufbau 75
Einflussfaktoren 75
pubset-bezogen 75
Benutzerkatalog 61, 952
Benutzergruppe eintragen 132
Benutzergruppe löschen 234
Benutzergruppeneintrag 324
Benutzerkennung 952
hinzufügen 217
persönliche, anzeigen 295
Privilegien anzeigen 301
reaktivieren 172
Schutzattribute 277
Schutzattribute ändern 172
Schutzattribute vereinbaren 241
SYSAUDIT 56
SYSHSMS 52
TSOS 52, 60
umhängen 367, 368
umhängen, Gruppenverwalter 367
Zugangskontrolle 76
Benutzerkennungskatalog 952
Benutzerklasse
BACL 425
GROUP 425
OTHERS 425
OWNER 425
Benutzerkommando 953
Benutzerorganisation 953

Benutzerrechte 953
Benutzerverwalter, systemglobal 368, 403, 413
Benutzerverwaltung 79, 953
  Beispiele 366
  Berechtigung 66
  gruppenspezifisch 72
  Organisation 66
  pubset-bezogen 75
  Rechte 80
  Regeln 366
  systemglobale 66
Berechtigung zur Benutzerverwaltung 66
bestimmen, Gruppenverwalter 216
Betrieb
  offline 958
  online 958
Betriebsmittel 963
  begrenzen 88, 91
  systemglobal 91
  verwalten 39
Beweis sichern 35, 953
Beweissicherung 953
BS2000
  Aufgabenbereiche 30

C
Catalog Identification (CATID) 957
CHANGE-GUARD-FILE (GUARDS-Kommando) 558
CHKPRV, siehe Handbuch Makroaufrufe
CHKSAC (GUARDS-Makro) 738
Co-owner protection 471
Command Profile 957
CONSLOG-Datei 953, 960
COPGUAD (GUARDS-Makro) 744
COPY-GUARD (GUARDS-Kommando) 561
COPY-TERMINAL-SET (SRPM-Kommando) 151
CREATE-GUARD (GUARDS-Kommando) 563
CREATE-PRIVILEGE-SET (SRPM-Kommando) 154
CREATE-TERMINAL-SET (SRPM-Kommando) 156
CREGUAD (GUARDS-Makro) 746
CUSTOMER-PRIVILEGE 49

D
Data Protection 954
Data Security 954
Datei
  Katalog 953
  Lesezugriff 424
  SRPM 61
Datei-Verwalter, SAT 56
Daten
  hinterlegen, Benutzergruppe 68
Daten hinterlegen
  Benutzergruppe 68
Datenschutz 954
Datensicherung 954
Datensichtstation 954
Default protection 449
definieren
  Benutzergruppe 68
  Rollen 960
  Sammelprivileg 43
  Verrechnung 380
  Zugangskontrolle 189
DELETE-GUARD (GUARDS-Kommando) 565
DELETE-PRIVILEGE-SET (SRPM-Kommando) 159
DELETE-TERMINAL-SET (SRPM-Kommando) 161
DELGUAD (GUARDS-Makro) 748
Dialogbetrieb
  Zugangskontrolle 189, 253
  Zugangskontrolle definieren 253

E
einfache Zugriffskontrollliste 420, 425, 955
Einflussfaktoren
  Benutzergruppenstruktur 75
einrichten
  Benutzergruppe, Gruppenverwalter 383
  Benutzergruppe, systemglobaler Benutzerverwalter 384
Einschränkung
  MODIFY-USER-GROUP 212

Einträge lesen
Gruppen 325
Guard-Attribute 676
GUARDS-Auswertung 673
GUARDS-Sicherungsdatei 922
Privileg 301
Sammelprivileg 310
Einzelprivileg 46
Encryption-Key-Verwaltung 60
ermitteln
Gruppenzugehörigkeit 340
ernennen
Gruppenverwalter 72
systemglobaler Benutzerverwalter 67

F
Fachwörter 951
Fehler
PRO6002 512
PRO6006 513
File Directory (TSOSCAT) 953
File-Transfer-Verwaltung 49
Privileg 49
Filter 955
First-Start 955
FIRST-STARTUP
Privilegienverteilung 46, 62
Frist 955
FT-ADMINISTRATION, Privileg 49
FTAC-ADMINISTRATION, Privileg 50
FTAC-Verwaltung, Privileg 50
Function Accumulation 951
Functionality Class 955
Funktionalitätsklasse 955
F2 35
funktionelle Übersicht
GUARDS-Kommandos 517
GUARDS-Makros 704
GUARDS-SAVE-Anweisungen 909
SRPM-Kommandos 124
SRPM-Makros 339

G
gemeinschaftlicher Speicherplatz 955
GETUGR (SRPM-Makro) 340
Group Administrator 956
Group Administrator Privilege 956
Group Entry 952
Group Identification 952
Group Member 956
Gruppen 71
Einträge lesen 325
Mitglied 71
Präfix 68, 137, 218
Struktur 71
Gruppenbeschreibungsdaten
Benutzergruppe 68
Gruppengrenzwert
ADD-USER-GROUP 132
Gruppeninformation
ausgeben 345
SRMSUG 345
Gruppenkennung 955
Gruppenmitglied 956
zuordnen 135
Gruppenpotential 956
ändern 74
Benutzergruppe 68
mit Verrechnung 68
ohne Verrechnung 69
verrechnen 380
verwalten 380
Gruppenpotential vergrößern
Benutzergruppe 389
Gruppenverwalter 389
systemglobaler Benutzerverwalter 389
Gruppenpotential verkleinern
Benutzergruppe 394
gruppenspezifische Benutzerverwaltung 72
Gruppenstruktur
hinterlegen 68
nach FIRST-STARTUP 81
Untergruppe 71
Gruppenverwalter 72, 413, 956
*UNIVERSAL 71, 80
absetzen 72

Benutzergruppe 403
Benutzergruppe löschen 413
Benutzergruppe umhängen 367
Benutzergruppen 80
Benutzerkennung umhängen 367
bestimmen 135, 216
einrichten einer Benutzergruppe 383
ernennen 72
Gruppenpotential vergrößern 389
Gruppenpotential verkleinern 394
Rechte 217
Rechte festlegen 136
Tätigkeiten 74
Gruppenverwalterrecht 956
*UNIVERSAL 71
MANAGE-GROUPS 73
MANAGE-MEMBERS 73
MANAGE-RESOURCES 72
Regeln 379
verwalten 379
Gruppenzugehörigkeit ermitteln 340
GUARD-ADMINISTRATION, Privileg 50
GUARDCOO, Subsystem 510
GUARDDEF, Subsystem 432, 509
GUARDS
Abkürzung 427
Auswertungsteil 439
Bedingungen 519
Bedingungen definieren 439
Bedingungsverwaltung 439
benötigte Dateien 509
Bestandteile 432
Definitionsteil 439
einrichten 563
Fehlerbehandlung 511
GUARDS-SAVE 432, 881
Makros 704
Objektverwaltung 439
Server-Task 680
SSINFO-Datei 507
Subsystem 509
Verknüpfung zu Objekt 439, 440
Verwaltungsteil 439
Zugriffsbedingung 439
GUARDS-SAVE
BACKUP-GUARDS 910
Installation 937
RESTORE-GUARDS 915
SHOW-BACKUP-FILE 922
starten 908
Guardskatalog
ändern 503
ARCHIVE 680
Fehler 513
Name 513
Server-Task 680
wechseln 503

H

Hardware-Audit 332
Hardware-Konfiguration, sichere 960
HARDWARE-MAINTENANCE, Privileg 51
hinterlegen, Gruppenstruktur 68
hinzufügen, Benutzergruppe 217
HOME-Pubset
wechseln 74
Home-Pubset
Austausch 74
HSMS-ADMINISTRATION, Privileg 52
HSMS-Verwaltung 52
Privileg 52

I

Identifizierung 35, 956
Identifizierung, persönliche 105
angeben 267
Inbetriebnahme
GUARDS 509
GUARDS-SAVE 937
Information, schutzwürdige 28
Installation 957
GUARDS 509
GUARDS-SAVE 937
IT-Sicherheitskriterien 957

J

Joinfile 952

K
Katalog, Benutzer 68
Katalogkennung (CATID) 957
Kennung wechseln, Sicherheitsbeauftragter 42
Kennung, Präfix 68
Kennwort 957
  ausprobieren 92
  Komplexität 92
  langes 267
  Lebensdauer 92
  minimale Länge 91
  vereinbaren 172
Kennwortschutz (Authentisierung) 91
Key-Tabelle
  Eintrag ändern 163
  Eintrag anzeigen 270
  Eintrag hinzufügen 129
  Eintrag löschen 232
Kommandoprofil 957
Komplexität, Kennwort 92
konvertieren, langes Kennwort 94
Konzept,Benutzergruppen 68
Korrektheit, Informationen 28

L
langes Kennwort 267
  eingeben 94, 267
  konvertieren 94
Lebensdauer, Kennwort 92
Linkage-Audit 332
LOGON
  Validierung 76
löschen
  Benutzergruppe 413
  Benutzergruppe, Voraussetzungen 234

M
Makros
  SRPM 339
MANAGE-GROUPS
  Gruppenverwalterrecht 73
MANAGE-MEMBERS
  Gruppenverwalterrecht 73
MANAGE-RESOURCES
  Gruppenverwalterrecht 72
MAREN
  Bandverwaltung 59
  Privileg 41
mehrstufige Gruppenstruktur 87
minimale Länge, Kennwort 91
Miteigentümerschutz 471
Mitglied 71
MODATTR (GUARDDEF-Makro) 750
MODCOO (GUARDCOO-Makro) 764
MODDEF (GUARDDEF-Makro) 771
MODGUAD (GUARDS-Makro) 779
MODIFY-ACCESS-CONDITIONS (GUARDS-Kommando) 568
MODIFY-COOWNER-PROTECTION-RULE (GUARDCOO-Kommando) 578
MODIFY-DEFAULT-PROTECTION-ATTR (GUARDDEF-Kommando) 584
MODIFY-DEFAULT-PROTECTION-RULE (GUARDDEF-Kommando) 597
MODIFY-GUARD-ATTRIBUTES (GUARDS-Kommando) 603
MODIFY-KEYTAB-ENTRY (SRPM-Kommando) 163
MODIFY-LOGON-PROTECTION (SRPM-Kommando) 170, 172
MODIFY-PRIVILEGE-SET (SRPM-Kommando) 207
MODIFY-TERMINAL-SET (SRPM-Kommando) 209
MODIFY-USER-GROUP
  Einschränkungen 212
MODIFY-USER-GROUP (SRPM-Kommando) 212
MODSAC (GUARDS-Makro) 781
MSCF 504
MSGGUAD (GUARDS-Makro) 791

N
Net-Storage
  Berechtigung zur Nutzung 144, 226
Netzverwaltung 52
  Privileg 52

Notification-Service-Administration
Privileg 53
Nutzung der Plattenkapazität
pubset-bezogen 76

O
Objekt 958
offline-Betrieb 958
online-Betrieb 958
openCRYPT-Session
maximale Anzahl 331
OPERATING, Privileg 53
Operator-Role 958
Operator-Roles
SECURITY-ADMINISTRATION 46, 48
Organisation der Benutzerverwaltung 66

P
Password 957
Personal Audit for Individual Accountibility 958
personenbezogene Beweissicherung 958
Persönliche Identifizierung 105
angeben 267
POSIX-ADMINISTRATION, Privileg 54
Potential
ADD-USER-GROUP 132
Präfix
Gruppen 68, 218
Kennung 68
PRINT-SERVICE-ADMINISTRATION,
Privileg 54
Privileg 959
ACS-ADMINISTRATION 49
Bandverwaltung 59
CUSTOMER-PRIVILEGE 49
Einträge lesen 301
Einzelprivileg 46
File-Transfer-Verwaltung 49
FT-ADMINISTRATION 49
FTAC-ADMINISTRATION 50
FTAC-Verwaltung 50
GUARD-ADMINISTRATION 50
HARDWARE-MAINTENANCE 51
HSMS-ADMINISTRATION 52
HSMS-Verwaltung 52
MAREN 41
Netzverwaltung 52
Notification-Service-Administration 53
OPERATING 53
POSIX-ADMINISTRATION 54
PRINT-SERVICE-ADMINISTRATION 54
PROP-ADMINISTRATION 55
RESET-PRIVILEGE 236
Sammelprivileg 41, 43, 44, 46
SAT-Datei-Verwaltung 56
SAT-FILE-EVALUATION 55
SAT-FILE-MANAGEMENT 56
SECURITY-ADMINISTRATION 46
SECURITY-ADMINISTRATION,
Sicherheitsbeauftragter 40
SECURITY-ADMINISTRATION,
Sicherheitsverwaltung 40
SET-PRIVILEGE 268, 951
SHOW-PRIVILEGE 301
SHOW-PRIVILEGE-SET 310
Sicherheitsbeauftragter 46, 48
STD-PROCESSING 57
SUBSYSTEM-MANAGEMENT 58
SW-MONITOR-ADMINISTRATION 59
systemglobale Benutzerverwaltung 61
Systemverwaltung 40
TAPE-ADMINISTRATION 59
TAPE-KEY-ADMINISTRATION 60
TSOS 46
USER-ADMINISTRATION 60
VIRTUAL-MACHINE-ADMINISTRATION 62
Privilegien
systemglobale Benutzerverwaltung 66
verwalten 39
Privilegien anzeigen
Benutzerkennung 301
Privilegienverteilung
FIRST-STARTUP 46, 62
nach Nicht-First-Start 64
Privilegienverwalter 958
Privilegienverwaltung 47
Sammelprivileg 47
Profil 959

PROP-ADMINISTRATION, Privileg 55
protokollieren
SAT 48
SECURITY-ADMINISTRATION 48
Sicherheitsbeauftragter 48
Umschalten 48
Public Space 955
Pubset 959
Gruppeneintrag erstellen 134
Zugriff, begrenzter 419

Q
Qualitätsstufe 959
Qualitätsstufe Q3 35

R
RDUID, siehe Handbuch Makroaufrufe
Readme-Datei 21
Rechte
Benutzerverwaltung 80
des Gruppenverwalters festlegen 136
Gruppenverwalter 217
Prüfung 33, 35
systemglobale 963
systemglobaler Benutzerverwalter 80
Verwaltung 33, 35
Regeln
Benutzerverwaltung 366
Gruppenverwalterrecht 379
REMCOO (GUARDCOO-Makro) 792
REMDEF (GUARDDEF-Makro) 796
REMOVE-ACCESS-CONDITIONS (GUARDS-Kommando) 606
REMOVE-COOWNER-PROTECTION-RULE (GUARDCOO-Kommando) 609
REMOVE-DEFAULT-PROTECTION-RULE (GUARDDEF-Kommando) 612
REMOVE-DEFAULT-PROTECTION-UID (GUARDDEF-Kommando) 615
REMOVE-KEYTAB-ENTRY (SRPM-Kommando) 232
REMOVE-USER-GROUP
SRPM 234
REMOVE-USER-GROUP (SRPM-Kommando) 234
REMSAC (GUARDS-Makro) 800
REMUID (GUARDDEF-Makro) 804
REPAIR-GUARD-FILE (GUARDS-Kommando) 619
RESET-PRIVILEGE (SRPM-Kommando) 236
RESTORE-GUARDS (GUARDS-SAVE-Anweisung) 915
Retention Period 960
RFA 505
Right, Access 964
Rollen
Datei-Eigentümer 436
definieren 960
Guard-Eigentümer 436
GUARDS 436

S
SACMGMT (GUARDS-Makro) 808
Sammelprivileg
CREATE-PRIVILEGE-SET 154
definieren 43
DELETE-PRIVILEGE-SET 159
Einträge lesen 310
MODIFY-PRIVILEGE-SET 207
Privileg 41, 43, 44, 46
Privilegienverwaltung 47
SAT-Privileg 55
SRPM 43
SAT
Datei-Verwalter 56
protokollieren 48
SAT-Datei-Verwaltung
Privileg 56
SAT-Dateien, Verwaltung 56
SAT-FILE-EVALUATION, Privileg 55
SAT-FILE-MANAGEMENT, Privileg 56
SAT-Privileg
Sammelprivileg 55
Schreibzugriff, Datei 424
Schutzattribut
Access 424
USER-ACCESS 424

Schutzattribute 960
anzeigen 277
Benutzerkennung 277
für existierende Benutzerkennungen vereinbaren 241
Standardwerte vereinbaren 170, 239, 273
Schutzattribute vereinbaren, Benutzerkennung 241
Schutzfrist 960
Schutzmechanismus
Basic Access Control List (BACL) 425
begrenzter Pubset-Zugriff 419
einfache Zugriffskontrollliste 425
Frist 420
Kennwort 420
Standard-Zugriffskontrolle 420
SCOPE-Attribut (GUARDS) 563, 604
Security Administrator 961
Security Attributes 960
Security Criteria 961
SECURITY-ADMINISTRATION
OPERATOR-ROLES 48
Operator-Roles 46
Privileg 46
protokollieren 48
Sicherheitsbeauftragter 46
Server-Task
Beendigung 513
GUARDS 513
SERVICE (Benutzerkennung) 63
Session 963
SET-LOGON-PROTECTION (SRPM-Kommando) 241
SET-PERSONAL-ATTRIBUTES (SRPM-Kommando) 267
SET-PRIVILEGE (SRPM-Kommando) 268
SF-Pubset 506
siehe Pubset 959
SHOW-ACCESS-ADMISSION (GUARDS-Kommando) 622
SHOW-ACCESS-CONDITIONS (GUARDS-Kommando) 632
SHOW-BACKUP-FILE (GUARDS-SAVE-Anweisung) 922
SHOW-COOWNER-ADMISSION-RULE (GUARDCOO-Kommando) 650
SHOW-COOWNER-PROTECTION-RULE (GUARDCOO-Kommando) 654
SHOW-DEFAULT-PROTECTION-ATTR (GUARDDEF-Kommando) 659
SHOW-DEFAULT-PROTECTION-RULE (GUARDDEF-Kommando) 664
SHOW-DEFAULT-PROTECTION-UID (GUARDDEF-Kommando) 669
SHOW-EVALUATED-CONDITIONS (GUARDS-Kommando) 673
SHOW-GUARD-ATTRIBUTES (GUARDS-Kommando) 676
SHOW-GUARD-MANAGEMENT-STATUS (GUARDS-Kommando) 680
SHOW-KEYTAB-ENTRY (SRPM-Kommando) 270
SHOW-LOGON-PROTECTION (SRPM-Kommando) 277
SHOW-OBJECT-PROTECTION-DEFAULT (GUARDDEF-Kommando) 683
SHOW-PERSONAL-LOGON-ADMISSION (SRPM-Kommando) 295
SHOW-PRIVILEG
Privileg 301
SHOW-PRIVILEGE (SRPM-Kommando) 301
SHOW-PRIVILEGE-SET (SRPM-Kommando) 310
SHOW-TERMINAL-SET (SRPM-Kommando) 314
SHOW-USER-GROUP (SRPM-Kommando) 324
SHUTDOWN 960
SHWACOO (GUARDCOO-Makro) 809
SHWATTR (GUARDDEF-Makro) 813
SHWCOO (GUARDCOO-Makro) 816
SHWDEF (GUARDDEF-Makro) 819
SHWGUAD (GUARDS-Makro) 822
SHWOBJ (GUARDDEF-Makro) 825
SHWSAC (GUARDS-Makro) 828
SHWUID (GUARDDEF-Makro) 843
Sichere Hardware-Konfiguration 960
Sicheres BS2000 961

Sicherheit
DV-Systeme 25
Fehlverhalten 25
Kriterien 35
Organisation 26
Sicherheitsbeauftragter 66
Sicherheitsbeauftragter 961
bei STARTUP 41
Kennung bei Auslieferung 41
Kennung wechseln 42
Privileg 46, 48
protokollieren 48
SECURITY-ADMINISTRATION 46
Sicherheit 66
STARTUP 41
STARTUP-PARAMETER-SERVICE 42
SYSPRIV 41
Sicherheitskonzeption, BS2000 29
Sicherheitskriterien 961
Bedeutung 36
F2/Q3 35, 36
Sicherheitsmaßnahmen, technische 29
Sicherheitsverwalter 961
Sicherheitsverwaltung, Privileg SECURITY-ADMINISTRATION 40
Single Sign On 109
Single-Feature-Pubset 506
siehe Pubset 959
SM-Pubset 506
siehe Pubset 959
SMS 506, 962
Speicherplatz, gemeinschaftlicher 955
SPVS 504
SRMSUG (SRPM-Makro) 345
Gruppeninformation 345
SRMUINF, siehe Handbuch Makroaufrufe
SRPM 962
ADD-KEYTAB-ENTRY 129, 163, 232, 270
Benutzergruppeneintrag 212
Benutzergruppenkennung eintragen 134
Datei 61, 134
funktionelle Übersicht 124
GETUGR 340
Makros 339
MODIFY-KEYTAB-ENTRY 163
MODIFY-LOGON-PROTECTION 172
MODIFY-USER-GROUP 212
REMOVE-KEYTAB-ENTRY 232
REMOVE-USER-GROUP 234
RESET-PRIVILEGE 236
Sammelprivilegien 43
SET-LOGON-PROTECTION 241
SET-PRIVILEGE 268
SHOW-KEYTAB-ENTRY 270
SHOW-LOGON-PROTECTION 277
SHOW-PRIVILEGE 301
SHOW-USER-GROUP 324
SRPM-Makro
GETUGR 340
SRMSUG 345
SSINFO
Datei 507, 511
Eigenschaften 507
Name bei GUARDS 511
SSINFO-Datei
Aufbau 507
Dateieigenschaften 507
fehlerhafte Steuerparameter 508
Kommandos 507
Verarbeitungseigenschaften 507
Standard, Zugriffskontrolle 424
Standardschutz 449
Stapelbetrieb, Zugangskontrolle 193, 257
STARTUP 962
Sicherheitsbeauftragter 41
STARTUP-PARAMETER-SERVICE
Sicherheitsbeauftragter 42
STD-PROCESSING, Privileg 57
Struktur, Gruppen 71
Subjekt 962
ALL-USERS 522, 570, 607
Benutzer 522, 607, 633
Gruppen 522, 571, 607
OTHERS 521, 570, 606
Subsystem
GUARDCOO 510
GUARDDEF 509
GUARDS 509

SUBSYSTEM-MANAGEMENT, Privileg 58
SW-MONITOR-ADMINISTRATION, Privileg 59
SYSAUDIT (Benutzerkennung) 56, 63
SYSDB (Benutzerkennung) 63
SYSDUMP (Benutzerkennung) 63
SYSFJAM (Benutzerkennung) 63
SYSGEN (Benutzerkennung) 63
SYSHSMS (Benutzerkennung) 52, 63
SYSMAREN (Benutzerkennung) 63
SYSNAC (Benutzerkennung) 63
SYSOPR (Benutzerkennung) 63
SYSPRIV
  Sicherheitsbeauftragter 41
SYSPRIV (Benutzerkennung) 63
SYSROOT (Benutzerkennung) 63
SYSSAG (Benutzerkennung) 63
SYSSNAP (Benutzerkennung) 63
SYSSPOOL (Benutzerkennung) 63
System Administration 963
System Resource 963
System-Managed-Pubset 506
  siehe Pubset 959
Systemeinleitung 962
systemglobal
  Benutzerverwalter 368, 403, 413
  Betriebsmittel 91
  Rechte 963
  umhängen 368
systemglobale Benutzerverwaltung 60, 66, 963
  Privileg 61
  Privilegien 66
systemglobale Privilegien
  anzeigen 301
  vergeben 268
systemglobale Privilegien entziehen
  Benutzerkennung 236
systemglobaler Benutzerverwalter
  absetzen 67
  einrichten einer Benutzergruppe 384
  ernennen 67
  ernennen/absetzen 67
  Gruppenpotential vergrößern 389
  Gruppenpotential verkleinern 395
  Rechte 80
Systemlauf 963
Systemressourcen 963
Systemverwalterrechte 963
Systemverwaltung 963
  Privileg 40
SYSUSER (Benutzerkennung) 63
SYSWSA (Benutzerkennung) 63

T

Tabelle der Privilegien 525, 574
TAPE-ADMINISTRATION, Privileg 59
TAPE-KEY-ADMINISTRATION, Privileg 60
Tätigkeiten
  Gruppenverwalter 74
Terminal 954
Terminal-Set 963
  anlegen 156
  anzeigen 314
  Kennung schützen 190, 254
  löschen 161
  modifizieren 209
Terminal-Sets 96
trennen, Zugangswege 95
TSOS
  Benutzerkennung 52, 60
  Privileg 46
TSOS (Benutzerkennung)
  Privilegienverteilung bei First Start 63
TSOS-Mitverwaltungsrecht, Einschränkung 487
  festlegen 489
  Wirksamkeit 488, 939
Typ, Zugriff 965
Type, Access 965

U

umhängen
  Benutzergruppe 215, 367, 368, 403
  Benutzerkennung 367, 368
  systemglobal 368
Umschalten, protokollieren 48
Untergruppe 71
  Gruppenstruktur 71
  maximale Anzahl festlegen 137
Unversehrtheit, Information 28

User Administration 953, 963
User Attribute 952
User Command 953
User Group 952
User Identification (USER-ID) 952
User Privilege 953
USER-ADMINISTRATION, Privileg 60

V
Validierung, LOGON 76
vereinbaren
  Bedingungen 519
  Kennwort 172
  Zugriffsbedingungen 519
vergeben
  systemglobale Privilegien 268
vergrößern des Gruppenpotentials
  Benutzergruppe 389
verkleinern des Gruppenpotentials
  Benutzergruppe 394
Verknüpfung, logisch oder 439
Verlust
  Integrität 28
  Verfügbarkeit 28
  Vertraulichkeit 28
verrechnen, Gruppenpotential 380
verwalten
  Benutzergruppe 72
  Betriebsmittel 39
  Gruppenpotential 380
  Gruppenverwalterrecht 379
  Privilegien 39
  SAT-Dateien 56
VIRTUAL-MACHINE-ADMINISTRATION
  Privileg 62
Vollständigkeit, Information 28
Voraussetzungen, Benutzergruppe löschen 234

W
wechseln
  Guardskatalog 558
  HOME-Pubset 74
Wiederaufbereitung 35
  Objekte 33

Z
Zugang
  Klasse 32, 964
Zugangskontrolle
  Benutzerkennung 76
  definieren 189, 193
  definieren, Dialogbetrieb 253
  Dialogbetrieb 189, 253
  Stapelbetrieb 193
Zugangsschutz 964
  Authentisierung 32
  Identifizierung 32
  mit Guards 104
  mit Terminal-Sets 96
Zugangswege trennen 95
Zugriff
  Typ 965
Zugriffsbedingung, Inhalt 439
Zugriffsberechtigter 964
Zugriffsberechtigung (Access Admission) 964
Zugriffskontrolle, Objekt 33
Zugriffskontrollliste
  einfache, Basic Access Control List (BACL) 420, 425, 955
Zugriffsrecht 964
  Ausführen 426
  BACL 426
  Lesen 426
  Schreiben 426
  Vergabe 426
Zugriffsrechte festlegen, Benutzerkennungen 76
Zugriffsschutz 964
  Rechteprüfung 33
  Rechteverwaltung 33
Zustand
  anzeigen 504, 680
  GUARDS 504, 680
  SHOW-GUARD-MANAGEMENT-STATUS 504