MIDRANGE
HANDBUCH

9 Kapitel

Sicherheit für Power i

Herausgeber: Rainer Huttenloher

IBM POWER Systems i Systemmanagement

Betriebssystem, Administration und Systemsteuerung, Datenhaltung, Datenbank und Integration, Client Connectivity, Netzwerk und Serverdienste

ITP VERLAG

Kapitel 9
Sicherheit für Power i

30. Ergänzung 3/2012

9.1 Sicherheit für Power i

„Die AS/400“ – sorry, jetzt heißt sie IBM Power i – ist das sicherste System der Welt?! Immer wieder wird dem Anwender diese Aussage unter die Nase gerieben. Fragen dazu – wie „Ist dem tatsächlich so?“, „Gehört das eventuell in die Vergangenheit?“ oder „Wie hat sich die Sicherheit im Laufe der Zeit verändert?“ – gilt es zu beantworten. Solche Antworten, in denen es um die Sicherheit der IBM Power i-Systeme geht, finden Sie in den folgenden Kapiteln.

Dieses Fachbuch bietet einen sehr komplexen Informationsbereich zu diesem Thema an. Niemand, der sich mit Security beschäftigt, kann von sich behaupten, darin perfekt zu sein. D.h. – eine perfekte Security gibt es nicht. Falls doch, dann ist der Umgang mit den Systemen so kompliziert geworden, dass man kaum noch damit arbeiten kann. Darum sollte man Kompromisse schließen – und zwar unter Einbeziehung eines praktischen Ansatzes und Einbeziehung einer ausreichenden, bestmöglichen und optimalen Sicherheit, so dass man letztendlich damit auch arbeiten kann.

Aber wo fängt man beim Thema Security an? Am Besten von vorn! Sorry, aber hier werden wir Informationen für Laien und fortgeschrittene Anwender gleichermaßen anbieten. Daher bitte ich den Spezialisten für Power i Systeme ein wenig um Geduld, da wir zuerst einmal mit den Basisinformationen beginnen werden, die allerdings für den Anfänger sehr wichtig sind. Die Fortgeschrittenen können an dieser Stelle diese wenigen Kapitel einfach überspringen.

9.1
Seite 2

9.2 Grundlegende Konzepte

Die Power i mit dem Betriebssystem IBM i wurde schon bei der Grundsteinlegung 1988 mit einem starken Fokus auf Sicherheit entwickelt. Ging es doch bei diesem System schon immer – auch als es noch AS/400 hieß – um unternehmenskritische Transaktionen. Millionen von Anwendern, die mit Milliarden von Transaktionen agieren, benötigen eben eine gewisse Stabilität und Sicherheit. Daher wurde auch der Ruf laut, dass die Power i Server zu den sichersten Systemen gehören, die man kaufen kann.

Damit wurde von Anfang an die Sicherheit als fester Bestandteil des Systems mit eingeplant und integriert. Sicherheit war somit keine nachträgliche Idee, die oberhalb des Betriebssystems angesiedelt wurde, wie es bei vielen anderen Rechnersystemen der Fall ist. Das objektorientierte Design machte einen IBM i Server resistent gegenüber Angriffen – wie z. B. denen von Viren.

Allein durch die Installation des Betriebssystems wird ein Basisschutz mitinstalliert. Viele einfach zu handhabende Sicherheitsmechanismen und Dienste erleichtern es Administratoren, den gewünschten Schutz ihres Systems zu erreichen.

Objekte
Die Power i ist ein objektorientiertes System. Wikipedia sagt dazu:

„Das IBM i System ist nach dem Prinzip der Objektbasiertheit aufgebaut, wodurch grundsätzlich alles im Betriebssystem, egal ob Benutzerprofil oder Programm, als Objekt mit Eigenschaften und Funktionen angesehen wird; dieses Prinzip ist jedoch nicht zu verwechseln mit Objektorientierung, wie sie bei Programmiersprachen zu verstehen ist. Gemäß Konvention beginnen alle Systemobjekte mit dem Buchstaben Q (z. B. QSYS oder QSECOFR).

Diese konsequente Objektbasiertheit bewirkt, dass Objekte (Programme, Dateien, Spools, Subsysteme etc.) ausschließlich über einen Satz von abschließend definierten Funktionen angesprochen werden können. Damit ist es beispielsweise nicht möglich, den Binärcode eines Programms frei zu verändern, da diese Art von Schnittstelle zwar für Objekte des Typs Datei (*FILE), aber nicht für Objekte des Typs Programm (*PGM) zur Verfügung steht. Dies unterscheidet OS/400 bzw. i5/OS – wie es neu heißt – grundlegend von den meisten anderen Betriebssystemen, wo vom Dateisystem lediglich Dateien verwaltet werden, deren Verwendungszweck jeweils nur durch eine Dateiendung und eventuell eine User-Zuordnung festgelegt wird.

9.2
Seite 2

Objekte werden in Bibliotheken verwaltet. Diese Bibliotheken können dabei keine Unterbibliotheken enthalten, sondern nur Objekte. Eine Ausnahme ist die Bibliothek QSYS, die sämtliche Bibliotheken enthält. Dateien selbst können in Members unterteilt werden, die man Teildateien nennt. In den Teildateien vom Dateityp PF-SRC können z. B. Quellcodes abgelegt werden, in PF-DTA werden Members als indizierbare Datentabellen abgelegt. In OS/400 hat jedes Member eine logische Satzlänge (LRECL). OS/400 kennt ursprünglich keine strukturfreien Dateien wie Unix. Dies wurde erst mit der Einführung des integrierten Dateisystems (IFS) möglich."

9.3 Was bietet das Power i System an Sicherheit

Es gibt drei Sicherheitsebenen:

– Systemebene

– Benutzerebene

– Objektebene

Die Sicherheit auf der Systemebene wird im Systemwert QSECURITY eingestellt. Dabei existieren fünf Sicherheitsstufen, die von keiner Sicherheit bis zur so genannten C2-Sicherheit – eine von der US-Regierung zertifizierte Sicherheitsstufe – reichen. Die Benutzerebene ist notwendig für das Anmelden an das System, wobei hier bereits diverse Berechtigungen festgelegt sind. Auf der Objektebene können Berechtigungen explizit für jedes Objekt vergeben werden. Zum Systemwert QSECURITY kommen wir nach Erläuterung der Grundlagen.

Des Weiteren sind Systemobjekte durch das Domain-Attribut des Objektes vor Manipulation geschützt. Ab einem bestimmten Wert in QSECURITY kann trotz Objektberechtigung nicht von einem Programmcode, der in der Domäne Benutzer läuft, auf ein Objekt der Domäne System zugegriffen werden. Bei dieser Sicherheitsverschärfung ist zu beachten, dass manche Software von Drittanbietern auf solche Zugriffe angewiesen ist.

Im Nachfolgenden sind einige Erläuterungen sowie Komponenten der verschiedenen Ebenen aufgeführt, die in späteren Kapiteln näher beleuchtet werden.

9.3
Seite 2

9.3.1 Sicherheit auf Systemebene

Auf Systemebene gibt es verschiedene Objekte, die verschiedene Ziele verfolgen:

Sicherheits-Funktionen	Vertraulichkeit	Integrität	Authentifizierung	Authorisierung	Protokollieren/ Auditieren
Benutzerprofil			X	X	X
Objektberechtigung				X	X
Objektsignierung		X			X
Systemwerte		X	X	X	X
Netzwerk-Attribute				X	
Digitale Zertifikate		X	X	X	
Security Auditjournal					X
Exit-Programme			X	X	X
Kerberos			X		X
DB2 Datenverschlüsselung	X				
Anwendungsverwaltung					
Viren-Scanner		X			

Benutzerprofile
Benutzerprofile beinhalten sicherheitsrelevante Informationen, die steuern, wie ein Anwender sich am System anmeldet, was er darf oder wie die Aktivitäten des Anwenders protokolliert (auditiert) werden.

Objektberechtigungen
Objektberechtigungen beinhalten Informationen darüber, wer diese wie verwenden darf. Die Objektberechtigung erteilt einem Anwender das Recht auf ein Objekt – z.B., dass ein Anwender ein Objekt benutzen, ein anderer das Objekt ändern und ein dritter überhaupt nicht auf das Objekt zugreifen darf.

Objektsignierung
Um ein Objekt vor Manipulation zu schützen, kann es signiert werden, um die Integrität zu gewährleisten. Digitale Zertifikate werden verwendet, um Objekte zu signieren. Außerdem enthalten sie einen öffentlichen Schlüssel (Public Key), um die Signatur zu prüfen.

9.3.1
Seite 2

Systemwerte
Systemwerte sind Teil der globalen Sicherheitseinstellung des Power i Systems. Die Systemwerte werden verwendet, um verschiedene Einstellungen des Systems anzupassen. Dazu gehören u.a. Systemwerte, um zu steuern, welche Informationen protokolliert (auditiert) werden müssen. Andere Systemwerte sind in der Lage zu entscheiden, nach welchen Kriterien ein Benutzer sein Kennwort vergeben kann. Systemwerte können mit dem Befehl WRKSYSVAL angezeigt und geändert werden.

Netzwerkattribute
Wie sich ein Power i System in ein Netzwerk integriert, wird zum Teil über die Netzwerkattribute gesteuert. Viele der Netzwerkattribute stammen noch aus der SNA- (System Network Architektur-) Zeit. Einige beinhalten TCP/IP-relevante Parameter (iSeries Access-Anforderungen – PCSACC – oder DDM/DRDA-Anforderungen – DDMACC). Mit den Befehlen DSPNETA bzw. CHGNETA können diese Einstellungen angezeigt bzw. geändert werden.

Digitale Zertifikate
Ein digitales Zertifikat ist wie ein Identifikationspapier, das verwendet wird, um die Identität bei elektronischen Transaktionen sicherzustellen. Immer mehr Anwendungen benutzen digitale Zertifikate für diesen Zweck. Auch das Power i System verwendet sie in den verschiedensten sicherheitsrelevanten Anwendungen.

Auditjournal
Ein sehr umfassendes Werkzeug zur Erhaltung der Transparenz in Power i Systemen ist das Auditjournal. Es wird verwendet, um alle Arten von Transaktionen im System aufzuzeichnen und zu protokollieren. Hauptsächlich wird das Auditjournal aus Sicherheitsgründen geführt, um jederzeit nachvollziehen zu können, wer im System welche Aktivitäten ausgeführt hat. Das Auditjournal auszulesen, ist nicht immer einfach, da jede Art von System-Aktivität ihren speziellen Aufbau im Auditjournal hat und somit entsprechend interpretiert werden muss. Der Befehl DSPJRN kann verwendet werden, um Daten aus dem Auditjournal (QAUDJRN) herauszulesen.

Exit-Programme
Exit-Programme sind Schnittstellen aus Anwendungen. Sie sind notwendig, damit diese Anwendungen miteinander oder mit Systemprozessen kommunizieren können. Mit Exit-Programmen können erweiterte Berechtigungsprüfungen in TCP/IP-Anwendungen durchgeführt werden, um Benutzer für bestimmte Objekte in TCP/IP-Anwendungen zu berechtigen oder kundenspezifische Protokollierungen durchzuführen.

Kerberos
Kerberos ist ein Sicherheitsmechanismus, der verwendet wird, um die Anwender in den Unternehmen systemübergreifend zu authentifizieren. Microsoft Windows verwendet beispielsweise Kerberos, um Benutzer in einer Windows-Domäne zu authentifizieren. Kerberos-Tickets werden verwendet, um Berechtigungen in einer Kerberos-Umgebung weiterzugeben. Damit entfällt die Notwendigkeit, dass Anwender, die auf verschiedene Systeme und Anwendungen zugreifen, sich immer wieder neu anmelden müssen. Systeme und Anwendungen sollten Kerberos unterstützen. Im IBM i System wird Enterprise Identity Mapping (EIM) verwendet, damit eine Verbindung zwischen Windows- und IBM i-Benutzern hergestellt wird.

DB2-Datenbankverschlüsselung
Eine Datenbankverschlüsselung wird benutzt, damit die Inhalte von Datenbanken verschlüsselt werden und damit sie einen noch höheren Schutz vor unberechtigtem Zugriff erhalten. Kryptographische Funktionen und APIs native im IBM i helfen diese Verschlüsselung zu realisieren.

Anwendungsverwaltung
Die Anwendungsverwaltung ermöglicht es den Administratoren festzulegen, welche Anwender auf welche Funktionen des Power i Systems zugreifen dürfen, wenn diese von Clients aus arbeiten.

Virenscan
Obwohl IBM i gegenüber Viren nicht anfällig ist (zumindest sind keinen Schäden bekannt), können im integrierten Dateisystem PC-Dokumente, die virenbefallen sind, gespeichert sein. Deshalb unterstützt IBM die Möglichkeit, Objekte über Drittanbieterprodukte gegen Virenbefall zu scannen und – im positiven Fall – eventuell die betreffenden Objekte über Betriebssystemfunktionen sperren zu lassen.

30. Ergänzung 3/2012

9.3.1
Seite 4

9.3.2 Sicherheit auf Netzwerkebene

Da Power i Systeme nahezu überall in Netzwerke integriert sind, hat IBM auch Funktionen implementiert, die den Schutz von Daten, die über Netzwerke gesandt werden, zu gewährleisten.

Sicherheits-Funktionen	Vertraulichkeit	Integrität	Authentifizierung	Authorisierung	Protokollieren Auditieren
IP Filterung und NAT			X	X	X
IDS		X			
VPN	X	X	X	X	X
L2TP			X	X	X
SSL/TLS	X	X	X	X	X
OpenSSH OpenSSL	X	X	X		
Kryptographie-Software	X	X	X		
Kryptographie-Hardware	X	X	X		

IP-Paketfilterung
IP-Paketfilterung erlaubt die Kontrolle des IP-Verkehrs in und aus dem Netzwerk heraus. Es schützt das Netzwerk durch die Filterung von Paketen – abhängig von den definierten Regeln.

NAT (Network Address Translation)
NAT übersetzt interne oder private IP-Adressen nach außen und trägt so zur Sicherheit bei, da interne Netzwerkadressen nach außen hin maskiert werden.

IDS (Intrusion Detection System)
IDS sammelt die Versuche von außen, die auf das System zuzugreifen. Dabei werden Protokollinformationen gesammelt und analysiert. Wenn diese eine kritische Masse übersteigen, wird von einer Netzwerkattacke ausgegangen, und es werden entsprechende Gegenmaßnahmen eingeleitet.

VPN (Virtual Private Network).
Ein VPM erlaubt die Verbindung aus einem geschützten Netzwerk heraus in ein anderes Netzwerk – über das öffentliche Internet hinweg. VPN kann über den iSeries Navigator installiert und konfiguriert werden. Die Daten in VPNs sind verschlüsselt und können von außen nicht mitgeschnitten werden.

L2TP (Layer 2 Tunneling Protocol)
L2TP ist ein Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht (Layer 2) des OSI-Modells zwischen zwei Netzwerken über das Internet tunnelt, um ein virtuelles privates Netzwerk (VPN) herzustellen.

Secure Sockets Layer/Transport Layer Security
Transport Layer Security (TLS) – weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL) – ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert.

Portable Utilities für i5/OS
Portable Utilities für i5/OS ist ein Lizenzprogramm für IBM i und beinhaltet OpenSSH, Open SSL und Zip Open Source. Das Programm wurde auf IBM i – unter Verwendung von PASE (Portable Application Solutions Environment – die Unix-Unterstützung im i5/OS) – implementiert.

OpenSSL
OpenSSL ist eine Open Source Software, die eine vollständige SSL-Implementierung durch SSL V3 und TSL V1 bietet. OpenSSL wird für SSL-Anwendungen genutzt.

OpenSSH
OpenSSH ist ebenfalls eine Open Source Software, die SecureShell und Secure Tunneling Service anbietet, damit beispielsweise der Datenverkehr über unsichere Netzwerke – wie das Internet – geschützt wird.

Kryptographie Software Support
Benutzeranwendungen können kryptographische Dienste indirekt über IBM i Funktionen – wie z.B. SSL, VPN IPSEC und LDAP – oder direkt über APIs anwenden.

Kryptographie Hardware Support
IBM Power i Systeme bieten verschiedene kryptografische Hardwarekomponenten an. Dazu gehören u. a. die kryptographischen Koprozessoren.

Sicherheit auf Anwendungsebene
Die Anwendungsebene ermöglicht den Benutzeranwendungen – wie FTP, Telnet, HTTP und anderen Netzwerkservices – mit dem Netzwerk zu interagieren.

Allerdings ist eine Software, die den Dienst der Anwendungsebene nutzt, nicht als Teil dieser Ebene zu bewerten. Beispielsweise gehört ein Web-Browser nicht zur Anwendungsebene, weil sie die Services, die von HTTP angeboten werden, dafür nutzt, um die Informationen ans Netzwerk zu senden. Im Folgenden sehen Sie einige Sicherheitsfunktionen der Applikationsebene und ihre Ziele:

Sicherheits-funktionen	Vertrau-lichkeit	Integrität	Authenti-fizierung	Authori-sierung	Protokol-lieren Auditieren
Validation Lists			X	X	X
Digitale Zertifikate		X	X	X	
Exit-Programme			X	X	X
SSL	X	X	X	X	X
Port-Ein-schränkungen				X	
Kerberos			X		X
Kryptographie-Software	X	X	X		
Kryptpgraphie-Hardware	X	X	X		
Secure Socket APIs	X	X	X	X	X
OpenSSL	X	X	X	X	X

Validation Lists
Validation Lists sind Objekte, in denen Benutzernamen und Kennwörter oder die SSL-Zertifikate bei Zugriffskontrolle gespeichert sind. Beispielsweise können Validation Lists für Einschränkungen bei Zugriff auf den HTTP-Server verwendet werden.

Digitale Zertifikate
In der Anwendungsebene bieten digitale Zertifikate eine Verschlüsselung durch den Einsatz von öffentlichen und privaten Schlüsseln, um den Netzwerkverkehr zu schützen.

Exit-Programme
Exit-Programme werden oben in der Systemebene unter „Exit-Programme" beschrieben. Allerdings können sie auch Teil der Anwendungsebene sein, wenn sie verwendet werden, um die Funktionalität von IBM i-Funktionen oder -Anwendungen hinzuzufügen Beispielsweise bietet der FTP-Server keine Standard-Schnittstelle, um eine Protokollierung von FTP-Unterbefehlen eines angemeldeten Benutzers zu aktivieren. Mit Hilfe des Exit-Points ist es möglich, eigene Exit-Programme zu schreiben, um solche Befehle zu protokollieren.

SSL
SSL auf Netzwerkebene wird in „Secure Sockets Layer / Transport Layer Security" erklärt. Es wird verwendet, um den Netzwerkverkehr zu verschlüsseln, aber es existiert auch auf der Anwendungsebene, da die Anwendungen SSL unterstützen müssen.

Port-Beschränkungen
Port-Beschränkungen werden verwendet, um Ports, die von nicht autorisierten Anwendungen und Anwendern benutzt werden, einzuschränken. Standardmäßig erlaubt TCP/IP jedem Benutzer einen Zugang über jeden Port.

Kerberos
Kerberos wurde bereits beschrieben. Das Kerberos-Protokoll ermöglicht die Authentifizierung und Überprüfung der Identität.

Kryptographische Software
Kryptographische Software wurde auf Netzwerkebene beschrieben. Benutzer-Anwendungen können kryptographische Dienste indirekt über IBM i Funktionen – wie SSL, VPN oder IPSec – nutzen. Benutzer-Anwendungen können auch auf kryptographische Dienste direkt über APIs zugreifen.

Kryptographische Hardware
Kryptographische Hardware wurde bereits auf der Netzwerkebene beschrieben. Diese Adapter können verwendet werden, um die Performance bei SSL zu verbessern. Allerdings bieten die kryptographischen Koprozessoren viele weitere Funktionen – wie z.B. PIN-Verarbeitung, Erzeugung von Signaturen, sichere Schlüsselspeicher etc.

Secure Socket APIs
Secure Socket APIs ermöglichen es den Programmierern, Secure Socket Anwendungen auf dem System zu erstellen.

OpenSSL
OpenSSL wird verwendet, um die Umgebung zu schaffen, die benötigt wird, um SSL-fähige Anwendungen ausführen zu können.

9.4 Sicherheitsstufe – QSECURITY

QSECURITY ist der grundlegende Wert zur Festlegung der Sicherheitsstufe im IBM i System. Genau damit haben so manche Unternehmen Probleme. Die ursprünglich sehr niedrig eingestellte Sicherheitsstufe des Systems wurde über Jahre hinweg nicht beachtet – und somit ist bei vielen Firmen eine Sicherheitsstufe vorhanden, die nicht von IBM empfohlen wurde.

Diese oben erwähnte oberste Sicherheitsstufe wird im Systemwert QSECURITY festgelegt. Für diejenigen, die mit Systemwerten nichts anfangen können kann mithilfe des Befehls WRKSYSVAL auf eine Vielzahl von Systemeinstellungen zugegriffen werden. Die Systemwerte können – abhängig von der Berechtigungsstufe des Benutzers – angezeigt bzw. geändert werden.

In neueren Versionen des IBM i Systems werden selbst die Systemwerte – zumindest die sicherheitsrelevanten – extra behandelt. Über die System Service Tools (SST) können sie vor Veränderungen geschützt werden.

Mit dem Befehl DSPSYSVAL QSECURITY kann die Sicherheitsstufe des IBM i angezeigt werden. Mit WRKSYSVAL QSECURITY kann sie angezeigt und geändert werden.

```
                              Systemwert ändern

Systemwert . . . . . :   QSECURITY
Beschreibung . . . . . :   Sicherheitsstufe des Systems


Auswahl eingeben und Eingabetaste drücken.

  Sicherheitsstufe des Systems   40_   20=Nur Kennwortsicherheit
                                       30=Kennwort- und Objektsicherheit
                                       40=Integrität von Kennwort, Objekt und
                                         Betriebssystem
                                       50=Integrität von Kennwort, Objekt und
                                         erweitertem Betriebssystem
```

Systemwert QSECURITY

9.4
Seite 2

Welche Sicherheitsstufen gibt es im IBM i und was steckt dahinter?

Sicherheitsstufe	Beschreibung
10	Keine Sicherheit. Jeder Benutzer kann sich am System anmelden (wird von IBM nicht mehr unterstützt).
20	Für die Anmeldung am System ist ein Kennwort erforderlich. Benutzer haben Zugriff auf alle Systemressourcen.
30	Für die Anmeldung am System ist ein Kennwort erforderlich. Für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung.
40	Für die Anmeldung am System ist ein Kennwort erforderlich. Für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung. Die Ausführung von Programmen schlägt fehl, wenn versucht wird, über nicht unterstützte Schnittstellen auf Objekte zuzugreifen.
50	Für die Anmeldung am System ist ein Kennwort erforderlich. Für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung. Die Ausführung von Programmen schlägt fehl, wenn versucht wird, nicht unterstützte Parameterwerte an unterstützte Schnittstellen zu übergeben oder über nicht unterstützte Schnittstellen auf Objekte zuzugreifen.

Die Sicherheitsstufe 10 spielt also sowieso keine Rolle mehr. Dagegen ist die Sicherheitsstufe 50 das andere Extrem, das ich in der Praxis auch noch nicht gesehen habe. Bleiben die Sicherheitsstufen 20 bis 40, mit denen die meisten Systeme arbeiten.

In Sicherheitsstufe 20 haben alle Benutzerprofile *ALLOBJ Berechtigung. Das bedeutet, dass die Objekt-Berechtigung sowie alle weiteren Objekte im Power i System uneingeschränkt verwendet werden können: Programme, Dateien, Benutzer, Ausgabewarteschlangen, Drucker, Bildschirme.

Jeder Benutzer – egal ob Geschäftsführer, Abteilungsleiter, Buchhalter, Verkäufer, Einkäufer, Lagerist etc. – hat bei Sicherheitsstufe 20 vollen Zugriff auf alles im System. Das ist nicht gut, meinen Sie vielleicht – und haben damit recht. Das bedeutet nämlich auch, dass jeder Benutzer Zugriff auf Buchhaltungsdaten, Kalkulationen, Konditionen und auf Lohndaten (sofern diese auf dem Power i System abgerechnet werden) hat.

Wie passt denn das zusammen? Sicheres System und Sicherheitsstufe 20? Hier sollte man die Arbeitsweise auf dem System in der Rückschau betrachten.

Ein wichtiges Merkmal bei der Verarbeitung von Anweisungen im IBM i sind Befehle. So ziemlich alle Aktionen im Betriebssystem sind mit Befehlen ausgestattet, die es einem Benutzer oder Administrator erlauben, bestimmte Funktionen aufzurufen. Um etwas zu arbeiten, ruft man WRKxxx auf, um etwas anzuzeigen DSPxxx und um etwas zu erstellen CRTxxx.

```
                                  Befehl auswählen

Auswahl eingeben und Eingabetaste drücken.
  1=Auswählen

Ausw  Befehl       Bibliothek  Text
 _    WRKACTJOB    QSYS        Mit aktiven Jobs arbeiten
 _    WRKALR       QSYS        Mit ALERTS arbeiten
 _    WRKALRD      QSYS        Mit ALERT-Beschreibungen arb.
 _    WRKALRTBL    QSYS        Mit ALERT-Tabelle arbeiten
 _    WRKAPPNSTS   QSYS        Mit APPN-Status arbeiten
 _    WRKARMJOB    QSYS        Work with ARM Jobs
 _    WRKASPJOB    QSYS        Mit ASP-Jobs arbeiten
 _    WRKAUT       QSYS        Mit Berechtigung arbeiten
 _    WRKAUTL      QSYS        Mit Berechtig.listen arbeiten
 _    WRKBNDDIR    QSYS        Mit Binderverzeichn. arbeiten
 _    WRKBNDDIRE   QSYS        Mit Binderverz.eintr. arbeiten
 _    WRKBPTBL     QSYS        Mit BOOTP-Tabelle arbeiten
```

Befehle WRK…

Ein Befehl funktioniert nur richtig, wenn man a) die zum Befehl dazugehörigen Parameter kennt und b), wenn man weiß, wie der Befehl korrekt heißt. Hierbei hilft das Betriebssystem IBM i weiter. Wenn man beispielsweise vorhat, sich nur etwas anzeigen zu lassen, dann gibt man DSP* ein und drückt die F4-Taste. Mit F4 werden neben dem Befehl auch noch die Werte angezeigt, mit denen die einzelnen Parameter gefüllt werden können.

```
                    Mit aktiven Jobs arbeiten (WRKACTJOB)

Auswahl eingeben und Eingabetaste drücken.

Ausgabe  . . . . . .  *          *, *PRINT

                 Zusätzliche Parameter

Statistik zurücksetzen . . . . .  *NO          *NO, *YES
Subsystem  . . . . . .  *ALL         Name, *ALL
     + für weitere Werte
CPU-Prozentgrenze  . . . . . .  *NONE        .1-99.9, *NONE
Antwortzeitgrenze  . . . . . .  *NONE        .1-999,9 Sek. *NONE
Folge  . . . . . .  *SBS         *SBS, *AUXIO, *CPU...
Jobname  . . . . . .  *ALL         Name, generisch*, *ALL...
Intervall für autom. Aktualis.    *PRV         5-999 Sekunden, *PRV
```

WRKACTJOB mit allen Parametern

```
          Wert für Parameter angeben                SEQ

Auswahl eingeben und Eingabetaste drücken.


Folge  . . . . . .  . . . .   *SBS

  *SBS                                  *THREADS
  *AUXIO                                *TYPE
  *CPU                                  *USER
  *CPUPCT
  *CURUSR
  *FUNCTION
  *INT
  *JOB
  *NUMBER
  *POOL
  *PTY
  *RSP
  *STS
```

Werte für Parameter Folge mit F4 gepromptet

Doch zurück zum Wichtigen: Befehle werden oftmals nicht einfach nur aufgerufen. Genau das unterscheidet IBM i auch beispielsweise von einem Unix: Die Befehle sind in Menüs eingebunden. Es gibt Menüs für alle möglichen Betriebssystemfunktionen, aber auch für eigene Programmaufrufe aus Warenwirtschaft, Buchhaltung etc. Mit GOxxx wird ein Menü aufgerufen – beispielsweise zeigt GO MAIN das Hauptmenü des Betriebssystems und GO ASSIST das Operational Assistant Menü.

```
MAIN                              i5/OS-Hauptmenü

Auswahlmöglichkeiten:

     1. Benutzeraufgaben
     2. Büroaufgaben
     3. Allgemeine Systemaufgaben
     4. Dateien, Bibliotheken und Ordner
     5. Programmierung
     6. Datenfernverarbeitung
     7. System definieren oder ändern
     8. Problembehandlung
     9. Menü anzeigen
    10. Unterstützende Informationen - Auswahlmöglichkeiten
    11. iSeries Access-Aufgaben

    90. Abmelden
```

Hauptmenü des IBM i

Aber was hat das jetzt mit Sicherheit zu tun, fragen Sie sich vielleicht? Ganz einfach: Menüs und Benutzer gehören beim IBM i oft fest zusammen.

Jeder Anwender bekommt im IBM i ein Benutzerprofil, das neben seinem Anmeldenamen auch sein Kennwort und viele Parameter beinhaltet, um diesen Anwender – nach der Anmeldung im System – individuell zu behandeln. Zu den Benutzerprofilen später aber mehr.

Ein wichtiges Merkmal, um auch bei Sicherheitsstufe 20 eine brauchbare Sicherheit zu bekommen, ist die Zuordnung eines Menüs. Daran ist die Option gekoppelt, dass ein Benutzer lediglich nur eine Menüauswahl aufrufen kann und sonst nichts.

So genannte „Zwangsmenüs“ – so heißt das Zauberwort hier. Im Benutzerprofil gibt es einen Parameter, der die Möglichkeit, in der Befehlszeile einer Bildschirmsitzung etwas eingeben zu können, steuert.

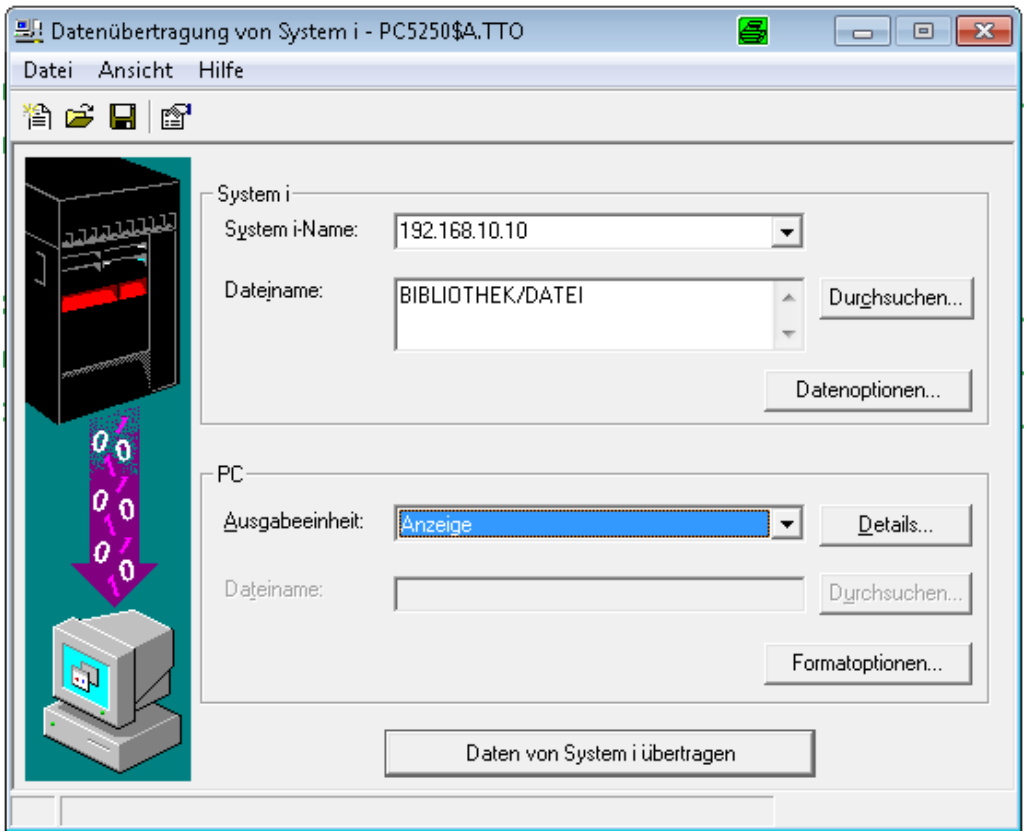
```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > RENGEL        Name
Benutzerkennwort . . . . . *SAME

Kennwort auf abgelaufen setzen    *NO          *SAME, *NO, *YES
Status . . . . . .  *ENABLED     *SAME, *ENABLED, *DISABLED
Benutzerklasse . . . . . .  *SECOFR      *SAME, *USER, *SYSOPR...
Unterstützungsstufe  . . . . .  *SYSVAL      *SAME, *SYSVAL, *BASIC...
Aktuelle Bibliothek  . . . . .  *CRTDFT      Name, *SAME, *CRTDFT
Aufzurufendes Startprogramm  . .  *NONE       Name, *SAME, *NONE
  Bibliothek . . . . . .  .                  Name, *LIBL, *CURLIB
Anfangsmenü  . . . . . .  .  MAIN        Name, *SAME, *SIGNOFF
  Bibliothek . . . . . .  .    *LIBL       Name, *LIBL, *CURLIB
Möglichkeiten einschränken . . .  *NO        *SAME, *NO, *PARTIAL, *YES
Text 'Beschreibung'  . . . . .  'Robert Engel'
```

*Möglichkeiten einschränken – LMTCPB *YES/*NO*

Wenn der Parameter „Möglichkeiten einschränken“ auf *NO steht, kann der Benutzer – bei Anzeige eines Menüs – die Befehlszeile nutzen und einen Befehl aus dem Betriebssystem oder der Anwendung bzw. aus den Programmen aufzurufen. Steht diese Möglichkeit auf *YES, kann der Anwender nur die Optionen aus dem Menü aufrufen, die ihm die Programmierer zur Verfügung gestellt haben.

Prima – bei Sicherheitsstufe 20 gibt es Zwangsmenüs und alles ist in Ordnung? Jeder Anwender kann nur das aufrufen, was im Menü steht und das war es!? Schön und gut, aber das Ganze hat einen Haken: Seit vielen Jahren gibt es nicht nur die gleichermaßen geliebte und gehasste Anzeige der 5250-Emulation, sondern auch eine externe Zugriffsmöglichkeit, die durch die Einführung des TCP/IP-Protokolls – damals noch für die AS/400 – entstanden ist. Vorher war die Kommunikation mit dem SNA-Protokoll (Systems Network Architektur) weitestgehend auf Host-Systeme beschränkt, nun kamen plötzlich die PCs mit all ihren Möglichkeiten ins Spiel.

So konnten und können die Anwender immer noch über eine einfache IBM System i Access-Sitzung mit den entsprechend installierten Optionen, Daten aus den Power i Systemen mit wenigen Mausklicks auf die PCs übertragen. Oder sie können Auswertungsprogramme starten, die über SQL-Anweisungen Daten aus diesen Power i Datenbanken – z. B. in Excel – übertragen.



Datenübertragung vom System i

Was ist jetzt noch die Sicherheitsstufe 20 wert, wenn jeder Anwender auf alle Daten des Systems uneingeschränkt (*ALLOBJ-Berechtigung) zugreifen kann? Ok – es soll tatsächlich Firmen geben, in denen jeder Mitarbeiter alles wissen darf, aber normalerweise ist so eine Vorgehensweise securitytechnisch gesehen eine Katastrophe.

Dagegen muss etwas unternommen werden. Empfehlenswert ist die Sicherheitsstufe 40, da selbst bei dieser, erfahrene Programmierer die Sicherheitsprüfungen nicht umgehen können. Wenn ein neues Power i System in Betrieb genommen werden soll, dann empfehlen alle Sicherheitsexperten grundsätzlich mit der Sicherheitsstufe 40 zu beginnen.

Auch aus anderen Gründen ist die Menüsicherheit mit Sicherheitsstufe 20 nicht ausreichend. Oftmals haben Anwender hier aber auch den Zugriff auf eine Befehlszeile oder auf eine Auswertungssoftware zur Analyse von Unternehmensdaten. Benutzer auf Sicherheitsstufe 20 sollten jedoch keinerlei Zugriff auf diese Befehlszeile oder auf Query-Funktionalität erhalten, denn das Benutzerprofil mit der Sonderberechtigung *ALLOBJ berechtigt sie zum uneingeschränkten Zugriff auf alle Daten im System.

Sicherheitsstufe 30 bietet eine spürbare Verbesserung der gesamten Sicherheit. Auch Sicherheitsstufe 40 kostet nicht zusätzliche Systemleistung oder Overhead. Sicherheitsstufe 40 verhindert potentielle Integritäts- oder Sicherheitsprobleme, die von Programmen ausgehen, die in besonderen Fällen die Sicherheitsvorkehrungen umgehen können.

9.4
Seite 8

9.4.1 Sicherheitsstufe 40

Nachfolgend finden Sie eine Zusammenfassung des erhöhten Schutzes auf Sicherheitsstufe 40.

Interne Schnittstellen – Das System unterbindet Versuche, Systemprogramme, die nicht als Schnittstellen auf Aufrufebene definiert sind, direkt aufzurufen. Beispiel: Direkter Aufruf des befehlsverarbeitenden Programms für den Befehl SIGNOFF. Der Schutz der internen Schnittstellen auf Sicherheitsstufe 40 und höher beinhaltet beispielsweise die Verhinderung des Zugriffs auf interne Systemstrukturen über die Zeiger-Funktionalität von Sprachen – wie C, PASCAL oder MI.

Jobübergabe – Wenn in einer Jobbeschreibung ein Benutzerprofilnamen als Wert für das Feld USER verwendet wird, können alle Jobs, die mit der Jobbeschreibung übergeben werden, mit Attributen ausgeführt werden, die von diesem Benutzerprofil stammen. Ein unberechtigter Benutzer könnte einen Sicherheitsverstoß begehen, indem er einen Job für die Ausführung unter dem in der Jobbeschreibung angegebenem Benutzerprofil übergibt.

***USE-Berechtigung** – Auf Sicherheitsstufe 30 wird der Job unter der Voraussetzung ausgeführt, dass die übergebende Person *USE-Berechtigung für die Jobbeschreibung besitzt. Auf Sicherheitsstufe 40 und höher muss der Benutzer, der den Job übergibt, *USE-Berechtigung für die Jobbeschreibung und das in der Jobbeschreibung angegebene Benutzerprofil besitzen. Anderenfalls wird der Job fehlschlagen. Diese Eigenschaft ist für die meisten Power i Systeme der wichtigste Vorteil der Sicherheitsstufe 40 gegenüber der Sicherheitsstufe 30. Die Standardberechtigung für die Benutzerprofile ist *EXCLUDE. Daher müssen die Benutzer ausdrücklich die Berechtigung erhalten, um die Jobs als andere Benutzer ausführen zu können.

Anmelden ohne Kennwort – Auf Sicherheitsstufe 30 und niedriger ist es bei bestimmten Subsystembeschreibungen möglich, sich ohne Benutzerkennung und Kennwort anzumelden. Auf Sicherheitsstufe 40 und höher verhindert das System jeden Versuch der Anmeldung ohne Benutzerkennung und Kennwort.

Ich empfehle Ihnen, Ihr Power i System mit Sicherheitsstufe 40 in Betrieb zu nehmen, wenn Sie nicht Software von Drittanbietern installiert haben, die mit den Restriktionen der Sicherheitsstufe 40 nicht kompatibel ist.

Planen Sie jedoch nach Möglichkeit nicht von Sicherheitsstufe 20 direkt auf Sicherheitsstufe 40 zu wechseln, solange Ihr System aktiv im Produktionsbetrieb ist.

9.4.1
Seite 2

Die vorbereitenden Schritte, die für einen reibungslosen Übergang auf Sicherheitsstufe 40 erforderlich sind, werden in zwei Abschnitten beschrieben: Von Sicherheitsstufe 20 auf Sicherheitsstufe 30 und von Sicherheitsstufe 30 auf Sicherheitsstufe 40. Wenn Sie die beschriebenen Schritte ausführen, können Sie Geschäftsleitung, Benutzer und Auditoren von Ihrer neuen Power i Sicherheitsstufe überzeugen und beeindrucken.

9.4.2 Von Sicherheitsstufe 20 auf Sicherheitsstufe 30 wechseln

Der Wechsel von Sicherheitsstufe 20 auf Sicherheitsstufe 30 geschieht, indem Sie den Systemwert QSECURITY auf 30 ändern. Die Aktivierung von Sicherheitsstufe 30 wird mit dem nächsten IPL ausgeführt. Wenn Sie von Sicherheitsstufe 20 auf Sicherheitsstufe 30 wechseln, ändert das System beim nächsten IPL alle Benutzerprofile. Sonderberechtigungen werden den Benutzerprofilen hinzugefügt bzw. entfernt und somit an die Sonderberechtigung für die Benutzerklasse angepasst.

Leider ist die Umstellung auf Sicherheitsstufe 30 nicht ganz unproblematisch. Wenn beispielsweise Ihr System Produktionsanwendungen auf einer niedrigeren Sicherheitsstufe ausführt, sollten Sie die Sicherheit auf Objektebene konfigurieren und testen, bevor Sie zur Sicherheitsstufe 30 wechseln. Wenn Sie den Systemwert ohne ausreichende Planung ändern, ist es möglich, dass Ihr Telefon ständig von frustrierten Anwendern belegt wird, die sich darüber beklagen, dass Aufgaben, die früher problemlos ausgeführt werden konnten, mit Nachrichten wie „keine Berechtigung“ fehlschlagen.

Wenn Sie auf Sicherheitsstufe 30 wechseln, wird die Berechtigung *ALLOBJ aus allen Benutzerprofilen entfernt, bei denen es sich nicht um die Benutzerklasse *SECOFR handelt. Benutzer, die früher über *ALLOBJ-Zugriff auf alle Objekte im System verfügten, benötigen nun spezifische Berechtigung für den Zugriff auf alle Objekte. Der nachfolgend beschriebene schrittweise Prozess ermöglicht den reibungslosen Übergang von Sicherheitsstufe 20 auf Sicherheitsstufe 30.

1. Ändern Sie den Systemwert QSECURITY nicht sofort von 20 auf 30. Arbeiten Sie weiter mit Sicherheitsstufe 20, während Sie den Benutzern die Berechtigung für die Objekte erteilen.
2. Weisen Sie den Benutzern Gruppen zu.
   - Bestimmen Sie, ob Benutzergruppen mit ähnlichen Jobanforderungen vorhanden sind – wie z.B. Benutzer aus der gleichen Abteilung, die Zugriff auf die gleichen Informationen benötigen. Einige Benutzer gehören eventuell zu keiner derartigen Gruppe.
   - Spezifizieren Sie die Sonderberechtigung *NONE, wenn Sie ein Gruppenprofil für Benutzer mit ähnlichen Anforderungen erstellen. Das Kennwort für Gruppenprofile sollte *NONE sein, um so die Anmeldung als Gruppenprofil zu verhindern. Ich empfehle eine Namenskonvention für Gruppenprofile (wie z. B. GRPXXX), um Gruppenprofile

eindeutig zu kennzeichnen. Ein Beispiel für den Befehl zur Erstellung eines Gruppenprofils für die Vertriebsabteilung ist:

```
CRTUSRPRF USRPRF(GRPVTR) +
PASSWORD(*NONE) SPCAUT(*NONE) +
TEXT('Gruppenprofil Vertriebsabteilung')
```

- Verwenden Sie den Befehl CHGUSRPRF (Benutzerprofil ändern), um individuelle Benutzerprofile einer Gruppe zuzuweisen.

  Wenn Sie die Benutzer einem Gruppenprofil zuweisen, empfehle ich die Verwendung des Parameters OWNER(*GRPPRF). Damit kennzeichnen Sie das Gruppenprofil als Eigner der neuen Objekte, die von den Benutzern in der Gruppe erstellt werden. Der Befehl für die Zuweisung der Benutzer zum Gruppenprofil GRPCTR lautet:

```
CHGUSRPRF USRPRF(user_profile) +
GRPPRF(GRPVTR) OWNER(*GRPPRF)
```

3. Erstellen Sie ein Testbenutzerprofil. Sie können das Testbenutzerprofil verwenden, um fehlende Berechtigung zu entdecken und das Problem zu korrigieren, bevor es sich auf die Produktionsbenutzer auswirkt. Wenn Sie die Testbenutzerprofile erstellen, weisen Sie die Sonderberechtigung *NONE zu und nehmen das Benutzerprofil in die Gruppe auf. Der folgende Befehl beschreibt die Erstellung des Testprofils für die Vertriebsgruppe:

```
CRTUSRPRF USRPRF (TESTVTR) PASSWORD(X) +
USRCLS(*USER) INLPGM(–) INLMNU(–) +
SPCAUT(*NONE) GRPPRF(GRPVTR) + TEXT('Testprofil
für die Vertriebsgruppe')
```

Die Parameterwerte, die im oben beschriebenen Wert als „'—“ angegeben werden, sollten dieselben sein wie die Werte, die den Benutzern in dieser Gruppe aktuell zugewiesen worden sind. Eine einfache Methode für das Kopieren der Parameter aus einem vorhanden Benutzerprofil besteht darin, den Befehl WRKUSRPRF – (Mit Benutzerprofil arbeiten) zu verwenden und die Kopieroption (Option 3) auszuwählen. Mit dieser Aktion wird eine Bedienerführung für das neue Profil mit den aktuellen Werten ausgegeben. Sie müssen nur noch Profilnamen, Benutzerklasse, Sonderberechtigung, Gruppenprofil und Text ändern.

4. Suchen und korrigieren Sie mit dem Testprofil für die Gruppe Bedingungen, bei denen die Nachricht „Nicht berechtigt“ angezeigt wird.
   - Melden Sie sich mit dem Benutzerprofil TESTVTR an und führen Sie die Aufgaben eines Benutzers in der Vertriebsgruppe aus.
   - Wenn eine Aufgabe mit der Nachricht „Nicht berechtigt“ angezeigt wird, verwenden Sie den Befehl GRTOBJAUT (Objektberechtigung erteilen), um den erforderlichen Zugriff auf das Gruppenprofil zuzuweisen oder die Zugriffsberechtigung für das Objekt auf *PUBLIC zu setzen.
   - Eine Alternative für die Erteilung von Zugriffsberechtigung ist die Verwendung der Berechtigungsübernahme durch Programme.
   - Arbeiten Sie weiterhin mit dem Benutzerprofil TESTVTR, bis Sie alle Aufgaben eines Gruppenmitglieds ausführen können.
5. Entfernen Sie die Berechtigung *ALLOBJ eines einzelnen Produktionsbenutzers in der Gruppe.
   - Informieren Sie diesen Benutzer, dass Sie die Systemsicherheit verbessern möchten. Fordern Sie ihn dazu auf, sich an Sie zu wenden, sobald sicherheitsbezogene Anwendungsprobleme auftreten.
   - Entfernen Sie mit Hilfe des Befehls CHGUSRPRF die Berechtigung SPCAUT(*ALLOBJ) aus diesem individuellen Profil. Wenn der Produktionsbenutzer Nachrichten zur Nichtberechtigung erhält, erteilen Sie die erforderliche Berechtigung der Allgemeinheit (*PUBLIC), dem Gruppenprofil oder dem individuellen Profil. In den meisten Fällen sollten die Objekte über die Berechtigung *PUBLIC verfügen oder über Berechtigung für das Gruppenprofil, deshalb ist nicht zu erwarten, dass andere Mitglieder der Gruppe Nachrichten über eine Nichtberechtigung erhalten.
   - Setzen Sie Ihre Arbeit fort, bis der Produktionsbenutzer alle Aufgaben ausführen kann.
6. Entfernen Sie mit dem Befehl CHGUSRPRF den Wert *ALLOBJ aus allen anderen Profilen der Gruppenmitglieder.
7. Löschen Sie das Testbenutzerprofil TESTVTR, das in Schritt 3 erstellt wurde. Nicht verwendete Profile, die bei Testläufen übriggeblieben sind oder von Benutzern stammen, die versetzt wurden und nicht mehr im System arbeiten, sind eine in vielen Systemen häufig anzutreffende Sicherheitslücke. Das Problem kann am einfachsten gelöst werden, indem die nicht verwendeten Benutzerprofile sofort gelöscht werden.
8. Wiederholen Sie die Schritte 3 bis 7 für jede weitere Gruppe. Wählen Sie jeweils eine Gruppe aus und bearbeiten Sie diese vollständig, bevor Sie die nächste Gruppe konfigurieren.

9. Nun wenden Sie sich den Benutzern zu, die nicht Mitglieder eines Gruppenprofils sind. Nachdem Sie alle Produktionsbenutzer, die Mitglieder einer Gruppe sind, mit ausreichender Berechtigung ausgestattet haben, müssen Sie die *ALLOBJ-Zugriffsrechte den übrigen Benutzern entziehen, die nicht Mitglied einer Gruppe sind. Der Befehl DSPAUTUSR (Berechtigte Benutzer anzeigen) kann alle Benutzerprofile und ihre Gruppenmitgliedschaft anzeigen.

   DSPAUTUSR kann darüber hinaus Profile anzeigen, die zu keinem Gruppenprofil gehören. Ich empfehle Ihnen, die Einstellungen für Benutzer, die zu keiner Gruppe gehören, erst nach Beendigung der Arbeit mit allen Gruppen vorzunehmen. Auf diese Weise können Sie die Anzahl der Anrufe reduzieren, die Sie von Benutzern mit Berechtigungsproblemen erhalten.

10. Vergeben Sie an privilegierte Benutzer Berechtigungen für die Arbeitsstationen. Wenn der Systemwert QLMTSECOFR (Zugriff des Sicherheitsadministrators auf die Einheiten begrenzen) 1 (Ja) beträgt, müssen Benutzer mit spezieller *ALLOBJ – oder *SERVICE-Berechtigung – wie z. B. QSECOFR – spezifische Berechtigung erhalten, um auf Einheiten mit Sicherheitsstufe 30 oder höher zuzugreifen. Geben Sie diesen Benutzern für die Arbeitsstation, die sie verwenden, *CHANGE-Berechtigung.

11. Ändern Sie den Systemwert. Nachdem Sie aus allen Profilen – außer denen der Benutzer der Benutzerklasse *SECOFR – die Berechtigung *ALLOBJ entfernt haben, können Sie den Systemwert QSECURITY von 20 auf 30 ändern, ohne die Benutzer in Aufruhr zu versetzen. Wenn Sie den Systemwert von 20 auf 30 ändern und ein IPL ausführen, wird *ALLOBJ aus allen Benutzerprofilen entfernt. Wenn Sie die Schritte 1 bis 10 befolgen, muss das System keine Sonderberechtigung hinzufügen oder entfernen, um die Standardeinstellungen für Sicherheitsstufe 30 zu berücksichtigen. Nachdem der Systemwert geändert wurde und ein IPL erfolgt ist, können Sie sich gratulieren. Aber vergewissern Sie sich, dass Sie nicht den letzten, wichtigen Schritt vergessen haben.

    Nachdem Sie die Benutzerprofile und Benutzergruppen mit der korrekten Berechtigung versehen haben, müssen Sie SAVSECDTA (Sicherheitsdaten speichern) oder SAVSYS (System sichern) ausführen, um eine Sicherungskopie der Benutzerprofile und Berechtigungen zu erstellen.

9.4.3 Von Sicherheitsstufe 30 auf Sicherheitsstufe 40 wechseln

Die Prozedur für den Wechsel von Sicherheitsstufe 30 auf Sicherheitsstufe 40 ähnelt dem Wechsel von Sicherheitsstufe 20 auf Sicherheitsstufe 30, aber Ihr Augenmerk sollte dabei auf den Programmen liegen, die gegen die Einschränkungen der Sicherheitsstufe 40 verstoßen, die weiter oben in diesem Kapitel beschrieben wurden.

In der folgenden Übersicht ist zu sehen, was in den unterschiedlichen Sicherheitsstufen unterstützt wird:

Funktionsübersicht Sicherheitsstufen	20	30	40	50
Benutzername zum Anmelden erforderlich.	Ja	Ja	Ja	Ja
Kennwort zum Anmelden erforderlich.	Ja	Ja	Ja	Ja
Kennwortschutz aktiv.	Ja	Ja	Ja	Ja
Menü und Startprogramm aktiv.	Ja	Ja	Ja	Ja
Einschränkung der Eingaben aktiv.	Ja	Ja	Ja	Ja
Ressourcenschutz aktiv.	Nein	Ja	Ja	Ja
Zugriff zu allen Objekten.	Ja	Nein	Nein	Nein
Sicherheitsauditierung aktiv.	Ja	Ja	Ja	Ja
Programme mit nicht unterstützten Interfaces verwenden. Diese laufen auf Fehler.	Nein	Nein	Ja	Ja
Erweiterter Hardwareschutz unterstützten.	Nein	Nein	Ja	Ja
*USRSPC, *USRIDX, und *USRQ Objekte können nur in Bibliotheken, die im Systemwert QALWUSRDMN angegeben sind, erstellt werden.	Ja	Ja	Ja	Ja
Pointer in Parametern werden für Benutzerdomänenprogramme im System und User State geprüft.	Nein	Nein/ Ja	Ja	Ja
Nachrichtenbehandlungs-regeln zwischen System und User State gefordert.	Nein	Nein	Nein	Ja
Einem Programm zu gewiesener Speicher kann nicht direkt geändert werden.	Nein	Nein	Ja	Ja
Interne Control Blocks sind geschützt.	Nein	Nein	Ja	Ja

30. Ergänzung 3/2012

9.4.3
Seite 2

Neben den in Tabelle 1 genannten Funktionen ist es wichtig zu wissen, dass die Sicherheitsstufe die standardmäßig vergebenen Sonderberechtigungen bestimmt. Um zu verstehen, wie Sonderberechtigungen zu den Benutzerklassen gehören, wenn Sie ein Benutzerprofil erstellen, drücken Sie die Hilfe-Taste auf dem Parameter „Benutzerklasse“. Hier wird das Zusammenspiel erläutert.

9.4.4 Hilfe zur Benutzerklasse

Gibt die Art des Benutzers an, der diesem Benutzerprofil zugeordnet ist: Sicherheitsbeauftragter, Sicherheitsadministrator, Programmierer, Systembediener oder Benutzer. Die Benutzerklasse steuert die im Menü gezeigten Auswahlmöglichkeiten. Sonderberechtigungen werden nur erteilt, wenn *USRCLS für den Parameter „Sonderberechtigung“ (SPCAUT) angegeben wird. Wurde SPCAUT(*USRCLS) angegeben, variieren die Sonderberechtigungen abhängig vom QSECURITY-Wert.

***SAME**
Der Wert ändert sich nicht.

***USER**
Auf QSECURITY-Sicherheitsstufe 10 oder 20 verfügt der Benutzer über die Berechtigungen *ALLOBJ und *SAVSYS.

Auf QSECURITY-Sicherheitsstufe 30 oder höher hat der Benutzer keine Sonderberechtigungen.

***SECOFR**
Auf allen Sicherheitsstufen verfügt der Sicherheitsbeauftragte über die folgenden Sonderberechtigungen:

*ALLOBJ
*SAVSYS
*JOBCTL
*SERVICE
*SPLCTL
*SECADM
*AUDIT
*IOSYSCFG

***SECADM**
Auf QSECURITY-Sicherheitsstufe 10 oder 20 verfügt der Sicherheitsadministrator über die Sonderberechtigungen *ALLOBJ, *SAVSYS, *SECADM und *JOBCTL.

Auf QSECURITY-Sicherheitsstufe 30 oder höher verfügt der Benutzer über die Sonderberechtigungen *SECADM.

***PGMR**
Auf QSECURITY-Sicherheitsstufe 10 oder 20 verfügt der Programmierer über die Sonderberechtigungen *ALLOBJ, *SAVSYS und *JOBCTL.

Auf QSECURITY-Sicherheitsstufe 30 oder höher hat der Benutzer keine Sonderberechtigungen.

30. Ergänzung 3/2012

9.4.4
Seite 2

***SYSOPR**
Auf QSECURITY-Sicherheitsstufe 10 oder 20 verfügt der Systembediener über die Sonderberechtigungen *ALLOBJ, *SAVSYS und *JOBCTL.

Auf QSECURITY-Sicherheitsstufe 30 oder höher verfügt der Benutzer über die Sonderberechtigungen *SAVSYS und *JOBCTL.

Wenn Sie ein Benutzerprofil erstellen, können Sie Sonderberechtigungen auf der Grundlage der Benutzer-Klasse auswählen. Sonderberechtigungen werden zu den Benutzerprofilen ebenfalls hinzugefügt oder davon entfernt, wenn Sie die Sicherheitsstufe ändern.

Sicherheitsstufe 40 betrifft fast jedes, wenn nicht gar jedes Objekt auf dem System. Da es viel bei der Umstellung auf Level 40 zu beachten gibt, sollte man wissen, dass es einen „empfohlenen Weg" gibt. Das Tool, das alle Experten empfehlen, ist das Auditjournal. Das Auditjournal muss erstellt und eingeschaltet werden. Der Inhalt sollte für eine Weile überwacht werden, um sicher zu sein, dass das System mit den Anwendungen die Sicherheitsstufe 40 oder höher unterstützt. Dies führt zur nächsten Frage: „Brauche ich die Journalisierung, damit die Sicherheitsstufe 40 laufen kann?"

Die einfache Antwort auf diese Frage ist „Ja", aber dabei handelt es sich nicht exakt um das gleiche Konzept wie die Datenbank-Journalisierung. Sie brauchen zum Einrichten des Auditjournals ein Journalobjekt auf Ihrem System und müssen die Journalempfänger an dieses anhängen – ähnlich wie bei der Datenbank-Journalisierung. Dann müssen Sie Ihrem System über die Systemwerte QAUDLVL und QAUDLVL2 beibringen, welche Art von Sicherheitsprüfungen aufgezeichnet und gesucht werden sollen.

Sicherheitsprüfungen deshalb, weil sie bereits seit der Sicherheitsstufe 30 existieren. Nur sind sie in Sicherheitsstufe 30 noch nicht wirksam, doch es gibt sie. Mit anderen Worten – ab Sicherheitsstufe 40 weiß das System, dass Ihr Code die Integrität oder andere Regeln der Sicherheitsstufe 40 oder 50 Regeln verletzt. Nachdem das System den Fehler aufgezeichnet hat, was sich natürlich auf die Leistung auswirkt, wird bei Sicherheitsstufe 30 das Programm trotzdem funktionieren. In Sicherheitsstufe 40 und 50, erzeugt diese Ausführung Meldungen und der Job schlägt fehl.

Die gute Nachricht ist, dass der Sprung von Sicherheitsstufe 30 auf 40 keine Änderungen an den Profilen oder Berechtigungslisten mit sich bringt, so dass es sich leicht umstellen lässt. Darüber hinaus hat es keinen Einfluss auf die Programme, die Berechtigungen übernehmen (so genannte Adopted Authority), sofern diese Standard-Interfaces verwenden.

Nach Konfiguration der Auditjournalisierung zur Fehleraufzeichnung sollten Sie eine Zeit lang alle Geschäftsvorfälle, die vorkommen, beobachten. Ideal ist es zum Ende des Geschäftsjahres – mit allen jährlichen, vierteljährlichen, monatlichen und täglichen Abläufen. Ziel muss es sein, so viele Prozesse wie möglich durchzuspielen, um festzustellen, ob die Einträge im Auditjournal mit dem Typ AF (Authority Failure – Berechtigungsfehler) generiert werden.

Die Einträge im Auditjournal vom Typ AF werden nicht viele sein, selten gibt es Auditjournale mit mehr als 100 Seiten. Das ist in der Regel keine große Sache in Bezug auf die Speicherung; die Auswirkungen auf die Leistung gehen Richtung Null.

Sie werden erstaunt sein, was auf Ihren Auditprotokollen alles erscheint. Sie tun bestimmt nur, was notwendig ist, um schnell auf die Sicherheitsstufe 40 wechseln zu können. Aber es gibt eine Menge von anderen Optionen, die Ihnen helfen können, Ihr System transparenter zu machen. Sollten Sie mit der Auswertung der Auditjournale an ihre Grenzen stoßen, gibt es einige Produkte von Security-Anbietern, die Ihnen die Arbeit durch vordefinierte Regeln und Auswertungen leichter machen.

Bevor Sie mit der Auditjournal-Prozedur beginnen, sollten Sie eine Bestandsaufnahme aller Software-Pakete auf Ihrem System vornehmen und alle Anbieter kontaktieren, um zu sehen, ob diese mit der Sicherheitsstufe 40 konform sind. Sollten sie nicht kompatibel sein, können Sie die Sicherheitsstufe 40 nicht umsetzen. D.h., Sie sollten ein Update installieren, damit es verfügbar ist. Die meisten Anbieter sind bereits mit ihrer Software-Version kompatibel, aber trotzdem liegt es an Ihnen, die Entscheidung zu treffen. Deshalb: Egal, was Ihnen die Verkäufer sagen, lassen Sie trotzdem das Journal für eine Weile laufen, um sicherzustellen, dass alles sauber funktioniert.

9.4.4
Seite 4

Bevor wir uns der Einrichtung und Anhängens des Journals widmen, lassen Sie uns die Art der Einträge, anschauen, nach denen Sie im Journal schauen müssen. Die beste Quelle dafür ist die Tabelle des IBM Sicherheits-Referenz-Handbuch – nachstehend in vereinachter Form:

Szenarienbeschreibung	30	40	50
Ein Programm versucht über nicht unterstützte Schnittstellen auf ein Objekt zuzugreifen.	Journal-eintrag AF[1]	Journal-eintrag AF[1] Operation schlägt fehl.	Journal-eintrag AF[1] Operation schlägt fehl.
Ein Programm versucht eine eingeschränkte Anweisung auszuführen.	Journal-eintrag AF[1]	Journal-eintrag AF[1] Operation schlägt fehl.	Journal-eintrag AF[1] Operation schlägt fehl.
Der Anwender, der einen Job übergibt, hat keine *USE-Berechtigung auf das Benutzerprofil, das in der Jobbeschreibung angegeben ist.	Journal-eintrag AF[1]	Journal-eintrag AF[1] Job läuft nicht.	Journal-eintrag AF[1] Job läuft nicht.
Ein Anwender versucht eine Standardanmeldung ohne Benutzer-ID und Kennwort.	Journal-eintrag AF[1]	Journal-eintrag AF[1] Anmeldung ist erfolglos.	Journal-eintrag AF[1] Anmeldung ist erfolglos.
Ein *USER State-Programm versucht auf den Systembereich der Platte zu schreiben, die als schreibgeschützt oder nicht berechtigt definiert ist.	Versuch könnte Erfolg haben.	Journal-eintrag AF[1,2] Operation schlägt fehl[2].	Journal-eintrag AF[1,2] Operation schlägt fehl[2].
Es wird versucht ein Programm, das keinen gültigen Validierungswert hat zurückzuspeichern[3].	Keine Validierung wird ausgeführt. Programm muss vor Verwendung neu umgesetzt werden.	Keine Validierung wird ausgeführt. Programm muss vor Verwendung neu umgesetzt werden.	Keine Validierung wird ausgeführt. Programm muss vor Verwendung neu umgesetzt werden.
Es wird versucht, ein Programm das einen Validierungswert hat, zurückzuspeichern.	Programm – Validation wird durchgeführt.	Programm – Validation wird durchgeführt.	Programm – Validation wird durchgeführt.
Es wird versucht, den Speicher, der dem Programm gewiesenen wurde, zu ändern.	Versuch ist erfolgreich.	Journal-eintrag AF[1,2] Operation schlägt fehl[2].	Journal-eintrag AF[1,2] Operation schlägt fehl[2].

Szenarienbeschreibung	30	40	50
Es wird versucht, den Adressraum eines Jobs zu ändern	Versuch ist erfolgreich.	Journal-eintrag AF[1,2] Operation schlägt fehl[2].	Journal-eintrag AF[1,2] Operation schlägt fehl[2].
Ein User State-Programm versucht ein System-Domain Programm aufzurufen oder die Steuerung zu übertragen.	Versuch ist erfolgreich	Journal-eintrag AF[1,2] Operation schlägt fehl[2].	Journal-eintrag AF[1,2] Operation schlägt fehl[2].
Es wird versucht, ein User Domain Objekt vom Typ *USRSPC, *USRIDX oder *USRQ in einer Bibliothek aus dem Systemwert QALWUSRDMN zu erstellen.	Operation schlägt fehl.	Operation schlägt fehl.	Operation schlägt fehl.
Ein User State-Programm sendet eine Abbruchnachricht an ein System State-Programm, das nicht direkt darüber im Programmstapel ist.	Versuch ist erfolgreich.	Versuch ist erfolgreich.	Operation schlägt fehl.
Ein Parameter wird an ein User Domain-Programm, das im System-State läuft, übergeben.	Versuch ist erfolgreich.	Parameter-prüfung wird durchgeführt.	Parameter-prüfung wird durchgeführt.
Ein von IBM gelieferter Befehl wird über CHGCMD geändert, um ein anderes Programm aufzurufen. Der Befehl wird wieder zurück zum IBM-Programm geändert. Ein Anwender versucht den Befehl aufzurufen.	Versuch ist erfolgreich.	Journal-eintrag AF[1,2,4] Operation schlägt fehl[2,4].	Journal-eintrag AF[1,2,4] Operation schlägt fehl[2,4].

Ein Berechtigungsfehler (AF) wird in das Auditjournal geschrieben,

1 wenn die Auditierung aktiv ist.

2 wenn der Prozessor den erweiterten Hardware-Speicherschutz unterstützt.

3 wenn die Programme, die vor V1R1 erstellt wurden, keinen Validierungswert haben.

4 wenn Sie einen von IBM gelieferten Befehl ändern. Dann kann er nicht länger als System Domain Programm aufgerufen werden.

Wenn Sie die Auditierungs-Funktion in einer unteren Sicherheitsstufe – wie z.B. 30 – verwenden, meldet das System Journaleinträge für die meisten Aktionen, die in der obigen Tabelle dargestellt sind. Sie erhalten Warnungen in Form von Journaleinträgen für potenzielle Integritätsverletzungen. Wie Sie in der Tabelle sehen können, verursachen Integritätsverletzungen auf Sicherheitsstufe 40 und höher Fehlermeldungen – die ausgeführte Operation schlägt fehl.

Die andere Sache, die die Sicherheitsstufe 40 abfängt, ist die Verwendung von nicht unterstützten Schnittstellen. Bei Sicherheitsstufe 40 und höher, verhindert das System Versuche, System-Programme aufzurufen, die nicht als Call-Level-Interface dokumentiert sind. Zum Beispiel funktioniert ein direkter Aufruf des Befehlsverarbeitungsprogramms für den SIGNOFF-Befehl nicht. Das System nutzt seine eigenen Tricks, um hier einzugreifen. Ohne es detailliert erklären zu wollen, wird das Domain Attribut eines Objekts und das State-Attribut eines Programms geprüft, um diesen Schutz zu erzwingen. Jedes Objekt gehört entweder zur *SYSTEM Domäne oder zur *USER Domäne. Auf *SYSTEM Domänen-Objekte kann nur von *SYSTEM State-Programmen oder Programmen, die den *System State erben, in einem unterstützten Mode (*INHERIT) zugegriffen werden. Die Programme sind entweder als *SYSTEM State, *INHERIT State oder *USER State eingestuft. Die *USER State-Programme können direkt nur auf *USER Domain-Objekte zugreifen. Sollten *USER State-Programme direkt *SYSTEM Domain-Objekte verwenden, dann endet das in einem Fehler, wie in obiger Tabelle angegeben.

Eine Domänen – oder State-Verletzung bewirkt, dass die Operation an der Sicherheitsprüfung der Stufe 40 und höher fehlschlägt. Bei allen Sicherheitsstufen wird ein Eintrag vom Typ AF in das Auditjournal geschrieben, wenn die Auditierungs-Funktion aktiv ist. Wenn aber eine Domänen – oder State-Verletzung auftritt, die Auditierungs-Funktion aktiviert ist und der Systemwert QAUDLVL *PGMFAIL enthalten ist, dann wird ein Eintrag vom Typ D oder R in das Auditjournal geschrieben, sobald versucht wird, ein nicht unterstütztes Interface zu verwenden.

Bei Sicherheitsstufe 40 und höher, muss ein Benutzer, um einen Job zu übergeben, die *USE-Berechtigung haben – sowohl für die Jobbeschreibung als auch für das Benutzerprofil, das in der Jobbeschreibung angegeben ist. Andernfalls schlägt die Übergabe fehl. Bei Sicherheitsstufe 30 läuft der Job, sobald der Benutzer, der den Job übergibt, die *USE-Berechtigung nur auf der Jobbeschreibung hat. Wenn die Audit-Funktion aktiviert ist und der Systemwert QAUDLVL *AUTFAIL enthält, wird ein AF-Eintrag mit Subtyp J in das Auditjournal geschrieben.

Jeder, der sich ohne Benutzer-ID und Kennwort bei Sicherheitsstufe 30 durch das Drücken der Enter-Taste über bestimmte Subsysteme anmeldet, erhält Zugriff auf das System. Bei Sicherheitsstufe 40 und höher stoppt das System den Versuch, sich so anzumelden. Wenn Audit aktiv ist und der Systemwert QAUDLVL *AUTFAIL enthält, wird ein AF-Eintrag, Subtyp S im Auditjournal aufgezeichnet.

Dann gibt es noch die Enhanced Hardware Storage Protection. Diese Hardware-Einrichtung ermöglicht es, Blöcke von System-Informationen auf der Festplatte als read-write, read-only oder ohne Zugriff zu definieren. Bei Sicherheitsstufe 40 und höher steuert das System, wie die *USER State-Programme auf diese geschützten Blöcke zugreifen. Diese Unterstützung ist auf Systemen mit Sicherheitsstufen kleiner als 40 nicht verfügbar. Diese Fähigkeit ist bei den meisten, aktuellen Power i Systemen verfügbar. Wenn die Auditierung aktiviert wird und der Systemwert QAUDLVL *PGMFAIL enthält, wird ein AF-Eintrag, Subtype R in das Auditjournal geschrieben, sollten solche Verletzungen auftreten.

Während der Auditierung auf Sicherheitsstufe 30 vor der Migration auf 40 haben Sie die Möglichkeit, Ressourcen-Sicherheit für alle Ihre Anwendungen zu testen. Deshalb beginnen Sie den Audit-Prozess, bevor Sie diesen Schritt machen. Auf diese Weise und durch eine gründliche Analyse der Journaleinträge sind Sie in der Lage herauszubekommen, wann Sie keine Probleme beim Umstieg auf die Sicherheitsstufe 40 haben werden.

Für den QAUDLVL-Systemwert sind – wie oben erwähnt – die beiden kritischen und einzustellenden Werte: *PGMFAIL und *AUTFAIL. *PGMFAIL protokolliert die Journaleinträge für alle Zugriffsversuche, die bei der Sicherheitsstufe die Integrität verletzen. *AUTFAIL erfasst die ungültigen (leeren) Anmeldungen sowie die fehlenden Berechtigungen auf Jobbeschreibungen und Benutzerprofile.

Nachdem Sie die Audit-Umgebung eingerichtet und aktiviert haben, ist Ihre Aufgabe jetzt die Überwachung des Auditjournals auf *AUTFAIL und *PGMFAIL Einträge. Und zwar während des Betriebs all Ihrer Anwendungen, solange Sie noch auf der Sicherheitsstufe 30 sind. Die wichtigsten Subtypen innerhalb der AF-Einträge sind:

– B
  Ein Programm hat eine restriktive Maschineninterface-Anweisung aufgerufen.
– C
  Ein Programm ist bei Objekt-Validierung fehlgeschlagen.
– D
  Programm hat auf ein Objekt über ein nicht unterstütztes Interface zugegriffen.

9.4.4
Seite 8

– J
  Jobbeschreibungs – und Benutzerprofil-Berechtigungsfehler.
– R
  Versuch auf geschützten Bereich der Festplatte zuzugreifen.
– S
  Standard-Anmeldeversuch ohne Benutzer-ID/Kennwort.

Dies sind die Codes, die auf das Vorkommen von Integritätsverletzungen bei den Anwendungen hinweisen, wenn Sie Sicherheitsstufe 40 verwenden.

Noch eines zum Schluss, bevor Sie beginnen, die Objekte zu erstellen, die benötigt werden, um Audit-Journalisierung zu implementieren: Alle Programme, die vor OS/400 Version 1 Release 3 erstellt wurden (und das dürften relativ wenige sein), haben keine Validierungs-Codes. Dies ist kein wirkliches Problem, aber es kann zu einem Problem mit Sicherheitsstufe 40 werden, wenn Sie diese Objekte zurückspeichern. Die einfachste Möglichkeit, dem zu entgegnen, ist ein CHGPGM auf jedes dieser Programme anzuwenden und den FRCCRT-Parameter zur Erstellung der Validierungs-Codes für diese Programme einzusetzen.

Mit der Sicherheitsstufe 40, die auf Ihren Einstellungen der drei System-Werte basiert – Objekt beim Zurückspeichern prüfen (QVFYOBJRST), Umsetzung beim Zurückspeichern erzwingen (QFRCCVNRST) und Objektrückspeicherung zulassen (QALWOBJRST) – wird das System die Aktion, die Sie anfordern, verwenden. Bei der Wiederherstellung arbeiten diese Werte als eine Reihe von Filtern, um festzustellen, ob ein Programm ohne Änderung wiederhergestellt, ob es neu erstellt (konvertiert), wie es wiederhergestellt oder ob es überhaupt nicht wiederhergestellt wird.

Nachdem Sie alle diese Fragen gelöst haben, stellen Sie auf Sicherheitsstufe 40 um.

9.5 Erstellen des Auditjournals und Starten der Auditierung

Um die Auditierung einschalten zu können, benötigen Sie die Sonderberechtigung *AUDIT in Ihrem Benutzerprofil. Um diese Sonderberechtigung zu bekommen, können Sie Ihr Benutzerprofil am Besten unter Verwendung des QSECOFR-Profils ändern.

Es könnte sein, dass die Auditierung auf Ihrem System bereits von einem anderen Anwender aktiviert wurde. Schauen Sie deshalb zum einen erst mal nach, ob ein Audit bereits aktiv ist – und zum anderen, ob Auditjournal und Journalempfänger existieren. Dann erstellen Sie – falls noch nicht vorhanden – die Journalreceiver in einer Bibliothek Ihrer Wahl, indem Sie den Befehl „Journalreceiver erstellen“ (CRTJRNRCV) ausführen. In diesem Beispiel wird eine Bibliothek namens AUDITLIB für Journalempfänger verwendet.

1. Prüfen Sie, welche Journale und Journalempfänger auf Ihrem System vorhanden sind:

```
WRKOBJ OBJ (* ALL / * ALL) OBJTYPE (* JRN)
WRKOBJ OBJ (* ALL / * ALL) OBJTYPE (* JRNRCV)
```

   Wenn Sie in Ihrem Unternehmen Datenbank-Journalisierung verwenden, dann werden Sie überrascht sein, wie viele Journale und Journalempfänger es auf Ihrem System gibt.

   Wenn Sie noch gar nicht Journalisieren, lassen Sie sich nicht von den vielen Standard-Datenbankjournalen abschrecken, die das System für sich braucht.

   Das Auditjournal gibt es nur einmal im System mit dem Namen QAUDJRN. Darüber hinaus muss das QAUDJRN-Journal in der Bibliothek QSYS stehen. Da ein Journal eine zentrale Filter – und Kontrollfunktion für die Aufzeichnung von Journaleinträgen ist, kann und soll QAUDJRN in der Bibliothek QSYS belassen werden.

2. Wenn Ihnen die Liste der Journale und Journalempfänger zu umfangreich zum Durchsuchen ist, dann können den Befehl WRKJRN verwenden, um den Status des Auditjournals zu sehen. Beispielsweise können Sie damit auch sehen, wie viele Empfänger erstellt wurden.

```
WRKJRN QAUDJRN
```

Wenn in Ihrer Firma bereits jemand das Auditjournal implementiert hat, dann können Sie in den meisten Fällen entweder:

– die Audit-Journalisierung durch das Setzen des Systemwerts QAUDCTL auf *NONE ausschalten,

– die gefundenen Journalreceiver löschen,

– mit Punkt 3. fortfahren.

oder

– die Systemwerte QAUDLVL und QAUDLVL2 prüfen und sicherstellen, dass die Werte *PGMFAIL und *AUTFAIL angegeben wurden.

– Sollten diese Optionen nicht enthalten sein, fügen Sie sie hinzu.

– Sollten diese Werte existieren und die Einstellungen in Ordnung sein, dann fahren Sie mit Schritt 6 fort.

3. Erstellen Sie eine Bibliothek für die Audit-Journalisierung.

```
CRTLIB LIB (AUDITLIB) TEXT ('Bibliothek für
Auditjournal Receiver) AUT (* EXCLUDE)
```

4. Erstellen Sie die Journalempfänger für die Auditierung. Dieser wird später an das Journal angehängt.

```
CRTJRNRCV JRNRCV (AUDITLIB/AUDRCV0001) TEXT ('Journal Receiver
für Auditjournalisierung") AUT (* EXCLUDE)
```

Da hier eine neue Bibliothek erstellt wird, stellen Sie sicher, dass die Bibliothek AUDITLIB und ihre Journalempfänger in die Backup-Routinen mit aufgenommen werden, so dass die Audit-Daten regelmäßig gesichert werden. Sollten Sie die Backup-Routinen nicht ändern können, stellen Sie die Audit-Journalempfänger in eine Bibliothek, die standardmäßig mit gesichert wird – z.B. QGPL (obwohl das nicht empfehlenswert ist). Stellen Sie die Journalempfänger nicht in die Bibliothek QSYS.

Wählen Sie einen Journalempfängernamen, mit dem eine Namenskonvention für zukünftige Journalempfänger – wie AUDRCV0001 – erstellt werden kann. Sie können die *GEN Option verwenden, wenn Sie die Journalempfänger ändern und die Namenskonvention fortsetzen. Diese Art der Namensgebung ermöglicht es Ihnen, das System verwalten zu lassen, wenn Ihre Journalempfänger voll sind.

Geben Sie einen Schwellwert für die Größe des Empfängers im Treshold-Parameter ein. Die Größe, die Sie wählen, sollte auf die Anzahl der Transaktionen auf Ihrem System und die Anzahl der Aktionen, die Sie auswählen, angepasst sein. Wenn Sie die automatische Journalreceiver-Verwaltung

– wie empfohlen – verwenden, muss die Journalreceiver-Schwelle mindestens 100.000 KB sein. Die Standardgröße, wie wir sie oben gewählt haben (durch Weglassen eines speziellen Wertes), ist als Schwellwert standardmäßig 1.500.000 KB. Geben Sie im Parameter AUT *EXCLUDE für die Einschränkung des Zugriffs auf die Informationen im Journal ein.

5. Erstellen Sie das QSYS-/ QAUDJRN-Journal mit dem Befehl „Create Journal“ (CRTJRN).

```
CRTJRN JRN (QSYS / QAUDJRN) JRNRCV (JRNLIB/AUDRCV0001)
MNGRCV (* SYSTEM) DLTRCV (* NO) AUT (* EXCLUDE)
TEXT ('Audit – Journal ")
```

Obwohl die Audit-Journalisierung eine Systemfunktion ist, wird das QAUDJRN-Journal nicht von IBM zur Verfügung gestellt. Sie müssen es selbst erstellen. Die Regeln für die Erstellung des Auditjournals lauten wie folgt:

– Der Name QSYS / QAUDJRN muss verwendet werden.

– Geben Sie den Namen des Journalempfängers, den Sie vorher erstellt haben, an.

– Geben Sie *EXCLUDE im AUT-Parameter an, um den Zugang auf die Informationen im Journal einzuschränken. Sie müssen die Berechtigung haben, um Objekte in die Bibliothek QSYS hinzuzufügen und um das Journal zu erstellen.

– Verwenden Sie den Parameter MNGRCV, damit das System die Journalempfänger ändern und neue hinzufügen kann – aber nur dann, wenn die angehängten Empfänger die Schwellwertgröße überschreiten. Wenn Sie diese Option wählen, müssen Sie den CHGJRN-Befehl nicht verwenden, um die Empfänger zu zu erstellen und neue manuell anzuhängen.

– Lassen Sie das System keine abgehängten Receiver löschen. Geben Sie DLTRCV (*NO) an, was auch die Standardeinstellung ist. Die QAUDJRN-Empfänger sind die Security Audit-Protokolle. Stellen Sie sicher, dass die entsprechend gesichert sind, bevor Sie sie löschen.

Einstellen der zusätzlichen Optionen für Auditjournal.

6. Stellen Sie die Audit-Ebene im (QAUDLVL) Systemwert ein. Zunächst werden Sie den Systemwert QAUDLVL2 nicht brauchen. Der ist nur erforderlich wenn der Systemwert QAUDLVL keinen Platz für weitere Einträge hat. Zum Verwalten der Prüfungen in den Systemwerten QAUDLVL und QAUDLVL2 verwenden Sie den Befehl WRKSYSVAL.

Beginnen Sie mit folgender Eingabe:

```
WRKSYSVAL QAUD*
```

Drücken Sie die Eingabetaste. Sie sehen die verfügbaren Systemwerte im Audit-Bereich:

```
                          Mit Systemwerten arbeiten
                                                                System:   PWI
Listenanfang bei . . . .   __________   Anfangszeichen des Systemwerts
Teilauflistung nach Art    _______      F4=Liste

Auswahl eingeben und Eingabetaste drücken.
  2=Ändern   5=Anzeigen

Auswahl  Systemwert  Art      Beschreibung
   _      QAUDCTL     *SEC     Protokollierungssteuerung
   _      QAUDENDACN  *SEC     Aktion bei Protokollierungsende
   _      QAUDFRCLVL  *SEC     Protokollierungsdaten erzwingen
   _      QAUDLVL     *SEC     Sicherheitsprotokollebene
   _      QAUDLVL2    *SEC     Erweiterung der Sicherheitsprotokollierung
```

Audit-Systemwerte

Merken Sie sich die Existenz des Systemwertes QAUDLVL2. Dieser kann später eine Rolle spielen, nachdem Sie bereits zur Sicherheitsstufe 40 migriert sind und viele andere Security Auditierungs-Funktionen aktiviert haben. Nun rufen Sie mit der Auswahl 2 den Systemwert QAUDLVL zum Ändern auf. Stellen Sie sicher, dass das Auditjournal auf Ihrem System noch nicht aktiv ist (das sollte in Schritt 1 und 2 passiert sein). Ergänzen Sie die Auditierungsparameter:

```
*AUTFAIL
*PGMFAIL
```

Sobald Sie durch die Analyse des Auditjournals festgestellt haben, dass Ihr System auf Sicherheitsstufe 40 umgestellt werden kann, können Sie im QAUDLVL-Systemwert weitere nützliche Optionen aktivieren. Während Sie mit dem Systemwert arbeiten, verwenden Sie die F1-Hilfetaste und lassen sich die Optionen und deren Erklärungen anzeigen. Wenn sie mal Experte auf dem Gebiet sind und mehr Funktionen aktivieren können, als im QAUDLVL-Systemwert Platz haben, dann setzen Sie die Liste im Systemwert QAUDLVL2 fort.

7. Sobald Sie die QAUDLVL-Werte festgelegt haben, ist es an der Zeit die Auditierung einzuschalten. Dies erfolgt über den Systemwert QAUDCTL. Sie starten das Auditjournal indem Sie den QAUDCTL Systemwert auf einen anderen Wert als *NONE einstellen – nämlich:

```
* AUDLVL und
* NOQTEMP
```

Stellen Sie sicher, dass die zwei Optionen eingegeben wurden. Das ist alles, was nötig ist, um den Test für die Sicherheit der Sicherheitsstufe 40 oder 50 durchzuführen.

Bitte beachten Sie, dass das QSYS/QAUDJRN-Journal existieren muss, bevor Sie den Systemwert QAUTCTL auf einen anderen Wert als *NONE einstellen. Wenn die Auditierung startet, versucht das System einen Datensatz in das Auditjournal zu schreiben. Wenn das nicht erfolgreich ist, erhalten Sie eine Fehlermeldung und die Auditierung startet nicht. Ebenso müssen Journal und Journalreceiver passend eingestellt sein.

Sobald Sie die Journalisierung eingeschaltet haben, lassen Sie das System eine Weile laufen – zumindest so lange, bis die üblichen Geschäftsvorfälle abgearbeitet sind.

Andere Befehle und Optionen bei der Auditierung
Wenn Sie bereit sind, ein umfangreiches Audit mitzumachen, können Sie die folgenden Befehle verwenden, um weitere hilfreiche Aufzeichnungen für Aktivitäten zu starten:

```
CHGUSRAUD
```

Dieser Befehl startet die Auditierung für individuelle Anwender.

```
CHGOBJAUD
CHGDLOAUD
```

Diese beiden Befehle schalten die Objektauditierung für bestimmte Objekte ein. Der CHGUSRAUD-Befehl kann wiederum verwendet werden, um bestimmte Objekte bei bestimmten Anwendern zu auditieren.

Stellen Sie sicher, dass der Systemwert QAUDENDACN auf *NOTIFY anstelle auf *PWRDWNSYS eingestellt ist. *PWRDWNSYS schaltet Ihr System ab, wenn die Auditierung keine Journaldaten wegschreiben kann. *NOTIFY sendet in diesem Fall eine Nachricht an den QSYSOPR (Systemoperator). *NOTIFY ist die Standardoption für diesen Systemwert.

Mit dem Systemwert QAUDFRCLVL können Sie steuern, wie oft Audit-Journaleinträge aus dem Speicher auf die Platte weggeschrieben werden. Mit der Standardeinstellung *SYS wird das vom System aus gesteuert. Die Journaleinträge werden nur dann auf die Platte geschrieben, wenn das System feststellt, dass dies abhängig von der internen Systemverarbeitung erforderlich ist. Diese Angabe liefert zwar die besten Protokollierungsergebnisse, kann aber auch zum höchsten Datenverlust bei einem abnormalen Ende des Systems führen.

Sie können auch einen Wert von 1 bis 100 angeben. Der Wert gibt die Anzahl der ins Sicherheitsprotokoll-Journal geschriebenen Journaleinträge an, bevor die Protokollierungsdaten auf die Platte geschrieben werden. Je kleiner diese Anzahl angegeben wird, umso höher sind die Auswirkungen auf die Systemleistung. Aber die Wahrscheinlichkeit der Erfassung des letzten Fehler auf der Festplatte im Falle eines Crashs steigt.

Prüfung des Journals
Sobald Sie die Journalisierung eingeschaltet haben, können Sie die Inhalte anschauen.

Die beste Möglichkeit, die Audit-Daten zu analysieren, besteht darin ein für diese Zwecke spezialisiertes Programm zu erwerben. Diese Programme lesen die Audit-Journale aus und übertragen sie – je nach Audittyp – in lesbare Protokolleinträge. Das ist wesentlich einfacher und effektiver, als für jeden Audittyp ein Programm zu schreiben, dass die unterschiedlichen Audittypen aus den Journalen ausliest und dass für jeden Audityp mit Rücksicht auf die interne Struktur des jeweiligen Typs die Daten aufbereitet.

Die Verwendung des Befehls DSPAUDJRNE zur Anzeige der Auditjournal-Einträge ist eine rudimentäre Möglichkeit, die Daten anzuzeigen. Die Berichte aus diesem Befehl geben Auskunft über die Eintragstypen und die Benutzerprofile, welche die Ereignisse ausgelöst haben. Sie können die Berichte auf bestimmte Zeiträume einschränken und einzelne Journalempfänger durchsuchen. Eine Ausgabe auf den Bildschirm ist ebenso möglich wie die Ausgabe in eine Spooldatei. Für den Befehl DSPAUDJRNE müssen Sie über die Sonderberechtigungen *ALLOBJ und *AUDIT verfügen.

Um einen Bericht über alle Berechtigungsfehler für alle Benutzerprofile zu erzeugen, verwenden Sie den Befehl:

```
DSPAUDJRNE ENTTYP (AF) USRPRF (* ALL) OUTPUT (*)
```

Natürlich können Sie den Ausgabe-Parameter auf *PRINT ändern, um einen Bericht zu erzeugen. Dabei können im besten Fall einige Zeilen, im schlechtesten Fall viele Seiten ausgegeben werden:

	Verletzungs-art		Benutzer-profil	Objekt-name	Bibliotheks-name	Objekt-art
000001	AF	A	QUSER	*N	*N	*DIR
000002	AF	A	QUSER	*N	*N	*DIR
000003	AF	A	QUSER	*N	*N	*DIR
000004	AF	A	QUSER	*N	*N	*DIR
000005	AF	A	QUSER	*N	*N	*DIR
000006	AF	A	QUSER	*N	*N	*DIR
000007	AF	A	QUSER	*N	*N	*DIR
000008	AF	A	QUSER	*N	*N	*DIR
000009	AF	A	QUSER	*N	*N	*DIR
000010	AF	A	QUSER	*N	*N	*DIR

DSPAUDJRNE-Ausgabe am Bildschirm

Beachten Sie die AF-Einträge und das A neben dem Eintrag. Der Typ „A“ ist harmlos. Die wichtigeren AF-Einträge sind die mit B, C, D, J, R und S. Diese wurden weiter vorne im Text beschrieben. Wenn Sie den Audit-Wert *NOQTEMP verwenden, werden die Vorgänge in QTEMP nicht auditiert. Diese QTEMP-Bibliotheken sind die temporären Bibliotheken je User und brauchen hier auch nicht berücksichtigt werden.

Denken Sie daran, Ihr Ziel ist es, keine der o. g. fehlerhaften Einträge mehr zu finden. Sobald Sie das erreicht haben und die zugrunde liegenden Probleme gelöst wurden, können Sie über den Befehl

```
WRKSYSVAL QSECURITY
```

den Wert der Sicherheitsstufe 40 einstellen. Sollten trotzdem nach der Umstellung Probleme auftreten, können Sie jederzeit wieder zurück zur Sicherheitsstufe 30 wechseln.

9.5
Seite 8

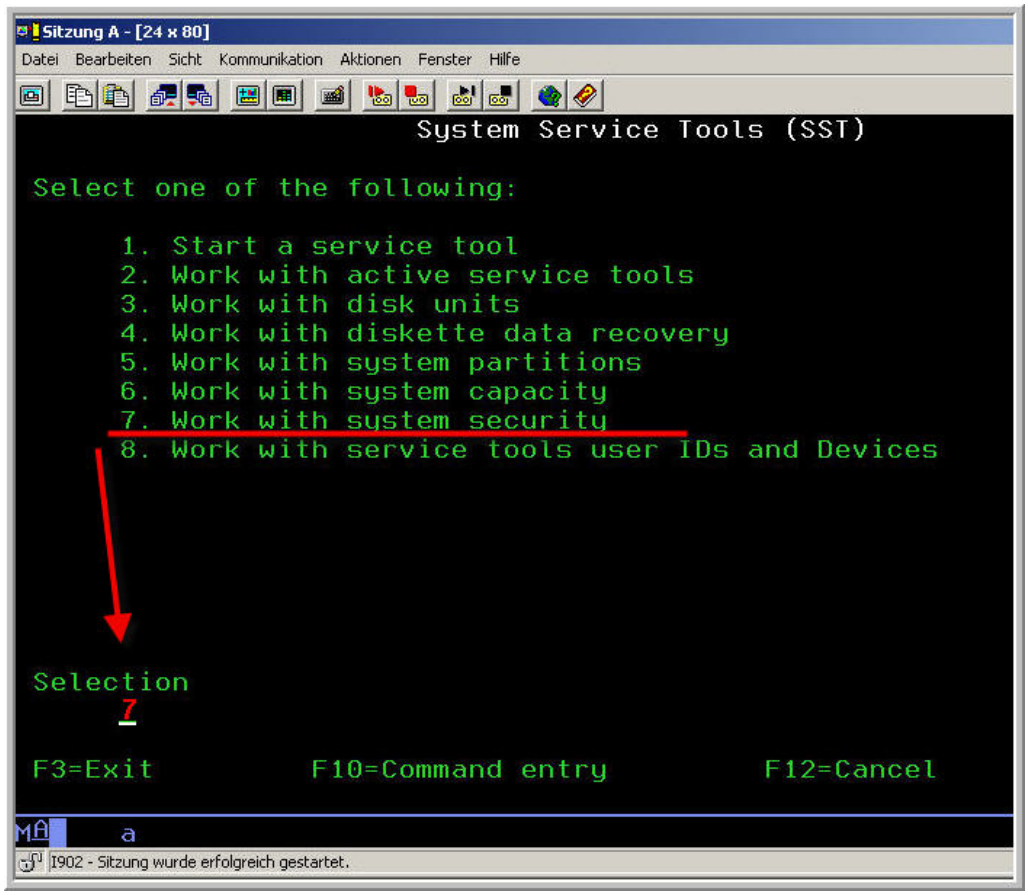
9.6 Systemwerte

Systemwerte sind globale Parameter, die für das gesamte System geltende Vorgaben enthalten.

Aber Vorsicht! Systemwerte beeinflussen das gesamte System. Die eingestellten Systemwerte können Sie mit i5/OS-Befehlen oder mit dem iSeries Navigator abfragen und/oder verändern. Ein Benutzer kann Systemwerte ändern, um z. B die Arbeitsumgebung zu definieren oder Sie können beispielsweise als Systemwert für das Datumsformat JJ/MM/TT, MM/TT/JJ, TT/MM/JJ oder julianisch angegeben werden. Auch die Bibliotheksliste ist ein Beispiel für die Verwendung von Systemwerten. Wann eine Systemwertänderung wirksam wird, ist vom jeweiligen Systemwert abhängig. Nicht alle Systemwertänderungen werden sofort nach ihrer Änderung vom System übernommen. Bei einigen Werten, wie etwa der Sicherheitsstufe QSECURITY wird die Änderung erst beim nächsten IPL des Servers wirksam. Informationen darüber, wann ein bestimmter Systemwert wirksam wird, finden Sie im entsprechenden Hilfetext für den Systemwert. Natürlich stellt sich auch die Frage „Wer darf Systemwerte ändern?“. Und auch darauf lässt sich keine eindeutige Antwort geben. Die Sonderberechtigungen im jeweiligen Benutzerprofil legen fest, ob ein Benutzer den entsprechenden Systemwert ändern darf. Welche Sonderberechtigungen für einen bestimmten Systemwert erforderlich sind, müssen Sie wiederum dem Hilfetext für den entsprechenden Systemwert entnehmen. Sie können zusätzlich über die Systemservice-Tools (SST) sicherheitsrelevante Systemwerte für Änderungen freigeben oder sperren. Hierzu öffnen Sie zunächst eine 5250-Emulation und geben den Befehl STRSST (start system servicetool) ein. Daraufhin öffnet sich ein Dialog für die Eingabe Ihres Benutzernamens und Kennwortes. Anschließend gelangen Sie in den folgenden Dialog:

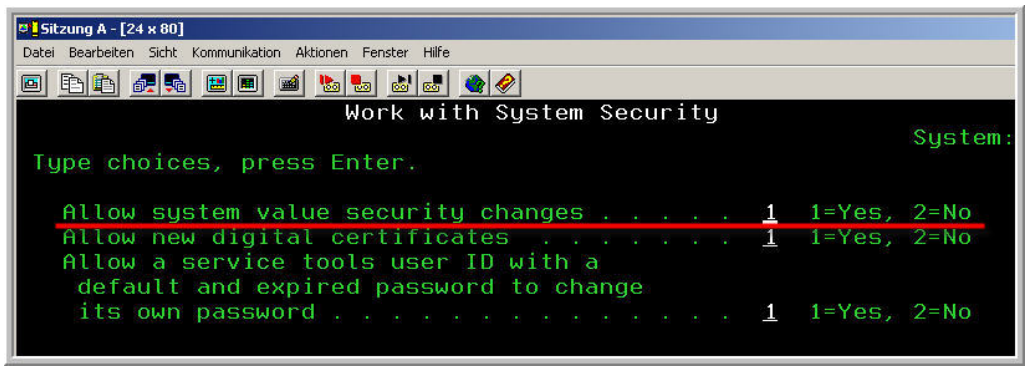
16. Ergänzung 9/2008

9.6
Seite 2



System Service Tools

Wenn Sie jetzt die Option 7 „Arbeiten mit Systemsicherheit“ wählen, erscheint ein weiterer Bildschirm.



Work with System Security

Hier können Sie im Feld „Ändern sicherheitsbezogener Systemwerte zulassen“ entweder den Wert 1 = Ja angeben, um die sicherheitsbezogenen Systemwerte zu entsperren, oder eine 2 = Nein eintragen, um die sicherheitsbezogenen Systemwerte zu sperren. Die Default-Einstellung erlaubt im Übrigen die Veränderung systemrelevanter Systemwerte. Falls Sie die Defaulteinstellung verändern und es wird anschließend versucht einen der sicherheitsrelevanten Systemwerte zu ändern, wird die Änderung zurückgewiesen und der Benutzer erhält die Nachricht „CPF18C0“. Sicherheitsrelevante Systemwerte sind in diesem Zusammenhang die folgenden Systemwerte:

Sicherheitsrelevante Systemwerte

Jedes Mal wenn Sie einen Systemwert ändern, sollten Sie anschließend die neuen Systemwerteinstellungen sichern, damit Ihnen keine Systemwertdaten verloren gehen, falls Ihre Systemwerte beschädigt werden. Systemwerte werden in der Systembibliothek QSYS gespeichert. Sie müssen also die Bibliothek QSYS sichern, um die aktuellen Systemwerteinstellungen zu sichern. Es ist egal, ob Sie eine Systemsicherung durchführen oder nur die Systemdaten sichern. Auch der Befehl SAVSYSINF (save systeminformation) ist zur Sicherung der Systemwerteinstellungen ausreichend. Falls Sie mit BRMS arbeiten, verwenden Sie die Sicherungsrichtlinie *SYSTEM oder *SYSGRP.

16. Ergänzung 9/2008

9.6
Seite 4

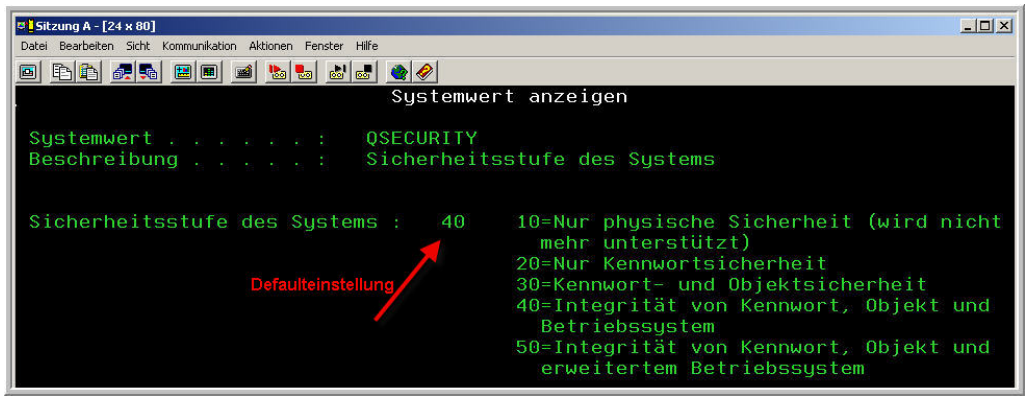
9.6.1 Systemwerteinstellungen mit i5/OS-Befehlen bearbeiten

Sie können jederzeit mit dem i5/OS-Befehl DSPSYSVAL (display system value) aktuelle Systemwerteinstellungen abfragen und – falls Sie die nötigen Berechtigungen besitzen – die Werte mit dem Befehl CHGSYSVAL (change system value) ändern. Außerdem bietet sich der Befehl WRKSYSVAL (work with system values) an, um mit Systemwerten zu arbeiten. Geben Sie auf einer Kommandozeile den Befehl WRKSYSVAL QPRTDEV ein. Daraufhin sollte der folgende Bildschirm erscheinen:

Der Befehl WRKSYSVAL QPRTDEV

Mit der Option „5 = Anzeigen“ können Sie jetzt den Standarddrucker Ihres Systems ermitteln.

Schauen wir uns auch noch den Systemwert QSECURITY etwas genauer an:



Ausgabe des Befehls DSPSYSVAL QSECURITY

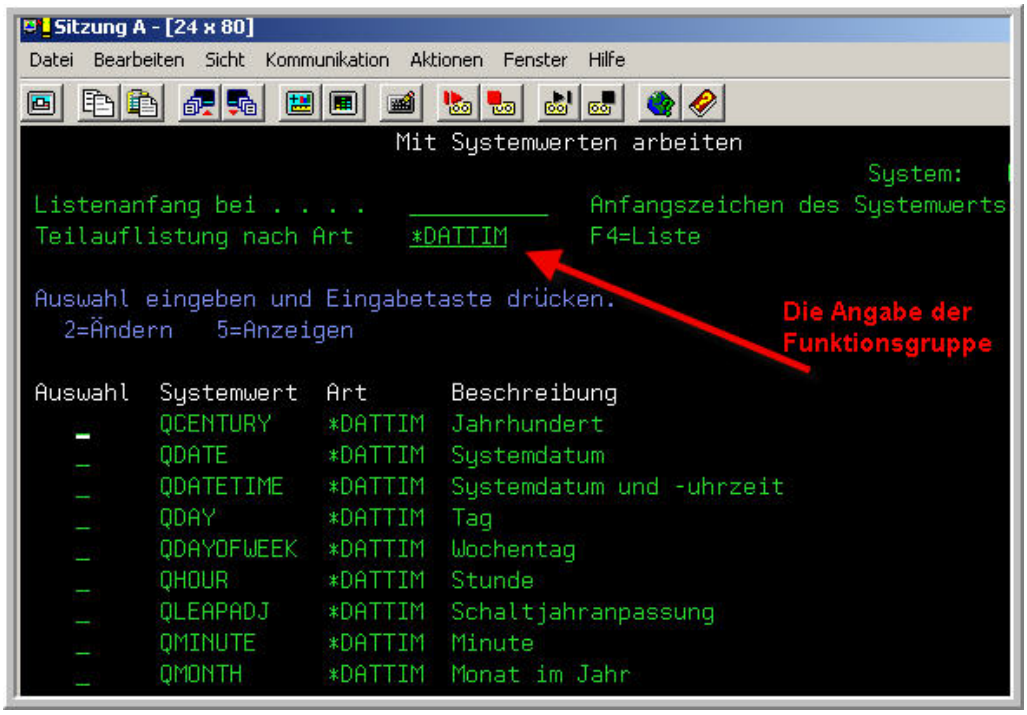
Der Systemwert QSECURITY legt die grundlegenden Sicherheitseinstellungen Ihres Servers fest. Vor dem Release V3R7 lieferte die IBM die Systeme in der Sicherheitsstufe 10 aus, um die Installation zu erleichtern. Die Sicherheitsstufe 10 wird allerdings seit dem Release V4R3 nicht mehr unterstützt. Alle Kunden mussten bei der Installation des Release V4R3 automatisch auf die Sicherheitsstufe 20 umstellen. Heute werden die Systeme in der Sicherheitsstufe 40 ausgeliefert.

9.6.1
Seite 2

Es gibt derzeit über 150 verschiedene Systemwerte, die in Funktionsgruppen zusammengefasst sind. Die Anzeige „Art des Systemwerts auswählen“ enthält diese Funktionsgruppen. Die Anzeige rufen Sie durch Drücken der Funktionstaste F4 auf, wenn der Positionsanzeiger im Feld „Teilauflistung nach Art...“ in der Anzeige „Mit Systemwerten arbeiten“ steht.

Die Systemwertarten – 5250-Ausgabe

Wenn Sie sich für die Kategorie *ALC entscheiden, enthält die Liste der Systemwerte anschließend nur die Zuordnungssystemwerte. Hierzu gehört der Systemwert QTOTJOB „Anfängliche Anzahl Jobs“ genauso wie der Systemwert QJOBMSGQMX „Maximale Größe der Jobnachrichtenwarteschlange“. *EDT fasst alle Editiersystemwerte zusammen. Die Gruppe *LIBL enthält u.a. die Systemwerte QSYSLIBL und QUSRLIBL. Beide Systemwerte gemeinsam bestimmen den grundlegenden Aufbau der Bibliothekssuchlisten auf Ihrem System. Die Systemwerte der Art *MSG definieren zahlreiche Protokolleinstellungen. Die Kategorie *SEC enthält die Sicherheitssystemwerte. Hier finden Sie auch den Systemwert QSECURITY. Grundlegende Einstellungen des Arbeitsspeichers werden mit Hilfe der Systemwerte der Art *STG vorgenommen und die Gruppe *SYSCTL steht synonym für die Systemsteuerungs-Systemwerte. Sie können die Einzelwerte einer Kategorie anzeigen, indem Sie einfach die entsprechende Systemwertart im Parameter „Teilauflistung nach Art“ eintragen. Ich lasse mir im nachfolgenden Bildschirm alle Systemwerte der Gruppe *DATTIM anzeigen:

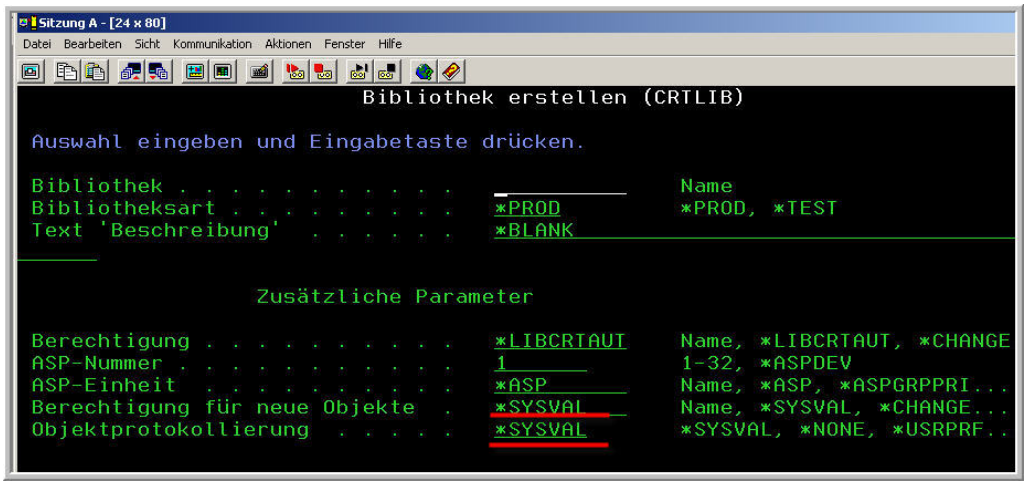


*Die Funktionsgruppe *DATTIM*

In der Funktionsgruppe *DATTIM werden alle relevanten Systemwerte zur Einstellung von Datum und Uhrzeit zusammengefasst.

Jede dieser Funktionsgruppen enthält also eine mehr oder minder große Anzahl Einzelwerte. Ich möchte an dieser Stelle nicht jede Kategorie detailliert erläutern, sondern werde hin und wieder in den entsprechenden Kapiteln auf die jeweils relevanten Systemwerte verweisen. Hinzu kommt, dass die Systemwerte mit fast jedem neuen Release erweitert bzw. einzelne Werte verändert werden. So hat IBM im Release V5R4 z. B. die Kategorie „Jobs“ um zwei neue Systemwerte erweitert. Mit dem ersten Systemwert QALWJOBITP, „Unterbrechen von Jobs zulassen“, können Sie festlegen, ob neue aktive Jobs unterbrochen werden dürfen, um benutzerdefinierte Exit-Programme auszuführen. Mit dem zweiten neuen Systemwert, „Druckausgabe für Jobprotokoll erstellen“ (QLOGOUTPUT), können Sie angeben, ob eine Druckausgabe für ein Jobprotokoll erstellt wird. Außerdem wurde der Systemwert „Aktionsüberwachung aktivieren“ (QAUDCTL) dahingehend geändert, dass Sie jetzt auch die Möglichkeit haben, Abrufereignisse zu überwachen und der Systemwert „Maximale Größe des Jobprotokolls“ (QJOBMSGQMX) erlaubt jetzt die Angabe, 64 MB für die Größe der Jobprotokolldateien zu nutzen. Außerdem wurde der Systemwert „Größe der Systemprotokolldatei“ (QHSTLOGSIZ) in der Kategorie „Nachrichten und Service“ um einen neuen Wert erweitert. Seit dem Release V5R4 kann das System täglich ein neues Systemprotokoll erstellen, anstatt immer nur dann ein neues Protokoll zu erstellen, wenn das aktuelle Protokoll voll ist. Sie sehen es gibt eine Vielzahl verschiedener Systemwerte, die sich zudem auch noch je nach Release unterscheiden können.

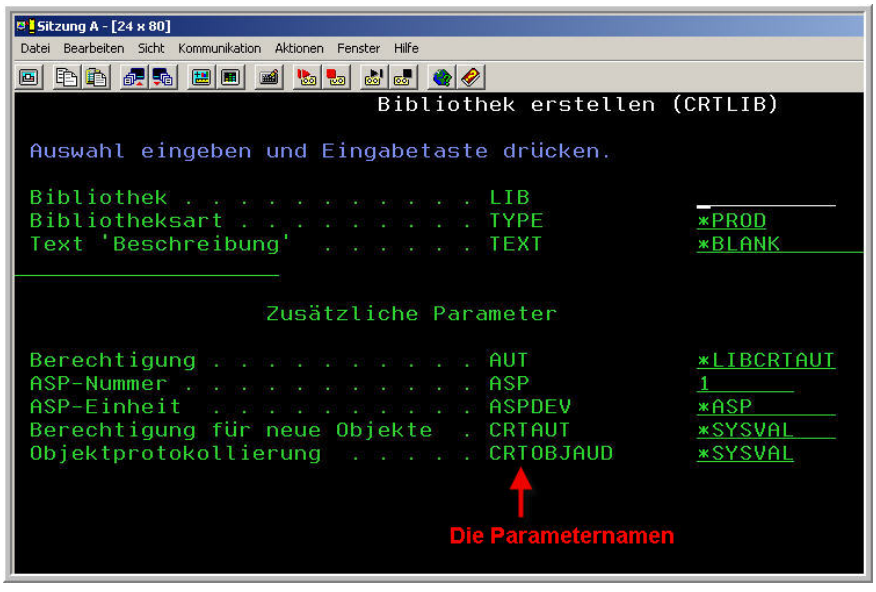
Viel wichtiger erscheint mir daher an dieser Stelle die Frage, wie finden Sie möglichst schnell die entsprechende Systemwerteinstellung, wenn Sie i5/OS-Befehle Systemwerteinstellungen nutzen? Schauen Sie sich dazu die folgende Abbildung an:



Der Befehl CRTLIB

Der Befehl CRTLIB (create libary) verwendet sowohl für die Einstellung der Objektprotokollierung als auch für die Berechtigungssteuerung Systemwerteinstellungen. Es ist naheliegend zu fragen: „Welche Systemwerte werden verwendet?“. Es scheint gar nicht so einfach, die entscheidenden Systemwerte zu finden, oder haben Sie Lust 150 Systemwerte zu durchsuchen? Aber es geht auch einfacher:

Lassen Sie sich zunächst die Parameternamen des Befehls CRTLIB anzeigen. Hierzu drücken Sie die Funktionstaste F11. Daraufhin sollte sich Ihre Bildschirmausgabe verändern:



Anzeige der Parameternamen

Sie können jetzt den Namen des entsprechenden Parameters lesen. Der Parameter CRTAUT steuert die „Berechtigung für neue Objekte“ und CRTOBJAUD bestimmt die Objektprotokollierung. Beide Parameterwerte werden von Systemwerten abgeleitet. Die hierfür verwendeten Systemwerte tragen den Namen des jeweiligen Parameters mit dem vorangestellten Buchstaben Q.

Auswahl	Systemwert	Art	Beschreibung
_	QCRTAUT	*SEC	Allgem. Berechtigung für neue Objekte erstellen
_	QCRTOBJAUD	*SEC	Objektprüfprotokollierung erstellen

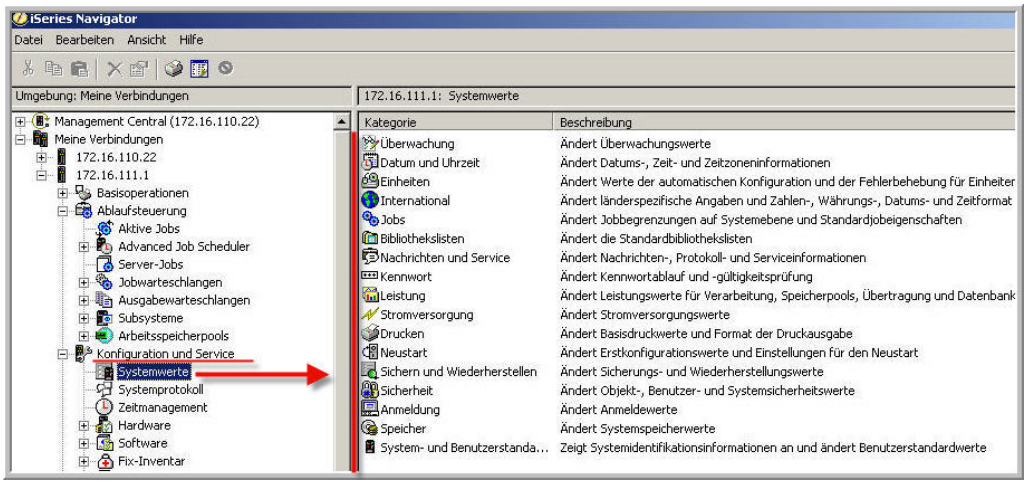
Die zugehörigen Systemwerte

Sie sehen, dass die Einstellung des Systemwertes QCRTOBJAUD festlegt, ob Objekte in der neuen Bibliothek aufgezeichnet werden und dass der Systemwert QCRTAUT die Berechtigung der neuen Objekte in der zu erstellenden Bibliothek bestimmt. Dies ist im Übrigen der Grund, warum die Öffentlichkeit *PUBLIC stets per Default ein CHANGE-Recht an allen Objekten einer Bibliothek erhält. Der Wert *CHANGE ist im Systemwert QCRTAUT hinterlegt!

9.6.1
Seite 6

9.6.2 Systemwerteinstellungen mit iSeries Navigator bearbeiten

Auch der iSeries Navigator bietet die Möglichkeit, mit Systemwerten zu arbeiten. Systemwerteinstellungen finden Sie im iSeries Navigator in der Rubrik „Konfiguration und Service“. Wenn Sie diese Rubrik öffnen, erhalten Sie die folgende Bildschirmausgabe:



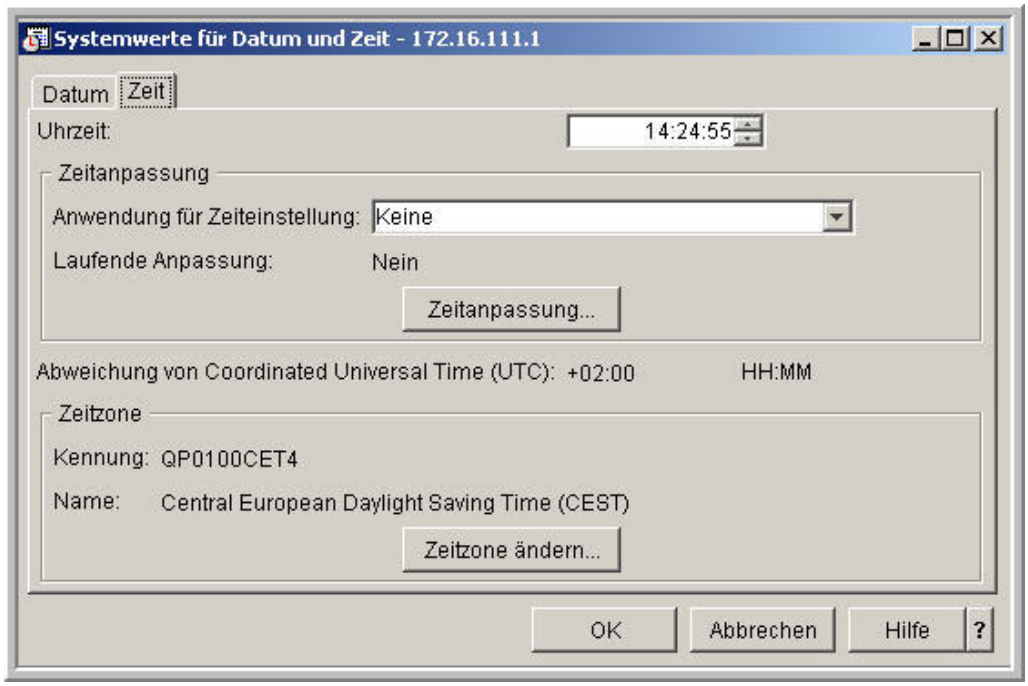
Mit Systemwerteinstellungen im iSeries Navigator arbeiten

Sie sehen, der iSeries Navigator fasst die Systemwerte ebenfalls in Funktionsgruppen zusammen. Hierbei geht der Operations Navigator aber weit über das Gruppenraster hinaus, das uns aus dem Befehl WRKSYSVAL bekannt ist. Es ist sicherlich leicht zu erkennen, dass hier eine differenzierte Gruppierung der Systemwertfunktionen vorgenommen wurde. Auch jetzt werde ich nicht alle oben gezeigten Gruppen detailliert mit Ihnen zusammen durchgehen, sondern nur stellvertretend einige Gruppen exemplarisch vorstellen.

16. Ergänzung 9/2008

9.6.2
Seite 2

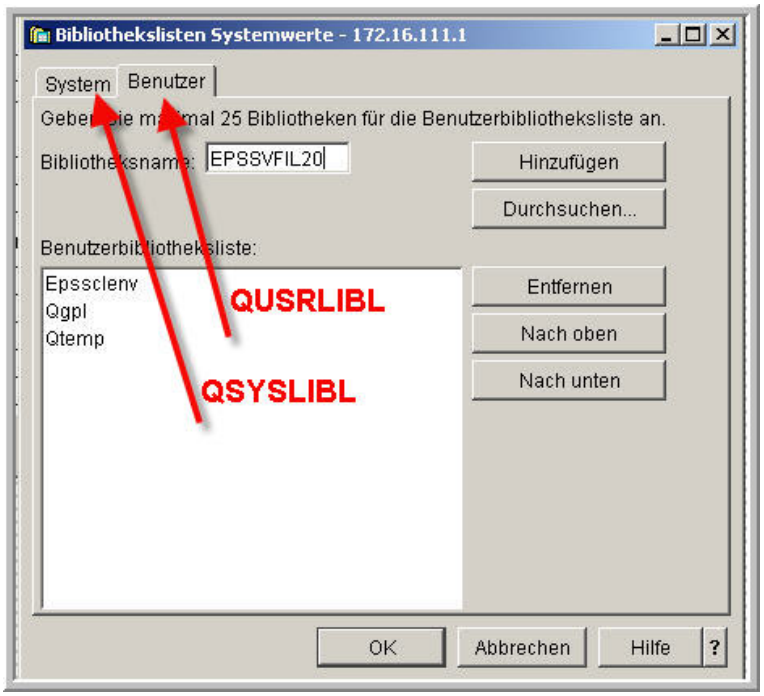
Ich öffne wie schon im 5250-Dialog zunächst die Funktionsgruppe „Datum und Uhrzeit“. So erhalten wir einen direkten Vergleich zwischen der 5250-Darstellung und dem iSeries Navigator:



Die Gruppe der Datums- und Zeitwerte

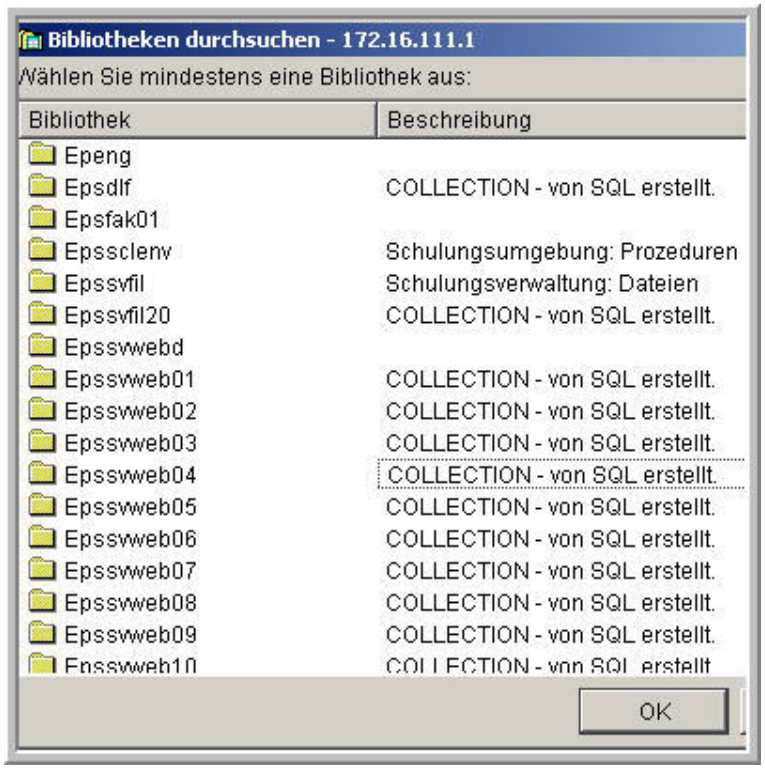
Die verschiedenen Systemwerte werden im iSeries Navigator nochmals über Register gruppiert. Dies erspart uns die Kenntnis der einzelnen Systemwertnamen. Der Systemwert QDATE wird u.a. im Register „Datum“ und der Systemwert QTIME im Register „Zeit“ dargestellt. Das Register „ZEIT“ gibt die Uhrzeit im Format HHMMSS an. Hierbei gilt: HH = Stunden, mm = Minuten und SS = Sekunden. Wenn Sie die Uhr mit diesem Systemwert einstellen, springt die Uhr entweder vorwärts oder rückwärts. Achtung! Dies kann zu unvorhersehbaren Ergebnissen führen, wenn Programme vor und nach der Änderung dieses Systemwerts auf die Uhr zugreifen. Zum Ändern der Systemzeit ist eine umfassende Kenntnis der Systemumgebung erforderlich. Wenn dieser Systemwert geändert wird, während eine automatische Zeitanpassung vorgenommen wird, wird die laufende Anpassung gestoppt. Eine automatische Zeitanpassung ist der manuellen Einstellung des Systemwerts QTIME stets vorzuziehen, denn die automatische Zeitanpassung stellt sicher, dass die Zeit nicht vorwärts oder rückwärts springt und so unvorhersehbare Fehler verursacht. Sie beschleunigt oder verlangsamt die Zeit eher ein wenig, bis die gewünschte Zeit erreicht ist.

Als nächstes bearbeiten wir die Systembibliothekssuchliste. Dafür öffnen wir selbstverständlich die Kategorie „Bibliothekslisten“. Zwei Systemwerte – QSYSLIBL und QUSRLIBL – bestimmen maßgeblich den Aufbau der Bibliothekssuchliste.



Systemwerte der Bibliotheksliste QSYSLIBL und QUSRLIBL

Hinter dem gezeigten Dialog steht die Bearbeitung des Systemwerts QUSRLIBL. Soll der Benutzerteil der Bibliothekssuchliste geändert werden, so geben Sie den Namen der gewünschten Bibliothek in den Parameter Bibliotheksname ein und drücken dann „Hinzufügen“. Ist Ihnen der Name der Bibliothek jedoch nur teilweise oder gar nicht bekannt, gehen Sie in den Dialog „Durchsuchen“. Daraufhin öffnet sich folgender Dialog:



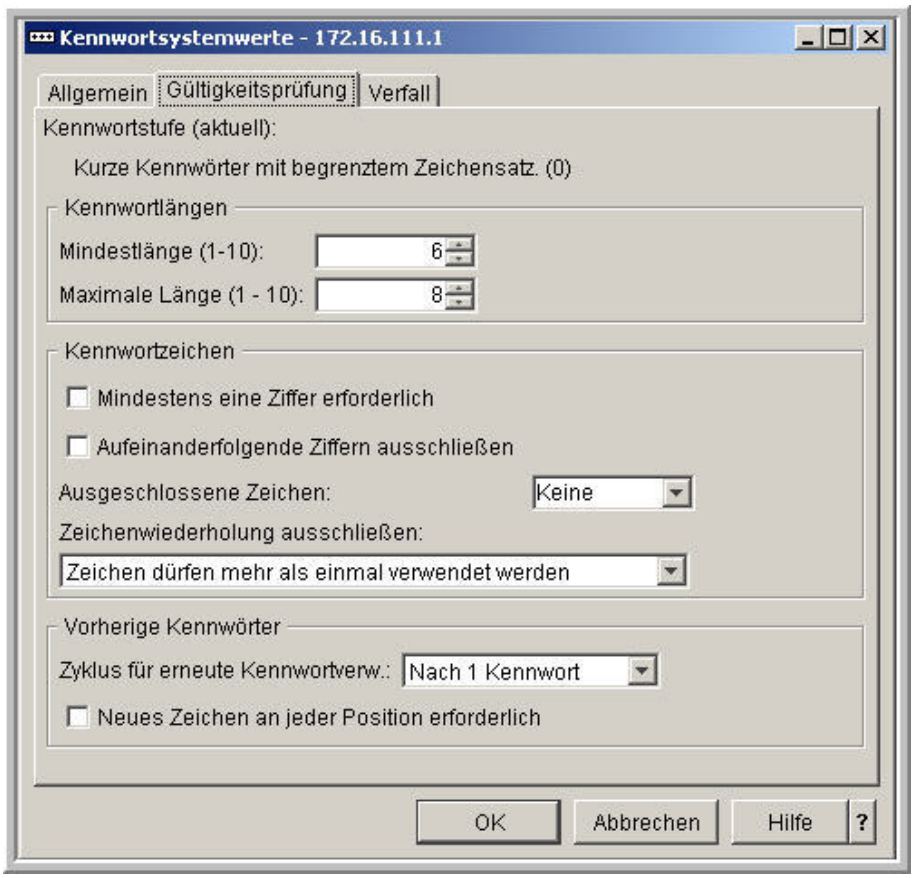
Bibliothek suchen

Wählen Sie aus der gezeigten Liste die gewünschte Bibliothek aus. Auch Mehrfach-Auswahlen sind möglich. Aber Achtung! Es werden hier nur die Bibliotheken des Systems angezeigt, für die Sie ein Leserecht besitzen. Nachdem Sie die betreffende Bibliothek markiert haben, beenden Sie den Dialog durch „OK“. Danach erscheint die ausgewählte Bibliothek im Register „Benutzer“. Verlassen Sie auch diesen Dialog mit dem Button „OK“, damit Ihre Änderungen übernommen werden.

Auch den Standarddrucker finden Sie im iSeries Navigator wieder. Dafür öffnen Sie die Gruppe „Drucker“.

Der Systemwert QPRTDEV

Abschließend möchte ich gern die Systemwertgruppe „Kennwort“ betrachten, da es mir immer wieder passiert, dass ich auf die unzulänglichen Möglichkeiten der Kennwortgestaltung einer iSeries angesprochen werde. Ein Vorwurf der nicht gerechtfertigt ist, wie Sie gleich sehen werden:



Die Kennwortsystemwerte

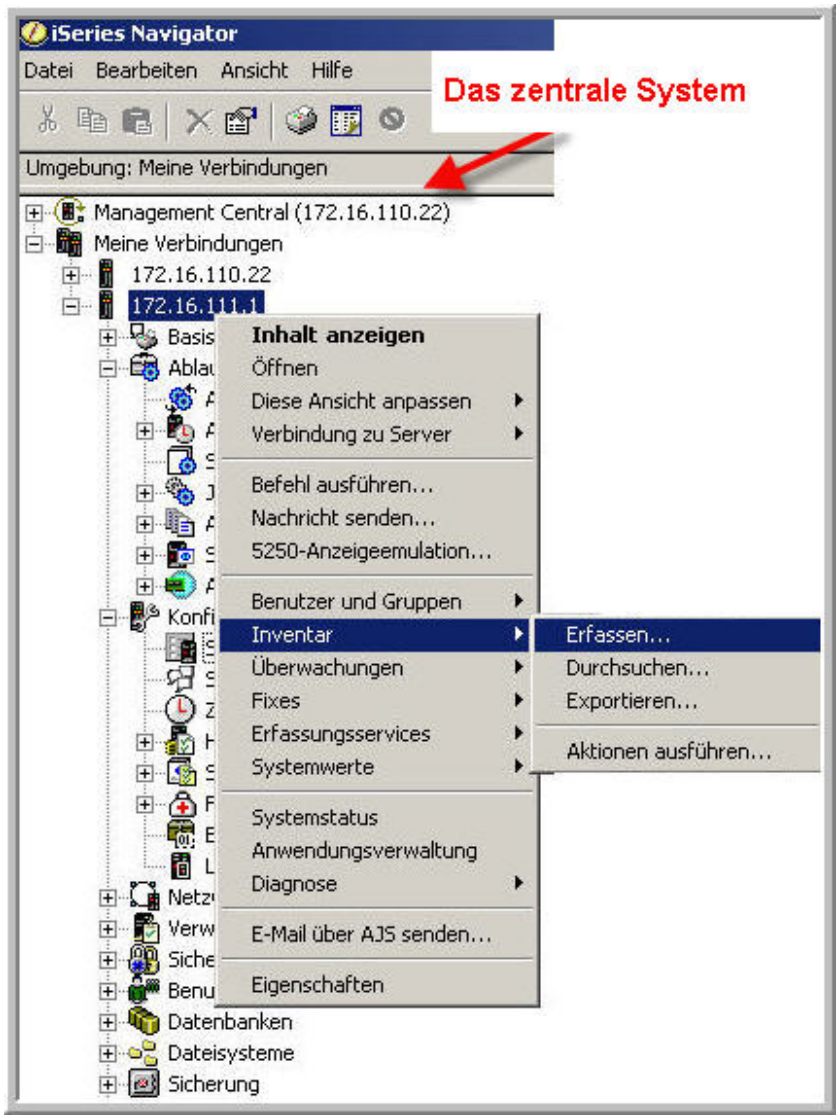
Kennwörter können auf einem iSeries Server ebenso komplex gestaltet werden wie auf jedem Windows System. Die Einstellungen für die Kennwortregeln sind allerdings von einer Vielzahl verschiedener Systemwerte abhängig. Allein das Register „Gültigkeitsprüfung“ fasst ca. zehn verschiedene Systemwerte zu einer Gruppe zusammen. In diesem Register legen Sie die Mindestanzahl der Zeichen (Systemwert QPWDMINLEN) für ein Kennwort fest. Die gültigen Werte sind abhängig von der Kennwortstufe Ihres Systems. Wird die Kennwortstufe 0 oder 1 angezeigt, lauten die gültigen Werte für die Mindestlänge 1 bis 10. Wird die Kennwortstufe 2 oder 3 angezeigt, lauten die gültigen Werte für die Mindestlänge 1 bis 128. Die Kennwortstufe wählen Sie im Register „Allgemein“ dieser Anzeige. Auch die maximale Länge des Kennwortes ist abhängig von der Kennwortstufe Ihres Systems. Wird Kennwortstufe 0 oder 1 angezeigt, lauten die gültigen Werte für die maximale Länge 1 bis 10. Wird Kennwortstufe 2 oder 3 angezeigt, lauten die gültigen Werte für die maximale Länge 1 bis 128. Der Standardwert beträgt 8 Zeichen. Neben

16. Ergänzung 9/2008

der Längenangabe können Sie auch den inhaltlichen Aufbau des Kennwortes bestimmen, d.h. Sie können die Verwendung numerischer Zeichen erzwingen oder die aufeinander folgende Verwendung numerischer Zeichen in einem Kennwort unterbinden. Diese Option bietet zusätzliche Sicherheit, da Benutzer in einem Kennwort keine Geburtsdaten, Telefonnummern oder Ziffernfolgen verwenden können. Außerdem können Sie Zeichen grundsätzlich verbieten. Verbieten Sie z. B. die Verwendung von Vokalen, kann der Benutzer tatsächlich existierende Wörter nicht als Kennwort verwenden. Alle anderen Einstellungen sind selbsterklärend und müssen an dieser Stelle nicht weiter erläutert werden.

Der iSeries Navigator bietet aber noch ein weiteres nützliches Feature, das es in dieser Form im 5250-Umfeld nicht gibt. Mit iSeries Navigator können Sie Ihre Systemwerteinstellungen innerhalb des Netzwerks über mehrere Systeme hinweg vergleichen und aktualisieren. Als Administrator müssen Sie ggf. die Systemwerteinstellungen auf vielen verschiedenen Systemen verwalten. Für diesen Fall ist es hilfreich sich ein Modellsystem aufzubauen, um dann die Systemwerte auf Ihrem Modellsystem mit den Werten auf einem oder mehreren Zielsystemen zu vergleichen. Es ist sogar möglich, die Systemwerte auf den Zielsystemen so zu aktualisieren, dass sie mit den Einstellungen des Modellsystems identisch sind. Wenn Sie möchten, können Sie auch eine Liste mit den Wertdifferenzen zwischen Modell- und Zielsystem generieren, statt die Werte auf dem Zielsystem tatsächlich zu ändern.

Eine Besonderheit gilt es hierbei jedoch zu beachten: Die Systemwerteinstellungen des Zielsystems werden nicht aktuell vom iSeries Server abgerufen, sondern sind in einem Inventar hinterlegt. Sie können an jedem Endpunktsystem seit V5R1 oder einer neueren Betriebssystemversion ein Inventar der Systemwerte anlegen. Erst wenn Sie diese Inventardaten zusammengestellt haben, sind die Informationen in iSeries Navigator für den Abgleich der Systemwerte verfügbar. Lassen Sie uns also zunächst ein entsprechendes Inventar erzeugen. Hierzu führen Sie entweder im Taskpad des Operations Navigator einen Doppelklick auf die Funktion „Inventar erfassen“ aus oder wählen über die Kontexttaste den Eintrag „Inventar erfassen“ aus.

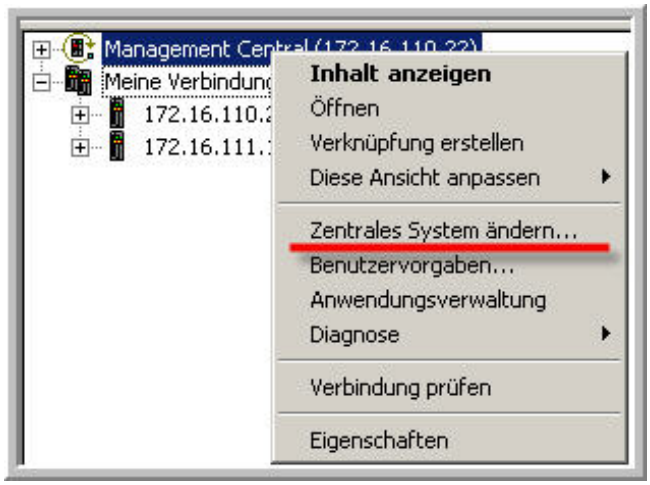


Inventar erfassen

Zunächst erscheint ein Informationsbildschirm, auf dem Ihnen mitgeteilt wird, dass eine Verbindung zum zentralen System hergestellt ist.

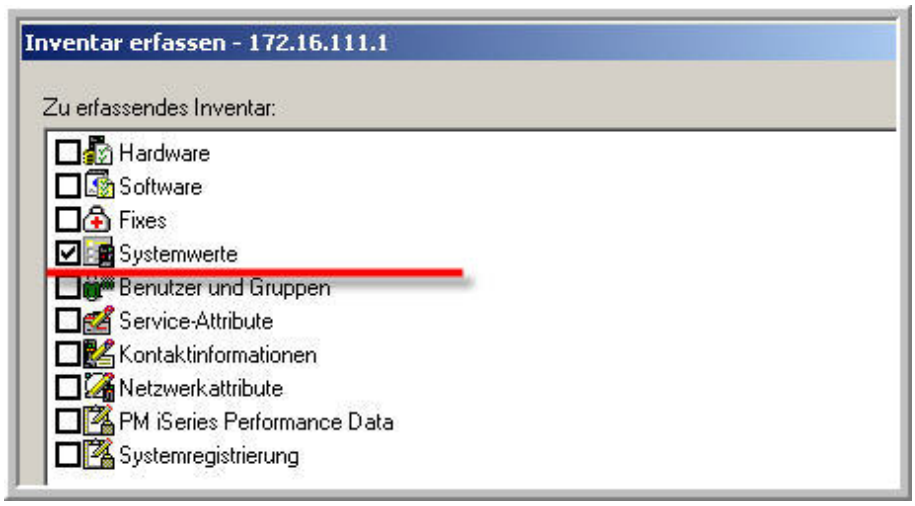
Der Informationsbildschirm

Die Inventarisierung und auch der spätere Abgleich sind Funktionen des Management Central, einem besonderen Feature des iSeries Navigator, das wir bislang nicht genutzt haben. Schauen Sie sich die Abbildung „Inventar erfassen“ noch einmal an. Dort sehen Sie die IP-Adresse des zentralen Systems. Das zentrale System wird als eine Art Hauptsystem im Netzwerk verstanden. Es übernimmt die gesamte Inventarisierung der Daten und die Datenübertragung zwischen den Endpunktsystemen. Sie legen das zentrale System fest, indem Sie den Eintrag „Management Central“ markieren und dann die rechte Maustaste drücken. Hier finden Sie den Menüpunkt „Zentrales System ändern“.



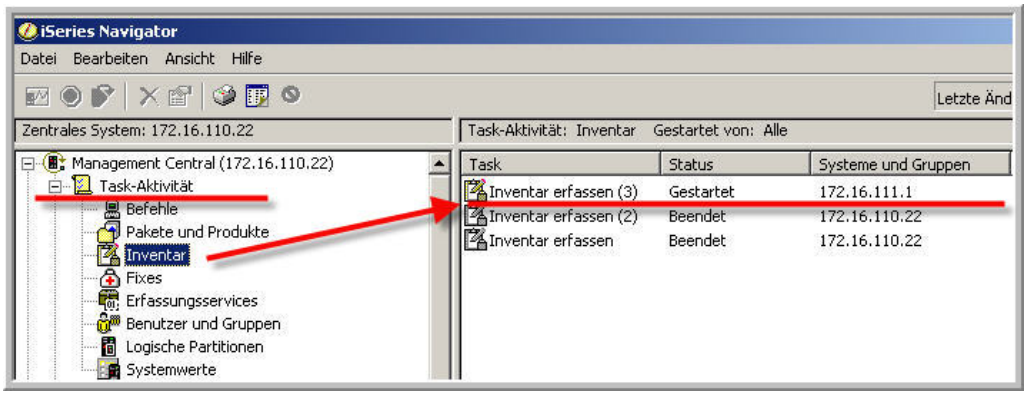
Das zentrale System festlegen

Zu diesem System wird für die Inventarisierung Ihrer Daten jetzt eine Verbindung hergestellt. Sie benötigen daher entsprechende Rechte für das zentrale System, andernfalls scheitert die Anforderung. Sobald die Verbindung hergestellt werden konnte, erscheinen die eigentlichen Dialogbildschirme:



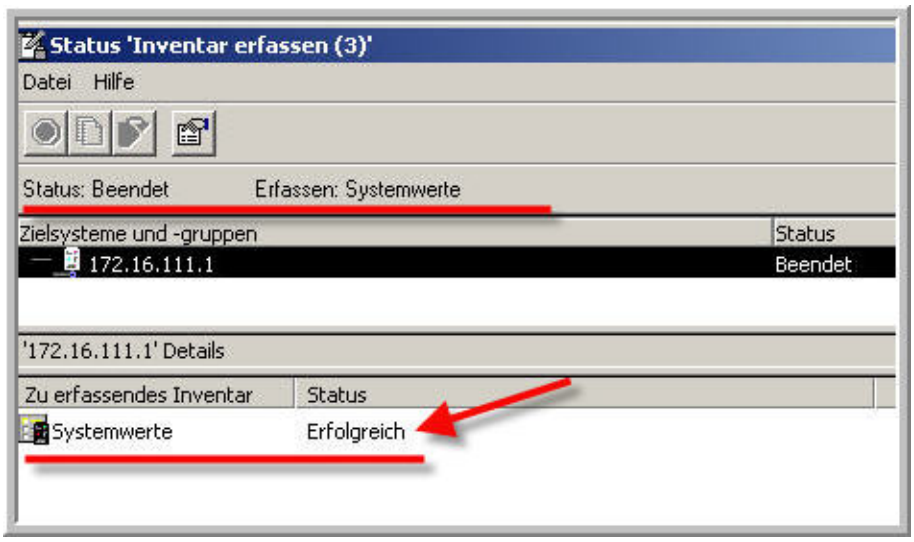
Inventarisierungsumfang festlegen

Im Dialog „Inventar erfassen“ können Sie eine Auswahl der Komponenten treffen, die inventarisiert werden sollen. Sie können einen oder mehrere Inventartypen zur Erfassung auswählen. Für den Moment ist die Inventarisierung der Systemwerte ausreichend. Die Erfassung des Inventars kann sofort ausgeführt werden oder für einen späteren Zeitpunkt geplant werden. Ich starte die Inventarisierung sofort und erhalte daraufhin ein Dialog-Fenster mit der Information, dass ein entsprechender Job auf dem zentralen System gestartet wurde. Den Inventarisierungsjob finden Sie im Management Central. Öffnen Sie „Management Central“ und den Eintrag „Task-Aktivität“. In der Kategorie „Inventar“ finden Sie die aktuellen Inventarisierungen, aber auch alte Jobs, die bereits beendet wurden:



Task-Aktivitäten anzeigen

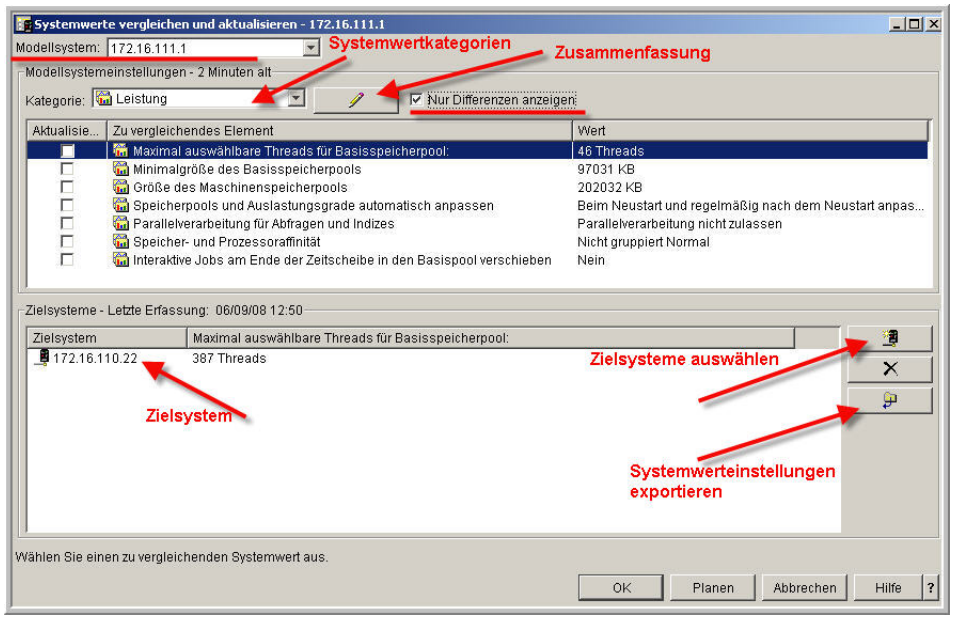
Sie müssen sich die Task-Aktivitäten aber nicht unbedingt anzeigen lassen. Denn sobald die Erfassung abgeschlossen ist, erhalten Sie einen entsprechenden Statusbildschirm. Auf diesem wird Ihnen mitgeteilt, dass die Inventarisierung abgeschlossen wurde. Diesem Bildschirm können Sie auch entnehmen, ob die Inventarisierung erfolgreich verlief:



Informationsbildschirm über den Abschluss der Erfassung

Meine Inventarisierung der Systemwerte wurde erfolgreich beendet, so dass ich jetzt mit dem Vergleich auf verschiedenen Systemen beginnen kann. Vorher aber noch eine kurze Anmerkung: Die Gesamterfassung des Inventars ist keine kurzfristige Aktion. Je mehr Komponenten des Systems erfasst werden, desto länger läuft der Erfassungsprozess. Laufzeiten von mehreren Stunden sind keine Seltenheit. Legen Sie deshalb die Inventarerfassung ggf. in die Nachtverarbeitung.

Ich benötige derzeit keine weiteren Inventarisierungen und öffne jetzt den Dialog für den Systemwertvergleich. Dafür markieren Sie zunächst eines der Endpunktsysteme. Im Kontextmenü wählen Sie „Systemwerte“. Daraufhin können Sie in der Unterauswahl „Vergleichen und aktualisieren“ auswählen, so dass sich der folgende Dialog öffnet:



Systemwerte vergleichen

Für diesen Vorgang benötigen Sie immer ein Modellsystem. Das Modellsystem entspricht einem System mit den optimalen Einstellungen für die Systemwerte. In den folgenden Beispielen ist das System 172.16.111.1 mein Modellsystem. Sie können auswählen, dass die Systemwerte des Modellsystems mit einem oder mehreren Zielsystemen verglichen werden sollen. Es wird zu jedem Zielsystem die aktuelle Einstellung für den Systemwert angezeigt, der in den Einstellungen für das Modellsystem ausgewählt wurde. Die Systemwerte der Zielsysteme werden vom zentralen System abgerufen. Damit diese Daten angezeigt werden, müssen Sie das Systemwerteinventar erfassen, das auf den Zielsystemen vorhanden ist. Wenn einer der Systemwerte nicht erfasst wurde, wird als Beschreibung für die letzte Erfassung der Status „Ein Teil des Inventars wurde nie erfasst“ ausgegeben, und der Wert lautet „Wert nicht erfasst“. Wenn keiner der Systemwerte für das Zielsystem erfasst wurde, lautet die Beschreibung der letzten Erfassung „Letzte Erfassung: Nie“. Den Status „Wert nicht erfasst“ erhalten Sie auch für Systemwerte, die vom Betriebssystem-Release des Zielsystems nicht unterstützt werden. Um ein Zielsystem hinzufügen, klicken Sie auf die Schaltfläche „Hinzufügen“. Anschließend wird eine Liste der verfügbaren Systeme angezeigt. Wählen Sie die gewünschten Systeme aus, und klicken Sie anschließend auf „Hinzufügen“. Um ein Zielsystem wieder aus der Liste zu entfernen, klicken Sie einfach auf die Schaltfläche „Aus Liste entfernen“. Nun müssen Sie auch noch die Kategorie der Systemwerte auswählen, die Sie anzeigen, vergleichen und aktualisieren wollen. Sie können die Systemwerte nach Kategorien anzeigen oder die Kategorie „Zusammenfassung“ auswählen, um alle Systemwerte anzuzeigen, die zur Aktualisierung ausgewählt wurden. Nachdem Sie einen der zu vergleichenden Werte ausgewählt haben, werden die entsprechenden Werte auf den Zielsystemen in der Liste für die Zielsysteme angezeigt. Nach Klicken auf die Schaltfläche „Export“ können Sie das Systemwerteinventar der Zielsysteme auch in einer Datei auf dem PC speichern.

Nützlich ist auch die Option „Nur Differenzen anzeigen“, um nur die Systemwerte und die Zielsysteme anzuzeigen, auf denen die Einstellung des Systemwerts vom Modellsystem abweicht. Falls Sie die Systemwerte jetzt abgleichen wollen, müssen Sie das Kontrollkästchen neben dem entsprechenden Systemwert aktivieren, der aktualisiert werden soll. Einige Systemwerte sind allerdings schreibgeschützt. Dies bedeutet, dass Sie den Wert nicht auswählen und aktualisieren können.

9.6.2
Seite 12

9.7 Sicherheitsrelevante Systemwerte

Der Power i-Befehl WRKSYSVAL eröffnet den Zugriff auf viele übergeordnet gültige Werte, die sogenannten Systemwerte. Hier können an zentraler Stelle Systemeinstellungen vorgenommen werden, die eine Vielzahl von Einstellungen betreffen, u. a. auch solche, die direkt oder indirekt die Sicherheit des Systems bestimmen und beeinflussen. In diesem Kapitel gehe ich auf diese Systemwerte ein und versuche, Ihnen einen ausführlichen Überblick über sie zu geben.

WRKSYSVAL

Der Einstieg erfolgt – wie oben erwähnt – mit dem Befehl WRKSYSVAL. Mit diesem Befehl können Sie sich die Systemwerte des Power i-Systems anzeigen lassen, aber auch Änderungen vornehmen oder eine Liste der Systemwerte ausdrucken.

```
                    Mit Systemwert arbeiten (WRKSYSVAL)

Auswahl eingeben und Eingabetaste drücken.

Systemwert . . . . . . . . . . .   *ALL_____     Name, generisch*...
Ausgabe  . . . . . . . . . . . .   *_____       *, *PRINT
```

WRKSYSVAL + F4

Sie können die Systemwertanzeige einschränken, indem Sie einen exakten Systemwertnamen eingeben oder einen generischen Namen mit * am Ende verwenden. Mit der Ausgabeoption *PRINT können Sie eine Liste der ausgewählten Systemwerte ausgeben:

```
                Aktueller                Gelieferter
Name            Wert                     Wert                 Beschreibung

QABNORMSW       0                        0                    Vorherige Systembeendigung
QACGLVL         *NONE                    *NONE                Abrechnungsebene
QACTJOB      >  601                      200                  Anfängliche Anzahl aktiver Jobs
QADLACTJ     >  550                      30                   Zusätzliche Anzahl aktiver Jobs
QADLSPLA        2048                     2048                 Zusätzlicher Speicher für Spool-Steuerblock
QADLTOTJ     >  600                      30                   Zusätzliche Anzahl aller Jobs
QALWJOBITP      0                        0                    Unterbrechung von Jobs zulassen
QALWOBJRST      *ALL                     *ALL                 Objektrückspeicherung zulassen
QALWUSRDMN      *ALL                     *ALL                 Benutzerdomänenobjekte in Bibliotheken zulassen
QASTLVL      >  *INTERMED                *BASIC               Unterstützungsstufe für Benutzer
QATNPGM         *ASSIST                  *ASSIST              Abrufprogramm
QAUDCTL      >  *AUDLVL                  *NONE                Protokollierungssteuerung
                *OBJAUD                  ' '
```

Ausdruck der Systemwerte

9.7
Seite 2

Mit der Auswahl * werden die Systemwerte zur Bearbeitung am Bildschirm angezeigt:

```
Listenanfang bei . . . .                 Anfangszeichen des Systemwerts
Teilauflistung nach Art     *ALL         F4=Liste

Auswahl eingeben und Eingabetaste drücken.
  2=Ändern   5=Anzeigen

Auswahl   Systemwert  Art       Beschreibung
   _      QABNORMSW   *SYSCTL   Vorherige Systembeendigung
   _      QACGLVL     *MSG      Abrechnungsebene
   _      QACTJOB     *ALC      Anfängliche Anzahl aktiver Jobs
   _      QADLACTJ    *ALC      Zusätzliche Anzahl aktiver Jobs
   _      QADLSPLA    *ALC      Zusätzlicher Speicher für Spool-Steuerblock
   _      QADLTOTJ    *ALC      Zusätzliche Anzahl aller Jobs
   _      QALWJOBITP  *SYSCTL   Unterbrechung von Jobs zulassen
   _      QALWOBJRST  *SEC      Objektrückspeicherung zulassen
   _      QALWUSRDMN  *SEC      Benutzerdomänenobjekte in Bibliotheken zulassen
                                                                  Weitere ...
Befehl
===>
F3=Verlassen    F4=Bedienerführung    F5=Neuanzeige    F9=Auffinden
F11=Nur Namen anzeigen    F12=Abbrechen
```

Mit Systemwerten arbeiten

Hier können Sie auf die zu ändernden Systemwerte positionieren und sie mit der Auswahl 5 anzeigen bzw. über die Auswahl 2 ändern.

Der Befehl DSPSYSVAL dient der Anzeige von Systemwerten ohne Änderungsmöglichkeit. Hier müssen Sie allerdings den Systemwert kennen und qualifiziert eingeben.

Achtung:

Einige sicherheitsrelevante Systemwerte können Sie nicht ändern, wenn sie zuvor im Betriebssystem vor Veränderungen geschützt worden sind. In den Service-Tools (SST) – über STRSST, Auswahl 7 (Work with System Security), gibt es u. a. den Parameter „Allow system value security changes". Ist dieser Parameter auf „2" (= No) gesetzt, werden die folgenden Systemwerte vor Veränderung geschützt:

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

Nachfolgend finden Sie eine Liste der sicherheitsrelevanten Systemwerte mit deren Bedeutung, mit Einstellmöglichkeiten und Erläuterungen. Die Erläuterungen zu den einzelnen Systemwerten und zu deren Parametern stammen weitestgehend aus der IBM Dokumentation und zeigen Ihnen, wie kongruentes Arbeiten mit dem Betriebssystem möglich ist.

9.7
Seite 4

9.7.1 QALWJOBITP

Unterbrechung von Jobs zulassen
Dieser Systemwert erlaubt es, Jobs zu unterbrechen und zeigt an, wie das System reagieren wird, wenn ein Benutzer die Unterbrechung eines Jobs anfordert, damit ein benutzerdefiniertes Exitprogramm in diesem Job ausgeführt werden kann.

Der Unterbrechungsstatus eines aktiven Jobs kann jederzeit geändert werden; die Änderung wird jedoch erst wirksam, wenn der Wert QALWJOBITP die Unterbrechung des Jobs zulässt.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:
0 Das System erlaubt keine Jobunterbrechung zur Ausführung benutzerdefinierter Exitprogramme. Alle neuen Jobs, die aktiv werden, dürfen standardmäßig nicht unterbrochen werden.
1 Das System erlaubt eine Jobunterbrechung zur Ausführung benutzerdefinierter Exitprogramme. Alle neuen Jobs, die aktiv werden, dürfen standardmäßig nicht unterbrochen werden.

9.7.1
Seite 2

9.7.2 QALWOBJRST

Objektrückspeicherung zulassen
Mit diesem Systemwert können Sie die Rückspeicherung von Objekten erlauben oder verhindern. Er gibt an, ob Objekte mit sicherheitsrelevanten Attributen zurückgespeichert werden können. Dieser Wert besteht aus einer Liste mit Werten, die das zurückzuspeichernde Objekt steuern. Der Wert kann als *ALL, *NONE oder als Liste einzelner Werte angegeben werden.

Änderungen an diesem Systemwert werden mit der Ausführung des nächsten Rückspeicherungsvorgangs wirksam. Der Vorgabewert ist *ALL.

Wenn versucht wird, ein Objekt auf dem System zurückzuspeichern, arbeiten drei Systemwerte gemeinsam als Filter. Sie bestimmen, ob das Objekt zurückgespeichert werden darf oder ob es während der Rückspeicherung konvertiert wird. Der erste Filter ist der Systemwert **QVFYOBJRST** (Objekt beim Zurückspeichern prüfen). Dieser Systemwert steuert das Zurückspeichern einiger Objekte, die digital signiert werden können. Der zweite Filter ist der Systemwert **QFRCCVNRST** (Umsetzung beim Zurückspeichern erzwingen). Mit Hilfe dieses Systemwerts kann angegeben werden, ob während des Zurückspeicherns Programme, Serviceprogramme, SQL-Pakete und Modulobjekte konvertiert werden sollen oder nicht. Er kann auch verhindern, dass Objekte zurückgespeichert werden. Vom dritten Filter werden nur Objekte verarbeitet, die die ersten beiden Filter passiert haben. Dieser dritte Filter ist der Systemwert **QALWOBJRST** (Zurückspeichern des Objekts erlauben). Er gibt an, ob Objekte mit sicherheitsrelevanten Attributen zurückgespeichert werden können.

Gültige Werte sind:

*ALL	Alle Objekte können mit oder ohne sicherheitsrelevante Attribute zurückgespeichert werden.
*NONE	Objekte mit sicherheitsrelevanten Attributen können nicht zurückgespeichert werden.
*ALWSYSSTT	Alle Programme, Serviceprogramme und Module mit dem Attribut für Systemstatus oder übernommenen Status können zurückgespeichert werden. Wenn das Objekt aufgrund der Einstellung des Systemwerts QFRCCVNRST konvertiert wird, wird ihm das Attribut für Benutzerstatus zugeordnet.
*ALWPGMADP	Programme und Serviceprogramme mit dem Attribut für Berechtigungsübernahme können zurückgespeichert werden.

9.7.2 Seite 2

*ALWPTF	Systemstatusobjekte oder Objekte mit übernommenem Status, die Berechtigungen übernehmen, Objekte, für die das Attribut S_ISUID (Benutzer-ID setzen) aktiviert ist, und Objekte, für die das Attribut S_ISGID (Gruppen-ID setzen) aktiviert ist, werden bei einer PTF-Installation im System zurückgeschrieben.
*ALWSETUID	Dateien, bei denen das Attribut S_ISUID (Benutzer-ID setzen) aktiviert ist, werden zurückgespeichert.
*ALWSETGID	Dateien, bei denen das Attribut S_ISGID (Gruppen-ID setzen) aktiviert ist, werden zurückgespeichert.
*ALWVLDERR	Objekte mit Gültigkeitsfehlern oder mit denen möglicherweise manipuliert wurde, werden zurückgespeichert. Wenn das Objekt aufgrund der Einstellung des Systemwerts QFRCCVNRST konvertiert wird, werden alle möglicherweise vorhandenen Gültigkeitsfehler korrigiert.

9.7.3 QALWUSRDMN

Benutzerdomänenobjekte in Bibliotheken zulassen
Dieser Systemwert gibt an, welche Bibliotheken im System die Benutzerdomänenobjekte *USRSPC (Benutzeradressbereich), *USRIDX (Benutzerindex) und *USRQ (Benutzerwarteschlange) enthalten können.

Eine Änderung dieses Systemwerts wird sofort wirksam. Bei Angabe von *ALL können alle Bibliotheken im System Benutzerdomänenversionen von USRxxx-Objekten enthalten. Wird eine Liste mit Bibliotheksnamen angegeben, können bei Anwendungen, die derzeit mit Benutzerdomänenobjekten (*USRxxx) arbeiten, Fehler auftreten, wenn die Anwendungen Benutzerdomänenobjekte in Bibliotheken verwenden, die nicht vom Systemwert zugelassen werden. Bei Angabe einer Bibliotheksliste oder von *DIR muss QTEMP in der Liste enthalten sein.

Bei Angabe eines Bibliotheksnamens können alle Bibliotheken mit diesem Namen, die in separaten, unabhängigen Zusatzspeicherpools vorhanden sind, Benutzerdomänenobjekte enthalten. Der Vorgabewert ist *ALL.

Um potenzielle Sicherheitsrisiken zu minimieren, wird folgendes Vorgehen empfohlen: Bevor eine Bibliothek zu QALWUSRDMN hinzugefügt wird, sollte sie im Basis-ASP oder in allen unabhängigen ASPs erstellt werden und die allgemeine Berechtigung *EXCLUDE erhalten.

Gültige Werte sind:

*ALL	Alle Bibliotheken im System können Benutzerdomänenversionen von *USRxxx-Objekten enthalten. Bei Angabe von *ALL wird auch *DIR einbezogen.
*DIR	Die Verzeichnisse können Benutzerdomänenobjekte enthalten. Bei Angabe von *DIR muss QTEMP in der Liste enthalten sein.
Bibliotheken	Bestimmte Bibliotheken angeben, die Benutzerdomänenversionen von *USRxxx-Objekten enthalten können. Es können bis zu 50 Bibliotheken aufgelistet werden; die Bibliothek QTEMP muss in der Liste enthalten sein.

9.7.3
Seite 2

9.7.4 QAUDCTL

Protokollierungssteuerung
Dieser Systemwert enthält die Ein-/Ausschalter für die Objekt- und Benutzeraktionsprotokollierung. Er aktiviert die mit den Befehlen CHGOBJAUD (Objektprotokollierung ändern) und CHGUSRAUD (Benutzerprotokollierung ändern) sowie die mit den Systemwerten QAUDLVL und QAUDLVL2 ausgewählte Protokollierung.

- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Eine Änderung dieses Systemwerts wird für alle Jobs im System sofort wirksam.

Der Vorgabewert ist *NONE.

Um die Protokollierung zu aktivieren, muss entweder *OBJAUD oder *AUDLVL angegeben werden. Soll die Protokollierung inaktiviert werden, *NONE angeben.

Einen oder mehrere der folgenden Werte angeben. Bei Angabe von *NONE ist kein weiterer Wert mehr zulässig.

Gültige Werte sind:

*NOTAVL	Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
*NONE	Auf dem System findet keine Sicherheitsprotokollierung statt. Dies ist der Standardwert.
*OBJAUD	Es werden Aktionen für Objekte protokolliert, die einen anderen Objektprotokollierungswert als *NONE haben. Der Objektprotokollierungswert wird im Befehl CHGAUD (Protokollierung ändern) oder im Befehl CHGOBJAUD (Objektprotokollierung ändern) festgelegt.

9.7.4
Seite 2

*AUDLVL	Die in den Systemwerten QAUDLVL und QAUDLVL2 angegebenen Aktionen werden im Sicherheitsprotokolljournal protokolliert. Die von den Aktionsprotokollierungswerten eines Benutzerprofils angegebenen Aktionen werden ebenfalls protokolliert. Die Aktionsprotokollierungswerte eines Benutzerprofils werden im Parameter AUDLVL des Befehls CHGUSRAUD (Benutzerprotokollierung ändern) angegeben.
*NOQTEMP	Die meisten Objekte werden in QTEMP nicht protokolliert. *NOQTEMP muss entweder mit *OBJAUD oder *AUDLVL angegeben werden. *NOQTEMP darf nicht allein angegeben werden.

- Das Journal QAUDJRN muss in der Bibliothek QSYS vorhanden sein, damit dieser Systemwert in einen anderen Wert als *NONE geändert werden kann.
- Das Journal QAUDJRN kann erst dann gelöscht oder aus der Bibliothek QSYS in eine andere Bibliothek verschoben werden, wenn dieser Systemwert in *NONE geändert worden ist.

9.7.5 QAUDENDACN

Aktion bei Protokollierungsende
Dieser Systemwert gibt die Aktion an, die vom System ausgeführt wird, wenn keine Protokollsätze an das Protokolljournal gesendet werden können, da beim Senden des Journaleintrags Fehler aufgetreten sind.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NOTIFY.

- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Gültige Werte sind:

*NOTAVL	Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
*NOTIFY	Nachdem ein Fehlerhinweis auf das fehlgeschlagene Senden des Journaleintrags an das Sicherheitsprotokolljournal der Nachrichtenwarteschlangen QSYSOPR und QSYSMSG gesendet wurde, wird die Aktion, die den Protokollierungsversuch ausgelöst hat, fortgesetzt. Bei Angabe des Werts *NOTIFY wird der Systemwert QAUDCTL auf *NONE gesetzt, um die Protokollierung auszuschalten. Wenn der Systemprotokollierungscode den Systemwert QAUDCTL ausschaltet, wird stündlich ein entsprechender Hinweis an die Nachrichtenwarteschlangen QSYSOPR und QSYSMSG (falls vorhanden) gesendet. Das stündliche Hinweisen stoppt, sobald die Protokollierung wieder eingeschaltet wird.

9.7.5
Seite 2

*PWRDWNSYS Das System wird mit dem Systemreferenzcode B900 3D10 beendet, wenn ein Versuch, die Protokollierungsdaten an das Sicherheitsprotokolljournal zu senden, fehlschlägt. Wenn danach ein IPL durchgeführt wird, hat das System den Status des eingeschränkten Betriebs, weshalb für dieses IPL eine zugeordnete Konsole erforderlich ist. Bei Angabe des Werts *PWRDWNSYS wird der Systemwert QAUDCTL auf *NONE gesetzt, um die Protokollierung auszuschalten. Bei dem IPL, der auf das Abschalten des Systems folgt, muss sich ein Benutzer mit den Sonderberechtigungen *AUDIT und *ALLOBJ am System anmelden.

Der Systemwert QAUDENDACN gilt nur für Protokolleinträge, die vom Betriebssystem gesendet werden.

9.7.6 QAUDFRCLVL

Protokollierungsdaten erzwingen
Protokolljournal in Zusatzspeicher stellen. Dieser Systemwert gibt die Anzahl der Protokolljournaleinträge an, die in das Sicherheitsprotokolljournal geschrieben werden können, bevor die Journaleintragsdaten in den Zusatzspeicher gestellt werden. Der Wert gibt auch die Anzahl der Protokollierungsdaten an, die verloren gehen könnten, falls das System abnormal beendet wird. Wenn Protokolljournaleinträge häufig in den Zusatzspeicher gestellt werden, kann sich dies negativ auf die Systemleistung auswirken. Mit diesem Systemwert kann das Journal QUADJRN geändert werden, um anzugeben, wie oft Protokollierungsdaten in den Zusatzspeicher gestellt werden sollen. Eine Änderung dieses Systemwerts wird sofort wirksam.

Der Vorgabewert ist *SYS.
- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Gültige Werte sind:

*NOTAVL	Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
*SYS	Die Journaleinträge werden nur dann in den Zusatzspeicher geschrieben, wenn das System feststellt, dass dies abhängig von der internen Systemverarbeitung erforderlich ist. Diese Angabe liefert zwar die besten Protokollierungsergebnisse, kann aber auch zum höchsten Datenverlust bei einem abnormalen Ende des Systems führen.
1–100	Die Anzahl der ins Sicherheitsprotokolljournal geschriebenen Journaleinträge, bevor die Protokollierungsdaten in den Zusatzspeicher geschrieben werden. Je kleiner diese Anzahl angegeben wird, umso höher sind die Auswirkungen auf die Systemleistung.

Wird ein Journaleintrag, bei dem es sich nicht um eine Objektprotokollierung handelt, ins Sicherheitsprotokolljournal geschrieben (beispielsweise mit dem Befehl SNDJRNE – Journaleintrag senden) und ist diese Auswahl angegeben, werden neben diesem Journaleintrag auch alle anderen Protokollierungsdaten in den Zusatzspeicher geschrieben.

9.7.6
Seite 2

9.7.7 QAUDLVL

Sicherheitsprotokollebene
Steuert die Ebene der Sicherheitsprotokollierung im System.

Wenn der Systemwert QAUDLVL den Wert *AUDLVL2 enthält, werden auch die Werte im Systemwert QAUDLVL2 verwendet. Wenn der Systemwert QAUDLVL nicht den Wert *AUDLVL2 enthält, werden die Werte im Systemwert QAUDLVL2 ignoriert.

- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Eine Änderung dieses Systemwerts wird für alle Jobs im System sofort wirksam. Der Vorgabewert ist *NONE.

Entweder *NONE oder eine beliebige Kombination aus den anderen Werten angeben.

Gültige Werte sind:

*NONE	Auf dem System findet keine Sicherheitsprotokollierung statt. Dies ist der Standardwert.
*AUDLVL2	Die zu überwachenden Sicherheitsaktionen werden anhand der beiden Systemwerte QAUDLVL und QAUDLVL2 bestimmt. · Wenn ausschließlich der Systemwert QAUDLVL2 verwendet werden soll, für den Systemwert QAUDLVL den Wert *AUDLVL2 angeben und die Protokollierungswerte dem Systemwert QAUDLVL2 hinzufügen. · Wenn beide Systemwerte verwendet werden sollen, können die Werte im Systemwert QAUDLVL zusammen mit dem Wert *AUDLVL2 gesetzt werden; anschließend alle zusätzlichen Werte dem Systemwert QAUDLVL2 hinzufügen.

9.7.7 Seite 2

*ATNEVT	Abrufereignisse werden protokolliert. Abrufereignisse sind Bedingungen, die eine weitere Auswertung erfordern, damit die Bedeutung der Bedingung für die Sicherheit festgestellt werden kann. Beispiel: Überwachungsereignisse, die auf einen unbefugten Zugriff hinweisen, müssen näher untersucht werden, um festzustellen, ob es sich bei der Bedingung tatsächlich um einen unbefugten Zugriff oder einen falschen Alarm handelt.
*AUTFAIL	Berechtigungsfehler werden protokolliert. Beispiele: · Alle Zugriffsfehler (Anmeldung, Berechtigung, Jobübergabe) · Unzulässiges Kennwort oder unzulässige Benutzer-ID an einer Einheit eingegeben
*CREATE	Alle Objekterstellungen werden protokolliert. In der Bibliothek QTEMP erstellte Objekte werden nicht protokolliert. Beispiele: · Neu erstellte Objekte · Objekte, die erstellt wurden, um ein bestehendes Objekt zu ersetzen.
*DELETE	Alle Löschungen externer Objekte im System werden protokolliert. Objekte, die aus der Bibliothek QTEMP gelöscht werden, werden nicht protokolliert.
*JOBBAS	Jobbasisfunktionen werden protokolliert. Beispiele: · Start- und Stoppdaten eines Jobs · Anhalten, Freigeben, Stoppen, Fortsetzen, Ändern, Unterbrechen, Beenden, abnormal Beenden und Zuordnen der PSR (Programmstartanforderungen) zu vorab gestarteten Jobeinträgen
*JOBCHGUSR	Änderungen des aktiven Benutzerprofils für einen Thread oder seiner Gruppenprofile werden protokolliert.

*JOBDTA	Aktionen, die einen Job betreffen, werden protokolliert. Beispiele: · Start- und Stoppdaten eines Jobs · Anhalten, Freigeben, Stoppen, Fortsetzen, Ändern, Unterbrechen, Beenden, abnormal Beenden und Zuordnen der PSR (Programmstartanforderungen) zu vorab gestarteten Jobeinträgen · Ändern des aktiven Benutzerprofils für einen Thread oder Ändern von Gruppenprofilen · *JOBDTA setzt sich aus zwei Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn beide Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *JOBDTA. *JOBDTA setzt sich aus folgenden Werten zusammen: · *JOBBAS · *JOBCHGUSR
*NETBAS	Netzbasisfunktionen werden protokolliert. Beispiele: · IP-Regelaktionen · Sockets-Verbindungen · APPN-Verzeichnissuchfilter · APPN-Endpunktfilter
*NETCLU	Operationen für Cluster oder Cluster-Ressourcengruppen werden protokolliert. Beispiele: · Hinzufügen, erstellen und löschen · Verteilung · Beenden · Übernehmen · Listeninformationen · Entfernen · Starten · Umschalten · Attribute aktualisieren

9.7.7
Seite 4

*NETCMN	Netzbetriebs- und Übertragungsfunktionen werden protokolliert. Beispiele: · Netzbasisfunktionen (siehe *NETBAS) · Operationen für Cluster oder Cluster-Ressourcengruppen (siehe *NETCLU) · Netzfehler (siehe *NETFAIL) · Sockets-Funktionen (siehe *NETSCK) · *NETCMN setzt sich aus mehreren Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn alle Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *NETCMN. *NETCMN setzt sich aus folgenden Werten zusammen: · *NETBAS · *NETCLU · *NETFAIL · *NETSCK
*NETFAIL	Netzfehler werden protokolliert. Beispiele: · Socket-Port nicht verfügbar
*NETSCK	Sockets-Tasks werden protokolliert. Beispiele: · Accept · Connect · DHCP-Adresse zugeordnet · DHCP-Adresse nicht zugeordnet · Gefilterte Mail · Mail zurückweisen
*NOTAVL	Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
*OBJMGT	Generische Objekttasks werden protokolliert. Beispiele: · Übertragen von Objekten · Umbenennen von Objekten
*OFCSRV	Office Vision werden protokolliert. Beispiele: · Änderungen des Systemverteilerverzeichnisses · Aufgaben, die die elektronische Post betreffen

*OPTICAL	Alle optischen Funktionen werden protokolliert. Beispiele: · Hinzufügen oder Entfernen einer optischen Kassette · Ändern der Berechtigungsliste, die zum Schützen eines optischen Datenträgers verwendet wird · Öffnen einer optischen Datei oder eines optischen Verzeichnisses · Erstellen oder Löschen eines optischen Verzeichnisses · Ändern oder Abrufen der Attribute eines optischen Verzeichnisses · Kopieren, Versetzen oder Umbenennen einer optischen Datei · Kopieren eines optischen Verzeichnisses · Sichern eines optischen Datenträgers · Initialisieren oder Umbenennen eines optischen Datenträgers · Ändern eines optischen Sicherungsdatenträgers in einen primären Datenträger · Sichern oder Freigeben einer optischen Datei im Wartestatus · Absolutes Lesen eines optischen Datenträgers
*PGMADP	Die Übernahme der Programmeignerberechtigung wird protokolliert.
*PGMFAIL	Programmfehler werden protokolliert. Beispiele: · Geblockte Anweisung · Fehler bei Gültigkeitsprüfung · Domänenfehler
*PRTDTA	Druckfunktionen werden protokolliert. Beispiele: · Drucken einer Spool-Datei · Drucken mit dem Parameter SPOOL (*NO)

*SAVRST	Informationen, die das Sichern und Zurückspeichern betreffen, werden protokolliert. Beispiele: · wenn Programme zurückgespeichert werden, die das Profil des Programmeigners übernehmen; · wenn Jobbeschreibungen zurückgespeichert werden, die Benutzernamen enthalten; · wenn sich der Eigner oder Berechtigungen bei zurückgespeicherten Objekten ändern; · wenn die Berechtigung für Benutzerprofile zurückgespeichert wird; · wenn ein Systemstatusprogramm zurückgespeichert wird; · wenn ein Systembefehl zurückgespeichert wird; · wenn ein Objekt zurückgespeichert wird.
*SECCFG	Die Sicherheitskonfiguration wird protokolliert. Beispiele: · Erstellen, Ändern, Löschen und Zurückspeichern von Benutzerprofilen · Programmänderungen (CHGPGM), die nicht das Profil des Eigners übernehmen · Änderungen der Systemwerte, Umgebungsvariablen und Netzwerkattribute · Änderungen der Subsystemleitwege · Das Zurücksetzen des Kennworts QSECOFR von DST auf den Vorgabewert · Das Anfordern des Standardwerts für das Kennwort zur ID des Sicherheitsbeauftragten für die Serviceprogramme · Änderungen des Objektprotokollierungsattributs
*SECDIRSRV	Änderungen oder Updates bei der Ausführung von Verzeichnis-Servicefunktionen werden protokolliert. Beispiele: · Änderung des Protokolls · Erfolgreicher Bind · Änderung der Berechtigung · Änderung des Kennworts · Änderung des Eigentumsrechts · Erfolgreiches Auflösen (unbind)

*SECIPC	Änderungen der Interprozesskommunikation werden protokolliert. Beispiele: · Änderung des Eigentumsrechts oder der Berechtigung eines IPC-Objekts · Erstellen, Löschen oder Abrufen eines IPC-Objekts · Zuordnung des gemeinsam genutzten Speichers
*SECNAS	Aktionen des Netzwerkauthentifizierungsservice werden protokolliert. Beispiele: · Service-Ticket gültig · Service-Principals stimmen nicht überein · Client-Principals stimmen nicht überein · Diskrepanz bei Ticket-IP-Adresse · Entschlüsselung des Tickets fehlgeschlagen · Entschlüsselung des Authentifikators fehlgeschlagen · Realm befindet sich nicht innerhalb Client- und lokalem Realm · Ticket ist Replay-Versuch · Ticket ist noch nicht gültig · Diskrepanz bei lokaler IP-Adresse · Entschlüsselung von KRB_AP_PRIV- oder KRB_AP_SAFE-Kontrollsummenfehler · KRB_AP_PRIV-, KRB_AP_SAFE-Zeitmarkenfehler, Replay-Fehler, oder Reihenfolgefehler · GSS accept – abgelaufene Berechtigungsnachweise, Kontrollsummenfehler, Kanalbindungen · GSS unwrap oder GSS verify – abgelaufener Kontext, Entschlüsseln/Decodieren, Kontrollsummenfehler, Reihenfolgefehler
*SECRUN	Sicherheitslaufzeitfunktionen werden protokolliert. Beispiele: · Änderungen des Objekteignerrechts · Änderungen der Berechtigungsliste oder der Objektberechtigung · Änderungen der Primärgruppe eines Objekts
*SECSCKD	Socket-Deskriptoren werden protokolliert. Beispiele: · Ein Socket-Deskriptor wurde einem anderen Job zugeordnet · Deskriptor empfangen · Deskriptor kann nicht benutzt werden

9.7.7
Seite 8

*SECURITY — Alle sicherheitsrelevanten Funktionen werden protokolliert.
- Sicherheitskonfiguration (siehe *SECCFG)
- Änderungen oder Updates bei der Ausführung von Verzeichnisservicefunktionen (siehe *SECDIRSRV)
- Änderungen der Interprozesskommunikation (siehe *SECIPC)
- Aktionen des Netzwerkauthentifizierungsservice (siehe *SECNAS)
- Sicherheitslaufzeitfunktionen (siehe *SECRUN)
- Socket-Deskriptor (siehe *SECSCKD)
- Verwendung der Prüffunktionen (siehe *SECVFY)
- Änderungen von Prüflistenobjekten (siehe *SECVLDL)

*SECURITY setzt sich aus mehreren Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn alle Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *SECURITY. *SECURITY setzt sich aus folgenden Werten zusammen:
- *SECCFG
- *SECDIRSRV
- *SECIPC
- *SECNAS
- *SECRUN
- *SECSCKD
- *SECVFY
- *SECVLDL

*SECVFY — Die Verwendung der Prüffunktionen wird protokolliert. Beispiele:
- Ein Zielbenutzerprofil wurde während einer Pass-Through-Sitzung geändert
- Es wurde eine interne Profilkennung generiert
- Alle Profilmerkmale wurden inaktiviert
- Es wurde die maximale Anzahl an Profilmerkmalen generiert
- Es wurde ein Profilmerkmal generiert
- Alle Profilmerkmale für einen Benutzer wurden inaktiviert
- Benutzerprofil wurde authentifiziert
- Ein Office-Benutzer startete oder beendete die Verarbeitung im Namen eines anderen Benutzers

*SECVLDL	Änderungen von Prüflistenobjekten werden protokolliert. Beispiele: · Hinzufügen, Ändern, Entfernen eines Prüflisteneintrags · Suchen eines Prüflisteneintrags · Erfolgreiche oder nicht erfolgreiche Überprüfung eines Prüflisteneintrags
*SERVICE	Das System i Security-Referenzhandbuch, IBM Form SC41-5302 enthält eine Liste aller protokollierten Servicebefehle und API-Aufrufe.
*SPLFDTA	Spooldateifunktionen werden protokolliert. Beispiele: · Erstellen, Löschen, Anzeigen, Kopieren, Anhalten und Freigeben einer Spooldatei · Daten aus einer Spool-Datei abrufen (QSPGETSP) · Spool-Dateiattribute ändern (CHGSPLFA)
*SYSMGT	Systemverwaltungstasks werden protokolliert. Beispiele: · HFS-Registrierung · Änderungen von Funktionen für die Oberfläche von Anwendungen · Änderungen der Systemantwortliste · Änderungen am Verzeichnis der relationalen Datenbanken (DRDA) · Netzdateioperationen

9.7.7
Seite 10

9.7.8 QAUDLVL2

Erweiterung der Sicherheitsprotokollierung
Dieser Systemwert ist erforderlich, wenn mehr als 16 Protokollierungswerte benötigt werden. Wird *AUDLVL2 als einer der Werte im Systemwert QAUDLVL angegeben, sucht das System auch im Systemwert QAUDLVL2 nach Protokollierungswerten.

Wenn der Systemwert QAUDLVL den Wert *AUDLVL2 enthält, werden auch die Werte im Systemwert QAUDLVL2 verwendet. Wenn der Systemwert QAUDLVL nicht den Wert *AUDLVL2 enthält, werden die Werte im Systemwert QAUDLVL2 ignoriert.

- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Eine Änderung dieses Systemwerts wird für alle Jobs im System sofort wirksam. Der Vorgabewert ist *NONE.

9.7.8
Seite 2

9.7.9 QCRTAUT

Allgemeine Berechtigung für Objekterstellung
Gibt die standardmäßige allgemeine Berechtigung an, die beim Erstellen von Objekten in einer Bibliothek verwendet wird. Wird der Wert *LIBCRTAUT des Schlüsselworts AUT in einem Befehl zur Objekterstellung verwendet – etwa um die allgemeine Berechtigung für ein Objekt festzulegen – so gibt der Wert CRTAUT der Bibliothek, in der das Objekt erstellt wird, an, welche allgemeine Berechtigung für das Objekt verwendet wird. Ist der Wert CRTAUT der Bibliothek auf *SYSVAL gesetzt, so wird der im Systemwert QCRTAUT angegebene Wert verwendet, um die allgemeine Berechtigung für das Objekt, das gerade erstellt wird, festzulegen.

Wird der Systemwert QCRTAUT in den Wert *USE oder *EXCLUDE geändert, wird damit der Zugriff auf neu erstellte Objekte eingeschränkt. Der Eigner des Objekts oder der Sicherheitsbeauftragte müssen möglicherweise weitere Berechtigungen erteilen, bevor das Objekt verwendet werden kann. Ein Beispiel dafür ist die Anmeldung an einer neu erstellten Einheit. Wurde die Einheit mit dem Befehl CRTDEVDSP oder durch automatische Konfiguration erstellt, so wird die allgemeine Berechtigung auf *USE oder *EXCLUDE gesetzt. Da die Berechtigung *CHANGE für die Einheitenbeschreibung erforderlich ist, um sich am System anmelden zu können, ist in diesem Fall eine Anmeldung nicht möglich.

Wird der Systemwert QCRTAUT in *ALL geändert, können alle Benutzer des Systems, mit Ausnahme der Benutzer, denen eine stärker einschränkende Berechtigung als *ALL erteilt wurde, die neu erstellten Objekte vollständig steuern. Sie können diese Objekte lesen, ändern, löschen und deren Sicherheit verwalten.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *CHANGE.

Gültige Werte sind:

*CHANGE	Die standardmäßige allgemeine Berechtigung lautet *CHANGE.
*ALL	Die standardmäßige allgemeine Berechtigung lautet *ALL.
*USE	Die standardmäßige allgemeine Berechtigung lautet *USE.
*EXCLUDE	Die standardmäßige allgemeine Berechtigung lautet *EXCLUDE.

9.7.9
Seite 2

9.7.10 QCRTOBJAUD

Objektprotokollierung
Dieser Systemwert gibt den Standardwert für die Protokollierung an, wenn Objekte in einer Bibliothek oder einem Verzeichnis erstellt werden. Lautet der CRTOBJAUD-Wert für die Bibliothek oder das Verzeichnis *SYSVAL, wird der Protokollierungswert für das zu erstellende Objekt durch den Wert festgelegt, der für den Systemwert QCRTOBJAUD angegeben ist.

Der Objektprotokollierungswert legt fest, ob beim Verwenden oder Ändern eines Objekts ein Protokolleintrag an das Systemprotokolljournal QAUDJRN in der Bibliothek QSYS gesendet wird. Der Protokolleintrag wird nur dann an das Systemprotokolljournal gesendet, wenn die Protokollierung im System aktiv ist. Um die Protokollierung zu starten, muss für den Systemwert QAUDCTL ein anderer Wert als *NONE angegeben werden.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NONE.

- Zum Ändern dieses Systemwerts ist die Sonderberechtigung *AUDIT erforderlich.
- Der Benutzer muss entweder über die Sonderberechtigung *ALLOBJ oder über die Sonderberechtigung *AUDIT verfügen, um diesen Systemwert anzuzeigen.

Gültige Werte sind:

*NOTAVL	Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
*NONE	Es werden keine Protokolleinträge beim Verwenden oder Ändern des Objekts gesendet.
*USRPRF	Es werden Protokolleinträge für das Objekt gesendet, das von einem Benutzer verwendet oder geändert wird, der derzeit protokolliert wird. Wird der Benutzer nicht protokolliert, werden auch keine Protokolleinträge gesendet. Um die Aktionen eines Benutzers zu protokollieren, muss sein Benutzerprofil mit dem Befehl CHGUSRAUD (Benutzerprotokollierung ändern) entsprechend geändert werden.
*CHANGE	Es werden Protokolleinträge für das Objekt gesendet, wenn es geändert wird.
*ALL	Es werden Protokolleinträge für das Objekt gesendet, wenn es verwendet oder geändert wird.

9.7.10
Seite 2

9.7.11 QDSPSGNINF

Steuerung der Anmeldeanzeigeinformationen
Dieser Systemwert steuert, ob der Benutzer eine Informationsnachricht angezeigt bekommt, die das Datum und die Uhrzeit der letzten Anmeldung sowie die Anzahl der ungültigen Anmeldeversuche angibt.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Die Anmeldeinformationen werden nicht angezeigt.
1	Die Anmeldeinformationen werden angezeigt.

9.7.12 QFRCCVNRST

Umsetzung beim Zurückspeichern erzwingen
Mit Hilfe dieses Systemwerts kann angegeben werden, ob die folgenden Objekttypen beim Zurückspeichern umgesetzt werden sollen oder nicht:

- Programme (*PGM)
- Serviceprogramme (*SRVPGM)
- SQL-Pakete (*SQLPKG)
- Module (*MODULE).

Dieser Systemwert kann auch verhindern, dass Objekte zurückgespeichert werden. Ein Objekt, das zwar vom System umgesetzt werden soll, dessen Umsetzung aber wegen unzureichender Erstellungsdaten nicht stattfinden kann, wird nicht zurückgespeichert.

Der *SYSVAL-Wert für den Parameter FRCOBJCVN der Rückspeicherungsbefehle (RST, RSTLIB, RSTOBJ, RSTLICPGM) übernimmt den Wert dieses Systemwerts. Durch Ändern des Systemwerts kann daher die Umsetzung für das gesamte System ein- oder ausgeschaltet werden. Der Parameter FRCOBJCVN kann den Systemwert jedoch in einigen Fällen überschreiben. Bei Angabe von *YES und *ALL für den Parameter FRCOBJCVN werden alle Einstellungen des Systemwerts überschrieben. Die Angabe von *YES und *RQD für den Parameter FRCOBJCVN entspricht der Angabe von ‚2' für diesen Systemwert und kann ihn überschreiben, wenn er ‚0' oder ‚1' lautet.

Wenn versucht wird, ein Objekt auf dem System zurückzuspeichern, arbeiten drei Systemwerte gemeinsam als Filter. Sie bestimmen, ob das Objekt zurückgespeichert werden darf oder ob es während der Rückspeicherung konvertiert wird. Der erste Filter ist der Systemwert QVFYOBJRST (Objekt beim Zurückspeichern prüfen). Dieser Systemwert steuert das Zurückspeichern einiger Objekte, die digital signiert werden können. Der zweite Filter ist der Systemwert QFRCCVNRST (Umsetzung beim Zurückspeichern erzwingen). Mit Hilfe dieses Systemwerts kann angegeben werden, ob während des Zurückspeicherns Programme, Serviceprogramme, SQL-Pakete und Modulobjekte konvertiert werden sollen oder nicht. Er kann auch verhindern, dass Objekte zurückgespeichert werden. Vom dritten Filter werden nur Objekte verarbeitet, die die ersten beiden Filter passiert haben. Der dritte Filter ist der Systemwert QALWOBJRST (Zurückspeichern des Objekts erlauben). Er gibt an, ob Objekte mit sicherheitsrelevanten Attributen zurückgespeichert werden können. Der Vorgabewert ist 1.

Bei allen Werten für QFRCCVNRST wird ein Objekt, das umgesetzt werden soll, dessen Umsetzung aber nicht erfolgen kann, nicht zurückgespeichert. Objekte, die über eine gültige Signatur einer vertrauenswürdigen Quelle verfügen, werden ohne Umsetzung der Werte dieses Systemwerts zurückgespeichert.

9.7.12
Seite 2

Gültige Werte sind:

0	Es erfolgt keine Umsetzung. Das Zurückspeichern wird durch nichts verhindert.
1	Objekte mit Gültigkeitsfehlern werden umgesetzt.
2	Objekte, die auf Grund der aktuellen Betriebssystemversion oder des aktuellen Systems umgesetzt werden müssen, werden umgesetzt. Objekte mit Gültigkeitsfehlern werden ebenfalls umgesetzt.
3	Objekte, die möglicherweise manipuliert wurden, Objekte mit Gültigkeitsfehlern und Objekte, die aufgrund der aktuellen Betriebssystemversion oder des aktuellen Systems umgesetzt werden müssen, werden umgesetzt.
4	Objekte, die genügend Erstellungsdaten für die Umsetzung enthalten, und nicht über die gültigen Signaturen verfügen, werden umgesetzt. Ein Objekt, das nicht genügend Erstellungsdaten enthält, wird ohne Umsetzung zurückgespeichert.

Anmerkung:

Objekte (mit oder ohne Signatur), die Gültigkeitsfehler enthalten, die möglicherweise manipuliert wurden oder die aufgrund der aktuellen Betriebssystemversion umgesetzt werden müssen, aber nicht umgesetzt werden können, werden nicht zurückgespeichert.

5	Objekte, die genügend Erstellungsdaten enthalten, werden umgesetzt. Ein Objekt, das nicht genügend Erstellungsdaten enthält, wird zurückgespeichert.

Anmerkung:

Objekte, die Gültigkeitsfehler enthalten, die möglicherweise manipuliert wurden oder die aufgrund der aktuellen Betriebssystemversion umgesetzt werden müssen, aber nicht umgesetzt werden können, werden nicht zurückgespeichert.

6	Alle Objekte ohne gültige digitale Signatur werden umgesetzt.

Anmerkung:

Ein Objekt mit einer gültigen digitalen Signatur, das außerdem Gültigkeitsfehler enthält, das möglicherweise manipuliert wurde oder das aufgrund der aktuellen Betriebssystemversion umgesetzt werden muss, aber nicht umgesetzt werden kann, wird nicht zurückgespeichert.

7 Jedes Objekt wird umgesetzt.

Wenn ein Objekt umgesetzt wird, wird seine digitale Signatur gelöscht. Das umgesetzte Objekt erhält den Benutzerstatus. Nach der Umsetzung haben Objekte einen fehlerlosen Gültigkeitswert und stehen nicht mehr im Verdacht, manipuliert worden zu sein.

9.7.13 QINACTITV

Zeitlimit für inaktiven Job
QINACTITV gibt an, wann das System bei nicht aktiven interaktiven Jobs eine Maßnahme ergreift. Der Systemwert QINACTMSGQ bestimmt die jeweils zu treffende Maßnahme. Weitere Informationen über das Erzwingen des Durchgriffs auf das Ziel und über TELNET-Sitzungen enthält das Handbuch Work Management. Lokale Jobs, die gegenwärtig an einem fernen System angemeldet sind, sind davon nicht betroffen.

Beispiel: Eine Datenstation ist direkt an System A angeschlossen, für das QINACTIV angegeben wurde. Wenn die Anmeldung an System B mit Datensichtgerätedurchgriff oder TELNET erfolgt, hat der in System A gesetzte Wert QINACTIV auf diese Datenstation keine Auswirkung. Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NONE.

Gültige Werte sind:

*NONE	Das System überprüft nicht, ob nicht aktive interaktive Jobs vorhanden sind.
5–300	Die Anzahl Minuten, die ein Job inaktiv sein kann, ehe eine entsprechende Maßnahme ergriffen wird.

9.7.14 QLMTDEVSSN

Einheitensitzungen begrenzen
Über diesen Systemwert wird die Anzahl der Einheitensitzungen gesteuert, bei denen sich ein Benutzer anmelden kann. Dabei wird nicht verhindert, dass der Benutzer an derselben Datenstation Gruppenjobs verwendet oder eine Systemanfrage durchführt (Taste für Systemanfrage). Der Vorgabewert ist 0.

Gültige Werte sind:

0	Benutzer sind nicht auf eine bestimmte Anzahl von Einheitensitzungen beschränkt.
1–9	Gibt die maximale Anzahl der gleichzeitig ablaufenden Einheitensitzungen an.

9.7.15 QLMTSECOFR

Einheitenzugriff des Sicherheitsbeauftragten begrenzen
Dieser Systemwert steuert, ob Benutzer mit den Sonderberechtigungen *ALLOBJ oder *SERVICE ausdrückliche Berechtigungen für bestimmte Datenstationen benötigen.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 1.

Anmerkung:

Zum Ändern dieses Systemwerts sind die Sonderberechtigungen *ALLOBJ und *SECADM erforderlich.

Gültige Werte sind:

0	Benutzer mit der Sonderberechtigung *ALLOBJ oder *SERVICE können sich an jeder Datenstation anmelden.
1	Benutzer mit der Sonderberechtigung *ALLOBJ oder *SERVICE können sich nur an der Einheit anmelden, für die sie eine ausdrückliche Berechtigung besitzen.

9.7.16 QMAXSGNACN

Maßnahme bei fehlgeschlagenen Anmeldeversuchen
Wird bei Erreichen der maximal zulässigen Anzahl Anmeldeversuche ausgeführt. Gibt an, wie das System reagiert, wenn die maximal zulässige Anzahl aufeinanderfolgender ungültiger Anmeldeversuche (Systemwert QMAXSIGN) erreicht ist.

Eine Änderung dieses Systemwerts wird beim nächsten Anmeldeversuch eines Benutzers am System wirksam. Der Vorgabewert ist ‚3'.

Gültige Werte sind:

1	Bei Erreichen des Grenzwerts wird die Einheit abgehängt.
2	Bei Erreichen des Grenzwerts wird das Benutzerprofil inaktiviert.
3	Bei Erreichen des Grenzwerts wird die Einheit abgehängt und das Benutzerprofil inaktiviert.

9.7.16
Seite 2

9.7.17 QMAXSIGN

Maximal zulässige Anmeldeversuche
Ungültige Anmeldeversuche bei gesicherten Systemen (Sicherheitsstufe 20 oder höher, siehe Systemwert QSECURITY) können folgende Ursachen haben:

- Falsche Benutzer-ID
- Falsches Kennwort

Das Benutzerprofil hat keine Berechtigung für die Einheit, an der die Benutzer-ID eingegeben wurde.

Anmerkung:

Ein Anmeldeversuch wird nicht als ungültiger Versuch gewertet, wenn Kennwörter erforderlich sind und für das Benutzerprofil das Kennwort *NONE angegeben ist. Der Benutzer erhält die Nachricht, dass diesem Benutzerprofil kein Kennwort zugeordnet ist. Auch wenn der Programm- oder Menüname ungültig ist, wenn die Benutzer-ID in einem nicht gesicherten System ungültig ist, wenn die aktuelle Bibliothek nicht gefunden werden kann oder wenn das Benutzerprofil keine *AUDIT-Berechtigung enthält und der Versuch stattfindet, nachdem aufgrund eines Protokollierungsfehlers ein IPL für das System durchgeführt wurde, wird der Anmeldeversuch nicht als ungültig bewertet.

Ist der maximale Wert von QMAXSIGN erreicht, wird die durch den Systemwert QMAXSGNACN festgelegte Maßnahme ausgeführt. Die Datenstation wird abgehängt und/oder das Benutzerprofil inaktiviert. Eine Nachricht wird an die Nachrichtenwarteschlange QSYSMSG gesendet, vorausgesetzt, diese Warteschlange ist vorhanden; andernfalls wird die Nachricht an QSYSOPR gesendet. Wird ein Profil inaktiviert, muss es vor dem Anmelden eines Benutzers wieder aktiviert werden. Wird eine Einheit abgehängt, muss diese vor dem Anmelden eines Benutzers wieder angehängt werden. Befindet sich das Steuersubsystem im eingeschränkten Status (so dass nur eine Einheit in diesem System verwendet werden kann) und wird die Einheit abgehängt, wird das System beendet und die eingeschalteten Lampen an der Steuerkonsole zeigen an, dass ein IPL durchgeführt werden muss.

Liegt die Anzahl der ungültigen Anmeldeversuche um 1 niedriger als der Wert für QMAXSIGN, wird eine Nachricht angezeigt. Diese Nachricht warnt den Benutzer, dass bei einem weiteren ungültigen Anmeldeversuch die im Systemwert QMAXSGNACN angegebene Maßnahme ausgeführt wird.

9.7.17
Seite 2

Eine Änderung dieses Systemwerts wird wirksam, wenn sich der nächste Benutzer am System anmeldet. Der Vorgabewert ist 3.

Gültige Werte sind:

1–25	Maximale Anzahl zulässiger Anmeldeversuche
*NOMAX	Es gibt keine maximale Anzahl zulässiger Anmeldeversuche.

9.7.18 QPWDCHGBLK

Kennwortänderung blockieren
Gibt an, wie lange die Änderung eines Kennworts nach einer erfolgreichen Kennwortänderung blockiert ist. Kennwortänderungen, die mit dem Befehl CHGUSRPRF (Benutzerprofil ändern) erfolgen, werden durch diesen Systemwert nicht eingeschränkt.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NONE.

Gültige Werte sind:

*NONE	Der Benutzer kann das Kennwort beliebig oft ändern. Es gibt keine Einschränkung.
1-99	Zeigt an, wie viele Stunden der Benutzer nach einer erfolgreichen Kennwortänderung warten muss, bevor er das Kennwort erneut ändern darf.

9.7.18
Seite 2

9.7.19 QPWDEXPITV

Intervall für Kennwortablauf
Gibt die Anzahl der Tage an, die ein Kennwort gültig ist. Das ermöglicht Kennwortsicherheit, da die Benutzer gezwungen sind, ihr Kennwort nach einer bestimmten Anzahl Tage zu ändern. Wenn das Kennwort innerhalb dieser Frist nicht geändert wird, kann sich der Benutzer nicht anmelden.

Sieben Tage vor Ablauf des Kennworts erhält der Benutzer beim Anmelden eine entsprechende Warnmeldung, auch wenn die Anmeldeinformationen nicht angezeigt werden (Systemwert QDSPSGNINF).

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NOMAX.

Gültige Werte sind:

*NOMAX	Ein Kennwort kann eine unbegrenzte Anzahl von Tagen verwendet werden.
1-366	Die Anzahl der Tage, bevor das Kennwort ungültig wird.

9.7.20 QPWDEXPWRN

Warnung vor Kennwortablauf
Steuert, wie viele Tage vor dem Kennwortablauf mit der Anzeige einer entsprechenden Warnung auf dem Anmeldebildschirm begonnen wird.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 7.

Gültige Werte sind:

1-99	Gibt an, wie viele Tage vor Kennwortablauf mit der Anzeige einer entsprechenden Warnung auf dem Anmeldebildschirm begonnen wird.

9.7.20
Seite 2

9.7.21 QPWDLMTAJC

Zusammenhängende Ziffern in Kennwort begrenzen
Gibt an, ob in Kennwörtern aufeinanderfolgende Ziffern erlaubt sind. Wenn die Verwendung von Datumsangaben und Sozialversicherungsnummern unzulässig ist, ist es schwieriger, ein Kennwort zu erraten.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Aufeinanderfolgende Ziffern sind zulässig.
1	Aufeinanderfolgende Ziffern sind nicht zulässig.

9.7.22 QPWDLMTCHR

Zeichen in Kennwort begrenzen
Kennwortsicherheit kann erreicht werden, wenn bestimmte Zeichen (z. B. Großbuchstaben) in Kennwörtern verboten sind. Da keine allgemein gebräuchlichen Wörter oder Begriffe eingegeben werden können, ist es schwierig, das Kennwort zu erraten.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist *NONE.

Gültige Werte sind:

*NONE	Es gibt keine unzulässigen Zeichen.
eingeschränkte Zeichen	Es können bis zu zehn eingeschränkte Zeichen angegeben werden. Gültige Zeichen für das Kennwort sind: A–Z, 0–9 und die Sonderzeichen #, $, das Unterstreichungszeichen (_) sowie §.

Anmerkung:

0123456789 kann nicht angegeben werden, wenn in einem Kennwort Zahlen erforderlich sind (siehe Systemwert QPWDRQDDGT).

Dieser Systemwert wird ignoriert, wenn das System mit QPWDLVL 2 bzw. 3 arbeitet.

Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.23 QPWDLMTREP

Zeichenwiederholung in Kennwort begrenzen
Damit wird verhindert, dass in einem Kennwort dasselbe Zeichen mehrmals verwendet wird (beispielsweise AAAA).

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Zeichen können mehrmals verwendet werden.
1	Zeichen können nur einmal verwendet werden.
2	Zeichen können nicht fortlaufend verwendet werden.

Anmerkung:

Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.24 QPWDLVL

Kennwortstufe
Gibt die Stufe für die Kennwortunterstützung im System an.

Die Kennwortstufe des Systems kann dahingehend festgelegt werden, dass Benutzerprofilkennwörter mit 1–10 Zeichen bzw. 1–128 Zeichen verwendet werden.

Die Kennwortstufe kann dahingehend festgelegt werden, dass eine ‚Kennphrase' als Kennwortwert verwendet wird. Der Begriff ‚Kennphrase' wird zuweilen in der Computerbranche verwendet, um einen Kennwortwert zu beschreiben, für den wenige bzw. keine Einschränkungen hinsichtlich der Zeichenlänge gelten. In einer Kennphrase können Leerzeichen zwischen einzelnen Zeichen verwendet werden. Das ermöglicht, dass ein Satz oder ein Satzteil als Kennwortwert verwendet werden kann.

Beim Ändern der Kennwortstufe des Systems von 1–10 Zeichen lange in 1–128 Zeichen lange Kennwörter ist Vorsicht geboten. Ist das System z. B. mit anderen Systemen in einem Netzwerk verbunden, müssen alle Systeme in der Lage sein, die längeren Kennwörter zu verarbeiten.

Im Handbuch System i Security Reference, IBM Form SC41-5302, werden weitere Überlegungen erläutert, die vor dem Ändern dieses Systemwerts angestellt werden sollten.

Eine Änderung dieses Systemwerts wird beim nächsten IPL wirksam. Um den aktuellen und den anstehenden Wert der Kennwortstufe anzuzeigen, wird der CL-Befehl DSPSECA (Sicherheitsattribute anzeigen) verwendet. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Das System unterstützt Benutzerprofilkennwörter mit einer Länge von 1–10 Zeichen. Die zulässigen Zeichen sind A–Z, 0–9 und die Zeichen $, §, # sowie das Unterstreichungszeichen. QPWDLVL 0 sollte verwendet werden, wenn das System mit anderen IBM i-Systemen in einem Netzwerk verbunden ist und diese Systeme entweder mit dem QPWDLVL-Wert 0 oder mit einem Betriebssystem-Release vor V5R1M0 ausgeführt werden. QPWDLVL 0 sollte verwendet werden, wenn das System mit einem anderen System, das die Kennwortlänge auf 1–10 Zeichen beschränkt, Daten austauscht.

9.7.24
Seite 2

QPWDLVL 0 muss verwendet werden, wenn das System mit Windows 95/98/ME-Unterstützung für Windows Network Neighborhood (i5/OS NetServer) und mit anderen Systemen, die Kennwörter mit einer Länge von 1–10 Zeichen verwenden, Daten austauscht.

Ist der QPWDLVL-Wert des Systems 0, erstellt das Betriebssystem das verschlüsselte Kennwort für QPWDLVL 2 und 3. Der Wert des Kennworts ist dem Benutzerprofilkennwort gleich.

1 QPWDLVL 1 entspricht der Unterstützung von QPWDLVL 0 mit der folgenden Ausnahme: Auf dem System gespeicherte Kennwörter, die mit Windows 95/98/ME-Unterstützung für Windows Network Neighborhood (i5/OS NetServer) verwendet werden sollen, werden im System gelöscht. Wird die Client-Unterstützung für i5/OS NetServer verwendet, ist die Verwendung des QPWDLVL-Werts 1 nicht möglich.

QPWDLVL 1 verbessert die Sicherheit des Systems, da alle Kennwörter für i5/OS NetServer im System gelöscht werden.

2 Das System unterstützt Benutzerprofilkennwörter mit einer Länge von 1–128 Zeichen. Zeichen in Groß- und Kleinbuchstaben sind zulässig. Das Kennwort kann aus beliebigen Zeichen bestehen. Die Groß- und Kleinschreibung des Kennworts muss beachtet werden.

QPWDLVL 2 wird als Kompatibilitätsstufe betrachtet. Die Kennwörter werden zur Authentifizierung von Anmeldevorgängen und anderen Kennworttests verwendet. Diese Stufe ermöglicht auch eine Rückkehr zu QPWDLVL 0 oder 1, vorausgesetzt, dass das jeweilige Kennwort den Längen- und Syntaxvorgaben von QPWDLVL 0 bzw. 1 entspricht.

QPWDLVL 2 kann verwendet werden, wenn das System mit der Windows 95/98/ME-Unterstützung für Windows Network Neighborhood (i5/OS NetServer) Daten austauscht, vorausgesetzt, das Kennwort ist 1–14 Zeichen lang.

QPWDLVL 2 kann nicht verwendet werden, wenn das System mit anderen Systemen in einem Netzwerk verbunden ist und diese Systeme entweder mit dem QPWDLVL-Wert 0 bzw. 1 oder mit einem Betriebssystem-Release vor V5R1M0 ausgeführt werden.

QPWDLVL 2 kann nicht verwendet werden, wenn das System mit einem anderen System, das die Kennwortlänge auf 1–10 Zeichen beschränkt, Daten austauscht.

3 Das System unterstützt Benutzerprofilkennwörter mit einer Länge von 1–128 Zeichen. Zeichen in Groß- und Kleinbuchstaben sind zulässig. Das Kennwort kann aus beliebigen Zeichen bestehen. Die Groß- und Kleinschreibung des Kennworts muss beachtet werden.

In der Veröffentlichung System i Security Reference, IBM Form SC41-5302, werden weitere Überlegungen erläutert, die vor dem Ändern der Kennwortstufe auf 3 angestellt werden sollten. Es ist nicht zulässig, QPWDLVL 3 wieder in 0 zu ändern.

QPWDLVL 3 kann nicht verwendet werden, wenn das System mit anderen Systemen in einem Netzwerk verbunden ist und diese Systeme entweder mit dem QPWDLVL-Wert 0 bzw. 1 oder mit einem Betriebssystem-Release vor V5R1M0 ausgeführt werden.

QPWDLVL 3 kann nicht verwendet werden, wenn das System mit einem anderen System, das die Kennwortlänge auf 1–10 Zeichen beschränkt, Daten austauscht.

QQPWDLVL 3 kann nicht verwendet werden, wenn das System mit der Windows 95/98/ME-Unterstützung für Windows Network Neighborhood (i5/OS NetServer) Daten austauscht.

9.7.25 QPWDMAXLEN

Maximale Kennwortlänge
Gibt die maximale Anzahl Zeichen pro Kennwort an.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 8.

Gültige Werte sind:

1–128	Die maximale Anzahl Zeichen, die für ein Kennwort zulässig ist.Wenn das System mit QPWDLVL 0 oder 1 arbeitet, sind 1–10 Zeichen zulässig. Wenn das System mit QPWDLVL 2 oder 3 arbeitet, sind 1–128 Zeichen zulässig.

Anmerkung:

Die maximale Kennwortgröße kann die im Systemwert QPWDMINLEN angegebene Mindestgröße nicht unterschreiten.

Anmerkung:

Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.25
Seite 2

9.7.26 QPWDMINLEN

Mindestkennwortlänge
Gibt die Mindestanzahl Zeichen für ein Kennwort an.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 6.

Gültige Werte sind:

1–128	Die Mindestanzahl von Zeichen für ein Kennwort. Wenn das System mit QPWDLVL 0 oder 1 arbeitet, sind 1–10 Zeichen zulässig. Wenn das System mit QPWDLVL 2 oder 3 arbeitet, sind 1–128 Zeichen zulässig.

Anmerkung:

Die Mindestgröße des Kennworts kann die im Systemwert QPWDMAXLEN angegebene maximale Kennwortgröße nicht überschreiten. Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.26
Seite 2

9.7.27 QPWDPOSDIF

Zeichenpositionen in Kennwort begrenzen
Dieser Systemwert kontrolliert die Position der Zeichen in einem neuen Kennwort. Damit wird verhindert, dass der Benutzer ein Kennwort angibt, das größtenteils mit dem alten Kennwort übereinstimmt. Beispielsweise könnte das Kennwort DJS2 nicht verwendet werden, wenn das vorhergehende DJS1 gelautet hat (D, J und S stehen an derselben Stelle).

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Es ist möglich, im neuen Kennwort das gleiche Zeichen an dieselbe Stelle zu setzen wie im vorhergehenden Kennwort.
1	Ein bestimmtes Zeichen kann nicht an dieselbe Stelle wie im vorhergehenden Kennwort gesetzt werden. Beispielsweise könnte das Kennwort DJS2 nicht verwendet werden, wenn das vorhergehende DJS1 gelautet hat (D, J und S stehen an derselben Stelle).

Anmerkung:

Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.27
Seite 2

9.7.28 QPWDRQDDGT

Ziffer in Kennwort erforderlich
Gibt an, ob in einem neuen Kennwort eine Ziffer erforderlich ist. Damit wird verhindert, dass der Benutzer nur Buchstaben verwendet.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Es sind keine Ziffern erforderlich.
1	Eine bzw. mehrere Ziffern sind erforderlich.

Anmerkung:

0123456789 ist als Angabe für den Systemwert QPWDLMTCHR nicht erlaubt, wenn in einem Kennwort Zahlen erforderlich sind.

Wenn im Systemwert QPWDRULES ein anderer Wert als *PWDSYSVAL angegeben ist, wird dieser Systemwert bei der Prüfung neuer Kennwörter auf Formatfehler ignoriert.

9.7.28
Seite 2

9.7.29 QPWDRQDDIF

Kontrolle auf doppelte Kennwörter
Dieser Systemwert begrenzt die Häufigkeit der Verwendung eines Kennworts.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist 0.

Gültige Werte sind:

0	Das Kennwort kann mit dem vorhergehenden identisch sein.
1	Ein Kennwort muss sich von den 32 vorhergehenden Kennwörtern unterscheiden.
2	Das Kennwort muss sich von den vorhergehenden 24 Kennwörtern unterscheiden.
3	Das Kennwort muss sich von den vorhergehenden 18 Kennwörtern unterscheiden.
4	Das Kennwort muss sich von den vorhergehenden zwölf Kennwörtern unterscheiden.
5	Das Kennwort muss sich von den vorhergehenden zehn Kennwörtern unterscheiden.
6	Das Kennwort muss sich von den vorhergehenden acht Kennwörtern unterscheiden.
7	Das Kennwort muss sich von den vorhergehenden sechs Kennwörtern unterscheiden.
8	Das Kennwort muss sich von den vorhergehenden vier Kennwörtern unterscheiden.

9.7.29
Seite 2

9.7.30 QPWDRULES

Kennwortregeln
Gibt die Regeln an, die zur Überprüfung eines Kennworts auf Formatfehler verwendet werden.

Änderungen dieses Systemwerts werden bei der nächsten Kennwortänderung wirksam. Der Vorgabewert ist *PWDSYSVAL.

Gültige Werte sind:

*PWDSYSVAL — Dieser Systemwert wird ignoriert, und alle anderen Kennwortsystemwerte werden zur Überprüfung eines Kennworts auf Formatfehler verwendet. Speziell die Systemwerte QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF und QPWDRQDDGT werden statt des Systemwerts QPWDRULES verwendet.

Anmerkung:

Wenn ein anderer Wert als *PWDSYSVAL für QPWDRULES angegeben wird, werden die Systemwerte QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF und QPWDRQDDGT ignoriert, wenn ein neues Kennwort auf Formatfehler überprüft wird.

*CHRLMTAJC — Das Kennwort darf keine identischen aufeinanderfolgenden Zeichen enthalten. Dieser Wert kann nicht angegeben werden, wenn der Wert *CHRLMTREP angegeben wurde.

*CHRLMTREP — Jedes Zeichen darf nur einmal im Kennwort enthalten sein. Dieser Wert kann nicht angegeben werden, wenn der Wert *CHRLMTAJC angegeben wurde.

*DGTLMTAJC — Das Kennwort darf keine identischen aufeinanderfolgenden Ziffern enthalten.

*DGTLMTFST — Als erstes Zeichen des Kennworts darf keine Ziffer verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *LTRLMTFST und *SPCCHRLMTFST angegeben wurden.

*DGTLMTLST — Als letztes Zeichen des Kennworts darf keine Ziffer verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *LTRLMTLST und *SPCCHRLMTLLST angegeben wurden.

9.7.30
Seite 2

*DGTMAXn	n steht für eine Zahl von 0 bis 9. Gibt die maximale Anzahl Ziffern an, die das Kennwort enthalten darf. Der Wert *DGTMAXn kann nur einmal angegeben werden. Wenn der Wert *DGTMINn ebenfalls angegeben wird, muss der für *DGTMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *DGTMINn angegeben wurde.
*DGTMINn	n steht für eine Zahl von 0 bis 9. Gibt die Mindestanzahl Ziffern an, die ein Kennwort enthalten muss. Der Wert *DGTMINn kann nur einmal angegeben werden. Wenn *DGTMAXn ebenfalls angegeben wird, muss der für *DGTMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *DGTMINn angegeben wurde.
*LMTSAMPOS	Ein bestimmtes Zeichen kann nicht an dieselbe Stelle wie im vorhergehenden Kennwort gesetzt werden.
*LMTPRFNAME	Das Kennwort in Großbuchstaben darf nicht den vollständigen Namen des Benutzerprofils (in aufeinanderfolgenden Positionen) enthalten.
*LTRLMTAJC	Das Kennwort darf keine identischen aufeinanderfolgenden Buchstaben enthalten.
*LTRLMTFST	Als erstes Zeichen des Kennworts darf kein Buchstabe verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *DGTLMTFST und *SPCCHRLMTFST angegeben wurden. Wenn das System mit einem Wert von 0 oder 1 für QPWDLVL arbeitet, können die beiden Werte *LTRLMTFST und *SPCCHRLMTFST nicht zusammen angegeben werden.
*LTRLMTLST	Als letztes Zeichen des Kennworts darf kein Buchstabe verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *DGTLMTLST und *SPCCHRLMTLST angegeben wurden.
*LTRMAXn	n steht für eine Zahl von 0 bis 9. Gibt die maximale Anzahl Buchstaben an, die das Kennwort enthalten darf. Der Wert *LTRMAXn kann nur einmal angegeben werden. Wenn der Wert *LTRMINn ebenfalls angegeben wird, muss der für *LTRMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *LTRMINn angegeben wurde.

*LTRMINn	n steht für eine Zahl von 0 bis 9. Gibt die Mindestanzahl Buchstaben an, die ein Kennwort enthalten muss. Der Wert *LTRMINn kann nur einmal angegeben werden. Wenn *LTRMAXn ebenfalls angegeben wird, muss der für *LTRMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *LTRMINn angegeben wurde.
*MAXLENnnn	nnn steht für eine Zahl von 1 bis 128 (ohne führende Nullen), die maximale Anzahl Zeichen pro Kennwort. Wenn das System mit QPWDLVL 0 oder 1 arbeitet, sind 1–10 Zeichen zulässig. Wenn das System mit QPWDLVL 2 oder 3 arbeitet, sind 1–128 Zeichen zulässig. Der angegebene nnn-Wert muss groß genug sein, um die Werte für *MIXCASEn, *DGTMAXn, *LTRMAXn, *SPCCHRMAXn aufzunehmen und die Einschränkungen bezüglich dem ersten und dem letzten Zeichen sowie die Anforderung bezüglich nicht aufeinanderfolgenden Zeichen zu erfüllen. Wenn *MINLENnnn ebenfalls angegeben wird, muss der für *MAXLENnnn angegebene nnn-Wert größer oder gleich dem nnn-Wert sein, der für *MINLENnnn angegeben wurde. Wurde der Wert *MAXLENnnn nicht angegeben, wird der Wert *MAXLEN10 angenommen, wenn das System mit einem Wert von 0 oder 1 für QPWDLVL arbeitet, oder *MAXLEN128, wenn das System mit einem Wert von 2 oder 3 für QPWDLVL arbeitet.
*MINLENnnn	nnn steht für eine Zahl von 1 bis 128 (ohne führende Nullen), die Mindestanzahl Zeichen für ein Kennwort. Wenn das System mit QPWDLVL 0 oder 1 arbeitet, sind 1–10 Zeichen zulässig. Wenn das System mit QPWDLVL 2 oder 3 arbeitet, sind 1–128 Zeichen zulässig. Wenn *MAXLENnnn ebenfalls angegeben wird, muss der für *MAXLENnnn angegebene nnn-Wert größer oder gleich dem nnn-Wert sein, der für *MINLENnnn angegeben wurde. Wird kein Wert für *MINLENnnn angegeben, wird der Wert 0 angenommen.

*MIXCASEn	n steht für eine Zahl von 0 bis 9. Das Kennwort muss mindestens n Großbuchstaben und n Kleinbuchstaben enthalten Dieser Wert wird zurückgewiesen, wenn das System mit einem Wert von 0 oder 1 für QPWDLVL arbeitet, da Kennwörter in Großbuchstaben angegeben werden müssen. Der Wert *MIXCASEn kann nur einmal angegeben werden. Wenn *LTRMAXn angegeben wird, muss der für *LTRMAXn angegebene n-Wert größer oder gleich dem zweifachen n-Wert sein, der für *MIXCASEn angegeben wurde.
*REQANY3	Das Kennwort muss Zeichen aus mindestens drei der folgenden vier Zeichenarten enthalten. · Großbuchstaben · Kleinbuchstaben · Ziffern · Sonderzeichen Wenn das System mit einem Wert von 0 oder 1 für QPWDLVL arbeitet, hat *REQANY3 dieselbe Auswirkung als ob *DGTMIN1, *LTRMIN1, und *SPCCHRMIN1 zusammen angegeben worden wären.
*SPCCHRLMTAJC	Das Kennwort darf keine identischen aufeinanderfolgenden Sonderzeichen enthalten.
*SPCCHRLMTFST	Als erstes Zeichen des Kennworts darf kein Sonderzeichen verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *DGTLMTFST und *LTRLMTFST ebenfalls angegeben wurden. Wenn das System mit einem Wert von 0 oder 1 für QPWDLVL arbeitet, können die beiden Werte *LTRLMTFST und *SPCCHRLMTFST nicht zusammen angegeben werden.
*SPCCHRLMTLST	Als letztes Zeichen des Kennworts darf kein Sonderzeichen verwendet werden. Dieser Wert kann nicht angegeben werden, wenn die Werte *DGTLMTLST und *LTRLMTLST angegeben wurden.

*SPCCHRMAXn	n steht für eine Zahl von 0 bis 9. Gibt die maximale Anzahl Sonderzeichen an, die das Kennwort enthalten darf. Der Wert *SPCCHRMAXn kann nur einmal angegeben werden. Wenn *SPCCHRMINn ebenfalls angegeben wird, muss der für *SPCCHRMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *SPCCHRMINn angegeben wurde.
*SPCCHRMINn	n steht für eine Zahl von 0 bis 9 und gibt die Mindestanzahl Sonderzeichen an, die ein Kennwort enthalten muss. Der Wert *SPCCHRMINn kann nur einmal angegeben werden. Wenn *SPCCHRMAXn ebenfalls angegeben wird, muss der für *SPCCHRMAXn angegebene n-Wert größer oder gleich dem n-Wert sein, der für *SPCCHRMINn angegeben wurde.

32. Ergänzung 9/2012

9.7.30
Seite 6

9.7.31 QPWDVLDPGM

Kennwortprüfprogramm
Damit wird den vom Benutzer geschriebenen Programmen ermöglicht, zusätzliche Kennwortprüfungen durchzuführen. Das Programm muss im System-ASP (ASP = Zusatzspeicherpool) oder in einem Basis-Benutzer-ASP vorhanden sein.

Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung

wirksam. Der Vorgabewert ist *NONE.

Gültige Werte sind:

*NONE	Es wird kein Kennwortprüfprogramm verwendet.
*REGFAC	Das Kennwortprüfprogramm wird von der Registrierungsfunktion abgerufen.
Programm-spezifikation	Der Name des Kennwortprüfprogramms. Diese Auswahl ist nur gültig, wenn das System mit QPWDLVL 0 bzw. 1 arbeitet.

Gültige Bibliothekswerte sind:

*LIBL	Das Kennwortprüfprogramm wird in der Bibliotheksliste gesucht.
*CURLIB	Das Kennwortprüfprogramm wird in der aktuellen Jobbibliothek gesucht. Ist keine aktuelle Bibliothek für den Job angegeben, wird QGPL verwendet.
Bibliotheksname	Den Namen der Bibliothek angeben, in der sich das Kennwortprüfprogramm befindet.

Anmerkung:

Aktuelles und neues Kennwort werden unverschlüsselt an das Prüfprogramm übermittelt. Das Prüfprogramm könnte Kennwörter in einer Datenbankdatei speichern und die Sicherheit im System beeinträchtigen.

Die empfohlene Einstellung für diesen Systemwert ist *NONE.

9.7.31
Seite 2

9.7.32 QRETSVRSEC

Server-Sicherheitsdaten sichern
Gibt an, ob die von einem Server benötigten Sicherheitsdaten zur Authentifizierung eines Benutzers auf einem Zielsystem über Client-Server-Schnittstellen auf dem Host-System gesichert werden können.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 0.

Der Systemwert QRETSVRSEC kann nur mit den Sonderberechtigungen *ALLOBJ und *SECADM geändert werden.

Gültige Werte sind:

0	Server-Sicherheitsdaten nicht sichern
1	Server-Sicherheitsdaten sichern

9.7.32

Seite 2

9.7.33 QRMTSIGN

Ferne Anmeldesteuerung
Dieser Systemwert gibt an, wie das System ferne Anmeldeanforderungen behandelt.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *FRCSIGNON.

Alle Werte werden wie unten beschrieben für Datenstationsdurchgriff, System i Navigator Work Station Function (WSF) und andere 5250-Emulationsprogramme auf programmierbaren Datenstationen unterstützt. Weitere Informationen über die Unterstützungsebene für TELNET-Sitzungen enthält das Handbuch Work Management.

Gültige Werte sind:

*FRCSIGNON	Alle fernen Sitzungen müssen sich der normalen Anmeldeprozedur unterziehen.
*SAMEPRF	Wenn Quellen- und Zielname des Benutzerprofils identisch sind, wird die Anmeldung möglicherweise umgangen und ferne Anmeldeversuche werden bearbeitet.
*REJECT	Es ist keine ferne Anmeldung zulässig.
*VERIFY	Nachdem geprüft wurde, ob der Benutzer zugriffsberechtigt ist, erlaubt das System eine Umgehung der Anmeldeprozedur.

9.7.33
Seite 2

9.7.34 QSCANFS

Dateisysteme prüfen
Dieser Systemwert gibt das integrierte Dateisystem an, dessen Objekte überprüft werden, wenn Exitprogramme mit einem der prüfungsbezogenen Exitpunkte des integrierten Dateisystems registriert werden.

Die prüfungsbezogenen IFS-Exitpunkte sind:
- QIBM_QP0L_SCAN_OPEN – IFS-Prüfung beim Öffnen des Exitprogramms
- QIBM_QP0L_SCAN_CLOSE – IFS-Prüfung beim Schließen des Exitprogramms

Weitere Informationen über Exitpunkte sind im Handbuch API-Themensammlung in der Kategorie Programmierung im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/ zu finden.

Anmerkung:

Zum Ändern dieses Systemwerts sind die Sonderberechtigungen

*ALLOBJ und *SECADM erforderlich.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *ROOTOPNUD. Um die Überprüfung auszuschalten, *NONE angeben.

Gültige Werte sind:

*NONE	Es werden keine Objekte des integrierten Dateisystems überprüft.
*ROOTOPNUD	Objekte vom Typ *STMF, die sich in *TYPE2-Verzeichnissen der Root(/) befinden, QOpenSys und benutzerdefinierte Dateisysteme werden überprüft.

9.7.34
Seite 2

9.7.35 QSCANFSCTL

Prüfung der Dateisysteme steuern
Dieser Systemwert steuert die Überprüfung des integrierten Dateisystems auf dem System, wenn Exitprogramme mit einem der prüfungsbezogenen Exitpunkte des integrierten Dateisystems registriert werden.

Die prüfungsbezogenen IFS-Exitpunkte sind:
- QIBM_QP0L_SCAN_OPEN – IFS-Prüfung beim Öffnen des Exitprogramms
- QIBM_QP0L_SCAN_CLOSE – IFS-Prüfung beim Schließen des Exitprogramms

Weitere Informationen über Exitpunkte sind im Handbuch API-Themensammlung in der Kategorie Programmierung im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/ zu finden.

Anmerkung:

Zum Ändern dieses Systemwerts sind die Sonderberechtigungen *ALLOBJ und *SECADM erforderlich.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *NONE.

Einen oder mehrere der folgenden Werte angeben. Bei Angabe von *NONE ist kein weiterer Wert mehr zulässig.

Gültige Werte sind:

*NONE	Es werden keine Steuerelemente für die prüfungsbezogen Exitpunkte des integrierten Dateisystems angegeben.
*ERRFAIL	Treten beim Aufrufen des Exitprogramms Fehler auf (z. B.: „Programm nicht gefunden“ oder „Exitprogramm meldet Fehler“), bricht das System die Anforderung ab, die den Programmaufruf ausgelöst hat. Wenn diese Option nicht angegeben wird, übergeht das System das Exitprogramm und behandelt es so, als würde das Objekt nicht überprüft.
*FSVRONLY	Es werden nur Zugriffe über die Dateiserver überprüft. Es werden z. B. sowohl Zugriffe über das Network File System als auch andere Dateiservermethoden überprüft. Wenn diese Option nicht angegeben wird, werden alle Zugriffe überprüft.

*NOFAILCLO	Anforderungen zum Schließen werden vom System nicht mit einem Prüffehler abgebrochen; das gilt auch dann, wenn das Objekt eine Überprüfung abgebrochen hat, die als Bestandteil der Abschlussoperation durchgeführt wurde. Dieser Wert überschreibt außerdem die *ERRFAIL-Spezifikation für die Abschlussverarbeitung, nicht jedoch für alle anderen prüfungsbezogenen Exitpunkte.
*NOPOSTRST	Nachdem Objekte zurückgespeichert wurden, werden sie nicht allein aus dem Grund überprüft, weil sie zurückgespeichert wurden. Wenn das Objektattribut besagt, dass „das Objekt nicht überprüft wird“, findet zu keiner Zeit eine Überprüfung statt. Wenn das Objektattribut besagt, dass „das Objekt nur überprüft wird, wenn es seit der letzten Überprüfung geändert wurde“, findet eine Überprüfung nur statt, falls es nach dem Zurückspeichern geändert wurde. Wenn *NOPOSTRST nicht angegeben wird, werden die Objekte nach dem Zurückspeichern mindestens ein Mal überprüft. Wenn das Objektattribut besagt, dass „das Objekt nicht überprüft wird“, findet nach dem Zurückspeichern einmal eine Überprüfung statt. Wenn das Objektattribut besagt, dass „das Objekt nur überprüft wird, wenn es seit der letzten Überprüfung geändert wurde“, findet nach dem Zurückspeichern eine Überprüfung statt, da das Zurückspeichern als Änderung am Objekt gilt. Generell kann es gefährlich sein, Objekte zurückzuspeichern, ohne sie nicht mindestens ein Mal zu überprüfen. Diese Option sollte nur dann verwendet werden, wenn feststeht, dass die Objekte vor der Sicherung überprüft wurden oder dass sie aus einer vertrauenswürdigen Quelle stammen.
*NOWRTUPG	Das System versucht nicht, einen Upgrade des Zugriffs für den an das Exitprogramm übermittelten Prüfdeskriptor durchzuführen, indem es Schreibzugriff erteilt. Wird diese Option nicht angegeben, versucht das System den Upgrade auf den Schreibzugriff.

*USEOCOATR	Das System verwendet die Spezifikation des Attributs „nur Objektänderung“, um das Objekt nur dann zu überprüfen, wenn es geändert wurde (d. h., wenn die Prüfsoftware einen Update meldet, findet keine zusätzliche Überprüfung statt.) Wenn diese Option nicht angegeben wird, wird das Attribut „nur Objektänderung“ nicht verwendet, d. h., das Objekt wird sowohl überprüft nachdem es geändert wurde, als auch wenn die Prüfsoftware einen Update meldet.

9.7.35
Seite 4

9.7.36 QSECURITY

Sicherheitsstufe des Systems
Dieser Systemwert gibt die Sicherheitsstufe im System an.

Eine Änderung dieses Werts wird beim nächsten IPL wirksam. Der Vorgabewert ist 40.

Gültige Werte sind:

20	Für die Anmeldung am System ist ein Kennwort erforderlich. Benutzer haben Zugriff auf alle Systemressourcen.
30	Für die Anmeldung am System ist ein Kennwort erforderlich; für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung.
40	Für die Anmeldung am System ist ein Kennwort erforderlich; für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung. Die Ausführung von Programmen schlägt fehl, wenn diese über nicht unterstützte Schnittstellen auf Objekte zuzugreifen versuchen.
50	Für die Anmeldung am System ist ein Kennwort erforderlich; für den Zugriff auf Objekte und Systemressourcen benötigt der Benutzer die entsprechende Berechtigung. Die Ausführung von Programmen schlägt fehl, wenn diese versuchen, nicht unterstützte Parameterwerte an unterstützte Schnittstellen zu übergeben oder über nicht unterstützte Schnittstellen auf Objekte zuzugreifen.

9.7.36
Seite 2

9.7.37 QSHRMEMCTL

Steuerung des gemeinsam benutzten Speichers
Steuert die Berechtigung von Benutzern zur Verwendung des gemeinsam genutzten Speichers (Shared Memory) bzw. des adressierten Speichers (Mapped Memory) mit Schreibmöglichkeit.

Anmerkung:

Zum Ändern dieses Systemwerts sind die Sonderberechtigungen *ALLOBJ und *SECADM erforderlich.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 1.

Gültige Werte sind:

0	Benutzer können keinen gemeinsam genutzten Speicher (Shared Memory) bzw. keinen adressierten Speicher (Mapped Memory) mit Schreibmöglichkeit verwenden. Dieser Wert bedeutet, dass Benutzer keine Shared-Memory-APIs (z. B. shmat() – Shared Memory Attach API) und keine adressierten Speicherobjekte mit Schreibmöglichkeit (z. B. mmap() – Memory Map a File API) verwenden können. Dieser Wert sollte in Umgebungen mit höheren Sicherheitsanforderungen verwendet werden.
1	Benutzer können einen gemeinsam genutzten Speicher oder einen adressierten Speicher mit Schreibmöglichkeit verwenden. Dieser Wert bedeutet, dass Benutzer Shared-Memory-APIs (z. B. shmat() – Shared Memory Attach API) und adressierte Speicherobjekte mit Schreibmöglichkeit (z. B. mmap() – Memory Map a File API) verwenden können. Dieser Wert sollte in Umgebungen verwendet werden, in denen Zeiger von Programmen in verschiedenen Jobs gemeinsam genutzt werden können.

9.7.37
Seite 2

9.7.38 QSSLCSL

SSL-Chiffrierspezifikationsliste
Gibt die Liste der Cipher Suites an, die vom Secure Sockets Layer (SSL) des Systems unterstützt werden. Die Werte sind schreibgeschützt, es sei denn, der Systemwert QSSLCSLCTL (SSL-Chiffriersteuerung) ist auf *USRDFN gesetzt.

Weitere Informationen zu System-SSL und SSL-Chiffrierverfahren enthält der Abschnitt zu SSL unter Security Reference im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Eine Änderung dieses Systemwerts wird für alle folgenden SSL-Systemsitzungen direkt wirksam. Die Vorgabwerte sind:

*RSA_AES_128_CBC_SHA,

*RSA_RC4_128_SHA,

*RSA_RC4_128_MD5,

*RSA_AES_256_CBC_SHA,

*RSA_3DES_EDE_CBC_SHA,

*RSA_DES_CBC_SHA,

*RSA_EXPORT_RC4_40_MD5,

*RSA_EXPORT_RC2_CBC_40_MD5,

*RSA_NULL_SHA und

*RSA_NULL_MD5.

Anmerkung:

Zur Änderung dieses Systemwerts sind die Sonderberechtigungen *IOSYSCFG, *ALLOBJ und *SECADM erforderlich.

Anmerkung:

Die Standard-Chiffrierspezifikationsliste wird vom System-SSL anhand der Reihenfolge der Werte in QSSLCSL sortiert. Die Einträge in der Standard-Chiffrierspezifikationsliste werden vom System definiert und können sich bei Releasegrenzen ändern. Wird ein Standardchiffrierverfahren aus den QSSLCSL-Ergebnissen gelöscht, wird das Chiffrierverfahren aus der Standardliste entfernt. Das Standardchiffrierverfahren wird der Standard-Chiffrierspezifikationsliste beim Einfügen in QSSLCSL hinzugefügt. Es ist nicht möglich, der Standardliste andere Chiffrierverfahren, die über die vom System für das Release definierte Gruppe hinausgehen, hinzuzufügen.

9.7.38
Seite 2

Ein Chiffrierverfahren kann QSSLCSL nicht hinzugefügt werden, wenn der erforderliche SSL-Protokollwert für die Cipher Suite nicht auch für den Systemwert QSSLPCL (SSL-Protokoll-Liste) eingestellt wurde.

Zum Hinzufügen einer Cipher Suite die Folgenummer und die Cipher Suite eingeben. Zum Ändern einer Cipher Suite die vorhandene Folgenummer und den Namen der Cipher Suite überschreiben. Zum Entfernen einer Cipher Suite die vorhandene Folgenummer und den Namen der Cipher Suite mit Leerzeichen überschreiben.

Gültige Werte sind:

*RSA_AES_128_CBC_SHA
Für das AES-Chiffrierverfahren (Advanced Encryption Standard = AES) mit Verkettung von Chiffrierblöcken (CBC) und 128-Bit-Schlüsseln werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von Nachrichtenauthentifizierungscodes (Message Authentication Code = MAC) wird der sichere Hash-Algorithmus (Safe Hash Algorithm = SHA) verwendet.

*RSA_RC4_128_SHA
Für das RC4-Chiffrierverfahren und die 128-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von Nachrichtenauthentifizierungscodes (Message Authentication Code = MAC) wird der sichere Hash-Algorithmus (Safe Hash Algorithm = SHA) verwendet.

*RSA_RC4_128_MD5
Für das RC4-Chiffrierverfahren und die 128-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von Nachrichtenauthentifizierungscodes (Message Authentication Code = MAC) wird der Nachrichtenauszugsalgorithmus 5 (Message Digest Algorithm 5 = MD5) verwendet.

*RSA_AES_256_CBC_SHA
Für das AES-Chiffrierverfahren (Advanced Encryption Standard = AES) mit Verkettung von Chiffrierblöcken (CBC) und 256-Bit-Schlüsseln werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird SHA verwendet.

*RSA_3DES_EDE_CBC_SHA
Für das Triple DES-Chiffrierverfahren mit Verschlüsselung/Entschlüsselung/ Verschlüsselung (EDE) und Verkettung von Chiffrierblöcken (CBC) sowie die 168-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von Nachrichtenauthentifizierungscodes (Message Authentication Code = MAC) wird der sichere Hash-Algorithmus (Safe Hash Algorithm = SHA) verwendet.

*RSA_DES_CBC_SHA
Für das DES-Chiffrierverfahren (Data Encryption Standard = DES) mit Verkettung von Chiffrierblöcken (CBC) und 56-Bit-Schlüsseln werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird SHA verwendet.

*RSA_EXPORT_RC2_CBC_40_MD5
Für das RC2-Chiffrierverfahren mit Verkettung von Chiffrierblöcken (CBC) und 40-Bit-Schlüsseln werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird der MD5-Algorithmus verwendet.

*RSA_EXPORT_RC4_40_MD5
Für das RC4-Chiffrierverfahren und die 40-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird der MD5-Algorithmus 5 verwendet.

*RSA_NULL_SHA
Hierfür werden RSA-Verschlüsselungsalgorithmen, aber keine Chiffrierverfahren verwendet. Zur Generierung von MAC-Codes wird SHA verwendet.

*RSA_NULL_MD5
Hierfür werden RSA-Verschlüsselungsalgorithmen, aber keine Chiffrierverfahren verwendet. Zur Generierung von MAC-Codes wird der MD5-Algorithmus verwendet.

*RSA_RC2_CBC_128_MD5
Für das RC2-Chiffrierverfahren mit Verkettung von Chiffrierblöcken (CBC) und 128-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird der MD5-Algorithmus verwendet.

*RSA_3DES_EDE_CBC_MD5
Für das Triple DES-Chiffrierverfahren mit Verschlüsselung/Entschlüsselung/Verschlüsselung (EDE) und Verkettung von Chiffrierblöcken (CBC) sowie die 168-Bit-Schlüssel werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von Nachrichtenauthentifizierungscodes (Message Authentication Code = MAC) wird der Nachrichtenauszugsalgorithmus 5 (Message Digest Algorithm 5 = MD5) verwendet.

*RSA_DES_CBC_MD5
Für das DES-Chiffrierverfahren (Data Encryption Standard = DES) mit Verkettung von Chiffrierblöcken (CBC) und 56-Bit-Schlüsseln werden die RSA-Verschlüsselungsalgorithmen verwendet. Zur Generierung von MAC-Codes wird der MD5-Algorithmus verwendet.

9.7.38
Seite 4

9.7.39 QSSLCSLCTL

SSL-Chiffriersteuerung
Gibt an, ob der Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) vom System oder vom Benutzer gesteuert wird.

Weitere Informationen zu System-SSL und SSL-Chiffrierverfahren enthält der Abschnitt zu SSL unter Security Reference im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist *OPSYS.

Anmerkung

Zur Änderung dieses Systemwerts sind die Sonderberechtigungen *IOSYSCFG, *ALLOBJ und *SECADM erforderlich.

Anmerkung

Beim Upgrade auf ein höheres Release werden zusätzliche Cipher Suite-Funktionen nicht automatisch hinzugefügt. Der Benutzer muss festlegen, welche neuen Cipher Suites verfügbar sind und diese dem Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) manuell hinzufügen.

Gültige Werte sind:

*OPSYS	Auf den Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) besteht nur Lesezugriff. Die im Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) enthaltenen Werte werden automatisch so geändert, dass sie die Liste der für das betreffende Betriebssystemrelease unterstützten Cipher Suites enthalten.

Anmerkung:

Wenn ein höheres Release mit neuen Cipher Suite-Funktionen installiert wird, erlaubt *OPSYS, dass die Werte automatisch mit neueren und besseren Chiffrierverfahren aktualisiert werden.

9.7.39
Seite 2

*USRDFN	Der Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) ist änderbar.

Anmerkung:

Beim Upgrade auf ein höheres Release werden zusätzliche Cipher Suite-Funktionen nicht automatisch hinzugefügt. Der Benutzer muss festlegen, welche neuen Cipher Suites verfügbar sind und diese dem Systemwert QSSLCSL (SSL-Chiffrierspezifikationsliste) manuell hinzufügen.

9.7.40 QSSLPCL

SSL-Protokolle
Gibt die SSL-Protokollversionen an, die vom System-SSL unterstützt werden.

Weitere Informationen zu System-SSL und SSL-Protokollen enthält der Abschnitt zu SSL unter Security Reference im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Eine Änderung dieses Systemwerts wird für alle folgenden SSL-Systemsitzungen direkt wirksam. Der Vorgabewert ist *OPSYS.

Anmerkung

Zur Änderung dieses Systemwerts sind die Sonderberechtigungen *IOSYSCFG, *ALLOBJ und *SECADM erforderlich.

Gültige Werte sind:

*OPSYS	Welche SSL-Protokolle unterstützt werden, wird vom System bestimmt. Auf jedem Betriebssystemrelease können andere Protokolle unterstützt werden. Weitere Informationen zu den von einem bestimmten Release unterstützten Systemwerten enthält der Abschnitt zu SSL unter Security Reference im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/
*TLSV1	Transport Layer Security Version 1.0 wird unterstützt. Dieser Wert kann nicht angegeben werden, wenn der Wert *OPSYS angegeben wurde.
*SSLV3	Secure Sockets Layer Version 3.0 wird unterstützt. Dieser Wert kann nicht angegeben werden, wenn der Wert *OPSYS angegeben wurde.
*SSLV2	Secure Sockets Layer Version 2.0 wird unterstützt. Dieser Wert kann nicht angegeben werden, wenn der Wert *OPSYS angegeben wurde.

9.7.41 QUSEADPAUT

Übernommene Berechtigung verwenden
Definiert, welche Benutzer Programme mit dem Attribut *USEADPAUT(*YES) (übernommene Berechtigung verwenden) erstellen können. Jeder Benutzer mit der erforderlichen Berechtigung kann Programme oder Serviceprogramme mit diesem Attribut erstellen, ändern oder aktualisieren.

Der Standardwert für QUSEADPAUT ist *NONE. Jeder Benutzer mit der erforderlichen Berechtigung kann Programme oder Serviceprogramme mit diesem Attribut erstellen, ändern oder aktualisieren.

QUSEADPAUT kann auch den Namen einer Berechtigungsliste enthalten. Die Berechtigung des Benutzers wird mit dieser Liste verglichen. Verfügt der Benutzer mindestens über die Berechtigung *USE für die genannte Berechtigungsliste, kann er Programme oder Serviceprogramme mit dem Attribut USEADPAUT(*YES) erstellen, ändern oder aktualisieren. Diese Berechtigung kann nicht von der übernommenen Berechtigung stammen.

Ist die im Systemwert genannte Berechtigungsliste nicht vorhanden, wird die gewünschte Funktion nicht abgeschlossen. Es wird eine entsprechend lautende Nachricht ausgegeben. Werden mehrere Funktionen über den Befehl oder das API angefordert und fehlt die Berechtigungsliste, wird die Funktion nicht ausgeführt. Wurde versucht, einen der Befehle CRTPASPGM (Pascal-Programm erstellen) oder CRTBASPGM (Basic-Programm erstellen) auszuführen, als die Berechtigungsliste nicht gefunden wurde, so kommt es zu einer Funktionsprüfung.

Die gültigen Werte für QUSEADPAUT sind *NONE oder der Name einer Berechtigungsliste.

Eine Änderung des Systemwerts tritt in Kraft, wenn die Programme des Benutzers erstellt werden. Der Vorgabewert ist *NONE.

9.7.41
Seite 2

9.7.42 QVFYOBJRST

Objekt beim Zurückspeichern prüfen
Dieser Systemwert gibt das Verfahren an, das für die Prüfung der Objektsignatur beim Zurückspeichern verwendet werden soll. Er bezieht sich auf folgende Objektarten: *CMD, *PGM, *SRVPGM, *SQLPKG und *MODULE. Außerdem bezieht sich der Wert auf *STMF-Objekte, die Java-Programme enthalten. Dieser Wert gibt auch die Richtlinie für PTFs an, die für das System angelegt werden, einschließlich vorläufiger Korrekturen des lizenzierten internen Codes.

Ist Digital Certificate Manager nicht auf dem System installiert, dann werden bei Prüfung des Systemwerts für die genannten Objekte alle Objekte als unsigniert behandelt.

Eine Änderung dieses Systemwerts wird sofort wirksam. Der Vorgabewert ist 3.

Programm-, Serviceprogramm- und Modulobjekte, die auf einem System mit einem Release vor V6R1 erstellt wurden, werden als nicht signiert betrachtet, wenn sie auf einem System mit V6R1 oder einem höheren Release zurückgespeichert werden. Umgekehrt werden Programm-, Serviceprogramm- und Modulobjekte, die in einem System mit V6R1 oder einem höheren Release erstellt oder umgesetzt wurden, als nicht signiert betrachtet, wenn sie auf einem System mit einem Release vor V6R1 zurückgespeichert werden.

Wenn versucht wird, ein Objekt auf dem System zurückzuspeichern, arbeiten drei Systemwerte gemeinsam als Filter. Sie bestimmen, ob das Objekt zurückgespeichert werden darf oder ob es während der Rückspeicherung konvertiert wird. Der erste Filter ist der Systemwert QVFYOBJRST (Objekt beim Zurückspeichern prüfen). Dieser Systemwert steuert das Zurückspeichern einiger Objekte, die digital signiert werden können. Der zweite Filter ist der Systemwert QFRCCVNRST (Umsetzung beim Zurückspeichern erzwingen). Mit Hilfe dieses Systemwerts kann angegeben werden, ob während des Zurückspeicherns Programme, Serviceprogramme, SQL-Pakete und Modulobjekte konvertiert werden sollen oder nicht. Er kann auch verhindern, dass Objekte zurückgespeichert werden. Vom dritten Filter werden nur Objekte verarbeitet, die die ersten beiden Filter passiert haben. Der dritte Filter ist der Systemwert QALWOBJRST (Zurückspeichern des Objekts erlauben). Er gibt an, ob Objekte mit sicherheitsrelevanten Attributen zurückgespeichert werden können.

9.7.42
Seite 2

Gültige Werte sind:

1 — Signaturen beim Zurückspeichern nicht prüfen. Objekte im Benutzerstatus unabhängig von der Signatur zurückspeichern.

Dieser Wert sollte nur dann verwendet werden, wenn signierte Objekte, deren Signaturprüfung aus einem akzeptablen Grund fehlgeschlagen ist, zurückgespeichert werden sollen. Allgemein gilt jedoch, dass das Zurückspeichern von Objekten mit ungültigen Signaturen auf dem System riskant ist. Die unten aufgeführten Hinweise sind zu beachten, bevor dieser Wert auf 1 gesetzt wird.

2 — Signaturen beim Zurückspeichern prüfen. Nicht signierte Befehle und Objekte im Benutzerstatus zurückspeichern. Signierte Befehle und Objekte im Benutzerstatus auch dann zurückspeichern, wenn ihre Signaturen nicht gültig sind. Dieser Wert sollte nur verwendet werden, wenn bestimmte Objekte mit ungültigen Signaturen zurückgespeichert werden sollen. Allgemein gilt jedoch, dass das Zurückspeichern von Objekten mit ungültigen Signaturen auf dem System riskant ist.

3 — Signaturen beim Zurückspeichern prüfen. Nicht signierte Befehle und Objekte im Benutzerstatus zurückspeichern. Signierte Befehle und Objekte im Benutzerstatus nur dann zurückspeichern, wenn die Signaturen gültig sind. Dieser Wert kann für normale Operationen verwendet werden, wenn zwar erwartet wird, dass einige der zurückzuspeichernden Objekte unsigniert sind, jedoch sichergestellt werden soll, dass alle signierten Objekte gültige Signaturen besitzen. Dies ist der Standardwert.

4 — Signaturen beim Zurückspeichern prüfen. Nicht signierte Befehle und Objekte im Benutzerstatus nicht zurückspeichern. Signierte Befehle und Objekte im Benutzerstatus auch dann zurückspeichern, wenn ihre Signaturen nicht gültig sind. Dieser Wert sollte nur verwendet werden, wenn bestimmte Objekte mit ungültigen Signaturen zurückgespeichert werden sollen, jedoch ausgeschlossen werden soll, dass unsignierte Objekte zurückgespeichert werden. Allgemein

gilt jedoch, dass das Zurückspeichern von Objekten mit ungültigen Signaturen auf dem System riskant ist.

5 Signaturen beim Zurückspeichern prüfen. Nicht signierte Befehle und Objekte im Benutzerstatus nicht zurückspeichern. Signierte Befehle und Objekte im Benutzerstatus nur dann zurückspeichern, wenn die Signaturen gültig sind.
Dieser Wert ist der restriktivste und sollte verwendet werden, wenn nur die Objekte, die durch gesicherte Quellen signiert wurden, zurückgespeichert werden sollen.

Objekte mit dem Attribut „System“ und Objekte mit dem Attribut „Übernommen“ müssen gültige Signaturen einer vertrauenswürdigen Quelle besitzen. Für Objekte in LIC-PTFs (LIC = Lizenzierter Interner Code) ist ebenfalls die gültige Signatur einer vertrauenswürdigen Quelle erforderlich. Wenn diese Objekte keine gültige Signatur haben, können sie, unabhängig vom Systemwert QVFYOBJRST, nicht zurückgespeichert werden.

Einige Befehle verwenden eine Signatur, die nicht alle Komponenten des Objekts abdeckt. Einige Komponenten der Befehle werden nicht signiert, andere wiederum nur, wenn sie einen anderen als den Standardwert enthalten. Bei dieser Art von Signatur können Änderungen am Befehl vorgenommen werden, die die Signatur nicht ungültig machen. Zu diesen Änderungen gehören:

- Befehlsvoreinstellungen ändern
- Einem Befehl ohne Programm zur Gültigkeitsprüfung ein solches Programm hinzufügen.
- Den Parameter ‚Ausführung wo zulässig‘ ändern
- Den Parameter ‚Benutzer begrenzt zulassen‘ ändern

Der Benutzer kann diesen Befehlen auch seine eigene Signatur hinzufügen, die diese Bereiche des Befehlsobjekts abdeckt.

9.7.42
Seite 4

9.8 Objekt- und Benutzerverwaltung

Der IBM Power i Server kann sehr vielfältig eingesetzt werden. Doch egal, ob Sie die IBM Power i als reinen Datenbank-Server oder als Applikations-Server einsetzen, eine zentrale Rolle Ihrer Tätigkeiten und Überlegungen sollte der Objekt und Benutzerverwaltung gelten. Auf einem kleinen System gibt es vielleicht nur ein oder zwei Personen, die Zugang zu allen Objekten erhält und es werden nur wenige Benutzerprofile und -gruppen benötigt. In großen Unternehmen hingegen werden Sie mit einer Vielzahl von Objekten konfrontiert, die verwaltet und für unterschiedliche Benutzergruppen berechtigt werden müssen. Doch egal wie komplex Ihr System ist, Sie benötigen verschiedene Benutzerprofile, die die individuellen Rechte und Zugangsberechtigungen für die Objekte bestimmen. Die IBM Power i unterstützt Benutzergruppen und Objektberechtigungskonzepte, die so einfach oder so komplex sind wie Sie es wünschen. Dabei ist das Benutzer- und Objektberechtigungskonzept abhängig von verschiedenen Systemwerten, wobei der Systemwert QSECURITY sicherlich eine entscheidende Rolle spielt.

9.8 Seite 2

9.9 Benutzer-ID – Ihr Schlüssel zum System i

Bestimmt haben Sie sich auch schon mal mit falscher Benutzer-ID und/oder falschem Kennwort an Ihrem System i angemeldet: „Wie war das noch mal mit dem Kennwort, das vom Facebook-Account oder doch das vom Electronic-Banking? Nein, die Richtlinien sehen ja vor, dass ein Kennwort alle 120 Tage geändert werden muss. Das war doch vor dem Urlaub. Keine Ahnung mehr, aber es gibt ja noch den Systemadministrator, der in solchen Fällen gerufen wird." Gut, dass wir immer noch ein „Hintertürchen" haben, um doch noch auf das System zugreifen zu können. Weil ohne System i geht bei vielen von uns im Büro nichts.

Benutzer-ID, User-ID, Account, es gibt eine Vielzahl von Bezeichnungen für das gleiche Merkmal, nämlich den Zugang zu unseren Computersystemen. Die Benutzer-ID ist das Merkmal, mit dem Sie als Individuum im System registriert sind, über das ihre Zugriffsmöglichkeiten auf Programme, Menüs, Daten, kurzum auf so ziemlich alles im System i gewährt – oder eben verweigert wird. Umso wichtiger ist es, mit Benutzer-IDs sorgsam umzugehen – oder würden Sie Ihren Mitarbeitern auch raten, den Haustürschlüssel – oder noch schlimmer – den Autoschlüssel einfach so unter die Tastatur ihres Bildschirms zu legen?

Nein, könnte uns nicht passieren? Schauen Sie doch mal nach! Die unrechtmäßige Verwendung von Benutzer-IDs ist ein Problem, dem sehr schwer beizukommen ist. Weiß man doch in der Regel nicht, wer sich ihrer bemächtigt hat, was der Grund hierfür war und was damit angestellt wird.

9.9
Seite 2

9.9.1 Rund um die Benutzer-ID

Die Benutzer-ID ist nur ein Steuerungsmerkmal der Zugriffsberechtigung. Wir alle wissen, dass das System i eine sehr ausgeprägte Sicherheit bietet. Von Haus aus wurde das von IBM so implementiert. Deshalb spielen neben der Benutzer-ID noch weitere Stellschrauben entscheidende Rollen.

Im vorangegangenen Kapitel wurden die sicherheitsrelevanten Systemwerte im Detail vorgestellt. Wenn Sie sich erinnern, fällt Ihnen zu Systemwerten wie QSECURITY, QMAXSIGN, QPWD… bestimmt einiges ein. Eine Benutzer-ID ist also nur so sicher wie das Umfeld, in das sie eingebettet ist. So können Sie gerne für jeden Benutzer eine ID festlegen, auch ein sehr komplexes Kennwort vergeben, aber wenn Sie den Systemwert QSECURITY auf „20“ gesetzt haben, nützt Ihnen das recht wenig, wenn Sie Benutzer davon abhalten wollen, bestimmte Anwendungen auszuführen oder auf bestimmte Daten zuzugreifen.

Auch ist es nicht unbedingt ratsam, beim Anlegen eines neuen Benutzers das Profil QSECOFR als Grundlage für die Erstellung einer Kopie zu verwenden. Zur Sicherheit gehört mehr, als einfach ein Benutzerprofil zu erstellen und die Berechtigungsstufe auf *USER zu setzen. Um die i5/OS-Sicherheitsmöglichkeiten umfassend zu nutzen, müssen Sie auch Begriffe wie „Gruppenprofile“, „übernommene Berechtigung“, „Objektberechtigung“, „OS/400-Systemsicherheitswerte“, „Netzwerksicherheit“ und vieles mehr verstehen.

Es ist einfach, zu behaupten, Ihr System sei sicher. Aber wie können Sie Gewissheit erlangen? Wenn Sie eine physische Datei erstellen und in dieser Datei Datensätze speichern, ist diese Datei dann automatisch sicher? Vermutlich nicht. Um für diese Datei echte Sicherheit zu gewährleisten, können Sie die Zugriffsstufe auf *PUBLIC *NONE einstellen und anschließend die Berechtigung für die Arbeit mit der Datei bestimmten Benutzerprofilen oder Sicherheitsberechtigungslisten zuweisen.

„Gruppenprofile“, „*PUBLIC *NONE“, „übernommene Berechtigung“? Für einige von Ihnen sind das noch Fremdworte, die im Laufe dieses Kapitels jedoch erklärt und in Zusammenhänge gebracht werden sollen.

Wie Sie gesehen haben, müssen Sie aufgrund der eingestellten Sicherheitsstufe für jeden Benutzer ein Benutzerprofil hinterlegen. Das Benutzerprofil enthält:

- grundlegende Sicherheitsinformationen über die Person,
- spezielle Berechtigungen für die Person,
- spezifische Jobverarbeitungsinformationen für die Person.

Auf einer iSeries sind mehrere Benutzerprofile der IBM vorhanden.

9.9.1
Seite 2

QPGMR	Programmierer- und Stapelbenutzerprofil
QSECOFR	Sicherheitsbeauftragter
QSRV	Serviceprofil, das von der Person genutzt wird, die den Service für das System durchführt.
QSYSOPR	Systemadministrator
QUSER	allgemeiner Benutzer

Alle Profile – mit Ausnahme des Profils QSECOFR – haben kein Kennwort. Sie können zwar theoretisch dem Profil QPGMR ein Kennwort zuweisen und sich am System damit anmelden, aber dies wird nicht von IBM empfohlen. Die Profile sollen als Kopiervorlage dienen. Kopieren Sie also einfach die benötigten Profile. Dadurch übernehmen Sie viele Parameter und müssen nur firmenspezifische Ergänzungen vornehmen. Es gibt noch weitere von IBM gelieferte Benutzerprofile, die Sie nicht kopieren sollten, denn hierbei handelt es sich um Benutzerprofile, die das System für interne Aufgaben verwendet.

QAUTPROF	Allgemeines IBM-Berechtigungsprofil
QBRMS	Backup Recovery Media- (BRM-) Profil
QDBSHR	Profil für den Datenbankzugriff
QDFTOWN	Alle Objekte auf einer iSeries benötigen einen Eigentümer. Ist ein Benutzerprofil nicht mehr gültig, geht das Eigentumsrecht an seinen Objekten an das Profil QDFTOWN über.
QDOC	Dokumentenprofil
QLPAUTO	Lizenzierter Programm-Autoinstallationsbenutzer
QLPINSTALL	Lizenzierter Programminstallationsbenutzer
QMSF	Profil für Post-Server
QNETSPLF	Netzspool-Profil
QSPL	Spool-Benutzer
QSYS	Interner Systembenutzer
QTCP	TCP/IP-Benutzer

Diese Profile dienen nicht dazu, sich im System anzumelden. Versuchen Sie nicht, die Profile zu ändern oder zu löschen. Wenn Sie es dennoch versuchen, können interne Funktionen plötzlich nicht mehr funktionieren.

9.9.2 Einzelprofile

Jeder Mitarbeiter Ihres Unternehmens sollte ein eigenes Benutzerprofil haben. Melden sich mehrere Personen unter einem Profilnamen an, ist die Identifizierung des Benutzers in Ihrem System nicht mehr möglich. Sie ersparen sich also unnötige Arbeit bei der Unterstützung Ihrer Anwender in der täglichen Arbeit, wenn Sie Einzelprofile anlegen, und Sie haben es damit sehr viel einfacher, die Benutzerberechtigungen zu bestimmen. Benutzerprofile sind Objekte des Typs *USRPRF.

CRTUSRPRF	Benutzerprofil erstellen
DSPUSRPRF	Benutzerprofil anzeigen
CHGUSRPRF	Benutzerprofil ändern
DLTUSRPRF	Benutzerprofil löschen
RSTUSRPRF	Benutzerprofil zurücksichern

Wenn Sie neue Benutzerprofile anlegen wollen, müssen Sie neben dem Profilnamen eine Reihe weiterer Parameter festlegen:

```
                    Benutzerprofil erstellen (CRTUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .   _________     Name
Benutzerkennwort . . . . . .  *USRPRF       Zeichenwert, *USRPRF, *NONE
Kennwort auf abgelaufen setzen *NO          *NO, *YES
Status . . . . . .  . . . .  *ENABLED       *ENABLED, *DISABLED
Benutzerklasse . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
Unterstützungsstufe  . . . . .  *SYSVAL     *SYSVAL, *BASIC, *INTERMED...
Aktuelle Bibliothek  . . . . .  *CRTDFT     Name, *CRTDFT
Aufzurufendes Startprogramm  . .  *NONE     Name, *NONE
  Bibliothek . . . . . .  . .   _________   Name, *LIBL, *CURLIB
Anfangsmenü  . . . . . .  . .   MAIN        Name, *SIGNOFF
  Bibliothek . . . . . .  . .     *LIBL     Name, *LIBL, *CURLIB
Möglichkeiten einschränken . . .  *NO       *NO, *PARTIAL, *YES
Text 'Beschreibung'  . . . . . .  *BLANK
_____


                                                                      Ende
F3=Verlassen   F4=Bedienerf.   F5=Aktualisieren   F10=Zusätzl. Parameter
F12=Abbrechen   F13=Verwendung der Anzeige   F24=Weitere Tasten
```

Erstellung eines Benutzerprofils

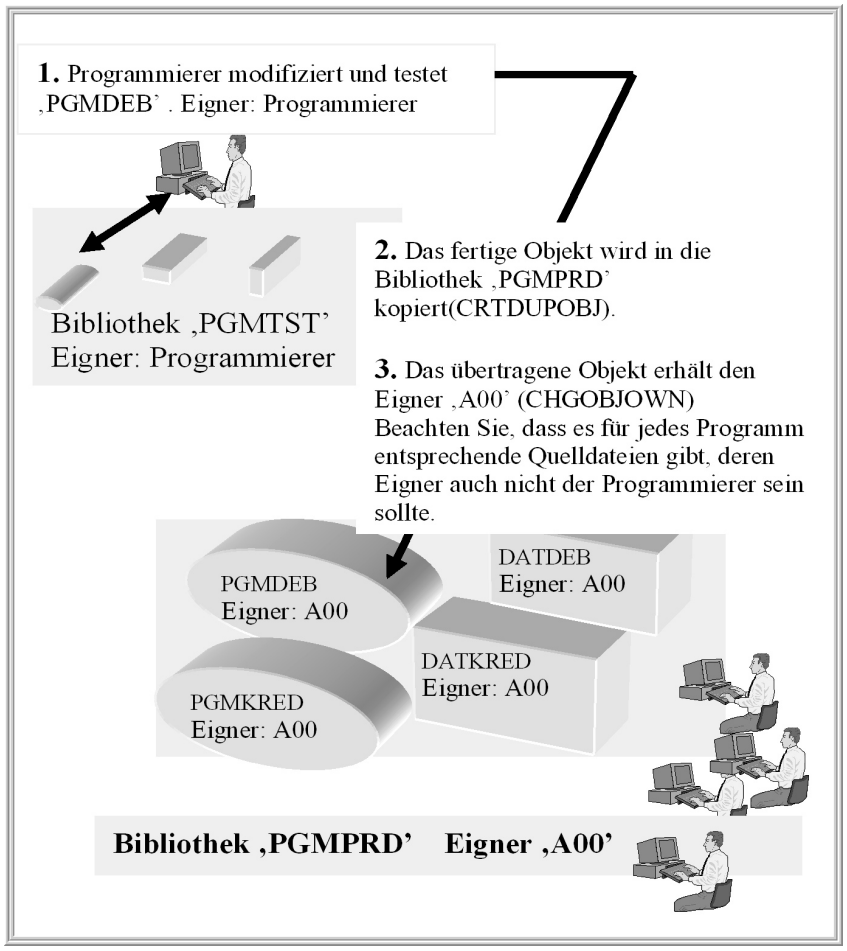
9.9.2
Seite 2

9.9.3 Gruppenprofile

Einige Mitarbeiter erstellen Objekte, z.B. Query-Abfragen, Programme oder Dateien. Für jedes der Objekte wird das entsprechende Benutzerprofil als Eigner eingetragen. Der Eigner verfügt über alle Rechte am Objekt. Sie können mit dem Befehl CHGOBJOWN den Eigentümer nachträglich ändern. Dabei haben Sie die Möglichkeit, die Berechtigungen des vorhergehenden Eigners zu widerrufen oder beizubehalten. Sie werden diesen Befehl sicherlich häufig verwenden, denn es ist nicht wünschenswert, dass ein Programmierer oder Anwender Eigentümer seiner erstellten Objekte bleibt, wenn er das Programm oder die Dateien für die Produktion frei gibt. Daher sollte das Objekteigentumsrecht bei der Objektfreigabe auf einen Eigner geändert werden, der keine Person ist. Das kann z.B. ein Benutzerprofil ohne Kennwort sein. Werden die Daten oder Programme zu Pflegezwecken überprüft, wird das Eigentumsrecht wieder auf das Profil des Programmierers übertragen.

Erinnern Sie sich an unser Beispiel?

Unser Programmierer, der das Programm OPDEB modifiziert, muss also das Eigentumsrecht an einen „unpersönlichen“ Eigner übertragen.



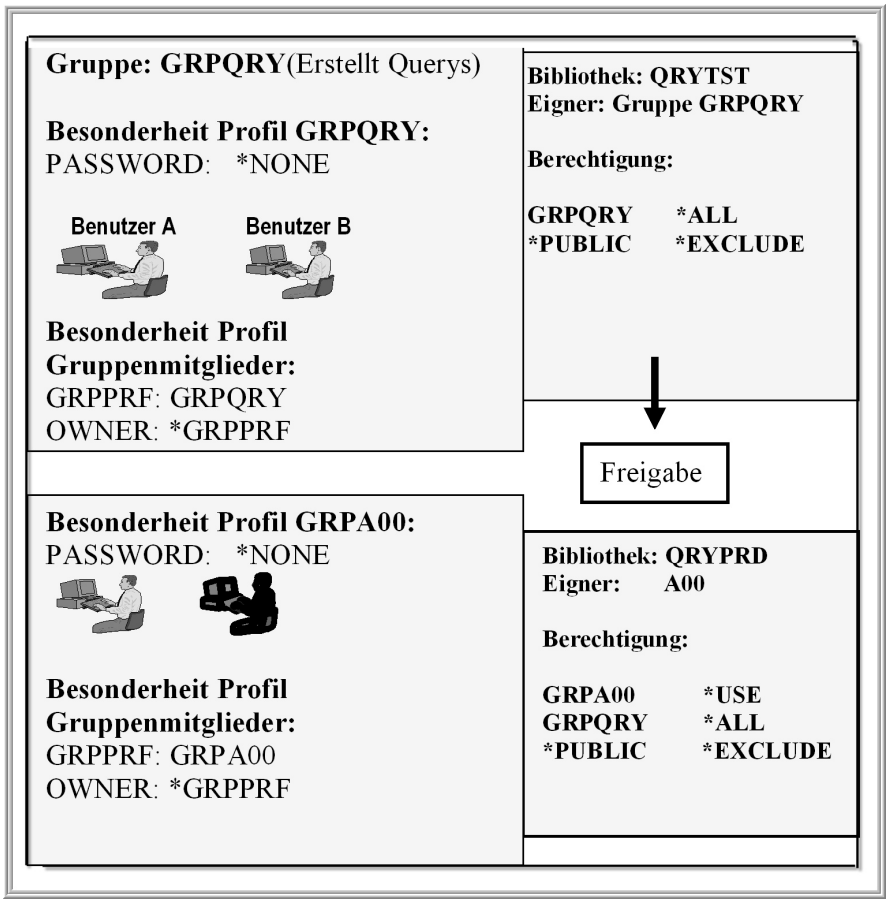
Eigentumsrechte übertragen

9.9.3
Seite 2

Dieser Vorgang erscheint zunächst etwas komplex, aber Sie können für diesen Änderungsdienst ein entsprechendes Verwaltungsprogramm schreiben, dass zukünftig diese Aufgabe wahrnimmt. Der Aufwand lohnt sich, denn:

- Wenn Sie das Schaubild betrachten, erkennen Sie, dass viele Objekte redundant im System gespeichert werden. Stellen Sie sich jetzt vor: Sie haben nicht nur einen Benutzer, der Objekte erstellt, sondern mehrere Personen. Dann können Sie wertvollen Plattenplatz sparen, wenn Sie Ihre Programmierer und Anwender zwingen, Sicherungskopien, alte Programme etc. regelmäßig zu löschen. Das erreichen Sie, indem Sie den maximalen Speicherbereich Ihrer Programmierer und/oder Anwender im Benutzerprofil (MAXSTG) begrenzen.
- Sie können Ihre freigegebenen, aktuellen Objekte jederzeit anhand des Eigners „A00“ identifizieren.
- Sie können aktive Benutzerprofile problemlos löschen.

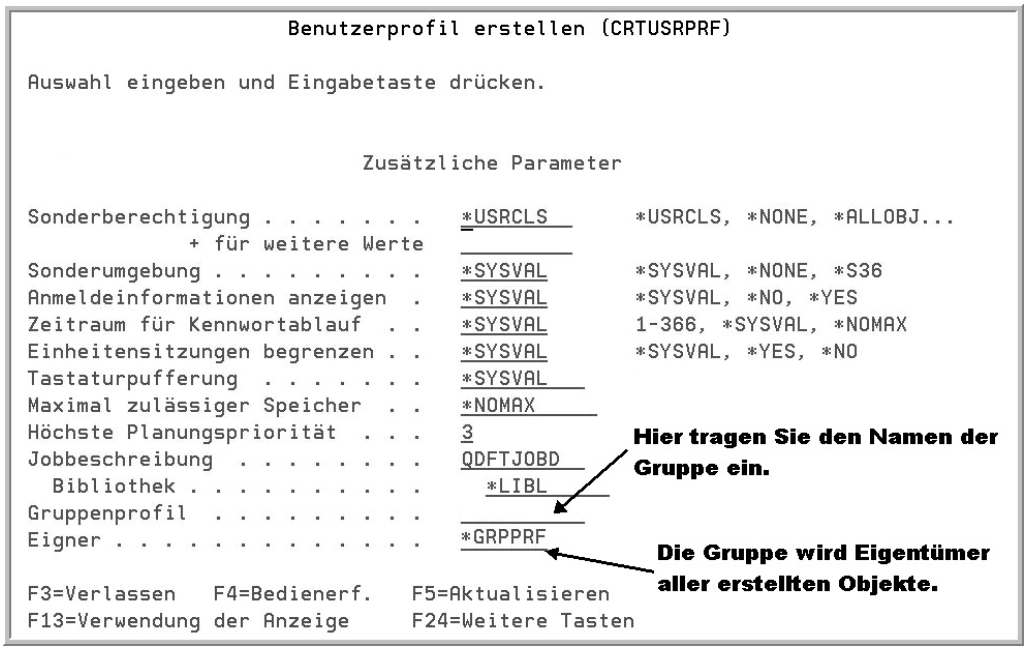
Neben dem Eigentumsrecht haben die Objekte öffentliche Berechtigungen. Wie Sie wissen, handelt es sich um die Berechtigungen, die gewährt werden, wenn keine spezifischen Rechte am Objekt vergeben werden. Das kann in der täglichen Praxis unter Umständen zu Berechtigungskonflikten führen. Eine Möglichkeit, derartige Probleme zu lösen, sind individuelle Berechtigungen einzelner Personen an den Objekten. Bei großen Anwenderkreisen haben Sie allerdings einen beträchtlichen Aufwand und sehr schnell werden Sie die Konflikte lösen, indem Sie *ALLOBJ-Berechtigungen vergeben. Es stellt sich daher die Frage, ob es nicht einfachere und weniger arbeitsintensive Methoden gibt, um Berechtigungsprobleme schon bei der Objekterstellung zu reduzieren. Das Problem kann durch Gruppenprofile gelöst werden. Gruppenprofile sind spezielle Benutzerprofile, denen die Eignerschaft an den Objekten übertragen wird. Die Gruppenmitglieder erhalten entsprechende Rechte an den Objekten der Gruppe.



Gruppenprofile erstellen

Wenn Sie Gruppenprofile benötigen, müssen Sie zunächst das Profil für die Gruppe erzeugen. Kennzeichnend für ein Gruppenprofil ist, dass kein Kennwort eingetragen wird. Dadurch können Sie sich mit dem Profil nicht anmelden. Es wird nur zur Steuerung der Objektberechtigungen verwendet. Für dieses Profil wird eine beliebige Benutzerklasse eingetragen, z.B. der Wert *USER. Die Gruppenmitglieder können die Sonderberechtigungen des Gruppenprofils übernehmen, wenn Ihre eigenen Berechtigungen nicht ausreichen. Nachdem das Profil GRPQRY und GRPA00 erstellt wurde, werden die Gruppenmitglieder der Gruppe zugeordnet.

9.9.3
Seite 4



Gruppenprofil zuordnen

Der Parameter „Gruppenprofil“ ordnet die einzelnen Profile der Gruppe zu. Der Parameter „Eigner“ bestimmt das Gruppenprofil zum späteren Objekteigner. Wenn Sie nicht wollen, dass der Objekteigner auf die Gruppe abgeändert wird, haben Sie eine weitere Möglichkeit: Tragen Sie als Gruppe wiederum das Gruppenprofil ein. OWNER (*USRPRF) gibt an, dass das Benutzerprofil – nicht das Gruppenprofil – Eigner der Objekte bleibt, die vom Benutzer erstellt werden. Jetzt müssen Sie über den Parameter GRPAUT spezifizieren, welche Berechtigungen die Gruppenmitglieder für die erstellten Objekte bekommen. Beachten Sie aber, dass die Eignerschaft und die Berechtigungen nur für zukünftige Objekte gelten. Alle bereits bestehenden Objekte sind von den Benutzerprofiländerungen nicht betroffen. Hier müssen Sie manuell die Eignerschaft auf die Gruppe übertragen oder die entsprechenden Objektberechtigungen vergeben.

Bei all Ihren Überlegungen bezüglich der Objekteigner, sollten Sie berücksichtigen, dass Sie Benutzerprofile nicht löschen können, wenn das Profil Eigentümer von Objekten ist. Der Befehl DLTUSRPRF stellt Ihnen drei Möglichkeiten zur Verfügung:

- Alle Objekte des Benutzers werden zusammen mit dem Profil gelöscht. Diese Möglichkeit setzt allerdings voraus, dass reale Benutzer nicht das Eigentumsrecht an produktiven Objekten besitzen.
- Alle Objekte des Benutzers werden an einen anderen Benutzer im System übertragen. Wenn Sie diese Möglichkeiten nutzen, behalten Sie natürlich alle Objekte des Benutzers. Das können beliebige Sicherungskopien, Testobjekte, vorangegangene Objektvarianten etc. sein. Sie werden

zukünftig ein Problem haben, die produktiven Objekte von den unproduktiven Objekten zu unterscheiden und nehmen den „Müll“ ehemaliger Mitarbeiter mit.

- Das Benutzerprofil wird nicht gelöscht, wenn der Benutzer Eigentümer von Objekten ist.

Und noch eine Anmerkung zum Schluss:

Die IBM unterstützt nicht den Befehl RNMOBJ (rename objekt) für Benutzerprofile, weil andere Objekte auf dieses Objekt verweisen. Wenn Sie ein Profil umbenennen wollen, gehen Sie folgendermaßen vor:

- Kopieren Sie das alte Benutzerprofil PROFALT in das neue Profil PROFNEU.
- Übertragen Sie an das neue Benutzerprofil alle persönlichen Berechtigungen des alten Profils:
  GRTUSRAUT GRTUSRAUT USER(PROF_NEU)
  REFUSER(PROF_ALT)
- Löschen Sie jetzt das alte Profil und übertragen Sie die Eigentumsrechte an alle anderen Objekten auf das neue Profil.
  DLTUSRPRF USRPRF(PROF_ALT)
  OWNOPJOPT(*CHGOWN PROF_NEU)

9.9.3
Seite 6

9.9.4 Berechtigungslisten

Ebenfalls erwähnt wurde der Begriff der Berechtigungslisten. Was sind Berechtigungslisten?

Eine Berechtigungsliste besteht aus einer Liste von Benutzern oder Gruppen, dem Typ der Berechtigung (verwenden, ändern und ausschließen) für jeden Benutzer oder jede Gruppe sowie einer Liste von Objekten, auf die diese Liste Zugriff bietet.

Wenn jeder Benutzer separat Zugriff auf jedes für die Arbeit erforderliche Objekt erhalten würde, hätte dies möglicherweise eine Unmenge an doppelter Arbeit zur Folge, da viele Benutzer auf dieselbe Gruppe von Objekten zugreifen müssen. Eine viel einfachere Methode für die Erteilung dieses Zugriffs ist die Erstellung von Berechtigungslisten. Benutzer und Gruppen erhalten dann die Berechtigung für diese Liste und damit die Zugriffsberechtigung auf alles, was in der Liste aufgeführt ist.

Sie können zum Beispiel eine Berechtigungsliste erstellen, in der eine Liste mit Objekten enthalten ist, die für eine Bestandsdatenbank benötigt werden. Ein Benutzer, der für die Bestellung neuer Lagerteile zuständig ist, kann die Berechtigung erhalten, den Inhalt der Datenbankobjekte anzuzeigen. Außerdem müsste die Benutzergruppe, die für den Transport und die Annahme zuständig ist, diese Datenbank aktualisieren, falls Teile im Lager eintreffen oder das Lager verlassen. Diese Gruppe kann die Berechtigung erhalten, den Inhalt der Objekte zu ändern.

Mit dem Befehl **WRKAUTL** (Mit Berechtigungslisten arbeiten) kann eine Liste von Berechtigungslisten angezeigt werden, die geändert werden können.

Einschränkungen:
- Es werden nur die Berechtigungslisten angezeigt, für die der Benutzer berechtigt ist.
- Um Operationen an Berechtigungslisten durchzuführen, muss der Benutzer über die Benutzungsberechtigung (*USE) für den von der

```
                Mit Berechtig.listen arbeiten (WRKAUTL)

Auswahl eingeben und Eingabetaste drücken.

Berechtigungsliste . . . . . .   __________    Name, generisch*, *ALL
```

Mit Berechtigungslisten arbeiten

9.9.4
Seite 2

Berechtigungsliste (AUTL)

Gibt die Berechtigungslisten an, die angezeigt werden sollen.

***ALL**
Es werden alle Berechtigungslisten angezeigt, deren Eigner der Benutzer ist und für die er die Berechtigung zum Anzeigen besitzt.

Generischer Name
Den generischen Namen der Berechtigungslisten angeben, die angezeigt werden sollen. Ein generischer Name besteht aus einem oder mehreren Zeichen, gefolgt von einem Stern (*). Wird ein generischer Name angegeben, werden alle Berechtigungslisten angezeigt, deren Namen dasselbe Präfix haben wie der generische Name.

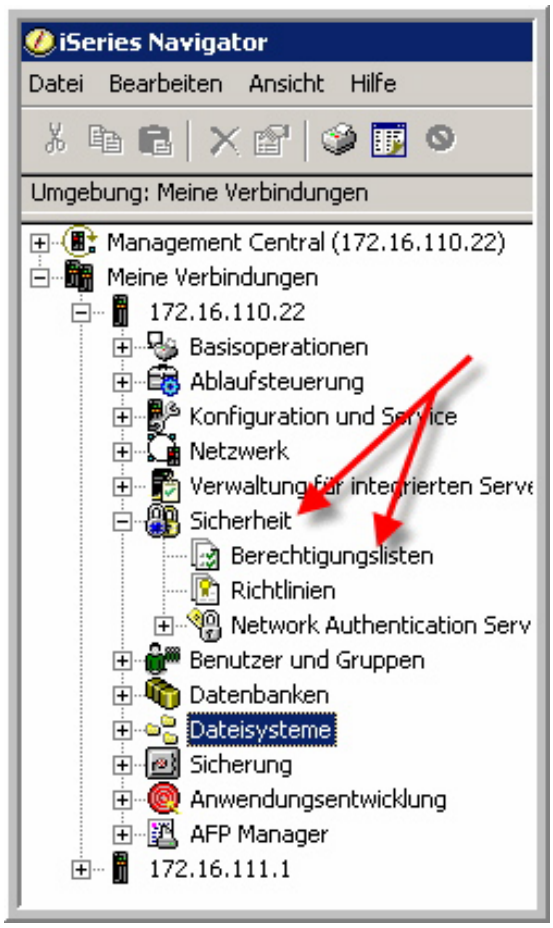
Name
Den Namen der Berechtigungsliste angeben, die angezeigt werden soll.

Beispiele für WRKAUTL:

```
WRKAUTLAUTL(FR*)
```

Mit diesem Befehl kann mit einer Liste aller Berechtigungslisten gearbeitet werden, deren Namen mit ‚FR' beginnen und für die die Berechtigung zum Anzeigen besteht.

Doch auch der iSeries Navigator bietet Ihnen die Möglichkeit mit Berechtigungslisten zu arbeiten:

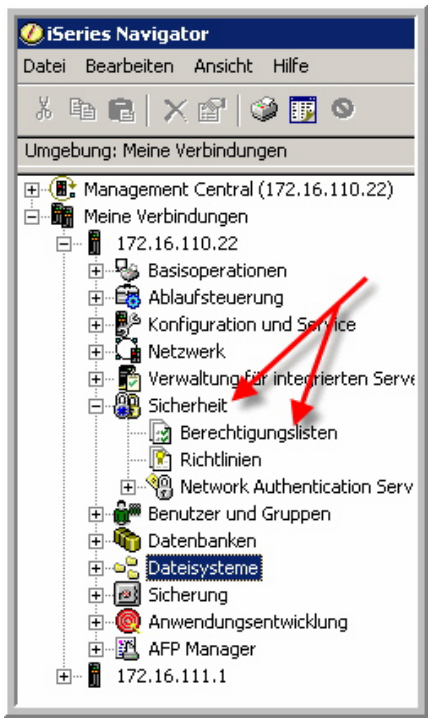


Berechtigungslisten im iSeries Navigator

Um Berechtigungslisten mit dem iSeries Navigator zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie zunächst die Verbindung zum entsprechenden iSeries Server her.
2. Erweitern Sie anschließend den Punkt „Sicherheit“.

9.9.4
Seite 4

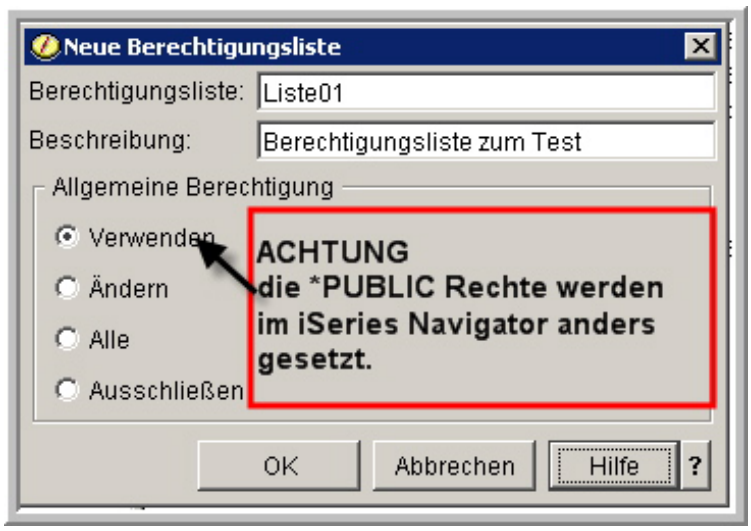


Berechtigungslisten erstellen

3. Markieren Sie jetzt den Eintrag „Berechtigungslisten“ mit der rechten Maustaste und wählen Sie „Neue Berechtigungsliste“.

Berechtigungsliste erstellen

Anschließend erscheint ein weiteres Fenster:

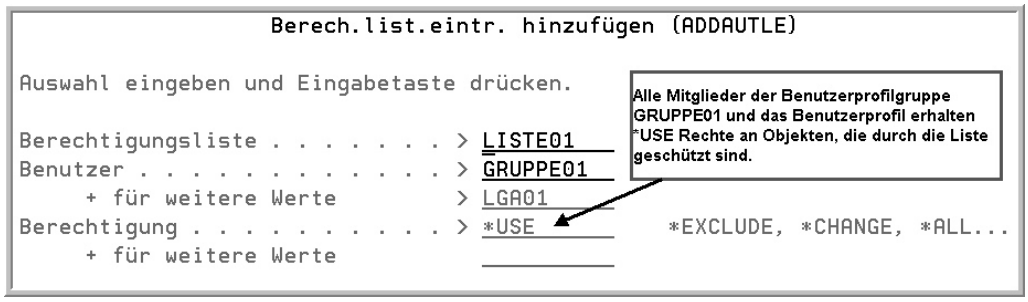


Berechtigungslisten erstellen

Sie sehen, auch im iSeries Navigator sind die Parameter eher spärlich. Eines fällt allerdings auf: der Parameter AUT hat im iSeries Navigator eine andere Default-Einstellung. Während die 5250-Emulation für die *PUBLIC-Rechte den Wert *CHANGE verwendet, erhalten die Mitglieder der Gruppe *PUBLIC nur *USE-Rechte, wenn die Liste im iSeries Navigator erstellt wird.

Benutzer hinzufügen und verwalten

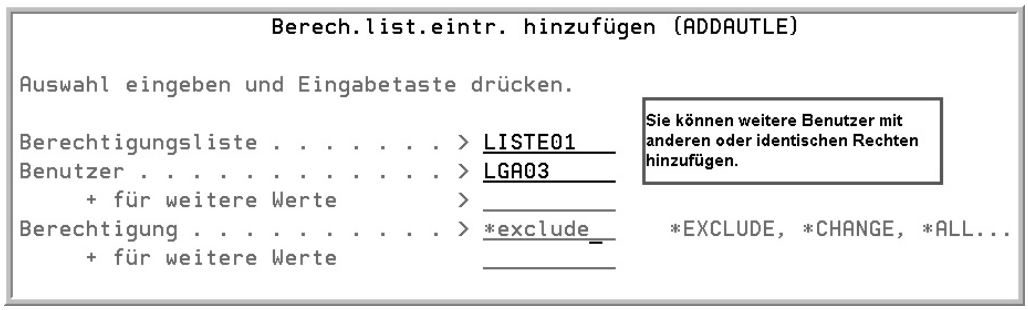
Im nächsten Schritt müssen in der Berechtigungsliste Benutzer und/oder Benutzergruppen hinzugefügt werden. Auch hierfür stehen zwei Interfaces zur Verfügung. In einer 5250-Emulation verwenden Sie die Befehle ADDAUTLE (add authority list entry), um Benutzer hinzuzufügen und den Befehl RMVAUTLE (remove authority list entry), um Benutzer zu entfernen.



Berechtigungslisteneinträge hinzufügen

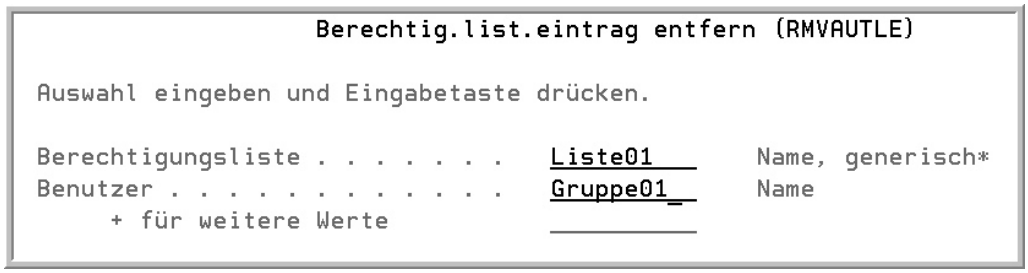
9.9.4
Seite 6

Es ist durchaus möglich, mehrere Benutzergruppen mit unterschiedlichen Zugriffsberechtigungen über eine Liste zu verwalten.



Weitere Einträge hinzufügen

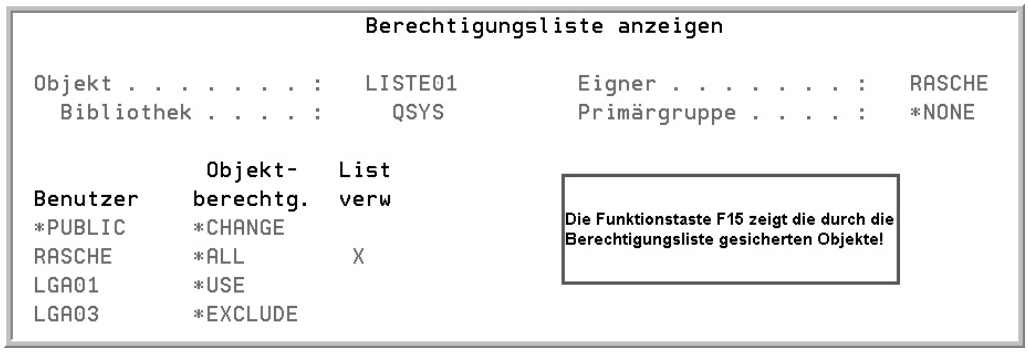
Genauso einfach ist es, Benutzer wieder aus der Liste zu entfernen:



Einträge entfernen

Sobald Sie einen Eintrag entfernen, sind die entsprechenden Objektberechtigungen entzogen und Sie können die Liste sogar bearbeiten, während die Benutzer angemeldet sind und die gesicherten Objekte in Gebrauch sind.

Zur Prüfung der Listeneinträge bietet sich der Befehl DSPAUTL (display authority list) an:



Berechtigungslisteneinträge anzeigen

In der Anzeige können Sie jederzeit die eingetragenen Benutzer und die zugeordneten Rechte anzeigen. Wenn Sie nun auch noch die gesicherten Objekte prüfen wollen, können Sie die Funktionstaste F15 nutzen.

```
                    Berechtigungslistenobjekte anzeigen

Berechtigungsliste . . . . . :   LISTE01
  Bibliothek . . . . . :     QSYS
Eigner . . . . . :   RASCHE
Primärgruppe . . . . . :   *NONE

                                                Primär-
Objekt      Bibliothek  Art       Eigner        gruppe       Text

  (Durch diese Berechtigungsliste werden keine Objekte gesichert)
```

Gesicherte Objekte anzeigen

Sie sehen, dass derzeit noch keine Objekte durch die Liste geschützt sind, d.h. bislang wird die Liste nicht verwendet.

Falls Sie Einträge verändern müssen, steht der Befehl CHGAUTLE (change authority list entry) zur Verfügung:

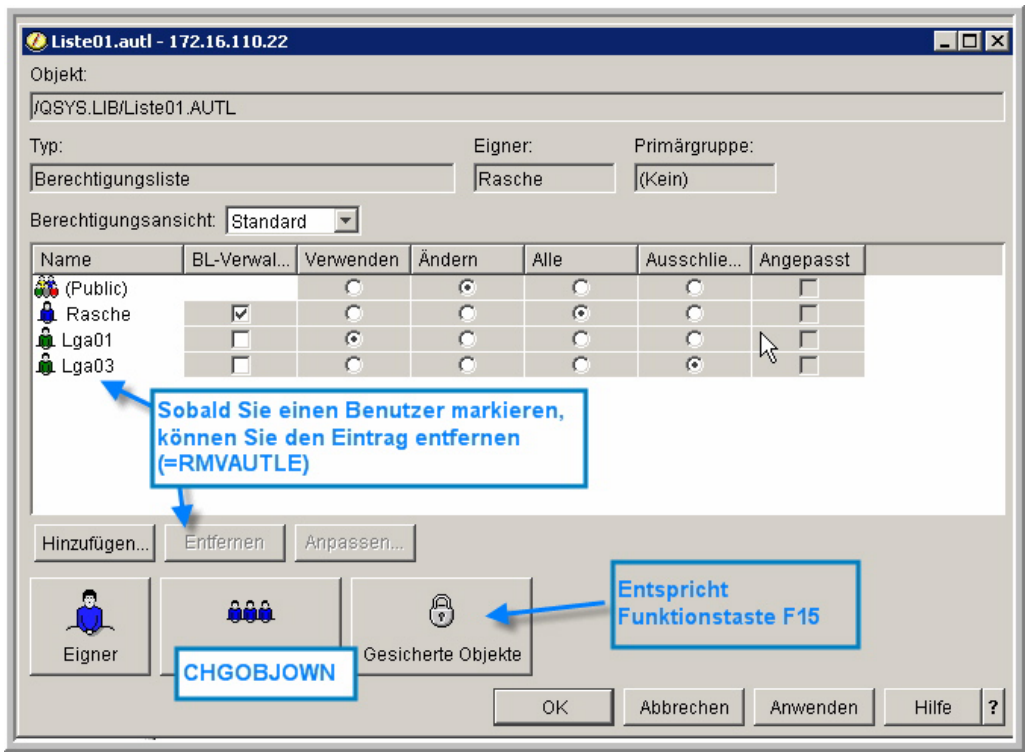
```
                  Berecht.listeneintrag ändern (CHGAUTLE)

Auswahl eingeben und Eingabetaste drücken.

Berechtigungsliste . . . . . .   Liste01     Name, generisch*
Benutzer . . . . . .             LGA01       Name, *PUBLIC
     + für weitere Werte                     _
Berechtigung . . . . . .         *USE        *EXCLUDE, *CHANGE,
     + für weitere Werte                     _
```

Listeneinträge verändern

Bevor wir nun Objekte mit der Berechtigungsliste verbinden, schauen wir uns kurz an, welche Möglichkeiten Sie im iSeries Navigator haben:

9.9.4
Seite 8

Wenn Sie eine der Berechtigungslisten mit einem Doppelklick öffnen, erhalten Sie die folgende Anzeige:



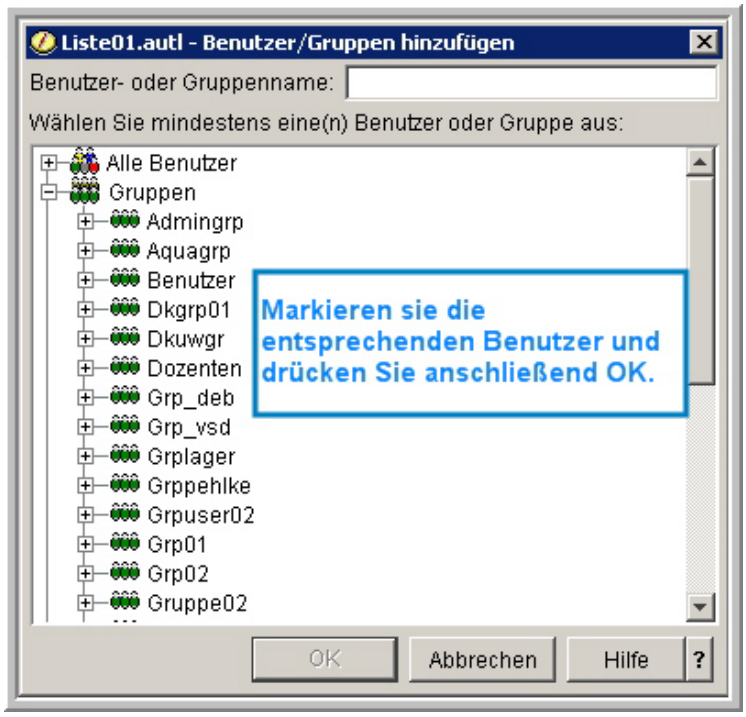
Listeneinträge mit dem iSeries Navigator verwalten

Der Navigator bietet bei der Verwaltung einige entscheidende Vorteile. Sie können die Einträge sehen und gleichzeitig ändern. Für die Änderung stehen Ihnen zwei Möglichkeiten zur Verfügung:

Wenn Sie einen Eintrag markieren und anschließend den Button „ANPASSEN“ nutzen, erscheint ein weiteres Fenster, in dem Sie die Veränderungen vornehmen. Sobald Sie Ihre Änderungen in dem zusätzlichen Fenster bestätigen, werden Sie übernommen.

Es geht aber auch einfacher. Klicken Sie einfach mit der Maus auf die Berechtigungen, um sie zu gewähren oder zu entziehen.

Falls Sie weitere Benutzer in die Liste aufnehmen wollen, wählen Sie „Hinzufügen“. Daraufhin erscheint ein Fenster, das Ihnen komfortabel die Auswahl weiterer Benutzer ermöglicht.



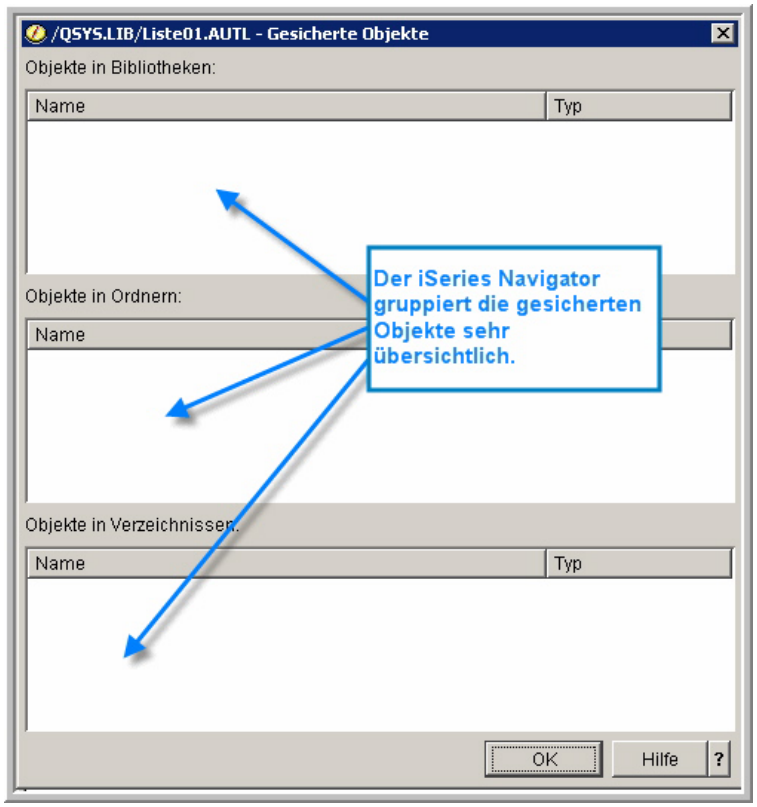
Weitere Benutzer auswählen

Sie können in dem Fenster Gruppenprofile und/oder einzelne Benutzerprofile markieren. Um mehrere Einträge zu markieren, stehen Ihnen im iSeries Navigator die SHIFT- oder die STRG-Taste zur Verfügung. Die Wirkung ist analog der Arbeit mit Windows. Sobald Sie Ihre Arbeit mit „OK“ bestätigen, werden die Einträge übernommen. Die neuen Benutzer erhalten automatisch die Berechtigung *USE. Dies lässt sich aber problemlos ändern, wie wir bereits festgestellt haben.

Natürlich können Sie sich im iSeries Navigator auch die gesicherten Objekte anzeigen lassen. Ich finde, dass die Darstellung im Navigator so sehr viel übersichtlicher ist, da hier die Objekte in drei Gruppen unterteilt werden:

- iSeries-Objekte, die in Bibliotheken gespeichert sind,
- iSeries-Dokumente, die in iSeries Ordnern gesichert wurden,
- und Objekte, die im IFS abgelegt sind.

9.9.4
Seite 10



Gesicherte Objekte

Objekte durch Berechtigungslisten schützen

Alles ist vorbereitet. Jetzt müssen Sie nur noch die Berechtigungslisten den entsprechenden Objekten zuordnen. Natürlich können Sie die Berechtigungslisten jedem Objekt einzeln zuordnen, indem Sie den Befehl EDTOBJAUT (Edit object authority) nutzen. Nur kann dieses Vorgehen ziemlich zeitaufwendig sein und empfiehlt sich daher nur, wenn Sie wenige Objekte ansprechen müssen. Besser ist es, Sie nutzen den Befehl GRTOBJAUT (Grant object authority).

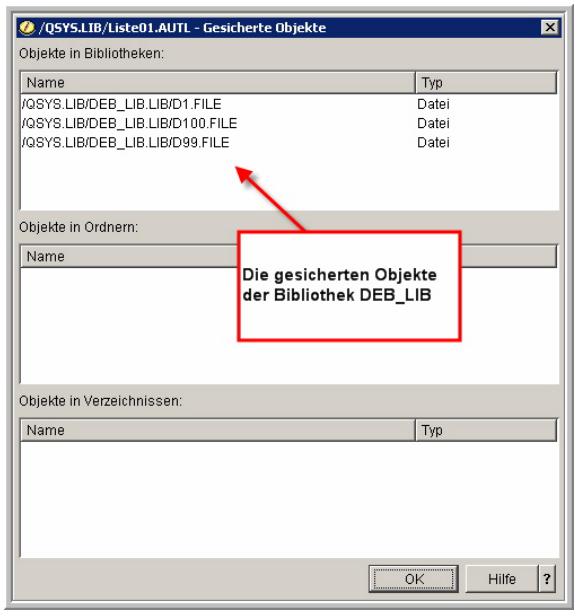
```
                    Objektberechtigung erteilen (GRTOBJAUT)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . .  *ALL          Name, generisch*, *ALL
  Bibliothek . . .    DEB_LIB     Name, *LIBL, *CURLIB, *ALL...
Objektart . . . . .   *ALL        *ALL, *ALRTBL, *BNDDIR...
ASP-Einheit . . . .   *           Name, *, *SYSBAS
Benutzer . . . . . .              Name, *PUBLIC
     + für weitere Werte
Berechtigung . . . .              *CHANGE, *ALL, *USE...
     + für weitere
Berechtigungsliste    Liste01     Name, *NONE
Bezugsobjekt . . .                Name
  Bibliothek . . .      *LIBL     Name, *LIBL, *CURLIB
Bezugsobjektart . .   *OBJTYPE    *OBJTYPE, *ALRTBL, *BNDDIR...
Referenz-ASP-Einheit  *           Name, *, *SYSBAS
Berechtigung ersetzen *NO         *NO, *YES
```

Objekte auswählen

Ein Objekt kann nur durch EINE Berechtigungsliste geschützt werden!

Der Befehl GRTOBJAUT

Sie sehen, dass ich mit einem Befehl alle Objekte der Bibliothek DEB_LIB durch unsere Berechtigungsliste schütze. Das Ergebnis sieht nach Ausführung des Befehls folgendermaßen aus:

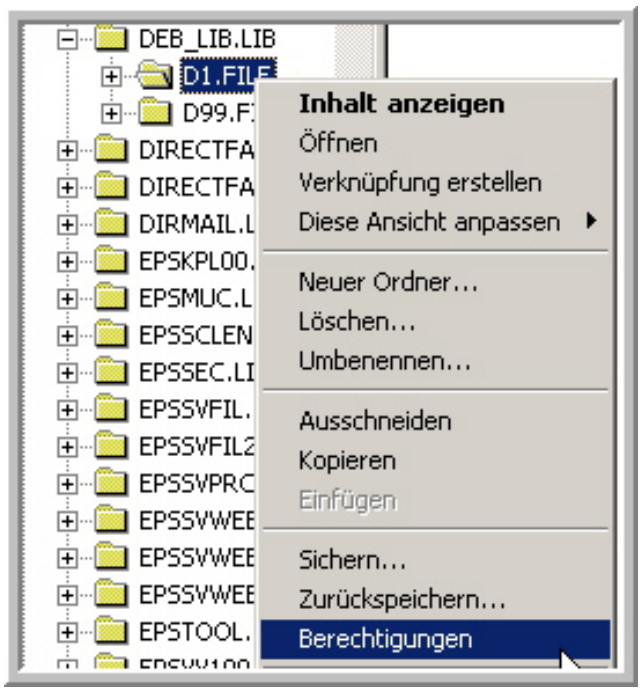


Das Ergebnis

9.9.4
Seite 12

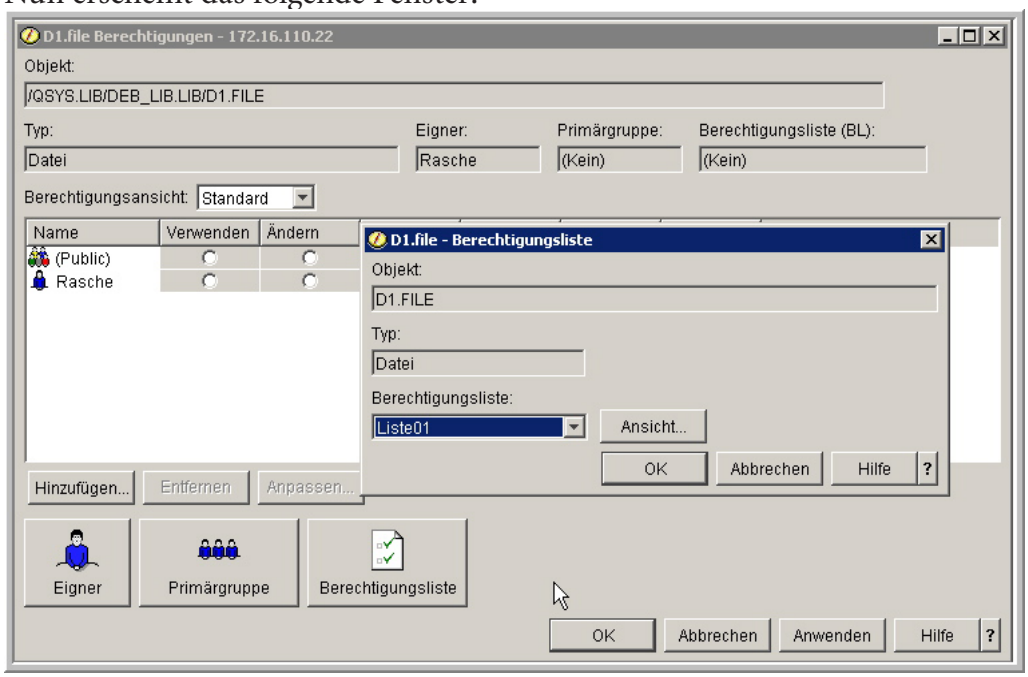
Jetzt erhalten die in der Berechtigungsliste hinterlegten Benutzer die hinterlegten Berechtigungen an den Objekten. Zukünftig reicht es aus, weitere Benutzer in die Listen aufzunehmen oder von der Liste zu entfernen, um die Berechtigungen zu entziehen oder zu gewähren. Genauso einfach ist es, weitere Objekte durch die Liste zu schützen: Sie müssen lediglich die Berechtigungsliste den Objekten zuordnen oder durch eine andere Liste ersetzen. Beachten Sie dabei, dass ein Objekt nur durch eine Berechtigungsliste geschützt werden kann.

Auch der iSeries Navigator ermöglicht es, neue Objekte einer Berechtigungsliste zuzuordnen. Dazu müssen Sie das IFS öffnen, einzelne Objekte mit der rechten Maustaste markieren und anschließend den Eintrag „Berechtigungen“ wählen. Daraufhin erscheint das folgende Fenster:



Objekte einer Berechtigungsliste zuordnen

Nun erscheint das folgende Fenster:



Einzelne Objekte einer Berechtigungsliste zuordnen

Leider ist es bislang nicht möglich, mehrere Objekte zu markieren und anschließend in einem Vorgang zuzuordnen, so dass der Navigator wenig geeignet erscheint, wenn Sie viele Objekte berücksichtigen müssen.

Neben der einfachen Handhabung bieten Berechtigungslisten **weitere Vorteile:**

- Sie können die Listen bearbeiten, während die Benutzer mit den gesicherten Objekten arbeiten.
- Falls Sie die gesicherten Objekte wieder herstellen müssen, ist eine erneute Zuordnung der Berechtigungslisten nicht erforderlich. Dies geschieht automatisch.
- Berechtigungslisten können nicht versehentlich gelöscht werden, denn das Betriebssystem stellt sicher, dass nur Listen gelöscht werden, die nicht verwendet werden.

Natürlich gibt es auch **Nachteile**.

Die Planung und Konfiguration der Berechtigungslisten erfordert etwas Zeit. Sie müssen Berechtigungslisten sorgfältig planen, um unnötigen System-Overhead zu vermeiden und um den Überblick über die bestehenden Listen und die gesicherten Objekte zu behalten. Ein Beispiel für die Planung und den Einsatz finden Sie im Kapitel „Ressourcenschutz durch Berechtigungslisten“.

9.9.4
Seite 14

9.9.5 Mit Benutzerprofilen arbeiten

Es gibt für einen Systemadministrator wohl keinen Befehl der ähnlich oft verwendet wird wie derjenige zum Bearbeiten von Benutzerprofilen. Das liegt wohl daran, dass dieser Befehl nicht nur zum Erstellen von Benutzerprofilen verwendet wird, sondern die einfachste Möglichkeit darstellt, gesperrte Kennwörter wieder freizugeben, Kennwörter für Benutzer zurückzusetzen etc. Mit WRKUSRPRF und F4 gelangen Sie zu den Parametern des Befehls.

```
                    Mit Benutzerprofilen arbeiten (WRKUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .   _________     Name, generisch*, *ALL

                Zusätzliche Parameter

Unterstützungsstufe  . . . . . .   *PRV        *PRV, *BASIC, *INTERMED...
```

WRKUSRPRF + F4

Hier können Sie die anzuzeigenden Benutzerprofile sowie die Unterstützungsstufe einschränken, um nur das/die Benutzerprofile anzuzeigen, die bearbeitet werden sollen.

Über die Unterstützungsstufe steuern Sie, welche Informationen Ihnen bei der Bearbeitung angezeigt werden sollen. Die Auswahl *BASIC z. B. zeigt Ihnen die Informationen in einer vereinfachten Darstellung an, bei der nur bestimmte Funktionen zur Verfügung stehen.

```
                          Mit Benutzerprofilen arbeiten

Auswahl eingeben und Eingabetaste drücken.
  1=Erstellen   2=Ändern   3=Kopieren   4=Löschen   5=Anzeigen
  12=Mit Objekten eines Eigners arbeiten

Ausw  Benutzerprofil  Text

  __    _________
  __      RENGEL        Robert Engel









                                                                      Ende
Parameter für Auswahlmöglichkeiten 1, 2, 3, 4 und 5 oder Befehl
===>
F3=Verlassen    F5=Aktualisieren    F12=Abbrechen    F16=Neuer Listenanfang
F17=Listenanfang bei    F21=Unterstützungsstufe auswählen    F24=Weitere
```

Mit Benutzerprofilen arbeiten

9.9.5
Seite 2

Sie können hier einzelne Benutzerprofile bearbeiten, neue Profile erstellen, kopieren, löschen und anzeigen sowie mit den Objekten arbeiten, deren Eigner das ausgewählte Benutzerprofil ist.

In dieser Anzeige haben Sie zudem die Möglichkeit, die Unterstützungsstufe generell zu ändern. Mit der Funktionstaste F21 setzen Sie die Unterstützungsstufe für Ihr Benutzerprofil nicht nur einmalig, sondern permanent.

```
                Unterstützungsstufe auswählen

  Aktuelle Unterstützungsstufe:   Erweitert


  Auswahl eingeben und Eingabetaste drücken.

    Unterstützungsstufe . . . .   2    1=Basis
                                       2=Erweitert




  F1=Hilfetext    F12=Abbrechen
```

Unterstützungsstufe einstellen

Der Wert für die Unterstützungsstufe ist hier nur exemplarisch zu sehen, gilt aber für eine Vielzahl von WRKxxx-Anzeigen gleichermaßen. Die Unterstützungsstufe können Sie an mehreren Stellen ändern, z. B.

- in einem WRKxxx-Befehl über das Schlüsselwort *ASTLVL (Assistance Level) nur für das einmalige Arbeiten mit dem Befehl;
- in einem WRKxxx-Befehl mit F21 zur permanenten Einstellung der Unterstützungsstufe nur für diesen Befehl;
- im Benutzerprofil über den Parameter „Unterstützungsstufe“ für die Anpassung der Unterstützungsstufe für alle Befehle, die dieser Benutzer aufruft;
- im Systemwert QASTLVL für die generelle Voreinstellung, wie neu angelegte Benutzerprofile ohne spezielle Einstellungen Befehlsanzeigen präsentiert bekommen.

Für die Unterstützungsstufe gibt es generell drei Auswahlmöglichkeiten:

***BASIC**
Die OA-Ebene der Systemanzeigen ist verfügbar. D.h. diese Anzeige ist vorwiegend für ungeübte Anwender vorgesehen, die eine Basisansicht der Parameter benötigten, ohne durch die Vielfalt der Werte verwirrt zu werden.

***INTERMED**
Eine Zwischenstufe der Systemanzeigen ist verfügbar. Hiermit sehen Sie die Parameter detaillierter und können die Schlüsselwörter einblenden.

***ADVANCED**
Eine erweiterte Stufe der Systemanzeigen ist verfügbar. Dies ist nicht für alle Befehle möglich, stellt aber die Spezialistenansicht von Befehlen dar.

Da der Befehl „Mit Benutzern arbeiten“ nicht alle drei Unterstützungsstufen anbietet (wie übrigens eine Menge anderer Befehle auch), zeige ich Ihnen im Folgenden exemplarisch die Darstellung des Befehls WRKSYSVAL (Anzeige Systemstatus) mit den unterschiedlichen Unterstützungsstufen:

```
                          Systemstatus anzeigen                  RAZLEE
                                                        16.02.13  09:01:01

Plattenspeicherplatz:
  Systemspeicher (in 1.000.000 Byte) . . . . . :     57219
  Belegter Systemspeicher  . . . . . :     76,87%

Benutzer:
  Angemeldet . . . . . :         2
  Vorübergehend abgemeldet . . . . . :         0
  Durch Systemabfrage oder Gruppenjobs ausgesetzt  . . . . :         0
  Abgemeldet mit noch nicht gedruckter Druckausgabe  . . . :        41

Stapeljobs:
  Wartet auf Nachrichten . . . . . :         0
  Wird ausgeführt  . . . . . :        60
  Bei Ausführung angehalten  . . . . . :         0
  Wird beendet . . . . . :         0
                                                                Weitere ...
Eingabetaste --> Weiter

F1=Hilfetext     F3=Verlassen    F5=Aktualisieren    F9=Befehlszeile
F12=Abbrechen    F21=Unterstützungsstufe auswählen
```

*WRKSYSSTS – Unterstützungsstufe *BASIC*

9.9.5
Seite 4

```
                          Mit Systemstatus arbeiten                  RAZLEE
                                                          16.02.13  09:02:56
% CPU benutzt  . . . . . :        3,1    Zusatzspeicher:
Abgelaufene Zeit . . . . :   15:56:52      System-ASP . . . . . :    57,21 G
Jobs im System . . . . . :       1231      % System-ASP benutzt . :    76,8724
% perm. Adressen . . . . :      0,007      Gesamtsumme  . . . . . :    57,21 G
% temp. Adressen . . . . :      0,016      Unges. Platz akt.
                                             belegt . . . . . :     3006 M
                                           Max. ungeschützt . . . :     3111 M
Änderungen (falls zulässig) eingeben und die Eingabetaste drücken.

System    Pool-     Reserv.    Max.  -DB-Seiten--  --Nicht-DB--
 Pool   Größe(M)  Größe (M)  Aktiv  fehl.  geles  fehl.  geles
   1     291,03     143,74  +++++    0,0    0,0    0,2    4,1
   2     683,03      24,52     42    0,1    3,9   13,9   47,6
   3    1058,67       8,63     52    0,0    0,0    0,0    0,0
   4      15,25       <.01      5    0,0    0,0    0,0    0,0
                                                              Ende
Befehl
===>
F3=Verlassen     F4=Bedienerführung    F5=Neuanzeige    F9=Auffinden
F12=Abbrechen    F19=Erweiterter Systemstatus           F24=Weitere Tasten
```

*WRKSYSSTS – Unterstützungsstufe *INTERMED*

```
                          Mit Systemstatus arbeiten                  RAZLEE
                                                          16.02.13  09:03:23
% CPU benutzt  . . . . . :        3,1    System-ASP . . . . . . . :    57,21 G
Abgelaufene Zeit . . . . :   15:57:18    % System-ASP benutzt . . :    76,8725
Jobs im System . . . . . :       1231    Gesamtzusatzspeicher . . :    57,21 G
% perm. Adressen . . . . :      0,007    Unges. Platz akt. belegt :     3006 M
% temp. Adressen . . . . :      0,016    Max. ungeschützt . . . . :     3111 M

Sys-    Pool-     Reserv.    Max.  -DB-Seiten-  -Nicht-DB--  Aktiv  Wart.  Aktiv
Pool   Größe M   Größe M     akt  fehl. geles  fehl. geles  Wart.  n.wäh  n.wäh
  1     291,03    143,74  +++++    0,0   0,0    0,2   4,1   18,7    0,0    0,0
  2     683,03     24,54     42    0,1   3,9   13,9  47,6  393,0    0,0    0,0
  3    1058,67      8,63     52    0,0   0,0    0,0   0,0    0,1    0,0    0,0
  4      15,25      <.01      5    0,0   0,0    0,0   0,0    0,0    0,0    0,0
                                                                      Ende
===>
F21=Unterstützungsstufe auswählen
```

*WRKSYSSTS – Unterstützungsstufe *ADVANCED*

Sie sehen hier sehr schön, wie die Anzeige mit zunehmender Unterstützungsstufe ins Detail geht.

Doch dies nur am Rande, zurück zu den Benutzerprofilen.

Die Funktionen zum Erstellen, Ändern und Anzeigen von Benutzerprofilen fasse ich in der Folge unter „Benutzerprofile bearbeiten“ zusammen. Zum Kopieren lässt sich wenig sagen, das ist mehr oder weniger selbsterklärend.

Doch bereits beim Löschen von Benutzerprofilen ist Vorsicht geboten. Löschen Sie bitte nicht einfach ein Benutzerprofil eines Anwenders, der z. B. aus dem Unternehmen ausgeschieden ist, sondern schauen Sie sich die Optionen beim Löschen des Profils genau an. Mehr dazu später.

Die Anzeige der Objekte, deren Eigner (Owner) das ausgewählte Benutzerprofil ist, zeigt Ihnen etwas mehr über den Benutzer an, weil Sie alle Objekte sehen, die dieser Benutzer erstellt oder übernommen hat. Auch dazu später mehr.

34. Ergänzung 3/2013

9.9.5
Seite 6

9.9.6 Benutzer erstellen/ändern

Mit Auswahl 1 bzw. 2 können Sie ein Benutzerprofil erstellen bzw. ändern, mit Auswahl 5 zeigen Sie das Profil an.

Was wird am häufigsten gemacht, wenn ein neuer Mitarbeiter ins Unternehmen kommt und ein Benutzerprofil für den Zugriff auf das Power i System braucht? Richtig, man sucht sich das Profil eines Kollegen raus, vorzugsweise das des Vorgängers in der gleichen Position, übernimmt bzw. kopiert dessen Berechtigungen und vergibt einen neuen Namen, ein neues Kennwort und allenfalls noch eine neue Bezeichnung.

Das ist grundsätzlich in Ordnung, allerdings sollte man sich nach dem Kopieren das neue Benutzerprofil genau anschauen, damit unerwünschte Nebeneffekte – wie zusätzliche Berechtigungen, die der Basisbenutzer vielleicht im Lauf der Zeit über Gruppenprofile (was das ist, wird später erklärt) erhalten hat – nicht ungeprüft für seinen Nachfolger übernommen werden. Auch Sonderwerte des Benutzerprofils würden so vielleicht unerwünschter Weise kopiert.

Um mehr Sachbezug zu bekommen, verwende ich bei der Erklärung der Parameter nicht die Funktion zum Erstellen eines Benutzerprofils, sondern die Anzeige zum Ändern.

Vorher ging es schon mal um die Unterstützungsebene. Nachfolgend eine Übersicht der Funktionen zum Ändern eines Benutzerprofils mit unterschiedlichen Unterstützungsstufen. (Ich arbeite im Weiteren mit der Unterstützungsstufe *INTERMED).

```
                              Benutzer ändern

Benutzer  . . . . . :   RENGEL

Auswahl eingeben und Eingabetaste drücken.

Benutzerbeschreibung  . .   Robert Engel
Kennwort  . . . . . .   *SAME
Benutzerart . . . . . .   *SECOFR          Art, F4=Liste
Benutzergruppe  . . . . .   RAZUSR          Name, F4=Liste

Befehlszeilenverwendung
  einschränken  . . . . .   N               J=Ja,N=Nein

Standardbibliothek  . . .                   Name
Standarddrucker . . . . .   *WRKSTN         Name, *WRKSTN, F4=Liste
In Programm anmelden  . .   *NONE           Name, *NONE
  Bibliothek  . . . . . .                   Name

Erstes Menü . . . . . .   MAIN              Name
  Bibliothek  . . . . . .     *LIBL         Name
                                                                  Weitere ...
F1=Hilfetext    F3=Verlassen    F5=Aktualisieren    F12=Abbrechen
```

*Benutzerprofil mit Unterstützungsstufe *BASIC*

9.9.6
Seite 2

Die am häufigsten verwendete Unterstützungsstufe *INTERMED zeigt Ihnen alle Details eines Benutzerprofils an und ermöglicht auch die Anzeige der Schlüselwörter für die einzelnenen Parameter des Profils.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > RENGEL         Name
Benutzerkennwort . . . . . *SAME          Zeichenwert, *SAME, *NONE
Kennwort auf abgelaufen setzen *NO        *SAME, *NO, *YES
Status . . . . . *ENABLED       *SAME, *ENABLED, *DISABLED
Benutzerklasse . . . . . *SECOFR        *SAME, *USER, *SYSOPR...
Unterstützungsstufe  . . . . . *SYSVAL        *SAME, *SYSVAL, *BASIC...
Aktuelle Bibliothek  . . . . . *CRTDFT        Name, *SAME, *CRTDFT
Aufzurufendes Startprogramm  . . *NONE        Name, *SAME, *NONE
  Bibliothek . . . . . .                      Name, *LIBL, *CURLIB
Anfangsmenü  . . . . . MAIN          Name, *SAME, *SIGNOFF
  Bibliothek . . . . . .   *LIBL          Name, *LIBL, *CURLIB
Möglichkeiten einschränken . . . *NO          *SAME, *NO, *PARTIAL, *YES
Text 'Beschreibung'  . . . . . 'Robert Engel'

                                                                      Ende
F3=Verlassen    F4=Bedienerf.    F5=Aktualisieren    F10=Zusätzl. Parameter
F12=Abbrechen   F13=Verwendung der Anzeige    F24=Weitere Tasten
```

*Benutzerprofil mit Unterstützungsstufe *INTERMED*

Mit der Funktionstaste F11 können Sie sich die Schlüsselwörter der Parameter anzeigen lassen, die dazu dienen, später auch mal eine Änderung eines Benutzerprofils ohne den Weg über das Benutzerinterface vornehmen zu können.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . USRPRF     >   RENGEL
Benutzerkennwort . . . . . PASSWORD       *SAME
Kennwort auf abgelaufen setzen  PWDEXP        *NO
Status . . . . . STATUS         *ENABLED
Benutzerklasse . . . . . USRCLS         *SECOFR
Unterstützungsstufe  . . . . . ASTLVL         *SYSVAL
Aktuelle Bibliothek  . . . . . CURLIB         *CRTDFT
Aufzurufendes Startprogramm  . . INLPGM         *NONE
  Bibliothek . . . . . .
Anfangsmenü  . . . . . INLMNU         MAIN
  Bibliothek . . . . . .                    *LIBL
Möglichkeiten einschränken . . . LMTCPB         *NO
Text 'Beschreibung'  . . . . . TEXT           'Robert Engel'

                                                                      Ende
F3=Verlassen    F4=Bedienerf.    F5=Aktualisieren    F10=Zusätzl. Parameter
F12=Abbrechen   F13=Verwendung der Anzeige    F24=Weitere Tasten
```

*Benutzerprofil mit Unterstützungsstufe *INTERMED und Anzeige der Schlüsselwörter*

Wenn Sie ein Benutzerprofil aufrufen, um es zu ändern, erhalten Sie zunächst eine Seite angezeigt (wie oben beim Benutzerprofil mit *INTERMED). Das ist aber beileibe nicht alles. Nur ein kleiner Teil wird auf der ersten Seite angezeigt. Auf die Vielfalt der Möglichkeiten können Sie mit Hilfe der Funktionstasten F9 und F10 zugreifen. F10 blendet dabei zusätzliche Parameter ein, F9 zeigt alle Parameter – auch diejenigen, die abhängig von Eingaben vorheriger Parameter sind – und eignet sich für eine Übersicht über alle Möglichkeiten, die eingegeben werden können.

So ein Benutzerprofil bietet eine Menge Einstellungsmöglichkeiten, mit denen unterschiedliche Bereiche der Darstellung und Sicherheit angepasst werden können. Schauen wir uns das mal im Detail an.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > RENGEL          Name
Benutzerkennwort . . . . . *SAME           Zeichenwert, *SAME, *NONE
Kennwort auf abgelaufen setzen *NO         *SAME, *NO, *YES
Status . . . . . *ENABLED      *SAME, *ENABLED, *DISABLED
Benutzerklasse . . . . . *SECOFR       *SAME, *USER, *SYSOPR...
Unterstützungsstufe  . . . . . *SYSVAL     *SAME, *SYSVAL, *BASIC...
Aktuelle Bibliothek  . . . . . *CRTDFT     Name, *SAME, *CRTDFT
Aufzurufendes Startprogramm  . . *NONE     Name, *SAME, *NONE
  Bibliothek . . . . . .                   Name, *LIBL, *CURLIB
Anfangsmenü  . . . . . MAIN           Name, *SAME, *SIGNOFF
  Bibliothek . . . . . .   *LIBL          Name, *LIBL, *CURLIB
Möglichkeiten einschränken . . . *NO       *SAME, *NO, *PARTIAL, *YES
Text 'Beschreibung'  . . . . . 'Robert Engel'
```

Benutzerprofil – Seite 1

Benutzerprofil

Dieser Parameter gibt das Benutzerprofil an, dessen Werte geändert werden sollen. Es kann ein numerischer Benutzerprofilname angegeben werden. Ein numerischer Benutzerprofilname muss mit dem Buchstaben Q beginnen.

Es können verschiedene Namenskonventionen realisiert werden, die von unternehmensinternen Regeln abhängig sein können. So vergeben manche kleinere Unternehmen Benutzerprofilnamen, bei denen an erster Stelle Vornamen und Nachnamen stehen, weil hierbei die Wahrscheinlichkeit doppelter Namen geringer ist, als wenn nur der Nachname oder nur der Vorname für das Benutzerprofil verwendet wird. Andere Unternehmen verwenden Nummerierungen (A15, B27 etc.) oder Benutzernamen, die Niederlassungsbezeichnungen mit beinhalten (MUCAMEIER, HAMBBECK etc.), die eine Zuordnung zur Filiale über den Benutzernamen ermöglichen und bei generischen Regeln die Verwaltung vereinfachen.

Grundsätzlich sind Sie in der Vergabe der Benutzerprofilnamen relativ frei (siehe unten), sollten aber – wenn möglich – Benutzernamen und Kennworte für iSeries-Systeme denen aus der Windows- oder Unix-Welt anpassen, um einen einfacheren Zugriff über Systemgrenzen hinweg zu ermöglichen.

Die folgenden von IBM gelieferten Objekte sind für diesen Parameter nicht gültig, weil es sich um reservierte Namen handelt:
QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QMGTC, QMSF, QNTP, QPEX, QPM400, QSNADS, QSPL, QSPLJOB, QSRVAGT, QSYS, QTCP, QTFTP, QTSTRQS, QYCMCIMOM, QYPSJSVR.

Benutzerkennwort

Dieser Parameter gibt das Kennwort an, mit dem sich ein Benutzer am System anmeldet. Das Kennwort ist einem Benutzerprofil zugeordnet und wird zur Darstellung des Benutzers im System verwendet. Das Kennwort sollte nur dem jeweiligen Benutzer bekannt sein. Es kann ein numerisches Kennwort angegeben werden.

Arbeitet das System mit Kennwortstufe 0 oder 1 und ist das Kennwort numerisch, so muss das Kennwort mit Q beginnen, z. B. Q1234. 1234 ist das Kennwort für die Anmeldung am System.

Die Kennwortstufe wird mit dem Systemwert QPWDLVL (Kennwortstufe) gesteuert.

Das neue Kennwort wird nicht anhand der Kennwortgültigkeitsregeln überprüft. Die Kennwortgültigkeitsregeln werden durch die Systemwerte (IBM i) definiert. Eine Beschreibung der Kennwortgültigkeitsregeln ist im Handbuch „System i Security Reference“, IBM Form SC41-5302, enthalten.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Diesem Benutzerprofil ist kein Kennwort zugeordnet. Benutzer können sich nicht mit einem Profil, für das PASSWORD(*NONE) angegeben ist, an einem System anmelden.

Wenn das System auf Kennwortstufe 0 oder 1 läuft, muss eine alphanumerische Zeichenfolge von maximal 10 Zeichen angegeben werden. Das erste Zeichen muss ein Buchstabe sein, die anderen Zeichen müssen alphanumerisch sein.

Wenn das System auf Kennwortstufe 2 oder 3 läuft, muss eine alphanumerische Zeichenfolge von maximal 128 Zeichen angegeben werden. Auf Kennwortstufe 2 oder 3 muss für das Kennwort Groß-/Kleinschreibung beachtet werden. Ist für die lokale Kennwortverwaltung (LCLPWDMGT) *NO angegeben, wird das lokale IBM i-Kennwort auf *NONE gesetzt, so dass für den Benutzer dieselben Einschränkungen gelten wie bei Angabe von *NONE für das Kennwort. Der angegebene Kennwortwert wird an andere IBM-Produkte oder -Lösungen gesendet, die eine Kennwortsynchronisation durchführen (siehe z. B. Integration von IBM i mit BladeCenter und System x unter http://www.ibm.com/systems/i/bladecenter/). Weitere Informationen zur Verwaltung der Kennwörter für das Produkt – wenn LCLPWDMGT(*NO) für das Benutzerprofil angegeben ist – sind in der entsprechenden Dokumentation zu finden.

Kennwort auf „abgelaufen" setzen (PWDEXP)

Dieser Parameter gibt an, ob das Kennwort eines Benutzers auf „abgelaufen" gesetzt ist. Ist das der Fall, muss der Benutzer das Kennwort ändern, um sich am System anmelden zu können. Beim Anmelden am System erscheint die Anzeige mit den Anmeldeinformationen, die auch eine Auswahl zum Ändern des Kennworts enthält.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NO**
Das Kennwort ist nicht auf „abgelaufen" gesetzt.

***YES**
Das Kennwort ist auf „abgelaufen" gesetzt.

9.9.6
Seite 6

Status (STATUS)

Dieser Parameter gibt den Status eines Benutzerprofils an. Das System deaktiviert ein Benutzerprofil, wenn Folgendes eintritt:

Das Benutzerprofil erreicht die maximal zulässige Anzahl an Kennwortüberprüfungen. Die maximale Anzahl von Kennwortüberprüfungen wurde erreicht, wenn die Anzahl der erfolglosen Kennwortüberprüfungsversuche die im Systemwert QMAXSIGN angegebene Grenze erreicht und im Systemwert QMAXSGNACN Auswahl 2 oder 3 angegeben wurde.

Ablaufdatum für Benutzerprofil wurde erreicht. Mit dem Befehl DSPUSRPRF (Benutzerprofil anzeigen) kann das Ablaufdatum für ein Benutzerprofil angezeigt werden.

Der Parameter STATUS ist im Befehl CRTUSRPRF (Benutzerprofil erstellen) oder im Befehl CHGUSRPRF (Benutzerprofil ändern) auf *DISABLED gesetzt.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***ENABLED**
Das Benutzerprofil berechtigt zur Anmeldung.

***DISABLED**
Das Benutzerprofil berechtigt erst dann zur Anmeldung, wenn es von einem berechtigten Benutzer erneut aktiviert wird. Stapeljobs können auch unter einem gesperrten Benutzerprofil übergeben werden.

Benutzerklasse (USRCLS)

Der Parameter „Benutzerklasse“ gibt die Art des Benutzers an, der einem Benutzerprofil zugeordnet ist: Sicherheitsbeauftragter, Sicherheitsadministrator, Programmierer, Systembediener oder Benutzer. Die Benutzerklasse steuert die im Menü gezeigten Auswahlmöglichkeiten. Sonderberechtigungen werden nur erteilt, wenn *USRCLS für den Parameter „Sonderberechtigung“ (SPCAUT) angegeben wird. Wurde SPCAUT(*USRCLS) angegeben, variieren die Sonderberechtigungen abhängig vom QSECURITY-Wert.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***USER**
Auf QSECURITY-Stufe 10 oder 20 verfügt der Benutzer über die Berechtigungen *ALLOBJ und *SAVSYS.

Auf QSECURITY-Stufe 30 oder höher hat der Benutzer keine Sonderberechtigungen.

***SECOFR**
Auf allen Sicherheitsstufen verfügt der Sicherheitsbeauftragte über die folgenden Sonderberechtigungen:

*ALLOBJ

*SAVSYS

*JOBCTL

*SERVICE

*SPLCTL

*SECADM

*AUDIT

*IOSYSCFG

***SECADM**
Auf QSECURITY-Stufe 10 oder 20 verfügt der Sicherheitsadministrator über die Sonderberechtigungen *ALLOBJ, *SAVSYS, *SECADM und *JOBCTL.

Auf QSECURITY-Stufe 30 oder höher verfügt der Benutzer über die Sonderberechtigungen *SECADM.

***PGMR**
Auf QSECURITY-Stufe 10 oder 20 verfügt der Programmierer über die Sonderberechtigungen *ALLOBJ, *SAVSYS und *JOBCTL.

Auf QSECURITY-Stufe 30 oder höher hat der Benutzer keine Sonderberechtigungen.

***SYSOPR**
Auf QSECURITY-Stufe 10 oder 20 verfügt der Systembediener über die Sonderberechtigungen *ALLOBJ, *SAVSYS und *JOBCTL.

Auf QSECURITY-Stufe 30 oder höher verfügt der Benutzer über die Sonderberechtigungen *SAVSYS und *JOBCTL.

Unterstützungsstufe (ASTLVL)

Dieser Parameter gibt an, welche Unterstützungsstufe verwendet werden soll.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Die im Systemwert QASTLVL definierte Unterstützungsstufe wird verwendet.

***BASIC**
Die einfache Schnittstelle für die Oberfläche von Anwendungen wird verwendet.

***INTERMED**
Die Systemschnittstelle wird benutzt.

***ADVANCED**
Die Systemschnittstelle für Experten wird verwendet. Damit mehr Einträge in der Liste angezeigt werden können, werden Auswahl- und Funktionstasten nicht angezeigt. Verfügt ein Befehl nicht über eine Schnittstelle für Experten (*ADVANCED), wird die normale Schnittstelle (*INTERMED) verwendet.

Aktuelle Bibliothek (CURLIB)

Dieser Parameter gibt den Namen der aktuellen Bibliothek an, die dem gerade durchgeführten Job zugeordnet ist. Beziehungsweise gibt dieser Parameter den Namen der Bibliothek an, die als aktuelle Bibliothek für einen Benutzer verwendet werden soll. Wenn *PARTIAL oder *YES für den Parameter „Möglichkeiten einschränken“ (LMTCPB) des Befehls CRTUSRPRF (Benutzerprofil erstellen) oder CHGUSRPRF (Benutzerprofil ändern) angegeben ist, kann der Benutzer die aktuelle Bibliothek weder beim Anmelden noch mit dem Befehl CHGPRF (Profil ändern) ändern.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***CRTDFT**
Der Benutzer hat keine aktuelle Bibliothek. Die Bibliothek QGPL wird standardmäßig als aktuelle Bibliothek benutzt.

Name
Den Namen der Bibliothek angeben, die als aktuelle Bibliothek für den Benutzer verwendet werden soll.

9.9.6
Seite 10

Aufzurufendes Startprogramm (INLPGM)

Dieser Parameter gibt bei interaktiven Jobs das Programm an, das aufgerufen wird, wenn ein neuer Leitwegschritt mit QCMD als Verarbeitungsprogramm der Anforderung gestartet wird. Wenn *PARTIAL oder *YES für den Parameter „Möglichkeiten einschränken“ (LMTCPB) angegeben ist, kann der Programmwert weder beim Anmelden noch mit dem Befehl CHGPRF (Profil ändern) geändert werden. Es können keine Parameter an das Programm übergeben werden.

Der Name einer IBM System /36-Umgebungsprozedur kann als Startprogramm angegeben werden, wenn die Prozedur eine Teildatei der Datei QS36PRC (in der Bibliotheksliste oder der angegebenen Bibliothek) ist und eine der folgenden Bedingungen wahr ist:

– *S36 wurde im Parameter SPCENV angegeben.

– Im Parameter SPCENV wurde *SYSVAL angegeben und der Systemwert QSPCENV lautet *S36.

Gültige Einzelwerte sind

***SAME**
Der Wert ändert sich nicht.

***NONE**
Nach Anmeldung des Benutzers wird kein Programm aufgerufen. Wurde für den Parameter Anfangsmenü (INLMNU) ein Menüname angegeben, wird dieses Menü angezeigt.

Qualifikationsmerkmal 1: Aufzurufendes Startprogramm

Name
Den Namen des Programms angeben, das nach der Anmeldung des Benutzers aufgerufen wird.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Das Programm wird in der aktuellen Bibliothek für den Job gesucht. Wenn keine Bibliothek als aktuelle Jobbibliothek angegeben ist, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, in der sich das Startprogramm befindet.

Anfangsmenü (INLMNU)

Dieser Parameter gibt das Anfangsmenü an, das angezeigt wird, wenn sich ein Benutzer am System anmeldet und das Leitwegprogramm des Benutzers der Befehlsprozessor QCMD ist. Wenn *YES für den Parameter „Möglichkeiten einschränken“ (LMTCPB) angegeben ist, kann der Benutzer das Menü weder beim Anmelden noch mit dem Befehl CHGPRF (Profil ändern) ändern.

Ein Menü der IBM System /36-Umgebung kann als Anfangsmenü angegeben werden, wenn eine der folgenden Bedingungen wahr ist:

– *S36 ist für den Parameter „Sonderumgebung“ (SPCENV) angegeben.
– Im Parameter SPCENV wurde *SYSVAL angegeben und der Systemwert QSPCENV lautet *S36.

Gültige Einzelwerte sind

***SAME**
Der Wert ändert sich nicht.

***SIGNOFF**
Das System meldet den Benutzer nach Beendigung des Programms ab. Dieser Wert ist für Benutzer vorgesehen, die nur zur Ausführung des Programms berechtigt sind.

Qualifikationsmerkmal 1: Anfangsmenü

Name
Den Namen des Anfangsmenüs angeben, das nach der Anmeldung des Benutzers am System aufgerufen wird.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Zur Lokalisierung des Menüs wird die aktuelle Bibliothek des Jobs verwendet. Wenn keine Bibliothek als aktuelle Jobbibliothek angegeben ist, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, in der sich das Anfangsmenü befindet.

Möglichkeiten einschränken (LMTCPB)

Dieser Parameter gibt an, bis zu welcher Grenze ein Benutzer das Programm, das Menü, die aktuelle Bibliothek und die Werte des Programms für die Abruftaste steuern kann. Es wird außerdem festgelegt, ob der Benutzer Befehle über die Befehlszeile ausführen kann. Auf Sicherheitsstufe 10 wird der Parameter ignoriert.

Beim Erstellen oder Ändern der Benutzerprofile anderer Benutzer können in diesem Parameter keine Werte angegeben werden, die anderen Benutzern umfangreichere Möglichkeiten einräumen als im eigenen Benutzerprofil definiert sind. Ist zum Beispiel im eigenen Benutzerprofil *PARTIAL beim Parameter „Möglichkeiten einschränken“ (LMTCPB) angegeben, kann für andere Benutzer *PARTIAL oder *YES angegeben werden. Die Angabe *NO für einen anderen Benutzer ist nicht zulässig.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NO**
Die Werte für Programm, Menü und aktuelle Bibliothek können bei der Anmeldung eines Benutzers im System geändert werden. Der Benutzer kann mit Hilfe des Befehls CHGPRF (Profil ändern) das Startprogramm, das Anfangsmenü, die aktuelle Bibliothek bzw. das Programm für die Abruftaste in seinem eigenen Benutzerprofil ändern. Befehle können über die Befehlszeile ausgeführt werden.

***PARTIAL**
In der Anmeldeanzeige können die Werte für Programm und aktuelle Bibliothek nicht geändert werden. Das Menü kann geändert werden und Befehle können über die Befehlszeile ausgeführt werden. Das Menü kann mit dem Befehl CHGPRF (Profil ändern) geändert werden. Das Programm, die aktuelle Bibliothek und das Programm für die Abruftaste können mit dem Befehl CHGPRF nicht geändert werden.

***YES**
In der Anmeldeanzeige können die Werte für Programm, Menü und aktuelle Bibliothek nicht geändert werden. Es können keine Befehle über die Befehlszeile oder durch Auswahl in einem Befehlsgruppenmenü, wie z. B. CMDADD, ausgeführt werden, Befehle können aber nach wie vor über die Befehlseingabeanzeige ausgeführt werden. Der Benutzer kann das Programm, das Menü, die aktuelle Bibliothek oder das Programm für die Abruftaste mit dem Befehl CHGPRF (Profil ändern) nicht ändern.

Text ‚Beschreibung' (TEXT)

Dieser Parameter betrifft den Text, mit dem das Objekt kurz beschrieben wird.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***BLANK**
Es wird kein Text angegeben.

Beschreibung
Maximal 50 Zeichen Text in Hochkommas angeben.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.


                Zusätzliche Parameter

Sonderberechtigung . . . . . .   ALLOBJ       *SAME, *USRCLS, *NONE...
                                 *AUDIT
                                 *IOSYSCFG
                                 *JOBCTL
                                 *SAVSYS
                                 *SECADM
                                 *SERVICE
                                 *SPLCTL
Sonderumgebung . . . . . .       *SYSVAL       *SAME, *SYSVAL, *NONE, *S36
Anmeldeinformationen anzeigen .  *SYSVAL       *SAME, *NO, *YES, *SYSVAL
Intervall für Kennwortablauf . .  *SYSVAL      1-366, *SAME, *SYSVAL, *NOMAX
Kennwortänderung blockieren  . .  *SYSVAL      1-99, *SAME, *SYSVAL, *NONE
Lokale Kennwortverwaltung  . . .  *YES         *SAME, *YES, *NO
```

Benutzerprofil – Seite 2

9.9.6
Seite 14

Sonderberechtigung (SPCAUT)

Dieser Parameter gibt die Sonderberechtigungen eines Benutzers an. Sonderberechtigungen sind zum Ausführen bestimmter Funktionen im System erforderlich. Sie können vielen der vom System bereitgestellten Benutzerprofile, einschließlich QSECOFR und QSYS, nicht entzogen werden.

Normalerweise werden folgende Sonderberechtigungen erteilt:

- Die Sonderberechtigung zur Systemsicherung (*SAVSYS) für Benutzer, die für die Systembedienung zuständig sind.
- Die Sonderberechtigung zur E/A-Systemkonfiguration (*IOSYSCFG) für Benutzer, die für das Ändern der Konfiguration von E/A-Einheiten des Systems zuständig sind.
- Der Benutzer erhält die Sonderberechtigung zur Jobsteuerung (*JOBCTL). Mit dieser Berechtigung kann der Benutzer sämtliche Jobs, die im System ausgeführt werden oder die sich in einer Jobwarteschlange oder Ausgabewarteschlange befinden, für die OPRCTL (*YES) angegeben ist, ändern, anzeigen, anhalten, freigeben, abbrechen oder löschen. Der Benutzer verfügt außerdem über die Berechtigung zum Laden des Systems, zum Starten von Ausgabeprogrammen und zum Stoppen aktiver Subsysteme.
- Die Sonderberechtigung des Sicherheitsadministrators (*SECADM) zur Erstellung, Änderung oder Löschung von Benutzerprofilen.
- Die Sonderberechtigung für alle Objekte (*ALLOBJ) für Benutzer, die mit Systemressourcen arbeiten.
- Die Servicesonderberechtigung (*SERVICE) für Benutzer, die Servicefunktionen ausführen.
- Die Sonderberechtigung zur Spool-Steuerung (*SPLCTL) für Benutzer, die alle den Spool-Betrieb betreffenden Funktionen ausführen.
- Die Sonderberechtigung *AUDIT für Benutzer, die Protokollierungsfunktionen ausführen.

Einschränkungen:

- Das Benutzerprofil, das ein anderes Benutzerprofil erstellt oder ändert, muss über alle zu vergebenden Sonderberechtigungen verfügen. Ein Benutzer muss über alle Sonderberechtigungen verfügen, damit er einem anderen Benutzerprofil alle Sonderberechtigungen erteilen kann.
- Ein Benutzer muss bei Verwendung des Befehls CRTUSRPRF über die Sonderberechtigungen *ALLOBJ und *SECADM verfügen, um einem anderen Benutzer die Sonderberechtigung *SECADM erteilen zu können.
- Ein Benutzer muss bei Verwendung des Befehls CHGUSRPRF über die Sonderberechtigungen *ALLOBJ, *SECADM und *AUDIT verfügen, um einem anderen Benutzer die Sonderberechtigung *AUDIT erteilen zu können.

Gültige Einzelwerte sind:

***SAME**
Der Wert ändert sich nicht.

***USRCLS**
Einem Benutzer werden abhängig von dem für den Parameter „Benutzerklasse“ (USRCLS) angegebenen Wert Sonderberechtigungen erteilt.

***NONE**
Einem Benutzer werden keine Sonderberechtigungen erteilt.

Weitere Werte

***ALLOBJ**
Einem Benutzer wird die Berechtigung für alle Objekte erteilt. Er kann auf alle Systemressourcen zugreifen, unabhängig davon, ob er über persönliche Berechtigungen verfügt oder nicht.

***AUDIT**
Einem Benutzer wird die Protokollierungsberechtigung erteilt, mit der Protokollierungsfunktionen ausgeführt werden können. Protokollierungsfunktionen schließen das Ein- und Ausschalten der Protokollierung für das System sowie die Steuerung der Protokollierungsstufe für ein Objekt oder einen Benutzer ein.

***JOBCTL**
Einem Benutzer wird die Berechtigung zur Jobsteuerung erteilt. Mit dieser Berechtigung kann der Benutzer sämtliche Jobs, die im System ausgeführt werden oder die sich in einer Job- oder Ausgabewarteschlange befinden, für die OPRCTL (*YES) angegeben ist, ändern, anzeigen, anhalten, freigeben, abbrechen oder löschen. Der Benutzer hat auch die Berechtigung, Ausgabeprogramme zu starten und aktive Subsysteme anzuhalten.

***SAVSYS**
Einem Benutzerprofil wird die Berechtigung zur Systemsicherung erteilt. Diese Berechtigung erlaubt dem Benutzer, alle Objekte im System zu sichern, zurückzuspeichern und den von diesen Objekten belegten Speicherplatz freizugeben, unabhängig davon, ob er über die Objektverwaltungsberechtigung verfügt oder nicht.

***IOSYSCFG**
Einem Benutzer wird die Berechtigung für E/A-Systemkonfigurationen erteilt. Damit erhält er die Berechtigung zum Ändern der Konfiguration von E/A-Einheiten des Systems.

***SECADM**
Einem Benutzer wird die Berechtigung des Sicherheitsadministrators erteilt. Er kann Benutzerprofile erstellen, ändern oder löschen, wenn er für die Befehle CRTUSRPRF (Benutzerprofil erstellen), CHGUSRPRF (Benutzerprofil ändern) und DLTUSRPRF (Benutzerprofil löschen) sowie das Benutzerprofil berechtigt ist. Diese Berechtigung befugt nicht zur Erteilung von Sonderberechtigungen, über die dieses Benutzerprofil nicht selbst verfügt. Um einem anderen Benutzer die Sonderberechtigung *SECADM erteilen zu können, muss ein Benutzer die Sonderberechtigungen *ALLOBJ und *SECADM haben.

***SERVICE**
Einem Benutzer wird die Serviceberechtigung erteilt. Er darf Servicefunktionen ausführen.

***SPLCTL**
Einem Benutzer wird die Berechtigung zur Spool-Steuerung erteilt. Er darf alle Spool-Funktionen ausführen.

Sonderumgebung (SPCENV)

Dieser Parameter gibt die Sonderumgebung an, in welcher der Benutzer nach der Anmeldung arbeitet.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QSPCENV wird verwendet, um die Systemumgebung nach der Anmeldung des Benutzers im System festzulegen.

***NONE**
Der Benutzer arbeitet nach der Anmeldung am System in der IBM i-Systemumgebung.

***S36**
Der Benutzer arbeitet nach der Anmeldung im System in der Umgebung IBM System /36.

Anmeldeinformationen anzeigen (DSPSGNINF)

Dieser Parameter gibt an, ob die Anzeige „Anmeldungsinformationen“ angezeigt wird.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Mit dem Systemwert QDSPSGNINF kann festgelegt werden, ob die Anzeige „Anmeldeinformationen“ aufgerufen wird.

***NO**
Die Anzeige mit den Anmeldeinformationen wird nicht aufgerufen.

***YES**
Die Anzeige mit den Anmeldeinformationen wird aufgerufen.

Intervall für Kennwortablauf (PWDEXPITV)

Dieser Parameter gibt an, in wie viel Tagen das Kennwort verfällt.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Mit dem Systemwert QPWDEXPITV kann der Zeitraum festgelegt werden, nach dem das Kennwort verfällt.

***NOMAX**
Das Kennwort wird nicht ungültig.

1-366
Die Anzahl der Tage seit der letzten Kennwortänderung bis zum Verfall des aktuellen Kennworts angeben. Gültig sind Werte von 1 bis 366.

9.9.6
Seite 18

Kennwortänderung blockieren (PWDCHGBLK)

Dieser Parameter gibt den Zeitraum an, in dem ein Kennwort nach einer erfolgreichen Kennwortänderung blockiert ist, d. h., nicht geändert werden darf. Mithilfe dieses Werts kann verhindert werden, dass Benutzer dasselbe abgelaufene Kennwort erneut benutzen, indem sie ihr Kennwort wiederholt ändern, um wieder den abgelaufenen Kennwortwert zu erhalten (dies würde der Absicht des Systemwerts QPWDRQDDIF widersprechen). Der Parameter verhindert jedoch nicht, dass der Systemadministrator einen Befehl wie CHGUSRPRF (Benutzerprofil ändern) zum Ändern eines Kennworts verwenden kann.

Außerdem verhindert dieser Parameter nicht, dass ein Benutzer sein Profilkennwort ändern kann, wenn der Wert für PWDEXP *YES ist. Dies ermöglicht dem Sicherheitsadministrator, ein Benutzerprofil mit einem abgelaufenen Kennwort zu erstellen und dem Benutzer zu erlauben, sich einmal anzumelden und das Kennwort zu ändern, ohne dass er durch den Wert zum Blockieren der Kennwortänderung daran gehindert würde.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Mit dem Systemwert QPWDCHGBLK kann der Wert für „Kennwortänderung blockieren“ festgelegt werden.

***NONE**
Das Kennwort kann jederzeit geändert werden.

1-99
Gibt die Anzahl Stunden an, die ein Benutzer nach einer erfolgreichen Kennwortänderung warten muss, bevor er das Kennwort erneut ändern kann.

Lokale Kennwortverwaltung (LCLPWDMGT)

Dieser Parameter gibt an, ob das Kennwort eines Benutzerprofils lokal verwaltet werden soll.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***YES**
Das Kennwort wird auf dem lokalen System verwaltet.

***NO**
Das Kennwort wird nicht auf dem lokalen System verwaltet. Bei Angabe dieses Werts wird das lokale IBM i-Kennwort auf *NONE gesetzt. Der im Kennwortparameter angegebene Kennwortwert wird an andere IBM-Produkte oder -Lösungen gesendet, die eine Kennwortsynchronisation durchführen (siehe z. B. Integration von IBM i mit BladeCenter und System x unter http://www.ibm.com/systems/i/bladecenter/).

Benutzer können ihr eigenes Kennwort in diesem Fall mit dem Befehl CHGPWD (Kennwort ändern) nicht ändern. Sie können sich außerdem nicht direkt am System anmelden.

Die Angabe dieses Werts wirkt sich auf andere IBM-Produkte oder -Lösungen aus, die eine Kennwortsynchronisation durchführen (siehe z. B. Integration von IBM i mit BladeCenter und System x unter http://www.ibm.com/systems/i/bladecenter/). Einzelheiten sind in der Dokumentation zu dem Produkt oder der Lösung zu finden.

Dieser Wert sollte verwendet werden, wenn ein Benutzer über eine andere Plattform, wie z. B. Windows, auf das System zugreifen muss.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Einheitensitzungen begrenzen . .   *SYSVAL        *SAME, *SYSVAL, *YES, *NO...
Tastaturpufferung  . . . . . .     *SYSVAL        *SAME, *SYSVAL, *NO...
Maximal zulässiger Speicher  . .   *NOMAX         Kilobyte, *SAME, *NOMAX
Höchste Planungspriorität  . . .   3             0-9, *SAME
Jobbeschreibung  . . . . . .       QDFTJOBD       Name, *SAME
  Bibliothek . . . . . .             QGPL         Name, *LIBL, *CURLIB
Gruppenprofil  . . . . . .         RAZUSR         Name, *SAME, *NONE
Eigner . . . . . .                 *USRPRF        *SAME, *USRPRF, *GRPPRF
Gruppenberechtigung  . . . . .     *NONE          *SAME, *NONE, *ALL...
Art der Gruppenberechtigung  . .   *PRIVATE       *PRIVATE, *PGP, *SAME
Zusätzliche Gruppenprofile . . .   *NONE          Name, *SAME, *NONE
     + für weitere Werte
Berechnungscode  . . . . . .       *BLANK
Dokumentkennwort . . . . . .       *SAME          Name, *SAME, *NONE
Nachricht- warteschl.  . . . . .   RENGEL         Name, *SAME, *USRPRF
  Bibliothek . . . . . .             QUSRSYS      Name, *LIBL, *CURLIB
```

Benutzerprofil – Seite 3

9.9.6
Seite 20

Einheitensitzungen begrenzen (LMTDEVSSN)

Dieser Parameter gibt an, ob die Anzahl der für einen Benutzer zulässigen Einheitensitzungen begrenzt werden soll. Davon sind jedoch nicht SYSREQ oder ein zweites Anmelden betroffen.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Mit dem Systemwert QLMTDEVSSN wird festgelegt, ob ein Benutzer nur eine begrenzte Anzahl Einheitensitzungen anmelden kann.

***NO**
Der Benutzer ist nicht auf eine bestimmte Anzahl von Einheitensitzungen begrenzt.

***YES**
Der Benutzer kann nur eine Einheitensitzung anmelden.

0
Der Benutzer ist nicht auf eine bestimmte Anzahl von Einheitensitzungen begrenzt. Dieser Wert hat dieselbe Bedeutung wie *NO.

1
Der Benutzer kann nur eine Einheitensitzung anmelden. Dieser Wert hat dieselbe Bedeutung wie *YES.

2-9
Der Benutzer wird auf die angegebene Anzahl von Einheitensitzungen begrenzt.

Tastaturpufferung (KBDBUF)

9.9.6
Seite 21

Dieser Parameter gibt den Tastaturpufferungswert an, der verwendet wird, wenn für ein Benutzerprofil ein Job initialisiert wird. Wenn die Eingabepufferung aktiviert ist, können die Tastenanschläge gepuffert werden. Wenn die Abruftastenpufferung aktiviert ist, wird die Abruftaste wie jede andere Taste gepuffert. Ist sie nicht aktiviert, wird die Abruftaste nicht gepuffert und selbst dann an das System gesendet, wenn bei dem Datensichtgerät die Eingabe gesperrt ist. Dieser Wert kann auch durch eine Benutzeranwendung gesetzt werden. Weitere Informationen enthält das Handbuch „API-Themensammlung“ in der Kategorie „Programmierung“ im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QKBDBUF wird verwendet, um den Tastaturpufferungswert zu bestimmen.

***NO**
Die Eingabepufferung und die Abruftastenpufferung werden nicht aktiviert.

***TYPEAHEAD**
Die Eingabepufferung wird aktiviert, die Abruftastenpufferung jedoch nicht.

***YES**
Die Eingabepufferung und die Abruftastenpufferung werden aktiviert.

9.9.6
Seite 22

Maximal zulässiger Speicher (MAXSTG)

Dieser Parameter gibt die maximale Größe des Zusatzspeichers (in Kilobyte) an, der einem Benutzerprofil zur Speicherung von permanenten Objekten zugeordnet wird. Wird das Maximum überschritten, wenn ein interaktiver Benutzer versucht, ein Objekt zu erstellen, wird eine Fehlernachricht angezeigt und das Objekt wird nicht erstellt. Wird das Maximum bei der Erstellung eines Objekts in einem Stapeljob überschritten, wird eine Fehlernachricht an das Jobprotokoll gesendet (abhängig von der Protokollierungsstufe des Jobs) und das Objekt wird nicht erstellt.

Der Speicher wird in Segmenten von jeweils 4 KB zugeordnet. Wird z. B. MAXSTG(9) angegeben, werden dem Profil 12 KB Speicher zugeordnet.

Bei der Planung des maximalen Speicherplatzes für Benutzerprofile müssen folgende Systemaktionen berücksichtigt werden:

Bei einer Wiederherstellungsoperation wird dem Benutzer, der die Operation durchführt, Speicherplatz zugeordnet und dann das Objekt an den Eigner übertragen. Bei einer Wiederherstellung mit großem Datenvolumen muss MAXSTG(*NOMAX) angegeben werden.

Einem Benutzerprofil, das einen Journalempfänger erstellt, wird der erforderliche Speicherplatz entsprechend dem größer werdenden Empfänger zugeordnet. Werden neue Empfänger mit JRNRCV(*GEN) erstellt, wird der Speicherplatz weiterhin demjenigen Benutzerprofil zugeordnet, dem der aktive Journalempfänger gehört. Handelt es sich um einen sehr aktiven Journalempfänger, muss MAXSTG(*NOMAX) angegeben werden.

Benutzerprofile, die erstellte Objekte an ihr Gruppenprofil übertragen, müssen über entsprechend großen Speicherplatz für die Aufnahme der Objekte verfügen, bevor diese an das Gruppenprofil übertragen werden.

Dem Eigner der Bibliothek wird Speicherplatz für die Beschreibungen der Objekte zugeordnet, die in der Bibliothek gespeichert sind, selbst wenn die Objekte einem anderen Benutzerprofil gehören. Beispiele für solche Objekte sind Text- und Programmreferenzen.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NOMAX**
Diesem Benutzerprofil wird der erforderliche Speicherplatz zugewiesen.

Größe
Den maximalen Speicherplatz für den Benutzer in Kilobyte angeben.

Höchste Planungspriorität (PTYLMT)

Dieser Parameter gibt die höchste Planungspriorität an, die ein Benutzer bei jedem dem System zu übergebenden Job haben darf. Dieser Wert steuert die Jobverarbeitungspriorität sowie die Ausgabepriorität für jeden Job, der unter diesem Benutzerprofil ausgeführt wird. Das bedeutet, dass die für die Parameter JOBPTY und OUTPTY in einem beliebigen Jobbefehl angegebenen Werte den PTYLMT-Wert des Benutzerprofils, unter dem der Job ausgeführt wird, nicht überschreiten können. Der Wert der Planungspriorität liegt zwischen 0 und 9, wobei 0 die höchste und 9 die niedrigste Priorität bezeichnet.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

0-9
Einen Wert zwischen 0 und 9 für die höchste Planungspriorität angeben, die dem Benutzer erlaubt ist.

Jobbeschreibung (JOBD)

Dieser Parameter gibt die Jobbeschreibung an, die für diejenigen Jobs verwendet wird, die über Subsystemdatenstationseinträge gestartet werden. Falls die Jobbeschreibung beim Erstellen oder Ändern eines Benutzerprofils noch nicht vorhanden ist, muss ein Bibliotheksqualifikationsmerkmal angegeben werden, da der Jobbeschreibungsname im Benutzerprofil gespeichert ist.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

Qualifikationsmerkmal 1: Jobbeschreibung

Name
Den Namen der Jobbeschreibung angeben, die für die Datenstationseinträge verwendet wird, deren Jobbeschreibungsparameterwerte auf den Benutzer JOBD(*USRPRF) hinweisen.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Die aktuelle Bibliothek für den Thread wird durchsucht. Ist keine aktuelle Bibliothek für den Thread angegeben, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, die durchsucht werden soll.

9.9.6
Seite 24

Gruppenprofil (GRPPRF)

Dieser Parameter gibt den Namen des Gruppenprofils eines Benutzers an, dessen Berechtigung verwendet wird, wenn dem Benutzer keine spezielle Berechtigung erteilt wurde. Der aktuelle Benutzer dieses Befehls muss über die Objektverwaltungsberechtigung (*OBJMGT) sowie die Änderungsberechtigung (*CHANGE) für das Profil verfügen, das für den Parameter Gruppenprofil (GRPPRF) angegeben ist. Die Berechtigung *OBJMGT kann nicht durch eine Programmübernahmeoperation erworben werden.

Wenn ein Gruppenprofil angegeben wird, erhält der Benutzer automatisch die Berechtigungen *CHANGE und *OBJMGT für das Gruppenprofil.

Die folgenden von IBM gelieferten Objekte sind für diesen Parameter nicht gültig.

QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPM400, QRJE, QSNADS, QSPL, QSPLJOB, QSRV, QSRVAGT, QSRVBAS, QSYS, QTCM, QTCP, QTFTP, QTSTRQS, QWEBADMIN, QWSERVICE, QYCMCIMOM, QYPSJSVR.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Das Benutzerprofil verfügt nicht über ein Gruppenprofil.

Name
Den Namen des mit einem Benutzerprofil zu verwendenden Gruppenprofils angeben.

Eigner (OWNER)

Dieser Parameter gibt an, welches Benutzerprofil der Eigner der Objekte werden soll, die von einem Benutzer erstellt werden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***USRPRF**
Das zum Job gehörige Benutzerprofil ist Eigner des Objekts.

***GRPPRF**
Das Gruppenprofil wird zum Eigner der neu erstellten Objekte und erhält alle Berechtigungen für das Objekt. Das dem Job zugeordnete Benutzerprofil hat keine spezielle Berechtigung für das Objekt. Bei Angabe von *GRPPRF muss für den Parameter Gruppenprofil (GRPPRF) der Name eines Benutzerprofils angegeben werden und der Parameter Gruppenberechtigung (GRPAUT) kann nicht angegeben werden.

Gruppenberechtigung (GRPAUT)

Dieser Parameter gibt die spezielle Berechtigung an, die einem Gruppenprofil für neu erstellte Objekte erteilt wird. Bei Angabe von *GRPPRF für den Parameter „Eigner“ (OWNER) ist eine Angabe dieses Parameters nicht zulässig.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Es wird keine Gruppenberechtigung erteilt.

***ALL**
Der Benutzer kann alle Operationen ausführen. Ausgenommen sind auf den Eigner beschränkte Operationen oder Operationen, die durch die Berechtigung zum Verwalten der Berechtigungsliste gesteuert werden. Der Benutzer kann die Objektexistenz steuern, die Sicherheit für das Objekt angeben, das Objekt ändern und allgemeine Funktionen für das Objekt durchführen. Der Benutzer kann außerdem das Eigentumsrecht für das Objekt ändern.

***CHANGE**
Der Benutzer kann alle Operationen ausführen, mit Ausnahme derjenigen, die auf den Eigner beschränkt sind oder von der Objektexistenzberechtigung (*OBJEXIST) sowie der Objektverwaltungsberechtigung (*OBJMGT) gesteuert werden. Der Benutzer kann das Objekt ändern und allgemeine Funktionen für das Objekt ausführen. Die Änderungsberechtigung (*CHANGE) schließt die Objektverwendungsberechtigung (*OBJOPR) sowie alle Datenberechtigungen ein. Falls das Objekt eine Berechtigungsliste ist, kann der Benutzer weder andere Benutzer hinzufügen noch Benutzer ändern oder entfernen.

***USE**
Der Benutzer kann grundlegende Operationen für das Objekt vornehmen, also z. B. ein Programm ausführen oder eine Datei lesen. Der Benutzer kann das Objekt nicht ändern. Die Berechtigung *USE stellt die Objektverwendungsberechtigung *OBJOPR, die Leseberechtigung *READ sowie die Ausführungsberechtigung *EXECUTE bereit.

***EXCLUDE**
Der Benutzer kann nicht auf das Objekt zugreifen.

Art der Gruppenberechtigung (GRPAUTTYP)

Dieser Parameter gibt die Art der Berechtigung an, die einem Gruppenprofil für neu erstellte Objekte erteilt werden soll. Bei Angabe von *NONE für den Parameter Gruppenberechtigung (GRPAUT) wird dieser Parameter ignoriert.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***PRIVATE**
Das Gruppenprofil erhält persönliche Berechtigung für neu erstellte Objekte, wobei der Berechtigungswert durch den Parameter GRPAUT bestimmt wird. Lautet der im Parameter GRPAUT angegebene Berechtigungswert *NONE, wird dieser Wert ignoriert.

***PGP**
Das Gruppenprofil wird zur Primärgruppe für neu erstellte Objekte, wobei der Berechtigungswert durch den Parameter GRPAUT bestimmt wird. Lautet der im Parameter GRPAUT angegebene Berechtigungswert *NONE, wird dieser Wert ignoriert.

Zusätzliche Gruppenprofile (SUPGRPPRF)

Dieser Parameter gibt die zusätzlichen Gruppenprofile eines Benutzers an. Diese Profile werden zusammen mit dem für den Parameter Gruppenprofil (GRPPRF) angegebenen Gruppenprofil verwendet, um die Berechtigung eines Benutzers festzulegen, wenn keine spezielle Benutzerberechtigung für den Job besteht. Wenn Profile für diesen Parameter angegeben werden, muss im Parameter GRPPRF ein Gruppenprofilname für das Benutzerprofil vorhanden sein, der entweder in diesem Befehl oder einem früheren Befehl CRTUSRPRF (Benutzerprofil erstellen) oder im Befehl CHGUSRPRF (Benutzerprofil ändern) angegeben wurde. Der aktuelle Benutzer des Befehls muss über die Objektverwaltungsberechtigung (*OBJMGT) sowie die Änderungsberechtigung (*CHANGE) für die Profile verfügen, die für diesen Parameter angegeben sind. Die Berechtigung *OBJMGT kann nicht durch eine Programmübernahmeoperation erworben werden.

Wenn ein Gruppenprofil angegeben wird, erhält der Benutzer automatisch die Berechtigungen *CHANGE und *OBJMGT für das Gruppenprofil.

Die folgenden von IBM gelieferten Benutzerprofile sind für diesen Parameter nicht gültig:

QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPM400, QRJE, QSNADS, QSPL, QSPLJOB, QSRV, QSRVAGT, QSRVBAS, QSYS, QTCM, QTCP, QTFTP, QTSTRQS, QWEBADMIN, QWSERVICE, QYCMCIMOM, QYPSJSVR.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Mit diesem Benutzerprofil werden keine zusätzlichen Gruppenprofile verwendet.

Name
Maximal 15 Gruppenprofilnamen angeben, die zusammen mit dem Benutzerprofil sowie dem im Parameter GRPPRF angegebenen Gruppenprofil bestimmen, ob ein Job Zugriff auf bestehende Objekte sowie Sonderberechtigung erhält.

9.9.6
Seite 28

Berechnungscode (ACGCDE)

Dieser Parameter gibt den diesem Benutzerprofil zugeordneten Berechnungscode an.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***BLANK**
Dem Benutzerprofil wird ein aus 15 Leerzeichen bestehender Berechnungscode zugeordnet.

Zeichenwert
Den aus 15 Zeichen bestehenden Berechnungscode für Jobs angeben, die den Berechnungscode des Benutzerprofils erhalten. Werden weniger als 15 Zeichen angegeben, wird die Zeichenfolge nach rechts mit Leerzeichen aufgefüllt.

Dokumentkennwort (DOCPWD)

Dieser Parameter gibt das Dokumentkennwort an, das Benutzern der DIA-Dokumentverteilungsservices ermöglicht, persönliche Verteilungen vor dem Zugriff von Personen zu schützen, die in ihrem Auftrag arbeiten.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Der Benutzer verwendet kein Dokumentkennwort.

Name
Das Dokumentkennwort angeben, das dem Benutzer zugeordnet werden soll. Das Kennwort muss 1 bis 8 alphanumerische Zeichen (Buchstaben A bis Z und Ziffern 0 bis 9) lang sein. Das erste Zeichen des Dokumentkennworts muss alphabetisch sein, die übrigen Zeichen können alphanumerisch sein. Eingebettete und führende Leerzeichen sowie Sonderzeichen sind unzulässig.

Nachrichtenwarteschlange (MSGQ)

Dieser Parameter gibt die Nachrichtenwarteschlange an, an die Nachrichten gesendet werden.

Anmerkung:

Die Nachrichtenwarteschlange wird erstellt, falls sie noch nicht besteht. Das für den Parameter Benutzerprofil (USRPRF) angegebene Benutzerprofil ist der Eigner der Nachrichtenwarteschlange.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***USRPRF**
Eine Nachrichtenwarteschlange mit demselben Namen wie die für den Parameter USRPRF angegebene wird als Nachrichtenwarteschlange für den Benutzer verwendet. Die Nachrichtenwarteschlange befindet sich in der Bibliothek QUSRSYS.

Qualifikationsmerkmal 1: Nachrichtenwarteschlange

Name
Den Namen der Nachrichtenwarteschlange angeben, die mit dem Profil verwendet werden soll.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Die aktuelle Bibliothek für den Thread wird durchsucht. Ist keine aktuelle Bibliothek für den Thread angegeben, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, die durchsucht werden soll.

9.9.6
Seite 30

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Zustellung . . . . . .   *NOTIFY       *SAME, *NOTIFY, *BREAK...
Bewertungscodefilter . . . . .   0           0-99, *SAME
Druckeinheit . . . . . .   *WRKSTN       Name, *SAME, *WRKSTN, *SYSVAL
Ausgabewarteschlange . . . . .   *WRKSTN       Name, *SAME, *WRKSTN, *DEV
  Bibliothek . . . . . .                 Name, *LIBL, *CURLIB
Abrufprogramm  . . . . . .   *SYSVAL       Name, *SAME, *SYSVAL...
  Bibliothek . . . . . .                 Name, *LIBL, *CURLIB
Sortierfolge . . . . . .   *SYSVAL       Name, *SAME, *SYSVAL, *HEX...
  Bibliothek . . . . . .                 Name, *LIBL, *CURLIB
Sprachen-ID  . . . . . .   *SYSVAL       *SAME, *SYSVAL...
Landes- oder Regions-ID  . . . .   *SYSVAL       *SAME, *SYSVAL...
Zeichensatz-ID . . . . . .   *SYSVAL       *SAME, *SYSVAL, *HEX...
Steuerung für Zeichen-ID . . . .   *SYSVAL       *SAME, *SYSVAL, *DEVD...
Jobattr. länderspez. Angaben . .   *SYSVAL       *SAME, *SYSVAL, *NONE...
     + für weitere Werte
```

Benutzerprofil – Seite 4

Zustellung (DLVRY)

Dieser Parameter gibt an, wie die für einen Benutzer an die Nachrichtenwarteschlange zu sendenden Nachrichten zugestellt werden sollen.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NOTIFY**
Der Job, dem die Nachrichtenwarteschlange zugeordnet ist, wird verständigt, wenn eine Nachricht in der Nachrichtenwarteschlange eintrifft. Bei interaktiven Jobs an einer Datenstation ertönt der akustische Alarm (sofern aktiviert), und der Anzeiger für eine anstehende Nachricht leuchtet auf. Wenn die Nachrichtenwarteschlange auch von anderen Jobs benutzt wird, kann der Zustellungsmodus nicht in *NOTIFY geändert werden.

***HOLD**
Die Nachrichten bleiben in der Nachrichtenwarteschlange, bis sie vom Benutzer oder einem Programm angefordert werden.

***BREAK**
Der Job, dem die Nachrichtenwarteschlange zugeordnet ist, wird unterbrochen, sobald eine Nachricht in der Nachrichtenwarteschlange eintrifft. Bei interaktiven Jobs ertönt der akustische Alarm (sofern aktiviert). Wird die Nachrichtenwarteschlange auch von anderen Jobs benutzt, kann der Zustellungsmodus nicht in *BREAK geändert werden.

***DFT**
Dieser Standardwert wird auf die Anfragenachricht gesendet. Ist in der Nachrichtenbeschreibung der Anfragenachricht keine Standardantwort angegeben, wird die Systemstandardantwort *N verwendet.

Bewertungscodefilter (SEV)

Dieser Parameter gibt den niedrigsten Bewertungscode an, mit dem Nachrichten im Durchbruch- oder Hinweismodus an einen Benutzer gesendet werden. Bei Nachrichten, die mit einem niedrigeren Bewertungscode als dem für diesen Parameter angegebenen Bewertungscode in die Nachrichtenwarteschlange gestellt werden, wird weder der Job unterbrochen, noch ertönt ein Signalton, noch leuchtet der Anzeiger für anstehende Nachrichten. Die Nachrichten verbleiben in der Warteschlange, bis sie mit dem Befehl DSPMSG (Nachricht anzeigen) angezeigt werden. Wenn *BREAK oder *NOTIFY beim Parameter „Zustellung" (DLVRY) angegeben wurde und bei Erhalt der Nachricht in der Nachrichtenwarteschlange aktiv ist, wird die Nachricht zugestellt, wenn der der Nachricht zugeordnete Bewertungscode gleich oder größer dem hier angegebenen Wert ist. Andernfalls wird die Nachricht in der Warteschlange zurückgehalten bis sie angefordert wird.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

0-99
Einen Bewertungscode von 00 bis 99 angeben.

Druckeinheit (PRTDEV)

Dieser Parameter gibt die Standarddruckereinheit für einen Benutzer an. Ist in der Druckerdatei zum Erstellen der Ausgabe angegeben, dass die Daten gespoolt werden sollen, so wird die Spool-Datei in die Ausgabewarteschlange derjenigen Einheit gestellt, die denselben Namen wie die Einheit hat.

Es wird davon ausgegangen, dass im Parameter „Ausgabewarteschlange" (OUTQ) die Standardwerte für Druckerdatei, Jobbeschreibung, Benutzerprofil und Datenstation angegeben sind.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***WRKSTN**
Der der Datenstation des Benutzers zugeordnete Drucker wird verwendet.

***SYSVAL**
Der im Systemwert QPRTDEV angegebene Wert wird verwendet.

Name
Den Namen eines Druckers angeben, der verwendet werden soll, um die Ausgabe eines Benutzers auszudrucken.

9.9.6
Seite 32

Ausgabewarteschlange (OUTQ)

Dieser Parameter gibt die Ausgabewarteschlange an, die von einem Benutzerprofil verwendet werden soll. Die Ausgabewarteschlange muss bereits bestehen, wenn dieser Befehl ausgeführt wird.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***WRKSTN**
Die der Arbeitsstation eines Benutzers zugeordnete Ausgabewarteschlange wird verwendet.

***DEV**
Die Ausgabewarteschlange, die dem für den Parameter Druckeinheit (PRTDEV) angegebenen Drucker zugeordnet ist, wird verwendet. Die Ausgabewarteschlange hat denselben Namen wie der Drucker. (Der Parameter DEV der Druckerdatei wird durch den Befehl CRTPRTF, CHGPRTF oder OVRPRTF bestimmt.)

Es wird davon ausgegangen, dass im Parameter „Ausgabewarteschlange" (OUTQ) die Standardwerte für Druckerdatei, Jobbeschreibung, Benutzerprofil und Datenstation angegeben sind.

Qualifikationsmerkmal 1: Ausgabewarteschlange

Name
Den Namen der Ausgabewarteschlange angeben, die von einem Benutzerprofil verwendet werden soll.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Die aktuelle Bibliothek für den Thread wird durchsucht. Ist keine aktuelle Bibliothek für den Thread angegeben, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, die durchsucht werden soll.

Abrufprogramm (ATNPGM)

9.9.6
Seite 33

Dieser Parameter gibt das Programm an, das für die Abruftaste eines Benutzers verwendet werden soll. Es wird aufgerufen, wenn in einem interaktiven Job die Abruftaste gedrückt wird. Das Programm ist nur aktiv, wenn eine Weiterleitung an den vom System bereitgestellten Befehlsprozessor QCMD besteht. Das Programm für die Abruftaste wird aktiviert, bevor das Startprogramm (sofern vorhanden) aufgerufen wird, und ist sowohl für das Programm als auch für das Menü aktiv. Ändert das Programm das ATNPGM (mit dem Befehl SETATNPGM), bleibt das neue Programm nur für die Dauer seiner Laufzeit aktiv. Wenn die Steuerung zurückgegeben wird und QCMD das Menü aufruft, wird wieder das ursprüngliche Programm für die Abruftaste aktiv. Wird der Befehl SETATNPGM aus den Menüs ausgeführt oder wird eine Anwendung aus den Menüs aufgerufen, überschreibt das neue Programm für die Abruftaste das ursprünglich angegebene. Bei Angabe von *YES oder *PARTIAL für den Parameter „Möglichkeiten einschränken“ (LMTCPB) im Befehl CRTUSRPRF (Benutzerprofil erstellen) oder im Befehl CHGUSRPRF (Benutzerprofil ändern), kann das Programm für die Abruftaste nicht geändert werden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QATNPGM wird verwendet.

***NONE**
Der Benutzer verwendet kein Programm für die Abruftaste.

***ASSIST**
Das Programm für die Abruftaste der einfachen Oberfläche von Anwendungen, QEZMAIN, wird verwendet.

Qualifikationsmerkmal 1: Abrufprogramm

Name
Den Namen des Programms für die Abruftaste angeben, das für ein Benutzerprofil verwendet werden soll.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

9.9.6
Seite 34

***CURLIB**
Die aktuelle Bibliothek für den Thread wird durchsucht. Ist keine aktuelle Bibliothek für den Thread angegeben, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, die durchsucht werden soll.

Sortierfolge (SRTSEQ)

Dieser Parameter gibt die Sortierfolgetabelle an, die zum Vergleich von Zeichenfolgen für ein Profil verwendet werden soll.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QSRTSEQ wird verwendet.

***HEX**
Es wird keine Sortierfolgetabelle verwendet. Die Hexadezimalwerte der Zeichen werden zur Festlegung der Sortierfolge verwendet.

***LANGIDUNQ**
Es wird eine Sortiertabelle mit Zeichen unterschiedlicher Wertigkeit verwendet.

***LANGIDSHR**
Es wird eine Sortiertabelle mit Zeichen gleicher Wertigkeit verwendet.

Qualifikationsmerkmal 1: Sortierfolge

Name
Den Namen der mit diesem Profil zu verwendenden Sortierfolgetabelle angeben.

Qualifikationsmerkmal 2: Bibliothek

***LIBL**
Alle Bibliotheken in der Bibliotheksliste des aktuellen Threads werden durchsucht, bis die erste Übereinstimmung gefunden wird.

***CURLIB**
Die aktuelle Bibliothek für den Thread wird durchsucht. Ist keine aktuelle Bibliothek für den Thread angegeben, wird QGPL verwendet.

Name
Den Namen der Bibliothek angeben, die durchsucht werden soll.

9.9.6
Seite 35

Sprachen-ID (LANGID)

Dieser Parameter gibt die für einen Benutzer zu verwendende Sprachen-ID an.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QLANGID wird verwendet.

Sprachen-ID
Die zu verwendende Sprachen-ID angeben. Weitere Informationen über gültige Sprachen-IDs enthält das Handbuch „Themensammlung zu i5/OS Globalization“ im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Landes- oder Regions-ID (CNTRYID)

Dieser Parameter gibt die für einen Benutzer zu verwendende Landes- oder Regions-ID an.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QCNTRYID wird verwendet.

Zeichenwert
Eine Landes- oder Regions-ID angeben. Zum Anzeigen einer vollständigen Liste der IDs – wenn die Bedienerführung für diesen Befehl angezeigt wird – den Cursor auf das Feld für diesen Parameter stellen und F4 (Bedienerführung) drücken.

9.9.6
Seite 36

Zeichensatz-ID (CCSID)

Dieser Parameter gibt die ID des codierten Zeichensatzes (CCSID) an, die für einen Benutzer verwendet werden soll.

Eine CCSID ist eine aus 16 Bits bestehende Zahl, die eine bestimmte Menge von Kennungen für Codeumsetzungsschemata, Zeichensatzkennungen, Codepagekennungen und weitere codierungsbezogene Informationen angibt, welche eine codierte grafische Darstellung eindeutig kennzeichnen.

Wird der CCSID-Wert geändert, hat die Änderung keine Auswirkung auf die gerade ausgeführten Jobs.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QCCSID wird verwendet.

***HEX**
Die CCSID 65535 wird verwendet.

Kennung
Die CCSID angeben, die für dieses Benutzerprofil verwendet werden soll. Weitere Informationen über gültige CCSIDs enthält das Handbuch „Informationen zu Globalization“ im iSeries Information Center unter http://www.ibm.com/eserver/iseries/infocenter.

Steuerung für Zeichen-ID (CHRIDCTL)

Dieser Parameter gibt die Steuerung der Zeichen-ID (CHRIDCTL) für einen Job an. Er steuert die Art der CCSID-Umsetzung, die für Bildschirmdateien, Druckerdateien und Anzeigengruppen durchgeführt wird. Bevor der Parameter verwendet werden kann, muss der Sonderwert *CHRIDCTL (CHRID) in den Befehlen zum Erstellen, Ändern und Überschreiben von Bildschirmdateien, Druckerdateien und Anzeigengruppen angegeben werden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QCHRIDCTL wird verwendet.

***DEVD**
Der Sonderwert *DEVD führt dieselbe Funktion aus wie im Befehlsparameter CHRID für Bildschirmdateien, Druckerdateien und Anzeigengruppen.

***JOBCCSID**
Der Sonderwert *JOBCCSID führt dieselbe Funktion aus wie im Befehlsparameter CHRID für Bildschirmdateien, Druckerdateien und Anzeigengruppen.

Jobattribut länderspezifische Angaben (SETJOBATR)

Dieser Parameter gibt an, welche Jobattribute aus den länderspezifischen Angaben (LOCALE) übernommen werden sollen, wenn der Job eingeleitet wird.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QSETJOBATR bestimmt, welche Jobattribute aus den länderspezifischen Angaben übernommen werden.

***NONE**
Es werden keine Jobattribute aus den länderspezifischen Angaben übernommen.

***CCSID**
Die ID des codierten Zeichensatzes (CCSID) aus den länderspezifischen Angaben wird verwendet. Der CCSID-Wert aus den länderspezifischen Angaben überschreibt die CCSID im Benutzerprofil.

9.9.6
Seite 38

***DATFMT**
Das Datumsformat aus den länderspezifischen Angaben wird verwendet.

***DATSEP**
Das Datumstrennzeichen aus den länderspezifischen Angaben wird verwendet.

***DECFMT**
Das Dezimalformat aus den länderspezifischen Angaben wird verwendet.

***SRTSEQ**
Die Sortierfolge aus den länderspezifischen Angaben wird verwendet. Die Sortierfolge aus den länderspezifischen Angaben überschreibt die im Benutzerprofil angegebene Sortierfolge.

***TIMSEP**
Das Zeittrennzeichen aus den länderspezifischen Angaben wird verwendet.

```
                    Benutzerprofil ändern (CHGUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Länderspezifische Angaben  . . .   *SAME

Benutzerangaben  . . . . . .  . .  *NONE          *SAME, *NONE, *CLKWD...
     + für weitere Werte
Benutzernummer . . . . . .  . . .  114           1-4294967294, *SAME
Gruppennummer  . . . . . .  . . .  *NONE          1-4294967294, *SAME, *GEN...
Benutzerverzeichnis  . . . . . .   *SAME

EIM-Zuordnung:
  EIM-Kennung  . . . . . .  . . .  *NOCHG
  Zuordnungstyp  . . . . . .  . .                 *TARGET, *SOURCE, *TGTSRC...
  Zuordnungsaktion . . . . . .  .                 *REPLACE, *ADD, *REMOVE
  EIM-Kennung erstellen  . . . .                  *NOCRTEIMID, *CRTEIMID
Ablaufdatum für Benutzerprofil     *NONE          Datum, *NONE, *USREXPITV...
Ablaufintervall f. Benutzerpr.                    1-366
```

Benutzerprofil – Seite 5

Länderspezifische Angaben (LOCALE)

9.9.6
Seite 39

Dieser Parameter gibt den Pfadnamen für die länderspezifischen Angaben an, die der Umgebungsvariablen LANG für diesen Benutzer zugeordnet sind.

Dieser Parameter ist unicodefähig. Weitere Informationen sind im Abschnitt „Unicode support in CL“ unter „CL-Themensammlung“ in der Kategorie „Programmierung“ im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/ zu finden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***SYSVAL**
Der Systemwert QLOCALE bestimmt den Pfadnamen für die länderspezifischen Angaben, der diesem Benutzer zugeordnet werden soll.

***NONE**
Dem Benutzer wird kein Pfadname für länderspezifische Angaben zugeordnet.

***C**
Dem Benutzer wird der Pfadname der länderspezifischen Angaben für die Programmiersprache C zugeordnet.

***POSIX**
Dem Benutzer wird der Pfadname der länderspezifischen Angaben für POSIX zugeordnet.

‘Pfadname’
Den Pfadnamen für die länderspezifischen Angaben angeben, der einem Benutzer zugeordnet werden soll.

9.9.6
Seite 40

Benutzerangaben (USROPT)

Gibt die Detailstufe des Hilfetexts an, die angezeigt werden soll, sowie die Standardbelegung der Tasten zum Vor- und Zurückblättern. Das System ruft mehrere Anzeigen auf, die für einen weniger erfahrenen Benutzer geeignet sind. Erfahrene Benutzer müssen noch eine zusätzliche Aktion durchführen, um detaillierte Informationen angezeigt zu bekommen. Werden Werte für diesen Parameter angegeben, zeigt das System detaillierte Informationen an, ohne dass der erfahrene Benutzer eine weitere Aktion durchführen muss.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Es werden keine Detailinformationen angezeigt.

***CLKWD**
Wenn die Bedienerführung für einen CL-Befehl angezeigt wird, werden statt der gültigen Parameterwerte die Parameterschlüsselwörter angezeigt.

***EXPERT**
Detailliertere Informationen werden angezeigt, wenn der Benutzer Anzeige- und Editieroperationen zum Definieren oder Ändern des Systems durchführt (z. B. Objektberechtigung editieren oder anzeigen).

***ROLLKEY**
Die Aktionen der Tasten zum Vor- und Zurückblättern werden umgekehrt.

***NOSTSMSG**
An den Benutzer gesendete Statusnachrichten werden nicht angezeigt.

***STSMSG**
An den Benutzer gesendete Statusnachrichten werden angezeigt.

***HLPFULL**
Der Hilfetext wird in einer Gesamtanzeige gezeigt, nicht in einem Fenster.

***PRTMSG**
Es wird eine Nachricht an die Nachrichtenwarteschlange eines Benutzers gesendet, wenn eine Spool-Datei für den Benutzer gedruckt oder vom Druckausgabeprogramm angehalten wird.

Benutzernummer (UID)

Dieser Parameter gibt die Benutzernummer (UID-Nummer) für ein Benutzerprofil an. Die UID-Nummer dient zur Kennzeichnung des Benutzers, wenn er mit dem Verzeichnisdateisystem arbeitet. Die UID-Nummer für einen Benutzer kann nicht geändert werden, wenn ein oder mehrere aktive Jobs für den Benutzer vorhanden sind.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

Nummer
Die dem Benutzerprofil zuzuordnende UID-Nummer angeben. Es kann ein Wert von 1 bis 4294967294 eingegeben werden. Die angegebene UID-Nummer darf nicht bereits einem anderen Benutzerprofil zugeordnet sein.

Gruppennummer (GID)

Dieser Parameter gibt die Gruppennummer (GID-Nummer) für ein Benutzerprofil an. Die GID-Nummer dient zur Kennzeichnung des Gruppenprofils, wenn ein Mitglied der Gruppe mit dem Verzeichnisdateisystem arbeitet. Die GID-Nummer für einen Benutzer kann in den folgenden Fällen nicht geändert werden:

Das Benutzerprofil ist die Primärgruppe eines Objekts in einem Verzeichnis.

Für den Benutzer sind ein oder mehrere aktive Jobs vorhanden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Der Benutzer verfügt nicht über eine GID-Nummer oder eine bestehende GID-Nummer wurde entfernt.

Dieser Wert kann nicht angegeben werden, wenn es sich bei dem Benutzer um ein Gruppenprofil oder die Primärgruppe eines Objekts handelt.

***GEN**
Die GID-Nummer wird für den Benutzer generiert. Das System generiert eine GID-Nummer, die nicht bereits einem anderen Benutzer zugeordnet ist. Die generierte GID-Nummer ist größer als 100.

Nummer
Die GID-Nummer angeben, die dem Benutzerprofil zugeordnet werden soll. Es kann ein Wert von 1 bis 4294967294 eingegeben werden. Die angegebene GID-Nummer darf nicht bereits einem anderen Benutzerprofil zugeordnet sein.

Benutzerverzeichnis (HOMEDIR)

Dieser Parameter gibt den Pfadnamen des Benutzerverzeichnisses für ein Benutzerprofil an. Das Benutzerverzeichnis ist das ursprüngliche Arbeitsverzeichnis des Benutzers. Das einem Prozess zugeordnete Arbeitsverzeichnis wird in einem Verzeichnisdateisystem zur Auflösung von Pfadnamen benutzt, die nicht mit einem Schrägstrich (/) beginnen. Existiert das angegebene Benutzerverzeichnis beim Anmelden eines Benutzers nicht, wird das Stammverzeichnis (/) zum ursprünglichen Arbeitsverzeichnis für den Benutzer.

Dieser Parameter ist unicodefähig. Weitere Informationen sind im Abschnitt „Unicode support in CL“ unter „CL-Themensammlung“ in der Kategorie „Programmierung“ im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/ zu finden.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***USRPRF**
Das dem Benutzer zugeordnete Benutzerverzeichnis lautet ‚/home/USRPRF‘, wobei ‚USRPRF‘ der Name des Benutzerprofils ist.

‘Pfadname’
Den Pfadnamen des Ausgangsverzeichnisses angeben, das einem Benutzer zugeordnet werden soll.

Weitere Informationen über das Angeben von Pfadnamen enthält der Abschnitt „Object naming rules“ des Handbuchs „CL-Themensammlung“ in der Kategorie „Programmierung“ im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

EIM-Zuordnung (EIMASSOC)

Dieser Parameter gibt an, ob für einen Benutzer eine EIM-Zuordnung (Enterprise Identity Mapping) zu einer EIM-Kennung verarbeitet werden soll.

- Die Informationen werden nicht im Benutzerprofil gespeichert und nicht mit gesichert oder zurückgespeichert.
- Wenn dieses System nicht für EIM konfiguriert ist, findet keine Verarbeitung statt. Wenn keine EIM-Operationen ausgeführt werden können, bedeutet das nicht, das der Befehl fehlschlägt.

Gültige Werte sind:

***NOCHG**
Die EIM-Zuordnungsinformation ändert sich nicht.

Element 1: EIM-Kennung
Gibt die EIM-Kennung für eine Zuordnung an.

***USRPRF**
Der Name der EIM-Kennung ist mit dem Namen des Benutzerprofils identisch.

Zeichenwert
Den Namen der EIM-Kennung angeben.

Element 2: Zuordnungstyp
Gibt den Zuordnungstyp an. Es wird empfohlen, für einen IBM i-Benutzer eine Zielzuordnung hinzuzufügen.

Zielzuordnungen dienen hauptsächlich zum Schutz vorhandener Daten. Sie werden bei Abgleichsuchoperationen gefunden (eimGetTargetFromSource()), können aber nicht als Quellenidentität für eine Abgleichsuchoperation verwendet werden.

Quellenzuordnungen dienen hauptsächlich für Authentifizierungszwecke. Sie können als Quellenidentität einer Abgleichsuchoperation benutzt werden, werden aber nicht als Ziel einer Abgleichsuchoperation gefunden. Administrative Zuordnungen werden benutzt, um anzuzeigen, dass einer EIM-Kennung eine Identität zugeordnet ist. Sie können aber nicht als Quelle einer Abgleichsuchoperation verwendet werden und werden nicht als Ziel bei einer solchen Suchoperation gefunden.

***TARGET**
Eine Zielzuordnung verarbeiten.

***SOURCE**
Eine Quellenzuordnung verarbeiten.

9.9.6
Seite 44

***TGTSRC**
Sowohl eine Ziel- als auch eine Quellenzuordnung verarbeiten.

***ADMIN**
Eine administrative Zuordnung verarbeiten.

***ALL**
Alle Zuordnungstypen verarbeiten.

Element 3: Zuordnungsaktion

***REPLACE**
Zuordnungen des angegebenen Typs werden aus allen EIM-Kennungen entfernt, die eine Zuordnung für ein Benutzerprofil und das lokale EIM-Register enthalten. Der angegebenen EIM-Kennung wird eine neue Zuordnung hinzugefügt.

***ADD**
Eine Zuordnung hinzufügen.

***REMOVE**
Eine Zuordnung entfernen.

Element 4: EIM-Kennung erstellen
Gibt an, ob die EIM-Kennung erstellt werden soll, wenn sie noch nicht besteht.

***NOCRTEIMID**
Die EIM-Kennung wird nicht erstellt.

***CRTEIMID**
Die EIM-Kennung wird erstellt, wenn sie noch nicht besteht.

Ablaufdatum für Benutzerprofil (USREXPDATE)

9.9.6
Seite 45

Dieser Parameter gibt das Datum an, zu dem ein Benutzerprofil abläuft und automatisch deaktiviert wird. Mit dem Befehl DSPEXPSCD (Verfallsplan anzeigen) kann eine Liste aller auf ein Ablaufdatum gesetzten Benutzerprofile angezeigt werden.

Wenn ein Benutzerprofil auf ein Ablaufdatum gesetzt wurde, wird eine nächtliche Ausführung des Jobs QSECEXP1 geplant.

Für die folgenden von IBM bereitgestellten Benutzerprofile kann kein Ablaufdatum für „Benutzerprofil“ angegeben werden:

QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QEJBSVR, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPM400, QSECOFR, QSNADS, QSPL, QSPLJOB, QSRVAGT, QSYS, QTCM, QTCP, QTFTP, QTMHHTTP, QTMHHTP1, QTSTRQS, QWEBADMIN, QWSERVICE, QYCMCIMOM, QYPSJSVR.

Gültige Werte sind:

***SAME**
Der Wert ändert sich nicht.

***NONE**
Das Benutzerprofil hat kein Ablaufdatum.

***USREXPITV**
Das Ablaufdatum für ein Benutzerprofil wird anhand des Werts errechnet, der für das Ablaufintervall des Benutzerprofils (Parameter USREXPITV) angegeben wurde.

Datum
Gibt das Datum an, zu dem ein Benutzerprofil abläuft. Das Datum muss im Jobdatumsformat angegeben werden.

9.9.6
Seite 46

Ablaufintervall für Benutzerprofil (USREXPITV)

Dieser Parameter gibt das Ablaufintervall (in Tagen) an, bevor es automatisch deaktiviert wird. Mit dem Befehl DSPUSRPRF (Benutzerprofil anzeigen) kann das Ablaufdatum für ein Benutzerprofil angezeigt werden. Mit dem Befehl DSPEXPSCD (Verfallsplan anzeigen) kann eine Liste aller auf ein Ablaufdatum gesetzten Benutzerprofile angezeigt werden.

Für diesen Parameter muss ein Wert angegeben werden, wenn für den Parameter USREXPDATE der Wert *USREXPITV angegeben wurde. Wenn für den Parameter USREXPDATE ein anderer Wert als *USREXPITV angegeben wurde, ist kein Wert für diesen Parameter zulässig.

1-366
Wenn für ein Benutzerprofil kein Ablaufdatum angegeben wurde oder das Benutzerprofil abgelaufen ist und der Parameter „Status“ auf *ENABLED gesetzt wurde, gibt dieser Wert die Anzahl der Tage zwischen dem aktuellen Datum und dem neuen Ablaufdatum des Benutzerprofils an. Wenn das Benutzerprofil noch nicht abgelaufen ist, wird das Ablaufintervall für das Benutzerprofil geändert, aber nicht das bestehende Ablaufdatum des Benutzerprofils. Gültig sind Werte von 1 bis 366.

9.9.7 Benutzerprofil löschen

Um ein Benutzerprofil aus dem System zu löschen, verwenden Sie den Befehl DLTUSRPRF. Sie müssen über die Sonderberechtigung *SECADM verfügen, um das durchführen zu können.

Das Löschen von Benutzerprofilen ist die sauberste Art, einen ausgeschiedenen Mitarbeiter aus einem System zu entfernen. Oftmals werden die Benutzerprofile bei Ausscheiden nur deaktiviert (Status *DISABLED). Dies hat jedoch zur Folge, dass ein Benutzerprofil auch mal wieder aktiviert werden kann und so ungewollte Zugriffe auf das System erfolgen können. Auch wird durch deaktivierte Benutzerprofile die Übersicht über die Benutzer komplizierter.

Das Löschen eines Benutzerprofils ist jedoch nicht ganz ungefährlich, weil je nach Tätigkeit des Mitarbeiters mit diesem Profil viele Objekte verbunden sein können. Wenn Sie beim Löschen also nicht aufpassen, so kann das zu unvorhersehbaren Ergebnissen führen, die manchmal nicht sofort, sondern erst später zu Tage treten.

Der Benutzer, der ein Profil löschen will, muss über die Benutzungsberechtigung (*USE) sowie die Objektexistenzberechtigung (*OBJEXIST) für das Benutzerprofil verfügen.

Für das Löschen einer Nachrichtenwarteschlange, die einem Benutzerprofil zugeordnet ist und dessen Eigner das Benutzerprofil ist, muss der Benutzer über die Berechtigungen *OBJEXIST, *USE und *DLT für die entsprechende Nachrichtenwarteschlange verfügen.

Das Löschen eines Benutzerprofils ist nicht möglich, während ein Benutzer unter diesem Profil aktiv ist oder wenn das Benutzerprofil ein Objekteigner ist und OWNOBJOPT(*NODLT) angegeben wurde. Alle Objekte des betroffenen Benutzerprofils müssen entweder erst mit dem Befehl CHGOBJOWN (Objekteigner ändern) auf andere Eigner übertragen oder aus dem System gelöscht werden. Die Objekte können auch mit der Angabe OWNOBJOPT(*DLT) gelöscht und das Eigentumsrecht kann mit der Angabe OWNOBJOPT(*CHGOWN Benutzerprofilname) geändert werden. Berechtigungen, die dem Benutzer erteilt wurden, müssen nicht gesondert mit dem Befehl RVKOBJAUT (Objektberechtigung entziehen) entzogen werden, sie werden automatisch beim Löschen des Benutzerprofils entzogen.

Zum Löschen jedes Objekts ist die Berechtigung *OBJEXIST für das Objekt erforderlich.

9.9.7
Seite 2

Ein Benutzerprofil kann nicht gelöscht werden, wenn es die Primärgruppe für ein Objekt ist. Alle Objekte, für die ein Benutzer die Primärgruppe ist, müssen entweder mit dem Befehl CHGOBJPGP (Primärgruppe des Objekts ändern) übertragen oder aus dem System gelöscht werden. Die Übertragung kann durchgeführt werden, indem PGPOPT(*CHGPGP Benutzerprofilname) zum Ändern der Primärgruppe angegeben wird.

Mit diesem Befehl wird die Unterstützungsfunktion des Systemverteilerverzeichnisses aufgerufen, um einen Benutzer aus dem Verzeichnis und, falls erforderlich, aus dem Verteiler zu löschen. Von der Unterstützungsfunktion wird für die Dateien des Systemverteilerverzeichnisses (QUSURSYS/QAOS*) Journalaufzeichnung und COMMIT-Steuerung verwendet. Wenn diese Funktion angefordert wird, muss die COMMIT-Steuerung inaktiv sein. Wenn die COMMIT-Steuerung beim Anfordern dieser Funktion aktiv ist, muss das Journal QUSRSYS/QAOSDIAJRN sein.

Weitere Hinweise zum Löschen von Benutzerprofilen:

1. Die Objekte der Art *USRPRF, *RCT und *AUTHLR, deren Eigner ein Benutzerprofil ist, werden nicht aus dem System gelöscht. Das Eigentumsrecht an diesen Objekten wird an das Benutzerprofil QDFTOWN übertragen.
2. Die Objekte der Art *PRDDFN, deren Eigner ein Benutzerprofil ist, werden nicht gelöscht. Das Eigentumsrecht wird an das Benutzerprofil QSYS übertragen.
3. Neben den aufgeführten Einschränkungen gelten alle den Befehl DLTLIB betreffenden Einschränkungen auch für die Angabe von OWNOBJOPT(*DLT). Z. B. kann ein Objekt nicht gelöscht werden, während es verwendet wird. Und auch eine physische Datei mit einer zugeordneten logischen Datei – wobei die logische Datei einen anderen Eigner hat – kann nicht gelöscht werden.
4. Das Löschen von Objekten der Art *LIB aus dem System, deren Eigner ein Benutzerprofil ist, ist nicht möglich, wenn Objekte in der Bibliothek ein anderes Benutzerprofil als Eigner haben. Das Eigentumsrecht an der Bibliothek wird an das Systembenutzerprofil QDFTOWN übertragen.
5. Das Löschen von Objekten der Art *DIR aus dem System, deren Eigner ein Benutzerprofil ist, ist nicht möglich, wenn Objekte in dem Verzeichnis ein anderes Benutzerprofil als Eigner haben. Das Eigentumsrecht am Verzeichnis wird an das Systembenutzerprofil QDFTOWN übertragen.
6. Das Löschen von Objekten der Art *BLKSF aus dem System, deren Eigner ein Benutzerprofil ist, ist nicht möglich, wenn Objekte im benutzerdefinierten Dateisystem (dargestellt durch *BLKSF) ein anderes Benutzerprofil als Eigner haben. Das Eigentumsrecht an dem benutzerdefinierten Dateisystem wird an das Systembenutzerprofil QDFTOWN übertragen.

7. Ein Benutzerprofil kann nicht gleichzeitig der Eigner des Objekts und die Primärgruppe des Objekts sein. Wenn der neue Eigner schon die Primärgruppe eines Objekts ist, dessen Eigner der aktuelle Benutzer ist, schlägt das Übertragen des Eigentumsrechts fehl. Wenn die neue Primärgruppe schon Eigner eines Objekts ist, für das der aktuelle Eigner die Primärgruppe ist, schlägt das Übertragen der Primärgruppe fehl.

```
                    Benutzerprofil löschen (DLTUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > RENGEL        Name
Auswahl eigener Objekte:
  Wert eigener Objekte . . . . .   *NODLT        *NODLT, *DLT, *CHGOWN
  Ben.profilname, wenn *CHGOWN     _____        Name
Angabe für Primärgruppe:
  Primärgruppenwert  . . . . . .   *NOCHG        *NOCHG, *CHGPGP
  Neue Primärgruppe  . . . . . .   _____        Name, *NONE
  Berecht. für neue Primärgruppe   _____        *OLDPGP, *PRIVATE, *ALL...
EIM-Zuordnung  . . . . . .   *DLT          *DLT, *NODLT

                                                                      Ende
F3=Verlassen    F4=Bedienerf.    F5=Aktualisieren    F12=Abbrechen
F13=Verwendung der Anzeige       F24=Weitere Tasten
```

DLTUSRPRF + F4

Benutzerprofil (USRPRF)

Dieser Parameter gibt ein zu löschendes Benutzerprofil an.

Die folgenden von IBM gelieferten Benutzerprofile sind für diesen Parameter nicht gültig:

QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QEJBSVR, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPGMR, QPM400, QSECOFR, QSNADS, QSPL, QSPLJOB, QSRV, QSRVAGT, QSRVBAS, QSYS, QSYSOPR, QTCM, QTCP, QTFTP, QTMHHTTP, QTMHHTP1, QTSTRQS, QUSER, QWEBADMIN, QWSERVICE, QYCMCIMOM, QYPSJSVR.

Name
Den Namen eines zu löschenden Benutzerprofils angeben.

9.9.7
Seite 4

Auswahl eigener Objekte (OWNOBJOPT)

Dieser Parameter gibt die Art der Maßnahmen an, die bei eigenen Objekten des Benutzerprofils durchzuführen sind.

Gültige Werte sind:

***NODLT**
Die eigenen Objekte des Benutzerprofils werden nicht geändert und das Benutzerprofil wird nicht gelöscht, wenn der Benutzer eigene Objekte hat.

***DLT**
Die eigenen Objekte des Benutzerprofils werden gelöscht. Das Benutzerprofil wird gelöscht, wenn alle eigenen Objekte erfolgreich gelöscht werden konnten.

Element 1: Wert eigener Objekte

***CHGOWN**
Die eigenen Objekte des Benutzerprofils gehen in das Eigentum des angegebenen Benutzerprofils über. Das Benutzerprofil wird gelöscht, wenn alle eigenen Objekte erfolgreich übertragen werden konnten.

Bei Angabe von *CHGOWN muss für das neue Benutzerprofil ein Benutzerprofilname angegeben werden. Das neue Benutzerprofil wird zum Eigner aller Objekte, deren Eigner das für den Parameter „Benutzerprofil“ (USRPRF) angegebene Benutzerprofil war.

Element 2: Benutzerprofilname, wenn *CHGOWN

Name
Den Namen des Benutzerprofils angeben, das der neue Eigner sein soll.

Angabe für Primärgruppe (PGPOPT)

Dieser Parameter gibt die Art der Maßnahmen an, die bei Objekten durchgeführt werden, für die das zu löschende Benutzerprofil die Primärgruppe ist.

Gültige Werte sind:

***NOCHG**
Die Objekte, für die das Benutzerprofil die Primärgruppe ist, ändern sich nicht, und das Benutzerprofil wird nicht gelöscht, wenn der Benutzer die Primärgruppe für eines der Objekte ist.

Element 1: Primärgruppenwert

***CHGPGP**
Die Objekte, für die das Benutzerprofil die Primärgruppe ist, werden in das angegebene Benutzerprofil übertragen. Das Benutzerprofil wird gelöscht, nachdem alle Objekte übertragen worden sind.

Wenn *CHGPGP angegeben wird, muss ein Benutzerprofilname oder *NONE angegeben werden. Wird ein Benutzerprofilname angegeben, ist dieser Benutzer die Primärgruppe für alle Objekte, für die das im Parameter USRPRF angegebene Benutzerprofil die Primärgruppe ist. Wird *NONE angegeben, ist allen Objekten, für die das im Parameter USRPRF angegebene Benutzerprofil die Primärgruppe ist, keine Primärgruppe mehr zugeordnet.

Element 2: Neue Primärgruppe

***NONE**
Den Objekten wird keine Primärgruppe zugeordnet.

Name
Den Namen des Benutzerprofils angeben, das die neue Primärgruppe sein soll. Das angegebene Benutzerprofil muss über eine Gruppennummer (gid) verfügen.

Element 3: Berechtigung für neue Primärgruppe

***OLDPGP**
Die neue Primärgruppe erhält dieselbe Berechtigung für ein Objekt wie die alte Primärgruppe.

***PRIVATE**
Verfügt die neue Primärgruppe über eine persönliche Berechtigung für ein Objekt, wird sie zur Primärgruppe für das Objekt und erhält als Primärgruppenberechtigung die bisherige persönliche Berechtigung. Verfügt die neue Primärgruppe über keine persönliche Berechtigung für ein Objekt, wird sie die neue Primärgruppe ohne Berechtigung für das Objekt.

***ALL**
Die neue Primärgruppe erhält die Berechtigung *ALL für ein Objekt.

***CHANGE**
Die neue Primärgruppe erhält die Berechtigung *CHANGE für ein Objekt.

***USE**
Die neue Primärgruppe erhält die Berechtigung *USE für ein Objekt.

***EXCLUDE**
Die neue Primärgruppe erhält die Berechtigung *EXCLUDE für ein Objekt.

EIM-Zuordnung (EIMASSOC)

Dieser Parameter gibt an, ob Enterprise Identity Mapping (EIM)-Zuordnungen für einen Benutzer im lokalen Register gelöscht werden sollen. Es werden alle Arten von Zuordnungen für den Benutzer im lokalen Register gelöscht, einschließlich Ziel- und Quellenzuordnungen, administrative Zuordnungen und Richtlinien. Wenn das System nicht für EIM konfiguriert ist, findet keine Verarbeitung statt. Wenn das System für EIM konfiguriert ist, aber keine Verbindung zu EIM hergestellt werden kann (z. B. weil der LDAP-Server, für den EIM konfiguriert ist, nicht aktiv ist), wird ein QSYEIM-Job übergeben, der für die Dauer von einer Stunde versucht, eine Verbindung zu EIM herzustellen. Falls die EIM-Zuordnungen nicht gelöscht werden können, bedeutet dies nicht, dass das Profil nicht gelöscht werden kann.

Nicht gelöschte Zuordnungen werden von einem neu erstellten gleichnamigen Profil verwendet.

***DLT**
EIM-Zuordnungen werden gelöscht.

***NODLT**
EIM-Zuordnungen werden nicht gelöscht.

Objekte eines Eigners anzeigen

Die Anzeige "Mit Objekten eines Eigners arbeiten" (WRKOBJOWN) zeigt eine Liste aller Objekte an, deren Eignern das ausgewählte Benutzerprofil ist. Außerdem werden die Bibliothek, in der sich die Objekte befinden, die jeweilige Objektart, die Attribute der Objekte sowie der jeweils zugehörige Text angezeigt.

Diese Auflistung zeigt Ihnen, bei welchen Objekten ein Benutzer als Eigner eingetragen ist. In den meisten Fällen sind das Objekte, die der entsprechende Benutzer erstellt hat, also z. B. Dateien, die durch Ausgaben aus Query entstanden sind, oder Programme, die durch Kompilieren aus Quellen entstanden sind etc.

```
                    Mit Objekten eines Eigners arbeiten

Benutzerprofil . . . . . :   RENGEL

Auswahl eingeben und Eingabetaste drücken.
  2=Berechtigung editieren   4=Löschen     5=Berechtigung anzeigen
  7=Umbenennen   8=Beschreibung anzeigen   9=Eigner ändern

Ausw  Objekt                Bibliothek    Art       Attribut    ASP-Einh.
  _     /home/liste.pdf/QP >              *STMF                 *SYSBAS
  _     /tmp/AUQSHF_output                *STMF                 *SYSBAS
  _     /tmp/AVQSHF_output                *STMF                 *SYSBAS
  _     /SMZVDTA/quarantin >              *STMF                 *SYSBAS
  _     /tmp/EXCQSH_output                *STMF                 *SYSBAS
  _     /tmp/IsLocked.sh                  *STMF                 *SYSBAS
  _     /tmp/JAQSHF_output                *STMF                 *SYSBAS
  _     /tmp/ODQSHF_output                *STMF                 *SYSBAS
  _     /tmp/RPT000001_All >              *STMF                 *SYSBAS
                                                                  Weitere ...
Parameter oder Befehl
===>
F3=Verlassen     F5=Aktual.    F9=Finden    F11=Beschreibungen anzeigen
F12=Abbrechen    F17=Anfang    F18=Ende     F24=Weitere Tasten
```

Mit Objekten eines Eigners arbeiten

Benutzerprofil

Dieser Parameter gibt den Namen eines Benutzerprofils an.

9.9.7
Seite 8

Auswahl

2=Berechtigung editieren
Die Berechtigung eines Benutzers für ein Objekt hinzufügen, ändern oder löschen.

4=Löschen
Löscht ein Objekt.

5=Berechtigung anzeigen
Zeigt eine Liste der Benutzer an, die zur Arbeit mit den angegebenen Objekten berechtigt sind.

7=Umbenennen
Ändert den Namen eines Objekts.

8=Beschreibung anzeigen
Zeigt die Namen und Attribute ausgewählter Objekte an. Diese Option wird für verzeichnisbasierte Objekte nicht unterstützt.

9=Eigner ändern
Ermöglicht es, das Eigentumsrecht für ein Objekt zu ändern.

Objekt
Der Name eines Objekts.

Bibliothek
Name der Bibliothek, die ein Objekt enthält, oder Name des Ordners, der ein Dokument enthält.

Art
Die Art eines Objekts, wie z. B. *PGM, *FILE oder *LIB.

Attribute
Da es mehrere Objektarten gibt, wird das Attribut zur näheren Beschreibung eines Objekts verwendet.

ASP-Einheit
Der Name der ASP-Einheit (ASP = Zusatzspeicherpool), in der sich ein Objekt befindet. *SYSBAS bedeutet, dass sich das Objekt im System-ASP oder in einem Basis-Benutzer-ASP befindet.

9.9.8 Objekte eines Eigners anzeigen

Die Anzeige „Mit Objekten eines Eigners arbeiten“ (WRKOBJOWN) zeigt eine Liste aller Objekte an, deren Eignern das ausgewählte Benutzerprofil ist. Außerdem werden die Bibliothek, in der sich die Objekte befinden, die jeweilige Objektart, die Attribute der Objekte sowie der jeweils zugehörige Text angezeigt.

Diese Auflistung zeigt Ihnen, bei welchen Objekten ein Benutzer als Eigner eingetragen ist. In den meisten Fällen sind das Objekte, die der entsprechende Benutzer erstellt hat, also z. B. Dateien, die durch Ausgaben aus Query entstanden sind, oder Programme, die durch Kompilieren aus Quellen entstanden sind etc.

```
                    Mit Objekten eines Eigners arbeiten

Benutzerprofil . . . . . :   RENGEL

Auswahl eingeben und Eingabetaste drücken.
  2=Berechtigung editieren   4=Löschen     5=Berechtigung anzeigen
  7=Umbenennen   8=Beschreibung anzeigen   9=Eigner ändern

Ausw  Objekt                 Bibliothek    Art       Attribut    ASP-Einh.
  _     /home/liste.pdf/QP >               *STMF                 *SYSBAS
  _     /tmp/AUQSHF_output                 *STMF                 *SYSBAS
  _     /tmp/AVQSHF_output                 *STMF                 *SYSBAS
  _     /SMZVDTA/quarantin >               *STMF                 *SYSBAS
  _     /tmp/EXCQSH_output                 *STMF                 *SYSBAS
  _     /tmp/IsLocked.sh                   *STMF                 *SYSBAS
  _     /tmp/JAQSHF_output                 *STMF                 *SYSBAS
  _     /tmp/ODQSHF_output                 *STMF                 *SYSBAS
  _     /tmp/RPT000001_All >               *STMF                 *SYSBAS
                                                                    Weitere ...
Parameter oder Befehl
===>
F3=Verlassen    F5=Aktual.    F9=Finden    F11=Beschreibungen anzeigen
F12=Abbrechen   F17=Anfang    F18=Ende     F24=Weitere Tasten
```

Mit Objekten eines Eigners arbeiten

Benutzerprofil
Dieser Parameter gibt den Namen eines Benutzerprofils an.

Auswahl
2=Berechtigung editieren
Die Berechtigung eines Benutzers für ein Objekt hinzufügen, ändern oder löschen.

4=Löschen
Löscht ein Objekt.

5=Berechtigung anzeigen
Zeigt eine Liste der Benutzer an, die zur Arbeit mit den angegebenen Objekten berechtigt sind.

7=Umbenennen
Ändert den Namen eines Objekts.

9.9.8
Seite 2

8=Beschreibung anzeigen
Zeigt die Namen und Attribute ausgewählter Objekte an. Diese Option wird für verzeichnisbasierte Objekte nicht unterstützt.

9=Eigner ändern
Ermöglicht es, das Eigentumsrecht für ein Objekt zu ändern.

Objekt
Der Name eines Objekts.

Bibliothek
Name der Bibliothek, die ein Objekt enthält, oder Name des Ordners, der ein Dokument enthält.

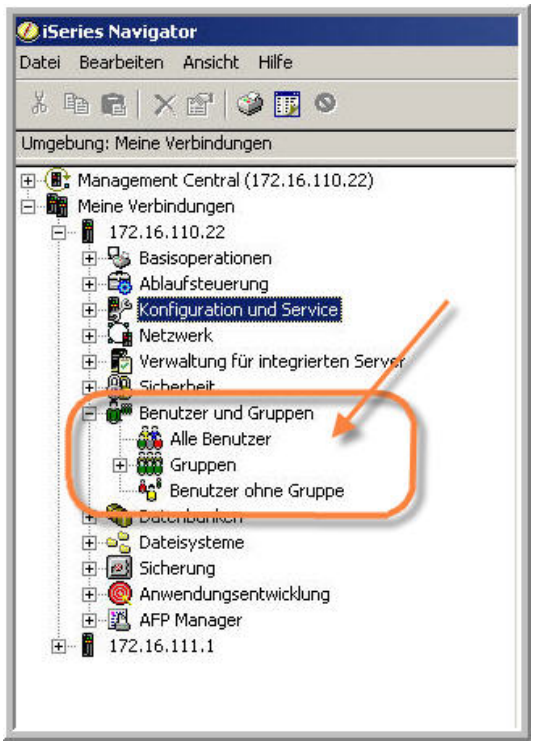
Art
Die Art eines Objekts, wie z. B. *PGM, *FILE oder *LIB.

Attribute
Da es mehrere Objektarten gibt, wird das Attribut zur näheren Beschreibung eines Objekts verwendet.

ASP-Einheit
Der Name der ASP-Einheit (ASP = Zusatzspeicherpool), in der sich ein Objekt befindet. *SYSBAS bedeutet, dass sich das Objekt im System-ASP oder in einem Basis-Benutzer-ASP befindet.

9.9.9 Benutzerverwaltung mit dem iSeries Navigator

Die Administration einer iSeries war lange Zeit die Domäne von 5250-Bildschirmen und -Dialogen. Mit Erscheinen der Client Access-Version 3.2 kam das Produkt iSeries Navigator auf den Windows Desktop. Während früher alle Funktionen einer iSeries aus dem 5250-Interface heraus installier-, konfigurier- und administrierbar waren, hat sich dieses Bild heute drastisch verändert. Heute existieren viele Funktionen, die ausschließlich dem iSeries Navigator vorbehalten sind. Die Dominanz der 5250-Bildschirme ist damit beendet. Ob dies gut oder schlecht ist, möchte ich nicht beurteilen. Fakt ist allerdings, dass der Navigator an vielen Stellen die tägliche Arbeit vereinfacht, so auch die Verwaltung der Benutzerprofile. Mit der Komponente „Benutzer und Gruppen" können Sie sich eine vollständige Liste aller Benutzerprofile und Gruppenprofile auf einer iSeries anzeigen lassen. Ausgehend von dieser Anzeige können Sie neue Profile erstellen oder bestehende verwalten.



Mit Benutzerprofilen arbeiten

Sie sehen, dass Sie sich „Alle Benutzer" anzeigen lassen können. Hierbei spielt die Gruppenzugehörigkeit einzelner Profile keine Rolle. Außerdem können „Gruppen" mit den entsprechenden Gruppenmitgliedern dargestellt werden. Eine Variante, die auf dem 5250-Interface nicht existiert. Und Sie haben zudem die Möglichkeit mit „Benutzern ohne Gruppe" zu arbeiten. So erhalten Sie einen umfassenden Überblick über die Organisation Ihrer Benutzerprofile.

9.9.9
Seite 2

Das Leistungsspektrum der Komponente „Alle Benutzer“ beinhaltet die folgenden Möglichkeiten:

- Benutzer zu vorhandener Gruppe hinzufügen,
- Kennwörter ändern,
- Benutzer kopieren,
- Benutzer erstellen,
- Benutzer löschen,
- Benutzer bearbeiten,
- Zertifikate für einen Benutzer öffnen.

Verwenden Sie die Komponente „Gruppen“, um

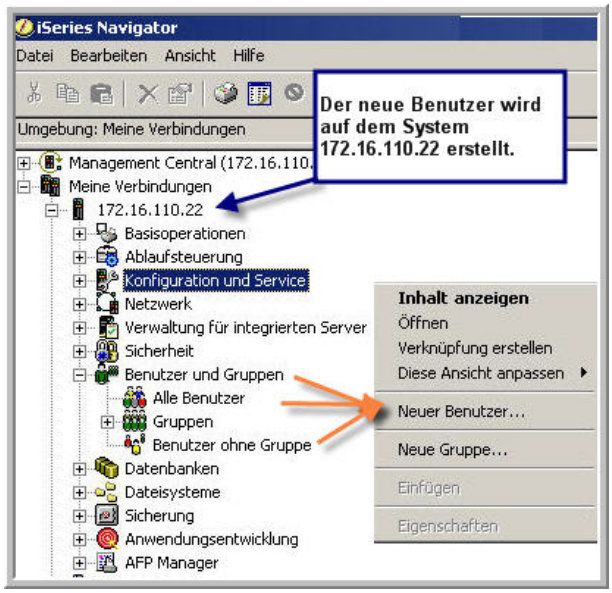
- Gruppen zu erstellen,
- Gruppen basierend auf einer anderen Gruppe zu erstellen,
- Gruppen zu löschen,
- Gruppen zu bearbeiten,
- Benutzer aus Gruppen zu entfernen.

Die Komponente „Benutzer ohne Gruppe“ bietet Ihnen die folgenden Möglichkeiten:

- Benutzer zu vorhandener Gruppe hinzufügen,
- Kennwörter ändern,
- Benutzer erstellen,
- Benutzer kopieren,
- Benutzer löschen,
- Benutzer bearbeiten,
- Zertifikate für einen Benutzer öffnen.

9.9.10 Einen neuen Benutzer erstellen

Generell besteht die Möglichkeit mit Management Central einen neuen Benutzer auf einem oder mehreren Endpunktsystemen oder auf allen Systemen in einer Systemverwaltungsgruppe zu erstellen. Sie können aber auch nur einen Benutzer auf einem einzelnen System erstellen. Zunächst erstelle ich lediglich einen neuen Benutzer auf einem System in unserer Liste der Verbindungen. Dazu erweitere ich das System in der Liste der Verbindungen auf dem ich den neuen Benutzer erstellen will und klicke jetzt mit der rechten Maustaste auf „Benutzer und Gruppen“ und wähle „Neuer Benutzer“. Alternativ können Sie auch auf „Alle Benutzer“ oder auf die Komponente „Benutzer ohne Gruppen“ klicken.

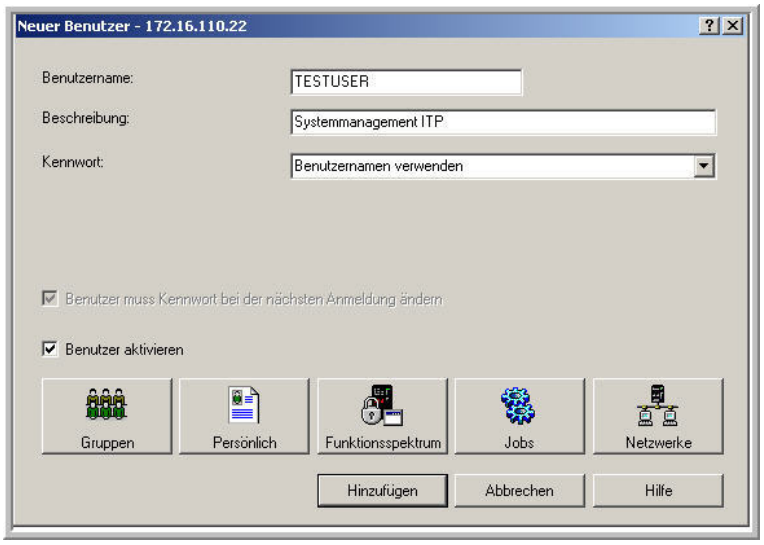


Einen neuen Benutzer anlegen

Anschließend öffnet sich ein Dialog, der sich mit dem CL-Befehl CRTUSRPRF vergleichen lässt. Da viele Parameter bereits detailliert besprochen wurden, verzichte ich an dieser Stelle auf eine erneute Erläuterung und nenne aus Gründen der Vergleichbarkeit lediglich den entsprechenden Parameter des Befehls CRTUSRPRF. Allerdings enthält der iSeries Navigator-Dialog an dieser Stelle auch Möglichkeiten, die das 5250-Interface bzw. der CRTUSRPRF-Befehl so nicht bietet. Diese Möglichkeiten werde ich zu gegebener Zeit entsprechend erläutern.

9.9.10
Seite 2

Beginnen wir aber zunächst mit dem Startfenster.

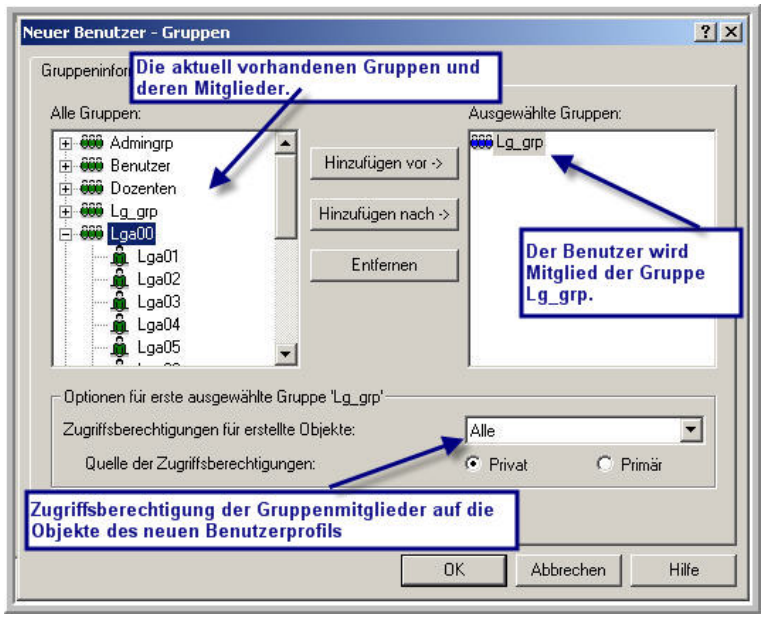


Der Startdialog „Neuer Benutzer“

Zunächst geben Sie den Benutzernamen (USRPRF), den beschreibenden Text (TEXT) und das Kennwort (PASSWORD) ein. Bei dem Kennwort lassen sich die Sonderwerte „Benutzername verwenden“ und „Kein Kennwort“ über ein Pulldown-Menü auswählen. Der Sonderwert „Kein Kennwort (*NONE) verwenden“ wird genutzt, um ein internes Benutzerprofil zu erzeugen, das nicht für die Anmeldung am System verwendet wird. Außerdem aktivieren bzw. deaktivieren Sie auf der ersten Seite das Profil und können damit einen Kennwortwechsel bei der nächsten Anmeldung (PWDEXP) erzwingen. Nachdem Sie die Grundparameter eingegeben haben, stehen am unteren Bildschirmrand weitere Schaltflächen zur Verfügung.

Der Dialog „Gruppen“

Ein Benutzer kann Mitglied einer Gruppe sein. Alle Mitglieder einer Gruppe verfügen über identische Berechtigungen. Normalerweise besteht eine Gruppe aus einem Personenkreis, der in derselben Unternehmensabteilung arbeitet, einen ähnlichen Aufgabenbereich hat und dieselben Anwendungen auf identische Weise nutzen muss.



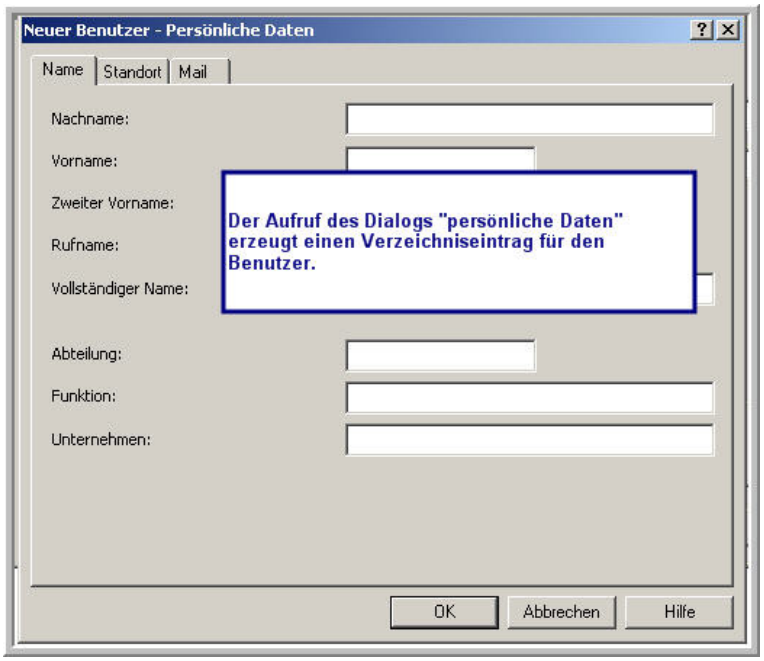
Zuordnung zu einer Gruppe

Auf der linken Seite sehen Sie alle existierenden Gruppenprofile und die aktuell zugeordneten Benutzer. Um das neu erstellte Profil einer Gruppe zuzuordnen, markiere ich auf der linken Seite eine Gruppe und drücke anschließend „hinzufügen vor“ oder „hinzufügen nach“. Die Gruppe erscheint daraufhin im rechten Bildschirmteil. Zusätzlich können Sie für die erste ausgewählte Gruppe des Benutzers weitere Berechtigungsoptionen angeben. Die Optionen (GRPAUT) bestimmen die Zugriffsberechtigungen der Gruppenmitglieder auf Objekte des neuen Benutzers. Mit dem iSeries Navigator können Sie die Objekteigenschaften nicht mehr an die Gruppe übertragen, d.h. der Benutzer „TESTUSER“ behält die Eignerschaft an allen Objekten, die er erstellt. Erstellt der Benutzer TESTUSER z. B. eine Query-Abfrage, ist er trotz der Gruppenmitgliedschaft Eigentümer des Objektes. Aufgrund der hinterlegten Option „ALLE“ dürfen allerdings alle Gruppenmitglieder auf das Objekt zugreifen als seien auch sie Objekteigentümer.

9.9.10
Seite 4

Der Dialog „Persönlich“

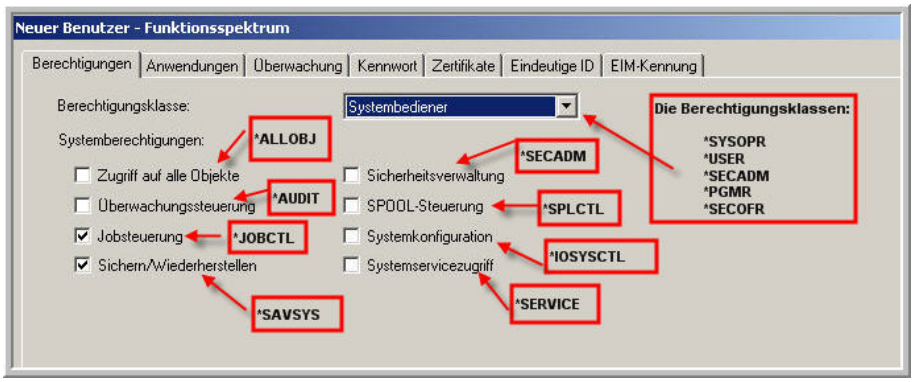
Der Dialog „Persönlich“ erzeugt für den Benutzer einen Verzeichniseintrag. Dies entspricht dem CL-Befehl ADDDIRE (add directory entry). Analog dem Befehl ADDDIRE können Sie weitreichende Benutzerdaten erfassen. Geben Sie hier den Namen, den Standort und die Mail-Optionen des Benutzers an.



Der Dialog „Persönliche Daten“

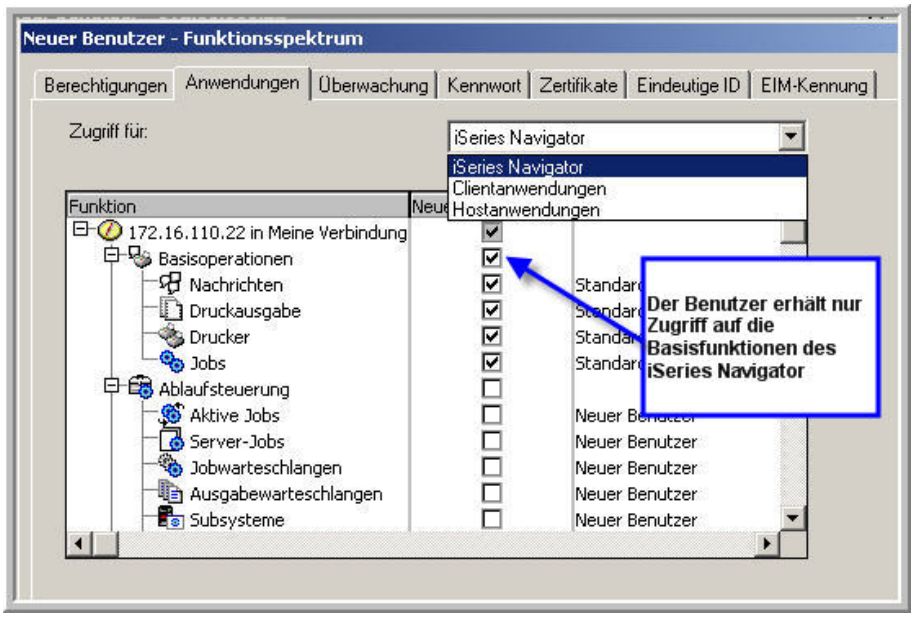
Der Dialog „Funktionsspektrum“

Im Dialog „Funktionsspektrum“ finden Sie wieder viele Parallelen zum CL-Befehl CRTUSRPRF. Im Register „Berechtigungen“ legen Sie die Benutzerklasse (USRCLS) fest und die entsprechenden Sonderberechtigungen (SPCAUT). Anders als im CL-Befehl können Sie allerdings sofort sehen, welche Sonderberechtigungen sich hinter den Benutzerklassen verbergen.



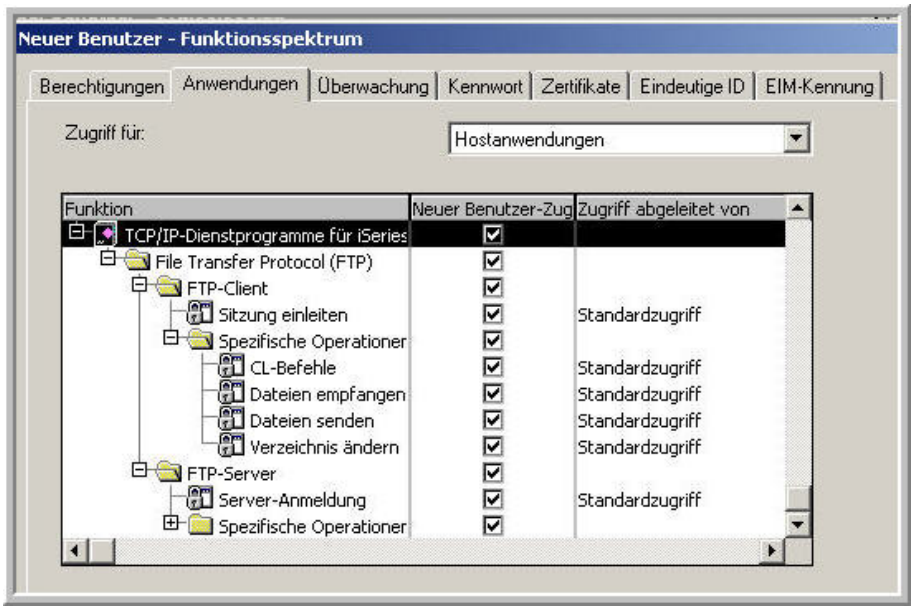
Benutzerberechtigungen hinterlegen

Das Register „Anwendungen“ ist Teil der Management-Zentralfunktion „Anwendungsverwaltung“ und auf dem 5250-Interface nicht verfügbar. Mit Hilfe der „Anwendungsverwaltung“ können einem Benutzer iSeries Navigator-Funktionen, Client Access-Funktionen und i5/OS-Dienstfunktionen gewährt bzw. entzogen werden.



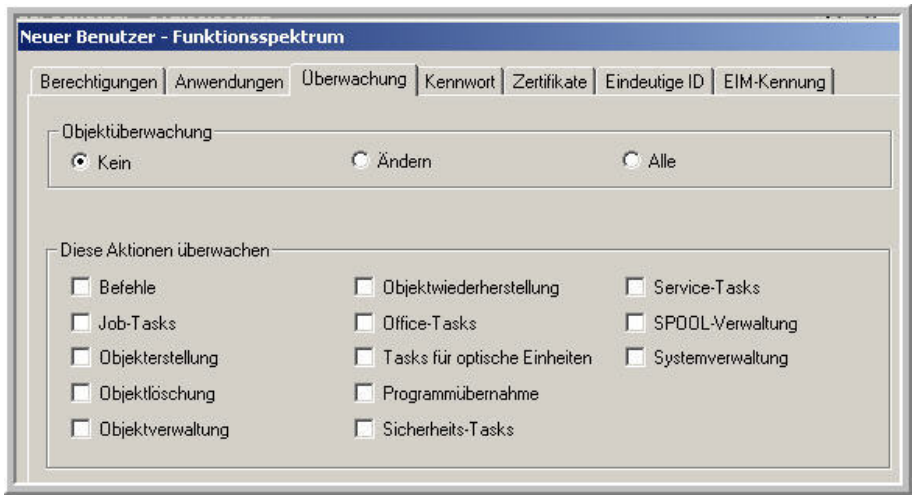
Zugriffsberechtigungen auf iSeries Navigator Funktionen

Oben sehen Sie die Darstellung aller iSeries Navigator-Funktionen. Hinter jeder Funktion steht ein Häkchen, welches bestimmt, ob der Benutzer die entsprechende Funktion nutzen darf. Entfernen Sie das Häkchen, so wird dem Benutzer die Nutzung der betreffenden Funktion entzogen – auch dann, wenn der Navigator in vollem Umfang auf dem entsprechenden PC installiert wurde. Diese Anwendungsverwaltung existiert auch für alle Client Access-Funktionen und i5/OS-Dienste. Sinnvoll ist im Bereich der Host-Anwendungen insbesondere die Möglichkeit, die Nutzung des FTP-Servers und -Clients im i5/OS einzuschränken.



Die Host-Anwendungen einschränken

Das Register „Überwachung“ entspricht dem CL-Befehl CHGUSRAUD. In diesem Register bestimmen Sie, welche Aktionen des Benutzers überwacht werden sollen. Die Aktivierung des Sicherheitsprotokolls ist meistens nur für einen kurzen Zeitraum erforderlich und sollte sehr sorgfältig geplant werden.



Benutzerüberwachung aktivieren

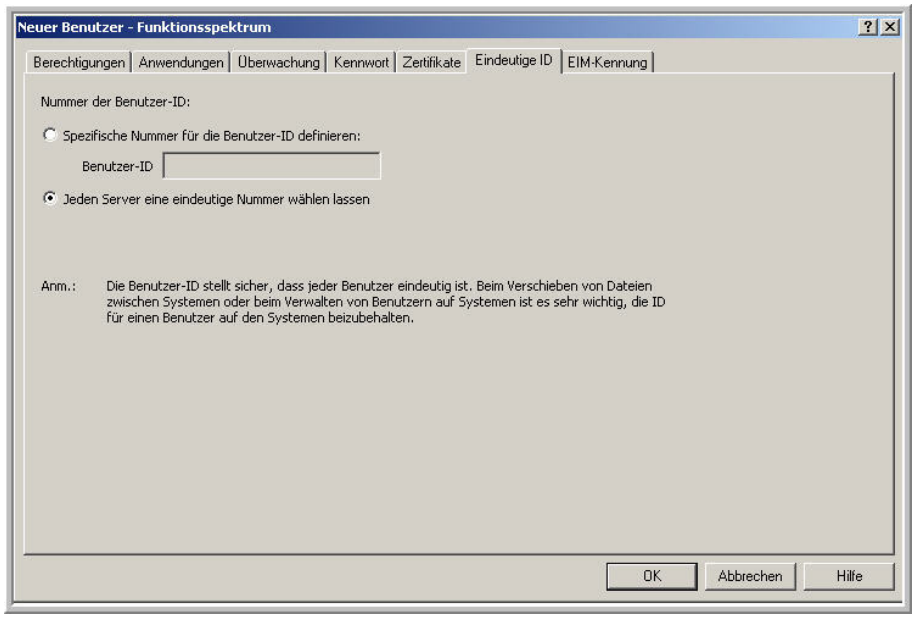
Im nächsten Register finden Sie wieder typische, den Kennwortverfall (PWD-EXPITV) steuernde Parameterwerte.

Kennworteinstellungen

Seit dem Release V5R4 können Sie entscheiden, ob die Kennwortverwaltung lokal auf dem iSeries System oder auf einer anderen Plattform verwaltet wird. Die Option entspricht dem Parameter LCLPWDMGT der Befehle CRTUSRPRF und CHGUSRPRF. Bei der Auswahl „Kennwort über eine andere Plattform verwalten“ wird das lokale i5/OS-Kennwort auf den Wert *NONE gesetzt. Der Benutzer ist dann nicht mehr in der Lage, sein eigenes Kennwort mit dem Befehl CHGPWD (Kennwort ändern) zu ändern. Außerdem kann er sich nicht direkt am System anmelden. Sie sollten diesen Wert nur verwenden, wenn der Benutzer ausschließlich über eine fremde Plattform wie Windows auf das System zugreifen muss.

Im Dialog „Funktionsspektrum – Zertifikate“ können Sie bestehende Zertifikate verwalten, die an einen Benutzer ausgegeben wurden. Ein Zertifikat bindet einen allgemeinen Schlüssel an den Benutzer, dem das Zertifikat gehört und ermöglicht somit die Authentifizierung des Zertifikateigners. Die Liste mit den Zertifikaten zeigt den Herausgeber des Zertifikats, die Seriennummer des Zertifikats und das Verfallsdatum des Zertifikats.

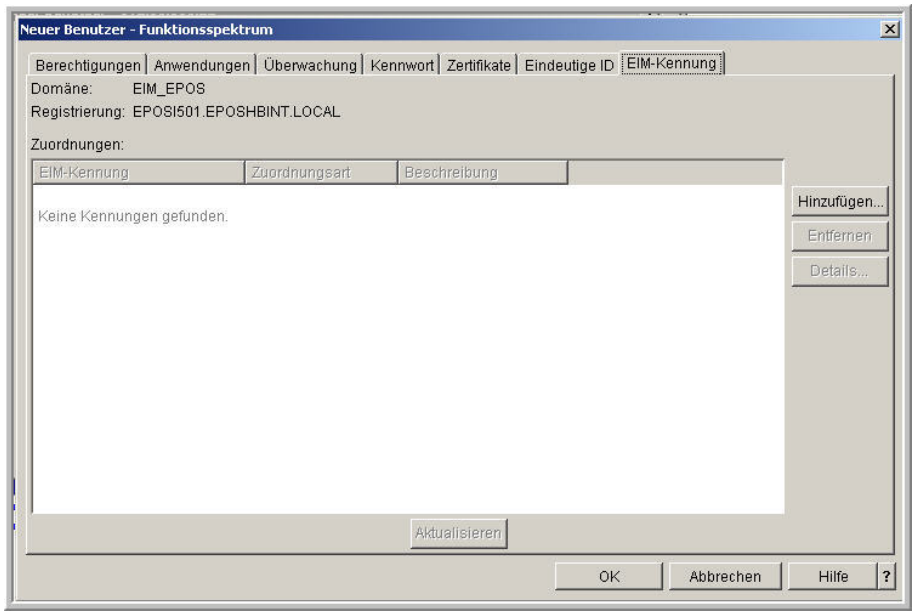
Das System verwendet eine interne eindeutige Benutzer-ID, um ein Benutzerprofil innerhalb eines Netzwerkes zu identifizieren und seine Berechtigungen zu überprüfen.



Die Benutzer-ID

In den meisten Fällen ist es am besten, wenn das System die Benutzer-ID für den neuen Benutzer wählt. Wenn Ihr iSeries-Server jedoch in ein Netzwerk integriert ist, müssen Sie möglicherweise selber die Werte für die Nummer der Benutzer-ID zuordnen, die mit denen übereinstimmt, die bereits auf den anderen Servern zugeordnet wurde. Nur so können Sie sicherstellen, dass die Benutzer-ID dieses Profils mit den anderen Systemen im Netzwerk übereinstimmt. Verwenden Sie in diesen Fällen einen Wert zwischen 1 und 4.294.967.294. Wenn Sie mit Management Central einen neuen Benutzer zu einem oder zu mehreren Endpunktsystemen hinzufügen, können Sie das zentrale System anhand des Inventars auf allen ausgewählten Systemen eine eindeutige Nummer festlegen lassen.

Der Dialog „EIM-Kennung“ ist nur für EIM-Benutzer gültig. Ein EIM-Benutzer ist Mitglied einer vordefinierten LDAP-Benutzergruppe (LDAP = Lightweight Directory Access Protocol) für eine bestimmte Domäne. Die in der LDAP-Benutzergruppe hinterlegten EIM-Zugriffsrechte bestimmen, welche Dienste der Benutzer innerhalb einer bestimmten Domäne nutzen darf. Damit aber auch Ihr iSeries-Server den Benutzer autorisieren kann, muss eine Verbindung zwischen dem iSeries Benutzerprofil und der entsprechenden EIM-Kennung hergestellt werden. Dies geschieht mit dem Dialog „EIM-Kennung“.

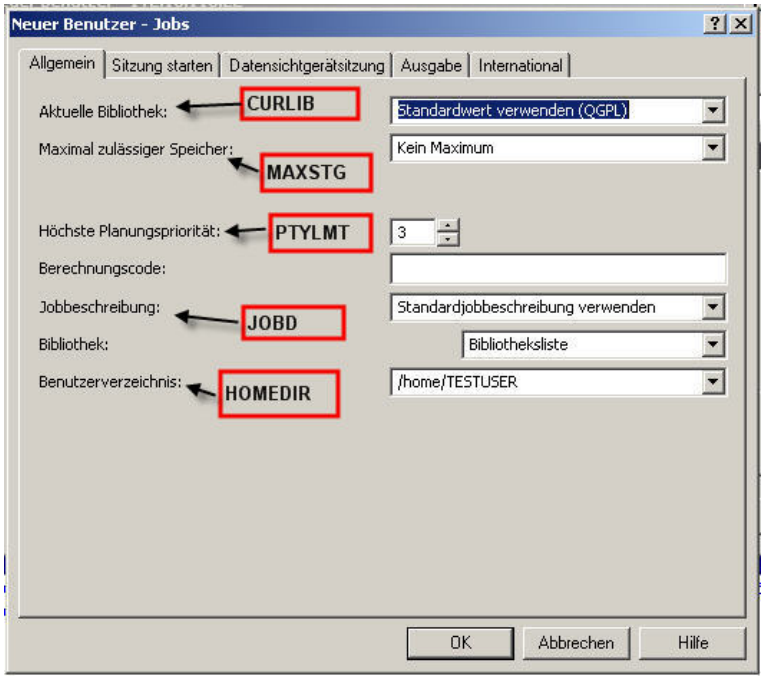


Zuordnung der EIM-Kennungen

9.9.10
Seite 10

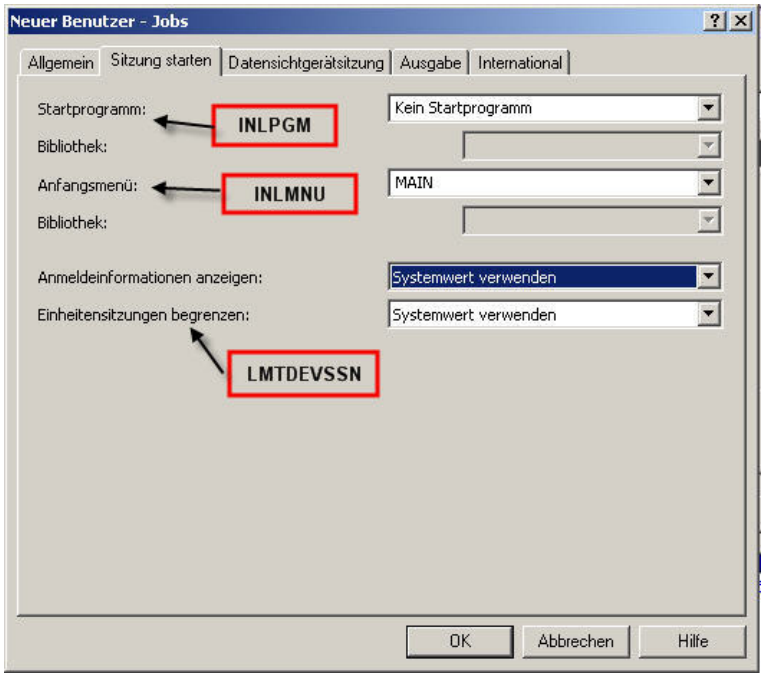
Der Dialog „Job“

Klicken Sie auf die Schaltfläche „Jobs“, um die Seite mit den Eigenschaften für Jobs anzuzeigen. Hier geben Sie die Joboptionen des Benutzers an. Die Parameter kennen Sie bereits und sollen daher an dieser Stelle nicht erneut erläutert werden. Zur Übersicht zeige ich Ihnen im Folgenden lediglich die entsprechenden Register mit dem Verweis auf die Parameternamen der CL-Befehle CRTUSRPRF und CHGUSRPRF.



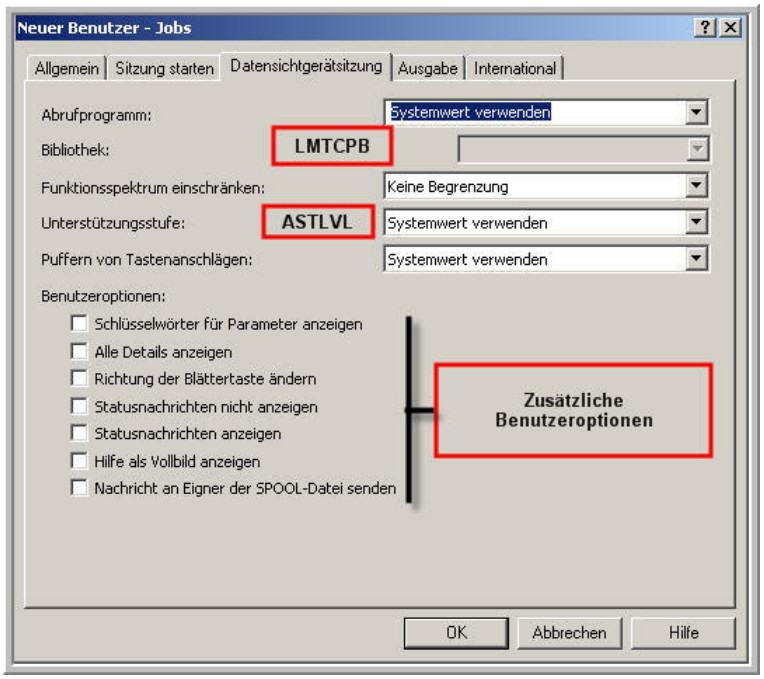
Der Dialog Jobs-Allgemein

Im nächsten Register sind alle Profilparameter zusammengefasst, die die Session eines Benutzers bestimmen. Hier hinterlegen Sie das Anfangsmenü und ggf. das benötigte Startprogramm.



Der Dialog „Jobs – Sitzung starten“

Der Dialog Jobs-Funktionsspektrum beinhaltet u.a. den Parameter LMT-CPB, der das Funktionsspektrum, das dem Benutzer auf dem iSeries-Server zur Verfügung steht, nicht, teilweise oder vollständig einschränkt.

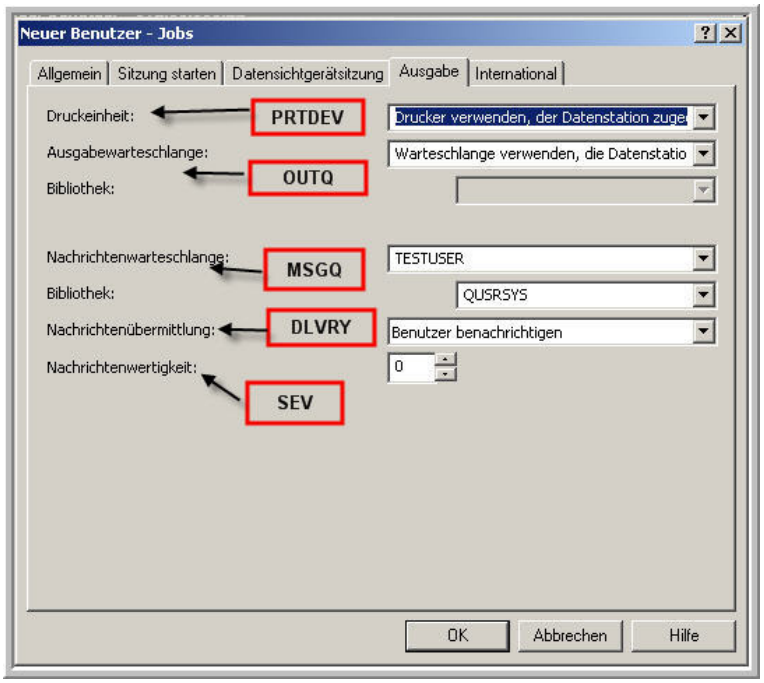


Der Dialog „Jobs – Datensichtgerätsitzung“

In der oberen Abbildung können Sie erkennen, dass dieser Dialog weitere Benutzeroptionen enthält, die den Befehlen CRTUSRPRF und CHGUSRPRF fehlen.

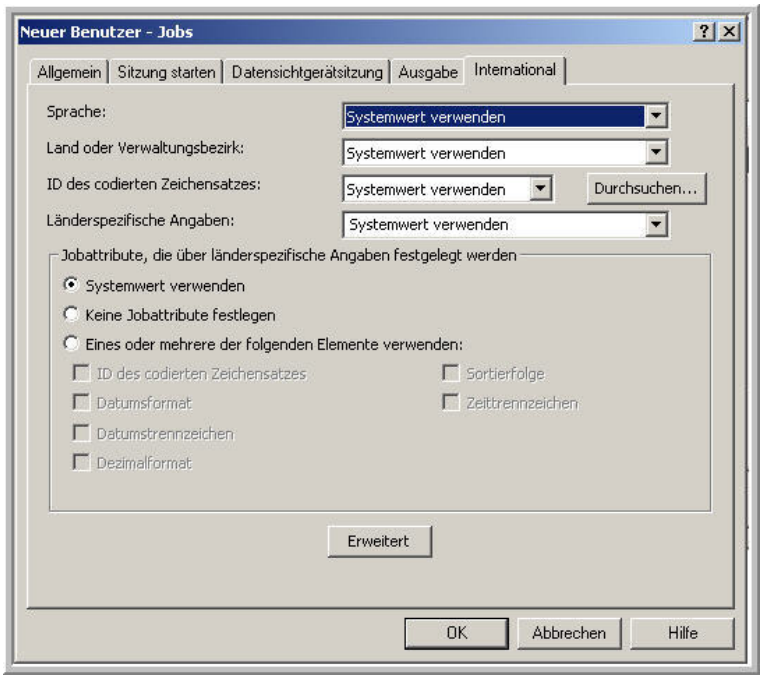
Wählen Sie die Option „Schlüsselwörter für Parameter anzeigen“, wenn anstelle der möglichen Parameterwerte die Schlüsselwörter für die Parameter angezeigt werden sollen. Die Option „Richtung der Blättertaste ändern“ bestimmt die Wirkungsweise der Bild-Auf und Bild-Up-Tasten, d.h. die Wirkungsweise der Taste zum Vorblättern und der Taste zum Zurückblättern werden umgekehrt. Falls Sie verhindern wollen, dass der Benutzer Meldungen in der Statuszeile erhält, müssen Sie die Option „Statusnachrichten nicht anzeigen“ aktivieren; andernfalls wählen Sie die Option „Statusnachrichten anzeigen“. Durch Auswahl der Option „Hilfe als Vollbild anzeigen“ werden stets alle Hilfetexte im Vollbildschirm und nicht in einem Fenster angezeigt. Wenn die Option „Nachricht an Eigner der SPOOL-Datei senden“ gewählt wird, erhält der Eigner der Spooldatei eine Nachricht, wenn ein Druckausgabeprogramm eine Spooldatei erstellt.

Im Dialog JOBS-Ausgabe ordnen Sie dem Benutzer einen spezifischen Drucker zu, der stets als Standarddrucker verwendet wird, wenn innerhalb des entsprechenden Jobs keine anderen Einstellungen vorgenommen wurden. An dieser Stelle wird auch die Nachrichtenwarteschlange zugeordnet.



Der Dialog „Jobs – Ausgabe“

Als letztes enthält der Dialog „Jobs – International“ die Profileinstellungen für die Sprache, Sortierfolgen und sonstige landestypischen Einstellungen.

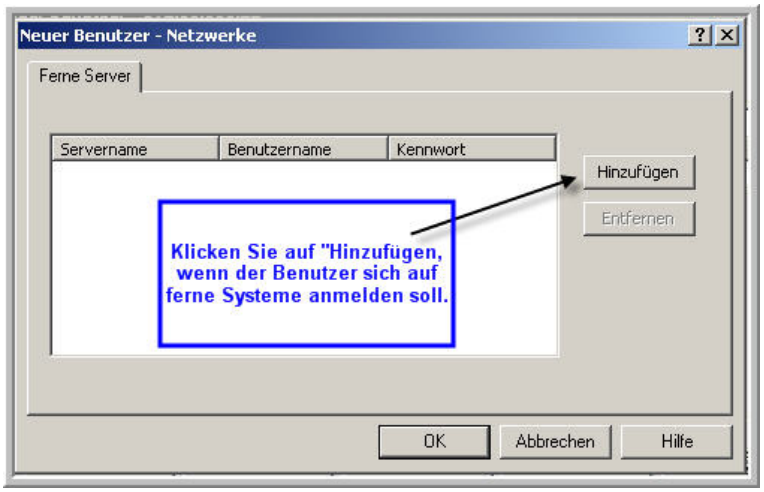


Der Dialog „Jobs-International“

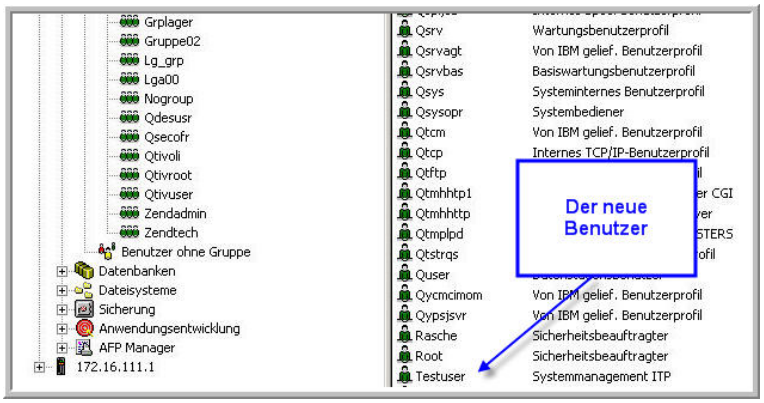
9.9.10
Seite 14

Der Dialog „Netzwerke“

Im Dialog „Netzwerke“ finden Sie eine Liste ferner Server. Diese Liste enthält den Namen des fernen Servers. Jeder Servereintrag muss eindeutig sein. Zusätzlich wird der Benutzername für den Server und das zugehörige Kennwort erfasst. Falls der Benutzer auf dem Server bereits existiert müssen Sie seine eindeutige Benutzer-ID verwenden. Sie können die Liste beliebig sortieren, indem Sie auf die entsprechende Überschriftenzeile klicken.



Wenn Sie alle Benutzereinstellungen erfasst haben, klicken Sie auf „OK“. Anschließend erscheint das Profil in Ihrer Benutzerliste.

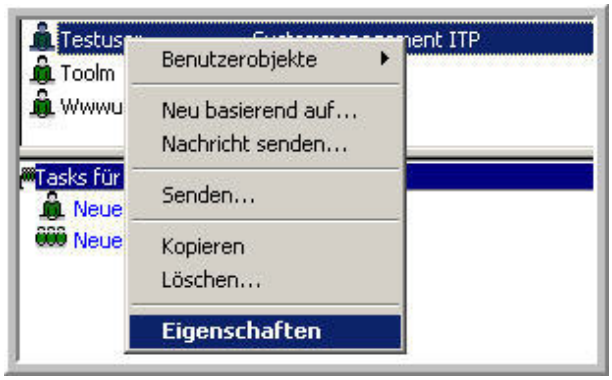


Das neue Benutzerprofil

9.9.11 Benutzer verwalten

Natürlich können Sie mit dem iSeries Navigator auch Ihre bestehenden Benutzerprofile verwalten, d.h. Benutzerprofile können verändert, kopiert oder auch gelöscht werden. Doch der iSeries Navigator kann mehr! Sie können Ihre Benutzergruppen sehr einfach und komfortabel verwalten und es ist sogar möglich, bestehende Benutzerprofile an andere iSeries-Server zu senden.

Benutzer ändern
Wenn Sie einen Benutzer ändern wollen, erweitern Sie zunächst wieder im iSeries Navigator das entsprechende System in Ihrer Liste der Verbindungen. Erweitern Sie dann den Eintrag „Benutzer und Gruppen“, und klicken auf „Alle Benutzer“, um alle Benutzer im System anzuzeigen. Wenn Sie jetzt mit der rechten Maustaste auf den zu bearbeitenden Benutzer klicken, können Sie anschließend die Eigenschaften auswählen und entsprechende Veränderungen vornehmen.

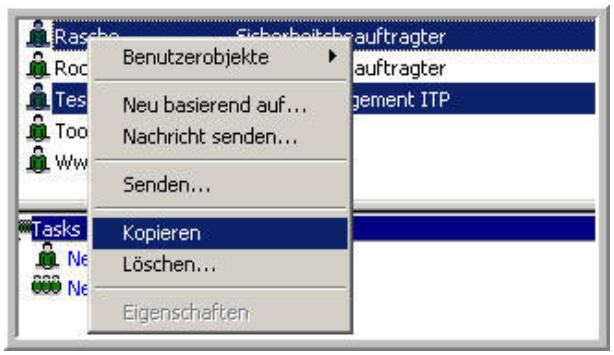


Die Benutzereigenschaften

Der anschließend erscheinende Dialog ist identisch mit der Neuanlage von Benutzern, so dass er hier nicht erneut gezeigt werden muss. Der Weg über die Eigenschaften ist die Standardaktion. Sie können aber auch einfach auf den Benutzer doppelklicken, den Sie ändern möchten. Auch dann erscheint der Dialog zur Änderung der Benutzereigenschaften.

Benutzer kopieren

Wenn Sie einen oder mehrere bestehende Benutzer kopieren wollen, um einen neuen Benutzer mit denselben Eigenschaften auf einem anderen System oder auf demselben System unter einem anderen Namen zu erstellen, selektieren Sie hierfür den oder die zu kopierenden Benutzer und klicken Sie wiederum mit der rechten Maustaste auf einen der Benutzer.



Benutzer kopieren

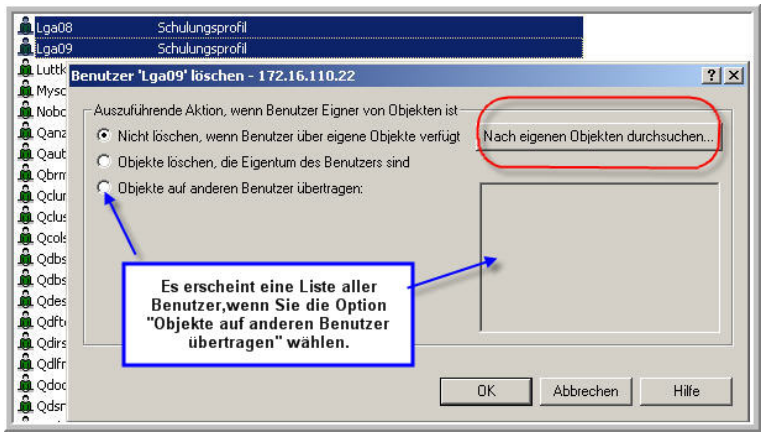
Sie sehen, dass ich mehrere Benutzer markiert habe und dann die Funktion „Kopieren“ ausgewählt habe. Wenn der Benutzer auf ein anderes Zielsystem erstellt werden soll, müssen Sie jetzt das Zielsystem in Ihrer Liste der Verbindungen erweitern. Klicken Sie anschließend mit der rechten Maustaste auf „Alle Benutzer“, „Benutzer ohne Gruppe“ oder auf eine bestimmte Gruppe, und wählen Sie den Eintrag „Einfügen“ aus, um den Benutzer zu kopieren.

Benutzer einfügen

Danach öffnet sich der Dialog „Neuer Benutzer“. Sie müssen jetzt nur noch die leeren Felder ausfüllen und ein neues Kennwort angeben. Für weitere Änderungen klicken Sie auf die entsprechenden Schaltflächen. Mit „OK“ erstellen Sie schließlich die Benutzerkopie. Der oben geschilderte Weg ist das Standardvorgehen. Sie können einen Benutzer auch einfach durch Drag & Drop in eine andere Gruppe oder auf ein anderes System kopieren.

Benutzer löschen

Ähnlich gehen Sie vor, wenn Sie ein oder mehrere Benutzerprofile löschen wollen. Wählen Sie den oder die Benutzer aus, der bzw. die gelöscht werden soll(en). Klicken Sie auch jetzt wieder mit der rechten Maustaste auf einen ausgewählten Benutzer, und wählen Sie „Löschen“. Anschließend öffnet sich der folgende Dialog:



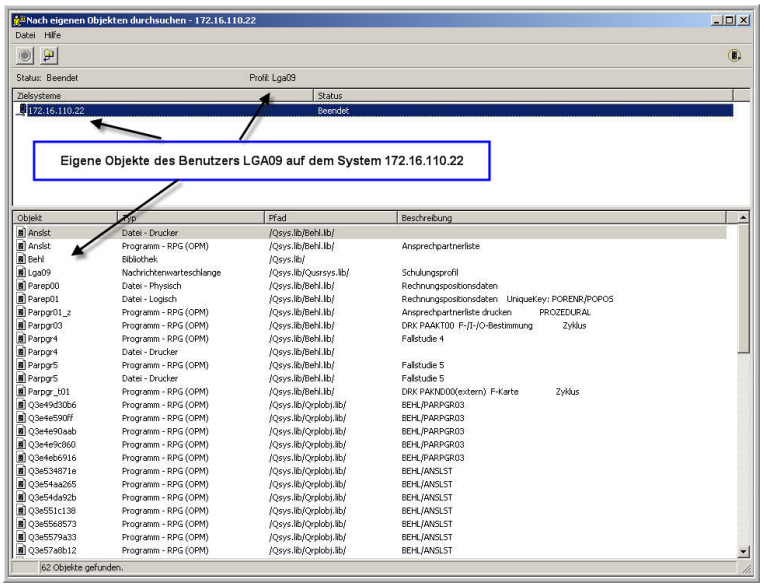
Der Dialog „Benutzer löschen“

Sie sehen, dass der Benutzer nicht gelöscht wird, wenn er Eigentümer von Objekten ist. Dies entspricht der Standardeinstellung des 5250-Dialoges.

Falls Sie prüfen wollen, welche Objekte dem Benutzer gehören, klicken Sie auf „Nach eigenen Objekten durchsuchen“, um die Objekte anzuzeigen, die dem Benutzer auf dem System gehören.

Suche nach eigenen Objekten

Die Suchergebnisse werden anschließend für jeden Benutzer in separaten Fenstern dargestellt.



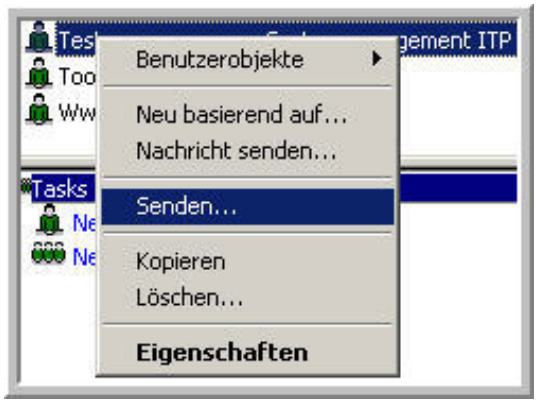
Das Suchergebnis für den Benutzer LGA09

Ebenso wie auf dem 5250-Interface können Sie die Objekte gemeinsam mit dem Profil löschen oder die Objekte auf einen neuen Eigner übertragen. Falls Sie das Eigentumsrecht der Objekte auf einen anderen Benutzer übertragen möchten, wählen Sie den gewünschten Benutzernamen aus der Liste der verfügbaren Benutzer aus. Die Objekte werden anschließend auf den neuen Benutzer übertragen, und zwar unabhängig von der aktuellen Berechtigung, die der Benutzer für die Objekte besitzt.

Benutzer an entfernte Systeme senden

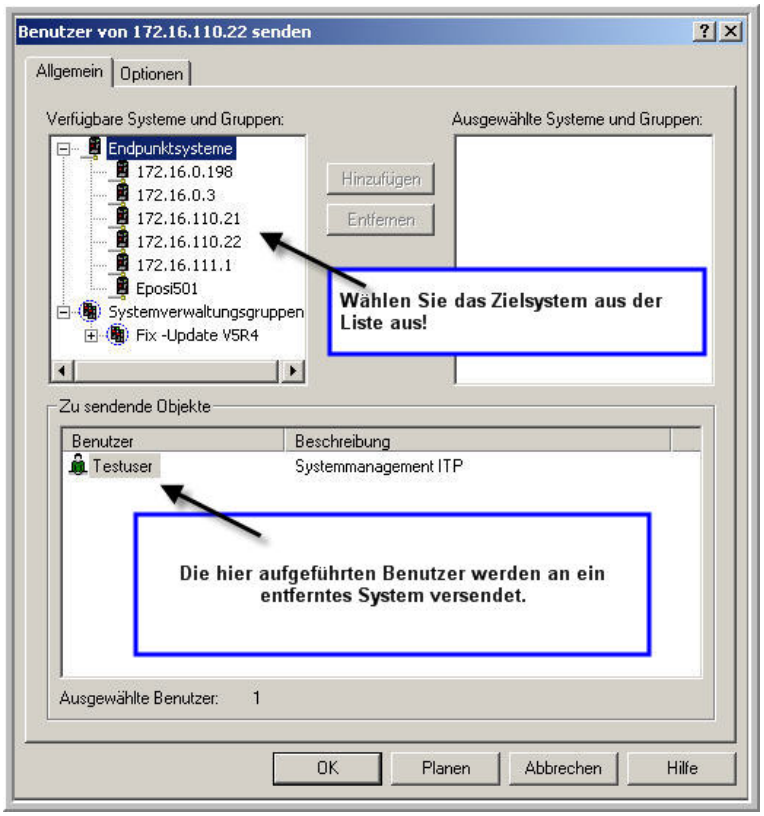
Sie können einen oder mehrere Benutzer an ein anderes System oder an alle Systeme einer Systemverwaltungsgruppe senden. Dabei werden so viele Benutzereigenschaften wie möglich auf das neue System kopiert. Die Informationen, die für jeden Benutzer gesendet werden, enthalten das Benutzerprofil, die persönlichen Berechtigungen, evtl. IDs für Enterprise Identity Mapping (EIM) sowie die Kennwörter. Für jeden gesendeten Benutzer wird automatisch ein Eintrag im Systemverteilerverzeichnis erstellt bzw. aktualisiert. Sie können mit Ausnahme einiger systemdefinierter Benutzer jedes Profil an entfernte Systeme senden. Die Namen der systemdefinierten Benutzerprofile beginnen normalerweise mit einem Q wie QSECOFR.

Wenn ich unseren TESTUSER an ein entferntes System senden will, muss ich wieder die Liste meiner Endpunktsysteme erweitern und den Benutzer markieren, der versendet werden soll.



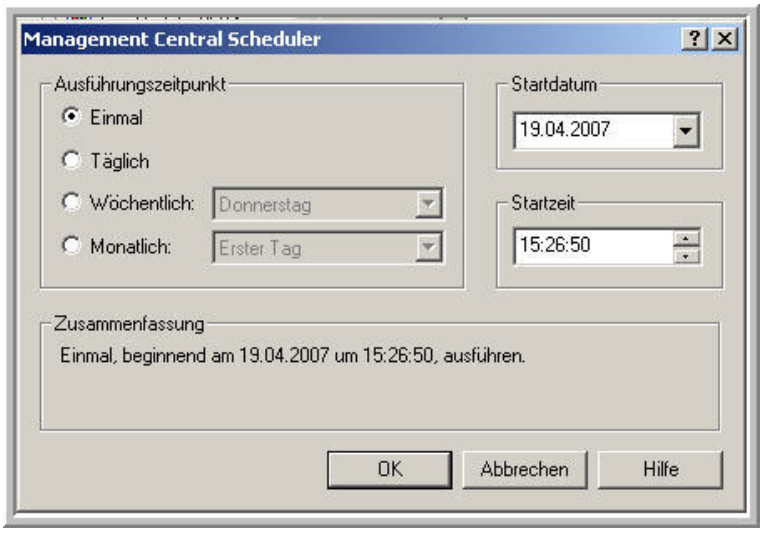
Benutzer senden

Anschließend öffnet sich ein weiterer Dialog.



Zielsysteme auswählen

Im rechten Fenster erscheint eine Liste mit Endpunktsystemen und Systemverwaltungsgruppen, an die eine Liste mit Benutzern oder Gruppen gesendet werden kann. Sie können ein System auswählen, indem Sie den entsprechenden Eintrag in der Liste der verfügbaren Systeme und Gruppen auswählen und dann auf „Hinzufügen“ klicken. Am unteren Bildschirmrand sehen Sie die Benutzer und Gruppen, die an die ausgewählten Endpunktsysteme und Systemverwaltungsgruppen gesendet werden. Klicken Sie auf den Reiter „Optionen“, um die Aktion anzugeben, die ausgeführt werden soll, wenn ein selektierter Benutzer bereits auf dem Zielsystem vorhanden ist. Sie können wählen, ob der bereits vorhandene Benutzer nicht geändert oder mit den Einstellungen des gesendeten Benutzers aktualisiert werden soll. Klicken Sie anschließend auf „OK“, um die Übertragung sofort zu starten, oder klicken Sie auf „Planen“, um festzulegen, wann der Task gestartet werden soll.

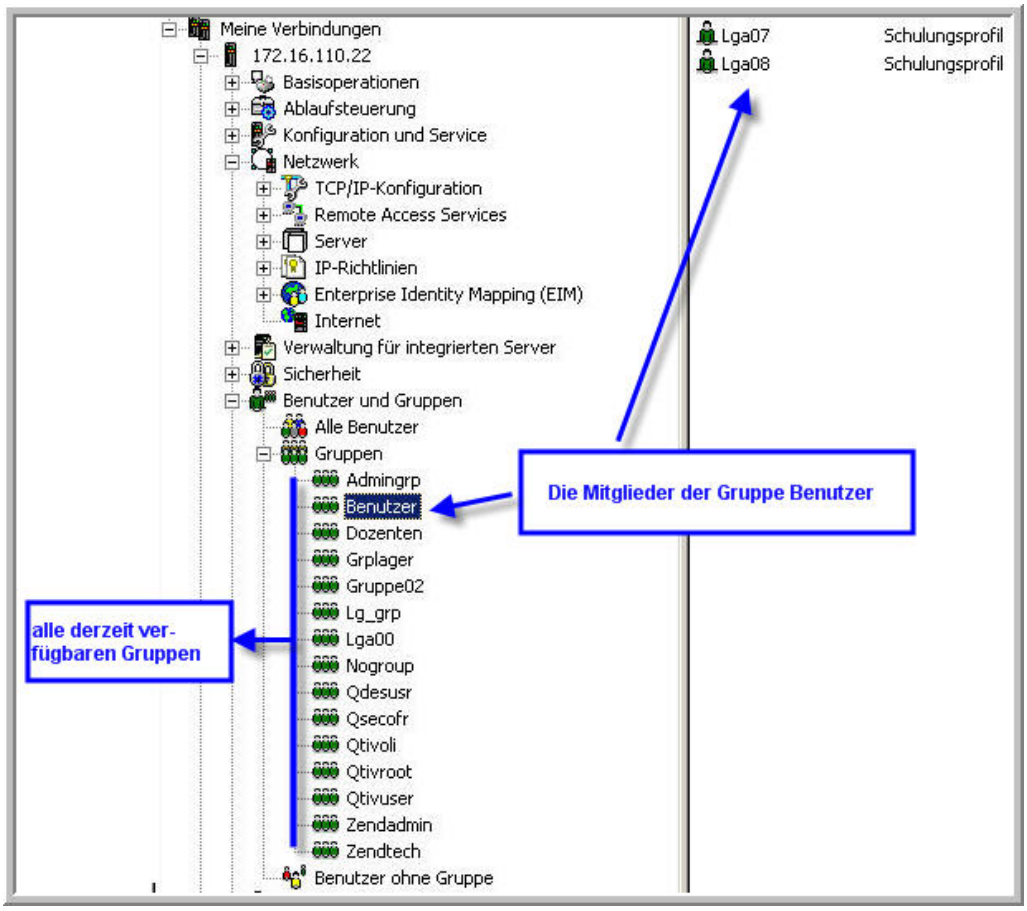


Den Sende-Task planen

Mit dem Management Central Scheduler können Sie bestimmen, wann die Management Central-Tasks ausgeführt werden sollen. Soll der Task nur einmalig ausgeführt werden, wählen Sie die Option „Einmal“. Der Task wird ein einziges Mal ausgeführt. Der Beginn wird durch das angegebene Datum und die Uhrzeit festgelegt. Sie können die Übertragung auch täglich, wöchentlich oder monatlich ausführen. Diese Optionen sind allerdings im Zusammenhang mit Benutzerprofilen wenig sinnvoll.

Benutzergruppen

Besonders einfach gestaltet sich die Arbeit mit Benutzergruppen mit Hilfe des iSeries Navigators. Im Gegensatz zum i5/OS, wo es den Objekttypus des Gruppenprofils nicht gibt, ist hier sehr wohl eine separate Bearbeitung von Benutzerprofilen, die den Status einer Gruppe haben, möglich. Erweitern Sie einfach „Benutzer und Gruppen". Im Verzeichniseintrag „Gruppen" werden alle Gruppenprofile Ihres Systems übersichtlich dargestellt.



Mit Benutzergruppen arbeiten

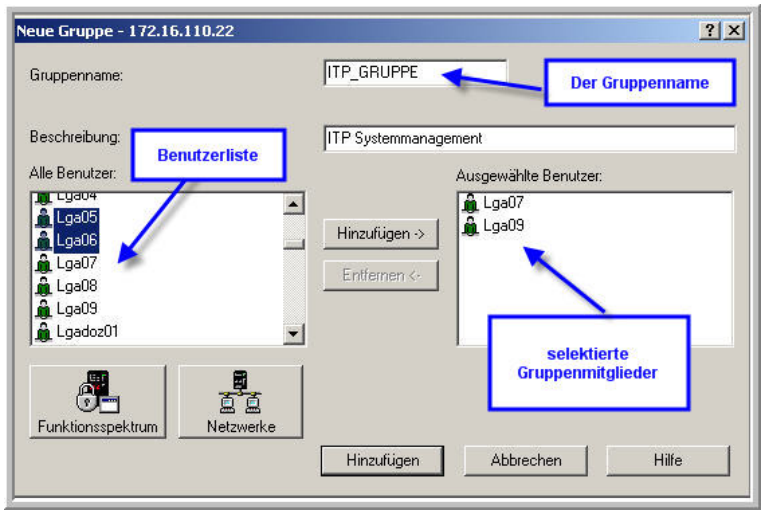
Sobald Sie eine Gruppe markieren, sehen Sie in der Detailanzeige des iSeries Navigator die Gruppenmitglieder. Ein Doppelklick auf eines der Member-Profile ermöglicht Ihnen die Änderung des Benutzers.

Neue Benutzergruppe

Interessant am iSeries Navigator ist insbesondere die Funktion „Neue Gruppe“. Dies würde einem CL-Befehl CRTGRPPRF entsprechen – nur als erfahrener iSeries Operator wissen Sie, dass IBM diesen Befehl niemals im 5250-Interface implementiert hat, aber im Navigator gibt es diese Funktion:

Eine neue Gruppe erstellen

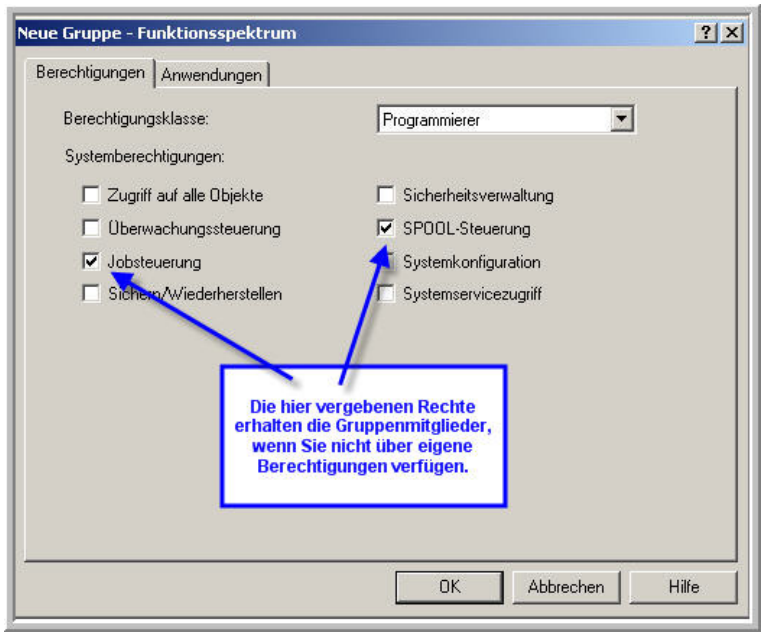
Um eine neue Gruppe zu erstellen, öffnen Sie entweder das Kontextmenü „Gruppen“ mit der rechten Maustaste und wählen „Neue Gruppe“ oder Sie klicken mit der rechten Maustaste auf den Verzeichniseintrag „Benutzer und Gruppen“. In beiden Fällen gelangen Sie in den zentralen Dialog, der es Ihnen ermöglicht, eine neue Benutzergruppe zu erstellen und dieser Gruppe Benutzerrechte und Funktionen zuzuordnen.



Gruppenmitglieder zuordnen

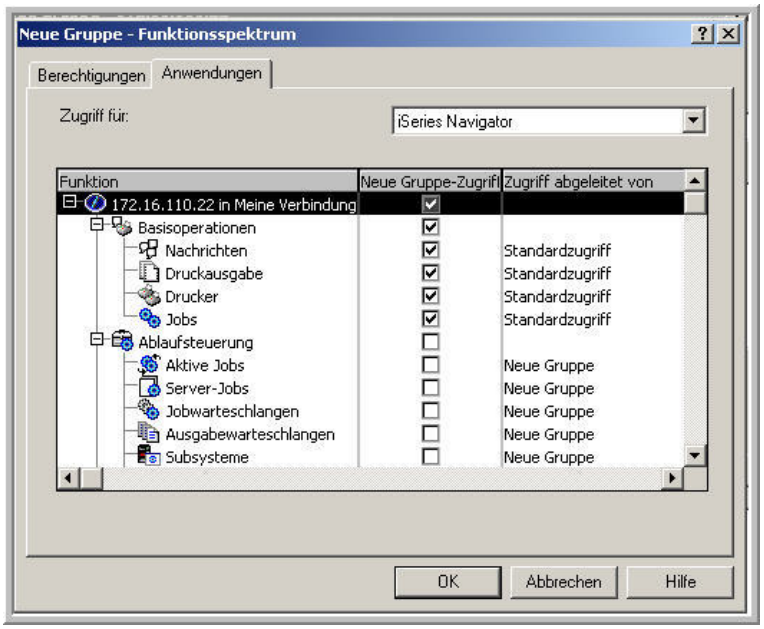
9.9.11
Seite 10

Sie sehen, dass ich der Gruppe zunächst einen sprechenden Namen gebe. In der Liste „Alle Benutzer“ finden Sie die Benutzerprofile, die der Gruppe zugeordnet werden können. Ich habe die User LGA07 und LGA09 selektiert und anschließend „Hinzufügen“ gewählt. Daraufhin erscheinen die Benutzer in der Liste der „ausgewählten Benutzer“. Falls weitere Benutzer hinzugefügt werden sollen, kann dieser Vorgang beliebig oft wiederholt werden – natürlich auch bei bereits bestehenden Gruppen. Da es möglich ist, die Sonderberechtigungen der Benutzer über die Gruppe zu steuern, steht uns jetzt noch der Dialog „Funktionsspektrum“ zur Verfügung, den Sie bereits kennen.



Die Sonderberechtigungen der Gruppe

Und auch die Anwendungsverwaltung können Sie zentral über die Gruppe steuern.



Die Anwendungsverwaltung

Wenn Sie alle Eingaben gemacht haben, klicken Sie auf „OK“. Die Gruppe ist erstellt und erscheint anschließend in der Liste Ihrer Gruppenprofile.

9.9.11
Seite 12

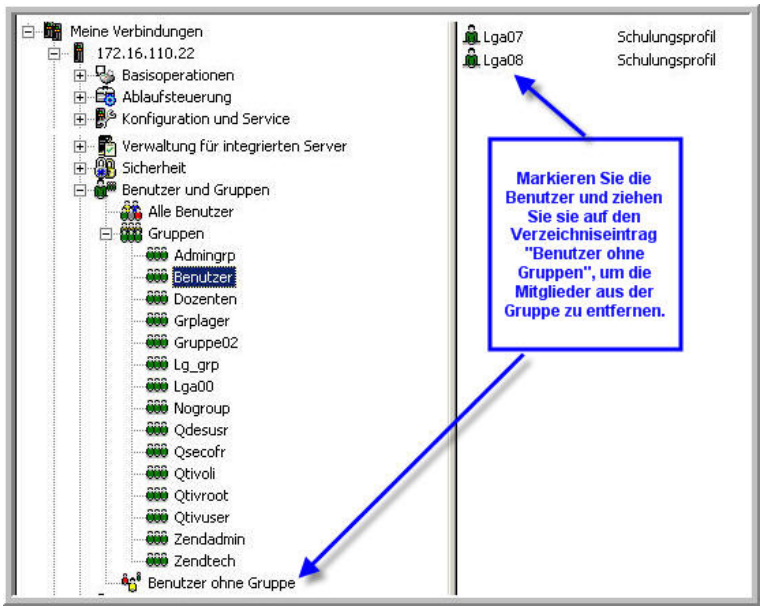
Benutzergruppenverwaltung

Die Verwaltung der Gruppen, d.h. das Ändern, Löschen und Kopieren ist identisch mit der Bearbeitung eines einzelnen Benutzerprofils und muss daher nicht erneut vorgestellt werden. Gruppenmitglieder können Sie wie erläutert über die Standarddialoge zuordnen und entfernen oder einfach mittels Drag & Drop zuordnen. Um Benutzerprofile einer Gruppe zuzuordnen, erweitern Sie den Eintrag „Alle Benutzer“ oder „Benutzer ohne Gruppe“, markieren die entsprechenden Benutzer und ziehen die Benutzer anschließend auf die entsprechende Gruppe. Fertig!

Ähnlich gehen Sie vor, um Benutzer aus einer Gruppe zu entfernen.

Öffnen Sie hierfür zunächst den Verzeichniseintrag „Gruppen“. In der Detailanzeige des iSeries Navigators werden die Gruppenmitglieder angezeigt. Markieren Sie die zu entfernenden Member. Mit der Kontexttaste steht Ihnen die Funktion „Aus Gruppe entfernen“ zur Verfügung.

Sie können aber auch hier die Drag & Drop-Funktion nutzen, indem Sie die Gruppenmitglieder markieren und anschließend auf den Verzeichniseintrag „Benutzer ohne Gruppen“ ziehen.



Benutzer aus einer Gruppe entfernen

Eine letzte Anmerkung zu dem Verzeichniseintrag „Benutzer ohne Gruppen“: Verwenden Sie „Benutzer ohne Gruppe“ um einzelne Benutzer, die sich in keiner Gruppe befinden, auf dem verwendeten iSeries-Server anzuzeigen und/oder um mit solchen Benutzern zu arbeiten. So kann es nicht passieren, dass Sie vergessen, einen Benutzer einer Gruppe zuzuordnen. Eine sehr sinnvolle Darstellung wie ich finde, die auch in dieser Form nicht auf dem 5250-Bildschirm existiert.

Sie sehen, die Verwaltung der Benutzerprofile im iSeries Navigator hat einiges zu bieten und besitzt viele Vorteile. Zudem ist die Bedienung denkbar einfach und komfortabel. Probieren Sie es aus!

9.9.11
Seite 14

9.10 Sicherheitsüberlegungen

Es wird viel über Computer-Sicherheit geschrieben. Was aber bedeutet Computer-Sicherheit? Ganz allgemein versteht man darunter die Einführung verschiedener Maßnahmen, die Ihre iSeries und deren Umgebung vor Sabotage, Spionage und alle Arten von zufälligen und weniger zufälligen Schäden bewahrt. Die Angst vor Maschinenausfall und Datenverlusten nutzen viele Hersteller und entwickeln geeignete Tools. Aber niemand – kein Auditor, kein Fremdanbieter – kann Ihnen sagen, welche Sicherheitsrichtlinien für Sie geeignet sind. Denn um entsprechende Maßnahmen zu ergreifen, müssen Sie zunächst einmal Ihre individuellen Risiken analysieren. Sie entscheiden, welche Systeme, welche Daten und welche Prozesse von Bedeutung für Ihr Unternehmen sind und daher in besonderem Maße geschützt werden sollten und welche Risiken Sie bereit sind zu akzeptieren. Erst dann sind Sie in der Lage, Ihre spezifischen Security-Richtlinien im Unternehmen zu implementieren. Auf einer iSeries können Sie u.a. Benutzerprofile, Objektberechtigungen, Objektsignierung, Auditjournale u.v.m. verwenden, um Ihr System zu schützen. Doch leider werden diese Bordmittel wenig oder gar nicht genutzt. In den folgenden Beiträgen soll daher die Bedeutung dieser Features für Ihre Sicherheitsstrategie erörtert werden.

Einige werden sich jetzt fragen, was soll das? Die iSeries war und ist eines der sichersten und zuverlässigsten Systeme am Markt, denn von Beginn an wurde bei der Entwicklung des Betriebssystems der Fokus auf integrierte Sicherheitsmechanismen gelegt. Das Betriebssystem i5/OS bietet eine integrierte Architektur kombiniert mit hoher Verfügbarkeit und einfach zu handhabenden Sicherheitsfeatures basierend auf der Mainframe-Technologie. Am wichtigsten ist hierbei sicherlich die Objekt-basierte Architektur des Servers. Nach wie vor ist es nicht möglich ein Datenobjekt in einen ausführbaren Code zu wandeln und umgekehrt. Warum dann aber die scheinbar nicht enden wollende Diskussion um das Thema Sicherheit?

Nun, im Gegensatz zu früher sind die iSeries-Server heute Bestandteil eines heterogenen Netzes und stehen nicht mehr isoliert. Noch vor einigen Jahren liefen die Applikationen ausschließlich auf der iSeries. Heute erfolgen die Zugriffe aus Web-Applikationen, über FTP-, ODBC- und JDBC-Schnittstellen. Die Zeiten haben sich geändert. Hat sich Ihre Sicherheitsstrategie auch entsprechend weiterentwickelt? Eine gute Strategie muss neben der eigentlichen Anwendungssicherheit insbesondere die Möglichkeiten des Betriebssystems und des Netzwerks nutzen, um die Verfügbarkeit des Servers und dessen Daten zu gewährleisten.

11. Ergänzung 06/2007

9.10
Seite 2

9.10.1 Verwendung von Benutzergruppen

Eine besondere Bedeutung in punkto Sicherheit haben die Benutzerprofile. Im Folgenden sollen aber nicht erneut die einzelnen Profilparameter detailliert besprochen werden. Dies ist bereits geschehen. Vielmehr geht es jetzt um den Einsatz und die Verwaltung von Benutzergruppen.

Gehen wir von folgendem Szenario aus: Mehrere Entwickler arbeiten in verschiedenen Projekten. Ohne den Einsatz von Gruppenprofilen könnte sehr schnell die folgende Situation auftreten: Der Programmierer A, nennen wir ihn „Mueller“, kompiliert ein Programm. Er wird Eigentümer des ausführbaren Programmobjekts.

```
Objekt . . . . . :   STRQUERY        Eigner . . . . . :   MUELLER
  Bibliothek . . . :     EPS002CR     Primärgruppe . . . :   *NONE
Objektart  . . . . :   *PGM          ASP-Einheit  . . . :   *SYSBAS

Aktuelle Berechtigungen ändern und Eingabetaste drücken.

  Objekt durch Berechtigungsliste geschützt . . . . . .   *NONE

                        Objekt-
Benutzer    Gruppe      berechtg.
*PUBLIC                 *CHANGE
MUELLER                 *ALL
```

Die Eignerberechtigungen

Der Objekteigner erhält stets alle Berechtigungen am Objekt, während alle anderen Personengruppen aufgrund der öffentlichen Berechtigungseinstellungen auf das Objekt zugreifen.

In unserem Beispiel bedeutet dies, dass jeder das Objekt nutzen aber nicht löschen darf. Will nun ein anderes Projektmitglied das Programmobjekt modifizieren, sendet das Betriebssystem folgende Fehlermeldung:

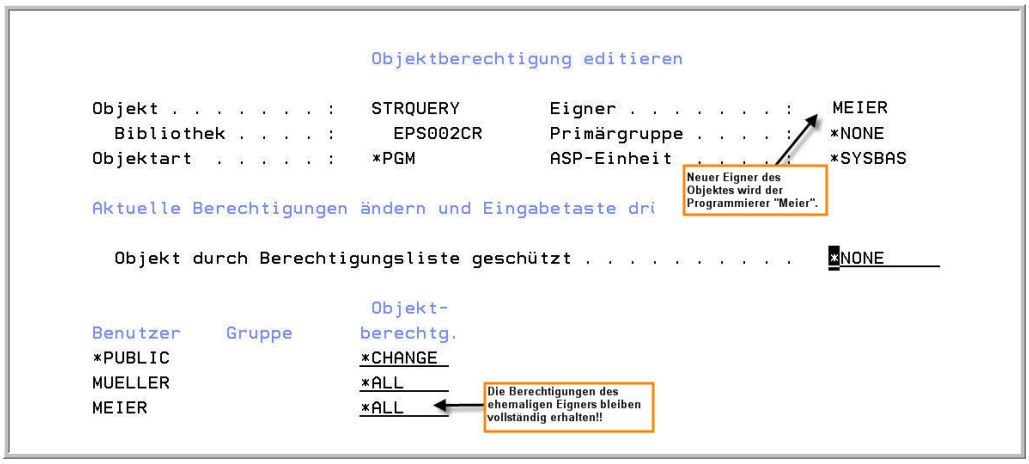
```
3>> CRTCLPGM PGM(EPS002CR/STRQUERY) SRCFILE(EPS002CR/QCLSRC)
    Nicht berechtigt für STRQUERY in Bibliothek EPS002CR Art *PGM.
    Programm STRQUERY nicht erstellt.
```

Unberechtigter Objektzugriff

Sie könnten selbstverständlich dem entsprechenden Programmierer die persönlichen Berechtigungen am Programmobjekt erteilen. Nur wer will für jedes Objekt und jeden Programmierer persönliche Berechtigungen verwalten?

Also lautet die Lösung häufig: *ALLOBJ-Berechtigung. Durch die Sonderberechtigung *ALLOBJ setzen Sie aber den Objektschutz des Betriebssystems außer Kraft. Genauso gut könnten Sie die Berechtigungsstufe von 30 auf 20 ändern. Sie müssen sich darüber im Klaren sein, dass Sie den Objektschutz für ALLE Objekte aufheben. Ihre Programmierer erhalten somit uneingeschränkten Zugriff auf jedes Objekt, auch auf alle Tabellen und die sich darin befindenden Daten. Ist das wirklich gewollt?

Und es passiert noch etwas:



Die Eignerberechtigungen

Anhand der Abbildung erkennen Sie, dass zwar der Eigentümer wechselt, nur bleiben die alten Eignerberechtigungen des Programmierers „Mueller“ erhalten. Er hat weiterhin vollen Zugriff auf das Objekt unabhängig davon, ob dieser Programmierer noch im Projekt arbeitet oder nicht. Stellen Sie sich vor, mehr als zwei Programmierer sind beteiligt und kompilieren die entsprechenden Programme. Sie haben keinen Überblick darüber, wer welche persönlichen Berechtigungen an den Objekten hat. Die Lösung für dieses Problem ist denkbar einfach:

Durch den Einsatz von Gruppenprofilen können Sie mit minimalem Verwaltungsaufwand den Zugriff auf die jeweiligen Objekte steuern. Gruppenprofile sind eine spezielle Ausprägung von Benutzerprofilen, d.h. Sie können mehrere Profile zu einer Gruppe zusammenfassen, um gemeinsame Berechtigungen für diese Personengruppe festzulegen. Gruppenprofile sind immer dann sinnvoll, wenn ein bestimmter Personenkreis, z. B. Ihre Programmierer identische Rechte und gemeinsamen Zugriff auf bestimmte Ressourcen benötigt.

Planen wir einfach mal ein Gruppenprofil für unsere Entwickler, die im Projekt „A07“ tätig sind. Zunächst müssen wir die Gruppe in Form eines Profils definieren.

```
                    Benutzerprofil erstellen (CRTUSRPRF)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .   GP_PJ_A07      Name
Benutzerkennwort . . . . . .  *NONE         Zeichenwert, *USRPRF, *NONE
Benutzerklasse . . . . . .    *PGMR         *USER, *SYSOPR, *PGMR...
Sonderberechtigung . . . . . .  *JOBCTL     *USRCLS, *NONE, *ALLOBJ...
            + für weitere Werte
```

Die Gruppe

Hierbei sollten Sie folgende Regeln beachten:

- Vereinbaren Sie Namenskonventionen für Ihre Gruppenprofile. Dadurch fällt es Ihnen später leichter, die Gruppen zu identifizieren. Ich verwende in meinem Beispiel die Projektbezeichnung „GP_PJ_A07“ als Gruppennamen, wobei das Prefix „GP_PJ“ anzeigt, dass es sich um ein Gruppenprofil für den Projektbereich handelt.
- Beachten Sie, dass eine Anmeldung unter dem Gruppennamen nie erforderlich ist und daher von vornherein unterbunden wird, indem das Kennwort auf den Wert *NONE gesetzt ist (PASSWORD is *NONE).
- Als letztes vergeben Sie die erforderlichen Sonderberechtigungen für die Gruppe. Die Gruppenmitglieder übernehmen die Berechtigungen der Gruppe, solange Sie keine persönlichen Berechtigungen erteilen.

In einem zweiten Schritt kann ich die Entwickler dem Projekt „A07“ zuordnen, indem ich Sie zu Membern der Gruppe „GP_PJ_A07“ mache.

```
Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > MEIER          Name
Benutzerkennwort . . . . . .  *SAME       Zeichenwert, *SAME, *NONE
Kennwort auf abgelaufen setzen  *NO       *SAME, *NO, *YES
Status . . . . . .  *ENABLED              *SAME, *ENABLED, *DISABLED
Benutzerklasse . . . . . .  *PGMR         *SAME, *USER, *SYSOPR...

                Zusätzliche Parameter
Sonderberechtigung . . . . . .  *NONE      <- Die Member erhalten keine persönlichen Sonderberechtigungen.
     + für weitere Werte
Gruppenprofil . . . . . .  GP_PJ_A07      <- Der Parameter GRPPRF bestimmt die erste Gruppe.
Eigner . . . . . .  *GRPPRF               <- Eigner zukünftiger Objekte wird die Gruppe.
```

Die Gruppenmember

Das erste Gruppenprofil wird über den Parameter GRPPRF im Benutzerprofil spezifiziert. Weitere Gruppen benennen Sie im Parameter SUPGRPPRF. Ein Benutzer kann insgesamt Mitglied in 16 unterschiedlichen Gruppen sein. Planen Sie die Gruppen und die Gruppenzugehörigkeiten aber vorsichtig. Die erste Gruppe (Parameter GRPPRF) sollte stets die Gruppe sein, deren Objekte der User am häufigsten verwendet. Wenn Sie dennoch mehrere Gruppen für einen User einsetzen müssen, beachten Sie das Verfahren, das die iSeries verwendet, um die Zugriffsberechtigung für ein Objekt zu prüfen.

Außerdem übertrage ich die Eignerschaft neuer Objekte an die Gruppe „GP_PJ_A07“. Dies kann ich mit dem Parameter OWNER festlegen. Wenn die Gruppe Eigentümer wird (OWNER is *GRPPRF), erhalten Gruppenmitglieder, die Objekte erzeugen, keine spezifischen Berechtigungen am Objekt. Ihre Zugriffsberechtigung wird nur durch die Gruppenzugehörigkeit bestimmt.

```
                        Objektberechtigung editieren

Objekt . . . . . :   STRQUERY        Eigner . . . . . :   GP_PJ_A07
  Bibliothek . . . :     EPS002CR    Primärgruppe . . . :   *NONE
Objektart  . . . . :   *PGM          ASP-Einheit  . . . :   *SYSBAS

Aktuelle Berechtigungen ändern und Eingabetaste drücken.

  Objekt durch Berechtigungsliste geschützt . . . . . .   *NONE

                        Objekt-
Benutzer    Gruppe      berechtg.
*PUBLIC                 *CHANGE
GP_PJ_A07               *ALL
```

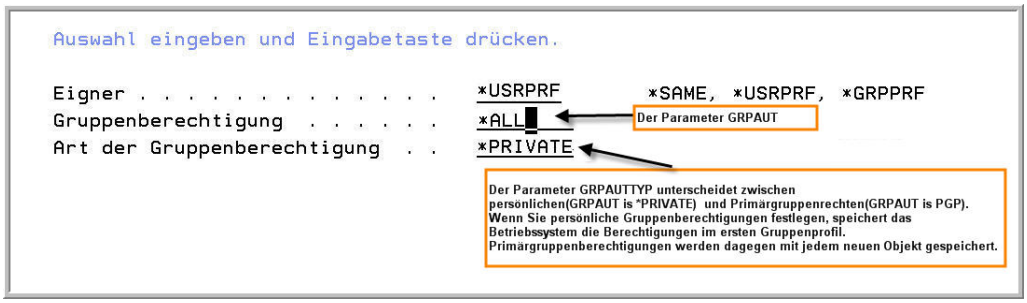
Die Eignerberechtigung

In Entwicklungs- oder Testumgebungen kann es sinnvoll sein, die Eignerschaft an die Gruppe zu übertragen (OWNER is *GRPPRF) wie in unserem Beispiel. Bedenken Sie aber, dass sich bestehende Objekteignerschaften nicht automatisch anpassen. Die Eignerschaft bestehender Objekte müssen Sie manuell mit dem Befehl CHGOBJOWN verändern.

```
                    Objekteigner ändern (CHGOBJOWN)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . .   strquery    Name
  Bibliothek . . . .   eps002cr    Name, *LIBL, *CURLIB
Objektart  . . . . .   *pgm       *ALRTBL, *AUTL, *BNDDIR...
ASP-Einheit  . . . .   *          Name, *, *SYSBAS
Neuer Eigner . . . .   GP_PJ_A07  Neuer Eigentümer des Objektes wird die Gruppe
                                  "GP_PJ_A07"
Aktuelle Eignerberechtigung  . .   *REVOKE   Aktuelle Eignerberechtigungen werden entzogen.
```

Bestehende Objekteignerschaften an die Gruppe übertragen

Falls die Gruppe nicht Eigentümer der Projektobjekte werden soll, gibt es eine andere Möglichkeit, die Gruppe zu berechtigen.



Persönliche und Primärgruppenrechte

In diesem Beispiel behält der Entwickler zwar die Objekteignerschaft, die Gruppenberechtigung wird aber zusätzlich durch die Parameter „GRPAUT“ und „GRPAUTTYP“ bestimmt, d.h. jedes Gruppenmitglied kann uneingeschränkt aufgrund seiner Gruppenzugehörigkeit und der Gruppenberechtigung *ALL auf das Programm zugreifen. Selbst wenn der Eigner des Objektes einer anderen Gruppe angehört, bleibt die Gruppenberechtigung bestehen und jeder, der zum Zeitpunkt des Zugriffs Mitglied der Gruppe ist, darf das Programmobjekt uneingeschränkt nutzen.

Und hier zeigt sich auch der Vorteil von Gruppenprofilen: Wenn neue Projektmitarbeiter hinzukommen, Mitarbeiter das Unternehmen verlassen oder die Projektzugehörigkeit wechselt, müssen Sie keine persönlichen Objektberechtigungen mehr erteilen, sondern nur die Gruppenzugehörigkeit durch Austausch der Gruppenprofilnamen ändern. Zusätzliche Sonderberechtigungen erteilen oder entziehen Sie der Gruppe anstatt einzelnen Benutzern. Dieses Vorgehen spart Zeit und ist sehr viel übersichtlicher als die Steuerung am einzelnen Profil.

Doch leider bietet die 5250-Oberfläche keine geeigneten Befehle, um schnell und einfach Gruppen und deren Mitglieder zu verwalten. Dieses Problem behebt die grafische Oberfläche des iSeries Navigator. Diese grafische Benutzeroberfläche ermöglicht einen schnellen Überblick über bestehende Gruppen und erlaubt es, mit einfachen Mitteln die Gruppenstruktur zu verändern. Leider ist es bislang nicht möglich mit iSeries Navigator Gruppen zu erstellen, die die Objekteignerschaften übernehmen. Der iSeries Navigator arbeitet grundsätzlich mit den Parametern „GRPAUT“ und „GRPAUTTYP“, um die Gruppenberechtigung festzulegen. Die Verwaltung solcher Gruppen ist allerdings problemlos möglich.

Trotz dieser kleinen Einschränkung ist der Einsatz der grafischen Oberfläche für die Benutzerverwaltung sinnvoll und selbst wenn die Planung der Gruppen und die Einrichtung zunächst etwas Zeit kostet, werden Sie schnell feststellen: Es lohnt sich!

9.10.1
Seite 6

9.10.2 Ressourcenschutz durch Berechtigungslisten

Der Zugriff auf die iSeries-Daten wird in der Regel mit drei Methoden realisiert:

Menüsicherheit, Bibliothekssicherheit und Objektschutz. Die Menüsicherheit beschränkt den Anwender auf bestimmte Menüpunkte und ist im Rahmen einer Sicherheitsstrategie sicherlich auch weiterhin sinnvoll, um die Sicherheit der iSeries-Anwendungen zu gewährleisten. Doch Anwendungssicherheit allein ist heute nicht mehr ausreichend, denn DDM, TCP/IP, ODBC, JDBC und IFS bieten neue Wege für den Zugang zu den iSeries-Daten. Natürlich können Sie diese neuen Zugriffsmethoden blockieren, um den Zugriff auf Ihre Daten zu verhindern. Sie können die „Türen" zur iSeries verschließen, so dass ein widerrechtlicher Zutritt unmöglich ist. Durch Exit-Programme könnten Sie z.B. versuchen, PC-Anfragen auf die iSeries-Daten zu kontrollieren. Der Nachteil dieser Strategie?

Für jede Zugriffsart müssen verschiedene Lösungen gefunden werden und was passiert, wenn Sie vergessen, eine der Türen abzuschließen? Dann ist der Zutritt doch möglich! Haben Sie alle Türen abgeschlossen? Und was ist, wenn eine der Türen sich gar nicht verschließen lässt?

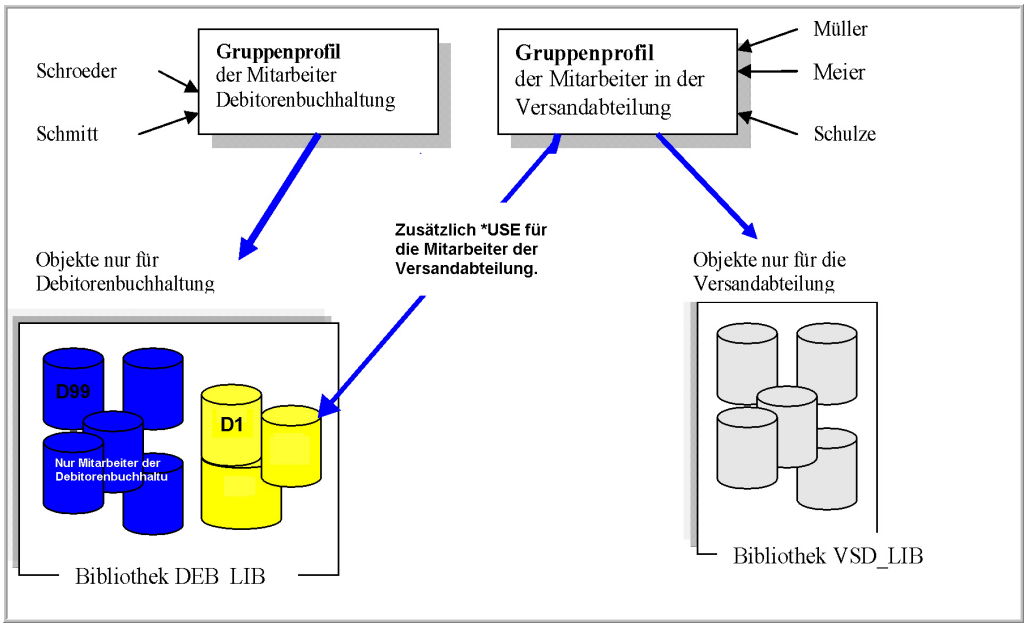
Besser ist es auf der iSeries selbst, die Ressourcen zu schützen. Ressourcensicherheit beinhaltet Bibliotheks- und Objektschutz gleichermaßen. Sie bestimmen über das Datenobjekt, wer in welchem Umfang mit den Daten arbeiten darf.

Das Problem dieser Sicherheitsstrategie ist die ständige Pflege der Zugriffsberechtigungen und der damit verbundene Verwaltungsaufwand. Jedes Mal, wenn ein neues Objekt erstellt wird, muss seine Berechtigung für jeden Benutzer korrekt gesetzt werden. Gleichzeitig müssen Sie darauf achten, dass die Mechanismen nicht zu streng sind, um nicht die Mitarbeiter bei der Arbeit zu behindern.

Sie können die Pflege der Berechtigungszuweisungen vereinfachen, wenn Sie die Berechtigungen organisieren, indem Sie die Objekte und die Benutzer zunächst klassifizieren. Gruppenprofile in Kombination mit Berechtigungslisten sind hervorragend dazu geeignet.

Stellen Sie sich folgendes Szenario vor: Jeder Mitarbeiter der Debitorenbuchhaltung gehört zum Gruppenprofil „GRPDEB". Alle Mitarbeiter der Versandabteilung gehören in die Gruppe „GRPVSD" usw. Aber was geschieht mit der Kundendatei? Beide Gruppen benötigen den Zugriff! Mitarbeiter der Debitorenabteilung dürfen die Kundendaten verändern, während die Versandmit-

arbeiter lediglich die Daten lesen. Ich muss also die Datenobjekte klassifizieren. Das hätte zur Folge, dass die Dateien der Debitorenbuchhaltung, die reinen Versanddateien und die gemeinsam genutzten Dateien je eine Datenklasse darstellen.



Die Ausgangssituation

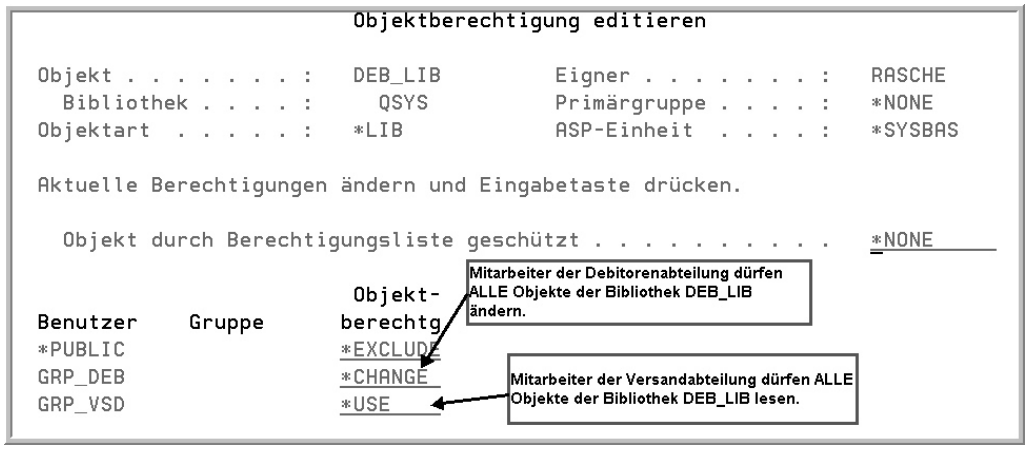
Jetzt kann ich sehr einfach bestimmen, welche Berechtigungsgruppe auf welche Datenklasse zugreifen darf und welche Operationen erlaubt sind. Wird ein neuer Mitarbeiter in der Versandabteilung eingestellt, muss ich den Benutzer lediglich der Benutzergruppe „Versand“ zuordnen und neue Datenobjekte ordne ich der entsprechenden Objektklasse zu.

Nun wissen Sie vielleicht, dass es die eben erfundenen Datenklassen auf einem iSeries-Server nicht gibt. Allerdings können Sie Objekte kategorisieren, indem Sie unterschiedliche Bibliotheken verwenden. Wenn dies nicht ausreichend oder nicht möglich ist, wie in unserem Beispiel, dann können Sie Objektberechtigungsklassen durch Berechtigungslisten auf Objektebene implementieren. Bevor Sie allerdings beginnen mit Berechtigungslisten zu arbeiten, sind ein paar Vorüberlegungen notwendig:

- Welche Objekte gehören zu welcher Berechtigungsliste? Objekte können nur einer Berechtigungsliste zugeordnet werden. Daher ist es notwendig, zunächst die Datenobjekte sorgfältig zu klassifizieren!
- Wie viele Berechtigungslisten sind erforderlich? Hier gibt es keine globale Antwort. Wenn Sie eine höhere Flexibilität benötigen, ist es empfehlenswert, mehrere Berechtigungslisten zu erstellen, mit denen Sie unterschiedliche Berechtigungsebenen implementieren können. Um die Datenpflege zu erleichtern, sollten Sie hingegen nicht zu viele Berechtigungslisten nutzen.

- Welche Namen sollen die Listen erhalten? Anders als die meisten iSeries-Objekte können die Berechtigungslisten nur in der Bibliothek QSYS gespeichert werden und daher müssen die Namen eindeutig und aussagekräftig gewählt werden. Sie sollten vielleicht die Namen mit einer entsprechenden Buchstabenkombination kennzeichnen, so kann problemlos festgestellt werden, zu welcher Anwendung oder „Objektkategorie" die Liste gehört. Ich verwende für mein Beispiel als Listennamen „L_VSD_DEB" für die Objekte beider Gruppen und „L_DEB" als Listennamen für Objekte der Debitorenbuchhaltung.

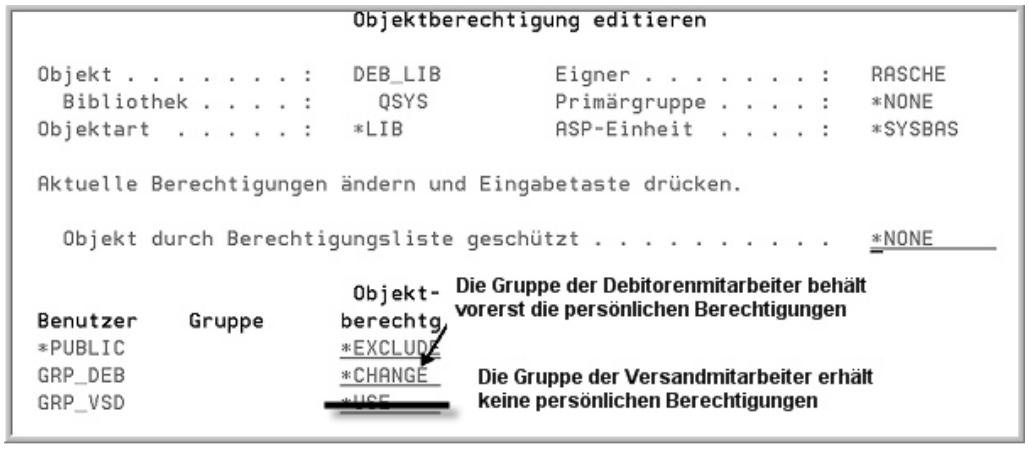
Zunächst erstellen wir die persönlichen Berechtigungen für die Bibliotheken:



Die persönlichen Berechtigungen an der Bibliothek DEB_LIB

Jetzt dürfte aber jedes Mitglied der Gruppe „GRP_VSD" ALLE Objekte in der Bibliothek „DEB_LIB" nutzen.

Besser ist es, wir arbeiten direkt mit einer Berechtigungsliste. Ich entferne also zunächst einmal wieder die persönliche Berechtigung für die Versandmitarbeiter.



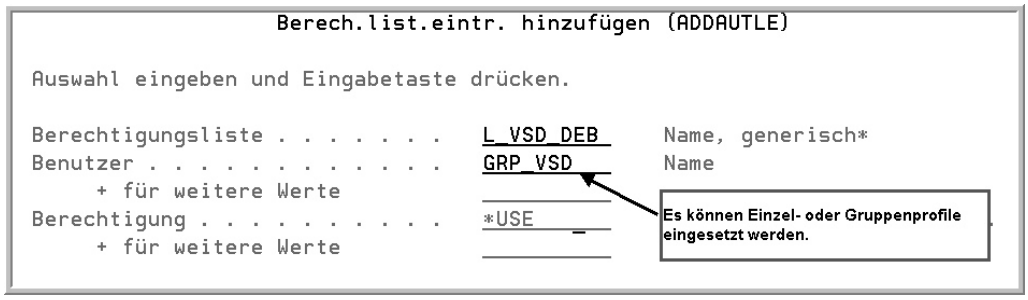
Persönliche Berechtigungen für die Versandgruppe entfernen

Stattdessen erstelle ich eine Berechtigungsliste, um die Versandmitarbeiter an den Objekten in der Bibliothek „DEB_LIB“ zu berechtigen:

```
                    Berechtigungsliste erstellen (CRTAUTL)

Auswahl eingeben und Eingabetaste drücken.

Berechtigungsliste . . . . . .   L_VSD_DEB     Name
Text 'Beschreibung'  . . . . . .   Berechtigungsliste Versand für Debitorendate
n_____
```

Die Berechtigungsliste L_VSD_DEB erstellen

In einem zweiten Schritt hinterlege ich in der Liste das Gruppenprofil „GRP_VSD“ mit der Berechtigung *USE.



Berechtigungslisteneintrag für die Gruppe der Versandmitarbeiter hinzufügen

Idealerweise verwenden Sie hier bereits Gruppenprofile, aber auch individuelle Profile sind möglich. Wenn unser Benutzer „Müller“ Mitglied der Gruppe „GRP_VSD“ ist, erhält er die *USE-Berechtigung für alle Objekte, die durch die Liste „DEB_VSD“ geschützt sind.

Soll der Benutzer „Müller“ dagegen *CHANGE-Rechte erhalten, können Sie das Profil als Individualprofil mit der Berechtigung *CHANGE in die Berechtigungsliste aufnehmen. Der Mitarbeiter „Müller“ erhielte *CHANGE-Rechte, während alle anderen Gruppenmitglieder nur *USE-Rechte besitzen.

Im letzten Schritt ordnen wir jetzt die Objekte zu, die durch die Liste geschützt werden sollen.

```
                    Objektberechtigung erteilen (GRTOBJAUT)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . . . . . . . . . > D1          Name, generisch*, *ALL
  Bibliothek . . . . . . . . . . >   DEB_LIB   Name, *LIBL, *CURLIB, *ALL...
Objektart  . . . . . . . . . . . > *FILE       *ALL, *ALRTBL, *BNDDIR...
ASP-Einheit  . . . . . . . . . .   *           Name, *, *SYSBAS
Benutzer . . . . . . . . . . . .   _           Name, *PUBLIC
     + für weitere Werte           _
Berechtigung . . . . . . . . . .   *CHANGE     *CHANGE, *ALL, *USE...
     + für weitere Werte           _
Berechtigungsliste . . . . . . . > L_VSD_DEB   Name, *NONE
Bezugsobjekt . . . . . . . . . .   _           Name
  Bibliothek . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
Bezugsobjektart  . . . . . . . .   *OBJTYPE    *OBJTYPE, *ALRTBL, *BNDDIR...
Referenz-ASP-Einheit . . . . . .   *           Name, *, *SYSBAS
Berechtigung ersetzen  . . . . . > *no         *NO, *YES
```

Objekte schützen

Für unser Beispiel müsste ich den Befehl für die Bibliothek „DEB_LIB“ und alle betroffenen Dateien wiederholen. Einfacher wäre es, wenn ich die Dateien generisch ansprechen könnte.

Sicherlich haben Sie bemerkt, dass ich auf die einzelnen Befehlsparameter nicht sehr detailliert eingehe und auch nicht den iSeries Navigator verwende. Beides wurde bereits ausführlich getan. Jetzt soll es lediglich um den Einsatz und die Planung der Berechtigungslisten gehen, um eine in sich geschlossene Sicherheitsstrategie zu implementieren.

Es ist also an der Zeit zu testen, ob alles so funktioniert wie wir es uns vorstellen. Ich melde mich dafür mit einem Versandprofil an und lasse mir den Inhalt der Datei D1 anzeigen:

```
                    Physische Teildatei anzeigen
Datei  . . . . . :   D1                 Bibliothek . . . :   DEB_LIB
Teildatei  . . . :   D1


*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...

  (Angegebene Teildatei enthält keine Datensätze)
```

Die Daten lesen

Kein Problem! Versuche ich dagegen den Inhalt der Datei zu löschen, erhalte ich die folgende Fehlermeldung:

```
Nachricht . . . :   Keine Berechtigung zum Löschen, Initialisieren oder
  Kopieren von Teildatei *N.
Ursache  . . . . :  Es liegt keine Berechtigung vor, Teildatei *N in Datei D1
  in der Bibliothek DEB_LIB zu löschen, zu initialisieren oder zu kopieren.
Fehlerbeseitigung:  Die erforderliche Berechtigung beim
  Sicherheitsbeauftragten oder beim Eigner von Datei D1 in der Bibliothek
  DEB_LIB einholen. Anschließend die Anforderung wiederholen.
```

Keine Berechtigung zum Löschen oder Verändern der Daten

Dies ist so ja auch gewollt. Alles scheint prima zu funktionieren. Doch was passiert, wenn wir auf eine Datei zugreifen, für die der Versandmitarbeiter keine Berechtigung erhalten soll? Löschen oder Ändern der Daten ist nicht möglich, aber wir erhalten problemlos lesenden Zugriff:

```
                      Physische Teildatei anzeigen
Datei  . . . . . :   D99                 Bibliothek . . . :   DEB_LIB
Teildatei  . . . :   D99

                                  Unser Berechtigungskonzept erlaubt den lesenden
*...+....1....+....2....+....3    Zugriff auf alle Dateien in der Bibliothek DEB_LIB.  .+....7....+...

  (Angegebene Teildatei enthält keine Datensätze)
```

Unser Berechtigungskonzept ist fehlerhaft

Was ist passiert? Nun, wir haben zwar keine Berechtigungen über die Berechtigungsliste erteilt, aber die Versandmitarbeiter gehören natürlich auch zur Gruppe *PUBLIC und die Öffentlichkeit hat derzeit an den Objekten der Bibliothek DEB_LIB ein *CHANGE-Recht:

```
                         Objektberechtigung editieren

Objekt . . . . . :   D99             Eigner . . . . . :   RASCHE
  Bibliothek . . . :     DEB_LIB     Primärgruppe . . . :   *NONE
Objektart  . . . . :   *FILE         ASP-Einheit  . . . :   *SYSBAS

Aktuelle Berechtigungen ändern und Eingabetaste drücken.

  Objekt durch Berechtigungsliste geschützt . . . . . .   *NONE

                      Objekt-                  Die öffentliche Berechtigung
Benutzer     Gruppe   berechtg.                erlaubt den Zugriff auf das Objekt
*PUBLIC               *CHANGE
RASCHE                *ALL
```

Die Objektberechtigung für das Objekt DEB_LIB/D99

Normalerweise interessiert diese Berechtigung nicht, da die Öffentlichkeit die Bibliothek nicht nutzen darf, aber in unserem Fall gewähren wir den Zutritt zur Bibliothek für die Versandmitarbeiter, die dann natürlich auf die Objekte der Bibliothek über genau diese öffentlichen Rechte zugreifen. Wir müssen also immer dann, wenn wir mit Objektrechten innerhalb einer Bibli-

othek arbeiten auch die Öffentlichkeitsrechte aller Objekte innerhalb der Bibliothek auf *EXCLUDE setzen:

```
GRTOBJAUT  OBJ(DEB_LIB/*ALL)  OBJTYPE(*ALL)  *USER(*PUBLIC)
AUT(*EXCLUDE)
```

Jetzt sind alle *PUBLIC-Rechte korrekt gesetzt und die Versandmitarbeiter haben keine Möglichkeit mehr auf die Datei D99 zuzugreifen.

```
Nachricht . . . :   Keine Berechtigung für Datei D99 in Bibliothek DEB_LIB.
Ursache  . . . . :  Es besteht keine Berechtigung, die Datei D99 in Bibliothek
  DEB_LIB zu benutzen.
Fehlerbeseitigung:  Die Benutzungsberechtigung vom Sicherheitsbeauftragten
  oder Dateieigner besorgen. Die Anforderung anschließend wiederholen.
```

Keine Berechtigung für Datei D99 in DEB_LIB

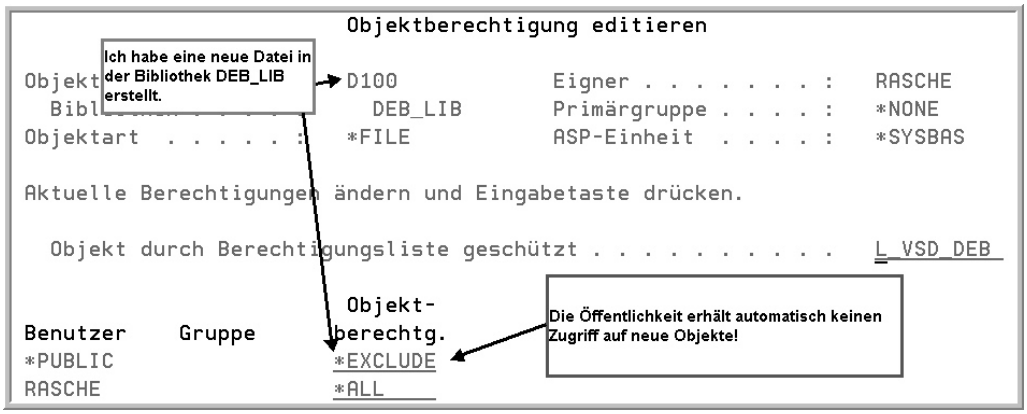
Ein Problem bleibt allerdings: Sobald Sie neue Objekte in der Bibliothek erstellen, müssten die *PUBLIC-Rechte immer manuell auf *EXCLUDE gesetzt werden, da das Betriebssystem in vielen Fällen der Öffentlichkeit zunächst das Recht einräumt, Objekte zu ändern. Hier könnten sich schnell Fehler einschleichen.

Es ist möglich, die Berechtigung *PUBLIC *EXCLUDE automatisch zu vergeben. Hierfür müssen Sie nur die Attribute der Bibliothek DEB_LIB folgendermaßen ändern:

```
                        Bibliothek ändern (CHGLIB)

Auswahl eingeben und Eingabetaste drücken.

Bibliothek . . . . . > DEB_LIB      Name, *CURLIB
Bibliotheksart . . . . . > *PROD    *SAME, *PROD, *TEST
Text 'Beschreibung'  . . . . .  *BLANK
_____
                                    Neue Objekte dieser Bibliothek erhalten
                                    automatisch die Berechtigung *PUBLIC
                Zusätzliche Parameter *EXCLUDE

Berechtigung für neue Objekte  . > *EXCLUDE   Name, *SAME, *SYSVAL...
Objektprotokollierung  . . . . .  *SYSVAL     *SAME, *SYSVAL, *NONE...
```

Bibliotheksattribute ändern

Die Öffentlichkeitsrechte neuer Objekte können durch den Parameter CRTAUT gesteuert werden. Für mein Beispiel ist das genau die richtige Lösung, denn so muss ich auf die *PUBLIC-Berechtigungen der Objekte nicht mehr achten.

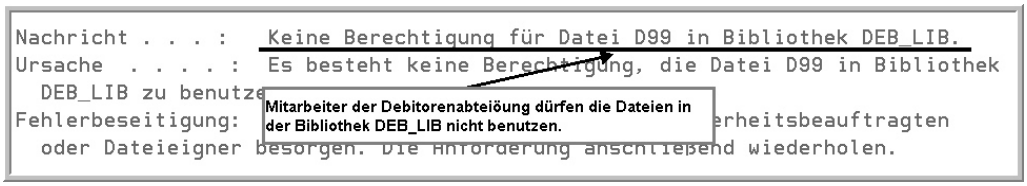


Die öffentliche Berechtigung für neue Objekte

ACHTUNG:

Der Parameter AUT der jeweiligen Bibliothek wird nur beachtet, wenn Objekte direkt erstellt werden, d.h. Objekte, die Sie z.B. mit dem CPYF-Befehl oder mit dem Befehl CRTDUPOBJ erstellen, ignorieren den AUT-Parameter der jeweiligen Bibliothek. Sie leiten Ihre Rechte vom kopierten Objekt ab.

Als letztes bleibt zu prüfen, ob die Mitarbeiter der Debitorenabteilung die Zugriffsrechte korrekt erhalten haben und hier stehen wir auch schon wieder vor einem erneuten Problem: Keiner der Debitorenmitarbeiter darf auf Dateien in der Bibliothek DEB_LIB zugreifen. Das kann nicht gewollt sein!!



Mitarbeiter der Debitorenbuchhaltung haben keinen Zugriff auf die Daten

Unsere Strategie funktioniert nur, wenn wir eine zweite Berechtigungsliste einsetzen oder persönliche Berechtigung für die Objekte der Bibliothek DEB_LIB erteilen. Ich entscheide mich für die Berechtigungsliste:

```
CRTAUTL  AUTL(L_DEB)
```

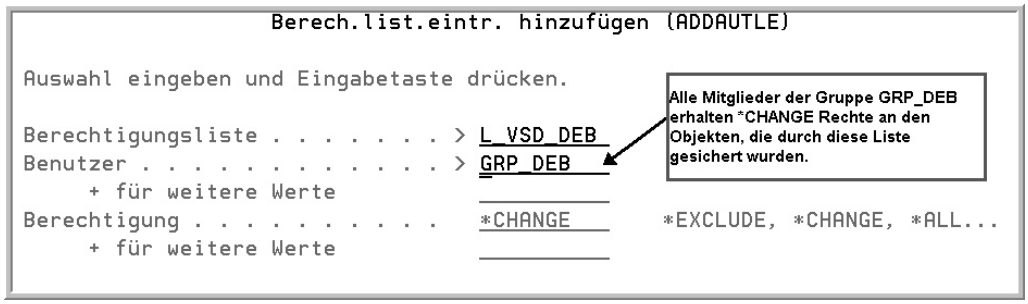
Dieser Liste ordne ich die Mitarbeiter der Debitorenbuchhaltung zu.

```
ADDAUTLE  AUTL(L_DEB)  USER(GRP_DEB)
```

In einem weiteren Schritt verwende ich die Liste L_DEB für alle Objekte der Bibliothek DEB_LIB die bislang nicht durch eine Berechtigungsliste geschützt sind.

Nun dürfen wir nur nicht die Objekte vergessen, die bereits durch die Liste L_VSD_DEB geschützt sind. Objekte können generell nur durch eine einzige Berechtigungsliste geschützt werden. Aber auch hier ist die Lösung einfach: Wir nehmen die Debitorenmitarbeiter in die Liste L_VSD_DEB auf und erteilen *CHANGE-Rechte. Es ist durchaus möglich, über eine Liste mehrere Persongruppen mit unterschiedlichen Zugriffsrechten zu verwalten.

Um den Mitarbeitern Zugriff auf die Objekte zu gewähren, die bereits durch die Berechtigungsliste L_VSD_DEB geschützt sind, ist eine Anpassung der Objekte selbst nicht mehr nötig. Die Zuordnung der Mitarbeiter zur Liste ist ausreichend.



Debitorenmitarbeiter berechtigen

Falls neue Mitarbeiter für die Debitorenabteilung eingestellt werden, ist es sogar ausreichend, den neuen Mitarbeiter nur in die Gruppe GRP_DEB aufzunehmen. Scheidet ein Mitarbeiter aus, entfernen Sie ihn aus der Gruppe. Mit neuen Objekten verfahren Sie ähnlich: Neue Objekte schützen Sie entweder durch die eine oder andere Berechtigungsliste, mehr Arbeit ist nicht erforderlich. Und genau hier ist auch der entscheidende Vorteil zu sehen:

- Mit wenigen Befehlen können Sie neue Benutzer oder neue Objekte hinzufügen und von Anfang an ist dafür gesorgt, dass die richtige Berechtigung zugewiesen wird. Indem Sie Benutzer in die Listen aufnehmen oder von der Liste entfernen, gewähren bzw. entziehen Sie die entsprechenden Objektberechtigungen für alle Objekte, die die Berechtigungsliste nutzen.
- Wenn Sie ein Benutzerprofil löschen, wird das Profil automatisch aus allen Berechtigungslisten entfernt.
- Sie können die Zugriffsberechtigungen über die Berechtigungsliste jederzeit ändern – auch während sich die betroffenen Objekte im Zugriff befinden. Sollen die Mitarbeiter der Debitorenabteilung z.B. *ALL-Rechte an den Dateiobjekten erhalten, müssen Sie nur die Berechtigung in den Listen abändern, und die veränderten Berechtigungen sind sofort wirksam.

12. Ergänzung 09/2007

- Hinzu kommt, dass die Verbindung zwischen dem Objekt und der Liste automatisch wiederhergestellt wird, wenn Sie Objekte wiederherstellen, die über eine Berechtigungsliste geschützt sind, d.h. Sie müssen die Objektberechtigungen nicht neu zuweisen.

Sie sehen, auch wenn Ihnen im ersten Moment der Einsatz der Berechtigungslisten kompliziert erscheint, lohnt sich der Aufwand. Die anfängliche Investition wird sich später auszahlen! Wichtig ist eine sorgfältige Planung:

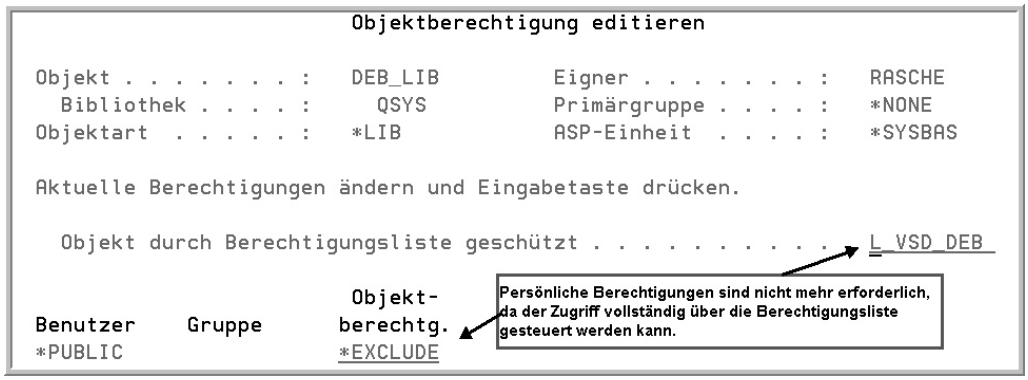
Schauen Sie sich hierfür noch einmal die Ausgangssituation an. Anfänglich haben wir die Objekte in drei Gruppen unterteilt, die sich in zwei unterschiedlichen Bibliotheken befanden. Wir haben die Objekte klassifiziert! Wenn Sie zwei Objektklassen innerhalb einer Bibliothek erhalten, benötigen Sie eine entsprechende Anzahl Berechtigungslisten.

Abschließend noch ein paar Bemerkungen, denn falsch platzierte Berechtigungslisten können auch unnötigen System-Overhead produzieren:

Gruppieren Sie immer zunächst die Objekte in Bibliotheken und schränken Sie – wenn möglich – nur den Zugriff auf die Bibliothek ein. Den Zugriff auf die Objekte innerhalb der Bibliothek steuern Sie über die *PUBLIC-Berechtigungen. Diese Technik wird als Bibliothekssicherheit bezeichnet. Sie positionieren also nur eine Wache an der „Haustür“ und erlauben innerhalb des „Hauses“ den Zugang zu allen „Räumen“.

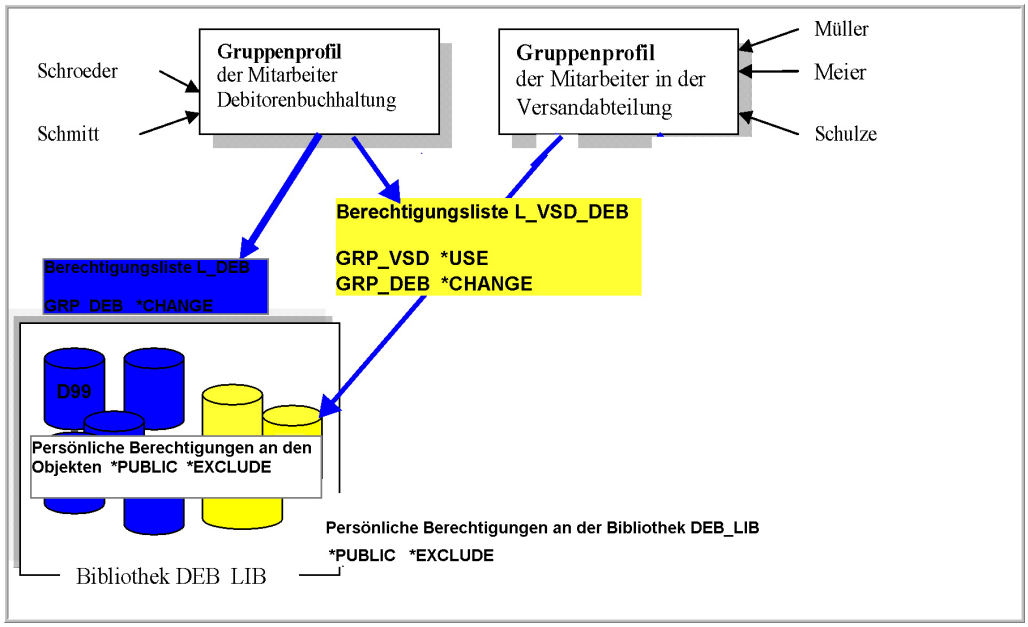
Nur wenn die Bibliothekssicherheit nicht ausreichend ist, da verschiedene Personengruppen mit unterschiedlichen Berechtigungen auf die Objekte zugreifen, setzen Sie Berechtigungslisten oder persönliche Berechtigungen ein. Um bei unserem Beispiel mit dem Haus zu bleiben: Sie gestatten den Zutritt an der „Haustür“, unterbinden aber den Zugang zu einzelnen „Räumen“. Vermeiden Sie hierbei aber Überschneidungen, d.h. gewähren Sie Ihren Mitarbeitern nicht den Zugriff über Einzelberechtigungen und gleichzeitig über eine Berechtigungsliste. Die Prüfung einer Berechtigungsliste bei gleichzeitiger persönlicher Berechtigung führt zu unnötigem System-Overhead. Es ist als ob Sie eine Wache an der „Tür“ positionieren, die sowohl den Mitarbeiterausweis (=persönliche Berechtigung) als auch eine Kontrollliste (=Berechtigungsliste) prüft. Fehlt dagegen die persönliche Berechtigung, muss der Benutzer nur anhand der „Kontrollliste“ identifiziert werden. Dies kann den Prozess beschleunigen. Auch mein kleines Beispiel hat bereits solch eine Überschneidung:

Die Mitarbeiter der Debitorenabteilung werden für die Bibliothek DEB_LIB sowohl über persönliche Berechtigungen als auch durch die Berechtigungsliste L_VSD_DEB berechtigt. Dies ist unnötig, wir können die persönlichen Berechtigungen entfernen ohne unser Berechtigungskonzept zu gefährden.



Die Berechtigungen für die Bibliothek DEB_LIB

Jetzt ist unser Berechtigungskonzept fertig und kann folgendermaßen dargestellt werden:



Das fertige Konzept

9.10.2
Seite 12

9.10.3 Berechtigungsübernahmen

Kennen Sie die folgenden Situationen? Ihre Vertriebsmitarbeiter sollen im Rahmen der Anwendung Kundendaten pflegen. Dazu gehören natürlich auch Adressänderungen. Die gleichen Mitarbeiter dürfen die Kundeninformationen aber nur lesen, wenn sie SQL oder andere Abfragetools verwenden.

Eine Mitarbeiterin der Lohn- und Gehaltsabteilung muss im Rahmen der Applikation auf die Lohn- und Gehaltsdaten zugreifen. Gleichzeitig wollen Sie dieser Mitarbeiterin aber auch Query zur Verfügung stellen, ohne den Zugriff auf einige Lohn- und Gehaltstabellen zu erlauben.

Die genannten Probleme tauchen auf, weil das Betriebssystem i5/OS es nicht zulässt, dass ein Benutzer in unterschiedlichen Situationen unterschiedliche Objektberechtigungen für ein Objekt besitzt. Diese Einschränkung lässt sich mit Berechtigungsübernahmen umgehen. Bei einer Berechtigungsübernahme erhält der Benutzer während der Programmausführung – also temporär – zusätzlich die Berechtigungen einer anderen Person oder besser gesagt eines anderen Benutzerprofils. Berechtigungsübernahmen sind hilfreich aber gleichzeitig mit Vorsicht einzusetzen. Das nachfolgende Kapitel soll daher nicht nur die Funktionsweise und Vorteile sondern auch die Risiken von Berechtigungsübernahmen verdeutlichen.

12. Ergänzung 09/2007

9.10.3
Seite 2

Berechtigungsübernahmen – wie funktioniert das?
Programme (*PGM), Serviceprogramme (*SRVPGM), SQL-Packages (*SQLPKG) und Java-Programme können die Rechte des Programmeigners adoptieren. Das ausführbare Objekt erbt somit zur Ausführungszeit die Objekt- und Sonderberechtigungen (*JOBCTL, *ALLOBJ, usw.) des Eigentümers. Es ist sehr einfach einem Programm die Berechtigungen zu übertragen.

```
                    RPG/400-Programm erstellen (CRTRPGPGM)

Auswahl eingeben und Eingabetaste drücken.

Umsetzungsauswahlmög. eingeben     *NONE          *NONE, *DATETIME, *VARCHAR...
     + für weitere Werte           _____
Sortierfolge . . . . . .           *HEX           Name, *HEX, *JOB, *JOBRUN...
  Bibliothek . . . . . .             _____        Name, *LIBL, *CURLIB
Sprachen-ID  . . . . . .           *JOBRUN        *JOB, *JOBRUN...
SAA-Markierung . . . . . .         *NOFLAG        *NOFLAG, *FLAG
Druckdatei . . . . . .             QSYSPRT        Name
  Bibliothek . . . . . .             *LIBL        Name, *LIBL, *CURLIB
Programm ersetzen  . . . . .       *YES           *YES, *NO
Ziel-Release . . . . . .           *CURRENT       *CURRENT, *PRV, V5R2M0, ...
Benutzerprofil . . . . . .         *USER          *USER, *OWNER
Berechtigung . . . . . .           *LIBCRTAUT     Name, *LIBCRTAUT, *ALL...
Phasen-Trace . . . . . .           *NO            *NO, *YES
Textzwischenspeicherauszug . . .   *NONE
```

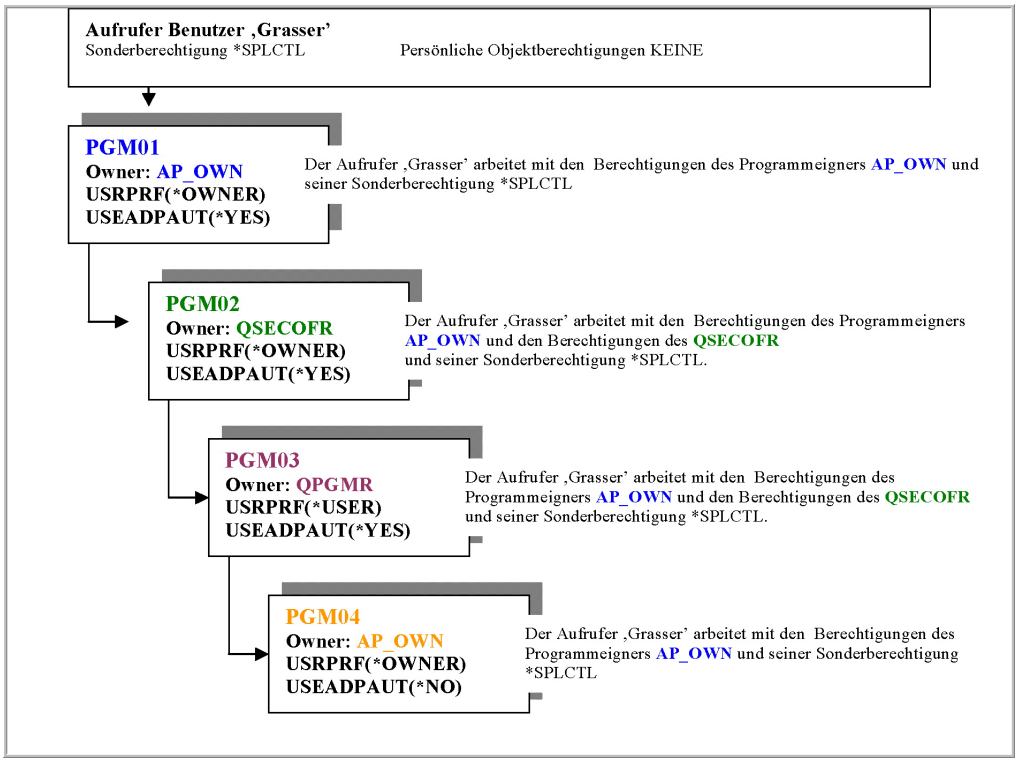
Der Parameter USRPRF im Befehl CRTxxxPGM

Jeder CRTxxxPGM-Befehl enthält den Parameter „Benutzerprofil“ (USRPRF). Der Standardwert USRPRF (*USER) führt dazu, dass nur die Zugriffsberechtigungen des Benutzers während der Programmausführung gültig sind. Kompilieren Sie hingegen das Programm mit der Einstellung USRPRF (*OWNER), berücksichtigt das Betriebssystem bei der Programmausführung sowohl die Benutzer- als auch die Programmeignerberechtigungen. Der ausführende Benutzer verfügt somit über die Berechtigungen des Programmeigners solange sich das Programmobjekt im Aufrufstapel (Stack) befindet. Wird das Programm beendet, hat der Benutzer wieder seine individuellen Objekt- und Sonderberechtigungen.

Das klingt zunächst sehr einfach. Dennoch verbirgt sich hier ein Risiko. Sie könnten einem Benutzer unbeabsichtigt erlauben, nicht zulässige Aktionen auszuführen. Alles was der Benutzer benötigt ist eine Kommandozeile oder ein geeignetes Tool, um die übernommenen Berechtigungen für seine Zwecke zu verwenden. Diese Sicherheitslücke tritt insbesondere dann auf, wenn Sie CL-Programme einsetzen, die Menüs zur Verfügung stellen. Übernimmt das CL-Programm die Berechtigungen seines Eigners, ist alles, was der Benutzer tut während sich das CL-Menüprogramm im Stapel befindet, ein Sicherheitsrisiko.

Warum? Menüs enthalten häufig Betriebssystembefehle, wie z.B. den Befehl WRKSPLF – „Mit Druckausgaben arbeiten“ und diese Betriebssystembefehle stellen eine Befehlszeile zur Verfügung! Dieses Risiko wird größer, wenn das Programm *JOBCTL- oder gar *ALLOBJ-Berechtigungen vom Programmeigner erbt. Mit der Sonderberechtigung *JOBCTL und einer Befehlszeile könnte der Benutzer jeden Job im System modifizieren. Ein Benutzer, der *ALLOBJ-Berechtigungen erbt, darf auf jedes Objekt im System zugreifen und hätte somit Zugang zu allen Firmendaten. Achten Sie also darauf, dass Ihre Programme, wenn Sie Berechtigungen übernehmen, keine Schnittstellen zum Betriebssystem beinhalten. Dies gilt jedoch nicht für Systemanfragen, für die Bearbeitung von Abbruchnachrichten oder Debug-Operationen. In diesen Fällen wird die Berechtigungsübernahme automatisch unterbrochen.

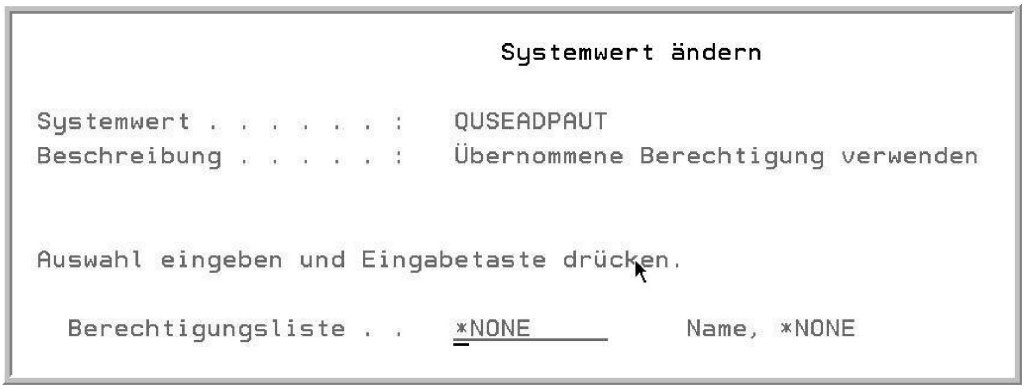
Ein weiteres Problem sind unbeabsichtigte Berechtigungsübernahmen: Programme, die mit der Einstellung USRPRF (*USER) kompiliert werden, können Berechtigungen anderer Programme übernehmen. Schuld daran ist der Parameter „übernommene Berechtigungen nutzen“(USEADPAUT). Dieser Parameter hat bei der Programmumwandlung immer die Einstellung *YES. Dadurch übernimmt ein Programm die Berechtigungen von Programmen, die weiter oben im Aufrufstapel stehen (siehe folgende Grafik).



Wirkungsweise der Berechtigungsübernahmen

9.10.3
Seite 4

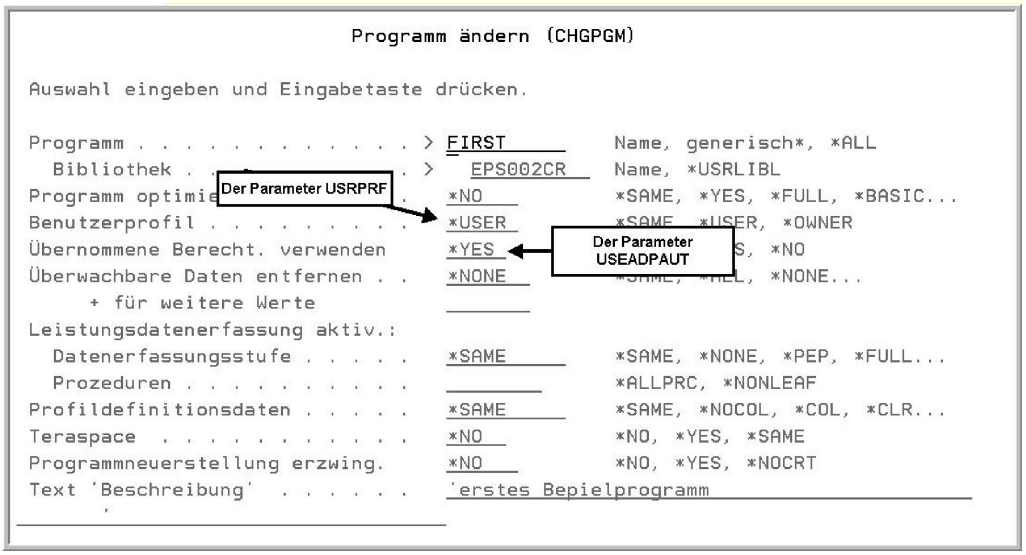
Programme können somit auf zwei unterschiedliche Arten Berechtigungen übernehmen. Zum einen ermöglicht der Parameter USRPRF (*OWNER) es dem Programm, die Berechtigungen des Programmeigners zu erben. Zum anderen kann ein Programm die Berechtigungen vorangegangener Programme im Aufrufstapel nutzen – USEADPAUT (*YES). Die zweite Möglichkeit lässt sich über den Systemwert QUSEADPAUT auf einen bestimmten Personenkreis einschränken.



Der Systemwert QUSEADPAUT

Dieser Systemwert definiert, welche Benutzer-Programme mit dem Wert USEADPAUT (*YES) erstellen dürfen. Die Defaulteinstellung *NONE erlaubt es zunächst allen Benutzern. Sie können aber den Namen einer Berechtigungsliste hinterlegen. Dies führt dazu, dass zunächst anhand dieser Liste die Benutzerberechtigungen überprüft werden und nur wenn der Benutzer mindestens die Berechtigung *USE hat, darf er Programme kompilieren, die die Berechtigung anderer im Aufrufstapel vorhandener Programme übernehmen.

Und noch etwas müssen Sie beachten: die Parameter USRPRF und USEADPAUT werden ignoriert, wenn Sie ein Programm erneut kompilieren. Das neue Programm wird stets über die gleichen Werte verfügen wie das ersetzte Programm. Um die Parameter zu ändern, müssen Sie entweder das alte Programmobjekt vor der Umwandlung explizit löschen oder die Werte mit dem Befehl „Programm ändern“(CHGPGM) manuell ändern.

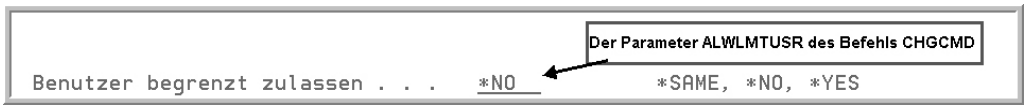


Der Befehl CHGPGM

Zum Schluss noch einige kritische Anmerkungen:

- Versuchen Sie, Ihre Objekte zu kategorisieren, d.h. ordnen Sie Ihre Objekte in Kategorien ein. Programme, Bildschirm- und Druckdateien speichern keine Daten. Datenbereiche und Tabellen dagegen enthalten Daten. Im Allgemeinen sollten Sie für die Datenobjekte die öffentlichen Berechtigungen auf *EXCLUDE setzen. Objekte, die keine Daten spezifizieren, können auch mit der *PUBLIC-Berechtigung *USE gespeichert werden. Eine gute Möglichkeit Objekte zu kategorisieren, besteht darin, sie in unterschiedlichen Bibliotheken zu organisieren. Wenn Sie eine Bibliothek erstellen, die ausschließlich Datenobjekte enthält, können Sie den Parameter „Berechtigungen erstellen“(CRTAUT) des Befehls „Bibliothek erstellen“(CRTLIB) auf *EXCLUDE setzen. Dadurch bestimmen Sie bereits beim Erstellen der Bibliothek, dass alle Objekte, die Sie in der Bibliothek mit einem entsprechenden CRT-Befehl erstellen, die öffentliche Berechtigung *EXCLUDE erhalten. Analog nutzen Sie natürlich die Berechtigung *USE für Ihre Programmbibliotheken. Nachteilig an dieser Methode ist, dass indirekt erzeugte Objekte unberücksichtigt bleiben, d.h. Objekte, die dupliziert oder durch den Befehl „Datei kopieren“(CPYF) erstellt werden, erhalten die öffentlichen Berechtigungen in Abhängigkeit der verwendeten Befehle und nicht aufgrund der Bibliothekseinstellung.

- Achten Sie auch darauf, dass Sie die Möglichkeiten Ihrer Benutzer, mit der Befehlszeile zu arbeiten, bereits im Benutzerprofil unterbinden. Wenn Sie den Parameter „Möglichkeiten einschränken“ (LMTCPB) auf *YES setzen, können Ihre Mitarbeiter keine Befehle nutzen – auch nicht unter übernommenen Berechtigungen. Falls es Befehle gibt, die Sie allgemeingültig zur Verfügung stellen wollen, ändern Sie mit dem Befehl „Befehl ändern“(CHGCMD) deren Parameter ALWLMTUSR auf *YES.



- Vermeiden Sie den Benutzer QSECOFR als Programmeigner bei Berechtigungsübernahmen. Auch auf die Sonderberechtigung *ALLOBJ sollten Sie im Rahmen von Berechtigungsübernahmen verzichten. Konfigurieren Sie lieber einige Pseudobenutzerprofile. Erteilen Sie diesen Profilen die nötigen Zugriffsberechtigungen für die Objekte, verzichten Sie aber – wenn möglich – auf Sonderberechtigungen und setzen Sie das Kennwort für die Pseudoprofile auf *NONE, so dass sich niemand mit diesen Profilen anmelden kann.
- Startprogramme, die im Benutzerprofil hinterlegt sind, sollten keine Berechtigungen übernehmen, denn diese Programme stehen im Aufrufstapel (Stack) solange der Benutzer interaktiv arbeitet und es kann schnell zu unbeabsichtigten Berechtigungsübernahmen kommen.
- Versuchen Sie – wenn möglich – Stapeljobs für die Berechtigungsübernahmen einzusetzen. Einerseits wirken sich die Batchjobs positiv auf die Systemleistung aus, andererseits können Batchjobs von übergeordneten Programmen keine Berechtigungen erben.

Berechtigungsübernahmen umsetzen

Erinnern Sie sich noch an das anfangs geschilderte Problem? Eine Mitarbeiterin der Lohn- und Gehaltsabteilung muss im Rahmen der Applikation auf alle Lohn- und Gehaltsdaten zugreifen. Außerdem soll dieser Mitarbeiterin auch Query zur Verfügung gestellt werden, ohne dabei den Zugriff auf einige Lohn- und Gehaltstabellen zu erlauben. Wir müssen dieser Mitarbeiterin also einerseits den vollen Zugriff auf die Lohn- und Gehaltstabellen ermöglichen und gleichzeitig sicherstellen, dass sie mit Query die Lohn- und Gehaltsdaten nicht lesen kann. Im Folgenden werden wir versuchen, dieses Problem beispielhaft zu lösen.

Zunächst benötigen wir einige Benutzerprofile:

Es ist empfehlenswert, die Objekte einer Anwendung stets einem Eigner zu übertragen, dadurch ersparen Sie sich viel Verwaltungsaufwand. In meinem Beispiel ist das Benutzerprofil „LG_APOWN“ für die Lohn- und Gehaltsbuchführung. Ein weiteres Benutzerprofil, „LG_QRY“ steuert den Zugriff auf die Bibliotheken und Tabellen mit Query. Mit dem dritten Profil „LG_USR“ soll sich die Mitarbeiterin der Lohn- und Gehaltsabteilung später anmelden. Ein viertes Profil kann Eigentümer verschiedener Objekte werden, die der Problemlösung dienen.

Wir haben demzufolge vier Profile, die folgendermaßen definiert sind:

Profilname	Beschreibung	Passwort	Sonder-Berechtigungen	Anfangs-Menü	Möglichkeiten einschränken
LG_QRY	Für Zugriff auf Bibliotheken/Objekte mit Query	*NONE	*NONE	Nicht erforderlich	Nicht erforderlich
LG_APOWN	Eigentümer der Anwendung Lohn- und Gehalt. Verfügt über alle Berechtigungen für die entsprechenden Lohn- und Gehaltsobjekte.	*NONE	Entsprechend der Anwendung	Nicht erforderlich	Nicht erforderlich
LG_USR	Beispielprofil für Mitarbeiter der Lohn- und Gehaltsabteilung	*YES	*NONE	LG_STR	*YES
LG_DIV	Pseudoprofil für diverse Objekte	*NONE	*NONE	Nicht erforderlich	Nicht erforderlich

Sie könnten dem Profil LG_USR zusätzlich eine aktuelle Bibliothek zuweisen, so dass die Query-Abfragen immer in dieser persönlichen Bibliothek gespeichert werden. Eigentümer der Bibliothek sollte dann das Profil „LG_USR“ sein, damit es alle Berechtigungen an der Bibliothek erhält.

Und jetzt benötigen wir noch ein Anfangsmenü „LG_MNU01“ für unsere Mitarbeiterin der Lohn- und Gehaltsabrechnung.

```
LG_MNU01                Lohn- und Gehaltsbuchführung            22.01.07
                                                                13:33:00
Auswahlmöglichkeiten:

              1. Lohnabrechnung
              2. Gehaltsabrechnung
              3. Personalstammdaten


             20. Queryabfragen erstellen



                                                        99. Abmelden




Auswahl oder Befehl
     ===
```

Anfangsmenü

Wenn die Mitarbeiterin den Menüpunkt 1 wählt, dann wird sie im Rahmen der Anwendung in der Lohn- und Gehaltsabrechnung arbeiten. Dafür schreiben wir ein kleines CL-Programm (LG_STR), das zunächst die entsprechenden Bibliotheken in die Suchliste der Mitarbeiterin aufnimmt. Außerdem übernimmt es die Berechtigungen des Applikation-Owners „LG_APOWN“, um auf die entsprechenden Objekte zugreifen zu können. Das Programm wird mit der Parametereinstellung USRPRF(*OWNER) kompiliert.

Mein CL-Programm „LG_STR“ sieht wie folgt aus:

```
PGM
ADDLIBLE LG_DATA /* Zuordnung der erforderlichen Bibliotheken */
ADDLIBLE LG_PGM
GO LG_MNU02      /* Menü der Lohn- und Gehaltsabrechnung */
RMVLIBLE LG_DATA /* Entfernen der Lohn- und Gehaltsbibliotheken
                    aus der Suchliste */
RMVLIBLE LG_PGM
ENDPGM
```

Eigentümer des Programms „LG_STR“, das die Lohn- und Gehaltsabrechnung startet, muss das Benutzerprofil „LG_ApOWN“ sein. Ich übertrage daher die Eignerschaft am ausführbaren Programmobjekt auf das entsprechende Profil.

```
                    Objekteigner ändern (CHGOBJOWN)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . > LG_STR      Name
  Bibliothek . . . . . *LIBL     Name, *LIBL, *CURLIB
Objektart . . . . . > *PGM      *ALRTBL, *AUTL, *BNDDIR...
ASP-Einheit . . . . . *          Name, *, *SYSBAS
Neuer Eigner . . . . . > LG_APOWN  Name
Aktuelle Eignerberechtigung . .  *REVOKE     *REVOKE, *SAME
```

Objekt-Eignerschaft übertragen

Mit einem zweiten CL-Programm „QRY_STR“ bestimmen wir die Query-Umgebung:

```
PGM
ADDLIBLE LG_DATA    /* Zuordnung der erforderlichen Bibliotheken */
STRQRY              /* Aufruf Query */
RMVLIBLE LG_DATA    /* Entfernen der Lohn- und Gehaltsbibliotheken
                       aus der Suchliste */
ENDPGM
```

Auch hier soll das Programm zur Ausführungszeit die Berechtigungen des Eigners erben (USRPRF*OWNER). Das Benutzerprofil „LG_QRY“ wird Eigentümer dieses Objekts.

Unsere Lösung ist fertig!

9.10.3
Seite 10

Schauen wir uns jetzt die Zugriffsberechtigungen der beteiligten Objekte an:

Objekt	Beschreibung	Eigentümer	*PUBLIC Berechtigung	Private Berechtigungen
Bibliothek LG_PGM	Lohn- u. Gehalts-Programmbibliothek	LG_ApOWN	*EXCLUDE	
Bibliothek LG_DATA	Lohn- und Gehalts-Datenbibliothek	LG_ApOWN	*EXCLUDE	Das Benutzerprofil LG_QRY erhält *USE-Berechtigung
Bibliothek DIV_OBJ	Diverse Objekte für unterschiedliche Applikationen	LG_DIV	*EXCLUDE	*USE-Berechtigung für alle User, die die entsprechenden Objekte nutzen (z. B. der Benutzer LG_USR)
Menü LG_MNU01 in DIV_OBJ	Anfangsmenü der Mitarbeiter Lohn- und Gehalt, die Query nutzen sollen.	LG_DIV	*EXCLUDE	*USE Berechtigung für die Benutzer der Lohn- und Gehaltsabteilung.
Programm LG_STR in DIV_OBJ	Startprogramm Lohn- und Gehalt	LG_ApOWN	*EXCLUDE	*USE Berechtigung für die Benutzer der Lohn- und Gehaltsabteilung.
Programm QRY_STR in DIV_OBJ	Startprogramm Query	LG_QRY	*EXCLUDE	*USE Berechtigung für die Benutzer der Lohn- und Gehaltsabteilung.
Lohn- und Gehaltstabellen ohne Query	Tabelle mit den Lohn- und Gehaltsdaten ohne Query	LG_ApOWN	*EXCLUDE	

Lohn- und Gehaltstabellen mit Query	Tabelle mit den Lohn- und Gehaltsdaten mit Query Zugriff	LG_ApOWN	*USE	
Programme Lohn- und Gehaltsabrechnung	Alle Programme	LG_ApOWN	*USE	

Wenn die Mitarbeiterin der Lohn- und Gehaltabteilung sich jetzt anmeldet, erhält sie zunächst das entsprechende Anfangsmenü in der Bibliothek „DIV_OBJ“ – gesteuert durch ihr Benutzerprofil.

```
LG_MNU01                Lohn- und Gehaltsbuchführung          23.01.07
                                                              14:23:40
Auswahlmöglichkeiten:

              1. Lohnabrechnung
              2. Gehaltsabrechnung
              3. Personalstammdaten


             20. Queryabfragen erstellen


                                                      99. Abmelden




Auswahl oder Befehl
     ____
```

Anfangsmenü

Die Mitarbeiterin braucht sowohl für die Bibliothek „DIV_OBJ“ als auch für das Menüobjekt „LG_MNU01“ die *USE-Berechtigung. Anstelle einer separaten Bibliothek könnte sie auch QGPL für die diversen Objekte nutzen. Ich vermeide es allerdings, eigene Objekte in IBM-Bibliotheken zu speichern. Entscheidet sich die Mitarbeiterin, anschließend in der Lohn- und Gehaltsanwendung zu arbeiten, wird das Programm „LG_STR“ aufgerufen. Für den Programmaufruf sind ebenfalls *USE-Rechte erforderlich. Das Programm „LG_STR“ adoptiert die Rechte des Programmeigners – also die Rechte des Benutzerprofils „LG_ApOWN“, so dass die Mitarbeiterin jetzt zusätzlich über die Rechte des Programmeigners verfügt. Innerhalb der Applikation erhält sie uneingeschränkten Zugriff auf alle Daten- und Programmobjekte.

Kehrt die Mitarbeiterin wieder zum Ausgangsmenü zurück, wird das Programm „LG_Start“ aus dem Programmstapel entfernt; die Rechte des Programmeigners sind nicht mehr wirksam.

Falls die Mitarbeiterin anschließend den Menüpunkt 20 wählt, startet das Programm „QRY_STR“. Auch hierfür sind *USE-Berechtigungen erforderlich. Dieses Programm adoptiert die Rechte des Eigners „LG_QRY“. Das Profil „LG_QRY“ hat die *USE-Berechtigung für die Datenbibliothek und darf aufgrund der *PUBLIC-Berechtigung *USE auf ausgewählte Tabellen der Lohn- und Gehaltsanwendung zugreifen. Dies würde aber nicht für die Mitarbeiterin ausreichen, denn die *PUBLIC-Berechtigungen können nicht vererbt werden. Sie wurde aber auch nicht explizit von der Nutzung der Datenobjekte ausgeschlossen; somit erhält auch sie Zugang zu den Objekten. Die übernommene Berechtigung benötigt sie lediglich für die Datenbibliothek. Diese Berechtigung verfällt, sobald die Anwenderin zum Ausgangsmenü zurückkehrt.

Falls sie Query aus der Lohn- und Gehaltsanwendung heraus aufrufen möchte, ist auch das kein Problem. In diesem Fall muss sie darauf achten, dass das Startprogramm „QRY_STR“ keine Rechte im Stack übergeordneter Programme übernimmt – das heißt: Der Parameter USEADPAUT des Programms „QRY_STR“ muss auf *NO gesetzt werden.

Auch wenn die Lösung im ersten Moment vielleicht etwas komplex erscheint, werden Sie sehr schnell feststellen, dass der anschließende Verwaltungsaufwand minimal ist. Sie könnten den Verwaltungsaufwand weiter minimieren, indem Sie für die erforderlichen *USE-Berechtigungen der diversen Objekte ein Gruppenprofil oder eine Berechtigungsliste einsetzen. Zukünftig ist es dann ausreichend, die Mitarbeiter der Lohn- und Gehaltsabteilung mit Query-Zugriff über das entsprechende Anfangsmenü zur Verfügung stellen – alles andere funktioniert automatisch!

Berechtigungsübernahmen kontrollieren

Wenn Sie sich jetzt entschließen, mit Berechtigungsübernahmen zu arbeiten, sollten Sie nicht vergessen, die Übernahmen von Zeit zu Zeit zu kontrollieren, indem Sie sich die Berechtigungsübernahmen anzeigen lassen. Der Befehl „Übernommene Programmberechtigungen anzeigen“ (DSPPGMADP) zeigt alle Objekte, die die Berechtigungen eines speziellen Benutzerprofils übernehmen.

```
                    Programmübernahme anzeigen (DSPPGMADP)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . > LG_APOWN     Name
Objektart  . . . . . .     *ALL         *ALL, *PGM, *SQLPKG, *SRVPGM
     + für weitere Werte
Ausgabe  . . . . . .       *           *, *PRINT, *OUTFILE
```

DSPPGMADP

Das Ergebnis

```
                          Programmübernahme anzeigen

Benutzerprofil . . . . . :   LG_APOWN

                                    ASP-
Objekt      Bibliothek  Art         Einheit     Attribut    Text
LG_STR      DIV_OBJ     *PGM        *SYSBAS     CLP         Startprogramm LG
```

Ergebnis des Befehls DSPPGMADP

Mir erscheint zur Überprüfung der Befehl „Objekte mit Berechtigungsübernahmen drucken“ (PRTADPOBJ) am geeignetsten, da hier Berichte aller Objekte gedruckt werden können. Sie erhalten zwei Berichte je Benutzerprofil. Der erste Bericht ist ein Gesamtbericht, der sämtliche Objekte beinhaltet, die die Berechtigungen des Benutzerprofils übernehmen. Der zweite Bericht enthält Änderungen – das heißt: Sie erhalten einen Überblick über die Objekte, die bei der letzten Ausführung des Befehls „PRTADPOBJ“ noch nicht zu den Objekten mit Berechtigungsübernahme für dieses Benutzerprofil gehörten. Der zweite Bericht erscheint nicht, wenn Sie das erste Mal den Befehl nutzen. Außerdem sollten Sie bedenken, dass die überprüften Benutzerprofile für die Dauer der Befehlsausführung gesperrt sind.

```
                  Obj. mit Ber.-Übernahme druck. (PRTADPOBJ)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .   *all_____     Name, generisch*, *ALL
Nur Änderungsbericht . . . . .   *NO_       *NO, *YES
```

Befehl PRTADPOBJ

```
Benutzerprofil . . . . . :  LG_APOWN
Sonderberechtigungen . . . . . :  *NONE
-------------Objekt--------------    --------------Bibliothek--------------
                      Allgem.                                 Allgem.     Persönl.
Name          Art     Berecht.    Name          ASP-Einh.     Berecht.    Berecht.
LG_STR        *PGM    *EXCLUDE    DIV_OBJ       *SYSBAS       *EXCLUDE      N
```

Ergebnis des Befehls PRTADPOBJ

Diese Betriebssystembefehle sind im Übrigen auch im Menü „SECBATCH“ hinterlegt.

```
SECBATCH    Sicherheitsberichte zur Stapelverarb. übergeben/planen
                                                        System:   EPOSI501
Auswahlmöglichkeiten:

  Berichte zur Stapelverarbeitung übergeben
     1. Objekte mit Berechtigungsübernahme
     2. Protokolljournaleinträge
     3. Berechtigungen für Berechtigungsliste
     4. Befehlsberechtigung
     5. Persönliche Befehlsberechtigung
     6. DFV-Datenschutz
     7. Verzeichnisberechtigung
     8. Persönliche Verzeichnisberechtigung
     9. Dokumentberechtigung
    10. Persönliche Dokumentberechtigung
    11. Dateiberechtigung
    12. Persönliche Dateiberechtigung
                                                              Weitere ...
Auswahl oder Befehl
===> _____________________________________________________________________

F1=Hilfetext   F3=Verlassen   F4=Bedienerführung   F9=Auffinden
F12=Abbrechen
```

Menü SecBatch

Nutzen Sie doch einfach diese Möglichkeiten, um potentielle Sicherheitsrisiken aufgrund von Berechtigungsübernahmen auf Ihrem System aufzuspüren!

9.11 Das Objektkonzept

Alle auf einer iSeries gespeicherten Elemente werden als Objekte bezeichnet. Objekte haben eine eindeutige Beschreibung und werden in Bibliotheken gespeichert. Im System iSeries werden somit zusammengehörige Informationen als Objekt zusammengefasst und verwaltet. Ein Objekt kann unter einem definierten Namen angesprochen und mit entsprechenden Systembefehlen bearbeitet werden. Alle Einzelinformationen – wie z.B. der Name, der Ersteller, der Objekteigner, das Datum der letzten Sicherung, Berechtigungen usw. – können nur über das Objekt bearbeitet werden. Die möglichen Objektarten (=-typen) werden automatisch vom System vergeben. Alle Objekte werden in Bibliotheken organisatorisch verwaltet und durch ihre Objektart klassifiziert. Objekte gleichen Namens sind in getrennten Bibliotheken erlaubt. Gleichnamige Objekte in derselben Bibliothek müssen sich durch ihre Objektart unterscheiden.

Zur Veranschaulichung:

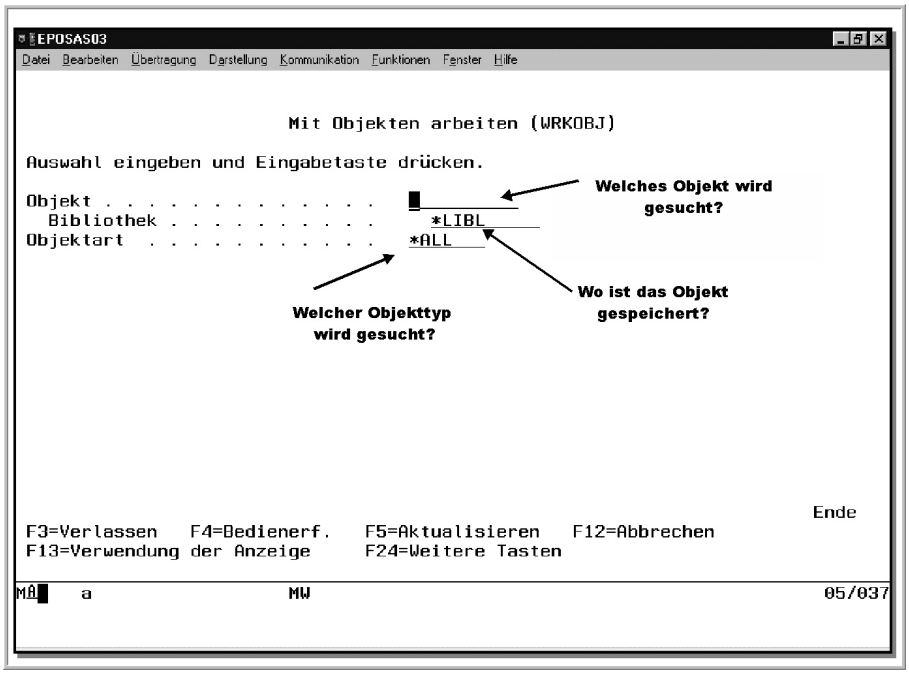
Sie erstellen eine Datei namens „KD001“ und ein Programm, das auch „KD001“ heißen soll. Die Datei bekommt vom System die Objektart *FILE. Nach der fehlerfreien Übersetzung Ihres Programms erhalten Sie das Objekt der Art *PGM. Beide Objekte können aufgrund der unterschiedlichen Objektart in einer Bibliothek verwaltet werden.

*LIB	Bibliotheken	*FILE	Dateien
*MSGF	Nachrichtendateien	*CMD	Befehle
*PGM	Programme	*JOBD	Jobbeschreibung
*JOBQ	Jobwarteschlangen	*OUTQ	Ausgabewarteschlangen

9.11
Seite 2

9.11.1 Zentrale Objektverwaltungsbefehle

Immer wieder kommt es vor, dass Sie eine Gruppe von Objekten bearbeiten möchten, oder aber Sie suchen ein ganz bestimmtes Objekt und können es nicht finden. Diese Probleme werden mit dem Befehl WRKOBJ gelöst.



Suchmaske für Objekte

Stellen Sie sich die folgenden Szenarien vor:

Sie möchten wissen, ob das Objekt „KUNDE“ existiert:

Suche nach einem bestimmten Objekt

Alle Objekte, die den Namen Kunde haben, werden angezeigt.

Wenn Sie die Objektart eingrenzen wollen, müssen Sie den gesuchten Objekttyp im Parameter Objektart eintragen.

9.11.1
Seite 2

Sie möchten wissen, welche Dateien in der Bibliothek „EPS005“ gespeichert sind:

```
                    Mit Objekten arbeiten (WRKOBJ)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . . . . . . . . . *ALL          Name, generisch*, *ALL
  Bibliothek . . . . . . . . . .  EPS005       Name, *LIBL, *CURLIB...
Objektart  . . . .  . . . . . .  *FILE         *ALL, *ALRTBL, *AUTL...
```

Suche in einer bestimmten Bibliothek

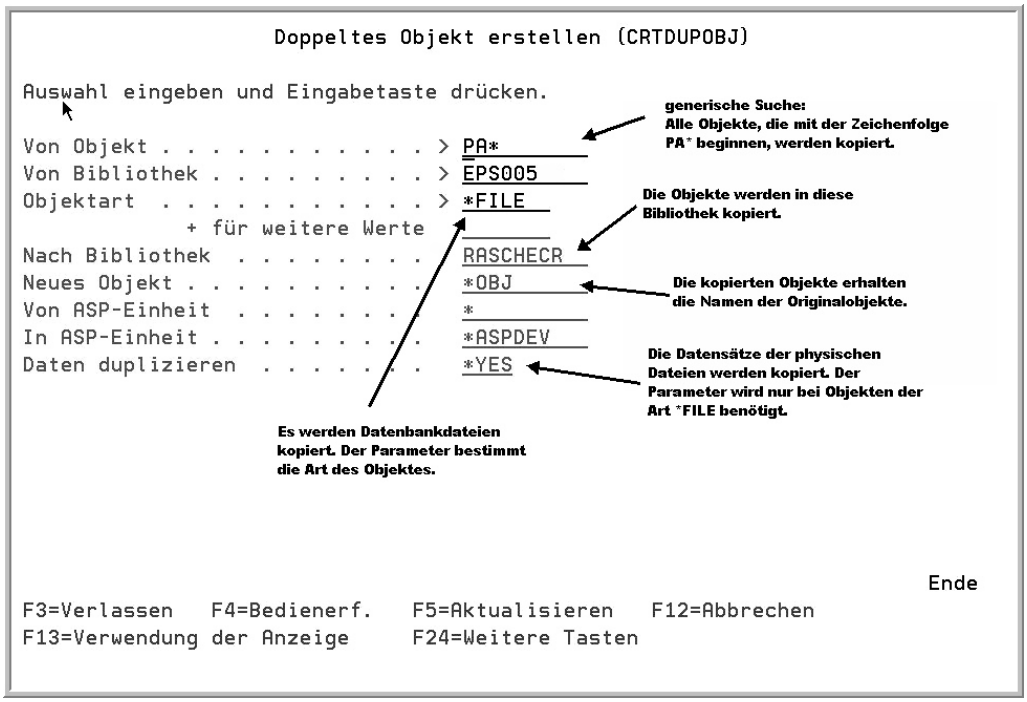
Sie möchten alle Dateien, die mit der Zeichenfolge „PA“ beginnen, bearbeiten:

```
                    Mit Objekten arbeiten (WRKOBJ)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . . . . . . . . .  PA*          Name, generisch*, *ALL
  Bibliothek . . . . . . . . . .   EPS005      Name, *LIBL, *CURLIB...
Objektart  . . . .  . . . . . .   *FILE        *ALL, *ALRTBL, *AUTL...
```

Suche nach einer bestimmten Zeichenfolge

Der Befehl WRKOBJ stellt Ihnen alle Objektbearbeitungsbefehle über entsprechende Auswahlen zur Verfügung. Natürlich können Sie die Befehle auch direkt einsetzen.

WRKOBJ	Mit Objekten arbeiten
CRTDUPOBJ	Objekt kopieren
RNMOBJ	Objekt umbenennen
DSPOBJD	Objektbeschreibung anzeigen
MOVOBJ	Objekt verschieben



Duplizieren eines Objektes

Beachten Sie bitte, dass für einige Objektattribute kein 100-prozentiges Duplikat erzeugt wird. Das doppelte Objekt verfügt zwar über identische Berechtigungen, aber Eigentümer des neuen Objekts wird der Benutzer, der das Objekt kopiert. Das neu erstellte Objekt muss umbenannt werden, wenn es in derselben Bibliothek wie das Originalobjekt gespeichert werden soll.

9.11.1
Seite 4

9.12 Objekte und Berechtigungen

In den vorangegangenen Kapiteln haben wir uns mit den übergeordneten Systemeinstellungen, sicherheitsrelevanten Systemwerten, Sicherheitsstufen und Benutzerprofilen sowie deren Einstellungen beschäftigt.

Objekte
Etwas Entscheidendes fehlt in dieser Aufstellung allerdings noch – die Objekte. Auf unserem IBM Power i-System beschäftigen wir uns ja ständig mit Objekten. Datenbanken sind Objekte, Programme sind Objekte, Datenwarteschlangen, Jobwarteschlangen, Spool-Dateien ebenso. Jedes Objekt besitzt Eigenschaften und u. a. auch Berechtigungen, mit denen gesteuert wird, welche Benutzer oder Benutzergruppen mit diesen Objekten arbeiten dürfen.

Objektberechtigungen
Objektberechtigungen beinhalten Informationen darüber, wer Objekte wie verwenden darf, also z. B., dass ein Anwender ein Objekt benutzen, ein zweiter Anwender das Objekt ändern und ein dritter überhaupt nicht auf das Objekt zugreifen darf.

In diesem Teil des Werks geht es also um Objekte und deren Berechtigungen. Den Einstieg dazu finden wir, indem wir mit Objekten arbeiten.

36. Ergänzung 9/2013

9.12
Seite 2

9.12.1 Objeke in Bibliotheken

Sie wissen bereits, dass alle iSeries-Objekte in Bibliotheken gespeichert werden. Bibliotheken sind Objekte der Art *LIB.

WRKLIB	Bibliotheken verwalten
DSPLIB	Bibliotheken anzeigen
DLTLIB	Bibliotheken löschen
CHGLIB	Bibliotheksattribute verändern
CRTLIB	Bibliotheken erstellen
CLRLIB	Bibliotheksinhalt löschen

Anders als Windows-Verzeichnisse können Bibliotheken nicht hierarchisch gruppiert werden – mit Ausnahme der Systembibliothek QSYS. In der Bibliothek QSYS werden sowohl alle Systembibliotheken als auch alle Benutzerbibliotheken als Eintrag geführt. Systembibliotheken sind dadurch gekennzeichnet, dass Ihr Name mit einem Q beginnt. Als Anwender sollten Sie Ihre Objekte nicht wahllos in Bibliotheken speichern, sondern bei der Erstellung und Benutzung von Bibliotheken bestimmte Regeln beachten und für Ihr Unternehmen dokumentieren.

- Alle Objekte einer Anwendung (Programme, Bildschirme etc.) verwalten Sie in einer Bibliothek.
- Alle Datenobjekte der Anwendung werden in einer separaten Bibliothek verwaltet. Eventuell werden Sie sich zu einem späteren Zeitpunkt entscheiden, für Ihre Dateien weitere Bibliotheken einzusetzen. Achten Sie deshalb darauf, dass Ihre Programme und Querys die Daten nicht mit dem Bibliotheksnamen adressieren, sondern über die Suchliste zugreifen. So erhalten Sie sich die nötige Flexibilität.
- Alle zusätzlichen Objekte (selbst erstellte Querys, eigene Befehle, geänderte Betriebssystemfunktionen usw.) sollten ebenfalls in separaten Bibliotheken gespeichert werden. Achten Sie auch hier auf die unqualifizierte Adressierung. Außerdem müssen Sie dafür sorgen, dass die erstellten Objekte nach der Testphase in offizielle Produktionsbibliotheken gespeichert werden. Nur so behalten Sie den Überblick über Ihre produktiven Objekte.

Kommen wir jetzt noch einmal auf die aktuelle Bibliothek des SIGNON-Bildschirms zurück. Die aktuelle Bibliothek (Current Library) ist die private Bibliothek eines Benutzers. Ein Benutzer, der keine eigenen Objekte erstellt, benötigt keine eigene Bibliothek. Nur Systemadministratoren, Programmierer und manchmal auch einige Anwender entwickeln und testen Objekte zunächst in privaten Bibliotheken. Aber achten Sie darauf, dass die erstellten

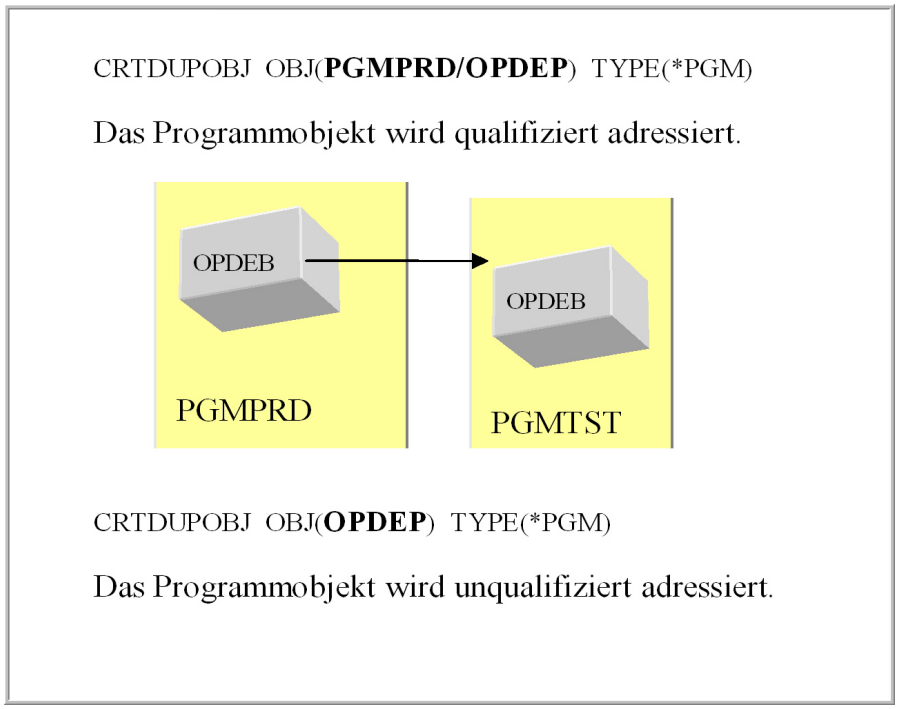
9.12.1
Seite 2

Objekte nach Abschluss der Testphase in die allgemeinen Bibliotheken übertragen werden. Denn sonst haben Sie bald eine Vielzahl von Bibliotheken, deren Inhalte Sie nicht mehr kennen und schlimmer noch: Objekte werden in Ihrem System redundant gespeichert und Sie wissen nicht mehr, welches der Objekte aktuell ist. Wenn Sie Ihre Bibliotheken deutlich strukturieren, verhindern Sie nicht nur ein kompliziertes Datensicherungs- und Berechtigungskonzept, sondern Sie ersparen sich auch viel Zeit und Arbeit bei der Pflege Ihres Systems.

9.12.2 Objektadressierung

Sie haben bereits etwas von der Bibliothekssuchliste gehört. Es stellt sich jetzt die Frage, was darunter zu verstehen ist. Stellen Sie sich folgendes vor:

Es gibt zwei Bibliotheken: PGMTST und PGMPRD. In der Bibliothek PGMTST werden Programme entwickelt und getestet. Die Bibliothek PGMPRD enthält alle freigegebenen produktiven Programme. In der Bibliothek PGMPRD befindet sich das Programm OPDEB. Einer der Programmierer kopiert das Programm zu Testzwecken in die Bibliothek PGMTST.

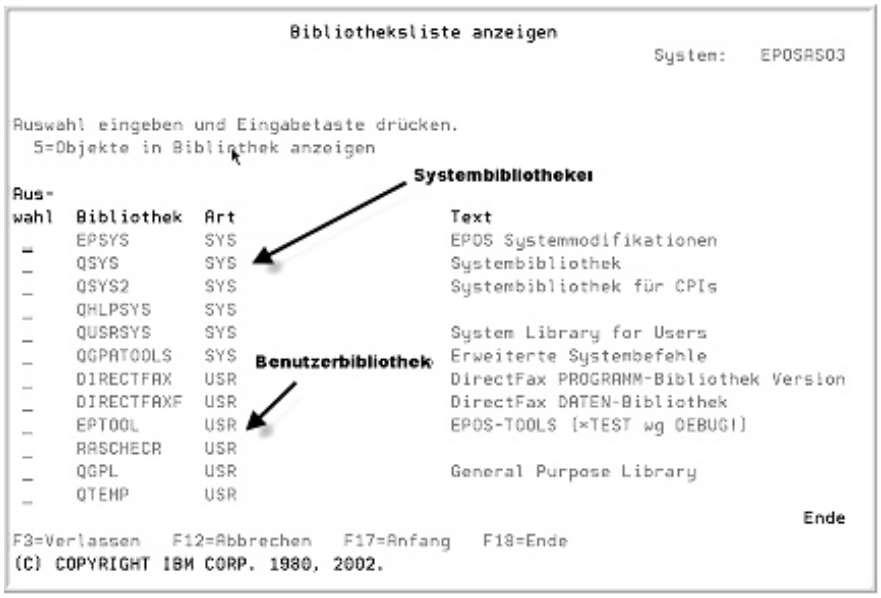


Qualifizierte und unqualifizierte Adressierung

Der Mitarbeiter hat zwei Möglichkeiten, um auf das Objekt zuzugreifen: mit Angabe des Bibliotheksnamens (qualifizierte Adressierung) oder ohne Angabe des Bibliotheksnamens (unqualifizierte Adressierung). Wenn Sie das Objekt ohne Bibliotheksnamen ansprechen, wird für die Suche des Objekts die Bibliotheksliste verwendet. Als Synonym für die Bibliotheksliste nutzt das System den Parameterwert *LIBL.

Die Bibliotheksliste wird jedem Benutzer automatisch vom System zugeordnet. Sie würden das Fehlen der Suchliste in Ihrer täglichen Arbeit schnell bemerken, denn Sie müssten jeden Betriebssystembefehl qualifizieren: QSYS/SNDMSG oder QSYS/SIGNOFF.

9.12.2
Seite 2



Bibliotheksliste eines Anwenders

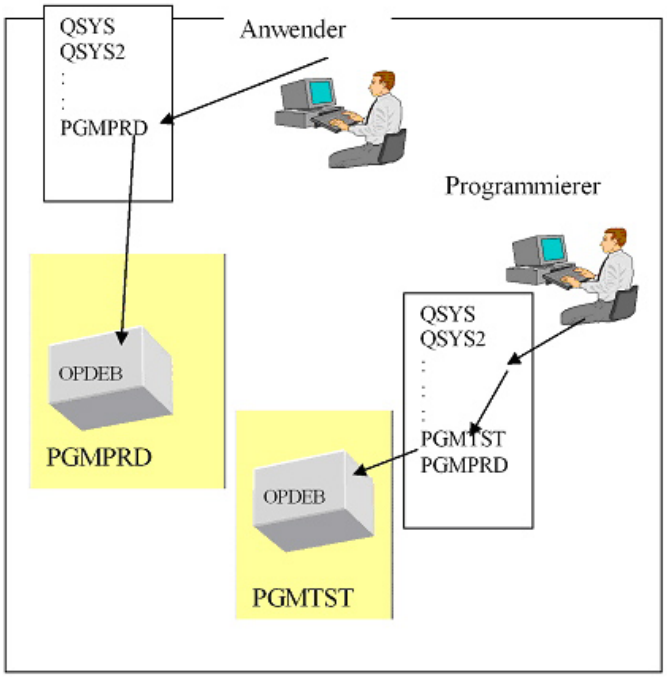
Die Suchliste beinhaltet sowohl System- als auch Benutzerbibliotheken. Welche Bibliotheken dem Job zugeordnet werden, wird durch die Systemwerte QSYSLIBL und QUSRLIBL festgelegt. Im Systemteil der Suchliste sind die Bibliotheken QSYS und QSYS2 eingetragen. Beide Bibliotheken enthalten das Betriebssystem. In der Bibliothek QHLPSYS sind umfangreiche Hilfetexte gespeichert. In der Bibliothek QUSRSYS werden u. a. Sicherheitsdaten gespeichert. Der Benutzerteil der Suchliste wird individuell aufgebaut und sollte Ihre Produktionsbibliotheken mit den freigegebenen Programm- und Query-Objekten sowie den Daten enthalten. Zusätzlich enthält der Benutzerteil zwei wichtige Systembibliotheken: QGPL und QTEMP. QGPL ist eine Bibliothek, die aufgrund der Voreinstellungen häufig als Zielbibliothek verwendet wird, wenn der Anwender vergisst, eine eigene Zielbibliothek zu benennen. Daher befinden sich in der Bibliothek QGPL häufig „verloren gegangene“ Objekte. QTEMP ist eine temporäre Bibliothek – d.h.: Alle Objekte, die Sie in dieser Bibliothek speichern, werden gelöscht, wenn Sie sich vom System abmelden. Jeder Benutzer hat eine eigene temporäre Bibliothek.

Obwohl die Suchliste normalerweise automatisch dem jeweiligen Benutzer zugeordnet wird, stehen verschieden Befehle zur Verfügung, die es gestatten, die Suchliste temporär – für die Dauer der Anmeldung – zu verändern.

DSPLIBL	Bibliotheksliste anzeigen
EDTLIBL	Bibliotheksliste editieren
ADDLIBLE	Bibliothekslisteneintrag hinzufügen
RMVLIBLE	Bibliothekslisteneintrag entfernen
CHGCURLIB	Aktuelle Bibliothek ändern
CHGUSRLIBL	Benutzerteil der Suchliste ändern

Was passiert jetzt in unserem Beispiel?

Die Anwender können mit den alten Objekten ungestört arbeiten, da Sie die Bibliothek PGMPRD in der Suchliste haben. Der Programmierer fügt die Bibliothek PGMTST in seine Suchliste vor die Bibliothek PGMPRD ein. Er testet und modifiziert das Programmobjekt, ohne den produktiven Betrieb zu stören, da das System die Suchliste sequentiell abarbeitet. Nach der Testphase wird das Objekt in die Bibliothek PGMPRD zurückkopiert – und die Anwender arbeiten mit den Programmmodifikationen.



Testen und Modifizieren eines Programmobjektes

Nutzen Sie dieses Wissen auch, um z.B. das Betriebssystem Ihren Anforderungen entsprechend anzupassen. Alle Systembefehle sind Objekte der Art *CMD. Sie könnten z.B. häufig genutzte Betriebsystemfunktionen umbenennen und dadurch den Aufruf der Funktion erleichtern. Um beispielsweise die Suchliste mit dem Befehl „DL“ anzuzeigen, müssen Sie nur den Befehl DSPLIBL (display Librarylist) kopieren (CRTDUPOBJ) und ihn dabei umbenennen. Ab sofort wird die Bibliothekssuchliste angezeigt, wenn Sie Ihren neuen Befehl „DL“ ausführen. Stellen Sie die Objektkopien aber bitte nicht in die Bibliothek QSYS, denn dann vermischt sich das Betriebssystem mit Ihren Modifikationen und Sie können bald nicht mehr Original und Kopie voneinander unterscheiden. Hinzu kommt, dass Ihre Modifikationen sich in einer separaten Bibliothek nicht störend bei einem Release-Wechsel auswirken können, da die Bibliothek QSYS im Originalzustand erhalten bleibt. Erstellen Sie sich also eine neue Bibliothek, die ausschließlich Ihre Modifikationen beinhaltet. Diese Bibliothek hinterlegen Sie im Systemwert QSYSLIBL vor die Bibliothek QSYS, denn es könnte auch mal erforderlich sein, den Originalna-

9.12.2
Seite 4

men beizubehalten und lediglich voreingestellte Parameterwerte zu verändern. Parameterwerte der Betriebssystemfunktionen überschreiben Sie mit dem Befehl CHGCMDDFT. In diesem Fall muss Ihre Funktion aber vor dem Original stehen, ansonsten werden Ihre Modifikationen nicht wirksam oder Sie müssten ständig qualifiziert zugreifen.

9.12.3 Objekttypen in Bibliotheken

Hier finden Sie eine Übersicht, welche Objekttypen in Bibliotheken gespeichert werden können:

***ALRTBL**
Das Objekt ALERT-Tabelle (*ALRTBL) enthält ALERT-Beschreibungen, die den Inhalt einer ALERT-Meldung der Systemnetzwerkarchitektur (SNA) für bestimmte Fehlerbedingungen definieren. Der IBM i Alert-Manager verwendet zur Erstellung einer Alert-Meldung Alert-Beschreibungen aus einer Alert-Tabelle.

***AUTL**
Das Objekt Berechtigungsliste (*AUTL) enthält eine Liste von Benutzern und deren Berechtigungen zum Schützen bzw. Benutzen anderer Objekte.

***BNDDIR**
Das Objekt Binderverzeichnis (*BNDDIR) enthält die Namen von Objekten, die Bibliothek, in der sie sich befinden, sowie die Objektart (*MODULE oder *SRVPGM). Anhand des Binderverzeichnisobjekts können die Namen der *MODULE- und *SRVPGM-Objekte im Befehl CRTPGM (Programm erstellen) oder im Befehl CRTSRVPGM (Serviceprogramm erstellen) zusammengefasst werden.

***CFGL**
Das Objekt Konfigurationsliste (*CFGL) enthält eine Liste von DFV-Einträgen, die von asynchroner Übertragung, APPN-Übertragung und der Übertragung für den Durchgriff auf Einzelhandelseinrichtungen zum Definieren ferner und lokaler Standorte und Netzwerkadressen verwendet werden.

***CHTFMT**
Das Objekt Diagrammformat (*CHTFMT) enthält Definitionen für die Darstellung von Diagrammen mit der Präsentationsgrafik (BGU). Mit dem Diagrammformat können Balkendiagramme oder andere Diagrammarten angegeben werden.

***CLD**
Das Objekt Beschreibung der länderspezifischen Angaben für die Programmiersprache ILE C (*CLD) enthält Formatierungsangaben für numerische Einheiten, Währungseinheiten, Sortierfolgen und Codepunktzuordnungen.

***CLS**
Das Objekt Klasse (*CLS) enthält die Umgebungsattribute zur Ausführung eines Jobs. Die von einem Leitwegschritt verwendete Klasse wird im Leitwegeintrag der Subsystembeschreibung angegeben.

***CMD**
Ein Objekt-Befehl (*CMD) fordert eine Funktion des Systems an.

***CNNL**
Das Objekt Verbindungsliste (*CNNL) enthält Konfigurationsinformationen, die vom System benötigt werden, um das Senden und Empfangen von Anrufen mit einem dienstintegrierenden digitalen Fernmeldenetz (ISDN) zu verwalten.

***COSD**
Das Objekt Serviceklassenbeschreibung (*COSD) enthält Bereiche von Verbindungs- und Knotenkenndaten, die für die Leitwegwahl einer APPN-Sitzung durch ein APPC-Netzwerk verwendet werden.

***CRG**
Das Objekt Clusterressourcengruppe (*CRG) definiert die Beziehung zwischen den Knoten (Systemen), die einer Gruppe an flexiblen Ressourcen zugeordnet sind. Das Objekt definiert auch die Aktionen, die bei einem Wechsel des Zugriffpunkts der flexiblen Ressourcen durchzuführen sind.

***CRQD**
Das Objekt Änderungsanforderungsbeschreibung (*CRQD) definiert eine Änderung, die in einem Systemnetzwerk vorzunehmen ist. Die Änderungsanforderungsbeschreibung umfasst eine oder mehrere Aktivitäten, mit denen die Änderung ausgeführt wird.

***CSI**
Das Objekt DFV-Nebeninformation (*CSI) enthält DFV-Informationen, die den Leitweg zum fernen System definieren, sowie Initialisierungsinformationen für eine DFV-Sitzung.

***CSPMAP**
Das Objekt Produktliste zwischen Systemen (*CSPMAP) enthält die Organisierung und die Merkmale von Informationen, die auf einer Anzeigen- oder Druckerseite bei der Ausführung eines Anwendungsprogramms angezeigt werden.

***CSPTBL**
Das Objekt Produkttabellen zwischen Systemen (*CSPTBL) enthält eine CSP/AE-Tabelle. Diese Tabelle ist eine Sammlung zugehöriger Datenelemente für die Gültigkeitsprüfung der Eingaben.

***CTLD**
Das Objekt Steuereinheitenbeschreibung (*CTLD) enthält die Merkmale einer Steuereinheit, die entweder direkt an das System oder an eine DFV-Leitung angeschlossen ist. Die Steuereinheitenbeschreibung wird für die Konfiguration verwendet.

***DEVD**
Das Objekt Einheitenbeschreibung (*DEVD) enthält eine Beschreibung einer an das System angeschlossenen Einheit und beschreibt alle Merkmale der Einheit. Die Einheitenbeschreibung (*DEVD) wird für die Konfiguration verwendet.

***DOC**
Das Objekt Dokument (*DOC) enthält den Text eines Dokuments sowie in der Dokumentbibliothek gespeicherte Informationen zur Beschreibung des Dokuments.

***DTAARA**
Das Objekt Datenbereich (*DTAARA) enthält einen Datenwert, der von verschiedenen Jobs verwendet und geändert werden kann.

***DTADCT**
Das Objekt Datenverzeichnis (*DTADCT) enthält Datei-, Format- und Felddefinitionen zur Beschreibung von Datenbankdateien.

***DTAQ**
Das Objekt Datenwarteschlange (*DTAQ) dient zum Übertragen und Speichern von Daten, die von verschiedenen Programmen innerhalb eines Jobs oder zwischen verschiedenen Jobs verwendet werden. Mehrere Jobs können Daten von einer einzigen Datenwarteschlange senden und empfangen.

***EDTD**
Das Objekt Editierbeschreibung (*EDTD) definiert Zahlenformate für Bildschirm- und Druckerdateien.

***EXITRG**
Das Objekt Repository des Exitregistrierungsservice (*EXITRG) enthält Exitpunkte und Benutzerexitprogramme.

***FCT**
Das Objekt Formularsteuertabelle (*FCT) enthält die Verarbeitungserfordernisse für die von einem Host-System empfangenen Daten zwecks Jobferneingabe (RJE).

***FILE**
Das Objekt Datei (*FILE) definiert eine Datenbankdatei, eine Einheitendatei oder zusammengehörige Datensätze innerhalb einer Datei.

***FLR**
Das Objekt Ordner (*FLR) dient als Verzeichnis für Dokumente und andere Ordner.

***FNTRSC**
Das Objekt Schriftartressource (*FNTRSC) enthält eine Darstellung dazu, wie Zeichen auf einer Seite abgebildet werden.

***FNTTBL**
Eine Schriftartentabelle (*FNTTBL) ist eine von PSF benutzte Tabelle, in der druckerresidente Schriftarten und Codepages den entsprechenden hostresidenten Schriftarten und Codepages zugeordnet sind.

***FORMDF**
Das Objekt Formulardefinition (*FORMDF) ist ein externes Bibliotheksressourcenobjekt in Rasterpunktarchitekturunterstützung, das die charakteristischen Merkmale des Formulars definiert.

***FTR**
Das Objekt Filter (*FTR) enthält Auswahleinträge, die Einheiten in Gruppen zusammenfassen. Das Objekt enthält ferner Aktionseinträge, die die für die Gruppe durchgeführte Aktion definieren.

***GSS**
Das Objekt Grafiksymbol (*GSS) enthält Zeichensätze, die von einem Grafikanwendungsprogramm verwendet werden können, um andere Zeichen als die Zeichen des mit dem Betriebssystem gelieferten Standardzeichensatzes anzuzeigen.

***IGCDCT**
Das Objekt Doppelbyte-Zeichensatzverzeichnis (*IGCDCT) wird von Character Generator Utility (CGU) zur Auswahl von Zeichen und Symbolen verwendet, die auf dem System benutzt werden.

***IGCSRT**
Das Objekt Doppelbyte-Zeichensatzsortiertabelle (*IGCSRT) wird von Character Generator Utility (CGU) zur Auswahl von Zeichen und Symbolen verwendet, die auf dem System benutzt werden.

***IGCTBL**
Das Objekt Doppelbyte-Zeichensatztabelle (*IGCTBL) enthält die Abbilder für die auf dem System verwendeten DBCS-Erweiterungszeichen. Das System verwendet diese Abbilder zum Anzeigen und Drucken von Erweiterungszeichen.

***IMGCLG**
Das Objekt Imagekatalog (*IMGCLG) enthält Informationen über Imagekatalogeinträge. Jeder Imagekatalogeintrag ist ein optisches Image, das als Datenstromdatei (*STMF) in einem vom Benutzer angegebenen Integrated File System-Verzeichnis vorhanden ist. Jeder Imagekatalog ist einem einzigen Integrated File System-Verzeichnis zugeordnet.

***IPXD**
Das Objekt Internetwork Packet Exchange Description (*IPXD) enthält Werte, die für die Konfiguration von IPX- und SPX-Kommunikationsprotokollen verwendet werden (SPX = Sequenced Packet Exchange). IPX- und SPX-Protokolle werden von IBM i für die Unterstützung der Novell NetWare** verwendet. Dazu gehören die Protokolle RIP (Router Information Protocol), SAP (Service Advertising Protocol), NLSP (Netware Link Services Protocol), SPX, IPX und andere NetWare-Funktionen. Eine IPX-Beschreibung wird vom Netzwerk-Server (NWS) für die NetWare-FSIOP-Verarbeitung sowie von der nativen IBM i NetWare-Unterstützung verwendet.

***JOBD**
Das Objekt Jobbeschreibung (*JOBD) enthält eine bestimmte Gruppe von jobbezogenen Attributen, die von einem bzw. mehreren Jobs verwendet werden können.

***JOBQ**
Das Objekt Jobwarteschlange (*JOBQ) enthält Einträge für zum Ablauf an das System übergebene Stapeljobs. Diese Stapeljobs werden vom Betriebssystem für den Ablauf aus der Jobwarteschlange ausgewählt.

***JOBSCD**
Das Objekt Jobplanungseintrag (*JOBSCD) enthält Einträge (Angaben zu Datum und Uhrzeit) für den Zeitpunkt, zu dem Stapeljobs an eine Jobwarteschlange übergeben werden.

***JRN**
Das Objekt Journal (*JRN) enthält Informationen zu Journal-Datenbankdateien und dient zu Datenbank- bzw. Pfadänderungen. Das System verwendet das Journal, um Daten über die Journalempfänger und Datenbankdateien bzw. den zugehörigen Pfad zu protokollieren.

***JRNRCV**
Das Objekt Journalempfänger (*JRNRCV) enthält Journaleinträge, die bei der Änderung von Datenbankdateien erstellt werden.

***LIB**
Das Objekt Bibliothek (*LIB) enthält Dateien, Programme und andere Objekte, die als Verzeichnis für andere Objekte dienen.

***LIND**
Das Objekt Leitungsbeschreibung (*LIND) definiert eine DFV-Leitung und beschreibt dem System ihre Zusatzeinrichtungen; dies umfasst die Beschreibung des an die Leitung angeschlossenen Modems (und seiner Zusatzeinrichtungen).

***LOCALE**
Das Objekt für länderspezifische Angaben (*LOCALE) enthält die Kombination aus Sprache, länderspezifischen Angaben und Zeichensatz, mit der bestimmte sprachliche Konventionen gekennzeichnet werden.

***M36**
Ein M36-Objekt (*M36) repräsentiert eine Advanced 36-Maschine. Auf einem IBM i-System können sich mehrere *M36-Objekte befinden. Jedes *M36-Objekt repräsentiert eine einzelne Advanced 36-Maschine.

***M36CFG**
Ein Objekt M36CFG (*M36CFG) definiert die Konfiguration, die beim IPL (einleitendes Programmladen) oder Starten für ein *M36-Objekt verwendet werden soll. Wurde das vorhandene System ausgehend von einer i5/OS Advanced 36, Modell 236, aufgerüstet, entspricht ein i5/OS Advanced 36-Maschinenkonfigurationsobjekt einer Konfigurationsteildatei auf einem IBM System /36. Das *M36CFG-Objekt hat den gleichen Namen und wird in der gleichen Bibliothek erstellt wie das *M36-Objekt.

***MEDDFN**
Ein Objekt Datenträgerdefinition (*MEDDFN) definiert die Datenträger und Einheiten, die für eine parallel durchgeführte Sicherung oder Rückspeicherung verwendet werden sollen.

***MENU**
Das Objekt Menü (*MENU) enthält Objekte, die zum Anzeigen in einem Menü verwendet werden.

***MGTCOL**
Ein Verwaltungserfassungsobjekt (*MGTCOL) wird von verschiedenen Systemfunktionen (z. B. Erfassungsservices, Management Central-Überwachungsfunktionen und Performance Explorer) zum Speichern von erfassten Leistungsdaten verwendet.

***MODD**
Das Objekt Modusbeschreibung (*MODD) enthält eine logische Gruppe von Sitzungen mit gemeinsamen Merkmalen, die von APPN- oder APPC-Protokollen verwendet werden.

***MODULE**
Ein Objekt der Art Modul (*MODULE) enthält eine Reihe von Anweisungen und Informationen, die erforderlich sind, wenn das Objekt zum Erstellen eines Binderprogramms verwendet wird. Modulobjekte werden als Ausgabe der CRTxxxMOD-Befehle erstellt.

***MSGF**
Das Objekt Nachrichtendatei (*MSGF) enthält Nachrichtenbeschreibungen, die zum Beschreiben der Status- und Fehlerbedingungen verwendet werden.

***MSGQ**
Das Objekt Nachrichtenwarteschlange (*MSGQ) enthält Nachrichten, die an eine Person, an ein Programm oder an das System gesendet oder von diesen abgerufen werden.

***NODGRP**
Ein Knotengruppenobjekt (*NODGRP) dient zur Identifizierung einer Gruppe von Systemen, über die eine verteilte Datei erstellt werden kann. Eine Knotengruppe enthält außerdem Informationen darüber, wie Daten über die verschiedenen Systeme (Knoten) verteilt werden. Das Knotengruppenobjekt kann beim Erstellen einer physischen Datenbankdatei mit dem Befehl CRTPF (Physische Datei erstellen) oder bei Verwendung der Anweisung CREATE TABLE in SQL (Structured Query Language) angegeben werden.

***NODL**
Das Objekt Knotenliste (*NODL) enthält eine Liste der SNA-Knoten. Der Name eines SNA-Knotens besteht aus einer Netzwerk-ID und einem Kontrollpunktnamen.

***NTBD**
Eine NetBIOS (Network Basic Input/Output System) -Beschreibung (*NTBD) enthält Werte, die als Verfahrensmerkmale für NetBIOS-Sitzungen dienen. NetBIOS-Sitzungen werden von FSIOP-Hardware- und Softwarekomponenten verwendet. Die NetBIOS-Beschreibung wird für die Konfiguration benutzt.

***NWID**
Das Objekt Netzwerkschnittstellenbeschreibung (*NWID) enthält Informationen zur Konfiguration einer Schnittstelle. Informationen, die vom System benötigt werden, um über die Schnittstelle mit einem dienstintegrierenden digitalen Fernmeldenetz (ISDN) kommunizieren zu können.

***NWSCFG**
Das NWS-Konfigurationsobjekt (*NWSCFG) definiert Attribute, die von einer NWS-Beschreibung (NWSD) mit iSCSI-Anschluss dazu verwendet werden, Verbindungssicherheit, Hardware und Konfiguration eines fernen Systems sowie Serviceprozessorattribute zu beschreiben.

***NWSD**
Das Objekt Netzwerk-Server-Beschreibung (*NWSD) enthält Informationen zur Konfiguration eines Netzwerk-Servers, Informationen, die vom System benötigt werden, um über die Systemschnittstelle kommunizieren und die Systemschnittstelle für einen FSIOP (File Serving Input/Output Processor) beschreiben zu können.

***OUTQ**
Das Objekt Ausgabewarteschlange (*OUTQ) enthält eine Liste von Spool-Dateien, die über ein Ausgabeprogramm an eine Ausgabeeinheit geschrieben werden.

***OVL**
Das Objekt Schablone (*OVL) enthält elektronische Versionen vordefinierter Informationen, z. B. von Briefköpfen etc.

***PAGDFN**
Das Objekt Seitendefinition (*PAGDFN) enthält Formatsteuerzeichen für Zeilendaten, Zeilenanzahl, Schriftartdruckrichtung und die Anordnung der Felder auf einer Seite.

***PAGSEG**
Das Objekt Seitensegment (*PAGSEG) enthält eine Darstellung der Standardteile einer Seite (z. B. Standardabsatz- und Standardunterschriftsinformationen).

***PDFMAP**
Eine PDF-Maske (*PDFMAP) ist ein von PSF verwendetes Objekt, das Spool-Dateiattributen Aktionen zuordnet, die beim Konvertieren einer Spool-Datei in eine PDF-Datei ausgeführt werden. Dazu gehört das Versenden als E-Mail, das Speichern der PDF-Datei im IFS oder das erneute Spoolen der PDF-Datei.

***PDG**
Das Objekt Druckdeskriptorgruppe (*PDG) enthält Druckdeskriptoren, die Benutzerauswahlmöglichkeiten zum Drucken enthalten.

***PGM**
Das Objekt Programm (*PGM) enthält eine Reihe von Anweisungen, die einem Computer mitteilen, wo sich eine Eingabe befindet, wie diese verarbeitet werden soll und wohin die Ergebnisse gestellt werden sollen. Programme können in verschiedenen Sprachen abgefasst sein (z. B. C, CL oder RPG).

***PNLGRP**
Das Objekt Anzeigengruppe (*PNLGRP) enthält Anzeigeninformationen oder Onlinehilfetexte, die an einem Bildschirm dargestellt werden.

***PRDAVL**
Das Produktverfügbarkeitsobjekt (*PRDAVL) enthält Datensätze aller bekannten IBM Software- und Kundenprodukte, die für das System zumindest definiert sind.

***PRDDFN**
Das Objekt Produktdefinition (*PRDDFN) enthält Produktinformationen, die geladen werden, wenn ein Lizenzprogramm auf dem System installiert wird. Zu diesen Informationen gehören Sonderumgebungen, Programmiercode und Produktsteuerinformationen, z. B. Programmname, Produkt-ID, Copyright und Modifikationsstufe.

***PRDLOD**
Das Objekt Produktlademodul (*PRDLOD) enthält Produktinformationen, die geladen werden, wenn ein Lizenzprogramm auf dem System installiert wird. Diese Informationen umfassen detaillierte Angaben u. a. zu Standort und Inhalt.

***PSFCFG**
Das Objekt PSF-Konfiguration (*PSFCFG) enthält zusätzliche Einheitenkonfigurationsdaten für einen AFP-Drucker. Diese Daten werden zusammen mit den Daten verwendet, die bei der mit dem Befehl CRTDEVPRT (Einheitenbeschreibung erstellen – Drucker) erstellten Druckereinheitenkonfiguration angegeben wurden.

***QMFORM**
Das Objekt Abfrageverwaltungsformular (*QMFORM) enthält das Format einer Abfrage oder eines Berichts, die/der vom Benutzer des Lizenzprogramms IBM Query für IBM i und der Systems Application Architecture (SAA) definiert wurde.

***QMQRY**
Das Objekt Abfrageverwaltungsabfrage (*QMQRY) enthält die Daten, die von einer Abfrage oder einem Bericht zurückgegeben werden sollen, die/der von einem Benutzer des Lizenzprogramms IBM Query für IBM i und der Systems Application Architecture (SAA) definiert wurde.

***QRYDFN**
Das Objekt Abfragedefinition (*QRYDFN) enthält Informationen über eine Abfrage oder einen Bericht, die/der von einem Benutzer des Lizenzprogramms IBM Query für IBM i definiert wurde.

***RCT**
Das Objekt Referenzcodeumsetztabelle (*RCT) enthält Informationen zur Unterstützung bei der Problemanalyse von Hardwarefehlern.

***SBSD**
Das Objekt Subsystembeschreibung (*SBSD) enthält eine Definition eines Subsystems und seiner Betriebsumgebung im System.

***SCHIDX**
Das Objekt Informationssuchindex (*SCHIDX) enthält Informationen, die von der Suchfunktion (STRSCHIDX) verwendet werden.

***SPADCT**
Das Objekt Benutzerdefiniertes Wörterverzeichnis (*SPADCT) enthält eine Liste von Wörtern, Synonymen und Silbentrennungsangaben.

***SQLPKG**
Das Objekt SQL-Paket (*SQLPKG) enthält Informationen, die von SQL zum Durchführen einer Anforderung eines Programms oder eines fernen Systems benötigt werden.

***SQLUDT**
Ein SQL-Objekt der Art UDT (User Defined Type) (*SQLUDT) enthält Informationen zu einer bestimmten Datenart, die in SQL mit der Anweisung CREATE DISTINCT TYPE erstellt wird. Diese Informationen werden von SQL verwendet, um Operationen unter Verwendung dieser speziellen Datenart durchzuführen.

***SQLXSR**
Ein *SQLXSR-Objekt (SQL Extensible Markup Language Schema Repository) enthält Informationen zur Verwendung einer XML-Spalte in einer Tabelle. Die Informationen im Objekt SQLXSR enthalten die Definition zur Strukturierung der Daten in der XML-Spalte der Tabelle. Beim Einfügen von Daten in die XML-Spalte werden sie anhand der Definition im Objekt SQLXSR validiert.

***SRVPGM**
Ein Serviceprogrammobjekt (*SRVPGM) enthält Anweisungen, die einem Computer mitteilen, wo sich die Eingabe befindet, wie diese verarbeitet werden soll und wohin die Ergebnisse gestellt werden sollen. Ein Serviceprogramm wird mit dem Befehl CRTSRVPGM (Serviceprogramm erstellen) erstellt. Es kann nicht auf dieselbe Weise wie ein Objekt *PGM aufgerufen werden.

***SSND**
Das Objekt Sitzungsbeschreibung (*SSND) enthält für die Funktion Jobferneingabe (RJE) alle Objekte und Einheiten für die RJE-Betriebsumgebung.

***SVRSTG**
Das Objekt Server-Speicherbereich (*SVRSTG) enthält Systemdateien und Daten, die von einer Netzwerk-Server-Beschreibung benutzt werden.

***S36**
Ein Objekt IBM System /36 (*S36) enthält Konfigurationsdaten, die von der System /36-Umgebung zum Ausführen von System /36-Jobs auf einem IBM i-System verwendet werden.

***TBL**
Das Objekt Umsetztabelle (*TBL) enthält eine Gruppe von Werten für Byte-to-Byte-Daten, oder zum Definieren einer Sortierfolge.

***TIMZON**
Das Objekt Zeitzonenbeschreibung (*TIMZON) enthält Informationen zur Berechnung der Ortszeit.

***USRIDX**
Das Objekt Benutzerindex (*USRIDX) enthält Suchfunktionen und ordnet Daten automatisch gemäß ihrem Wert an.

***USRPRF**
Das Objekt Benutzerprofil (*USRPRF) enthält Angaben, die einen Benutzer gegenüber dem System kennzeichnen, und steuert, welche Systemfunktionen und Anzeigen dem Benutzer zur Verfügung stehen.

***USRQ**
Das Objekt Benutzerwarteschlange (*USRQ) enthält eine Liste der Nachrichten für andere Anwendungsprogramme.

***USRSPC**
Das Objekt Benutzerbereich (*USRSPC) enthält eine große Menge Daten, die vom Benutzer geändert und verwendet werden können.

***VLDL**
Das Objekt Prüfliste (*VLDL) enthält Daten, die eine ID beinhalten, Daten, die beim Speichern verschlüsselt werden, und Daten im freien Format.

***WSCST**
Das Objekt Datenstationsbenutzeranpassung (*WSCST) enthält angepasste Tabellen mit Informationen über lokale und ferne Datenstationssteuereinheiten zur Unterstützung weiterer Bildschirme und Drucker oder neudefinierter Tastaturen.

9.12.3
Seite 12

9.12.4 Integriertes Dateisystem (IFS)

Sie wissen aus den vorherigen Kapiteln, dass alle i5/OS-Objekte in Bibliotheken organisiert werden. Dabei könnte leicht der Eindruck entstehen, dass dieses Bibliothekskonzept das alleinige Ordnungssystem auf einem i5-Server ist.

Doch auf einem i5-Server müssen nicht nur klassische i5/OS-Daten gespeichert werden; auch Videos, Bilddateien u. v. m. sollten auf einem Datenbankserver abgelegt werden. Auch muss es möglich sein, i5/OS-Daten anderen Systemen zur Verfügung zu stellen. Andere Systeme haben aber andere Dateisysteme – und jedes dieser Systeme hat eine individuelle logische Struktur und vor allem eigene Regeln, wenn es um den Datenzugriff geht. Aus diesem Grund unterstützt das Betriebssystem i5/OS bereits seit einigen Jahren unterschiedliche Dateisysteme, die alle unter dem Begriff Integrated File System (IFS) vereint wurden. Dabei unterstützt das IFS sowohl das Bibliothekskonzept eines i5-Servers, kennt aber auch die Eigenschaften eines Windows- oder Unix-Dateisystems. Nur dadurch ist es möglich, dass Sie beispielsweise auf dem i5-Server eine Unix-Shell öffnen können – ohne eine Unix- oder Linux-Partition einzurichten. Geben Sie hierzu einfach den folgenden Befehl auf einer i5/OS-Befehlszeile ein:

```
CALL QP2TERM
```

Daraufhin öffnet sich ein neues Fenster, das die Eingabe diverser Unix-Befehle erlaubt:

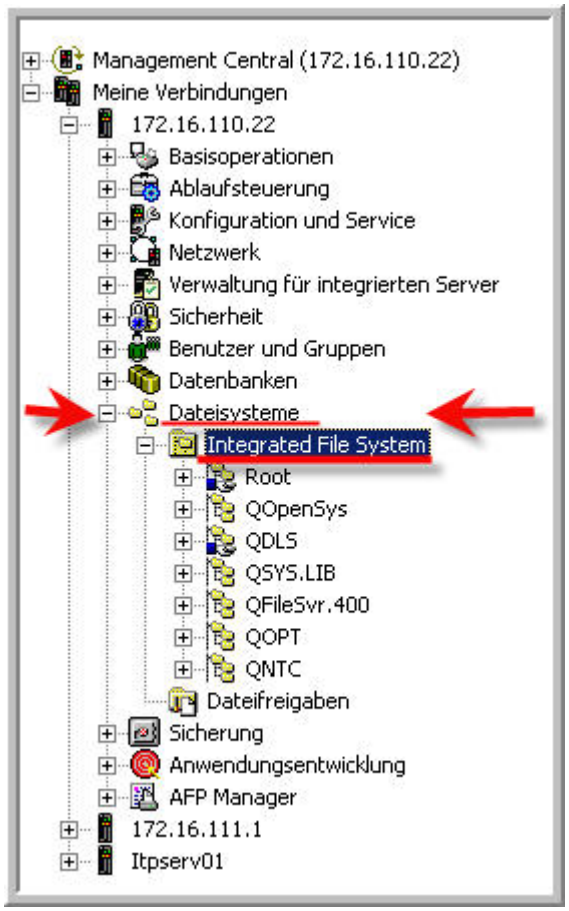
```
> ls
  bin       include   lbin      lpp       share
  ccs       krb5      lib       sbin      vacpp
  $


===>
```

Unix-Shell

Das IFS sehen Sie im 5250-Umfeld immer nur partiell; auch die Administration dieser Dateisysteme ist in diesem 5250-Umfeld recht aufwendig.

9.12.4
Seite 2

IBM hat aber die Dateisysteme als eigenständigen Bereich in den iSeries Navigator integriert. Öffnen Sie im iSeries Navigator die Verbindung zu Ihrem Server und erweitern Sie anschließend den Eintrag: „Dateisysteme“.



iSeries Navigator – Dateisysteme

Der Bereich „Dateisysteme“ im iSeries Navigator dient der Verwaltung des „Integrated File Systems“(IFS) im i5/OS. Die gezeigte Struktur ist vergleichbar mit einem PC- oder Unix-System und sollte daher schnell zu erlernen sein. Durch eine hierarchische Struktur werden die Daten logisch angeordnet, so dass – eine vernünftige Struktur vorausgesetzt – auf sie optimal zugegriffen werden kann.

Wenn Sie – wie ich es bereits getan habe – den Eintrag „Integrated Files System“ erweitern, sehen Sie eine Liste aller verfügbaren Dateisysteme für die Sie berechtigt sind. Schauen wir uns zunächst die einzelnen Verzeichnisse im Überblick an:

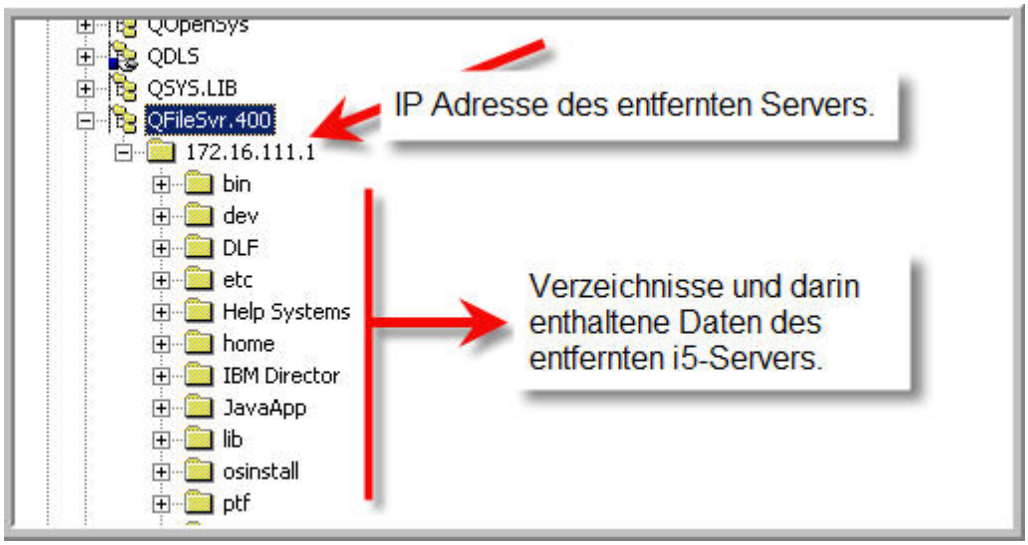
Verzeichnis „ROOT“
Root ist das sogenannte Windows- oder OS/2-kompatible Dateisystem. Wenn Sie hier Daten speichern, werden die Daten im ASCII-Format als „Streamfiles“ abgelegt. Die Namenskonventionen und Eigenschaften dieses Dateisystems entsprechen denen der Windows-Welt.

Verzeichnis „QOpenSys“
Dieses Dateisystem ist Unix-kompatibel. Daten, die hier gespeichert werden, sind ebenfalls im ASCII-Format als sogenannte Streamfiles vorhanden. Allerdings entsprechen die Namenskonventionen denen der Unix-Welt.

Verzeichnis „QDLS“
Das „Document Library System“(QDLS) beinhaltet heute vorwiegend PC-Dateien. Früher wurden in diesen Verzeichnissen auch Office-Vision-Dokumente gespeichert. Der Unterschied zum Dateisystem „ROOT“ besteht vor allem im verwendeten Zeichensatz: Daten in „QDLS“ werden nämlich im EBCDIC-Format als Streamfiles abgelegt. Die Namenskonventionen in diesem Bereich entsprechen denen der MS-DOS-Welt.

Verzeichnis „QSYS.LIB“
Auch das Bibliothekskonzept der i5 ist nichts anderes als ein Verzeichnissystem. Dieses klassische Ordnungssystem finden Sie im Eintrag „QSYS.LIB“. Daten, die hier gespeichert sind, werden im EBCDIC-Format als sogenannte Record-Files abgelegt. Die Namenskonventionen entsprechen denen der i5/OS-Welt.

Verzeichnis „QfileSvr.400“
„QfilsSrv ist ein Brückenverzeichnis. Wenn Sie unterhalb von QfileSvr.400 ein Verzeichnis erzeugen, das den Host-Namen oder die IP-Adresse eines entfernten iSeries-Servers trägt, gelangen Sie automatisch in das „Integrated File System“ des entfernten Systems.



Wirkungsweise des Verzeichnisses „QFileSvr.400“

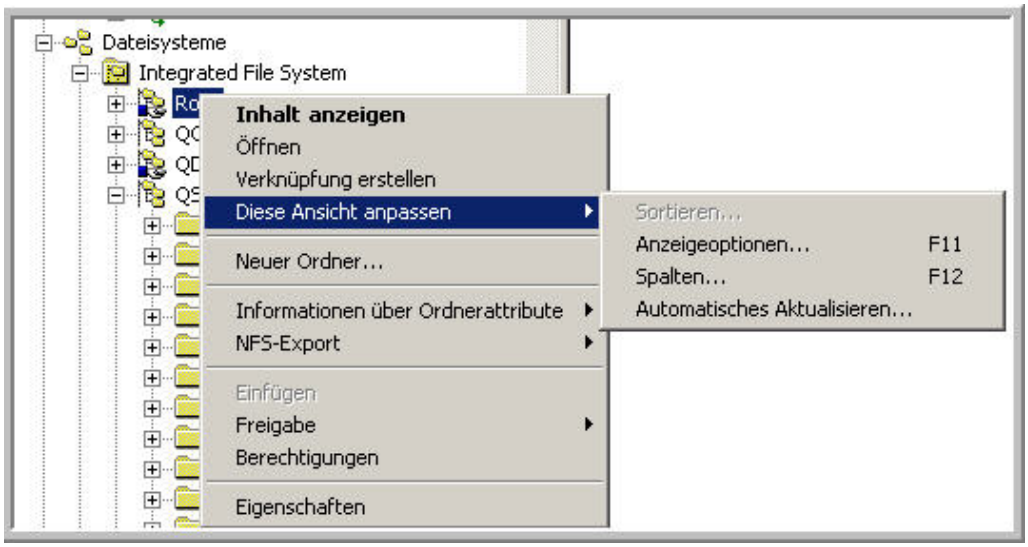
Verzeichnis „QOPT“
„QOPT“ erlaubt den Zugriff auf optische Speichermedien. So erhalten Sie Zugriff auf das CD-Rom-Laufwerk Ihres Servers.

Verzeichnis „QNTC“
Auch das Verzeichnis „QNTC“ ist ein Brückenverzeichnis zu anderen Systemen. Es ermöglicht den Zugriff auf andere Windows-Systeme. Wenn Sie unterhalb von „QNTC“ ein Verzeichnis mit dem Computernamen eines im Netzwerk befindlichen Windows-Systems erzeugen, so erhalten Sie hierüber einen Zugriff auf die freigegebenen Ressourcen dieses Systems. Voraussetzung dafür ist allerdings eine lauffähige Konfiguration des iSeries-Net Servers.

Nachdem wir nun die einzelnen Verzeichnisse im Überblick kennen, ist es an der Zeit, herauszufinden, welche Funktionen das IFS bereitstellt.

9.12.5 Grundfunktionen – „Integriertes Dateisystem"

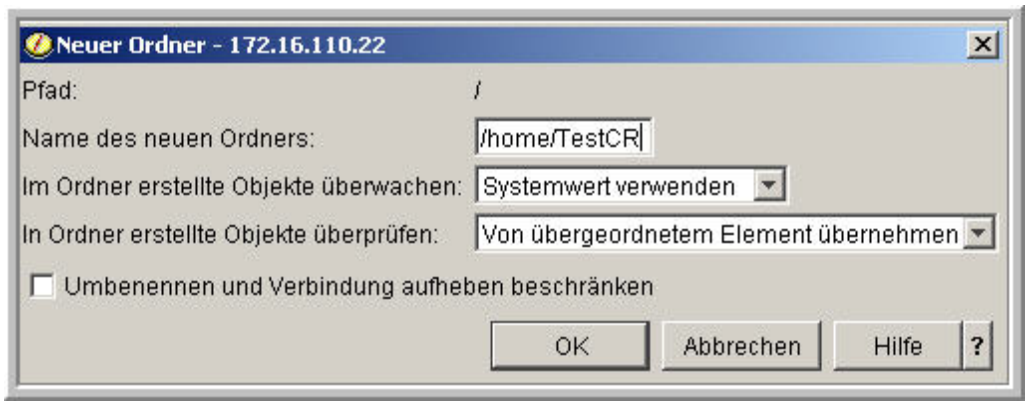
Ich werde sicherlich im Folgenden nicht jedes Kontextmenü und jede Funktion detailliert erläutern können. Dies würde einerseits den Rahmen dieses Buchs sprengen, andererseits würden sich viele Erklärungen wiederholen, da häufig die Kontextmenüs der verschiedenen Verzeichnissysteme sowie der in den Verzeichnissen gespeicherten Objekte identisch aufgebaut sind. Schauen wir uns zunächst stellvertretend das Kontextmenü des Dateisystems „ROOT" an:



Kontextmenü des Dateisystems „ROOT"

Der Kontextmenüaufbau ist für alle Dateisysteme identisch. Wie in den anderen Kontextmenüs des iSeries Navigators finden wir zunächst die **Standardfunktionen: „Inhalte anzeigen", „Verknüpfungen auf dem Desktop erstellen"** usw. Auch die Ansicht lässt sich wie in anderen Anzeigen individuell anpassen. Sie können Filter setzen („Anzeigeoptionen"), um das angezeigte Datenvolumen einzuschränken, aber auch die Spaltenreihenfolgen im Ausgabebildschirm individuell bestimmen.

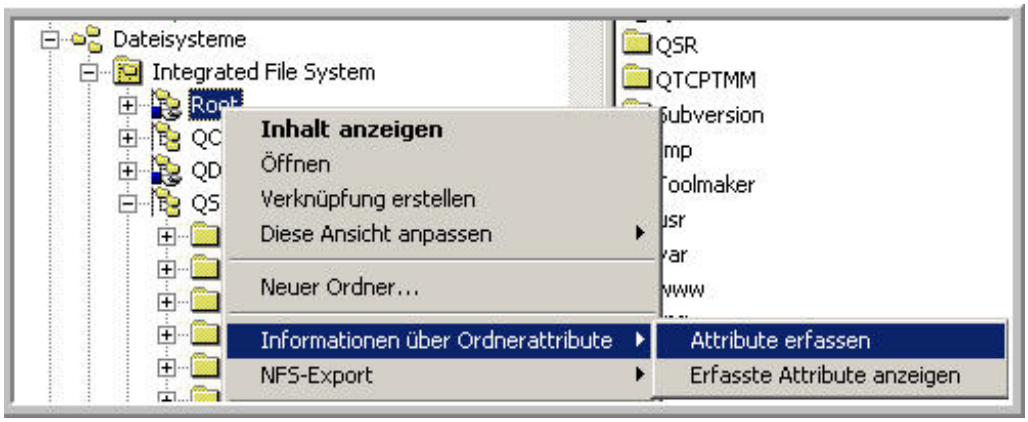
Auch der **Eintrag „Neuer Ordner“** spricht für sich. Wählen Sie diese Funktion, so öffnet sich folgender Dialog:



Neuer Ordner erstellen

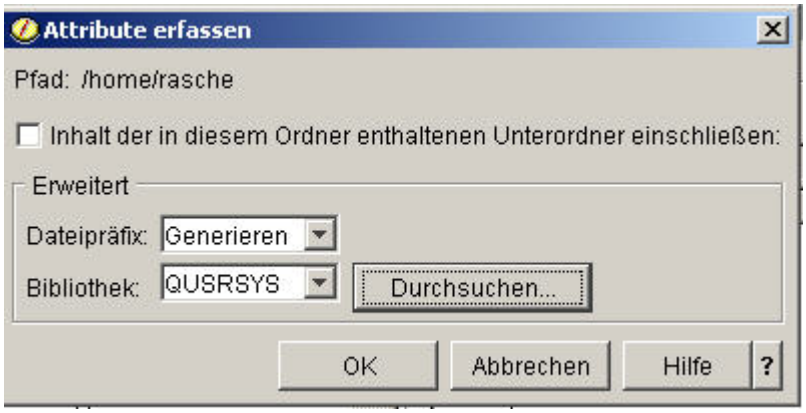
In das Eingabefeld tragen Sie den Namen des neuen Ordners ein. In diesem Fall wird der Ordner „TESTCR“ im „ROOT“-Verzeichnis unterhalb des Ordners „HOME“ erstellt. Beabsichtigen Sie – so wie ich es getan habe –, den Ordner unterhalb von „/Home“ zu erstellen, dann müssen Sie entweder im oben gezeigten Dialog den kompletten Pfad eintragen oder das Kontextmenü des entsprechenden Unterordners verwenden. Ob i5/OS einen Überwachungseintrag an das Systemprotokolljournal (Objekt QAUDJRN in der Bibliothek QSYS) sendet, wenn das Objekt verwendet oder geändert wird, bestimmt die Option „Im Ordner erstellte Objekte überwachen“. Weiterführende Informationen hierzu enthält das Kapitel 2.3.2.4. Die Option „In Ordner erstellte Objekte überprüfen“ gibt an, ob die im Ordner erstellten Objekte überprüft werden, wenn Exit-Programme entsprechend registriert sind. Diese Option kann nur für Dateien in den Dateisystemen „Root“ (/), „QOpenSys“ sowie in benutzerdefinierten Dateisystemen angegeben werden. Obwohl dieses Attribut für Objekte in i5/OS-Bibliotheken (Ordnertyp 1) definiert werden kann, werden nur Objekte in Ordnern vom Typ 2 überprüft.

Kommen wir wieder zurück zum ursprünglichen Kontextmenü:



„Informationen über Ordnerattribute“

Sie können über die im Ordner gespeicherten Objekte **„Attribute erfassen“** lassen. Wenn Sie die Attribute erfassen lassen, öffnet sich zunächst ein neuer Dialog:



„Attribute erfassen“

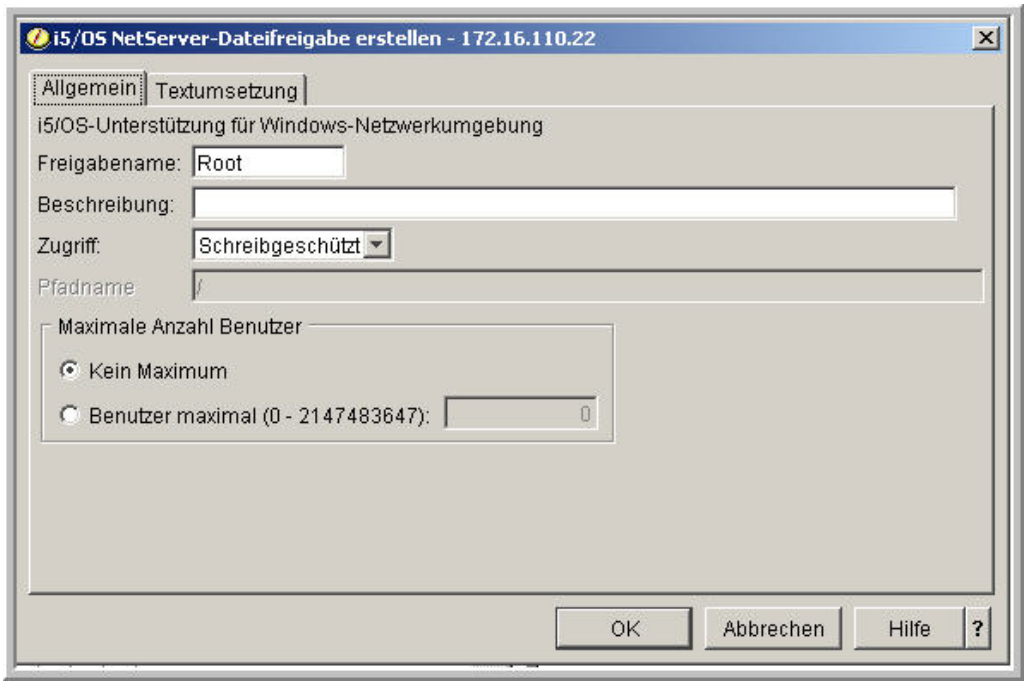
Im Dialog legen Sie ein Dateipräfix und die Bibliothek fest, um die Daten zu speichern. Anschließend erhalten Sie zwei Dateien, die die generierten Daten enthalten. Diese Daten enthalten Angaben über die Größe der gespeicherten Objekte, Datum der Erstellung, Datum der letzten Änderung u.v.m. Probieren Sie es einfach einmal aus. Die erfassten Daten lassen sich im Übrigen sehr einfach über SQL anzeigen und natürlich auch individuell auswerten.

Wenn Sie mit Unix-Servern arbeiten, können Sie das gewählte Dateisystem mit der **Funktion „NFS-Export“** in die Unix-Umgebung exportieren.

Die **Kontextfunktion „Einfügen“** ist nur verfügbar, wenn Sie zuvor ein Objekt in das Windows-Clipboard kopiert haben. Anschließend kann es mithilfe der Funktion „Einfügen“ in einen anderen Ordner des Dateisystems kopiert werden.

9.12.5
Seite 4

Mit der **Funktion „Freigabe“** sollten wir uns ein wenig ausführlicher beschäftigen. Hier arbeiten Sie mit Objekten und Funktionen des i5/OS Netservers. Der Netserver ist seit OS/400 V4R2 eine Komponente, die die NETBIOS-Schnittstelle im TCP/IP-Protokollstapel aktiviert und damit den i5-Server Microsoft-Netzwerk-kompatibel macht. Wählen Sie im Kontextmenü eines Verzeichnisses die Funktion „Freigabe“, dann öffnet sich ein entsprechender Dialog, der es Ihnen ermöglicht, den Ordner freizugeben.



Dateifreigaben erstellen

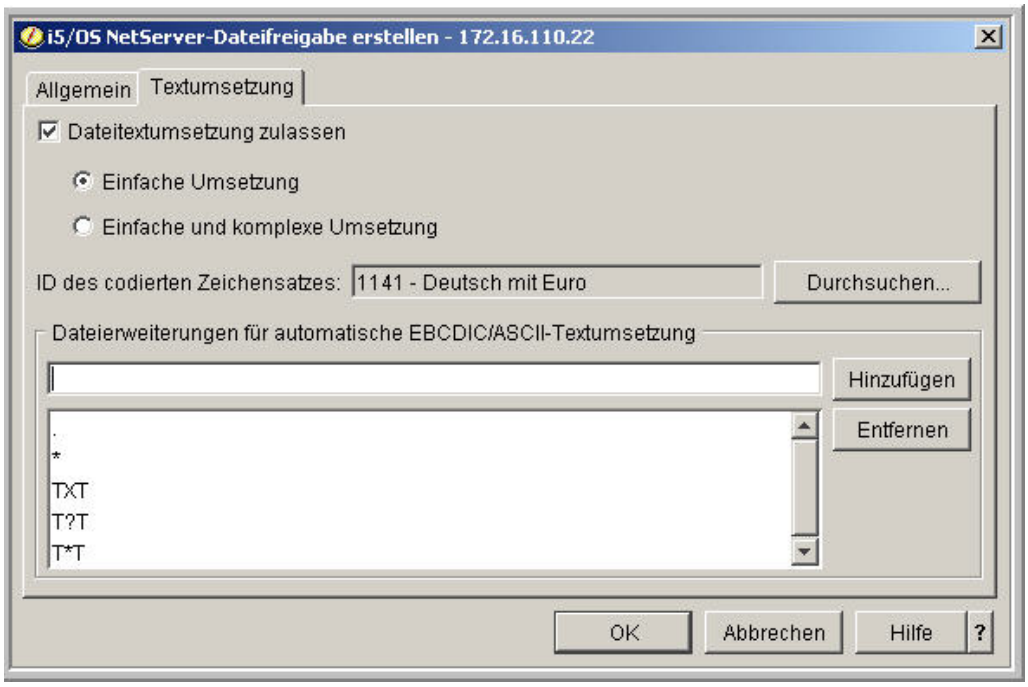
Als Erstes müssen Sie einen Freigabenamen wählen. Vorgeschlagen wird stets der Name der freizugebenden Ressource. Auch einen beschreibenden Text können Sie hinzufügen. Für den Zugriff haben Sie die Wahl zwischen:

– Lesezugriff:
  Nur lesender Zugriff ist über diese Freigabe möglich.

– Schreib-/Lesezugriff:
  Lesender und schreibender Zugriff ist über die Freigabe möglich.

Außerdem können Sie bestimmen, wie viele Benutzer die Ressource gleichzeitig verwenden dürfen.

Im Register „Textumsetzung“ wird die Übersetzung von EBCDIC-Inhalten nach ASCII gesteuert.



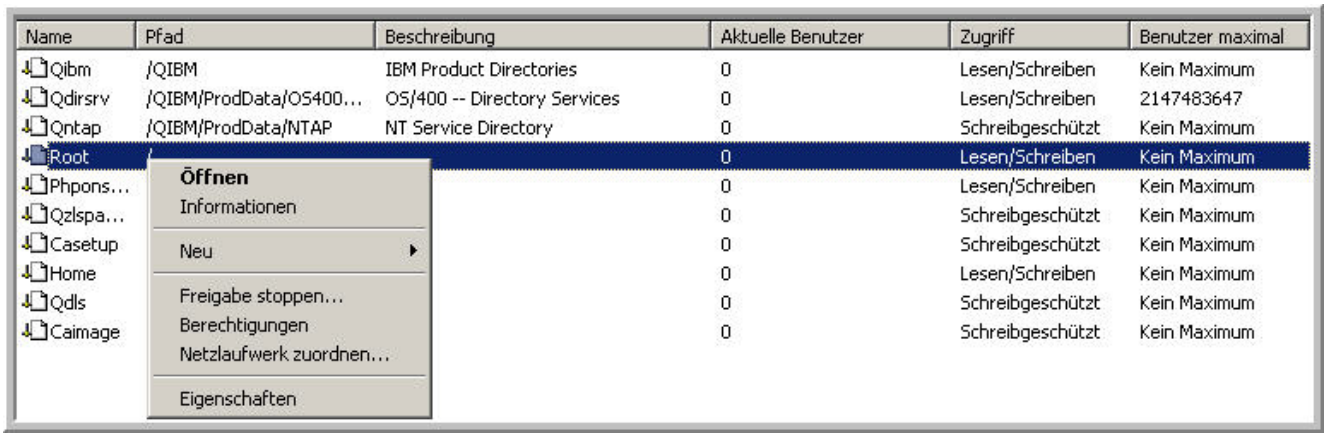
Dateifreigaben – Textumsetzung

Im Vordergrund steht hier die automatische Zeichenumsetzung. Zunächst müssen Sie aber die automatische Textumsetzung aktivieren, indem Sie die Option „Dateitextumsetzung zulassen“ markieren. Wählen Sie diese Option aus, um die Unterstützung für die automatische Textumsetzung für Dateien mit Erweiterungen zu aktivieren. Die betroffenen Dateien geben Sie anschließend im Feld „Dateierweiterungen für automatische EBCDIC-ASCII-Umsetzung“ an. Wenn Sie diese Option nicht zulassen, sind alle anderen Felder deaktiviert. Welche CCSID vom System zum Umsetzen der Objekte von EBCDIC in ASCII verwendet wird, können Sie individuell bestimmen, indem Sie auf die Schaltfläche „Durchsuchen…“ klicken. Abschließend definieren Sie noch, welche Objekte umgesetzt werden sollen. Hierzu erstellen Sie Schablonen für entsprechende Dateierweiterungen. Folgende Möglichkeiten stehen Ihnen zur Verfügung:

17. Ergänzung 12/2008

Zeichen	Bedeutung
*	Alle Dateien – unabhängig von deren Endung – werden umgesetzt.
.	Es werden nur Dateien umgesetzt, die keine Dateiendung haben.
Beliebige Zeichenfolge	Alle Dateien mit der hier genannten Dateiendung werden umgesetzt. Wenn Sie beispielsweise die Zeichenfolge „TXT“ wählen, dann würde die Datei „BSP.TXT“ von EBCDIC nach ASCII konvertiert werden.
Platzhalter: ? oder *	Innerhalb der Zeichenfolge können Sie Platzhalter verwenden, um einzelne oder mehrere Zeichen zu maskieren. Sie könnten beispielsweise die Endung „T?T“ für die Umsetzung erfassen. Eine Datei mit der Endung „TBT“, wird dann automatisch umgesetzt werden. Das Fragezeichen („?“) steht damit stellvertretend für ein Zeichen. Wenn mehrere Zeichen maskiert werden sollten, dann müssen Sie einfach anstelle des Fragezeichens das Sternzeichen („*“) verwenden.

Wenn alle Eingaben fertig sind, klicken Sie auf „OK“, um die Freigabe zu erstellen. Alternativ steht Ihnen aber auch der Eintrag „Dateifreigaben“ zur Verfügung. Wenn Sie den Eintrag „Dateifreigaben“ markieren, können Sie auf der rechten Bildschirmseite alle freigegebenen Objekte sehen.



Kontextmenü der Dateifreigaben

Zusätzlich sehen Sie, wie viele Benutzer derzeit mit dem freigegebenen Objekt arbeiten. Außerdem werden die Freigabeeigenschaften dargestellt. Wenn Sie das Kontextmenü einer Freigabe öffnen, dann stehen weitere Möglichkeiten der Bearbeitung zur Verfügung:

Öffnen: Öffnet das mit der Freigabe verbundene Verzeichnis direkt im Microsoft Explorer.

Informationen: Öffnet ebenfalls das mit der Freigabe verbundene Verzeichnis im Microsoft Explorer, jedoch aus der Sicht der Microsoft-Netzwerkumgebung heraus.

Neu: Erstellt eine neue Freigabe aufgrund der Eigenschaften der markierten Freigabe.

Berechtigungen: Es können Berechtigungen für die freigegebene Ressource erteilt werden, um den Zugriff auf einzelne Personen oder Personengruppen zu beschränken.

Netzwerklaufwerk zu ordnen: Ordnet einer freigegebenen Ressource ein Laufwerk auf Ihrem Desktop zu.

Netzwerklaufwerk zuordnen

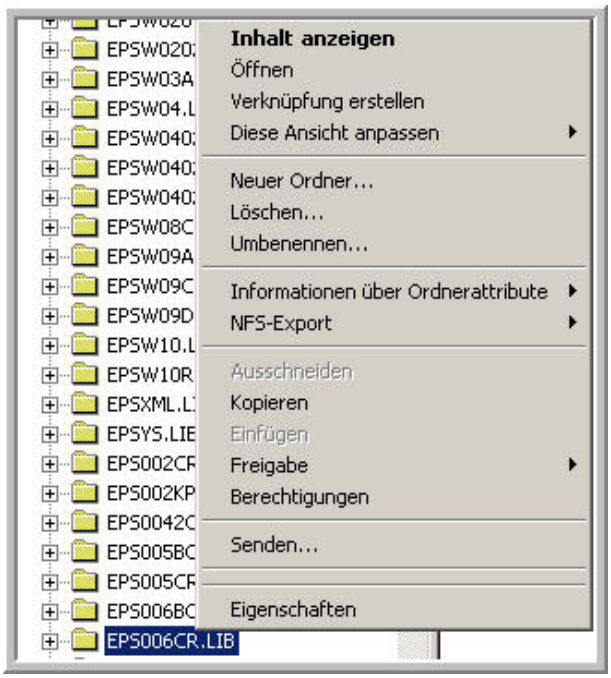
Es werden hier nur Laufwerksbuchstaben zur Verfügung gestellt, die auf Ihrem Desktop noch frei sind. Standardmäßig wird der Windows-Benutzer an die iSeries zur Verbindungsanmeldung übergeben. Sind Windows- und iSeries-Benutzer nicht identisch, dann geben Sie hier einen iSeries-Benutzer und dessen Kennwort ein. Außerdem können Sie festlegen, dass bei jedem Neustart Ihres Windows-PC die Laufwerkszuordnung automatisch erfolgen soll.

Eigenschaften: Wenn Sie nachträglich die Freigabeoptionen korrigieren wollen, müssen Sie den Dialog „Eigenschaften“ öffnen.

9.12.5
Seite 8

9.12.6 Mit Ordnern und Objekten arbeiten

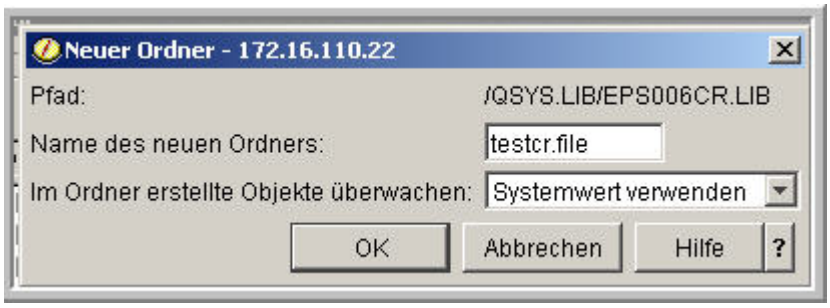
Wenn Sie sich das Kontextmenü eines Ordners ansehen, werden Sie feststellen, dass Sie viele der Funktionen bereits von den Dateiverzeichnissen her kennen:



Kontextmenü eines Ordners

Die Dateifunktionen werden lediglich um einige Funktionen ergänzt:

Neuer Ordner:
Sie können einen neuen Ordner innerhalb des Verzeichnisses erstellen. Mancher mag sich wundern, wenn er die obere Abbildung genau betrachtet. Geöffnet ist das Kontextmenü der Bibliothek „EPS006CR“. Eine Bibliothek kann doch gar keinen weiteren Ordner beinhalten? Wie soll dieser Menüpunkt dann gedeutet werden? Ganz einfach. Wenn Sie über das Kontextmenü einer Bibliothek einen Ordner erstellen, wird eine physische Datei erstellt. Sie müssen daher auch die Namenskonvention „.file“ verwenden – wie folgende Grafik zeigt:

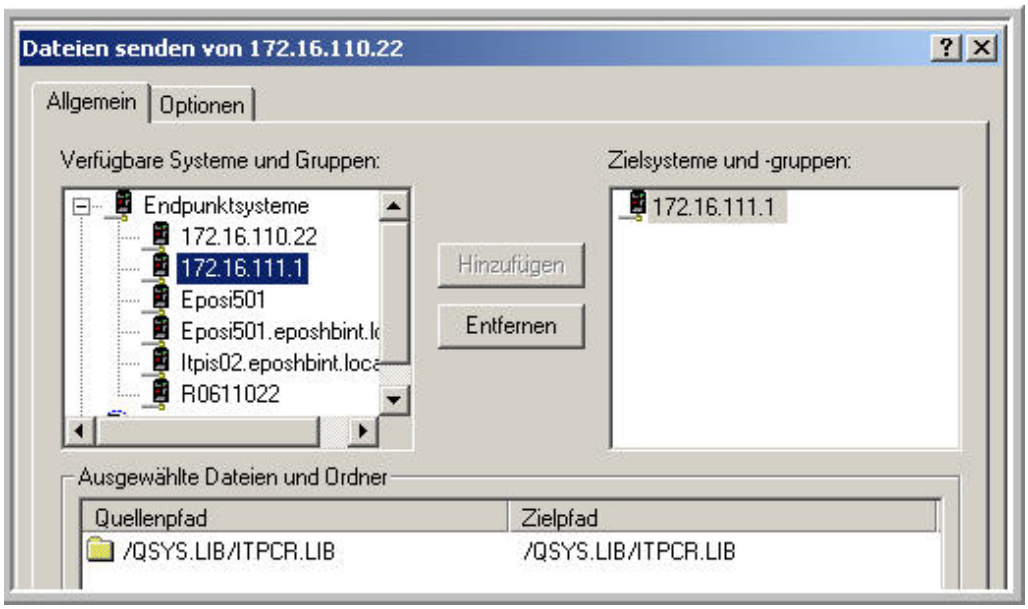


Neuer Ordner

9.12.6
Seite 2

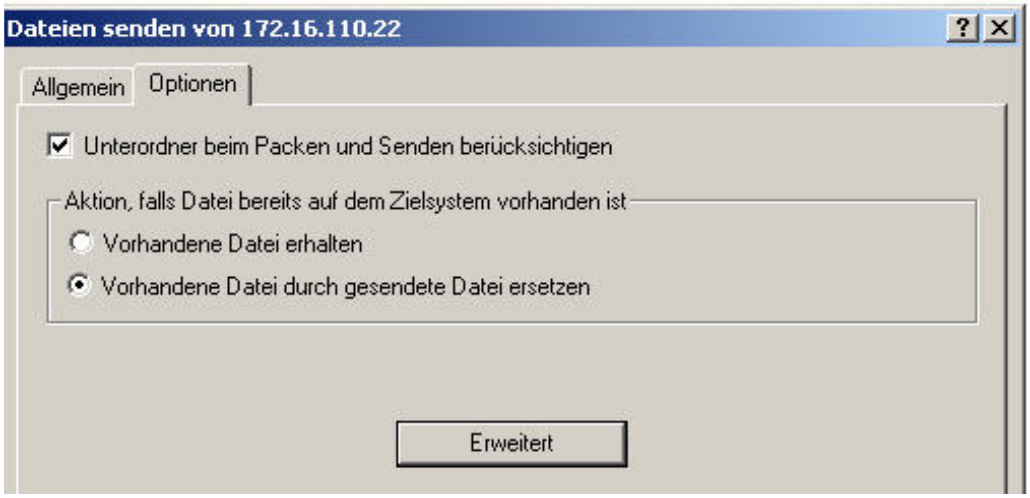
Die **Funktionen „Löschen“, „Umbenennen“, „Ausschneiden“, „Kopieren und „Einfügen“** sollten Ihnen aus der Windows-Welt hinlänglich bekannt sein; sie bergen auch im IFS keine Besonderheiten.

Senden:
Die Funktion „Senden“ ist eine „Management-Central-Funktion“. Sie erlaubt das entsprechende Verzeichnis an ein oder mehrere entfernte System zu senden. Voraussetzung für das Versenden von Dateien oder Ordnern ist demnach eine Verbindung zum Management-Central-System. Wenn die Verbindung erfolgreich hergestellt werden konnte, erscheint folgender Dialog:



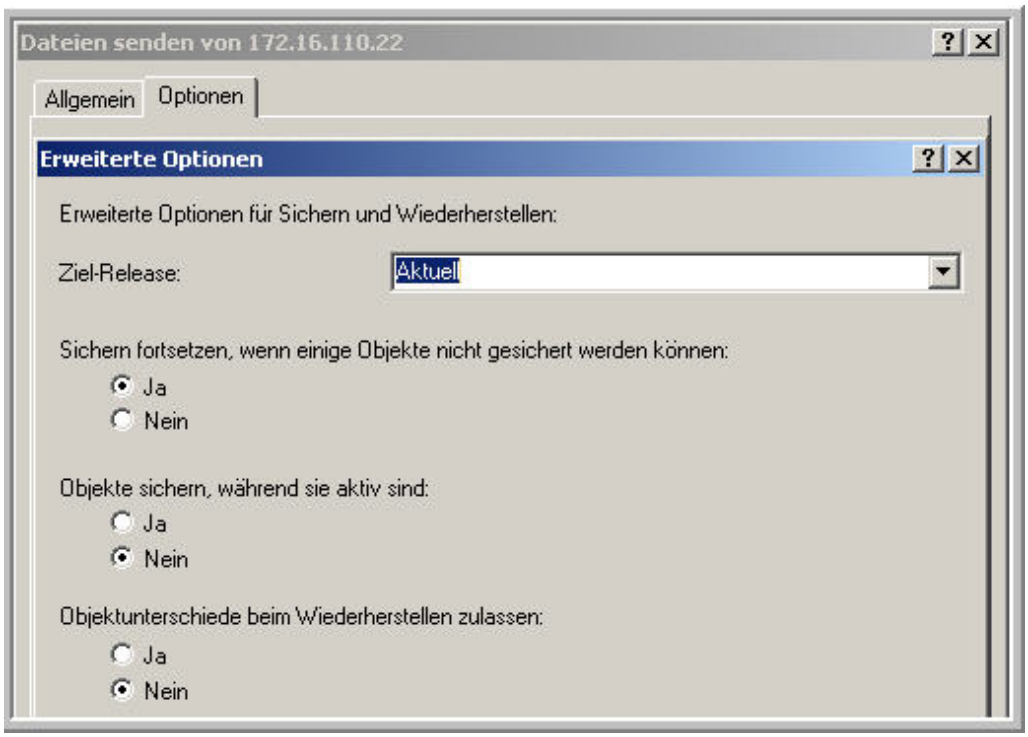
„Dateien senden“

Sie müssen lediglich das oder die Zielsysteme in der Liste der Endpunktsysteme auswählen. Die zu sendenden Objekte stehen bereits im unteren Bildschirmbereich. Das Register „Optionen“ bietet weitere Einstellungen:



Dateien senden – Optionen

Über „Optionen“ können Sie Unterordner in die Verteilung miteinbeziehen und entscheiden, was passieren soll, wenn die Daten bereits auf dem empfangenden System vorhanden sind. Zusätzlich können Sie noch den Button „Erweitert“ nutzen, der Ihnen weitere Optionen zur Verfügung stellt:

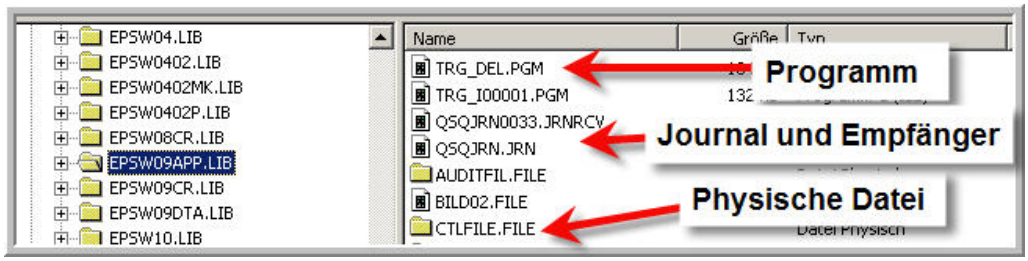


Dateien senden – Erweiterte Optionen

Sobald Sie alle Einstellungen vorgenommen haben, klicken Sie auf den Button „OK“, um die Übertragung zu starten. Den Job finden Sie anschließend im Management Central im Eintrag „Task-Aktivität“ → „Pakete und Produkte“. Hier können Sie auch prüfen, ob die Übertragung erfolgreich verlaufen ist.

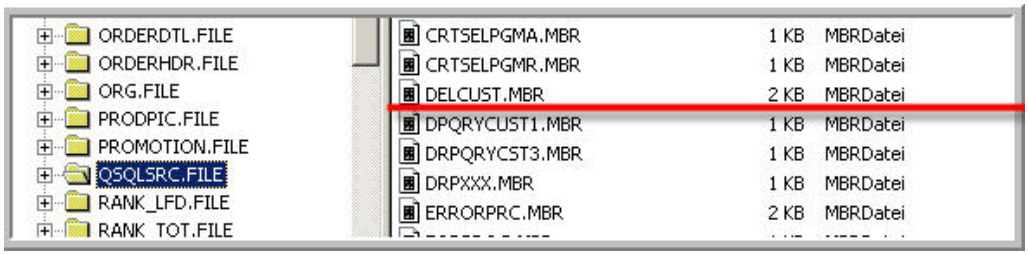
Auf Objektebene des iSeries Navigator sind sogar „Drag-and-Drop“-Funktionen aktiviert, um Dateien zu verschieben. Wenn Sie eine Datei markieren und anschließend bei gedrückter Maustaste in einen anderen Ordner verschieben, werden Sie feststellen, dass sich der Mauszeiger entsprechend verändert. Haben Sie den Zielordner erreicht, wird das Objekt in den neuen Zielordner kopiert. Die „Drag-and-Drop“-Funktion ist auch über Systemgrenzen hinweg einsetzbar. Sollten Sie Verbindungen zu zwei oder mehr Systemen unterhalten, dann expandieren Sie einfach das Dateisystem auf dem zweiten System und ziehen das zu versetzende Objekt mit der Maus auf das gewünschte Verzeichnis des zweiten Systems.

Auch mit Objekten in den i5/OS-Bibliotheken können Sie so verfahren. Hierfür müssen Sie das Dateisystem „QSYS.LIB“ erweitern. Es stellt die Bibliotheken des i5-Servers dar. Natürlich gelten hier die Namenskonventionen der eigentlichen i5-Umgebung: 10-stellige Namen, ausschließlich Großschreibung usw. Etwas gewöhnungsbedürftig ist die Darstellung der einzelnen Objektarten, die als Namenserweiterungen abgebildet werden.



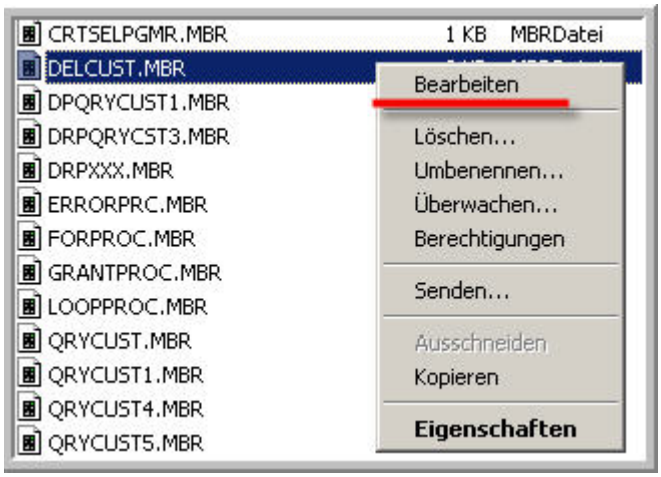
Objekte der Bibliothek „EPSW09APP.LIB“

Die Bibliothek „EPSW09APP“ heißt im IFS „EPSW09APP.LIB“. In der Bibliothek befindet sich das Programm „TRG_DEL“, das im IFS „TRG_DEL.PGM“ heißt. Aus der physischen Datei „CTLFILE“ wird „CTLFILE.FILE“ usw. Innerhalb der Bibliothek „EPSW09APP.LIB“ existiert auch die Quellendatei „QSQLSRC“, in der sich verschiedene SQL-Skriptdateien als „Member“ befinden. Mit diesen Membern will ich jetzt arbeiten:



Mit Membern einer Quellendatei arbeiten

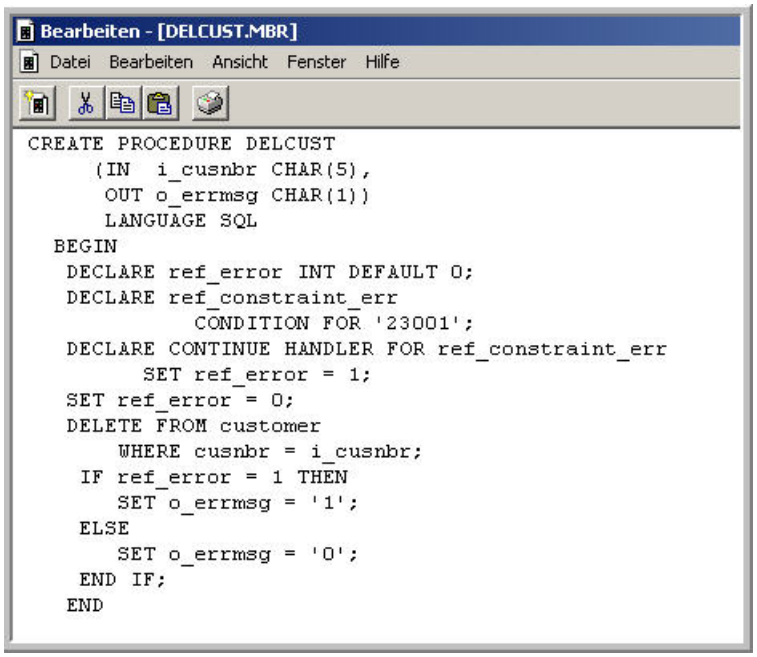
Sie können in der Abbildung sehen, dass es im Verzeichnis „QSQLSRC.FILE“ das Objekt „DELCUST.MBR“ gibt. Hierbei handelt es sich um eine Teildatei, die ich öffnen und editieren möchte. Für die Teildatei fordere ich zunächst das Kontextmenü an.



Kontextmenü der Teildatei

Die einzelnen Menüpunkte sind in den vorherigen Abschnitten hinlänglich erklärt, so dass ich nur auf die Auswahl „Bearbeiten“ eingehen werde.

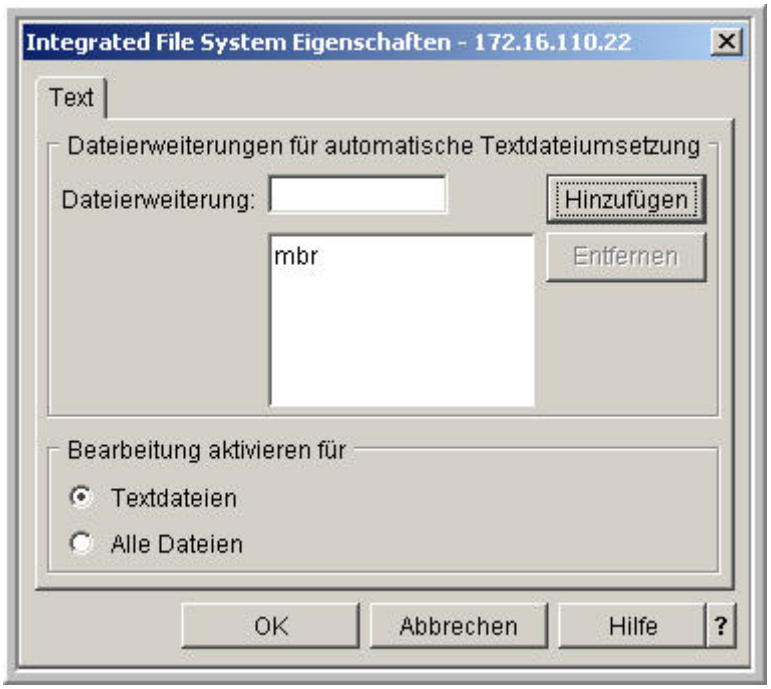
Wenn ich diese Auswahl treffe, dann öffnet sich der Editor des iSeries Navigator, mit dem Quellentexte bearbeitet werden können.



iSeries Navigator-Editor

Diesen Editor dürfen sie natürlich nicht mit SEU verwechseln. Syntaxprüfungen oder ähnliches sind diesem Editor vollkommen unbekannt. Sollten Sie im Kontextmenü die Auswahl „Bearbeiten“ deaktiviert finden, so kann dies unterschiedliche Ursachen haben:

1. Vielleicht sind Sie nicht berechtigt, mit dem Member zu arbeiten. In diesem Fall müssen zunächst die entsprechenden Rechte vergeben werden.
2. In den Eigenschaften des Integrated File System ist die Namenserweiterung für die Bearbeitung der Textfiles nicht angegeben. Öffnen Sie zur Überprüfung die Eigenschaften des Verzeichnisses „Integrated File System“. Daraufhin sollte der folgende Dialog erscheinen:



Eigenschaften des IFS

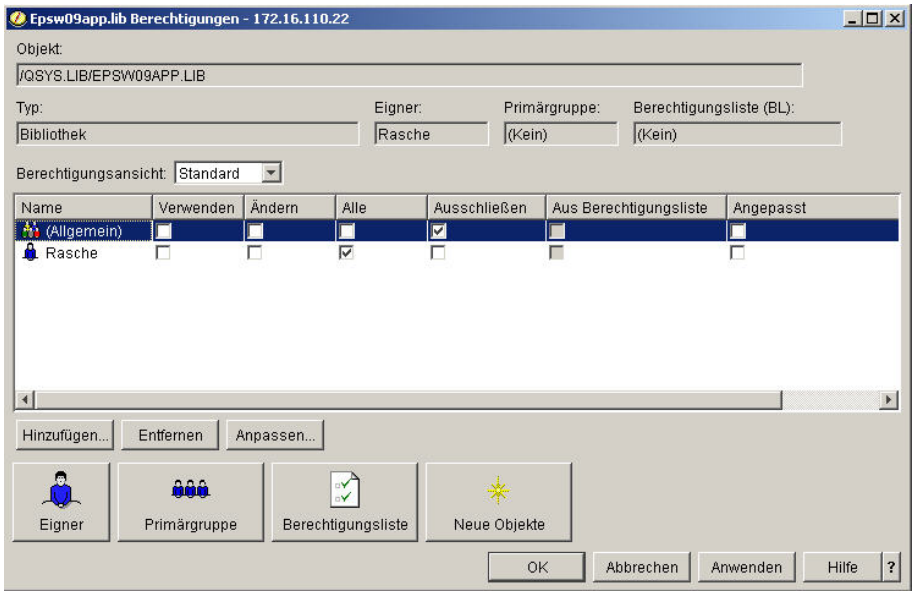
Dieser Dialog wird benötigt, um die Bearbeitung von Text- und Datendateien mit dem Editor des iSeries Navigator im Integrated File System übergreifend zu steuern. Sie sehen in der Abbildung oben, dass Textdateien mit der Namenserweiterung „.mbr“ direkt verarbeitet werden können. Wenn das Eigenschaftenfenster nicht die entsprechende Dateierweiterung enthält, können Sie die Teildatei auch nicht bearbeiten.

Wenn keiner der genannten Gründe zutrifft und dennoch die Funktion „Bearbeiten“ deaktiviert ist, greifen Sie eventuell auf eine Textdatei im Streamfile-Format zu und haben in den Eigenschaften für das Integrated File System die Option „Textdateien“ anstatt „Alle Dateien“ aktiviert. In diesem Fall müssen Sie die Eigenschaften des IFS entsprechend ändern.

Zum Schluss muss noch eine Funktion erwähnt werden, die bislang in allen Kontextmenüs vorhanden war – über die wir aber bisher nicht gesprochen haben.

Funktion „Berechtigungen“

Um im „Integrated File System“ mit Berechtigungen zu arbeiten, werden in den Kontextmenüs der diversen Hierarchiestufen entsprechende Auswahlen zur Verfügung gestellt. Wenn Sie diese Auswahl treffen, wird der nachfolgende Dialog geöffnet:



Dialog „Berechtigungen“

9.12.6
Seite 8

Dieser Dialog teilt sich in mehrere Bereiche auf. Im oberen Bereich sehen Sie das betroffene Objekt sowie den Objekttyp. Sie können erkennen, wer Eigentümer des Objekts ist und ob das Objekt über eine Berechtigungsliste geschützt wird. Der mittlere Bereich dient der Arbeit mit Benutzern und deren Rechte am Objekt. Hier werden Lese-, Schreib und Ausführungsrechte sowie sogenannte Objektverwaltungsrechte gewährt bzw. verweigert.

Über die Schaltfläche „Hinzufügen…“ werden neue Benutzer, denen Objektzugriffsrechte gewährt werden sollen, interaktiv aus der Benutzerverwaltung übernommen. Mit dem Button „Entfernen“ löscht man dagegen einen Benutzer aus der Liste der berechtigten Anwender. Mit dem Button „Anpassen…“ können Sie mittels eines Detaildialogs die einzelnen Rechte verändern.

Im unteren Bereich des Fensters finden Sie weitere Schaltflächen, mit denen Sie die Eignerschaft eines Objekts ändern. Auch hier greifen Sie wieder direkt auf die Daten der Benutzerverwaltung zu. Mit der Schaltfläche Berechtigungsliste wählen Sie aus den im System gespeicherten Berechtigungslisten diejenige aus, durch die Ihr Objekt geschützt werden soll. Falls Ihnen der Begriff der „Berechtigungsliste“ fremd sein sollte und Sie sich bislang noch nicht mit Berechtigungen auf einem i5-Server auseinandersetzen mussten, finden Sie weiterführende Informationen im entsprechenden Kapitel.

9.12.7 Objekte im integrierten Dateisystem

***BLKSF**
Eine blockorientierte Datei (*BLKSF) repräsentiert ein benutzerdefiniertes Dateisystem, das sich in einem bestimmten Zusatzspeicherpool (ASP) befindet. Diese Art von Datei ermöglicht es, das benutzerdefinierte Dateisystem als Einheit anzuzeigen und zu verwalten. Die Benutzer erhalten Zugriff auf ein benutzerdefiniertes Dateisystem, indem die blockorientierte Datei an den Namensbereich des integrierten Dateisystems (Integrated File System – IFS) angehängt wird.

***CHRSF**
Ein zeichenorientiertes Gerätedateiobjekt (*CHRSF) ist einer Einheit oder Ressource eines Computersystems zugeordnet. Es hat Pfadnamen, die in Verzeichnissen erscheinen und verwendet denselben Zugriffsschutz wie reguläre Dateien.

***DDIR**
Das Objekt Verteiltes Verzeichnis (*DDIR) wird im IFS verwendet. Ein *DDIR-Objekt kann auf einem System vorhanden sein, und die Systeme im Netzwerk können darauf zugreifen.

***DIR**
Das Objekt Verzeichnis (*DIR) wird im IFS verwendet.

***DSTMF**
Das Objekt Verteilte Datenstromdatei (*DSTMF) wird im IFS verwendet. Ein *DSTMF-Objekt kann auf einem System vorhanden sein, und die Systeme im Netzwerk können darauf zugreifen. Eine Datenstromdatei enthält einen kontinuierlichen Datenstrom. Beispiele für Datenstromdateien:
– Dokumente, die in IBM i-Ordnern gespeichert sind
– PC-Dateien
– UNIX-Dateien

***FIFO**
Ein First In/First Out-Objekt (*FIFO) ist ein von UNIX definierter Dateityp. Dabei handelt es sich um eine Datei, die für Lese- und Schreibzugriffe geöffnet werden kann und die die Eigenschaft hat, dass alle Daten nach dem FIFO-Verfahren gelesen werden. Dabei werden die Daten, die am längsten vorhanden sind, zuerst gelesen. Sind die Daten gelesen, werden sie aus der Datei entfernt. Alle übrigen Daten werden gelöscht, sobald alle geöffneten Instanzen geschlossen sind. Sind keine Daten verfügbar oder ist die FIFO-Datei zu einem bestimmten Zeitpunkt voll, können bei Lese- und Schreibzugriffen Blockierungen auftreten.

36. Ergänzung 9/2013

***SOCKET**
Das Objekt Lokaler Socket (*SOCKET) ermöglicht die gleichzeitige Ausführung zweier Jobs auf dem gleichen System, um eine Kommunikationsverbindung zueinander herzustellen. Das Objekt wird zugeordnet, wenn einer der Jobs die Socket-Funktion bind() verwendet.

Wenn die Verbindung hergestellt ist, können die Jobs Daten untereinander austauschen, indem sie Socket-Funktionen wie sendto() und recvmsg() oder die Socket-Funktion connect() gefolgt von Funktionen des IFS, wie write() und read(), verwenden.

Ist die Kommunikation der Jobs beendet, verwendet jeder Job die Funktion close(), um die Socket-Verbindung zu beenden. Der lokale Socket verbleibt so lange im System, bis er mit der Funktion unlink() oder dem Befehl RMVLNK (Verbindung entfernen) entfernt wird.

Ein lokaler Socket kann nicht gesichert werden.

***STMF**
Das Objekt Datenstromdatei (*STMF) wird im integrierten Dateisystem verwendet. Eine Datenstromdatei enthält einen kontinuierlichen Datenstrom. Beispiele für Datenstromdateien:
– Dokumente, die in IBM i-Ordnern gespeichert sind
– PC-Dateien
– UNIX-Dateien

***SYMLNK**
Eine symbolische Verbindung (*SYMLNK) enthält den Pfadnamen eines IFS, der auf ein anderes Objekt verweist. Das andere Objekt kann vorhanden sein oder nicht. Wenn über die symbolische Verbindung auf ein Objekt verwiesen wird, verwendet das System den in der symbolischen Verbindung angegebenen Pfadnamen, um das Objekt zu lokalisieren.

Sie sehen, es gibt eine schier unüberschaubare Anzahl verschiedener Objekttypen, die man mehr oder weniger oft benötigt. Ehrlich gesagt, viele dieser Objekttypen habe ich noch nie benutzt bzw. benötigt.

Allen Objekttypen ist gemeinsam, dass man Benutzern, Gruppen oder Berechtigungslisten Rechte auf sie zuweisen kann.

9.12.8 Objektberechtigungen

Um Rechte für ein Objekt zu vergeben, kann man verschiedene Möglichkeiten nutzen, die teilweise abhängig vom Typ des Objekts sind. So unterscheidet man grundsätzlich die Berechtigungsvergaben für Objekte, die in Bibliotheken gespeichert und z. B. mit **WRKOBJ** bearbeitet werden, von Rechten für IFS-Objekte, die z. B. über **WRKLNK** vergeben werden.

9.12.8
Seite 2

9.12.9 Berechtigungen für Bibliotheksobjekte

Wollen Sie sich die Berechtigungen für Objekte anzeigen lassen, verwenden Sie den Befehl DSPOBJAUT (Objektberechtigung anzeigen).

```
                    Objektberechtigung anzeigen (DSPOBJAUT)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . > SMZ4          Name
  Bibliothek . . . . . *LIBL     Name, *LIBL, *CURLIB
Objektart . . . . . > *LIB       *ALRTBL, *AUTL, *BNDDIR...
ASP-Einheit . . . . . *          Name, *, *SYSBAS
Ausgabe . . . . . *              *, *PRINT, *OUTFILE
```

Auswahl bei Objektberechtigungen anzeigen

Nach Eingabe der Auswahlparameter erhalten Sie die Anzeige der Berechtigungen.

```
                        Objektberechtigung anzeigen

Objekt . . . . . :   SMZ4          Eigner . . . . . :   SECURITY2P
  Bibliothek . . . . :   QSYS      Primärgruppe . . . . :   *NONE
Objektart . . . . . :   *LIB       ASP-Einheit . . . . :   *SYSBAS

Objekt durch Berechtigungsliste geschützt . . . . . :   *NONE

                       Objektbe-
Benutzer    Gruppe     rechtigung
*PUBLIC                 *USE
SECURITY2P              *ALL

                                                                Ende
Eingabetaste --> Weiter

F3=Verlassen    F11=Objektberechtigungen detailliert anzeigen    F12=Abbrechen
F17=Anfang      F18=Ende
```

Objektberechtigungen

Die Bedeutung der Werte entnehmen Sie der nachstehenden Erläuterung des Befehls „Objektberechtigungen editieren".

Die Anzeige „Objektberechtigung editieren", die mit Auswahl 2 aus **WRKOBJ** oder über den Befehl **EDTOBJAUT** aufgerufen werden kann, zeigt eine Liste der Benutzer an, die momentan objektberechtigt sind, sowie die Berechtigungsebenen, die ihnen jeweils zugewiesen wurden. Benutzer können der Liste hinzugefügt oder aus ihr entfernt werden, und die Berechtigungsebenen der Benutzer können geändert werden.

9.12.9
Seite 2

Bei einer Änderung der allgemeinen Berechtigung für von IBM gelieferte Objekte können Probleme auftreten. Wird beispielsweise die allgemeine Berechtigung der Nachrichtenwarteschlange QSYSOPR in eine Berechtigung geändert, die weniger Rechte umfasst als die Berechtigung *CHANGE, so können Fehler bei Systemprogrammen auftreten. Die Berechtigung der Systemprogramme reicht nämlich nicht aus, um z. B. Nachrichten an die Nachrichtenwarteschlange QSYSOPR zu senden.

Berechtigungsebenen können auf zwei Arten angegeben werden:

1. Einen der vordefinierten Systemwerte für Objektberechtigungsebenen zuordnen (*USE, *ALL, *CHANGE oder *EXCLUDE).
2. Benutzerdefinierte Berechtigungsebenen zuordnen. Benutzerdefinierte Berechtigungsebenen werden erstellt, indem die Spalten, die nach dem Drücken der Funktionstaste 11 beim Anzeigen von Details erscheinen, mit X gefüllt bzw. die X daraus entfernt werden.

Bei allen Verfahren bestimmt das System die Objektberechtigungswerte bzw. die speziellen Berechtigungen aufgrund der eingegebenen Informationen. Wenn für einen Benutzer sowohl die Objektberechtigungswerte als auch die speziellen Berechtigungen eingegeben werden, werden stets die speziellen Berechtigungen verwendet.

Mit der Taste F11 kann durch drei verschiedene Versionen der Objektberechtigungsanzeigen geblättert werden:

- Anzeige „Keine Details anzeigen“. Diese Anzeige enthält systemdefinierte Berechtigungsuntergruppen und USER DEF:

Benutzer	Gruppe	Objekt-berechtg.
*PUBLIC		*USE
QSYS		*ALL

- Anzeige „Objektberechtigung”:

			Objekt-	----------Objekt----------				
Benutzer	Gruppe		berechtg.	Opr	Verw.	Exist.	Ändern	Referenz
*PUBLIC			*USE	X				
QSYS			*ALL	X	X	X	X	X

- Anzeige „Datenberechtigung”:

		Objekt-	----------Daten----------				
Benutzer	Gruppe	berechtg.	Lesen	Hinzuf	Aktual	Lösch.	Ausf.
*PUBLIC		*USE	X				X
QSYS		*ALL	X	X	X	X	X

Um die Berechtigungsebene eines Benutzers zu ändern, werden die entsprechenden Spalten der Benutzerzeile überschrieben. Außer bei der Spalte „Objektberechtigung" wird dem Benutzer durch Eingabe eines „X" in die Spalte die genannte Berechtigung erteilt bzw. durch Eingabe einer Leerstelle in die Spalte die Berechtigung entzogen. Um die Spalte „Objektberechtigung" zu ändern, überschreibt man einfach die alte Berechtigung durch die neue.

Um der Liste Benutzer hinzuzufügen, drücken Sie die Funktionstaste 6 (Neue Benutzer hinzufügen). Die daraufhin erscheinende Anzeige erlaubt die Eingabe neuer Benutzer und Berechtigungsebenen.

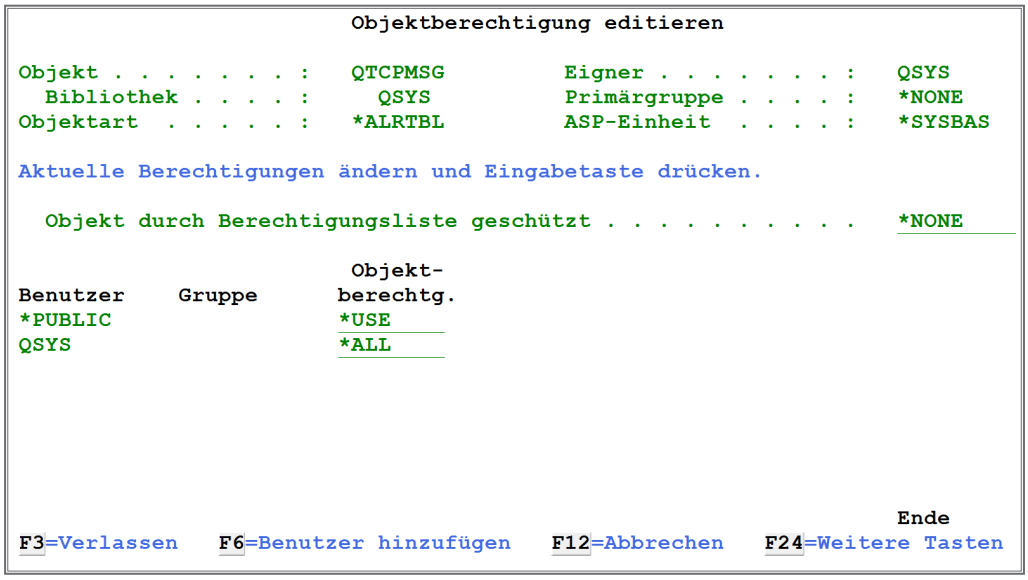
```
                          Neue Benutzer hinzufügen

Objekt . . . . . :   #CGULIB          Eigner . . . . . :   QSYS
  Bibliothek . . . :     QSYS         Primärgruppe . . . :   *NONE
Objektart  . . . . :   *LIB           ASP-Einheit  . . . :   *SYSBAS

Neue Benutzer eingeben und Eingabetaste drücken.

              Objekt-
Benutzer      berechtg.
              _________
              _________
              _________
              _________
              _________
              _________
              _________
              _________
              _________
              _________
                                                              Weitere ...
F3=Verlassen    F11=Objektberechtigungen detailliert anzeigen    F12=Abbrechen
F17=Anfang      F18=Ende
```

Neue Benutzer hinzufügen

Um Benutzer aus der Liste zu entfernen, werden in alle angezeigten Berechtigungsspalten Leerstellen eingegeben (auch in die Spalte „Objektberechtigung"). Erscheint „Weitere..." rechts unten in der Anzeige, sind weitere Informationen vorhanden. Taste „Bild auf" (Vorblättern) drücken, um zum Ende der angezeigten Informationen zu gelangen. Taste „Bild ab" (Zurückblättern) drücken, um zum Anfang zurückzukehren.

Das System ändert die Berechtigung nur, nachdem die Eingabetaste gedrückt wurde. Wenn bei der Anzeige einer Liste nach Eingabe von Änderungen die Eingabetaste erneut gedrückt wird, so wird die Liste mit den entsprechenden Änderungen angezeigt. Nach erneutem Drücken der Eingabetaste – ohne Verändern der angezeigten Liste durch Eingabe – wird an den Ausgangspunkt zurückgekehrt, von dem aus die Editierfunktion angefordert wurde.

9.12.9
Seite 4



Objektberechtigung editieren

Objekt
Name des Objekts, für das Informationen angezeigt werden.

Bibliothek
Der Name der Bibliothek, die dieses Objekt enthält.

Objektart
Die Objektart. Sie beschreibt die Art des angezeigten Objekts.

Eigner
Der Eigner des genannten Objekts.

Primärgruppe
Der Name des Benutzerprofils, das die Primärgruppe des Objekts ist. Die Primärgruppe kann mit dem Befehl CHGOBJPGP (Objektprimärgruppe ändern) geändert werden.

ASP-Einheit
Der Name der ASP-Einheit (ASP = Zusatzspeicherpool), in der sich das Objekt befindet. *SYSBAS bedeutet, dass sich das Objekt im System-ASP oder einem Basis-Benutzer-ASP befindet.

Berechtigungsliste
Der Name der Berechtigungsliste, mit der das genannte Objekt gesichert wird. Der Wert *NONE zeigt an, dass bei der Bestimmung der Berechtigung für das Objekt keine Berechtigungsliste verwendet wird.

Den gezeigten Wert überschreiben, um die Berechtigungsliste zu ändern, die zur Sicherung des Objekts verwendet wird. *NONE oder Leerstellen eingeben, falls keine Liste verwendet werden soll.

Benutzer
Die Benutzerprofilnamen der Benutzer, die über spezielle Berechtigungen für dieses Objekt verfügen. Der Wert *PUBLIC legt die Berechtigungen aller Benutzer fest, die nicht speziell genannt werden und keine Mitglieder der Berechtigungsliste sind, die zur Sicherung dieses Objekts verwendet wird. Der Wert *GROUP bestimmt die Berechtigungen für das Gruppenprofil des aktuellen Benutzers, das in der Spalte „Gruppe" erscheint. *GROUP kann mehrmals erscheinen, wenn der Benutzer die Berechtigung für das Objekt aus mehreren Gruppen erhält.

Der Wert *ADOPT definiert alle Berechtigungen, die das Objekt vom aktuellen Job übernimmt. Wird *ADOPT angezeigt, führt dieser Job ein Programm aus, welches das Benutzerprofil des Programmeigners angenommen hat und dessen Eigner für das Objekt berechtigt ist.

Gruppe
Der Name des Gruppenprofils, aus dem der Benutzer die Berechtigung erhält. Der Name eines Gruppenprofils wird angezeigt, wenn der Wert der Benutzerspalte *GROUP lautet.

Objektberechtigung
Die Berechtigungen, die ein Benutzer für ein Objekt besitzt. Benutzern können mehrere verschiedene Objektberechtigungsebenen zugeordnet werden. Dabei handelt es sich um folgende Ebenen:

***ALL**
Erlaubt alle Operationen am Objekt bis auf diejenigen, die auf den Eigner begrenzt sind oder die durch die Berechtigung zur Verwaltung der Berechtigungsliste kontrolliert werden.

***CHANGE**
Erlaubt alle Operationen am Objekt bis auf diejenigen, die auf den Eigner begrenzt sind oder die durch die Objektexistenzberechtigung, die Objektänderungsberechtigung, die Objektreferenzberechtigung und die Objektverwaltungsberechtigung gesteuert werden.

***EXCLUDE**
Alle Operationen am Objekt sind verboten.

***USE**
Erlaubt den Zugriff auf die Objektattribute sowie die Benutzung des Objekts. Der Benutzer kann das Objekt nicht ändern.

USER DEF
Wird vom System angezeigt, wenn die Sonderobjektberechtigungen und Sonderdatenberechtigungen keiner der vordefinierten oben angegebenen Objektberechtigungsebenen entsprechen. Die Sonderberechtigungen werden angezeigt, wenn die Funktionstaste „Details anzeigen" gedrückt wird.

Der Wert *AUTL ist auch gültig, wenn allgemeine Berechtigungen definiert werden. Er zeigt an, dass die in der von diesem Objekt verwendeten Berechtigungsliste angegebenen Angaben zur allgemeinen Berechtigung verwendet werden sollen, um die Berechtigung festzulegen.

Die Objektberechtigung kann geändert werden, indem der aktuelle Wert mit einem neuen Wert überschrieben wird.

Berechtigungen auf das Objekt
Die speziellen Berechtigungen, über die der Benutzer für das Objekt verfügt. Ein „X" in der Spalte zeigt an, dass der Benutzer die angegebene Berechtigung für das aufgeführte Objekt besitzt.

Bei bestimmten Objekten mit der Angabe *FILE wird möglicherweise ein Schrägstrich (/) in der Spalte angezeigt. Er besagt, dass der Benutzer über die angegebene Berechtigung für einige, aber nicht alle Felder in der Datei verfügt.

Die speziellen Datenberechtigungen sind:

Opr
Objektverwendungsberechtigung (gelegentlich abgekürzt als Objopr) bietet die Berechtigung, sich die Objektattribute anzeigen zu lassen und das Objekt so zu verwenden, wie es durch die Datenberechtigung des Benutzers für das Objekt angegeben ist.

Verwaltung
Objektverwaltungsberechtigung umfasst die Berechtigung, die Sicherheitsstufe anzugeben, das Objekt zu verschieben oder es umzubenennen sowie dem Objekt Teildateien hinzuzufügen, wenn es sich um eine Datenbankdatei handelt.

Existenz
Objektexistenzberechtigung umfasst die Berechtigung, die Objektexistenz und das Eigentumsrecht zu kontrollieren.

Änderung
Objektänderungsberechtigung umfasst die Berechtigung zum Ändern der Attribute eines Objekts, wie z. B. Auslöser für eine Datenbankdatei hinzufügen oder entfernen und einer Datenbankdatei Teildateien hinzufügen.

Referenz
Objektreferenzberechtigung umfasst die Berechtigung, das Objekt als erste Ebene in einer referenziellen Integritätsbedingung anzugeben.

Durch Eingabe von „X" bzw. einer Leerstelle können spezielle Objektberechtigungen erteilt oder entfernt werden.

Berechtigung auf Daten
Die speziellen Berechtigungen eines Benutzers für die in einem Objekt enthaltenen Daten. Ein „X“ in der Spalte zeigt an, dass der Benutzer die angegebene Berechtigung besitzt.

Bei bestimmten Objekten mit der Angabe *FILE wird möglicherweise ein Schrägstrich (/) in der Spalte angezeigt. Ein Schrägstrich zeigt an, dass der Benutzer über die angegebene Berechtigung für einige, aber nicht alle Felder in der Datei verfügt.

Die speziellen Datenberechtigungen sind:

Lesen
Die Leseberechtigung erlaubt den Zugriff auf den Inhalt eines Objekts.

Hinzufügen
Die Hinzufügeberechtigung erlaubt es, einem Objekt Einträge hinzuzufügen.

Aktualisieren
Die Aktualisierungsberechtigung erlaubt es, den Inhalt der vorhandenen Einträge eines Objekts zu ändern.

Löschen
Die Löschberechtigung erlaubt es, Einträge aus einem Objekt zu entfernen.

Ausführen
Die Ausführungsberechtigung umfasst die Berechtigung zur Ausführung eines Programms oder zur Suche in einer Bibliothek oder in einem Verzeichnis.

Durch Eingabe von „X“ bzw. einer Leerstelle können Datenberechtigungen erteilt oder entfernt werden.

Objektberechtigungen können jedoch nicht nur interaktiv vergeben werden, sondern werden oftmals auch via Command zugewiesen. Dafür gibt es den Befehl **GRTOBJAUT**.

```
                    Objektberechtigung erteilen (GRTOBJAUT)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . .                            Name, generisch*, *ALL
  Bibliothek . . . . . .     *LIBL            Name, *LIBL, *CURLIB, *ALL...
Objektart . . . . . .                         *ALL, *ALRTBL, *BNDDIR...
ASP-Einheit . . . . . .      *               Name, *, *SYSBAS
Benutzer . . . . . .                          Name, *PUBLIC
     + für weitere Werte
Berechtigung . . . . . .     *CHANGE          *CHANGE, *ALL, *USE...
     + für weitere Werte
Berechtigungsliste . . . . . .                Name, *NONE
Bezugsobjekt . . . . . .                      Name
  Bibliothek . . . . . .       *LIBL          Name, *LIBL, *CURLIB
Bezugsobjektart . . . . . .  *OBJTYPE         *OBJTYPE, *ALRTBL, *BNDDIR...
Referenz-ASP-Einheit . . . . .  *             Name, *, *SYSBAS
Berechtigung ersetzen . . . . .  *NO         *NO, *YES


                                                                      Ende
F3=Verlassen    F4=Bedienerf.    F5=Aktualisieren    F12=Abbrechen
F13=Verwendung der Anzeige       F24=Weitere Tasten
```

Objektberechtigungen erteilen

Hier können Sie die oben beschriebenen Parameterwerte einem Objekt direkt über die Befehlsschnittstelle zuweisen.

Berechtigungen werden erteilt für:

- Benannte Benutzer
- Benutzer (*PUBLIC), die keine besonderen Berechtigungen für ein Objekt oder eine Berechtigungsliste haben.
- Benutzer eines Objekts, auf das durch die Parameter Bezugsobjekt (REFOBJ) und Bezugsobjektart (REFOBJTYPE) verwiesen wird.
- Berechtigungslisten

Bei Angabe von AUT(*AUTL) wird die allgemeine Berechtigung für ein Objekt aus der allgemeinen Berechtigung der Berechtigungsliste übernommen, die das Objekt schützt.

Mit dem Parameter AUTL wird ein Objekt durch eine Berechtigungsliste geschützt oder die Berechtigungsliste für ein Objekt entfernt.

Benutzerprofile können nicht durch eine Berechtigungsliste (*AUTL) geschützt werden.

Dieser Befehl kann von einem Objekteigner oder von einem Benutzer mit Objektverwaltungsberechtigung für ein angegebenes Objekt verwendet werden. Ein Benutzer mit Objektverwaltungsberechtigung kann anderen Benutzern jede Berechtigung erteilen, über die er selbst verfügt, mit Ausnahme der Objektverwaltungsberechtigung. Nur der Eigner eines Objekts oder ein Benutzer mit der Sonderberechtigung für alle Objekte (*ALLOBJ) kann einem Benutzer die Objektverwaltungsberechtigung erteilen.

Ein Benutzer mit der Berechtigung *ALL kann eine neue Berechtigungsliste zuordnen.

Beim Erteilen von Benutzerberechtigungen wird mit dem Parameter REPLACE festgelegt, ob die angegebenen Berechtigungen die Berechtigungen, über die der Benutzer verfügt, ersetzen sollen. Mit dem Standardwert REPLACE(*NO) wird die angegebene Berechtigung erteilt, aber keine Berechtigung entzogen, die die angegebene überschreitet, es sei denn, die Berechtigung *EXCLUDE wird erteilt.

Mit REPLACE(*YES) werden dem Benutzer seine aktuellen Berechtigungen entzogen und dann die angegebene Berechtigung erteilt. Bei der Berechtigungsvergabe über ein Bezugsobjekt wird mit diesem Befehl die angegebene Berechtigung erteilt, aber keine Berechtigung, die die angegebene überschreitet, entzogen, es sei denn, die Berechtigung *EXCLUDE wird erteilt.

Mit diesem Befehl wird die angegebene Berechtigung erteilt, aber es werden keine Berechtigungen entzogen, die mehr Rechte umfassen als die angegebenen Berechtigungen. Eine Ausnahme besteht beim Erteilen der Berechtigung *EXCLUDE oder der Angabe REPLACE(*YES).

Einschränkungen:

- Dieser Befehl **GRTOBJAUT** muss eine exklusive Sperre für eine Datenbankdatei erhalten, bevor einem Benutzer die Lese- oder Objektverwendungsberechtigung erteilt werden kann.
- Fordert ein Benutzer die Berechtigung für einen anderen angegebenen Benutzer für eine Einheit an, die momentan von einem weiteren berechtigten Benutzer verwendet wird, so wird keine Berechtigung für die Einheit erteilt.
- Die Objektart *AUTL kann nicht angegeben werden.
- AUT(*AUTL) ist nur gültig in Verbindung mit USER(*PUBLIC).
- Ein Benutzer muss entweder der Eigner des Objekts sein oder über die Berechtigung *ALL verfügen, um den Parameter AUTL verwenden zu können.
- Der Benutzer muss über die Objektverwaltungsberechtigung für das Objekt verfügen.
- Handelt es sich bei dem Objekt um eine Datei, muss der Benutzer über die Objektverwendungs- und die Objektverwaltungsberechtigung verfügen.

- Für Datensichtgeräte oder Nachrichtenwarteschlangen von Datenstationen, die einem Datensichtgerät zugeordnet sind, gilt außerdem, dass diesem Befehl der Befehl ALCOBJ (Objekt zuordnen) vorangehen und der Befehl DLCOBJ (Objekt freigeben) folgen muss, wenn dieser Befehl GRTOBJAUT nicht an der Einheit eingegeben wird, für die die Berechtigungen erteilt werden.
- Für die ASP-Einheit (ASP = Zusatzspeicherpool) ist die Berechtigung *USE erforderlich, sofern eine solche Einheit angegeben ist.

Es wird empfohlen, die allgemeine Berechtigung für von IBM gelieferte Objekte nur nach Prüfung aller möglichen Folgen zu ändern. Wird die allgemeine Berechtigung für die Nachrichtenschlange QSYSOPR in eine einschränkendere Berechtigung als *CHANGE geändert, können einige Systemprogramme beispielsweise nicht mehr ausgeführt werden. Die Systemprogramme verfügen dann nicht mehr über die erforderliche Berechtigung zum Senden von Nachrichten an die Nachrichtenwarteschlange QSYSOPR. Weitere Informationen enthält das Handbuch System i Security Reference, IBM Form SC41-5302.

9.12.10 Berechtigungen für IFS-Objekte

Wollen Sie sich die Berechtigungen für IFS-Objekte anzeigen lassen, verwenden Sie den Befehl DSPAUT (Objektberechtigung anzeigen).

```
                    Berechtigung anzeigen (DSPAUT)

 Auswahl eingeben und Eingabetaste drücken.

 Objekt . . . . . .   '/temp'
_____
 Symbolische Verbindung . . . . .  *NO          *NO, *YES
 Ausgabe  . . . . . .  *           *, *PRINT
```

Auswahl bei IFS-Objektberechtigungen anzeigen

Nach Eingabe der Auswahlparameter erhalten Sie die Anzeige der Berechtigungen.

```
                          Berechtigung anzeigen

Objekt . . . . . :   /temp
Art  . . . . . :   DIR
Eigner . . . . . :   QSECOFR
Primärgruppe . . . . . :   *NONE
Berechtigungsliste . . . . . :   *NONE

            Daten-     ----Objektberechtigungen----
Benutzer    berecht.  Exist  Verw  Änder  Referenz
*PUBLIC     *RWX        X      X      X       X
QSECOFR     *RWX        X      X      X       X









                                                                  Ende
Eingabetaste --> Weiter

F3=Verlassen    F11=Datenberechtigungen detailliert anzeigen    F12=Abbrechen
F17=Anfang      F18=Ende
```

IFS-Objektberechtigungen

Die Bedeutung der Werte entnehmen Sie der nachstehenden Erläuterung des Befehls „IFS-Objektberechtigungen editieren".

Die Anzeige „Mit Berechtigungen arbeiten", die mit Auswahl 9 aus **WRKLNK** vor einem Objekt aufgerufen werden kann, enthält eine Liste der Benutzer, die über die Berechtigung für das angeforderte Objekt verfügen, sowie die speziellen Berechtigungen dieser Benutzer. Die gleiche Anzeige kann über den Befehl **WRKAUT** erreicht werden, bei dem allerdings der Objektname als Parameterwert mitgegeben werden muss.

9.12.10
Seite 2

Die allgemeine Berechtigung, die Eignerberechtigung und die Berechtigung der Primärgruppe werden ebenfalls angezeigt.

Es können auch Parameter in die Befehlszeile eingegeben und die Eingabetaste gedrückt werden, um den Befehl sofort auszuführen. Sollen weitere Parameterwerte angegeben werden, die Funktionstaste 4 (Bedienerführung) drücken. Wenn Parameter eingegeben werden und mehr als eine Auswahl getroffen wird, gelten die Parameter für alle eingegebenen Auswahlmöglichkeiten.

Um einen Befehl unmittelbar auszuführen, den Befehl eingeben und die Eingabetaste drücken. Für Hilfe bei der Befehlseingabe: den Befehl eingeben und Funktionstaste 4 (Bedienerführung) drücken.

Mit der Taste F11 kann durch zwei verschiedene Versionen der Berechtigungsanzeigen geblättert werden:

- Die Anzeige „Objektberechtigung anzeigen“, in der die systemdefinierten Datenberechtigungsgruppen und die Objektberechtigungen aufgelistet werden.
- Die Anzeige „Datenberechtigungen detailliert anzeigen“.

Ist diese Anzeige abgeschlossen, kehrt der Benutzer durch Drücken der Eingabetaste wieder in die Anzeige zurück, von der aus diese Anzeige aufgerufen wurde.

```
                          Mit Berechtigung arbeiten

Objekt . . . . . :   /alex
Art  . . . . . :   DIR
Eigner . . . . . :   RAZLEEIL
Primärgruppe . . . . . :   *NONE
Berechtigungsliste . . . . . :   *NONE

Auswahl eingeben und Eingabetaste drücken.
  1=Benutzer hinzufügen   2=Benutzerberechtigung ändern
  4=Benutzer entfernen

                  Daten-     -------------Datenberechtigungen-------------
Ausw  Benutzer    berecht.  Objopr  Lesen  Hinzu  Aktual  Lösch.  Ausführ.
 _    *PUBLIC     *RWX        X       X      X      X       X        X
 _    RAZLEEIL    *RWX        X       X      X      X       X        X
 _    QDIRSRV     *X          X                                       X
                                                                    Ende
Parameter oder Befehl
===>
F3=Verlassen    F4=Bedienerführung    F5=Aktualisieren    F9=Auffinden
F11=Objektberechtigungen anzeigen     F12=Abbrechen       F24=Weitere Tasten
```

Objektberechtigung für IFS-Objekte

Objekt
Der Pfadname des Objekts, für das Informationen angezeigt werden sollen.

Art
Die Art des Objekts.

Häufig vorkommende Objektarten, die wahrscheinlich in dieser Anzeige enthalten sind:

AUTL	Berechtigungsliste
BLKSF	Blockorientierte Einheitendatei
CFGL	Konfigurationsliste
CHRSF	Zeichenorientierte Einheitendatei
CLS	Klasse
CMD	Befehl
CTLD	Steuereinheitenbeschreibung
DDIR	Verteiltes Verzeichnis
DEVD	Einheitenbeschreibung
DIR	Verzeichnis
DOC	Dokument
DSTMF	Verteilte Datenstromdatei
FIFO	First-In/First-Out-Einheitendatei
FILE	Datenbank- oder Einheitendatei
FLR	Ordner
JOBD	Jobbeschreibung
JOBQ	Jobwarteschlange
LIB	Bibliothek
LIND	Leitungsbeschreibung
MSGQ	Nachrichtenwarteschlange
OUTQ	Ausgabewarteschlange
PGM	Programm
SBSD	Subsystembeschreibung
STMF	Datenstromdatei
SYMLNK	Symbolische Verbindung
USRPRF	Benutzerprofil

Datenbankteildateien werden ebenfalls als Objektart MBR angesehen. Einzelheiten über alle Objektarten enthält das Handbuch CL-Themensammlung in der Kategorie Programmierung im IBM i Information Center unter http://www.ibm.com/systems/i/infocenter/.

Eigner
Der Eigner des genannten Objekts.

Primärgruppe
Der Name des Benutzerprofils, das die Primärgruppe des Objekts ist. Die Primärgruppe kann mit dem Befehl CHGPGP (Primärgruppe ändern) geändert werden.

Berechtigungsliste
Der Name der Berechtigungsliste, mit der das genannte Objekt gesichert wird. Der Wert *NONE zeigt an, dass bei der Bestimmung der Berechtigung für das Objekt keine Berechtigungsliste verwendet wird.

Benutzer
Die Namen der Benutzer, die zur Verwendung des Objekts berechtigt sind. Der Wert *PUBLIC zeigt die Berechtigungen der Benutzer an, die nicht speziell genannt werden und sich nicht auf der Berechtigungsliste des Objekts befinden. Der Wert *NOUSRRPRP zeigt an, dass das Benutzerprofil, das eine Berechtigung für dieses Objekt besitzt, auf diesem System nicht vorhanden ist.

Berechtigung auf Daten
Die Datenberechtigung, über die der Benutzer für ein Objekt verfügt. Benutzern können verschiedene systemdefinierte Datenberechtigungsebenen zugeordnet werden. Dabei handelt es sich um folgende Ebenen:

***RWX**
Erlaubt die Ausführung sämtlicher Operationen für das Objekt, mit Ausnahme der Operationen, die auf den Eigner beschränkt sind oder durch die Objektrechte gesteuert werden.

***RX**
Erlaubt Zugriff auf die Objektattribute sowie die Benutzung des Objekts. Der Benutzer kann das Objekt nicht ändern.

***RW**
Erlaubt Zugriff auf die Objektattribute sowie die Änderung des Objekts. Der Benutzer hat keine Berechtigung zum Verwenden des Objekts.

***WX**
Erlaubt die Verwendung und die Änderung des Objekts. Der Benutzer hat keinen Zugriff auf die Objektattribute.

***R**
Erlaubt Zugriff auf die Objektattribute.

***W**
Erlaubt die Änderung des Objekts.

***X**
Erlaubt die Verwendung des Objekts.

***EXCLUDE**
Alle Operationen am Objekt sind verboten.

***NONE**
Wird vom System angezeigt, wenn der Benutzer keine Datenberechtigungen hat.

USER DEF
Wird vom System angezeigt, wenn die speziellen Datenberechtigungen nicht mit den zuvor aufgeführten, vordefinierten Datenberechtigungsebenen übereinstimmen. Die speziellen Datenberechtigungen können mit der Funktionstaste zum detaillierten Anzeigen der Berechtigungen aufgelistet werden.

Der Wert *AUTL ist auch gültig, wenn allgemeine Berechtigungen definiert werden. Er zeigt an, dass die Angaben in der von diesem Objekt verwendeten Berechtigungsliste zur allgemeinen Berechtigung verwendet werden sollen, um diese Berechtigungen festzulegen.

Berechtigungen auf Objekte
Die Objektberechtigungen, über die der Benutzer für das Objekt verfügt. Ein „X“ in der Spalte bedeutet, dass der Benutzer über die angegebene Objektberechtigung für das aufgeführte Objekt verfügt. Die speziellen Objektberechtigungen sind:

Existenz
Objektexistenzberechtigung umfasst die Berechtigung, die Objektexistenz und das Eigentumsrecht zu kontrollieren.

Verwaltung
Objektverwaltungsberechtigung umfasst die Berechtigung, die Sicherheitsstufe anzugeben, das Objekt zu verschieben oder es umzubenennen, sowie dem Objekt Teildateien hinzuzufügen, wenn es sich um eine Datenbankdatei handelt.

Änderung
Objektänderungsberechtigung umfasst die Berechtigung zum Ändern der Attribute eines Objekts, wie z. B. Auslöser für eine Datenbankdatei hinzufügen oder entfernen und einer Datenbankdatei Teildateien hinzufügen.

Referenz
Objektreferenzberechtigung umfasst die Berechtigung, das Objekt als erste Ebene in einer referenziellen Integritätsbedingung anzugeben.

9.12.10

Seite 6

9.12.11 Objekteigner

Vorstehend haben wir schon mehrfach den Begriff „Objekteigner“ gelesen. Was hat es damit auf sich?

Wie in vielen Betriebssystemen gibt es auch im IBM i einen Besitzer eines Objekts. Das ist in der Regel der Benutzer, der das Objekt erstellt hat oder der dessen Eignerschaft später übernommen hat.

Der Eigner eines Objekts verfügt immer über alle für das Objekt zutreffenden Berechtigungen, wenn diese nicht ausdrücklich entzogen wurden. Der Objekteigner hat die Berechtigung, allen Benutzern beliebige Berechtigungen für das Objekt zu erteilen. Eigner können außerdem sich selbst Berechtigungen erteilen, die zuvor entzogen wurden. Sie können z. B. als Vorsichtsmaßnahme einige ihrer speziellen Berechtigungen aufheben und dann im Bedarfsfall wieder erteilen.

Ein Benutzer mit der Sonderberechtigung *ALLOBJ verfügt über die vollständige Berechtigung für alle Objekte und kann das Eigentumsrecht an jedem Objekt übertragen. Alle Benutzer verfügen über die Hinzufüge- und Löschberechtigung für ihre eigenen Benutzerprofile, d. h., die Benutzer können durch Übertragen des Objekteigentumsrechts Objekte in ihren Benutzerprofilen hinzufügen oder (selbst erstellte) Objekte aus ihren Benutzerprofilen löschen.

Einschränkungen:

- Um das Eigentumsrecht übertragen zu können, muss jeder Benutzer (einschließlich des derzeitigen Objekteigners) über folgende Berechtigungen verfügen:
  - Objektexistenzberechtigung (*OBJEXIST) für das Objekt (außer für die Berechtigungsliste)
  - Objektverwendungsberechtigung (*OBJOPR) und Objektexistenzberechtigung (*OBJEXIST), wenn es sich bei dem Objekt um eine Datei, eine Bibliothek oder eine Subsystembeschreibung handelt.
  - Die Sonderberechtigung für alle Objekte (*ALLOBJ) oder das Eigentumsrecht, wenn das Objekt eine Berechtigungsliste ist.
  - Hinzufügeberechtigung (*ADD) für das Benutzerprofil des neuen Eigners
  - Löschberechtigung (*DLT) für das Benutzerprofil des gegenwärtigen Eigners

  - Die Sonderberechtigung für alle Objekte (*ALLOBJ) oder die Sonderberechtigung des Sicherheitsadministrators (*SECADM), um den Objekteigner eines Programms oder eines SQL-Pakets, das die Berechtigung des Eigners übernimmt, ändern zu können.
  - Benutzungsberechtigung (*USE) für die ASP-Einheit (ASP = Zusatzspeicherpool), sofern eine angegeben ist.
- Wird bei Datensichtgeräten dieser Befehl nicht an der Einheit eingegeben, dessen Eigentumsrecht oder von dessen Warteschlange das Eigentumsrecht geändert werden soll, dann sollten vor diesem Befehl zuerst der Befehl ALCOBJ (Objekt zuordnen) und dann der Befehl DLCOBJ (Objekt freigeben) ausgeführt werden.
- Die Objektarten *DOC und *FLR können nicht angegeben werden, der Benutzer muss DLO-Unterstützung (Dokumentaustausch) verwenden.
- Eine Änderung des Eigentumsrechts für ein Objekt, dem ein Berechtigungsobjekt zugeordnet ist, bewirkt auch eine Änderung im Eigentumsrecht des Berechtigungsobjekts.

Mit dem Befehl CHGOBJOWN kann die Eignerschaft eines Objekts an ein anderes Benutzerprofil übertragen werden. Die Berechtigungen anderer Benutzer für das Objekt werden davon nicht berührt:

```
                    Objekteigner ändern (CHGOBJOWN)

Auswahl eingeben und Eingabetaste drücken.

Objekt . . . . . .                  Name
  Bibliothek . . . . . .   *LIBL     Name, *LIBL, *CURLIB
Objektart . . . . . .               *ALRTBL, *AUTL, *BNDDIR...
ASP-Einheit . . . . . .  *          Name, *, *SYSBAS
Neuer Eigner . . . . . .            Name
Aktuelle Eignerberechtigung . .  *REVOKE  *REVOKE, *SAME
```

Objekteigner ändern

Neuer Eigner (NEWOWN)
Gibt das Benutzerprofil oder den neuen Eigner eines Objekts an. Das Benutzerprofil muss bereits vorhanden sein, wenn dieser Befehl ausgeführt wird.

Aktuelle Eignerberechtigung (CUROWNAUT)
Gibt an, ob die Berechtigungen für den aktuellen Eigner entzogen werden, wenn die Angabe für den Eigner geändert wird.

***REVOKE**
Dem aktuellen Eigner wird die Berechtigung entzogen, wenn das Objekteignerrecht einem neuen Eigner übertragen wird.

***SAME**
Die Berechtigung des aktuellen Eigners bleibt als persönliche Berechtigung für das Objekt bestehen.

Beispiel für CHGOBJOWN:

```
CHGOBJOWNOBJ(USERLIB/PROGRAM1) OBJTYPE(*PGM) NEWOWN(ANN)
```

Mit diesem Befehl wird dem Benutzer ANN das Eigentumsrecht an dem Programm PROGRAM1, das sich in der Benutzerbibliothek USERLIB befindet, zugeordnet. Dem aktuellen Eigner wird die Berechtigung entzogen.

9.12.11

Seite 4

9.12.12 Primärgruppe

Ein weiterer Begriff, der erwähnt wurde, ist die Primärgruppe. Was ist das?

Sie können eine Primärgruppe für ein Objekt festlegen. Der Name der Primärgruppe und die Primärgruppenberechtigungen werden zusammen mit dem Objekt gespeichert. Die Verwendung von Primärgruppen resultiert in einer besseren Performance als die Verwendung der Gruppenberechtigung, wenn Rechte auf ein Objekt geprüft werden.

Ein Profil muss ein Gruppenprofil sein (eine GID – Parameter im Benutzerprofil – haben), um als Primärgruppe zu einem Objekt zugewiesen werden zu können. Das gleiche Profi kann nicht zugleich der Eigner des Objekts und die Primärgruppe sein.

Wenn ein Benutzer ein neues Objekt erstellt, steuern die Parameter im Benutzerprofil, ob die Gruppe des Benutzers die Berechtigung an das Objekt weitergibt und welcher Typ von Berechtigungen vergeben wird.

Der Parameter „Gruppenberechtigungstyp“ (GRPAUTTYP) im Benutzerprofil kann verwendet werden, um die Benutzergruppe zur Primärgruppe für ein Objekt zu machen. Die Zuweisung von Berechtigung und Eignerschaft zu neuen Objekten zeigt, wie Berechtigung zugeordnet wird, wenn neue Objekte erstellt werden. Für ein verzeichnisbasiertes Objekt in einigen Dateisystemen erbt das Objekt die Primärgruppe des übergeordneten Verzeichnisses. Wenn z. B. das übergeordnete Verzeichnis als Primärgruppe RUD hat, wird RUD Probleme bekommen, wenn er versucht irgendetwas im übergeordneten Verzeichnis zu erstellen. Dies passiert deshalb, weil das gleiche Profil nicht gleichzeitig beides sein kann, Eigner und Primärgruppe für das gleiche Objekt.

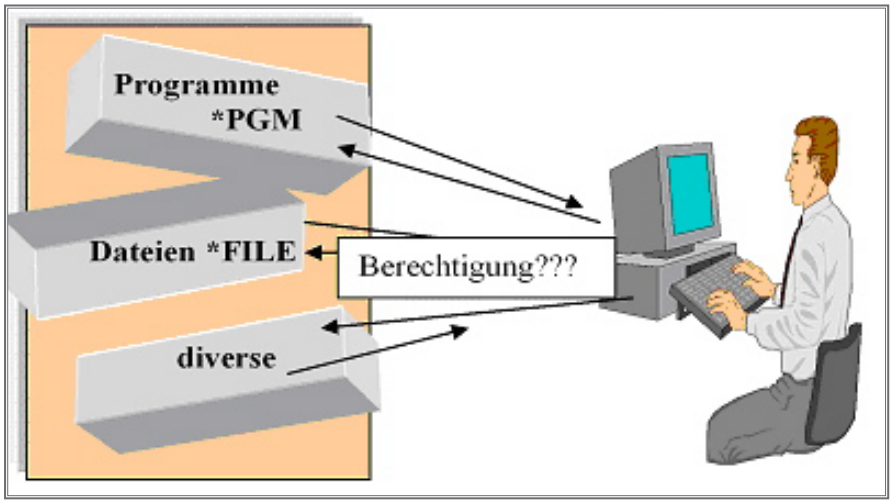
Sie können die Primärgruppe für ein bibliotheks- oder verzeichnisbasiertes Objekt mit Hilfe der folgenden Befehle ändern:

- Primärgruppe des Objekts ändern (CHGOBJPGP)
- Primärgruppe ändern (CHGPGP)
- Option 9 aus „Mit Objekten über Primärgruppen arbeiten“ (WRKOBJPGP)

Sie können die Berechtigung der Primärgruppe mit dem Befehl „Objektberechtigungen bearbeiten“ (**EDTOBJAUT**) oder den Grant- und Revoke-Befehlen ändern. Sie können die Primärgruppenberechtigung für ein bibliotheks- oder verzeichnisbasiertes Objekt mit dem Befehl „Berechtigung ändern“ (**CHGAUT**) oder mit dem Befehl „Mit Berechtigung arbeiten“ (**WRKAUT**) ändern.

9.12.12
Seite 2

9.13 Ressourcenschutz



Wer darf was?

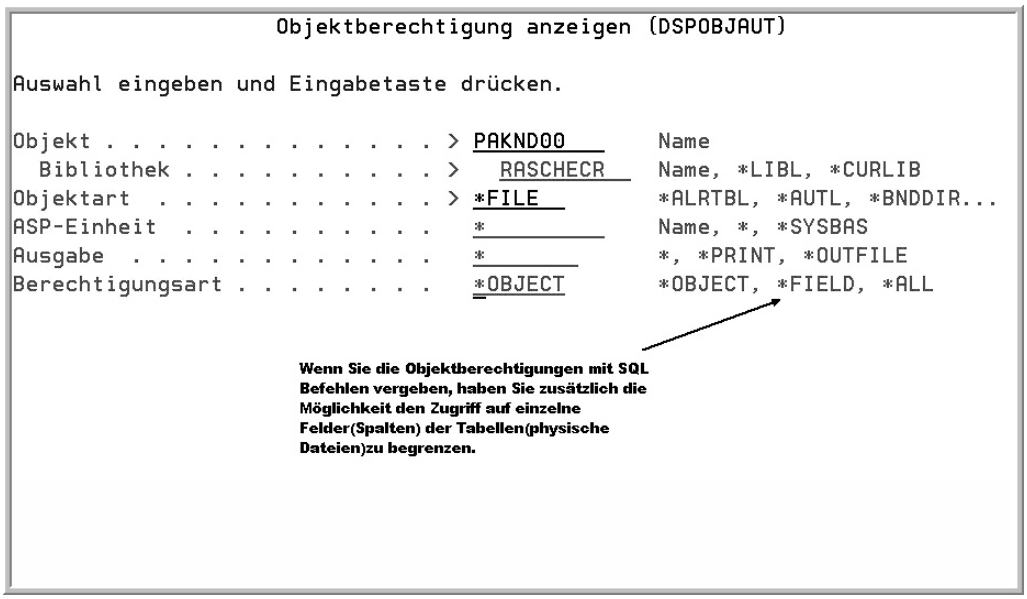
Wir wissen jetzt, wie Objekte organisiert werden, aber wie steuern wir die Zugriffsberechtigungen auf die einzelnen Objekte?

Für jedes iSeries-Objekt gibt es eine eigene Liste, wer was mit dem Objekt tun kann. Das nennt man Ressourcenschutz. Sicherheitsberechtigungen auf Objektebene unterscheiden sich von Berechtigungen auf Benutzerebene. Benutzerberechtigungen benennen für jeden Benutzer Vollmachten auf breiter Ebene, wohingegen Objekte über eine Liste von Benutzern verfügen, die mit dem Objekt arbeiten dürfen. Zunächst ist relevant, wer das Eigentumsrecht an dem Objekt besitzt. Es gibt eine Vielzahl von Benutzern und nur einer kann das Eigentumsrecht besitzen. Anderen Benutzern muss der Zugriff über spezifische Berechtigungen gewährt werden.

9.13
Seite 2

9.13.1 Objektberechtigungen verwalten

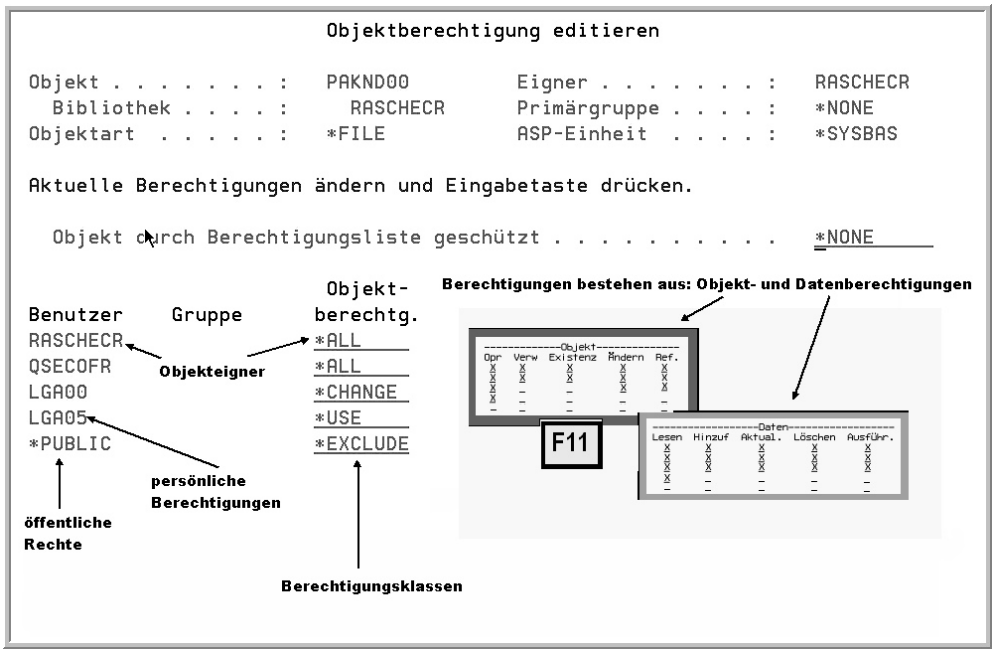
Ob Sie Objekte bearbeiten können, ist somit von Ihren spezifischen Objektberechtigungen abhängig.



Objektberechtigung anzeigen

Die Objektberechtigungen werden in persönliche Berechtigungen und öffentliche Berechtigungen unterteilt. Persönliche Berechtigungen sind Berechtigungen, die an bestimmte Benutzer vergeben werden. Allgemeine Berechtigungen gelten für alle nicht explizit genannten Benutzer und werden mit *PUBLIC gekennzeichnet. Zusätzlich wird zwischen Objektberechtigungen, d.h. Berechtigungen, die das Objekt selbst betreffen und den Datenberechtigungen differenziert. Die Datenberechtigungen beziehen sich auf den Inhalt des Objektes.

9.13.1
Seite 2



Berechtigungsklassen für Objekte

Die iSeries verwaltet die Objektberechtigungen in Objektberechtigungsklassen. Man unterscheidet die folgenden Berechtigungsklassen:

***ALL**

Der Benutzer kann alle Operationen am Objekt ausführen. Er kann die Objektexistenz steuern, die Berechtigungen für das Objekt bestimmen und das Objekt verändern. Er hat Zugriff auf alle Daten des Objektes. Es sei denn, die Daten werden durch eigene Objektberechtigungen geschützt.

***CHANGE**

Der Benutzer erhält alle Berechtigungen zum Ausführen des Objektes. Ausgenommen sind die Operationen, die über die Objektexistenzberechtigung entscheiden. Die Berechtigung *CHANGE umfasst die Änderungsberechtigungen, die Objektverwendungsberechtigung und alle Datenberechtigungen.

***USE**

Die Berechtigung *USE besagt, dass der Anwender die Objekte verwenden kann und Leseberechtigung sowie Ausführungsberechtigung für die Daten besitzt.

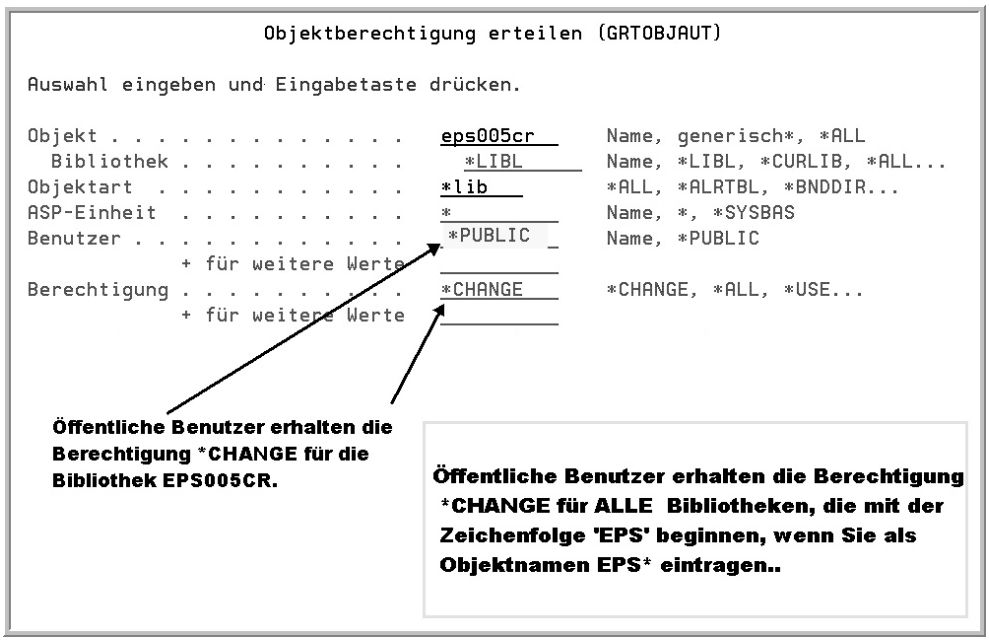
***EXCLUDE**

Der Benutzer kann nicht auf das Objekt zugreifen.

Das Erteilen, Widerrufen und Ändern von Objektberechtigungen geschieht am einzelnen Objekt. Für die Bearbeitung stehen Ihnen verschiedene Befehle zur Verfügung:

EDTOBJAUT	Objektberechtigungen editieren
RVKOBJAUT	Objektberechtigungen entziehen
GRTOBJAUT	Objektberechtigungen gewähren
DSPOBJAUT	Objektberechtigungen anzeigen

Da die Berechtigungsvergabe am einzelnen Objekt ziemlich zeitraubend sein kann, ermöglicht die iSeries die generische Identifikation von Objekten, so dass Sie mit einem Befehl alle Objekte in einer Bibliothek modifizieren können. Mit dieser Methode sparen Sie zwar Zeit, aber der Einsatz sollte sorgfältig geplant werden.



Erteilen einer Objektberechtigung

Viele Unternehmen verzichten bislang auf eine Ressourcen-Schutzstrategie, da der Schutz der Daten durch Menüs gewährleistet werden konnte. Heute sind die iSeries-Systeme aber mit anderen Plattformen vernetzt. Dieser Trend wird sich in Zukunft vermutlich weiter fortsetzen. Lokale und Remote-Benutzer erhalten dadurch neue Methoden, um auf die Daten ihrer iSeries zuzugreifen. Viele der neuen Funktionen, die IBM mit neuen Betriebssystemen ausliefert (wie z.B. FTP, ODBC, IFS oder Operation Navigator), bieten neue Wege für den Zugriff auf die Daten im Netzwerk. Das bedeutet aber nicht, dass Sie sich wieder in die „gute alte Zeit“ zurücksehnen sollten. Verteilte Computer- und Client-Server-Anwendungen haben sich etabliert und genießen zunehmende Popularität. Sie sollten daher den Einfluss der neuen Möglichkeiten bei ihrer Sicherheitsstrategie berücksichtigen.

9.13.1
Seite 4

9.14 Native Sicherheitstools

Haben Sie schon einmal versucht „Go Security“ in einer 5250-Sitzung aufzurufen? Sie werden – entsprechende Rechte vorausgesetzt – staunen, was damit alles möglich ist. „Go Security“ ist sozusagen ein Einstieg in die vielfältigen Möglichkeiten der IBM Power i Security. Schauen wir mal, was uns dieses Menü alles bietet:

```
SECURITY                          Sicherheit
                                                    System:   RAZLEE
Auswahlmöglichkeiten:

     1. Mit Objektberechtigung arbeiten
     2. Mit Berechtigungslisten arbeiten
     3. Bürosicherheit
     4. Eigenes Kennwort ändern
     5. Eigenes Benutzerprofil ändern
     6. Mit Benutzerprofilen arbeiten
     7. Mit Systemwerten arbeiten
     8. Sicherheits-Tools

    70. Zugehörige Befehle



Auswahl oder Befehl
===>

F3=Verlassen    F4=Bedienerführung    F9=Auffinden    F12=Abbrechen
F13=Unterstützende Informationen      F16=Systemhauptmenü
```

Menü Security

Wenn Sie aufmerksam gelesen haben, stimmen Sie bestimmt mit mir überein, dass wir die Inhalte der Menüpunkte 1 bis 7 bereits ausführlich beschrieben haben. Schauen wir also mal in Menüpunkt 8 – „Sicherheits-Tools“.

9.14
Seite 2

9.14.1 Sicherheitstools

Hierher kommen Sie auch direkt mit „Go Sectools“. In diesem Menü finden Sie viele nützliche Funktionen, die es Ihnen erlauben, sicherheitsrelevante Zustände im System zu prüfen und einzustellen.

```
SECTOOLS                        Sicherheits-Tools
                                                          System:   RAZLEE
Auswahlmöglichkeiten:

  Mit Profilen arbeiten
     1. Standardkennwörter analysieren

     2. Liste aktiver Profile anzeigen
     3. Liste aktiver Profile ändern
     4. Profilaktivität analysieren

     5. Aktivierungsplan anzeigen
     6. Eintrag im Aktivierungsplan ändern

     7. Verfallsplan anzeigen
     8. Eintrag im Verfallsplan ändern

                                                                Weitere ...
Auswahl oder Befehl
===>

F1=Hilfetext    F3=Verlassen    F4=Bedienerführung    F9=Auffinden
F12=Abbrechen
```

Menü Sectools

9.14.1
Seite 2

9.14.1.1 Standardkennwörter analysieren

Würden Sie als Ihr Kennwort Ihren Benutzernamen verwenden? Man mag es nicht glauben, aber tatsächlich gibt es nicht wenige Systeme, bei denen das so gehandhabt wird. Das ist natürlich ein gefundenes Fressen für unliebsame Kollegen, die so versuchen, unberechtigt an Informationen zu gelangen.

Relativieren kann man das nur ansatzweise. Verantwortliche argumentieren dann zum Beispiel, dass die betreffenden Benutzerprofile ja mit dem Attribut „Anfangsmenü" = *SIGNOFF versehen sind. Ok, damit kann sich schon mal niemand interaktiv am System anmelden, weil direkt auf die Anmeldung die Abmeldung erfolgt. Aber haben Sie schon mal darüber nachgedacht, dass ein Zugriff ja beispielsweise aus Excel via ODBC erfolgen kann? Dabei muss sich niemand interaktiv anmelden und erhält trotzdem Zugriff!

Also nichts wie weg mit diesen unseligen Kombinationen. Rufen Sie Menüpunkt 1 oder den Befehl ANZDFTPWD auf:

```
                Standardkennwörter analysieren (ANZDFTPWD)

Auswahl eingeben und Eingabetaste drücken.

Aktion für Profile . . . . . .   *NONE        *NONE, *DISABLE, *PWDEXP
                                 _____
```

Mit dem Befehl ANZDFTPWD (Standardkennwörter analysieren) kann ein Bericht gedruckt werden, der alle Benutzerprofile im System enthält, für die ein Standardkennwort gilt. Außerdem kann mit Hilfe dieses Befehls eine Aktion für die Profile durchgeführt werden. Ein Profil hat dann ein Standardkennwort, wenn das Kennwort des Benutzerprofils mit dem Namen des Profils übereinstimmt.

Wenn das System auf der Kennwortstufe 2 oder 3 ausgeführt wird, werden sowohl Werte in Großschreibung als auch Werte in Kleinschreibung für den Benutzerprofilnamen geprüft. Werte für den Benutzerprofilnamen in gemischter Groß-/Kleinschreibung werden allerdings nicht geprüft. Wenn für das Benutzerprofil JAMES also zum Beispiel das Kennwort ‚JAMES' oder ‚james' definiert ist, dann identifiziert das System diese Angabe als ein Standardkennwort. Die Kennwörter ‚JaMeS' oder ‚James' werden hingegen nicht als Standardkennwörter identifiziert.

Einschränkung: Der Benutzer muss über die Sonderberechtigungen *ALLOBJ und *SECADM verfügen, um diesen Befehl verwenden zu können.

9.14.1.1
Seite 2

Das Format des Berichts richtet sich nach der für die Profile durchgeführten Aktion. Wird keine Aktion durchgeführt, enthält jeder Eintrag den Namen und Status (STATUS) des Benutzerprofils, eine Angabe darüber, ob das Kennwort abgelaufen ist (PWDEXP) sowie die Textbeschreibung des Profils (TEXT). Wird eine Aktion für die Profile durchgeführt, enthält jeder Eintrag außerdem die Werte, die für STATUS und PWDEXP gelten, nachdem das Profil geändert wurde.

Die Liste der Benutzerprofile mit Standardkennwörtern wird zusätzlich in die Systemdatei QASECPWD in der Bibliothek QUSRSYS gestellt. Jeder Eintrag enthält den Namen des Benutzerprofils, die Werte für STATUS und PWDEXP vor und nach der Änderung sowie den TEXT-Wert. Wurde keine Aktion angefordert, gibt es kein zweites Wertepaar STATUS/PWDEXP.

Aktion für Profile (ACTION)
Die Aktion, die für Benutzerprofile mit einem Standardkennwort ausgeführt werden soll.

- ***NONE** – Für Profile mit Standardkennwort wird keine Aktion durchgeführt.
- ***DISABLE** – Das Feld STATUS des Benutzerprofils erhält den Wert *DISABLED.
- ***PWDEXP** – Das Feld PWDEXP des Benutzerprofils erhält den Wert *YES.

Beispiele für ANZDFTPWD

ANZDFTPWD ACTION(*DISABLE *PWDEXP)

Mit diesem Befehl werden alle Benutzerprofile im System analysiert. Alle Benutzerprofile im System, für die ein Standardkennwort definiert ist, werden deaktiviert, und die entsprechenden Kennwörter werden als abgelaufen definiert.

Nachdem der Befehl gelaufen ist, schauen Sie mit WRKSPLF nach der generierten Spooldatei (mit Benutzerdaten ANZDFTPWD). Wenn Sie sich die anzeigen lassen, erscheint ein Bericht, der ungefähr folgendermaßen aussieht:

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPWD                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Benutzerprofile mit Standardkennwörtern                                  Seite     1
5770SS1 V7R1M0  100423                                                  RAZLEE    05.04.14  14:01:59 CEST
 Aktion für Profile . . . . . . . . . . . . . :   *NONE
 Benutzer-
 profil         STATUS         PWDEXP     Text
 RAZLEEAA       *ENABLED        *NO       Razlee Austra
 RAZLEEFR1      *ENABLED        *NO       Razlee-Benutzer Frankreich
 TEST11         *ENABLED        *NO       Sicherheitsbeauftragter
 USRMMTEST      *ENABLED        *NO       Test user MMa
                                       * * * * *  E N D E  D E R  L I S T E  * * * * *
```

Sie sehen hier einige Benutzer, die Standardkennwörter haben. Versuchen Sie erst gar nicht, diese auf dem Dokumentationssystem zu erreichen, sie sind natürlich nur zu Dokumentationszwecken erstellt und nach dem Screenshot geändert worden.

Sie sehen an diesem Beispiel nicht nur, dass die Benutzer gleiche Kennwörter und Benutzernamen haben, sondern auch, dass diese aktiviert (Status *ENABLED) sind und die Kennwörter zudem nicht auf „enabled“ stehen, da für PWDEXP *NO angegeben ist. Insgesamt ein hohes Sicherheitsrisiko.

9.14.1.1

Seite 4

9.14.1.2 Liste aktiver Profile

Gibt es auf Ihrem System die Anforderung, Benutzerprofile nach einem bestimmten Inaktivitätszeitraum zu deaktivieren? Hierfür beschreiben wir bald, welche Möglichkeiten der Anzeige Ihnen für diese Profile zur Verfügung stehen.

Nun geht es zunächst darum, die Liste der Benutzerprofile anzuzeigen, die davon nicht betroffen sein sollen. Es gibt Benutzerprofile, die wichtig sind, mit denen sich aber nie jemand interaktiv anmelden wird. Insbesondere Verbindungsbenutzerprofile für automatisierte Aktivitäten sind davon betroffen. Damit Sie nicht versehentlich solch ein Profil deaktivieren, sind im Betriebssystem Möglichkeiten vorgesehen, die nachfolgend beschrieben werden.

```
                    Liste aktiver Profile anzeigen (DSPACTPRFL)

Auswahl eingeben und Eingabetaste drücken.

Ausgabe  . . . . . .  *          *, *PRINT
```

Mit dem Befehl DSPACTPRFL (Liste aktiver Profile anzeigen) wird die Liste der Benutzerprofile angezeigt, die immer als aktiv gelten und somit nicht von der Befehlsfunktion ANZPRFACT (Profilaktivität analysieren) deaktiviert werden. Diese IBM-Benutzerprofile, die niemals als inaktiv angenommen werden, werden nicht aufgelistet. Diese Informationen wurden mit dem Befehl CHGACTPRFL (Liste aktiver Profile ändern) zusammengestellt. Wenn der Befehl DSPACTPRFL (Liste aktiver Profile anzeigen) vor dem Befehl CHGACTPRFL ausgegeben wird, erstellt das System einen leeren Bericht.

Einschränkung: Der Benutzer muss über die Sonderberechtigung für alle Objekte (*ALLOBJ) verfügen, um diesen Befehl auszuführen.

Ausgabe (OUTPUT)
Gibt an, ob die Ausgabe des Befehls an der anfordernden Datenstation angezeigt oder gedruckt werden soll.

- * – Eine durch einen interaktiven Job angeforderte Ausgabe wird angezeigt. Eine von einem Stapeljob angeforderte Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.
- ***PRINT** – Die Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.

```
                          Liste aktiver Profile

  Folgende Profile werden nicht inaktiviert (*DISABLED), wenn
    sie die nebenstehende Anzahl an Tagen inaktiv waren  . . :   *NOMAX


Benutzer-                 Benutzer-                 Benutzer-
profil                    profil                    profil
RENGEL
```

Liste aktiver Profile

9.14.1.2
Seite 2

Beispiele für DSPACTPRFL
DSPACTPRFL OUTPUT(*PRINT)

Mit diesem Befehl wird die Liste der Profile gedruckt, die vom Befehl ANZPRFACT (Profilaktivität analysieren) immer als aktiv angenommen werden.

9.14.1.3 Liste aktiver Profile ändern

Verwenden Sie diesen Befehl, um diejenigen Benutzerprofile anzugeben, die nie deaktiviert werden sollen, auch wenn sie über den Schwellwert der Inaktivität hinausgehen.

```
                    Liste aktiver Profile ändern (CHGACTPRFL)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .          _____       Name
     + für weitere Werte
Aktion . . . . . .                  *ADD        *ADD, *REMOVE
```

Liste aktiver Profile ändern

Mit dem Befehl CHGACTPRFL (Liste aktiver Profile ändern) werden der Liste derjenigen Profile, die vom Befehl ANZPRFACT (Profilaktivität analysieren) immer als aktiv betrachtet werden, Benutzer hinzugefügt, oder aus der Liste werden Benutzer entfernt. Diese Profile werden niemals deaktiviert, auch dann nicht, wenn sie während der angegebenen Anzahl von Tagen inaktiv waren.

Es wird empfohlen, dieser Liste alle Profile hinzuzufügen, die für eigene Anwendungsobjekte erstellt wurden und nicht zum Anmelden verwendet werden. Weiterhin sollten alle übrigen IBM-Profile („Q“-Profile) hinzugefügt werden, die nicht deaktiviert werden sollen. Die in der folgenden Liste enthaltenen Profile müssen nicht hinzugefügt werden, da sie nie als inaktiv gelten.

Die folgenden Benutzerprofile werden nie als inaktiv angesehen: QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QEJBSVR, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPM400, QSECOFR, QSNADS, QSPL, QSPLJOB, QSRV, QSRVAGT, QSRVBAS, QSYS, QTCM, QTCP, QTFTP, QTMHHTTP, QTMHHTP1, QTSTRQS, QWEBADMIN, QWSERVICE, QYCMCIMOM und QYPSJSVR.

Profile, die mit dem Befehl DLTUSRPRF (Benutzerprofil löschen) gelöscht werden, werden automatisch aus der Liste der aktiven Profile entfernt.

Diese Informationen können mit dem Befehl DSPACTPRFL (Liste aktiver Profile anzeigen) angezeigt werden.

Einschränkung: Der Benutzer muss über die Sonderberechtigung für alle Objekte (*ALLOBJ) verfügen, um diesen Befehl auszuführen.

9.14.1.3
Seite 2

Benutzerprofil (USRPRF)
Dies ist ein erforderlicher Parameter und betrifft den Namen des Benutzerprofils, das der Liste der aktiven Benutzer hinzugefügt oder daraus entfernt werden soll.

Für diesen Parameter können mehrere Werte eingegeben werden.

Aktion (ACTION)
Gibt an, ob das Benutzerprofil der Datei, die die Liste der immer aktiven Benutzer enthält, hinzugefügt oder daraus gelöscht werden soll. Die Profile in dieser Liste werden nicht von der Befehlsfunktion ANZPRFACT (Profilaktivität analysieren) deaktiviert.

- ***ADD** – Das Profil wird der Liste hinzugefügt und gilt damit niemals als inaktiv.
- ***REMOVE** – Das Profil wird aus der Liste entfernt und gilt damit nach der angegebenen Anzahl von Tagen als inaktiv.

Beispiele für CHGACTPRFL
CHGACTPRFL USRPRF(JMBLOCK GARRY)ACTION(*ADD)

Mit diesem Befehl wird die Liste der Benutzerprofile geändert, die immer als aktiv angenommen werden. Die Benutzerprofile JMBLOCK und GARRY werden der Liste der Profile hinzugefügt, die vom Befehl ANZPRFACT (Profilaktivität analysieren) immer als aktiv angenommen werden.

9.14.1.4 Profilaktivität analysieren

Mit dem Befehl ANZPRFACT (Profilaktivität analysieren) wird festgestellt, ob Profile während der angegebenen Anzahl von Tagen inaktiv waren.

```
                    Profilaktivität analysieren (ANZPRFACT)

Auswahl eingeben und Eingabetaste drücken.

Anzahl inaktiver Tage  . . . . .   _______          1-366, *NOMAX
```

Profilaktivität analysieren

War ein Profil während dieses Zeitraums inaktiv, wird es deaktiviert. Das Datum, an dem das Benutzerprofil zuletzt benutzt wurde, wird verwendet, um die Anzahl von Tagen festzustellen, an denen ein Benutzerprofil inaktiv war. Ist das Datum der letzten Benutzung nicht angegeben, wird das Datum des Zurückspeicherns verwendet. Ist das Datum des Zurückspeicherns nicht angegeben, wird das Erstellungsdatum verwendet.

Wenn ein Profil deaktiviert wird, wird eine Nachricht an die Nachrichtenwarteschlange des Benutzers gesendet, der den Befehl ANZPRFACT abgesetzt hat. Die von diesem Befehl deaktivierten Profile sollten überprüft werden, um festzustellen, ob sie noch benötigt werden. Falls nicht, sollten sie gelöscht werden.

Benutzerprofile können von dieser Verarbeitung ausgenommen werden, indem sie mit dem Befehl CHGACTPRFL (Liste aktiver Profile ändern) der Liste der Profile hinzugefügt werden, die immer als aktiv gelten.

Es wird empfohlen, dieser Liste alle Profile hinzuzufügen, die für eigene Anwendungsobjekte erstellt wurden und nicht zum Anmelden verwendet werden. Weiterhin sollten alle übrigen IBM-Profile („Q“-Profile) hinzugefügt werden, die nicht deaktiviert werden sollen. Die in der folgenden Liste enthaltenen Profile müssen nicht hinzugefügt werden, da sie nie als inaktiv gelten.

QANZAGENT, QAUTPROF, QCLUMGT, QCLUSTER, QCOLSRV, QDBSHR, QDBSHRDO, QDFTOWN, QDIRSRV, QDLFM, QDOC, QDSNX, QEJB, QEJBSVR, QFNC, QGATE, QIBMHELP, QIPP, QLPAUTO, QLPINSTALL, QLWISVR, QMGTC, QMSF, QNETSPLF, QNFSANON, QNTP, QPEX, QPM400, QSECOFR, QSNADS, QSPL, QSPLJOB, QSRV, QSRVAGT, QSRVBAS, QSYS, QTCM, QTCP, QTFTP, QTMHHTTP, QTMHHTP1, QTSTRQS, QWEBADMIN, QWSERVICE, QYCMCIMOM und QYPSJSVR.

Diese Informationen können mit dem Befehl DSPACTPRFL (Liste aktiver Profile anzeigen) angezeigt werden.

9.14.1.4
Seite 2

Wenn für den Parameter INACDAYS ein Wert angegeben wird, wird täglich über einen Jobplanungseintrag QSECIDL1 überprüft, ob Profile für die angegebene Anzahl von Tagen inaktiv waren.

Um die Funktion „Profilaktivität analysieren" auszuschalten, geben Sie *NOMAX für die Anzahl inaktiver Tage an.

Der Job ANZPRFACT läuft über Nacht. Falls die Ausführungszeit dieses Jobs geändert werden soll, kann mit dem Befehl CHGJOBSCDE (Jobplanungseintrag ändern) der Job QSECIDL1 geändert werden.

Einschränkung: Der Benutzer muss über die Sonderberechtigungen *ALLOBJ, *SECADM und *JOBCTL verfügen, um diesen Befehl verwenden zu können.

Anzahl inaktiver Tage (INACDAYS)
Dies ist ein erforderlicher Parameter.

- Tage – Die Anzahl der Tage, die ein Benutzerprofil inaktiv sein kann, bevor es deaktiviert wird. Profile, die für die angegebene Anzahl von Tagen inaktiv waren, werden deaktiviert. Gültig sind Werte von 1 bis 366 oder *NOMAX.
- *NOMAX – Es gelten keine Profile als inaktiv.

Beispiele für ANZPRFACT
ANZPRFACT INACDAYS(30)

Mit diesem Befehl wird analysiert, ob Profile in den letzten 30 Tagen aktiv waren oder nicht. Benutzerprofile, die für mindestens 30 Tage inaktiv waren, werden deaktiviert.

9.14.1.5 Aktivierungsplan anzeigen

Haben Sie auch Befürchtungen, dass mit Benutzerprofilen von Mitarbeitern außerhalb der regulären Arbeitszeiten „herumgespielt“ wird? Das können Sie einfach verhindern, indem Sie die Benutzerprofile nach Feierabend deaktivieren und vor Arbeitsbeginn wieder aktivieren.

Dies bewerkstelligt die Funktion zum Eintragen und zur Anzeige der davon betroffenen Profile.

```
                    Aktivierungsplan anzeigen (DSPACTSCD)

Auswahl eingeben und Eingabetaste drücken.

Ausgabe  . . . . . . . . . . . . .   *_____          *, *PRINT
```

Aktivierungsplan anzeigen

Mit dem Befehl DSPACTSCD (Aktivierungsplan anzeigen) werden Benutzerprofile, deren Aktivierungs- und Deaktivierungszeitpunkt sowie die Tage, an denen sie aktiv werden, angezeigt. Diese Informationen befinden sich in der Datei QASECACT in der Bibliothek QUSRSYS und wurden mit dem Befehl CHGACTSCDE (Eintrag im Aktivierungsplan ändern) zusammengestellt.

Einschränkung: Der Benutzer muss über die Sonderberechtigung für alle Objekte (*ALLOBJ) verfügen, um diesen Befehl auszuführen.

Ausgabe (OUTPUT) – Gibt an, ob die Ausgabe des Befehls an der anfordernden Datenstation angezeigt oder ob sie gedruckt werden soll.

- * – Eine durch einen interaktiven Job angeforderte Ausgabe wird angezeigt. Eine von einem Stapeljob angeforderte Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.
- ***PRINT** – Die Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.

9.14.1.5
Seite 2

Beispiele für DSPACTSCD
DSPACTSCD OUTPUT(*)

Mit diesem Befehl wird der Aktivierungsplan mit der Spoolausgabe des Jobs am Bildschirm angezeigt:

```
                    Aktivierungsplan für Benutzerprofile

Benutzer-       Aktivie-        Inaktivie-
profil          rungszeit       rungszeit       Tage
RAZLEEFR1       07:00:00         18:00:00       *MON *TUE *WED *THU *FRI
```

In diesem Fall wird das Benutzerprofil RAZLEEFR1 von Montag bis Freitag jeweils um 7:00 Uhr aktiviert und um 18:00 Uhr deaktiviert.

9.14.1.6 Eintrag im Aktivierungsplan ändern

Um Benutzerprofile in die automatische Deaktivierung/Aktivierung aufzunehmen, müssen Sie diese hier hinterlegen.

```
                Eintrag im Aktiv.-Plan ändern (CHGACTSCDE)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .  __________   Name
Aktivierungszeit . . . . . .  _____      Zeit, *NONE
Inaktivierungszeit . . . . . .  _____    Zeit, *NONE
Tage . . . . . .  *ALL                   *ALL, *MON, *TUE, *WED...
     + für weitere Werte      ____
```

Eintrag im Aktivierungsplan ändern

Mit Hilfe des Befehls CHGACTSCDE (Eintrag im Aktivierungsplan ändern) kann ein Benutzerprofil zur Verfügung gestellt werden, das nur für das Anmelden während eines bestimmten Zeitraums an bestimmten Tagen gültig ist.

Wird ein neuer Plan für ein Benutzerprofil angegeben (CHGACTSCDE erneut für diesen Benutzer verwenden), ersetzt das System den vorhandenen Plan für diesen Benutzer durch die neuen Informationen.

Wenn ein Profil aktiviert oder deaktiviert wird, wird eine Nachricht an die Nachrichtenwarteschlange des Benutzers gesendet, der den Befehl CHGACTSCDE abgesetzt hat.

Der Aktivierungs- und der Deaktivierungszeitpunkt sind so definiert, dass sie für den gleichen Tag gelten. Wird beispielsweise als Aktivierungszeit 07:00 Uhr, als Deaktivierungszeit 18:00 Uhr und als Tag *MON angegeben, wird das Profil montags um 7:00 Uhr aktiviert und um 18:00 Uhr deaktiviert. Soll der Aktivierungszeitraum mehrere Tage umfassen, also beispielsweise von montags 23:00 Uhr bis dienstags 07:00 Uhr gelten, muss *ALL als Tag angegeben werden. (Das Profil ist dann täglich von 23:00 Uhr bis 07:00 Uhr aktiv.)

Um ein Benutzerprofil aus der Datei zu entfernen, so dass es nicht mehr aktiviert und deaktiviert wird, ENBTIME(*NONE) DSBTIME(*NONE) angeben.

Der Aktivierungsplan kann mit dem Befehl DSPACTSCD (Aktivierungsplan anzeigen) angezeigt werden.

Einschränkung: Der Benutzer muss über die Sonderberechtigungen *ALLOBJ, *SECADM und *JOBCTL verfügen, um diesen Befehl verwenden zu können.

9.14.1.6
Seite 2

Benutzerprofil (USRPRF)
Dies ist ein erforderlicher Parameter. Er betrifft den Namen des Benutzerprofils, das für einen bestimmten Zeitraum aktiviert werden soll.

Aktivierungszeit (ENBTIME)
Dies ist ein erforderlicher Parameter. Er betrifft die Uhrzeit an den angegebenen Tagen, zu der der Job zur Aktivierung des Benutzerprofils übergeben wird.

Ein Profil wird nicht zur angegebenen Uhrzeit aktiviert, wenn die Anzahl der maximal zulässigen ungültigen Anmeldeversuche erreicht wurde.

Anmerkung:

Obwohl die Uhrzeit mit Sekunden angegeben werden kann, kann auf Grund der Maßnahmen zur Übergabe eines Jobs und der Auslastung des Systems die exakte Uhrzeit, zu der der Job übergeben wird, von der angegebenen Uhrzeit abweichen.

- ***NONE** – Das Profil wird nicht aktiviert.
- **Aktivierungszeit** – Die Zeit, die das Benutzerprofil aktiv ist.

Deaktivierungszeit (DSBTIME)
Dies ist ein erforderlicher Parameter. Er betrifft die Uhrzeit an den angegebenen Tagen, zu der der Job zur Deaktivierung des Benutzerprofils übergeben wird.

Anmerkung:

Obwohl die Uhrzeit mit Sekunden angegeben werden kann, kann auf Grund der Maßnahmen zur Übergabe eines Jobs und der Auslastung des Systems die exakte Uhrzeit, zu der der Job übergeben wird, von der angegebenen Uhrzeit abweichen.

- ***NONE** – Das Profil wird nicht deaktiviert.
- **Inaktivierungszeit** – Die Zeit, die das Benutzerprofil inaktiv ist.

Tage (DAYS)
Die Wochentage, an denen der Job zur Aktivierung und/oder Deaktivierung des Benutzerprofils übergeben wird.

- ***ALL** – Der Job wird jeden Tag übergeben.
- ***MON** – Der Job wird montags übergeben.
- ***TUE** – Der Job wird dienstags übergeben.
- ***WED** – Der Job wird mittwochs übergeben.
- ***THU** – Der Job wird donnerstags übergeben.
- ***FRI** – Der Job wird freitags übergeben.
- ***SAT** – Der Job wird samstags übergeben.
- ***SUN** – Der Job wird sonntags übergeben.

Für diesen Parameter können mehrere Werte eingegeben werden.

Beispiele für CHGACTSCDE

```
CHGACTSCDE USRPRF(GARRY)ENBTIME(,07:00:00‘)
DSBTIME(,18:00:00‘) DAYS(*MON,*TUE,*WED,*THU,*FRI)
```

Mit diesem Befehl wird der Aktivierungsplan für das Benutzerprofil GARRY geändert. Das Benutzerprofil GARRY wird jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag um 7:00 Uhr aktiviert und um 18:00 Uhr an diesen Tagen wieder deaktiviert. Über das Wochenende bleibt das Benutzerprofil deaktiviert.

9.14.1.6

Seite 4

9.14.1.7 Verfallsplan anzeigen

Mitarbeiter, die das Unternehmen verlassen, sollten keine aktivierten Benutzerprofile hinterlassen. Daher sollten Sie sich angewöhnen, Profile ausgeschiedener Mitarbeiter umgehend zu deaktivieren. Sie brauchen das nicht an dem Tag zu tun, an dem der Mitarbeiter das letzte Mal da ist, auch hierfür bietet Ihnen das Betriebssystem Funktionen an.

```
                        Verfallsplan anzeigen (DSPEXPSCD)

Auswahl eingeben und Eingabetaste drücken.

Ausgabe  . . . . . .  *          *, *PRINT
```

Verfallsplan anzeigen

Mit dem Befehl DSPEXPSCD (Verfallsplan anzeigen) wird die Liste der Benutzerprofile, ihr Verfallsdatum und die durchzuführende Aktion (Profil deaktivieren oder löschen) angezeigt. Wenn keine Benutzerprofile für den automatischen Ablauf definiert wurden, wird ein leerer Bericht erzeugt.

Soll das Profil gelöscht werden, wird auch die Angabe für die eigenen Objekte (*NODLT, *DLT, *CHGOWN) sowie die Angabe für die Primärgruppe (*NOCHG, *CHGPGP) angezeigt. Lautet die Angabe für die eigenen Objekte *CHOWN, wird der neue Eigner angezeigt. Lautet die Angabe für die Primärgruppe *CHGPGP, werden die neue Primärgruppe und die Berechtigung für die neue Primärgruppe angezeigt.

Die Benutzerprofileinträge wurden aus folgenden Angaben hinzugefügt:

- Befehl CRTUSRPRF (Benutzerprofil erstellen) oder CHGUSRPRF (Benutzerprofil ändern) unter Angabe des Parameters USREXPDATE (Ablaufdatum für Benutzerprofil) oder des Parameters USREXPITV (Ablaufintervall für Benutzerprofil).
- Befehl CHGEXPSCDE (Eintrag im Verfallsplan ändern) wurde ausgeführt, um ein Benutzerprofil zu einem bestimmten Datum auszuführen oder zu deaktivieren.

Einschränkung: Der Benutzer muss über die Sonderberechtigung für alle Objekte (*ALLOBJ) verfügen, um diesen Befehl auszuführen.

Ausgabe (OUTPUT)
Gibt an, ob die Ausgabe des Befehls an der anfordernden Datenstation angezeigt oder ob sie gedruckt werden soll.

- * – Eine durch einen interaktiven Job angeforderte Ausgabe wird angezeigt. Eine von einem Stapeljob angeforderte Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.
- ***PRINT** – Die Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.

9.14.1.7
Seite 2

Beispiele für DSPEXPSCD
DSPEXPSCD OUTPUT(*)

Mit diesem Befehl werden alle Einträge im Verfallsplan angezeigt.

```
                          Verfallsplan für Benutzerprofile

                                              Angabe
Benutzer-    Verfalls-                        eigene    Neuer
profil         datum      Aktion             Objekte   Eigner
RAZLEEFR1    30.09.14     *DISABLE
```

Verfallsplan für Benutzerprofile

9.14.1.8 Eintrag im Verfallsplan ändern

Natürlich müssen diese Verfallsdaten zunächst einmal eingetragen werden, bevor sie angezeigt werden können.

```
                Eintrag im Verfallsplan ändern (CHGEXPSCDE)

Auswahl eingeben und Eingabetaste drücken.

Benutzerprofil . . . . . .   __________    Name
     + für weitere Werte     __________
Verfallsdatum  . . . . . .   __________    Datum, *NONE
Aktion . . . . . . . . . .   *DISABLE      *DISABLE, *DELETE
Auswahl eigener Objekte:
  Wert eigener Objekte . . . . .  *NODLT    *NODLT, *DLT, *CHGOWN
  Ben.profilname, wenn *CHGOWN    __________ Name
Angabe für Primärgruppe:
  Primärgruppenwert  . . . . . .  *NOCHG    *NOCHG, *CHGPGP
  Neue Primärgruppe  . . . . . .  __________ Name, *NONE
  Berecht. für neue Primärgruppe  _________  *OLDPGP, *PRIVATE, *ALL...
```

Eintrag im Verfallsplan ändern

Mit dem Befehl CHGEXPSCDE (Eintrag im Verfallsplan ändern) kann das Verfallsdatum für ein Benutzerprofil angegeben werden. Das verfallene Benutzerprofil kann entweder deaktiviert oder gelöscht werden.

Um einen Benutzerprofileintrag so zu ändern, dass er nicht mehr verfällt, EXPDATE(*NONE) angeben.

Diese Informationen können mit dem Befehl DSPEXPSCD (Verfallsplan anzeigen) angezeigt werden.

Wurde geplant, ein Profil zu deaktivieren oder zu löschen, wird der Job QSECEXP1 jede Nacht ausgeführt.

Einschränkung: Der Benutzer muss über die Sonderberechtigungen *ALLOBJ, *SECADM und *JOBCTL verfügen, um diesen Befehl verwenden zu können.

Benutzerprofil (USRPRF)
Dies ist ein erforderlicher Parameter. Er betrifft den Namen des Benutzerprofils, das ablaufen soll.

Für diesen Parameter können mehrere Werte eingegeben werden.

Verfallsdatum (EXPDATE)
Dies ist ein erforderlicher Parameter. Er betrifft das Verfallsdatum für das bzw. die Benutzerprofile.

- ***NONE** – Das Profil sollte aus der Liste der Benutzerprofile, die ablaufen sollen, entfernt werden.
- **Verfallsdatum** – Das Verfallsdatum des Profils.

9.14.1.8
Seite 2

Aktion (ACTION)
Die Aktion, die für das verfallene Benutzerprofil durchgeführt werden soll.

- ***DISABLE** – Das Profil wird deaktiviert.
- ***DELETE** – Das Profil wird gelöscht. Kann das Benutzerprofil nicht gelöscht werden, wird es deaktiviert.

Auswahl eigener Objekte (OWNOBJOPT)
Die Art der Arbeitsgänge, die bei den eigenen Objekten des zu löschenden Benutzerprofils durchgeführt werden sollen.

Element 1: Angabe für eigene Objekte

- ***NODLT** – Die eigenen Objekte des Benutzerprofils werden nicht geändert und das Benutzerprofil wird nicht gelöscht, wenn der Benutzer eigene Objekte hat.
- ***DLT** – Die eigenen Objekte dieses Benutzerprofils werden gelöscht. Das Benutzerprofil wird gelöscht, nachdem alle eigenen Objekte gelöscht und alle Primärgruppenobjekte übertragen wurden.
- ***CHGOWN** – Die eigenen Objekte dieses Benutzerprofils gehen in das Eigentum des angegebenen Benutzerprofils über. Das Benutzerprofil wird gelöscht, nachdem alle eigenen Objekte übertragen worden sind.
- Bei Angabe von *CHGOWN muss für das neue Benutzerprofil ein Benutzerprofilname angegeben werden. Das neue Benutzerprofil ist Eigner aller Objekte, deren Eigner das im Parameter USRPRF angegebene Benutzerprofil war.

Element 2: Benutzerprofil des neuen Eigners

- Name des Benutzerprofils – Der Name des Benutzerprofils.
- Angabe für Primärgruppe (PGPOPT) – Die Art der Operationen, die mit den Objekten durchgeführt werden sollen, für die das zu löschende Benutzerprofil die Primärgruppe ist.
- *NOCHG – Die Objekte, für die das Benutzerprofil die Primärgruppe ist, ändern sich nicht, und das Benutzerprofil wird nicht gelöscht, wenn der Benutzer die Primärgruppe für eines der Objekte ist.

Element 1: Primärgruppe von Objekten ändern

- ***CHGPGP** – Die Objekte, für die das Benutzerprofil die Primärgruppe ist, werden in das angegebene Benutzerprofil übertragen. Das Benutzerprofil wird gelöscht, nachdem alle Objekte übertragen worden sind.
- Bei Angabe von *CHGPGP muss der Name eines Benutzerprofils oder *NONE angegeben werden. Wird der Name eines Benutzerprofils angegeben, wird dieser Benutzer zur Primärgruppe für alle Objekte, für die das im Parameter USRPRF angegebene Benutzerprofil die Primärgruppe ist. Wird *NONE angegeben, besteht für alle Objekte, für die das im Parameter USRPRF angegebene Benutzerprofil die Primärgruppe ist, keine Primärgruppenzuordnung mehr.

Element 2: Benutzerprofil einer neuen Primärgruppe

- **Name des Benutzerprofils** – Der Name des Benutzerprofils. Das angegebene Benutzerprofil muss über eine Gruppennummer (GID) verfügen.
- ***NONE** – Den Objekten wird keine Primärgruppe zugeordnet.

Element 3: Neue Primärgruppenberechtigung

- ***OLDPGP** – Die neue Primärgruppe erhält dieselbe Berechtigung für das Objekt wie die alte Primärgruppe.
- ***PRIVATE** – Verfügt die neue Primärgruppe über eine persönliche Berechtigung für das Objekt, wird sie die Primärgruppe für das Objekt, und die bisherige persönliche Berechtigung wird als Primärgruppenberechtigung übernommen. Verfügt die neue Primärgruppe über keine persönliche Berechtigung für das Objekt, wird sie die Primärgruppe, jedoch ohne Berechtigung für das Objekt.
- ***ALL** – Die neue Primärgruppe erhält die Berechtigung *ALL für das Objekt.
- ***CHANGE** – Die neue Primärgruppe erhält die Berechtigung *CHANGE für das Objekt.
- ***USE** – Die neue Primärgruppe erhält die Berechtigung *USE für das Objekt.
- ***EXCLUDE** – Die neue Primärgruppe erhält die Berechtigung *EXCLUDE für das Objekt.

Beispiele für CHGEXPSCDE

CHGEXPSCDE USRPRF(RAZLEEFR1)EXPDATE(‚30/09/2014‘)
ACTION(*DELETE)

Mit diesem Befehl wird der Verfallsplaneintrag für das Benutzerprofil RAZLEEFR1 geändert. Das Benutzerprofil RAZLEEFR1 wird am 30. September 2014 gelöscht.

9.14.1.8

Seite 4

9.14.1.9 Interne Profildaten drucken

Wissen Sie, was sich hinter einem Benutzerprofil verbirgt? Dieser Befehl zeigt Ihnen auf, was im Laufe der Zeit alles an ein Benutzerprofil gekoppelt wurde.

```
                    Interne Profildaten drucken (PRTPRFINT)

Auswahl eingeben und Eingabetaste drücken.

Auswählen nach . . . . . .   *USRPRF       *USRPRF, *PCTFULL
Benutzerprofil . . . . . .   *ALL          Name, generisch*, *ALL
Voll (Prozentsatz) . . . . .  99.90        0.01-100.00
```

Interne Profildaten drucken

Mit dem Befehl PRTPRFINT (Interne Profildaten drucken) kann ein Bericht gedruckt werden, der Informationen über die Anzahl der Einträge in einem Benutzerprofilobjekt (*USRPRF) enthält. Die Anzahl der Einträge im Benutzerprofil bestimmt dessen Größe.

In einem Benutzerprofil können vier Arten Einträge vorkommen:

Eigene Objekte – Für jedes Objekt, das einem Benutzer gehört, ist in seinem Benutzerprofil (*USRPRF) ein Eintrag „eigene Objekte“ vorhanden.

Persönliche Berechtigungen – Für jede persönliche Berechtigung, die einem Benutzer erteilt wurde, ist in seinem Benutzerprofil (*USRPRF) ein Eintrag „persönliche Berechtigung“ vorhanden.

Objekte mit Berechtigung – Für jeden Benutzer, dem eine persönliche Berechtigung für ein Objekt erteilt wurde, das zu einem anderen Profil gehört, ist im Profil (*USRPRF) des Objekteigners ein Eintrag „Objekt mit Berechtigung“ vorhanden.

Primärgruppenberechtigungen – Für jedes Objekt, für das ein Benutzer die Primärgruppe ist, ist in seinem Benutzerprofil (*USRPRF) ein Eintrag „Primärgruppe“ vorhanden.

Mit jedem Eintrag wächst das Benutzerprofilobjekt (*USRPRF) weiter an. Alle Einträge zusammengenommen bestimmen die Größe des Benutzerprofils. Ein Benutzerprofil (*USRPRF) kann ca. zehn Millionen Einträge für Objekte im Zusatzspeicherpool des Systems enthalten. Darüber hinaus kann es weitere zehn Millionen Einträge für jeden unabhängigen angehängten Zusatzspeicherpool enthalten, in dem Objekte des Profils gespeichert sind bzw. der Objekte enthält, für die das Profil über persönliche Berechtigungen verfügt oder für die es als primäres Gruppenprofil definiert ist. Ein Benutzerprofil kann für die Objekte in den einzelnen Zusatzspeicherpools maximal jeweils zehn Millionen Einträge umfassen.

9.14.1.9
Seite 2

Die Gesamtzahl der Einträge entscheidet darüber, wie „voll" ein Benutzerprofil ist. Der mit diesem Befehl erstellte Bericht gibt in Form einer Prozentzahl Auskunft darüber, wie voll das Benutzerprofil ist (statt die Anzahl der Einträge in dem Profil anzugeben). Der Bericht enthält außerdem eine Prozentzahl für jede der vier Eintragsarten im *USRPRF.

Anmerkung:

Durch Rundung kann die Prozentzahl, die angibt, wann ein Profil voll ist, über 100 % liegen.

Dieser Bericht kann wahlweise für alle Benutzerprofile, einen Teil der Profile, ein bestimmtes Profil oder für alle Profile, die bis zu einem bestimmten Mindestprozentsatz voll sind, ausgeführt werden.

Beispielsweise kann der Bericht für das Profil CJW ausgeführt werden, oder er kann für alle Profile ausgeführt werden, die mindestens zu 90,90 % voll sind.

Anmerkung:

Wenn für das System unabhängige Zusatzspeicherpools angehängt wurden, können die im Bericht ausgewiesenen Prozentwerte anders als erwartet ausfallen. Diese Prozentwerte werden für jedes Profil auf Basis der Gesamtanzahl der verwendeten Einträge ermittelt. Dieser Wert wird durch die Gesamtanzahl der Einträge dividiert, die für dieses spezielle Profil verfügbar sind. Die Gesamtanzahl der für ein Profil verfügbaren Einträge variiert möglicherweise in Abhängigkeit davon, ob das Profil über Einträge für Objekte verfügt, die sich in einem angehängten, unabhängigen Zusatzspeicherpool befinden. Wenn das System zum Beispiel über zwei angehängte, unabhängige Zusatzspeicherpools verfügt und das Profil TESTUSER1 nur in einem dieser Zusatzspeicherpools Objekteinträge hat, dann stehen für das Profil TESTUSER1 20 Millionen Einträge zur Verfügung. Wenn das Profil TESTUSER2 über Objekteinträge in beiden unabhängigen Zusatzpools verfügt, beträgt die Gesamtanzahl der für TESTUSER2 verfügbaren Einträge 30 Millionen. Sind beide unabhängigen Zusatzspeicherpools jedoch abgehängt, dann beträgt die Gesamtanzahl der verfügbaren Einträge für die Profile TESTUSER1 und TESTUSER2 zehn Millionen.

Empfehlungen, wie verhindert werden kann, dass Profile voll werden:

- Es sollte nicht ein einziges Profil der Eigner sämtlicher Objekte im System sein. Beispielsweise ist es empfehlenswert, für jede Anwendung ein separates Profil zu haben, das der Eigner der Anwendung ist.
- Von IBM bereitgestellte Profile, wie zum Beispiel QSECOFR und QPGMR, sollten nicht als Eigner für eine Benutzeranwendung zugeordnet werden. Diese Profile sind bereits die Eigner vieler Objekte und werden schnell voll, wenn ihnen auch noch Benutzerobjekte (Nicht-IBM-Objekte) zugeordnet werden.
- Werden mehreren Benutzern persönliche Berechtigungen für viele Objekte erteilt, sollte die Verwendung einer Berechtigungsliste zum Sichern der Objekte in Erwägung gezogen werden. Eine Berechtigungsliste erfordert im Profil des Benutzers einen einzigen Eintrag, der die persönliche Berechtigung für diese Liste angibt, während bei Objekten ein persönlicher Berechtigungseintrag für jedes Objekt erforderlich ist. Im Profil des Objekteigners erfordern Berechtigungslisten lediglich einen Eintrag „Objekt mit Berechtigung“ für jeden Benutzer, der für die Berechtigungsliste berechtigt ist, anstelle eines solchen Eintrags für jedes Objekt, multipliziert mit der Anzahl der Benutzer, denen persönliche Berechtigung erteilt wird.

  Berechtigungslisten sind besonders nützlich, wenn persönliche Berechtigungen für Dateien erteilt werden. Dateien sind komplexe Objekte. Bei komplexen Objekten besteht jeweils ein Eintrag für jeden Bestandteil des Objekts.
  Beispiel: Im Profil eines Dateieigners ist ein Eignereintrag für jeden Bestandteil der Datei vorhanden, einschließlich ein oder zwei Einträgen für jede Teildatei. (Physische Dateien haben zwei Einträge pro Teildatei.) Wird zehn Benutzern eine persönliche Berechtigung erteilt und besteht die Datei aus 50 Teildateien, führt dies zu 100 Einträgen für „Objekte mit Berechtigung“ im Profil des Eigners. Bei Verwendung einer Berechtigungsliste bleiben die Eignereinträge gleich, aber die Anzahl der Einträge für „Objekte mit Berechtigung“ reduziert sich auf einen Eintrag für jeden Benutzer, der Berechtigung für die Berechtigungsliste erhält, durch die die Datei geschützt wird.

Anmerkung:

Der Prozentsatz, der angibt, wann ein Benutzerprofil voll ist, sollte nicht mit dem maximal zulässigen Speicher (MAXSTG) verwechselt werden, den ein Profil belegen kann. Dabei handelt es sich um zwei völlig verschiedene Konzepte.

Einschränkung: Der Benutzer muss über die Sonderberechtigung für alle Objekte (*ALLOBJ) verfügen, um diesen Befehl auszuführen.

9.14.1.9
Seite 4

Auswählen nach (SELECT)
Gibt an, nach welchen Kriterien die Benutzerprofile für den Bericht ausgewählt werden.

- ***USRPRF** – Benutzerprofile werden auf der Basis des für den Parameter USRPRF angegebenen Profilnamens für den Bericht ausgewählt.
- ***PCTFULL** – Benutzerprofile werden auf der Basis des für den Parameter PCTFULL angegebenen Werts für den Bericht ausgewählt.

Benutzerprofil (USRPRF)
Wenn für den Parameter „Auswählen nach" (SELECT) der Wert *USRPRF angegeben wurde, müssen Sie die Benutzerprofile angeben, die in den Bericht aufgenommen werden sollen.

- ***ALL** – Alle Benutzerprofile werden in den Bericht aufgenommen.
- **Benutzername** – Der Name des Benutzerprofils, das in den Bericht aufgenommen werden soll.
- **Generischer Benutzername** – Der generische Name des Benutzerprofils, das in den Bericht aufgenommen werden soll. Ein generischer Name ist eine Zeichenfolge bestehend aus einem oder mehreren Zeichen, auf die ein Stern (*) folgt.

Voll (Prozentsatz) (PCTFULL)
Wenn für den Parameter „Auswählen nach" (SELECT) der Wert *PCTFULL angegeben wurde, müssen Sie einen Wert eingeben, der als voller Prozentwert verwendet wird. Benutzerprofile, die mindestens zu dem Prozentsatz belegt sind, der in diesem Parameter angegeben ist, werden in den Bericht aufgenommen. Der angegebene Wert muss zwischen 0,01 und 100,00 liegen.

- **99,90** – Benutzerprofile, die zu mindestens 99,90 % mit Einträgen gefüllt sind, werden in den Bericht aufgenommen.
- **Belegungsprozentwert** – Ein Wert zwischen 0,01 und 100,00 für den Belegungsprozentwert.

Beispiele für PRTPRFINT
PRTPRFINT SELECT(*PCTFULL)PCTFULL(99.00)

Mit diesem Befehl wird ein Bericht der internen Informationen eines Benutzerprofils für alle Benutzerprofile gedruckt, die zu mindestens 99 % belegt sind.

```
Datei . . . . . :   QPSECPPI                                                Seite/Zeile 1/1
Steuerung . . . .   _                                                       Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                    Interne Benutzerprofildaten                                  Seite     1
5770SS1 V7R1M0  100423                                                  RAZLEE    09.04.14  14:23:31 CEST
 Auswählen nach . . . . . :   *PCTFULL
 Voll (Prozentsatz) . . . . . :     0,05
                              Prozentsatz an     Prozentsatz an     Prozentsatz an     Prozentsatz an
 Benutzer-          Voll      Einträgen für      Einträgen mit      Einträgen für      Primärgruppen-
 profil         (Prozentsatz) Eigene Objekte     pers. Berecht.     berecht. Ben.        einträgen
 QLWISVR             0,07          0,01               0,06               0,00               0,00
 QSYS                0,58          0,45               0,00               0,13               0,00
                                   * * * * *  E N D E   D E R   L I S T E  * * * * *
```

Beispiel für interne Benutzerprofildaten

9.14.1.9

Seite 6

9.14.1.10 Sicherheitsprotokollierung ändern

Viele Wege führen nach Rom. So auch diese Funktion im Menü SECTOOLS. Obwohl wir die Auditierung bereits behandelt haben, sollten diese drei Funktionen nicht fehlen.

```
                    Sicherheitsprotokoll. ändern (CHGSECAUD)

Auswahl eingeben und Eingabetaste drücken.

Systemwert QAUDCTL . . . . . .   *AUDLVL        *SAME, *ALL, *NONE...
                                 *OBJAUD
                                 *NOQTEMP
Protokollierungswerte  . . . . .  *ATNEVT        *SAME, *ALL, *DFTSET...
                                 *AUTFAIL
                                 *CREATE
                                 *DELETE
                                 *JOBDTA
                                 *OBJMGT
                                 *PGMADP
                                 *PGMFAIL
                                 *SAVRST
                                 *SECURITY
                                 *SERVICE
                                 *SPLFDTA
     + für weitere Werte         *SYSMGT
                                                              Weitere ...
F3=Verlassen    F4=Bedienerf.    F5=Aktualisieren    F12=Abbrechen
F13=Verwendung der Anzeige       F24=Weitere Tasten
```

```
                    Sicherheitsprotokoll. ändern (CHGSECAUD)

Auswahl eingeben und Eingabetaste drücken.

Anfänglicher Journalempfänger  .   AUDRCV0001     Name
  Bibliothek . . . . . .           QGPL           Name, *CURLIB
```

Sicherheitsprotokollierung ändern

Mit dem Befehl CHGSECAUD (Sicherheitsprotokollierung ändern) können die aktuellen Einstellungen der Systemwerte geändert werden, die die Protokollierung auf dem System steuern. Ist das Sicherheitsprotokolljournal QAUDJRN beim Absetzen des Befehls nicht vorhanden, wird es zusammen mit dem ersten Journalempfänger erstellt.

Einschränkung: Der Benutzer benötigt die Sonderberechtigungen *ALLOBJ und *AUDIT, um diesen Befehl verwenden zu können.

9.14.1.10
Seite 2

Systemwert QAUDCTL (QAUDCTL)
Die Einstellung für den Systemwert QAUDCTL.

Einzelwerte:
- ***SAME** – Der Systemwert QAUDCTL wird nicht geändert.
- ***ALL** – Der Systemwert QAUDCTL erhält die Werte *AUDLVL, *OBJAUD und *NOQTEMP.

Andere Werte (max. drei Wiederholungen):
- ***NOTAVL** – Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.
- ***NONE** – Auf dem System findet keine Sicherheitsprotokollierung statt. Dies ist der Standardwert.
- ***OBJAUD** – Es werden Aktionen für Objekte protokolliert, die einen anderen Objektprotokollierungswert als *NONE haben. Der Objektprotokollierungswert wird im Befehl CHGAUD (Protokollierung ändern) oder im Befehl CHGOBJAUD (Objektprotokollierung ändern) festgelegt.
- ***AUDLVL** – Die in den Systemwerten QAUDLVL und QAUDLVL2 angegebenen Aktionen werden im Sicherheitsprotokolljournal protokolliert. Die von den Aktionsprotokollierungswerten eines Benutzerprofils angegebenen Aktionen werden ebenfalls protokolliert. Die Aktionsprotokollierungswerte eines Benutzerprofils werden im Parameter AUDLVL des Befehls CHGUSRAUD (Benutzerprotokollierung ändern) angegeben.
- ***NOQTEMP** – Die meisten Objekte werden in QTEMP nicht protokolliert. *NOQTEMP muss entweder mit *OBJAUD oder *AUDLVL angegeben werden. *NOQTEMP darf nicht allein angegeben werden.

Anmerkung:

- Das Journal QAUDJRN muss in der Bibliothek QSYS vorhanden sein, damit dieser Systemwert in einen anderen Wert als *NONE geändert werden kann.
- Das Journal QAUDJRN kann erst dann gelöscht oder aus der Bibliothek QSYS in eine andere Bibliothek verschoben werden, wenn dieser Systemwert auf *NONE gesetzt worden ist.

Protokollierungswerte (QAUDLVL)
Die Einstellungen für die Systemwerte QAUDLVL und QAUDLVL2.

Wenn 16 oder weniger Werte angegeben werden, werden diese Werte im Systemwert QAUDLVL gesetzt. Werden mehr als 16 Werte angegeben, werden 15 der angegebenen Werte im Systemwert QAUDLVL zusammen mit dem Wert *AUDLVL2 angegeben. Die verbleibenden Werte werden im Systemwert QAUDLVL2 definiert.

Einzelwerte:
- ***SAME** – Die Systemwerte werden nicht geändert.
- ***ALL** – Alle Werte (mit Ausnahme der Werte, die automatisch eingebunden werden) werden ausgewählt. Beispiel: *SECURITY umfasst *SECCFG, so dass *SECCFG nicht zum Systemwert hinzugefügt wird).
- ***DFTSET** – Dem Systemwert werden die Werte *AUTFAIL, *CREATE, *DELETE, *SECURITY und *SAVRST zugeordnet.
- ***NONE** – Auf dem System wird keine Aktionsüberwachung zu Sicherheitszwecken ausgeführt. Dies ist der werkseitig eingestellte Wert.

Andere Werte (max. 115 Wiederholungen):
- ***ATNEVT** – Abrufereignisse werden protokolliert. Abrufereignisse sind Bedingungen, die eine weitere Auswertung erfordern, damit die Bedeutung der Bedingung für die Sicherheit festgestellt werden kann.

  Beispiel:
  – Überwachungsereignisse, die auf einen unbefugten Zugriff hinweisen, müssen näher untersucht werden, um festzustellen, ob es sich bei der Bedingung tatsächlich um einen unbefugten Zugriff oder einen falschen Alarm handelt.
- ***AUTFAIL** – Berechtigungsfehler werden protokolliert.

  Beispiele:
  – Alle Zugriffsfehler (Anmeldung, Berechtigung, Jobübergabe)
  – Unzulässiges Kennwort oder Benutzer-ID an einer Einheit eingegeben
- ***CREATE** – Alle Objekterstellungen werden protokolliert.
  In der Bibliothek QTEMP erstellte Objekte werden nicht protokolliert.

  Beispiele:
  – Neu erstellte Objekte
  – Objekte, die erstellt wurden, um ein bestehendes Objekt zu ersetzen
- ***DELETE** – Alle Löschungen externer Objekte im System werden protokolliert. Objekte, die aus der Bibliothek QTEMP gelöscht werden, werden nicht protokolliert.

9.14.1.10
Seite 4

- ***JOBBAS** – Jobbasisfunktionen werden protokolliert.

  Beispiele:
  – Start- und Stoppdaten eines Jobs
  – Anhalten, Freigeben, Stoppen, Fortsetzen, Ändern, Unterbrechen, Beenden, abnormal Beenden und Zuordnen der PSR (Programmstartanforderungen) zu vorab gestarteten Jobeinträgen
- ***JOBCHGUSR** – Änderungen des aktiven Benutzerprofils für einen Thread oder eines seiner Gruppenprofile werden protokolliert.
- ***JOBDTA** – Aktionen, die einen Job betreffen, werden protokolliert.

  Beispiele:
  – Start- und Stoppdaten eines Jobs
  – Anhalten, Freigeben, Stoppen, Fortsetzen, Ändern, Unterbrechen, Beenden, abnormal Beenden und Zuordnen der PSR (Programmstartanforderungen) zu vorab gestarteten Jobeinträgen
  – Ändern des aktiven Benutzerprofils für einen Thread oder Ändern von Gruppenprofilen

Anmerkung:

*JOBDTA setzt sich aus zwei Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn beide Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *JOBDTA. *JOBDTA setzt sich aus folgenden Werten zusammen:

- *JOBBAS
- *JOBCHGUSR

- ***NETBAS** – Netzbasisfunktionen werden protokolliert.

  Beispiele:
  – IP-Regelaktionen
  – Sockets-Verbindungen
  – APPN-Verzeichnissuchfilter
  – APPN-Endpunktfilter

- ***NETCLU** – Operationen für Cluster oder Cluster-Ressourcengruppen werden protokolliert.

  Beispiele:
  – Hinzufügen, Erstellen und Löschen
  – Verteilung
  – Beenden
  – Übernehmen
  – Listeninformationen
  – Entfernen
  – Starten
  – Umschalten
  – Attribute aktualisieren

- ***NETCMN** – Netzbetriebs- und Übertragungsfunktionen werden protokolliert.

  Beispiele:
  – Netzbasisfunktionen (siehe *NETBAS)
  – Operationen für Cluster oder Cluster-Ressourcengruppen (siehe *NETCLU)
  – Netzfehler (siehe *NETFAIL)
  – Sockets-Funktionen (siehe *NETSCK)

Anmerkung:

*NETCMN setzt sich aus mehreren Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn alle Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *NETCMN. *NETCMN setzt sich aus folgenden Werten zusammen:

- *NETBAS
- *NETCLU
- *NETFAIL
- *NETSCK

9.14.1.10
Seite 6

- ***NETFAIL** – Netzfehler werden protokolliert.

  Beispiel:
  – Socket-Port nicht verfügbar

- ***NETSCK** – Sockets-Tasks werden protokolliert.

  Beispiele:
  – Accept
  – Connect
  – DHCP-Adresse zugeordnet
  – DHCP-Adresse nicht zugeordnet
  – Gefilterte Mail
  – Mail zurückweisen

- ***NOTAVL** – Der Benutzer, der den Befehl ausführt, ist nicht berechtigt, den aktuellen Protokollierungswert anzuzeigen. Der Systemwert kann nicht in *NOTAVL (nicht verfügbar) geändert werden.

- ***OBJMGT** – Generische Objekttasks werden protokolliert.
  Beispiele:
  – Übertragen von Objekten
  – Umbenennen von Objekten

- ***OFCSRV** – OfficeVision wird protokolliert.

  Beispiele:
  – Änderungen des Systemverteilerverzeichnisses
  – Aufgaben, die die elektronische Post betreffen

- ***OPTICAL** – Alle optischen Funktionen werden protokolliert.

  Beispiele:
  – Hinzufügen oder Entfernen einer optischen Kassette
  – Ändern der Berechtigungsliste, die zum Schützen eines optischen Datenträgers verwendet wird
  – Öffnen einer optischen Datei oder eines optischen Verzeichnisses
  – Erstellen oder Löschen eines optischen Verzeichnisses
  – Ändern oder Abrufen der Attribute eines optischen Verzeichnisses
  – Kopieren, Versetzen oder Umbenennen einer optischen Datei
  – Kopieren eines optischen Verzeichnisses
  – Sichern eines optischen Datenträgers
  – Initialisieren oder Umbenennen eines optischen Datenträgers
  – Ändern eines optischen Sicherungsdatenträgers in einen primären Datenträger
  – Sichern oder Freigeben einer optischen Datei im Wartestatus
  – Absolutes Lesen eines optischen Datenträgers

- ***PGMADP** – Die Übernahme der Programmeignerberechtigung wird protokolliert.
- ***PGMFAIL** – Programmfehler werden protokolliert.

  Beispiele:
  – Geblockte Anweisung
  – Fehler bei Gültigkeitsprüfung
  – Domänenfehler
- ***PRTDTA** – Druckfunktionen werden protokolliert.

  Beispiele:
  – Drucken einer Spooldatei
  – Drucken mit dem Parameter SPOOL(*NO)
- ***SAVRST** – Informationen, die das Sichern und Zurückspeichern betreffen, werden protokolliert,
  – wenn Programme zurückgespeichert werden, die das Profil des Programmeigners übernehmen.
  – wenn Jobbeschreibungen zurückgespeichert werden, die Benutzernamen enthalten.
  – wenn sich der Eigner oder Berechtigungen bei zurückgespeicherten Objekten ändern.
  – wenn die Berechtigung für Benutzerprofile zurückgespeichert wird.
  – wenn ein Systemstatusprogramm zurückgespeichert wird.
  – wenn ein Systembefehl zurückgespeichert wird.
  – wenn ein Objekt zurückgespeichert wird.
- ***SECCFG** – Die Sicherheitskonfiguration wird protokolliert.

  Beispiele:
  – Erstellen, Ändern, Löschen und Zurückspeichern von Benutzerprofilen
  – Programmänderungen (CHGPGM), die nicht das Profil des Eigners übernehmen
  – Änderungen der Systemwerte, Umgebungsvariablen und Netzwerkattribute
  – Änderungen der Subsystemleitwege
  – Das Zurücksetzen des Kennworts QSECOFR von DST auf den Vorgabewert
  – Das Anfordern des Standardwerts für das Kennwort der ID des Sicherheitsbeauftragten für die Serviceprogramme
  – Änderungen des Objektprotokollierungsattributs

9.14.1.10
Seite 8

- ***SECDIRSRV** – Änderungen oder Updates bei der Ausführung von Verzeichnisservicefunktionen werden protokolliert.

  Beispiele:
  – Änderung des Protokolls
  – Erfolgreicher Bind
  – Änderung der Berechtigung
  – Änderung des Kennworts
  – Änderung des Eigentumsrechts
  – Erfolgreiches Auflösen (unbind)

- ***SECIPC** – Änderungen der Interprozesskommunikation werden protokolliert.

  Beispiele:
  Änderung des Eigentumsrechts oder der Berechtigung eines IPC-Objekts
  Erstellen, Löschen oder Abrufen eines IPC-Objekts
  Zuordnung des gemeinsam genutzten Speichers

- ***SECNAS** – Aktionen des Netzwerkauthentifizierungsservice werden protokolliert.

  Beispiele:
  – Service-Ticket gültig
  – Service-Principals stimmen nicht überein
  – Client-Principals stimmen nicht überein
  – Diskrepanz bei Ticket-IP-Adresse
  – Entschlüsselung des Tickets fehlgeschlagen
  – Entschlüsselung des Authentifikators fehlgeschlagen
  – Realm befindet sich nicht innerhalb Client- und lokalem Realm
  – Ticket ist Replay-Versuch
  – Ticket noch nicht gültig
  – Diskrepanz bei lokaler IP-Adresse
  – Entschlüsselung von KRB_AP_PRIV- oder KRB_AP_SAFE-Kontrollsummenfehler
  – KRB_AP_PRIV- oder KRB_AP_SAFE- Zeitmarkenfehler, Replay-Fehler, Reihenfolgefehler
  – GSS accept – abgelaufene Berechtigungsnachweise, Kontrollsummenfehler, Kanalbindungen
  – GSS unwrap oder GSS verify – abgelaufener Kontext, entschlüsseln/decodieren, Kontrollsummenfehler, Reihenfolgefehler

- ***SECRUN** – Sicherheitslaufzeitfunktionen werden protokolliert.

  Beispiele:
  – Änderungen des Objekteignerrechts
  – Änderungen der Berechtigungsliste oder der Objektberechtigung
  – Änderungen der Primärgruppe eines Objekts

- ***SECSCKD** – Socket-Deskriptoren werden protokolliert.

  Beispiele:
  – Ein Socket-Deskriptor wurde einem anderen Job zugeordnet.
  – Deskriptor empfangen
  – Deskriptor kann nicht benutzt werden.

- ***SECURITY** – Alle sicherheitsrelevanten Funktionen werden protokolliert.

  Beispiele:
  – Sicherheitskonfiguration (siehe *SECCFG)
  – Änderungen oder Updates bei der Ausführung von Verzeichnisservicefunktionen (siehe *SECDIRSRV)
  – Änderungen der Interprozesskommunikation (siehe *SECIPC)
  – Aktionen des Netzwerkauthentifizierungsservice (siehe *SECNAS)
  – Sicherheitslaufzeitfunktionen (siehe *SECRUN)
  – Socket-Deskriptor (siehe *SECSCKD)
  – Verwendung der Prüffunktionen (siehe *SECVFY)
  – Änderungen von Prüflistenobjekten (siehe *SECVLDL)

Anmerkung:

*SECURITY setzt sich aus mehreren Werten zusammen, damit die Protokollierung genauer angepasst werden kann. Wenn alle Werte angegeben werden, führt dies zur gleichen Art der Protokollierung wie bei Angabe von *SECURITY. *SECURITY setzt sich aus folgenden Werten zusammen:

*SECCFG

*SECDIRSRV

*SECIPC

*SECNAS

*SECRUN

*SECSCKD

*SECVFY

*SECVLDL

9.14.1.10
Seite 10

- ***SECVFY** – Die Verwendung der Prüffunktionen wird protokolliert.

  Beispiele:
  – Ein Zielbenutzerprofil wurde während einer Pass-Through-Sitzung geändert.
  – Es wurde eine interne Profilkennung generiert.
  – Alle Profilmerkmale wurden deaktiviert.
  – Es wurde die maximale Anzahl an Profilmerkmalen generiert.
  – Es wurde ein Profilmerkmal generiert.
  – Alle Profilmerkmale für einen Benutzer wurden inaktiviert.
  – Ein Benutzerprofil wurde authentifiziert.
  – Ein Office-Benutzer startete oder beendete die Verarbeitung im Namen eines anderen Benutzers.

- ***SECVLDL** – Änderungen von Prüflistenobjekten werden protokolliert.

  Beispiele:
  – Hinzufügen, Ändern, Entfernen eines Prüflisteneintrags
  – Suchen eines Prüflisteneintrags
  – Erfolgreiche oder nicht erfolgreiche Überprüfung eins Prüflisteneintrags

- ***SERVICE** – Die Veröffentlichung „System i Security Reference“, IBM Form SC41-5302 enthält eine Liste aller protokollierten Servicebefehle und API-Aufrufe.

- ***SPLFDTA** – Spooldateifunktionen werden protokolliert.

  Beispiele:
  – Erstellen, Löschen, Anzeigen, Kopieren, Anhalten und Freigeben einer Spooldatei
  – Daten aus einer Spooldatei abrufen (QSPGETSP)
  – Spooldateiattribute ändern (CHGSPLFA)

- ***SYSMGT** – Systemverwaltungstasks werden protokolliert.

  Beispiele:
  – HFS-Registrierung
  – Änderungen von Funktionen für die Oberfläche von Anwendungen
  – Änderungen der Systemantwortliste
  – Änderungen am Verzeichnis der relationalen Datenbanken (DRDA)
  – Netzdateioperationen

Anfänglicher Journalempfänger (INLJRNRCV)
Der Journalempfänger, der als erster Journalempfänger bei der Erstellung des Sicherheitsprotokolljournals QAUDJRN generiert wird. Dieser Parameter wird ignoriert, wenn das Sicherheitsprotokolljournal bereits vorhanden ist.

- Qualifikationsmerkmal 1: Anfänglicher Journalempfänger
  - **AUDRCV0001** – Der Standardwert für den ersten Journalempfänger.
  - **Name** – Der Name des Journalempfängers, der erstellt wird.
- Qualifikationsmerkmal 2: Bibliothek
  - **QGPL** – Der Standardbibliothekswert für den ersten Journalempfänger.
  - ***CURLIB** – Der Journalempfänger wird in der aktuellen Jobbibliothek gesucht. Ist für den Job keine aktuelle Bibliothek angegeben, wird QGPL verwendet.
  - **Name** – Die Bibliothek, in der der Journalempfänger erstellt werden soll.

Beispiele für CHGSECAUD

Beispiel 1:
CHGSECAUD QAUDCTL(*AUDLVL)QAUDLVL(*DFTSET)

Mit diesem Befehl wird die Systemprüffunktion aktiviert. Hierzu wird sichergestellt, dass das Sicherheitsjournal vorhanden ist. Außerdem wird der Systemwert QAUDCTL auf den Wert *AUDLVL gesetzt und der Systemwert QAUDLVL auf die Standardwertegruppe.

Beispiel 2:
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*AUTFAIL *CREATE *DELETE *JOBDTA*NETBAS *NETFAIL *OBJMGT*OPTICAL *PGMADP *PGMFAIL *PRTDTA *SAVRST *SECCFG*SECDIRSRV *SECRUN *SERVICE *SPLFDTA *SYSMGT)

Mit diesem Befehl wird die Systemprüffunktion aktiviert. Hierzu wird sichergestellt, dass das Sicherheitsjournal vorhanden ist. Außerdem wird der Systemwert QAUDCTL auf den Wert *AUDLVL gesetzt, und die Systemwerte QAUDLVL und QAUDLVL2 werden auf die angegebenen Werte gesetzt. Der Systemwert QAUDLVL enthält *AUDLVL2, *AUTFAIL, *CREATE, *DELETE, *JOBDTA, *NETBAS, *NETFAIL, *OBJMGT, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDTA, *SAVRST, *SECCFG, *SECDIRSRV und *SECRUN. Der Systemwert QAUDLVL2 enthält *SERVICE, *SPLFDTA und *SYSMGT.

9.14.1.10

Seite 12

9.14.1.11 Sicherheitsprotokollierung anzeigen

Mit dem Befehl DSPSECAUD (Sicherheitsprotokollierung anzeigen) werden aktuelle Informationen über das Sicherheitsprotokolljournal angezeigt sowie über die aktuellen Einstellungen der Systemwerte, die die Protokollierung im System steuern.

Einschränkung: Der Benutzer muss über die Sonderberechtigung (*AUDIT) verfügen, um diesen Befehl auszuführen.

```
                    Sicherheitsprotokoll. anzeigen (DSPSECAUD)

Auswahl eingeben und Eingabetaste drücken.

Ausgabe  . . . . . .  *          *, *PRINT
```

Sicherheitsprotokollierung anzeigen

Ausgabe (OUTPUT)
Gibt an, wohin die Befehlsausgabe gesendet wird.

- * – Eine von einem interaktiven Job angeforderte Ausgabe wird angezeigt. Eine von einem Stapeljob angeforderte Ausgabe wird zusammen mit der Spoolausgabe des Jobs gedruckt.
- ***PRINT** – Die Ausgabe wird mit der Spoolausgabe des Jobs gedruckt.

Beispiele für DSPSECAUD
DSPSECAUD

Mit diesem Befehl werden aktuelle Informationen zum Sicherheitsprotokolljournal und zu den aktuellen Einstellungen der Systemwerte angezeigt, mit denen die geprüften Komponenten gesteuert werden.

```
                  Aktuelle Sicherheitsprotokollierungswerte

Werte des Sicherheitsprotokollierungsjournals

  Sicherheitsjournal QAUDJRN ist vorhanden  :   Ja

  Journalempfänger für QAUDJRN  . . . . . :   AUDITR5126
    Bibliothek  . . . . . :     SMZ4DTA

Systemwerte für Sicherheitsprotokollierung

  Aktueller Systemwert QAUTCTL  . . . . . :   *AUDLVL   *OBJAUD   *NOQTEMP

  Aktueller Systemwert QAUDLVL  . . . . . :   *ATNEVT   *AUTFAIL  *CREATE
                                              *DELETE   *JOBDTA   *OBJMGT
                                              *PGMADP   *PGMFAIL  *SAVRST
                                              *SECURITY *SERVICE  *SPLFDTA
                                              *SYSMGT

                                                                  Weitere ...
Eingabetaste --> Weiter

F3=Verlassen    F12=Abbrechen
```

Anzeige der Sicherheitsprotokolleinstellungen

9.14.1.11

Seite 2

9.14.1.12 Protokolljournaleinträge kopieren

Auditierung ist eine feine Sache, geht doch keine Information aus dem Betriebssystem mehr verloren. Dumm nur, das die Anzeige der Auditjournaleinträge nicht so einfach über eine SQL-Abfrage oder Query erfolgen kann, sondern spezielle Funktionen zum Auslesen der Journalempfänger verwendet werden müssen. Eine Möglichkeit ist das Kopieren der Journaleinträge in eine physische Datei, um diese dann weiter auswerten zu können.

```
                Protokolljournaleint. kopieren (CPYAUDJRNE)

Auswahl eingeben und Eingabetaste drücken.

Journaleintragsarten . . . . . AF              *ALL, AD, AF, AP, AU, CA...
     + für weitere Werte
Ausgabedateipräfix . . . . . . QAUDIT          Name
  Bibliothek . . . . . . . . .   QTEMP          Name, *CURLIB
Auswahl für Ausgabeteildatei:
  Teildatei für Ausgabe . . . . *FIRST         Name, *FIRST
  Sätze ersetzen od. hinzufügen *REPLACE       *REPLACE, *ADD
Benutzerprofil . . . . . . . . . *ALL          Name, *ALL
Zu durchsuchender Journalempf.:
  Start Journalempfänger . . . . *CURRENT      Name, *CURRENT, *CURCHAIN
    Bibliothek . . . . . . . . .                Name, *LIBL, *CURLIB
  Ende Journalempfänger  . . . .               Name, *CURRENT
    Bibliothek . . . . . . . . .                Name, *LIBL, *CURLIB
Startdatum und Uhrzeit:
  Startdatum . . . . . . . . . . *FIRST        Datum, *FIRST
  Startzeit  . . . . . . . . . .               Zeit
                                                                Weitere ...
F3=Verlassen   F4=Bedienerf.   F5=Aktualisieren   F12=Abbrechen
F13=Verwendung der Anzeige     F24=Weitere Tasten
```

Protokolljournaleinträge kopieren

Mit dem Befehl CPYAUDJRNE (Protokolljournaleinträge kopieren) können Sicherheitsprotokollsätze vom Sicherheitsprotokolljournal (QAUDJRN) in eine oder mehrere Ausgabedateien kopiert werden. Jede ausgewählte Protokolleintragsart wird in eine separate Ausgabedatei kopiert.

Zur Anzeige der Protokolljournaleinträge, die in die Ausgabedatei kopiert wurden, kann der Befehl RUNQRY (Abfrage ausführen) verwendet werden, mit dem die Sätze einschließlich ihrer Spaltenüberschriften angezeigt werden können. Die Kombination aus dem Befehl CPYAUDJRNE und dem anschließend angegebenen Befehl RUNQRY bietet eine ähnliche Funktionalität wie der Befehl DSPAUDJRNE (Protokolljournaleinträge anzeigen), hat jedoch folgende Vorteile:

- Alle Jobeintragsarten werden unterstützt.
- Alle Protokolljournaleintragsfelder werden kopiert und sind dann verfügbar.

Informationen über alle möglichen Arten von Protokolleinträgen enthält Kapitel 9 in „System i Security Reference“, IBM Form SC41-5302.

9.14.1.12
Seite 2

Einschränkungen:

- Um diesen Befehl verwenden zu können, muss der Benutzer über die Sonderberechtigung *AUDIT verfügen.
- Der Benutzer muss über die Berechtigungen *EXECUTE und *ADD für die angegebene Bibliothek verfügen, um in dieser eine neue Ausgabedatei zu erstellen.
- Der Benutzer muss außerdem über die Berechtigungen *OBJOPR, *OBJMGT, *ADD und *DLT verfügen, um eine Teildatei einer bereits vorhandenen Ausgabedatei hinzuzufügen oder zu aktualisieren.

Journaleintragsarten (ENTTYP)
Gibt die Jobeintragsarten an, die in eine Ausgabedatei kopiert werden sollen.

Einzelwert:

***ALL** – Alle Protokolleintragsarten werden ausgewählt.

Eintragsarten (bis zu 74 Wiederholungen):

AF – Berechtigungsfehler

AD – Protokollierungsänderungen

AP – Übernommene Berechtigung anfordern

AU – Attributänderungen

CA – Änderungsberechtigung

CD – Befehlszeichenfolge

CO – Objekterstellung

CP – Änderung des Benutzerprofils

CQ – Änderung des *CRQD-Objekts

CU – Cluster Management-Operationen

CV – Verbindungsprüfung

CY – Verschlüsselungskonfiguration

DI – Verzeichnisservices

DO – Objektlöschung

DS – Rücksetzung des DST-Sicherheitskennworts

EV – Umgebungsvariablenoperationen

GR – Generischer Datensatz

GS – Socket-Deskriptor wurde einem anderen Job zugeordnet

IM – Überwachung auf unbefugten Zugriff

IP – Interprozesskommunikation

IS – Internet-Sicherheitsverwaltung

JD – Zum Benutzerparameter einer Jobbeschreibung wechseln

JS – Aktionen für Jobs

KF – Schlüsselringdatei

LD – Verzeichniseintrag verbinden, Verbindung aufheben oder Verzeichniseintrag suchen

ML – Postaktionen für Büroanwendungen

NA – Änderung des Netzattributs

ND – Unzulässige Verzeichnissuchfilter

NE – Unzulässige Sitzungsendpunktfilter

OM – Versetzen oder Umbenennen von Objekten

OR – Objekt wiederhergestellt

OW – Änderung des Objekteigentumsrechts

O1 – (Optischer Zugriff) Einzeldatei oder Verzeichnis

O2 – (Optischer Zugriff) Doppeldatei oder Verzeichnis

O3 – (Optischer Zugriff) Datenträger

PA – Programmänderung zur Übernahme der Berechtigung

PG – Änderungen einer Primärgruppe für ein Objekt

PO – Druckausgaben

PS – Profilumschaltung

PW – Ungültige Kennwörter

RA – Berechtigungsänderung während Wiederherstellung

RJ – Jobbeschreibung mit angegebenem Benutzerprofil wiederherstellen

RO – Objekteigneränderung während der Wiederherstellung

RP – Wiederherstellung des Programms für übernommene Berechtigung

RQ – Wiederherstellung eines *CRQD-Objekts

RU – Wiederherstellung der Benutzerprofilberechtigung

RZ – Änderung einer Primärgruppe bei der Wiederherstellung

9.14.1.12
Seite 4

SD – Änderungen am Systemverteilerverzeichnis

SE – Änderung des Subsystemleitwegeintrags

SF – Aktionen für Spooldateien

SG – Asynchrone Signale

SK – Verbindungen über gesicherte Sockets

SM – Änderungen der Systemverwaltung

SO – Benutzerdatenaktionen für die Serversicherheit

ST – Verwendung von Servicetools

SV – Änderungen von Systemwerten

VA – Änderung einer Zugriffssteuerungsliste

VC – Starten oder Beenden einer Verbindung

VF – Schließen der Serverdateien

VL – Überschreitung des Kontengrenzwerts

VN – An- und Abmeldung am Netzwerk

VO – Aktionen für Prüflisten

VP – Fehler beim Netzwerkkennwort

VR – Netzwerkressourcenzugriff

VS – Starten oder Beenden einer Serversitzung

VU – Änderung eines Netzwerkprofils

VV – Änderung des Servicestatus

XD – Erweiterungen von Verzeichnisservices

X0 – Netzwerkauthentifizierung

X1 – Identitätstoken

YC – Änderungen von DLO-Objekten

YR – Lesen von DLO-Objekten

ZC – Objektänderungen

ZR – Lesen von Objekten

Ausgabedateipräfix (OUTFILE)
Gibt das Präfix aller Datenbankdateien an, in die die Befehlsausgabe weitergeleitet wird. Ist keine Ausgabedatei vorhanden, wird eine vom Befehl in der angegebenen Bibliothek erstellt. Wird vom Befehl eine Ausgabedatei erstellt, dann erhält die Datei die allgemeine Berechtigung *EXCLUDE.

- **Qualifikationsmerkmal 1: Ausgabedateipräfix**
  - **QAUDIT** – Alle Namen für die Datenbankausgabedateien beginnen mit der Zeichenfolge ‚QAUDIT'. Hierbei wird die Protokolleintragsart an den Namen angehängt, um den vollständigen Dateinamen zu bilden.
    Beispiel: Wenn ENTTYP(ZR) angegeben wurde, lautet der Dateiname QAUDITZR.
  - **Namenspräfix** – Die ersten Zeichen (Stellen 1–8) des Namens aller Datenbankdateien angeben, in die die Protokolleinträge kopiert werden sollen. Die Protokolleintragsart wird an das Namenspräfix angefügt, um den vollständigen Namen der Datenbankdatei zu bilden. Wurde als Namenspräfix zum Beispiel FEB2004 definiert und ENTTYP(AF) angegeben, dann wird als Name der Datenbankdatei FEB2004AF verwendet.
- **Qualifikationsmerkmal 2: Bibliothek**
  - **QTEMP** – Die Datei wird in der Jobbibliothek QTEMP gesucht.
  - ***CURLIB** – Die Datei wird in der aktuellen Threadbibliothek gesucht. Ist für den Thread keine aktuelle Bibliothek angegeben, wird QGPL verwendet.
  - **Name** – Den Namen der Bibliothek angeben, die durchsucht werden soll.

Auswahl für Ausgabeteildatei (OUTMBR)
Gibt den Namen der Datenbankteildatei an, in die die Ausgabe des Befehls gestellt wird.

- **Element 1: Teildatei für Ausgabe**
  - ***FIRST** – Die Ausgabe wird in der ersten Teildatei der Datei gespeichert. Wird OUTMBR(*FIRST) angegeben und verfügt die Datei über keine Teildateien, erstellt das System eine Teildatei mit dem Namen der Datei, die mit Hilfe der Parameter „Ausgabedateipräfix" (OUTFILE) und „Journaleintragsarten" (ENTTYP) generiert wurde. Ist die Teildatei bereits vorhanden, können neue Sätze am Ende der bereits vorhandenen Teildatei hinzugefügt oder gelöscht werden. Alternativ hierzu kann der Inhalt der Teildatei gelöscht und anschließend durch neue Sätze ersetzt werden.
  - **Name** – Den Namen der Teildatei angeben, in die die Ausgabe gestellt werden soll. Ist die Teildatei noch nicht vorhanden, wird sie vom System erstellt.

- **Element 2: Sätze ersetzen oder hinzufügen**
  - ***REPLACE** – Das System löscht den Inhalt der vorhandenen Teildatei und fügt die neuen Sätze hinzu.
  - ***ADD** – Das System fügt die neuen Sätze am Ende der vorhandenen Sätze hinzu.

Benutzerprofil (USRPRF)
Gibt den Namen der Journaleinträge des Benutzerprofils an, die in die Ausgabedateien aufgenommen werden sollen.
- ***ALL** – In die Ausgabedateien werden Einträge für alle Benutzerprofile aufgenommen.
- **Name** – Den Namen des Benutzerprofils angeben, dessen Journaleinträge in die Ausgabedateien kopiert werden sollen.

Zu durchsuchender Journalempfänger (JRNRCV)
Gibt den ersten und letzten Journalempfänger an, deren Journaleinträge durchsucht werden.

Anmerkung:

Wenn die maximale Anzahl von Empfängern (256) im Journalempfängerbereich überschritten wird, tritt ein Fehler auf und es werden keine Journaleinträge kopiert.

Einzelwerte:
- ***CURRENT** – Die Journaleinträge im momentan zugeordneten Journalempfänger werden durchsucht.
- ***CURCHAIN** – Die Journaleinträge in der zur Zeit angehängten Journalempfängerkette werden durchsucht. Wird die Kette unterbrochen, erstreckt sich der Journalempfängerbereich vom Journalempfänger, bei dem die Kette zuletzt unterbrochen wurde, bis einschließlich zu dem Journalempfänger der angehängt ist, wenn mit dem die Umsetzung der Journaleinträge begonnen wird.

- **Element 1: Start Journalempfänger**
- **Qualifikationsmerkmal 1: Start Journalempfänger**
  - **Name** – Den Namen des ersten Journalempfängers angeben, dessen Einträge durchsucht werden sollen.
- **Qualifikationsmerkmal 2: Bibliothek**
  - ***LIBL** – Der Journalempfänger wird in der Bibliotheksliste gesucht.
  - ***CURLIB** – Der Journalempfänger wird in der aktuellen Jobbibliothek gesucht. Ist für den Job keine aktuelle Bibliothek angegeben, wird QGPL verwendet.
  - **Name** – Den Namen der Bibliothek angeben, in der sich der Journalempfänger befindet.

- **Element 2: Ende Journalempfänger**

  Einzelwerte:
  – ***CURRENT** – Der Journalempfänger, der zur Zeit angehängt ist, wird als letzter Journalempfänger verwendet.

- **Qualifikationsmerkmal 1: Ende Journalempfänger**
  – **Name** – Den Namen des letzten Journalempfängers angeben, dessen Einträge durchsucht werden sollen.

Qualifikationsmerkmal 2: Bibliothek
– ***LIBL** – Der Journalempfänger wird in der Bibliotheksliste gesucht.
– ***CURLIB** – Der Journalempfänger wird in der aktuellen Jobbibliothek gesucht. Ist für den Job keine aktuelle Bibliothek angegeben, wird QGPL verwendet.
– **Name** – Den Namen der Bibliothek angeben, in der sich der Journalempfänger befindet.

Startdatum und Uhrzeit (FROMTIME)
Gibt das Datum und die Uhrzeit des ersten zu suchenden Journaleintrags an.

Einzelwerte:
– ***FIRST** – Gibt an, dass die Suche beim ersten Satz im Journalempfänger beginnen soll.

- **Element 1: Startdatum**
  – **Datum** – Das Startdatum angeben. Die Suche beginnt beim ersten Journaleintrag mit oder nach dem angegebenen Startzeitpunkt (Uhrzeit und Datum).

- **Element 2: Startzeit**
  – **Zeit** – Die Startzeit angeben. Die Suche beginnt beim ersten Journaleintrag mit oder nach dem angegebenen Startzeitpunkt (Uhrzeit und Datum).
  Die Uhrzeit kann mit oder ohne Trennzeichen angegeben werden:
  Wird kein Zeittrennzeichen verwendet, eine Zeichenfolge von vier oder sechs Ziffern (hhmm oder hhmmss) eingeben, wobei
  hh = Stunden, mm = Minuten und ss = Sekunden.
  Wird ein Zeittrennzeichen verwendet, eine Zeichenfolge von fünf oder acht Ziffern angegeben, wobei zwischen den Stunden, Minuten und Sekunden das für den Job festgelegte Zeittrennzeichen verwendet wird. Wird dieser Befehl in der Befehlszeile eingegeben, muss die Zeichenfolge in Hochkommas eingeschlossen werden. Wird ein anderes Zeittrennzeichen als das für den Job festgelegte verwendet, kann der Befehl nicht ausgeführt werden.

9.14.1.12
Seite 8

Enddatum und Uhrzeit (TOTIME)
Gibt das Datum und die Uhrzeit der Erstellung des letzten zu suchenden Journaleintrags an.

Einzelwerte:
– ***LAST** – Gibt an, dass die Suche beim ersten Satz im Journalempfänger enden soll.

- **Element 1: Enddatum**
  – Datum – Das Enddatum angeben. Die Suche endet beim ersten Journaleintrag mit oder vor dem angegebenen Endzeitpunkt (Uhrzeit und Datum).
- **Element 2: Endzeit**
  – Zeit – Die Endzeit angeben. Die Suche endet beim ersten Journaleintrag mit oder vor dem angegebenen Endzeitpunkt (Uhrzeit und Datum).
  Die Uhrzeit kann mit oder ohne Trennzeichen angegeben werden:
  Wird kein Zeittrennzeichen verwendet, eine Zeichenfolge von vier oder sechs Ziffern (hhmm oder hhmmss) eingeben, wobei hh = Stunden, mm = Minuten und ss = Sekunden.
  Wird ein Zeittrennzeichen verwendet, eine Zeichenfolge von fünf oder acht Ziffern angegeben, wobei zwischen den Stunden, Minuten und Sekunden das für den Job festgelegte Zeittrennzeichen verwendet wird. Wird dieser Befehl in der Befehlszeile eingegeben, muss die Zeichenfolge in Hochkommas eingeschlossen werden. Wird ein anderes Zeittrennzeichen als das für den Job festgelegte verwendet, kann der Befehl nicht ausgeführt werden.

Beispiele für CPYAUDJRNE
Beispiel 1: Berechtigungsfehlersätze kopieren (AF)

CPYAUDJRNE ENTTYP(AF) – Mit diesem Befehl werden alle Protokolleinträge mit der Angabe eines Berechtigungsfehlers im aktuellen Journalempfänger kopiert und in der Teildatei QAUDITAF der Datenbankdatei QTEMP/QAUDITAF gespeichert.

Die kopierten Protokolleinträge können mit dem Befehl RUNQRY wie folgt angezeigt werden:
RUNQRY QRY(*NONE) QRYFILE((QTEMP/QAUDITAF))

Beispiel 2: Zwei Eintragsarten kopieren
CPYAUDJRNE ENTTYP(CO DO) OUTFILE(AUDITLIB/SYSTEM1)

Mit diesem Befehl können alle Protokolleinträge mit der Angabe „Objekterstellung“ oder „Objektlöschung“ im aktuellen Journalempfänger kopiert und in den Datenbankdateien AUDITLIB/SYSTEM1CO und AUDITLIB/SYSTEM1DO gespeichert werden.

Die kopierten Protokolleinträge können mit dem Befehl RUNQRY wie folgt angezeigt werden:

RUNQRY QRY(*NONE) QRYFILE((AUDITLIB/SYSTEM1CO))
OUTTYPE(*DISPLAY) OUTFORM(*RUNOPT)

RUNQRY QRY(*NONE) QRYFILE((AUDITLIB/SYSTEM1DO))
OUTTYPE(*DISPLAY) OUTFORM(*RUNOPT)

Beispiel 3: Alle Eintragsarten kopieren
CPYAUDJRNE ENTTYP(*ALL) OUTFILE(SAVEAUDIT/JUNE)
OUTMBR(SMITHJ *REPLACE) USRPRF(SMITHJ)
JRNRCV(*CURCHAIN) FROMTIME(‘06/01/2004’ ‘00:00:00’)
TOTIME(‘07/01/2004’ ‘00:00:00’)

Mit diesem Befehl können alle Protokolleinträge des Benutzerprofils SMITHJ in eine Gruppe von Datenbankdateien in der Bibliothek SAVEAUDIT kopiert werden, deren Name im Format JUNExx angegeben ist. Hierbei steht xx für die Protokolleintragsart. Die Suche nach Protokolleinträgen wird für alle Journalempfänger der aktuellen Journalempfängerkette durchgeführt. Nur die Protokolleinträge, die zwischen 12.00 Uhr nachts am 01. Juni 2004 und 12.00 Uhr nachts am 01. Juli 2004 geschrieben wurden, werden kopiert.

Anmerkung:

Die Ausführung dieses Befehls kann einen sehr langen Zeitraum in Anspruch nehmen. Die gesamte Journalempfängerkette wird wiederholt nach allen Protokolleintragsarten durchsucht.

9.14.1.12

Seite 10

9.14.1.13 Sicherheitsberichte zur Stapelverarbeitung übergeben/planen

Auditoren lieben Berichte. Mit Berichten können Sicherheitseinstellungen festgehalten und jederzeit nachgelesen werden. Entsprechend fällt der Abschnitt über Sicherheitsberichte etwas umfangreicher aus.

Mit Hilfe des Menüs „Sicherheitsberichte zur Stapelverarbeitung übergeben/planen“ (SECBATCH) können ein oder mehrere der mit den Sicherheitstools erstellten Berichte an eine Jobwarteschlange übergeben werden, damit sie zu einem späteren Zeitpunkt als Stapeljob ausgeführt werden. Die einzelnen Berichte können auch als Stapeljobs geplant werden, die einmal oder regelmäßig übergeben werden sollen.

Auswahl 1: Objekte mit Berechtigungsübernahme (PRTADPOBJ)
Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu den Objekten druckt, die die Sonderberechtigungen und persönlichen Berechtigungen eines angegebenen Benutzerprofils übernehmen sollen.

```
                              Objekte mit Berechtigungsübernahme (Gesamt)                    Seite     1
5770SS1 V7R1M0  100423                                                        RAZLEE    18.04.14  11:16:16 CEST
 Benutzerprofil . . . . . . . . :   DB
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 --------------Objekt---------------     --------------Bibliothek--------------
                           Allgem.                                 Allgem.      Persönl.
 Name           Art        Berecht.     Name           ASP-Einh.   Berecht.     Berecht.
 TESTPROC       *PGM       *CHANGE      ARD2           *SYSBAS     *CHANGE        N
                                  Objekte mit Berechtigungsübernahme (Änderungen)                Seite     2
5770SS1 V7R1M0  100423                                                        RAZLEE    18.04.14  11:16:16 CEST
 Benutzerprofil . . . . . . . . :   DB
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 Letzter Änderungsbericht . . . :   04.11.14  13:35:56
```

9.14.1.13
Seite 2

Auswahl 2: Protokolljournaleinträge (DSPAUDJRNE)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Sicherheitsjournal-Protokollbericht erstellt. Welche Art von Bericht erstellt wird, richtet sich nach den angegebenen Protokolleintragsarten und Benutzerprofilen. Der Bericht kann auf bestimmte Kalenderdaten und Uhrzeiten beschränkt werden.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPQUPRFIL                                        Seite/Zeile 1/29
Steuerung . . . .   _______                                          Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                                    ABFRAGENAME  . . . . QSECCO
                                                    BIBLIOTHEKSNAME  . . QSYS
                                                    DATEI        BIBLIOTHEK   TEILDATEI    FORMAT
                                                    QASYCOJ4     QTEMP        QASYCOJ4     QASYCOJ4
                                                    DATUM  . . . . . . . 18.04.14
                                                    UHRZEIT  . . . . . . 11:18:51
18.04.14  11:18:51
  Eintragsart Benutzer-  Objekt-    Bibliotheks- Objekt-  Büro-      DLO-         Ordner-
              profil     name       name         art      benutzer-  Name         pfad
                                                          name
Zeitmarke
CO     N      QSYS       *N         *N           *SOCKET
2014-04-18-06.01.35.444400
CO     N      #SYSLOAD   OBJD       #SYSLOAD     *FILE
2014-04-18-06.05.18.107536
CO     N      #SYSLOAD   PRB        #SYSLOAD     *FILE
2014-04-18-06.05.18.866384
CO     N      QSYS       *N         *N           *SOCKET
2014-04-18-06.06.35.880080
```

Auswahl 3: Berechtigungen für Berechtigungsliste (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der alle im System enthaltenen Berechtigungslisten enthält sowie die Benutzer, die für die einzelnen Berechtigungslisten berechtigt sind.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                         Seite/Zeile 1/1
Steuerung . . . .   _______                                          Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                                Seite     1
5770SS1 V7R1M0  100423                                                  RAZLEE    18.04.14  11:19:47 CEST
 Berecht.-              Primär-                  Berech-   List  ----------Objekt----------  ----------Daten-----------
 liste       Eigner     gruppe     Benutzer      tigung    verw  Opr  Ver  Exist  Änd.  Ref  Les.  Hin  Akt  Lös  Ausf.
 ADPAUT      QSECOFR    *NONE      *PUBLIC       *CHANGE         X                           X     X    X    X     X
                                   QSECOFR       *ALL      X     X    X     X     X     X    X     X    X    X     X
 QIWSADM     QSECOFR    *NONE      *PUBLIC       *USE            X                           X                      X
                                   QSECOFR       *ALL      X     X    X     X     X     X    X     X    X    X     X
 QLWISVR     QSYS       *NONE      *PUBLIC       *EXCLUDE
                                   QSYS          *ALL      X     X    X     X     X     X    X     X    X    X     X
                                   QTMHHTTP      *USE            X                           X                      X
 QOPTSEC     QSYS       *NONE      *PUBLIC       *CHANGE         X                           X     X    X    X     X
                                   QSYS          *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPMCCDATA   QSYS       *NONE      *PUBLIC       *EXCLUDE
                                   QSYS          *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPMCCFCN    QSYS       *NONE      *PUBLIC       *EXCLUDE
                                   QSYS          *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPQSPLJOB   QSYS       *NONE      *PUBLIC       *EXCLUDE
                                   QSYS          *ALL      X     X    X     X     X     X    X     X    X    X     X
```

Auswahl 4: Befehlsberechtigung (PRTPUBAUT)

9.14.1.13
Seite 3

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer Bibliothek enthaltenen Befehlen (*CMD) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    18.04.14  11:21:36 CEST
 Objektart  . . . . . . . . . . :   *CMD
 Angegebene Bibliothek  . . . . :   *ALL

                                        Berecht.-   Berech-   ----------Objekt----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausführ.
 #COBLIB     CRTS36CBL   *SYSBAS     QSYS        *NONE       *USE       X                          X                          X
 #RPGLIB     CRTS36RPG   *SYSBAS     QSYS        *NONE       *USE       X                          X                          X
 #RPGLIB     CRTS36RPGR  *SYSBAS     QSYS        *NONE       *USE       X                          X                          X
 #RPGLIB     CRTS36RPT   *SYSBAS     QSYS        *NONE       *USE       X                          X                          X
 ARPEGGIOL   ADSPIFSSAV  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ARSTCMDIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ARSTLIBIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ARSTOBJIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ASAVCHGIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ASAVCMDIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ASAVLIBIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ASAVOBJIFS  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 ARPEGGIOL   ATSTIFSSAV  *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
```

Auswahl 5: Persönliche Befehlsberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Befehlen druckt sowie zu den Benutzern, die für die einzelnen Befehle berechtigt sind.

Auswahl 6: DFV-Datenschutz (PRTCMNSEC)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht mit Sicherheitsinformationen über die DFV-Konfiguration des Systems erstellt.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECCMN                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                DFV-Informationen (Gesamt)                             Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    18.04.14  11:24:41 CEST
 Objektart  . . . . . . . . . . :   *DEVD

                          Einheiten-     Sicherer     Standort-                  Einzelne     Vordefin.     SNUF-Progr.
 Objektname   Objektart   kategorie      Standort     kennwort     APPN-fähig    Sitzung      Sitzung       Start
 #2345        *DEVD       *DSP
 A            *DEVD       *DSP
 ALEXS2       *DEVD       *DSP
 DSP01        *DEVD       *DSP
 GGS01        *DEVD       *DSP
 GGS1         *DEVD       *DSP
 GMGS01       *DEVD       *DSP
 LINETTCP     *DEVD       *NET
```

9.14.1.13
Seite 4

Auswahl 7: Verzeichnisberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste der Verzeichnisse (*DIR) druckt, für die nicht die allgemeine Berechtigung *EXCLUDE gilt.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R1M0  100423                                                  RAZLEE    03.05.14  15:18:08 CEST
 Objektart  . . . . . . . . . . :   *DIR
 Verzeichnis  . . . . . . . . . :   /iSecurity
                                    Berecht.-    Daten-     ---------Objekt----------   ---------------Daten----------------
 Objekt                 Eigner      liste        berecht.   Ver   Exist   Änder   Ref   Opr   Lese   Hin   Akt   Dlt   Ausf.
 SMS                    RENGEL      *NONE        *RX                                    X     X                          X
 report output          SECURITY2P  *NONE        *RX                                    X     X                          X
 DB-Gate                RAZLEEILOF  *NONE        *RX                                    X     X                          X
 IBI                    RENGEL      *NONE        *RX                                    X     X                          X
 tmp                    RAZLEEILOF  *NONE        *RX                                    X     X                          X
                             * * * * *   E N D E   D E R   L I S T E   * * * * *
```

Auswahl 8: Persönliche Verzeichnisberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen auf dem System enthaltenen Verzeichnissen druckt sowie zu den Benutzern, die für die einzelnen Verzeichnisse berechtigt sind.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen (Gesamt)                              Seite     1
5770SS1 V7R1M0  100423                                                  RAZLEE    03.05.14  15:19:15 CEST
 Verzeichnis  . . . . . . . . . :   /isecurity
 Berechtigung *PUBLIC . . . . . :   *RX
 Objektart  . . . . . . . . . . :   *DIR
                                    Primär-      Berecht.-                Daten-      -----------Objekt-----------
 Objekt                 Eigner      gruppe       liste        Benutzer    berecht.    Ver    Exist    Änder    Ref
 SMS                    RENGEL      *NONE        *NONE        *PUBLIC     *RX
                                                              RENGEL      *RWX        X      X        X        X
 report output          SECURITY2P  *NONE        *NONE        *PUBLIC     *RX
                                                              SECURITY2P  *RWX        X      X        X        X
 DB-Gate                RAZLEEILOF  *NONE        *NONE        *PUBLIC     *RX
                                                              RAZLEEILOF  *RWX        X      X        X        X
 IBI                    RENGEL      *NONE        *NONE        *PUBLIC     *RX
                                                              RENGEL      *RWX        X      X        X        X
 tmp                    RAZLEEILOF  *NONE        *NONE        *PUBLIC     *RX
                                                              RAZLEEILOF  *RWX        X      X        X        X
                                  * * * * *   E N D E   D E R   L I S T E   * * * * *
```

Auswahl 9: Dokumentberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einem Ordner enthaltenen Dokumenten (*DOC) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Dabei ist der Name des Ordners anzugeben, der durchsucht werden soll.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                      Seite/Zeile 1/1
Steuerung . . . .   _                                             Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:23:51 CEST
 In Ordner  . . . . . . . . . . :   QDIADOCS
                              Berecht.-      Berech-       Sicherheits-
 Dokument         Eigner      Liste          tigung        stufe
 QHSTPRT          QSYS        *NONE          *USE          *NONE
 QINDUSR          QSYS        *NONE          *USE          *NONE
 QPROFDOC         QSYS        *NONE          *USE          *NONE
 QPROFNOT         QSYS        *NONE          *USE          *NONE
                                  * * * * *  E N D E   D E R   L I S T E  * * * * *
```

Auswahl 10: Persönliche Dokumentberechtigung (PRTPVTAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen in einem bestimmten Ordner enthaltenen Dokumenten druckt sowie zu den Benutzern, die für die einzelnen Dokumente berechtigt sind. Der Name des Ordners, der durchsucht werden soll, muss angegeben werden.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                      Seite/Zeile 1/1
Steuerung . . . .   _                                             Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen drucken (Gesamt)                  Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:24:52 CEST
 Objektart  . . . . . . . . . . :   *DOC
 In Ordner  . . . . . . . . . . :   QDIADOCS
                              Primär-        Berecht.-                                  Berech-
 DLO              Eigner      gruppe         liste         Sicherheitsstufe  Benutzer     tigung
 QHSTPRT          QSYS        *NONE          *NONE         *NONE             QSYS         *ALL
                                                                            *PUBLIC      *USE
 QINDUSR          QSYS        *NONE          *NONE         *NONE             QSYS         *ALL
                                                                            *PUBLIC      *USE
 QPROFDOC         QSYS        *NONE          *NONE         *NONE             QSYS         *ALL
                                                                            *PUBLIC      *USE
 QPROFNOT         QSYS        *NONE          *NONE         *NONE             QSYS         *ALL
                                                                            *PUBLIC      *USE
                                  * * * * *  E N D E   D E R   L I S T E  * * * * *
```

9.14.1.13
Seite 6

Auswahl 11: Dateiberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer Bibliothek enthaltenen Dateien (*FILE) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   ________                                        Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:25:48 CEST
 Objektart  . . . . . . . . . . :   *FILE
 Angegebene Bibliothek  . . . . :   TEMP
                                                Berecht.-   Berech-   ----------Objekt-----------  ----------Daten-----------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 TEMP        P11000      *SYSBAS     QDFTOWN     *NONE       *CHANGE    X                          X     X    X    X      X
 TEMP        P11000_     *SYSBAS     QDFTOWN     *NONE       *CHANGE    X                          X     X    X    X      X
 TEMP        P11000_ORG  *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
 TEMP        SQLSAMPLE   *SYSBAS     QSECOFR     *NONE       *CHANGE    X                          X     X    X    X      X
                          * * * * *  E N D E  D E R  L I S T E  * * * * *
```

Auswahl 12: Persönliche Dateiberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Dateien druckt sowie zu den Benutzern, die für die einzelnen Dateien berechtigt sind.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   ________                                        Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:26:44 CEST
 Bibliothek . . . . . . . . . . :   TEMP
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *FILE
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                       Primär-     Berecht.-               Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner    gruppe      liste       Benutzer    tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 AUSYSID     RENGEL    *NONE       SECURITY1P  *PUBLIC     *EXCLUDE
                                               RENGEL      *ALL       X    X     X      X     X     X     X    X    X     X
                                               SECURITY1P  *ALL       X    X     X      X     X     X     X    X    X     X
 GSCALP      RENGEL    *NONE       SECURITY1P  *PUBLIC     *EXCLUDE
                                               RENGEL      *ALL       X    X     X      X     X     X     X    X    X     X
 GSCALP0001  RENGEL    *NONE       SECURITY1P  *PUBLIC     *EXCLUDE
                                               RENGEL      *ALL       X    X     X      X     X     X     X    X    X     X
                                               SECURITY1P  *ALL       X    X     X      X     X     X     X    X    X     X
 GSILOGP     SECURITY1P *NONE       SECURITY1P  *PUBLIC     *EXCLUDE
                                               SECURITY1P  *ALL       X    X     X      X     X     X     X    X    X     X
 GSILOGP_T   QSECOFR   *NONE       SECURITY1P  *PUBLIC     *EXCLUDE
```

Auswahl 13: Ordnerberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von im System enthaltenen Ordnern (*FLR) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                    Seite/Zeile 1/1
Steuerung . . . .   _                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)          Seite     1
5770SS1 V7R1M0  100423                                    RAZLEE    03.05.14  15:27:48 CEST

                        Berecht.-   Berech-     Sicherheits-
 Ordner       Eigner    liste       tigung      stufe          In Ordner
 QDIADOCS     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2924     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2928     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2932     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2939     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2940     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2942     QSYS      *NONE       *CHANGE     *NONE          *NONE
 QIWSADM      QSECOFR   QIWSADM     *USE        *NONE          *NONE
 MODEL        QSECOFR   QIWSADM     *USE        *NONE          QIWSADM
 USER         QSECOFR   QIWSADM     *USE        *NONE          QIWSADM
                          * * * * *  E N D E  D E R  L I S T E  * * * * *
```

Auswahl 14: Persönliche Ordnerberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen im System enthaltenen Ordnern druckt sowie zu den Benutzern, die für die einzelnen Ordner berechtigt sind.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen drucken (Gesamt)            Seite     1
5770SS1 V7R1M0  100423                                    RAZLEE    03.05.14  15:28:35 CEST
 Objektart  . . . . . . . . . . :   *FLR
 In Ordner  . . . . . . . . . . :   *NONE
                          Primär-     Berecht.-                                 Berech-
 DLO          Eigner      gruppe      liste       Sicherheitsstufe  Benutzer    tigung
 PS           QSPLJOB     *NONE       *NONE       *NONE             QSPLJOB     *ALL
                                                                    *PUBLIC     *EXCLUDE
 QDIADOCS     QSYS        *NONE       *NONE       *NONE             QSYS        *ALL
                                                                    *PUBLIC     *CHANGE
 QFOSDIA      QSECOFR     *NONE       *NONE       *NONE             QSECOFR     *ALL
                                                                    *PUBLIC     *EXCLUDE
 QFOS2924     QSYS        *NONE       *NONE       *NONE             QSYS        *ALL
                                                                    *PUBLIC     *CHANGE
 QFOS2928     QSYS        *NONE       *NONE       *NONE             QSYS        *ALL
                                                                    *PUBLIC     *CHANGE
 QFOS2932     QSYS        *NONE       *NONE       *NONE             QSYS        *ALL
                                                                    *PUBLIC     *CHANGE
 QFOS2939     QSYS        *NONE       *NONE       *NONE             QSYS        *ALL
```

9.14.1.13
Seite 8

Auswahl 15: Jobbeschreibungsberechtigung (PRTJOBDAUT)
Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer angegebenen Bibliothek enthaltenen Jobbeschreibungen druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet und für die ein Benutzername in der Jobbeschreibung angegeben ist.

```
                                        Spool-Datei anzeigen
Datei . . . . . :   QPSECJOBD                                                  Seite/Zeile 1/1
Steuerung . . . .   ________                                                   Spalten     1 - 130
Suchen  . . . . .   _____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                           Jobbeschreibungen mit Zugriffsberechtigung (Gesamt)                          Seite     1
5770SS1 V7R1M0  100423                                                    RAZLEE    03.05.14  15:29:19 CEST
 Angegebene Bibliothek  . . . . :   *ALL
                                                    -----------------Sonderberechtigungen------------------
             Job-                                   Benutzer-    *ALL   *AUD   *IOSYS   *JOB   *SAV   *SEC   *SER   *SPL
 Bibliothek  beschreib.  ASP-Einh.   Eigner         profil        OBJ    IT      CFG     CTL    SYS    ADM   VICE    CTL
 QGPL        QCTXFORM    *SYSBAS     QSYS          QUSER
 QGPL        QSPLAFPW    *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLDBR     *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLDKTR    *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLDKTW    *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLPRTW    *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLRMTW    *SYSBAS     QSPL          QSPLJOB
 QGPL        QSPLSTRWTR  *SYSBAS     QSPL          QSPLJOB
 QHTTPSVR    QZHBHTTP    *SYSBAS     QSYS          QTMHHTTP
 QHTTPSVR    QZSRCOLS    *SYSBAS     QSYS          QTMHHTTP
 QINMEDIA    QSPLERROR   *SYSBAS     QSYS          QSPLJOB
 QPDA        RLUJD       *SYSBAS     QSYS          QUSER
 QPDA        SDAJD       *SYSBAS     QSYS          QUSER
```

Auswahl 16: Bibliotheksberechtigung (PRTPUBAUT)

9.14.1.13
Seite 9

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von im System enthaltenen Bibliotheken (*LIB) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Es kann auch angegeben werden, eine Liste bestimmter innerhalb dieser Bibliotheken enthaltener Objektarten zu drucken, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                                   Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   _____                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:30:08 CEST
 Objektart  . . . . . . . . . . :   *LIB
 Angegebene Bibliothek  . . . . :   QSYS
                                                 Berecht.-  Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        #CGULIB     *SYSBAS     QSYS        *NONE      *USE      X                          X                          X
 QSYS        #COBLIB     *SYSBAS     QSYS        *NONE      *USE      X                          X                          X
 QSYS        #DFULIB     *SYSBAS     QSYS        *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        #DSULIB     *SYSBAS     QSYS        *NONE      *USE      X                          X                          X
 QSYS        #LIBRARY    *SYSBAS     QSYS        *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        #RPGLIB     *SYSBAS     QSYS        *NONE      *USE      X                          X                          X
 QSYS        #SEULIB     *SYSBAS     QSYS        *NONE      *USE      X                          X                          X
 QSYS        ALEX        *SYSBAS     RAZLEEILOF  *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        ALEX2       *SYSBAS     RAZLEEILOF  *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        ARD         *SYSBAS     RAZLEEILOF  *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        ARD2        *SYSBAS     RAZLEEILOF  *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        ARPEGGIOL   *SYSBAS     ARPEGGIO    *NONE      *CHANGE   X                          X     X    X    X       X
 QSYS        ARPZIP      *SYSBAS     RAZLEEILIL  *NONE      *CHANGE   X                          X     X    X    X       X
```

Auswahl 17: Persönliche Bibliotheksberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen auf dem System enthaltenen Bibliotheken druckt sowie zu den Benutzern, die für die einzelnen Bibliotheken berechtigt sind.

```
                                   Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   _____                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:30:44 CEST
 Bibliothek . . . . . . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . . . . . . :   *LIB
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                      Primär-    Berecht.-                Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner   gruppe     liste      Benutzer      tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #CGULIB     QSYS     *NONE      *NONE      *PUBLIC       *USE      X                          X                          X
                                            QSYS          *ALL      X    X    X      X      X    X     X    X    X       X
 #COBLIB     QSYS     *NONE      *NONE      *PUBLIC       *USE      X                          X                          X
                                            QSYS          *ALL      X    X    X      X      X    X     X    X    X       X
 #DFULIB     QSYS     *NONE      *NONE      *PUBLIC       *CHANGE   X                          X     X    X    X       X
                                            QSYS          *ALL      X    X    X      X      X    X     X    X    X       X
 #DSULIB     QSYS     *NONE      *NONE      *PUBLIC       *USE      X                          X                          X
                                            QSYS          *ALL      X    X    X      X      X    X     X    X    X       X
 #LIBRARY    QSYS     *NONE      *NONE      *PUBLIC       *CHANGE   X                          X     X    X    X       X
                                            QSYS          *ALL      X    X    X      X      X    X     X    X    X       X
 #RPGLIB     QSYS     *NONE      *NONE      *PUBLIC       *USE      X                          X                          X
```

9.14.1.13
Seite 10

Auswahl 18: Objektberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von angegebenen Objektarten druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Die Objektart, nach der gesucht werden soll, muss angegeben werden.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R1M0  100423                                          RAZLEE    03.05.14  15:31:35 CEST
 Objektart  . . . . . . . . . . . :   *AUTL
 Angegebene Bibliothek  . . . . :   QSYS
                                                Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.   Eigner     liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        ADPAUT      *SYSBAS     QSECOFR    *NONE       *CHANGE    X                          X     X    X    X      X
 QSYS        QIWSADM     *SYSBAS     QSECOFR    *NONE       *USE       X                          X                       X
 QSYS        QOPTSEC     *SYSBAS     QSYS       *NONE       *CHANGE    X                          X     X    X    X      X
 QSYS        QPWFSERVER  *SYSBAS     QSYS       *NONE       *USE       X                          X                       X
 QSYS        QSYLMTJAVA  *SYSBAS     QSYS       *NONE       *USE       X                          X                       X
                          * * * * *  E N D E  D E R  L I S T E  * * * * *
```

Auswahl 19: Persönliche Berechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von angegebenen Objektarten druckt sowie die persönlichen Berechtigungen für die einzelnen Objekte. Die Objektart, nach der gesucht werden soll, muss angegeben werden.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen (Gesamt)                              Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    18.08.14  10:33:37 CEST
 Berecht.-              Primär-                 Berech-   List  ----------Objekt----------  ----------Daten----------
 liste       Eigner     gruppe      Benutzer    tigung    verw  Opr  Ver  Exist  Änd.  Ref  Les.  Hin  Akt  Lös  Ausf.
 ADPAUT      QSECOFR    *NONE       *PUBLIC     *CHANGE           X                          X     X    X    X      X
                                    QSECOFR     *ALL       X      X    X     X     X     X    X     X    X    X      X
 QIWSADM     QSECOFR    *NONE       *PUBLIC     *USE              X                          X                       X
                                    QSECOFR     *ALL       X      X    X     X     X     X    X     X    X    X      X
 QLWISVR     QSYS       *NONE       *PUBLIC     *EXCLUDE
                                    QSYS        *ALL       X      X    X     X     X     X    X     X    X    X      X
                                    QTMHHTTP    *USE              X                          X                       X
 QOPTSEC     QSYS       *NONE       *PUBLIC     *CHANGE           X                          X     X    X    X      X
                                    QSYS        *ALL       X      X    X     X     X     X    X     X    X    X      X
 QPMCCDATA   QSYS       *NONE       *PUBLIC     *EXCLUDE
                                    QSYS        *ALL       X      X    X     X     X     X    X     X    X    X      X
 QPMCCFCN    QSYS       *NONE       *PUBLIC     *EXCLUDE
```

Auswahl 20: Programmberechtigung (PRTPUBAUT)

9.14.1.13
Seite 11

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer Bibliothek enthaltenen Programmen (*PGM) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. In diese Liste werden nur Programme aufgenommen, die vom Benutzer aufgerufen werden können und deren Berechtigung nicht *EXCLUDE lautet.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   _                                               Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                            Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    18.08.14  10:38:08 CEST
 Objektart  . . . . . . . . . . :   *PGM
 Angegebene Bibliothek  . . . . :   *ALL
                                                 Berecht.-   Berech-   ----------Objekt-----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner       liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 #CGULIB     QCGEXIT1    *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #COBLIB     #CB00       *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #DFULIB     #DFEX       *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #DFULIB     #DFMP       *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #DFULIB     QDZEXIT1    *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #DSULIB     #EDIS       *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #DSULIB     QSUEXTED    *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #RPGLIB     #AUTO       *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
 #RPGLIB     #RPG        *SYSBAS     QSYS        *NONE       *USE      X                             X                        X
```

Auswahl 21: Persönliche Programmberechtigung (PRTPVTAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Programmen druckt sowie zu den Benutzern, die für die einzelnen Programme berechtigt sind.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   _                                               Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    19.08.14  07:47:58 CEST
 Bibliothek . . . . . . . . . . :   RLG
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *PGM
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                        Primär-     Berecht.-               Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner     gruppe      liste       Benutzer    tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 RE_AUD      RENGEL     *NONE       *NONE       *PUBLIC     *CHANGE   X                             X     X    X    X    X
                                                RENGEL      *ALL      X    X    X      X      X    X     X    X    X    X
 RE_AUD_     RENGEL     *NONE       *NONE       *PUBLIC     *CHANGE   X                             X     X    X    X    X
                                                RENGEL      *ALL      X    X    X      X      X    X     X    X    X    X
 RE_AUD__    RENGEL     *NONE       *NONE       *PUBLIC     *CHANGE   X                             X     X    X    X    X
                                                RENGEL      *ALL      X    X    X      X      X    X     X    X    X    X
 RE_AUD_MMA  RAZLEEFR   *NONE       *NONE       *PUBLIC     *CHANGE   X                             X     X    X    X    X
                                                RAZLEEFR    *ALL      X    X    X      X      X    X     X    X    X    X
                                                RENGEL      *ALL      X    X    X      X      X    X     X    X    X    X
```

9.14.1.13
Seite 12

Auswahl 22: Benutzerprofilberechtigung (PRTPUBAUT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von im System enthaltenen Benutzerprofilen druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QSYSPRT                                          Seite/Zeile 1/6
Steuerung . . . .   _______                                          Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Hardcopy-Ausgabe                                  Seite   1
   5770SS1 V7R2M0 140418                      Hardcopy-Ausgabe      RAZLEE         19.08.14 07:48:07            Seite
   Bildschirmeinheit . . . . :  QPADEV0004
   Benutzer  . . . . . . . . :  RENGEL
                                    Spool-Datei anzeigen
 Datei . . . . . :   QPSECPVT                                         Seite/Zeile 1/1
 Steuerung . . . .                                                    Spalten     1 - 130
 Suchen  . . . . .
 *...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....
                              Persönliche Berechtigungen (Gesamt)                          Seite
 5770SS1 V7R2M0  140418                                                RAZLEE    19.08.14  07:47:58 CES
  Bibliothek . . . . . . . . . . :   RLG
    Berechtigung *PUBLIC . . . . :     *CHANGE
  Objektart  . . . . . . . . . . :   *PGM
  ASP-Einheit  . . . . . . . . . :   *SYSBAS
                        Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
  Objekt      Eigner    gruppe      liste      Benutzer    tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
  RE_AUD      RENGEL    *NONE       *NONE      *PUBLIC     *CHANGE    X                              X     X    X    X     X
                                               RENGEL      *ALL       X    X     X      X     X    X     X    X    X     X
```

Auswahl 23: Persönliche Benutzerprofilberechtigung (PRTPVTAUT)

9.14.1.13
Seite 13

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht zu allen auf dem System enthaltenen Benutzerprofilen druckt sowie zu den Benutzern, die für die einzelnen Benutzerprofile berechtigt sind.

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                  Seite     1
5770SS1 V7R2M0  140418                                        RAZLEE    19.08.14  07:48:36 CEST
 Objektart  . . . . . . . . . . :   *USRPRF
 Angegebene Bibliothek  . . . . :   QSYS
                                          Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.  Eigner  liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        QDBSHR      *SYSBAS    QSYS                USER DEF                                    X         X
 QSYS        QDBSHRDO    *SYSBAS    QSYS                USER DEF                                    X         X
 QSYS        QTMPLPD     *SYSBAS    QSYS                USER DEF   X
                          * * * * *  E N D E  D E R  L I S T E  * * * * *
```

```
                                  Spool-Datei anzeigen
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen (Gesamt)                            Seite     1
5770SS1 V7R2M0  140418                                        RAZLEE    19.08.14  07:49:09 CEST
 Bibliothek . . . . . . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . . . . . . :   *USRPRF
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                        Primär-     Berecht.-                Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner     gruppe      liste      Benutzer      tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #SYSLOAD    QSECOFR    *NONE                  *PUBLIC       *EXCLUDE
                                               QSECOFR       *ALL      X    X    X      X      X    X     X    X    X    X
                                               #SYSLOAD      USER DEF  X    X                       X     X    X    X    X
 ARPEGGIO    RAZLEEILIL *NONE                  *PUBLIC       *EXCLUDE
                                               RAZLEEILIL    *ALL      X    X    X      X      X    X     X    X    X    X
                                               ARPEGGIO      USER DEF  X    X                       X     X    X    X    X
 CODESCOPE   RENGEL     *NONE                  *PUBLIC       *EXCLUDE
                                               RENGEL        *ALL      X    X    X      X      X    X     X    X    X    X
                                               CODESCOPE     USER DEF  X    X                       X     X    X    X    X
```

9.14.1.13
Seite 14

Auswahl 24: Job- und Ausgabewarteschlangenberechtigung (PRTQAUT)
Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht mit Informationen über die Ausgabe- und Jobwarteschlangenberechtigungen für Objekte in einer angegebenen Bibliothek erstellt.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECQ                                          Seite/Zeile 1/1
Steuerung . . . .   _____                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Warteschlangenberechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    19.08.14  07:50:33 CEST
 Angegebene Bibliothek  . . . . :   *ALL
                                                    Berech-
 Bibliothek     Objekt         Art          Eigner  tigung      DSPDTA     OPRCTL     AUTCHK
 #SYSLOADX      OUTPUT         *OUTQ        QSECOFR *EXCLUDE    *NO        *YES       *OWNER
 #SYSLOADX      #SYSLOADQ      *JOBQ        QSECOFR *EXCLUDE    *NONE      *NO        *DTAAUT
 FB400          FBACKUPQ       *JOBQ        QSECOFR *USE        *NONE      *YES       *OWNER
 QDP4           QZSNDPR        *JOBQ        QSYS    *USE        *NONE      *YES       *OWNER
 QGPL           QDKT           *OUTQ        QPGMR   *USE        *NO        *YES       *OWNER
 QGPL           QPFROUTQ       *OUTQ        QSYS    *CHANGE     *YES       *YES       *OWNER
 QGPL           QPRINT         *OUTQ        QPGMR   *USE        *NO        *YES       *OWNER
 QGPL           QPRINTS        *OUTQ        QPGMR   *USE        *NO        *YES       *OWNER
 QGPL           QPRINT2        *OUTQ        QPGMR   *USE        *NO        *YES       *OWNER
 QGPL           QBASE          *JOBQ        QPGMR   *USE        *NONE      *YES       *OWNER
 QGPL           QBATCH         *JOBQ        QPGMR   *USE        *NONE      *YES       *OWNER
```

Auswahl 25: Subsystemberechtigung (PRTSBSDAUT)
Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer Bibliothek enthaltenen Subsystembeschreibungen druckt, die im DFV-Eintrag einen Standardbenutzer enthalten.

```
                                    Spool-Datei anzeigen
Datei . . . . . :   QPSECSBSD                                       Seite/Zeile 1/1
Steuerung . . . .   _____                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                            Subsystembeschreibung (Gesamt)                           Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    19.08.14  07:51:11 CEST
 Angegebene Bibliothek  . . . . :   *ALL
                                                Standard-   ----------------Sonderberechtigungen-----------------
 Subsystem-   Subsystem-            Subsystem-  benutzer-   *ALL  *AUD  *IOSYS  *JOB  *SAV  *SEC  *SER  *SPL
 bibliothek   name        ASP-Einh. eigner      profil      OBJ   IT    CFG     CTL   SYS   ADM   VICE   CTL
 QINMEDIA     QSYSWRK     *SYSBAS   QSYS        QUSER
 QINMEDIA     QSYSWRK     *SYSBAS   QSYS        QPM400                    X       X
 QINMEDIA     QSYSWRK     *SYSBAS   QSYS        QPM400                    X       X
 QINPRIOR     QCMN        *SYSBAS   QSYS        QUSER
 QINPRIOR     QCMN        *SYSBAS   QSYS        QIJS
 QINPRIOR     QSYSWRK     *SYSBAS   QSYS        QUSER
 QINPRIOR     QSYSWRK     *SYSBAS   QSYS        QPM400                    X       X
 QINPRIOR     QSYSWRK     *SYSBAS   QSYS        QIJS
 QINPRIOR     QSYSWRK     *SYSBAS   QSYS        QPM400                    X       X
```

Auswahl 26: Systemsicherheitsattribute (PRTSYSSECA)

9.14.1.13
Seite 15

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht mit sicherheitsrelevanten Systemwerten und Netzwerkattributen in eine Spooldatei ausgibt. Der Bericht enthält die aktuellen und die empfohlenen Werte.

```
Datei . . . . . :   QPSECATTR                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                            Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                   Systemsicherheitsattribute                                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    19.08.14  07:58:04 CEST
 Systemwert
 Name                 Aktueller Wert                          Empfohlener Wert
    QALWOBJRST        *ALL                                    *NONE
    QALWUSRDMN        *ALL                                    QTEMP
    QATNPGM           QEZMAIN   QSYS                          *NONE
    QAUDCTL           *AUDLVL   *OBJAUD   *NOQTEMP            *AUDLVL   *OBJAUD   *NOQTEMP
    QAUDENDACN        *NOTIFY                                 *NOTIFY
    QAUDFRCLVL        *SYS                                    *SYS
    QAUDLVL           *ATNEVT   *AUTFAIL  *CREATE   *DELETE   *AUDLVL2
                      *JOBDTA   *OBJMGT   *PGMADP   *PGMFAIL
                      *SAVRST   *SECURITY *SERVICE  *SPLFDTA
                      *SYSMGT
    QAUDLVL2          *NONE                                   *AUTFAIL  *CREATE   *DELETE   *SAVRST
                                                              *SECURITY
```

Auswahl 27: Auslöserprogramme (PRTTRGPGM)

Mit dieser Auswahl übergeben Sie einen Stapeljob, mit dem eine Liste von Programmen ausgedruckt werden kann, die als Auslöserprogramme für die Dateien in einer angegebenen Bibliothek definiert wurden.

```
Datei . . . . . :   QPSECTRG                                           Seite/Zeile 1/1
Steuerung . . . .   _______                                            Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Auslöserprogramm (Gesamtbericht)                                 Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  09:25:43 CET
 Angegebene Bibliothek  . . . . :   *ALL

                                                                                                 Wiederh.
                                  ------------------------------------Auslöser-------------------------------------  Änd.
 Bibliothek Datei      ASP-Einh.   Name                 Art  Bibliothek Programm    Uhrzeit   Ereignis   Bedingung   zulass.
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Einfügen                Nein
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Löschen                 Nein
 ASN        IBMSN00006 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV85   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00006 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV85   Vor       Löschen                 Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Einfügen                Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Löschen                 Nein
 QRECOVERY  QADBERAP   *SYSBAS     Q__QRECOVERY_QADBE > *SYS QSYS       QDBERAPTRG Vor       Aktual.    Ändern       Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Einfügen                Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Aktual.    Ändern       Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Löschen                 Ja
 QSYS       QADBFCST   *SYSBAS     Q__QSYS_QADBFCST__ > *SYS QSYS       QDBXESND   Nach      Einfügen                Ja
```

9.14.1.13
Seite 16

Auswahl 28: Benutzerobjekte (PRTUSROBJ)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der eine Liste von in einer angegebenen Bibliothek enthaltenen Objekten druckt, die nicht von IBM erstellt wurden.

```
Datei . . . . . :   QPSECPUO                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerobjekte (Gesamt)                                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  09:31:49 CET
 Angegebene Bibliothek  . . . . :   QSYS
 Bibliothek   Objekt       Art        ASP-Einh.    Attribut    Eigner       Beschreibung
 QSYS         QLIC         *PGM       *SYSBAS      CLP         QSECOFR
 QSYS         QQFENDSVR    *PGM       *SYSBAS
 QSYS         QACGJRN      *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0001   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0002   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0003   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0004   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0005   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0006   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0007   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0008   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0009   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0010   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0011   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0012   *JRNRCV    *SYSBAS                  RENGEL
```

Auswahl 29: Benutzerprofilinformationen (PRTUSRPRF)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht mit Informationen über alle Benutzerprofile im System erstellt. In den Bericht können Berechtigungs-, Umgebungs-, Kennwort- oder alle Informationen (*ALL) über ausgewählte Benutzerprofile aufgenommen werden.

```
Datei . . . . . :   QPSECUSR                                                  Seite/Zeile 1/1
Steuerung . . . .   ________                                                  Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerprofilinformationen                                 Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  09:37:01 CET
 Berichtsart  . . . . . . . . . :   *AUTINFO
 Auswählen nach . . . . . . . . :   *SPCAUT
 Sonderberechtigungen . . . . . :   *ALL
                        ------------Sonderberechtigungen-------------                          Art
                                    *IO                                    Gruppen-          der
 Benutzer-    Gruppen-     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Benutzer-           berech-     Gruppen-    Möglichk.
 profil       profile       OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  klasse     Eigner   tigung      berecht.    einschr.
 #SYSLOAD     *NONE         X     X    X     X     X     X    X      X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
 ARPEGGIO                                                      *USER      *USRPRF  *NONE       *PRIVATE    *YES
              DB            X     X    X     X     X     X    X      X
              FORGOT
 CODESCOPE    *NONE                                           *PGMR      *USRPRF  *NONE       *PRIVATE    *NO
 DB           *NONE         X     X    X     X     X     X    X      X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
 DISKSCOPE                  X                X           X    X           *SECOFR    *GRPPRF  *NONE       *PRIVATE    *NO
              QSECOFR       X     X    X     X     X     X    X      X
 FILESCOPE    *NONE                                           *PGMR      *USRPRF  *NONE       *PRIVATE    *NO
 FORGOT       *NONE                                           *USER      *USRPRF  *NONE       *PRIVATE    *YES
                                                                                                          Weitere ...
```

9.14.1.13
Seite 17

Auswahl 30: Interne Benutzerprofildaten (PRTPRFINT)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der einen Bericht mit internen Informationen über die in einem Benutzerprofilobjekt (*USRPRF) enthaltene Anzahl der Einträge druckt. Die Anzahl der Einträge in einem Profil bestimmt dessen Größe. Der Befehl PRTPRFINF (Interne Profildaten drucken) stellt anhand der Anzahl Einträge fest, wie „voll“ ein Benutzerprofilobjekt (*USRPRF) ist. Weitere Einzelheiten finden Sie in den Hilfetexten zum Befehl PRTPRFINT.

```
Datei . . . . . :   QPSECPPI                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Interne Benutzerprofildaten                                  Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  09:37:31 CET
 Auswählen nach . . . . . :   *USRPRF
 Benutzerprofil . . . . . :   *ALL
                            Prozentsatz an     Prozentsatz an     Prozentsatz an     Prozentsatz an
 Benutzer-          Voll    Einträgen für      Einträgen mit      Einträgen für      Primärgruppen-
 profil        (Prozentsatz) Eigene Objekte     pers. Berecht.     berecht. Ben.        einträgen
 #SYSLOAD           0,00          0,00               0,00               0,00               0,00
 ARPEGGIO           0,00          0,00               0,00               0,00               0,00
 CODESCOPE          0,00          0,00               0,00               0,00               0,00
 DB                 0,00          0,00               0,00               0,00               0,00
 DISKSCOPE          0,00          0,00               0,00               0,00               0,00
 FILESCOPE          0,00          0,00               0,00               0,00               0,00
 FORGOT             0,00          0,00               0,00               0,00               0,00
 QANZAGENT          0,00          0,00               0,00               0,00               0,00
 QAUTPROF           0,00          0,00               0,00               0,00               0,00
 QBRMS              0,00          0,00               0,00               0,00               0,00
 QCLUMGT            0,00          0,00               0,00               0,00               0,00
 QCLUSTER           0,00          0,00               0,00               0,00               0,00
```

Auswahl 31: Objektintegrität prüfen (CHKOBJITG)

Mit dieser Auswahl übergeben Sie einen Stapeljob, der alle Objekte überprüft, die Eigentum eines angegebenen Benutzerprofils sind. Auf diese Weise kann festgestellt werden, ob Objekte geändert wurden und dadurch ein Verstoß gegen die Objektintegrität vorliegt. Ist dies der Fall, werden Objektname, Bibliothek, Objektart, Objekteigner und Art des Verstoßes in einer angegebenen Datenbankdatei protokolliert.

Das oder die Benutzerprofile, deren Objekte auf Verstöße gegen die Integrität überprüft werden, müssen angegeben werden. Der qualifizierte Name der Datenbankdatei, an die die Ausgabe weitergeleitet wird, muss ebenfalls angegeben werden.

9.14.1.13
Seite 18

Auswahl 40: Objekte mit Berechtigungsübernahme (PRTADPOBJ)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu den Objekten erstellt, die die Sonderberechtigungen und privaten Berechtigungen eines angegebenen Benutzerprofils übernehmen.

```
                Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                          Name, *JOBD
Auszuführender Befehl  . . . . . > PRTADPOBJ USRPRF(*ALL)

Häufigkeit . . . . . .                        *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . .     *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . .   *CURRENT       Zeit, *CURRENT
Sichern  . . . . . .           *NO            *NO, *YES
```

```
Datei . . . . . :   QPSECADP                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit Berechtigungsübernahme (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  09:42:00 CET
 Benutzerprofil . . . . . :   #SYSLOAD
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 -------------Objekt---------------     --------------Bibliothek--------------
                           Allgem.                                Allgem.      Persönl.
 Name           Art        Berecht.     Name           ASP-Einh.  Berecht.     Berecht.
 UPDATEFB4      *PGM       *EXCLUDE     QGPL           *SYSBAS    *CHANGE        J
                         Objekte mit Berechtigungsübernahme (Änderungen)                 Seite     2
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  09:42:00 CET
 Benutzerprofil . . . . . :   #SYSLOAD
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 -------------Objekt---------------     --------------Bibliothek--------------
                           Allgem.                                Allgem.      Persönl.
 Name           Art        Berecht.     Name           ASP-Einh.  Berecht.     Berecht.
 UPDATEFB4      *PGM       *EXCLUDE     QGPL           *SYSBAS    *CHANGE        J
                              Objekte mit Berechtigungsübernahme (Gesamt)                    Seite     3
```

Auswahl 41: Protokolljournaleinträge (DSPAUDJRNE)

9.14.1.13
Seite 19

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Sicherheitsjournal-Protokollbericht erstellt. Welche Art von Bericht erstellt wird, richtet sich nach den angegebenen Protokolleintragsarten und Benutzerprofilen. Der Bericht kann auf bestimmte Kalenderdaten und Uhrzeiten beschränkt werden.

```
                Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . .                 Name, *JOBD
 Auszuführender Befehl  . . . . . > DSPAUDJRNE ENTTYP(AF) USRPRF(*ALL) JRNRCV(*C
URRENT)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . .                *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . *CURRENT   Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . *NONE        *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . *CURRENT   Zeit, *CURRENT
```

Auswahl 42: Berechtigungen für Berechtigungsliste (PRTPVTAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der alle im System enthaltenen Berechtigungslisten enthält sowie die Benutzer, die für die einzelnen Berechtigungslisten berechtigt sind.

```
                Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . .                 Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*AUTL) CHGRPTONLY(*NO) AUT
LOBJ(*NO)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . .                *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . *CURRENT   Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . *NONE        *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . *CURRENT   Zeit, *CURRENT
```

9.14.1.13
Seite 20

Auswahl 43: Befehlsberechtigung (PRTPUBAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer Bibliothek enthaltenen Befehlen (*CMD) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .   _____          Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*CMD) CHGRPTONLY(*NO) LIB(
*ALL)
                                    _____
                                    _____
                                    _____
                                    _____
                                    _____
 Häufigkeit . . . . . . . . . . .   _____          *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte           _____
 Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                        Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  10:28:43 CET
 Objektart  . . . . . . . . . . :   *CMD
 Angegebene Bibliothek  . . . . :   *LIBL
                                          Berecht.-   Berech-   ----------Objekt-----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.  Eigner  liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        ADDAJE      *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDALRACNE  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDALRD     *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDALRSLTE  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDASPCPYD  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDAUTLE    *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDBKP      *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDBNDDIRE  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDCADMRE   *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDCADNODE  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDCFGLE    *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDCKMKSFE  *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
 QSYS        ADDCLUMON   *SYSBAS    QSYS    *NONE      *USE      X                             X                       X
```

Auswahl 44: Persönliche Befehlsberechtigung (PRTPVTAUT)

9.14.1.13
Seite 21

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Befehlen druckt sowie zu den Benutzern, die für die einzelnen Befehle berechtigt sind.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .  _____          Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*CMD) CHGRPTONLY(*NO) LIB(
RLG)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .  _____          *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .  *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .  *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte          _____
 Geplante Uhrzeit . . . . . . . .  *CURRENT       Zeit, *CURRENT
 Sichern  . . . . . . . . . . . .  *NO           *NO, *YES
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  10:37:04 CET
 Bibliothek . . . . . . . . . . :   QGPL
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *CMD
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                      Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner   gruppe      liste      Benutzer    tigung    Opr Ver Exist Änder Ref  Lese Hin Akt Lös Ausf.
 ADDCSWND    RENGEL   *NONE       *NONE      *PUBLIC     *CHANGE    X                          X   X   X   X   X
                                             RENGEL      *ALL       X   X   X   X   X      X   X   X   X   X
                                             QPGMR       *ALL       X   X   X   X   X      X   X   X   X   X
 AJB         RENGEL   *NONE       *NONE      *PUBLIC     *USE       X                          X                X
                                             RENGEL      *ALL       X   X   X   X   X      X   X   X   X   X
                                             QSYS        *ALL       X   X   X   X   X      X   X   X   X   X
 AJZ         RENGEL   *NONE       *NONE      *PUBLIC     *USE       X                          X                X
                                             RENGEL      *ALL       X   X   X   X   X      X   X   X   X   X
                                             QSYS        *ALL       X   X   X   X   X      X   X   X   X   X
 APYRLOBJ    RENGEL   *NONE       *NONE      *PUBLIC     *USE       X                          X                X
                                             RENGEL      *ALL       X   X   X   X   X      X   X   X   X   X
```

9.14.1.13
Seite 22

Auswahl 45: DFV-Datenschutz (PRTCMNSEC)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht mit Sicherheitsinformationen über die DFV-Konfiguration des Systems erstellt.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTCMNSEC CHGRPTONLY(*NO)
                                                                  *ONCE, *WEEKLY, *MONTHLY
Häufigkeit . . . . . .
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECCMN                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                DFV-Informationen (Gesamt)                                Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  10:39:19 CET
 Objektart  . . . . . :   *DEVD

                          Einheiten-     Sicherer     Standort-                  Einzelne     Vordefin.     SNUF-Progr.
 Objektname     Objektart kategorie      Standort     kennwort      APPN-fähig   Sitzung      Sitzung       Start
 #2345          *DEVD     *DSP
 A              *DEVD     *DSP
 ALEXS2         *DEVD     *DSP
 BLINKI         *DEVD     *DSP
 DSP01          *DEVD     *DSP
 GGS01          *DEVD     *DSP
 GGS1           *DEVD     *DSP
 GMGS01         *DEVD     *DSP
 LINETTCP       *DEVD     *NET
 OPT03          *DEVD     *OPT
 OPT04          *DEVD     *OPT
 OPT99          *DEVD     *OPT
 PCHOLLE1       *DEVD     *DSP
 PCHOLLE2       *DEVD     *DSP
```

Auswahl 46: Verzeichnisberechtigung (PRTPUBAUT)

9.14.1.13
Seite 23

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste der Verzeichnisse (*DIR) druckt, für die nicht die allgemeine Berechtigung *EXCLUDE gilt.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .  _____________  Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*DIR) CHGRPTONLY(*NO) DIR(
'/iSecurity')
                                                                              +
                                                                              +
                                                                              +
                                                                              +
                                                                              +
Häufigkeit . . . . . . . . . . . .  _____________  *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . . .  *CURRENT      Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . . .  *NONE         *NONE, *ALL, *MON, *TUE...
     + für weitere Werte            _____
Geplante Uhrzeit . . . . . . . . .  *CURRENT      Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  10:40:50 CET
 Objektart  . . . . . . . . . . :   *DIR
 Verzeichnis  . . . . . . . . . :   /iSecurity
                                    Berecht.-    Daten-     ---------Objekt----------   ---------------Daten----------------
 Objekt                 Eigner      liste        berecht.   Ver   Exist   Änder   Ref   Opr   Lese   Hin   Akt   Dlt   Ausf.
 SMS                    RENGEL      *NONE        *RX                                    X     X                          X
 report output          SECURITY1P  *NONE        *RX                                    X     X                          X
 DB-Gate                RAZLEEILOF  *NONE        *RX                                    X     X                          X
 IBI                    RENGEL      *NONE        *RX                                    X     X                          X
 tmp                    RAZLEEILOF  *NONE        *RX                                    X     X                          X
 Capture                RENGEL      *NONE        *RX                                    X     X                          X
                        Objekte mit allgemeiner Berechtigung (Änderungen)                Seite     2
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  10:40:50 CET
 Objektart  . . . . . . . . . . :   *DIR
 Verzeichnis  . . . . . . . . . :   /iSecurity
 Letzter Änderungsbericht . . . :   03.05.14  15:18:07
                                    Berecht.-    Daten-     ---------Objekt----------   ---------------Daten----------------
 Objekt                 Eigner      liste        berecht.   Ver   Exist   Änder   Ref   Opr   Lese   Hin   Akt   Dlt   Ausf.
```

9.14.1.13
Seite 24

Auswahl 47: Persönliche Verzeichnisberechtigung (PRTPVTAUT)
Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen auf dem System enthaltenen Verzeichnissen druckt sowie zu den Benutzern, die für die einzelnen Verzeichnisse berechtigt sind.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                          Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*DIR) CHGRPTONLY(*NO) DIR(
'/iSecurity')
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
Häufigkeit . . . . . .                        *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . .     *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  10:43:19 CET
 Verzeichnis  . . . . . :   /iSecurity
 Berechtigung *PUBLIC . . . . . :   *RX
 Objektart  . . . . . :   *DIR
                                  Primär-      Berecht.-                  Daten-      -----------Objekt-----------
 Objekt                 Eigner    gruppe       liste        Benutzer      berecht.    Ver    Exist    Änder    Ref
 SMS                    RENGEL    *NONE        *NONE        *PUBLIC       *RX
                                                            RENGEL        *RWX         X       X        X       X
 report output          SECURITY1P *NONE       *NONE        *PUBLIC       *RX
                                                            SECURITY1P    *RWX         X       X        X       X
 DB-Gate                RAZLEEILOF *NONE       *NONE        *PUBLIC       *RX
                                                            RAZLEEILOF    *RWX         X       X        X       X
 IBI                    RENGEL    *NONE        *NONE        *PUBLIC       *RX
                                                            RENGEL        *RWX         X       X        X       X
 tmp                    RAZLEEILOF *NONE       *NONE        *PUBLIC       *RX
                                                            RAZLEEILOF    *RWX         X       X        X       X
 Capture                RENGEL    *NONE        *NONE        *PUBLIC       *RX
                                                            RENGEL        *RWX         X       X        X       X
```

Auswahl 48: Dokumentberechtigung (PRTPUBAUT)

9.14.1.13
Seite 25

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einem Ordner enthaltenen Dokumenten (*DOC) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Der Name des Ordners, der durchsucht werden soll, muss angegeben werden.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . .                 Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*DOC) CHGRPTONLY(*NO) FLR(
PS)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . .                *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . *CURRENT    Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . *NONE         *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . *CURRENT    Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                              Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  10:45:01 CET
 In Ordner  . . . . . :   PS
                            Berecht.-      Berech-        Sicherheits-
 Dokument         Eigner    Liste          tigung         stufe
   (Es sind keine DLO-Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                            Objekte mit allgemeiner Berechtigung (Änderungen)                          Seite     2
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  10:45:01 CET
 In Ordner  . . . . . :   PS
                            Berecht.-      Berech-        Sicherheits-
 Dokument         Eigner    Liste          tigung         stufe
   (Es sind keine DLO-Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                                  * * * * *  E N D E   D E R   L I S T E  * * * * *
```

9.14.1.13
Seite 26

Auswahl 49: Persönliche Dokumentberechtigung (PRTPVTAUT)
Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen in einem bestimmten Ordner enthaltenen Dokumente druckt sowie zu den Benutzern, die für die einzelnen Dokumente berechtigt sind. Der Name des Ordners, der durchsucht werden soll, muss angegeben werden.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .   _____________   Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*DOC) CHGRPTONLY(*NO) FLR(
PS)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .   _____________   *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte           _____
 Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   _____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen drucken (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  10:46:28 CET
 Objektart  . . . . . . . . . . :   *DOC
                            Primär-       Berecht.-                          Berech-
 DLO            Eigner      gruppe        liste        Sicherheitsstufe      tigung
   (Es sind keine DLO-Objekte zum Auflisten vorhanden.)
                              * * * * *  E N D E  D E R  L I S T E  * * * * *
```

Auswahl 50: Dateiberechtigung (PRTPUBAUT)

9.14.1.13
Seite 27

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer Bibliothek enthaltenen Dateien (*FILE) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .                Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*FILE) CHGRPTONLY(*NO) LIB
(*ALL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .                  *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                    Seite/Zeile 1/1
Steuerung . . . .   _____                                       Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  11:01:35 CET
 Objektart  . . . . . . . . . . :   *FILE
 Angegebene Bibliothek  . . . . :   *ALL
                                                 Berecht.-  Berech-   ----------Objekt-----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 #CGULIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #COBLIB     QSBLSRC     *SYSBAS     QSYS        *NONE      USER DEF  X    X                        X     X    X    X      X
 #DFULIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #DSULIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #LIBRARY    P1          *SYSBAS     QSYS        *NONE      *CHANGE   X                             X     X    X    X      X
 #LIBRARY    QS36SRC     *SYSBAS     QPGMR       *NONE      USER DEF  X    X                        X     X    X    X      X
 #RPGLIB     QRPG2SRC    *SYSBAS     QSYS        *NONE      USER DEF  X    X                        X     X    X    X      X
 #RPGLIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #SDALIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #SEULIB     QS36PRC     *SYSBAS     QSYS        *NONE      *USE      X                             X                       X
 #SYSLOAD    PDSPAJB     *SYSBAS     #SYSLOAD    *NONE      *CHANGE   X                             X     X    X    X      X
 #SYSLOAD    PDSPSTS     *SYSBAS     #SYSLOAD    *NONE      *CHANGE   X                             X     X    X    X      X
 #SYSLOAD    PRB         *SYSBAS     #SYSLOAD    *NONE      *CHANGE   X                             X     X    X    X      X
```

9.14.1.13
Seite 28

Auswahl 51: Persönliche Dateiberechtigung (PRTPVTAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Dateien druckt sowie zu den Benutzern, die für die einzelnen Dateien berechtigt sind.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .                Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*FILE) CHGRPTONLY(*NO) LIB
(QGPL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               

Häufigkeit . . . . . . . . . . .                  *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  11:15:13 CET
 Bibliothek . . . . . . . . . . :   QGPL
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *FILE
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                      Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner   gruppe      liste      Benutzer    tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 AUCSGNFM    RAZLEEILOF *NONE     *NONE      *PUBLIC     *CHANGE   X                              X     X    X    X     X
                                             RAZLEEILOF  *ALL      X    X    X      X     X     X     X    X    X     X
                                             RAZLEEDEGG  *ALL      X    X    X      X     X     X     X    X    X     X
 B           RAZLEEILOF *NONE     *NONE      *PUBLIC     *CHANGE   X                              X     X    X    X     X
                                             RAZLEEILOF  *ALL      X    X    X      X     X     X     X    X    X     X
 DSPPTF      RAZLEEILOF *NONE     *NONE      *PUBLIC     *CHANGE   X                              X     X    X    X     X
                                             RAZLEEILOF  *ALL      X    X    X      X     X     X     X    X    X     X
 DUMMY       RAZLEEILOF *NONE     *NONE      *PUBLIC     *EXCLUDE
                                             RAZLEEILOF  *ALL      X    X    X      X     X     X     X    X    X     X
 FB4TXTSRC   #SYSLOAD   *NONE     *NONE      *PUBLIC     *CHANGE   X                              X     X    X    X     X
                                             #SYSLOAD    *ALL      X    X    X      X     X     X     X    X    X     X
```

Auswahl 52: Ordnerberechtigung (PRTPUBAUT)

9.14.1.13
Seite 29

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von im System enthaltenen Ordnern (*FLR) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .                    Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*FLR) CHGRPTONLY(*NO)


Häufigkeit . . . . . . . . . . .                      *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .   *CURRENT           Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .   *NONE              *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .   *CURRENT           Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:00:25 CET

                          Berecht.-   Berech-     Sicherheits-
 Ordner        Eigner     liste       tigung      stufe          In Ordner
 QDIADOCS      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2924      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2928      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2932      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2939      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2940      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QFOS2942      QSYS       *NONE       *CHANGE     *NONE          *NONE
 QIWSADM       QSECOFR    QIWSADM     *USE        *NONE          *NONE
 MODEL         QSECOFR    QIWSADM     *USE        *NONE          QIWSADM
 USER          QSECOFR    QIWSADM     *USE        *NONE          QIWSADM
                          Objekte mit allgemeiner Berechtigung (Änderungen)                                  Seite     2
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:00:25 CET
 Letzter Änderungsbericht . . . :   03.05.14  15:27:48
                          Berecht.-   Berech-     Sicherheits-
 Ordner        Eigner     liste       tigung      stufe          In Ordner
```

9.14.1.13
Seite 30

Auswahl 53: Persönliche Ordnerberechtigung (PRTPVTAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen auf dem System enthaltenen Ordnern druckt sowie zu den Benutzern, die für die einzelnen Ordner berechtigt sind.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .                Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*FLR) CHGRPTONLY(*NO)


Häufigkeit . . . . . . . . . . .                  *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .  *CURRENT        Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .  *NONE           *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .  *CURRENT        Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Persönliche Berechtigungen drucken (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:01:14 CET
 Objektart  . . . . . . . . . . :   *FLR
 In Ordner  . . . . . . . . . . :   *NONE
                            Primär-       Berecht.-                                    Berech-
 DLO             Eigner     gruppe        liste        Sicherheitsstufe    Benutzer    tigung
 PS              QSPLJOB    *NONE         *NONE        *NONE               QSPLJOB     *ALL
                                                                          *PUBLIC     *EXCLUDE
 QDIADOCS        QSYS       *NONE         *NONE        *NONE               QSYS        *ALL
                                                                          *PUBLIC     *CHANGE
 QFOSDIA         QSECOFR    *NONE         *NONE        *NONE               QSECOFR     *ALL
                                                                          *PUBLIC     *EXCLUDE
 QFOS2924        QSYS       *NONE         *NONE        *NONE               QSYS        *ALL
                                                                          *PUBLIC     *CHANGE
 QFOS2928        QSYS       *NONE         *NONE        *NONE               QSYS        *ALL
                                                                          *PUBLIC     *CHANGE
 QFOS2932        QSYS       *NONE         *NONE        *NONE               QSYS        *ALL
                                                                          *PUBLIC     *CHANGE
 QFOS2939        QSYS       *NONE         *NONE        *NONE               QSYS        *ALL
```

Auswahl 54: Jobbeschreibungsberechtigung (PRTJOBDAUT)

9.14.1.13
Seite 31

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer angegebenen Bibliothek enthaltenen Jobbeschreibungen druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet und für die ein Benutzername in der Jobbeschreibung angegeben ist.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTJOBDAUT LIB(*ALL) CHGRPTONLY(*NO)
                                                                        
                                                                        
                                                                        
                                                                        
                                                                        
                                                                        
Häufigkeit . . . . . .               *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECJOBD                                   Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Jobbeschreibungen mit Zugriffsberechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:01:58 CET
 Angegebene Bibliothek  . . . . :   *ALL
                                                    ----------------Sonderberechtigungen----------------
             Job-                                   Benutzer-    *ALL   *AUD   *IOSYS   *JOB   *SAV   *SEC   *SER   *SPL
 Bibliothek  beschreib.  ASP-Einh.    Eigner        profil        OBJ    IT      CFG     CTL    SYS    ADM   VICE    CTL
 QGPL        QCTXFORM    *SYSBAS      QSYS          QUSER
 QGPL        QSPLAFPW    *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLDBR     *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLDKTR    *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLDKTW    *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLPRTW    *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLRMTW    *SYSBAS      QSPL          QSPLJOB
 QGPL        QSPLSTRWTR  *SYSBAS      QSPL          QSPLJOB
 QHTTPSVR    QZHBHTTP    *SYSBAS      QSYS          QTMHHTTP
 QHTTPSVR    QZSRCOLS    *SYSBAS      QSYS          QTMHHTTP
 QINMEDIA    QSPLERROR   *SYSBAS      QSYS          QSPLJOB
 QINPRIOR    QSPLERROR   *SYSBAS      QSYS          QSPLJOB
 QINSYS      QSPLERROR   *SYSBAS      QSPL          QSPLJOB
                                                                                        Weitere ...
```

9.14.1.13
Seite 32

Auswahl 55: Bibliotheksberechtigung (PRTPUBAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von im System enthaltenen Bibliotheken (*LIB) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Es kann auch angegeben werden, eine Liste bestimmter in diesen Bibliotheken enthaltener Objektarten zu drucken, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . .                  Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*LIB) CHGRPTONLY(*NO) FILA
UT(*NO) CMDAUT(*NO) PGMAUT(*NO) JOBDAUT(*NO)


 Häufigkeit . . . . . .                *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . .  *CURRENT  Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . .    *NONE     *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . .  *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .                                                   Spalten     1 - 130
Suchen  . . . . .
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:03:36 CET
 Objektart  . . . . . :   *LIB
 Angegebene Bibliothek  . . . . :   QSYS
                                          Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.  Eigner  liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        #CGULIB     *SYSBAS    QSYS    *NONE      *USE       X                          X                          X
 QSYS        #COBLIB     *SYSBAS    QSYS    *NONE      *USE       X                          X                          X
 QSYS        #DFULIB     *SYSBAS    QSYS    *NONE      *CHANGE    X                          X     X    X    X       X
 QSYS        #DSULIB     *SYSBAS    QSYS    *NONE      *USE       X                          X                          X
 QSYS        #LIBRARY    *SYSBAS    QSYS    *NONE      *CHANGE    X                          X     X    X    X       X
 QSYS        #RPGLIB     *SYSBAS    QSYS    *NONE      *USE       X                          X                          X
 QSYS        #SEULIB     *SYSBAS    QSYS    *NONE      *USE       X                          X                          X
 QSYS        ALEX        *SYSBAS    RAZLEEILOF *NONE   *CHANGE    X                          X     X    X    X       X
 QSYS        ALEX2       *SYSBAS    RAZLEEILOF *NONE   *CHANGE    X                          X     X    X    X       X
 QSYS        ARD         *SYSBAS    RAZLEEILOF *NONE   *CHANGE    X                          X     X    X    X       X
 QSYS        ARD2        *SYSBAS    RAZLEEILOF *NONE   *CHANGE    X                          X     X    X    X       X
 QSYS        ARPEGGIOL   *SYSBAS    ARPEGGIO   *NONE   *CHANGE    X                          X     X    X    X       X
 QSYS        ARPZIP      *SYSBAS    RAZLEEILIL *NONE   *CHANGE    X                          X     X    X    X       X
                                                                                                                Weitere ...
```

Auswahl 56: Persönliche Bibliotheksberechtigung (PRTPVTAUT)

9.14.1.13
Seite 33

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen auf dem System enthaltenen Bibliotheken druckt sowie zu den Benutzern, die für die einzelnen Bibliotheken berechtigt sind.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*LIB) CHGRPTONLY(*NO)
                                                                        +
                                                                        +
                                                                        +
                                                                        +
                                                                        +
                                                                        +
Häufigkeit . . . . . .               *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:05:02 CET
 Bibliothek . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . :   *LIB
 ASP-Einheit  . . . . . :   *SYSBAS
                       Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner    gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #CGULIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                             X                      X
                                               QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 #COBLIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                             X                      X
                                               QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 #DFULIB     QSYS      *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X    X
                                               QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 #DSULIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                             X                      X
                                               QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 #LIBRARY    QSYS      *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X    X
                                               QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 #RPGLIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                             X                      X
                                                                                                                  Weitere ...
```

9.14.1.13
Seite 34

Auswahl 57: Objektberechtigung (PRTPUBAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste angegebener Objektarten druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Die Objektart, nach der gesucht werden soll, muss angegeben werden.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .                Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*FILE) CHGRPTONLY(*NO) LIB
(QGPL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
Häufigkeit . . . . . . . . . . .                  *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .  *CURRENT        Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .  *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .  *CURRENT        Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:07:14 CET
 Objektart  . . . . . . . . . . :   *FILE
 Angegebene Bibliothek  . . . . :   QGPL

                                          Berecht.-  Berech-  ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.  Eigner  liste     tigung   Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QGPL        AUCSGNFM    *SYSBAS    RAZLEEILOF  *NONE     *CHANGE  X                        X     X    X    X      X
 QGPL        B           *SYSBAS    RAZLEEILOF  *NONE     *CHANGE  X                        X     X    X    X      X
 QGPL        DSPPTF      *SYSBAS    RAZLEEILOF  *NONE     *CHANGE  X                        X     X    X    X      X
 QGPL        FB4TXTSRC   *SYSBAS    #SYSLOAD    *NONE     *CHANGE  X                        X     X    X    X      X
 QGPL        JOBL2755    *SYSBAS    RENGEL      *NONE     *CHANGE  X                        X     X    X    X      X
 QGPL        QAAPFILE    *SYSBAS    QPGMR       *NONE     *USE     X                        X                       X
 QGPL        QAAPFILE$   *SYSBAS    QPGMR       *NONE     *USE     X                        X                       X
 QGPL        QAAPFILE#   *SYSBAS    QPGMR       *NONE     *USE     X                        X                       X
 QGPL        QAAPFILE§   *SYSBAS    QPGMR       *NONE     *USE     X                        X                       X
 QGPL        QAFCGRPH    *SYSBAS    QSYS        *NONE     *USE     X                        X                       X
 QGPL        QAFCPFDDTA  *SYSBAS    QSYS        *NONE     *USE     X                        X                       X
 QGPL        QAFCTUTDBF  *SYSBAS    QSYS        *NONE     *USE     X                        X                       X
 QGPL        QAFCTUTOR   *SYSBAS    QSYS        *NONE     *USE     X                        X                       X
                                                                                                        Weitere ...
```

Auswahl 58: Persönliche Berechtigung (PRTPVTAUT)

9.14.1.13
Seite 35

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste angegebener Objektarten und persönlicher Berechtigungen druckt. Die Objektart, nach der gesucht werden soll, muss angegeben werden.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .                Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*FILE) CHGRPTONLY(*NO) LIB
(QGPL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .                  *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   ________                                    Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:08:08 CET
 Bibliothek . . . . . . . . . . :   QGPL
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *FILE
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                      Primär-     Berecht.-              Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner   gruppe      liste       Benutzer   tigung    Opr Ver Exist Änder Ref  Lese Hin Akt Lös Ausf.
 AUCSGNFM    RAZLEEILOF *NONE     *NONE       *PUBLIC    *CHANGE   X                        X    X   X   X   X
                                              RAZLEEILOF *ALL      X   X   X     X    X    X    X   X   X   X
                                              RAZLEEDEGG *ALL      X   X   X     X    X    X    X   X   X   X
 B           RAZLEEILOF *NONE     *NONE       *PUBLIC    *CHANGE   X                        X    X   X   X   X
                                              RAZLEEILOF *ALL      X   X   X     X    X    X    X   X   X   X
 DSPPTF      RAZLEEILOF *NONE     *NONE       *PUBLIC    *CHANGE   X                        X    X   X   X   X
                                              RAZLEEILOF *ALL      X   X   X     X    X    X    X   X   X   X
 DUMMY       RAZLEEILOF *NONE     *NONE       *PUBLIC    *EXCLUDE
                                              RAZLEEILOF *ALL      X   X   X     X    X    X    X   X   X   X
 FB4TXTSRC   #SYSLOAD   *NONE     *NONE       *PUBLIC    *CHANGE   X                        X    X   X   X   X
                                              #SYSLOAD   *ALL      X   X   X     X    X    X    X   X   X   X
                                                                                                    Weitere ...
```

9.14.1.13
Seite 36

Auswahl 59: Programmberechtigung (PRTPUBAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer Bibliothek enthaltenen Programmen (*PGM) druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet. In diese Liste werden nur Programme aufgenommen, die vom Benutzer aufgerufen werden können und deren Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . . .   _____          Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*PGM) CHGRPTONLY(*NO) LIB(
*ALL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .   _____          *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE          *NONE, *ALL, *MON, *TUE...
      + für weitere Werte           _____
 Geplante Uhrzeit . . . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:09:12 CET
 Objektart  . . . . . . . . . . :   *PGM
 Angegebene Bibliothek  . . . . :   QGPL
                                          Berecht.-   Berech-   ----------Objekt----------  ----------Daten-----------
 Bibliothek  Objekt      ASP-Einh.  Eigner  liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QGPL        PPP333      *SYSBAS    RAZLEEILOF *NONE    *ALL       X    X     X      X     X     X     X    X    X      X
 QGPL        RL#QCMD     *SYSBAS    QSECOFR    *NONE    *USE       X                              X                       X
 QGPL        RZMENU      *SYSBAS    RENGEL     *NONE    *CHANGE    X                              X     X    X    X      X
                          * * * * *  E N D E   D E R   L I S T E  * * * * *
```

Auswahl 60: Persönliche Programmberechtigung (PRTPVTAUT)

9.14.1.13
Seite 37

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen in einer bestimmten Bibliothek enthaltenen Programmen druckt sowie zu den Benutzern, die für die einzelnen Programme berechtigt sind.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . . . . . . . . .   __________     Name, *JOBD
 Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*PGM) CHGRPTONLY(*NO) LIB(
QGPL)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . . . . . . .   __________     *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . . . .   *CURRENT      Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . . . . .   *NONE         *NONE, *ALL, *MON, *TUE...
      + für weitere Werte           __________
 Geplante Uhrzeit . . . . . . . .   *CURRENT      Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                    Seite/Zeile 1/1
Steuerung . . . .   _                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:13:22 CET
 Bibliothek . . . . . . . . . . :   QGPL
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *PGM
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                       Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner    gruppe      liste      Benutzer    tigung    Opr Ver Exist Ände Ref  Lese Hin Akt Lös Ausf.
 PPP333      RAZLEEILOF *NONE      *NONE      *PUBLIC     *ALL       X   X    X    X    X    X    X   X   X    X
                                              RAZLEEILOF  *ALL       X   X    X    X    X    X    X   X   X    X
 RL#QCMD     QSECOFR   *NONE      *NONE      *PUBLIC     *USE       X                        X                   X
                                              QSECOFR     *ALL       X   X    X    X    X    X    X   X   X    X
 RZMENU      RENGEL    *NONE      *NONE      *PUBLIC     *CHANGE    X                        X    X   X   X    X
                                              RENGEL      *ALL       X   X    X    X    X    X    X   X   X    X
                                              QPGMR       *ALL       X   X    X    X    X    X    X   X   X    X
 SYSLOADUPC  #SYSLOAD  *NONE      *NONE      *PUBLIC     *EXCLUDE
                                              #SYSLOAD    *ALL       X   X    X    X    X    X    X   X   X    X
                                              QPGMR       *USE       X                        X                   X
                                              QSECOFR     *ALL       X   X    X    X    X    X    X   X   X    X
                                                                                                          Weitere ...
```

9.14.1.13
Seite 38

Auswahl 61: Benutzerprofilberechtigung (PRTPUBAUT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von im System enthaltenen Benutzerprofilen druckt, deren allgemeine Berechtigung nicht *EXCLUDE lautet.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .  _____          Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPUBAUT OBJTYPE(*USRPRF) CHGRPTONLY(*NO)


Häufigkeit . . . . . . . . . . .  _____          *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .  *CURRENT       Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .  *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte          _____
Geplante Uhrzeit . . . . . . . .  *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUB                                        Seite/Zeile 1/1
Steuerung . . . .   _____                                           Spalten     1 - 130
Suchen  . . . . .   _____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:14:09 CET
 Objektart  . . . . . . . . . . :   *USRPRF
 Angegebene Bibliothek  . . . . :   QSYS
                                        Berecht.-   Berech-   ----------Objekt----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausführ.
 QSYS        QDBSHR      *SYSBAS     QSYS                   USER DEF                                    X         X
 QSYS        QDBSHRDO    *SYSBAS     QSYS                   USER DEF                                    X         X
 QSYS        QTMPLPD     *SYSBAS     QSYS                   USER DEF   X
                        Objekte mit allgemeiner Berechtigung (Änderungen)                  Seite     2
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:14:09 CET
 Objektart  . . . . . . . . . . :   *USRPRF
 Angegebene Bibliothek  . . . . :   QSYS
 Letzter Änderungsbericht . . . :   08.19.14  07:48:37
                                        Berecht.-   Berech-   ----------Objekt----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausführ.
   (Es sind keine Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                                  * * * * *  E N D E  D E R  L I S T E  * * * * *

                                                                                              Ende
```

Auswahl 62: Persönliche Benutzerprofilberechtigung (PRTPVTAUT)

9.14.1.13
Seite 39

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu allen auf dem System enthaltenen Benutzerprofilen druckt sowie zu den Benutzern, die für die einzelnen Benutzerprofile berechtigt sind.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                        Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPVTAUT OBJTYPE(*USRPRF) CHGRPTONLY(*NO)

Häufigkeit . . . . . .                      *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT         Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE              *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT         Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPVT                                        Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:15:08 CET
 Bibliothek . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . :   *USRPRF
 ASP-Einheit  . . . . . :   *SYSBAS
                      Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner   gruppe      liste      Benutzer    tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #SYSLOAD    QSECOFR  *NONE                  *PUBLIC     *EXCLUDE
                                             QSECOFR     *ALL      X    X    X      X      X    X     X    X    X    X
                                             #SYSLOAD    USER DEF  X    X                       X     X    X    X    X
 ARPEGGIO    RAZLEEILIL *NONE                *PUBLIC     *EXCLUDE
                                             RAZLEEILIL  *ALL      X    X    X      X      X    X     X    X    X    X
                                             ARPEGGIO    USER DEF  X    X                       X     X    X    X    X
 CODESCOPE   RENGEL   *NONE                  *PUBLIC     *EXCLUDE
                                             RENGEL      *ALL      X    X    X      X      X    X     X    X    X    X
                                             CODESCOPE   USER DEF  X    X                       X     X    X    X    X
 DB          RAZLEEIL *NONE                  *PUBLIC     *EXCLUDE
                                             RAZLEEIL    *ALL      X    X    X      X      X    X     X    X    X    X
                                                                                                                Weitere ...
```

9.14.1.13
Seite 40

Auswahl 63: Job- und Ausgabewarteschlangenberechtigung (PRTQAUT)
Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht mit Informationen über die Ausgabe- und Jobwarteschlangenberechtigungen für Objekte in einer angegebenen Bibliothek erstellt.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTQAUT LIB(*ALL) CHGRPTONLY(*NO)


Häufigkeit . . . . . .               *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECQ                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                         Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Warteschlangenberechtigung (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:16:30 CET
 Angegebene Bibliothek  . . . . :   *ALL
                                                  Berech-
 Bibliothek     Objekt       Art          Eigner   tigung     DSPDTA     OPRCTL     AUTCHK
 #SYSLOADX      OUTPUT       *OUTQ        QSECOFR  *EXCLUDE   *NO        *YES       *OWNER
 #SYSLOADX      #SYSLOADQ    *JOBQ        QSECOFR  *EXCLUDE   *NONE      *NO        *DTAAUT
 FB400          FBACKUPQ     *JOBQ        QSECOFR  *USE       *NONE      *YES       *OWNER
 QDP4           QZSNDPR      *JOBQ        QSYS     *USE       *NONE      *YES       *OWNER
 QGPL           QDKT         *OUTQ        QPGMR    *USE       *NO        *YES       *OWNER
 QGPL           QPFROUTQ     *OUTQ        QSYS     *CHANGE    *YES       *YES       *OWNER
 QGPL           QPRINT       *OUTQ        QPGMR    *USE       *NO        *YES       *OWNER
 QGPL           QPRINTS      *OUTQ        QPGMR    *USE       *NO        *YES       *OWNER
 QGPL           QPRINT2      *OUTQ        QPGMR    *USE       *NO        *YES       *OWNER
 QGPL           QBASE        *JOBQ        QPGMR    *USE       *NONE      *YES       *OWNER
 QGPL           QBATCH       *JOBQ        QPGMR    *USE       *NONE      *YES       *OWNER
 QGPL           QFNC         *JOBQ        QFNC     *USE       *NONE      *YES       *OWNER
 QGPL           QINTER       *JOBQ        QPGMR    *USE       *NONE      *YES       *OWNER
 QGPL           QPGMR        *JOBQ        QPGMR    *USE       *NONE      *YES       *OWNER
                                                                                     Weitere ...
```

Auswahl 64: Subsystemberechtigung (PRTSBSDAUT)

9.14.1.13
Seite 41

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer Bibliothek enthaltenen Subsystembeschreibungen druckt, die im DFV-Eintrag einen Standardbenutzer enthalten.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTSBSDAUT LIB(*ALL) CHGRPTONLY(*NO)

Häufigkeit . . . . . .               *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECSBSD                                   Seite/Zeile 1/1
Steuerung . . . .                                               Spalten     1 - 130
Suchen  . . . . .
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Subsystembeschreibung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:17:13 CET
 Angegebene Bibliothek  . . . . :   *ALL
                                                 Standard-   ----------------Sonderberechtigungen-----------------
 Subsystem-   Subsystem-                Subsystem-  benutzer-  *ALL   *AUD   *IOSYS  *JOB   *SAV   *SEC   *SER   *SPL
 bibliothek   name         ASP-Einh.    eigner      profil      OBJ    IT     CFG     CTL    SYS    ADM    VICE    CTL
 QINMEDIA     QSYSWRK      *SYSBAS      QSYS        QUSER
 QINMEDIA     QSYSWRK      *SYSBAS      QSYS        QPM400                     X       X
 QINMEDIA     QSYSWRK      *SYSBAS      QSYS        QPM400                     X       X
 QINPRIOR     QCMN         *SYSBAS      QSYS        QUSER
 QINPRIOR     QCMN         *SYSBAS      QSYS        QIJS
 QINPRIOR     QSYSWRK      *SYSBAS      QSYS        QUSER
 QINPRIOR     QSYSWRK      *SYSBAS      QSYS        QPM400                     X       X
 QINPRIOR     QSYSWRK      *SYSBAS      QSYS        QIJS
 QINPRIOR     QSYSWRK      *SYSBAS      QSYS        QPM400                     X       X
 QINSYS       QCMN         *SYSBAS      QSYS        QUSER
 QINSYS       QCMN         *SYSBAS      QSYS        QIJS
 QINSYS       QSYSWRK      *SYSBAS      QSYS        QUSER
 QINSYS       QSYSWRK      *SYSBAS      QSYS        QPM400                     X       X
                                                                                          Weitere ...
```

9.14.1.13
Seite 42

Auswahl 65: Systemsicherheitsattribute (PRTSYSSECA)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht zu sicherheitsrelevanten Systemwerten und Netzwerkattributen in eine Spooldatei ausgibt. Der Bericht enthält die aktuellen und die empfohlenen Werte.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . . .                Name, *JOBD
Auszuführender Befehl  . . . . . > PRTSYSSECA

Häufigkeit . . . . . . . . . . .                    *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .   *CURRENT        Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .   *NONE           *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .   *CURRENT        Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECATTR                                        Seite/Zeile 1/1
Steuerung . . . .   ________                                         Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Systemsicherheitsattribute                                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    26.10.14  20:17:48 CET
 Systemwert
 Name                Aktueller Wert                          Empfohlener Wert
    QALWOBJRST       *ALL                                    *NONE
    QALWUSRDMN       *ALL                                    QTEMP
    QATNPGM          QEZMAIN   QSYS                          *NONE
    QAUDCTL          *AUDLVL   *OBJAUD   *NOQTEMP            *AUDLVL   *OBJAUD   *NOQTEMP
    QAUDENDACN       *NOTIFY                                 *NOTIFY
    QAUDFRCLVL       *SYS                                    *SYS
    QAUDLVL          *ATNEVT   *AUTFAIL  *CREATE   *DELETE   *AUDLVL2
                     *JOBDTA   *OBJMGT   *PGMADP   *PGMFAIL
                     *SAVRST   *SECURITY *SERVICE  *SPLFDTA
                     *SYSMGT
    QAUDLVL2         *NONE                                   *AUTFAIL  *CREATE   *DELETE   *SAVRST
                                                             *SECURITY
    QAUTOCFG         1                                       0
    QAUTORMT         1                                       0
    QAUTOVRT         512                                     0
                                                                                   Weitere ...
```

Auswahl 66: Auslöserprogramme (PRTTRGPGM)

9.14.1.13
Seite 43

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu terminieren, mit dem eine Liste von Programmen ausgedruckt werden kann, die als Auslöserprogramme für die Dateien in einer angegebenen Bibliothek definiert wurden.

```
                    Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                 Name, *JOBD
Auszuführender Befehl  . . . . . > PRTTRGPGM LIB(*ALL) CHGRPTONLY(*NO)

Häufigkeit . . . . . .               *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . *CURRENT  Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . *CURRENT  Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECTRG                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Auslöserprogramm (Gesamtbericht)                                Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:19:43 CET
 Angegebene Bibliothek  . . . . :   *ALL

                                                                                                Wiederh.
                                  ------------------------------------Auslöser-------------------------------------  Änd.
 Bibliothek Datei      ASP-Einh.   Name                  Art  Bibliothek Programm   Uhrzeit   Ereignis   Bedingung   zulass.
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Einfügen                Nein
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00001 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNJLV8   Vor       Löschen                 Nein
 ASN        IBMSN00006 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV85   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00006 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV85   Vor       Löschen                 Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Einfügen                Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Aktual.    Immer        Nein
 ASN        IBMSN00023 *SYSBAS     QSYS_TRIG_ASN_____ > *SYS QDP4       QZSNCV86   Vor       Löschen                 Nein
 QRECOVERY  QADBERAP   *SYSBAS     Q__QRECOVERY_QADBE > *SYS QSYS       QDBERAPTRG Vor       Aktual.    Ändern       Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Einfügen                Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Aktual.    Ändern       Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach      Löschen                 Ja
 QSYS       QADBFCST   *SYSBAS     Q__QSYS_QADBFCST__ > *SYS QSYS       QDBXESND   Nach      Einfügen                Ja
                                                                                                                  Weitere ...
```

9.14.1.13
Seite 44

Auswahl 67: Benutzerobjekte (PRTUSROBJ)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der eine Liste von in einer angegebenen Bibliothek enthaltenen Objekten druckt, die nicht von IBM erstellt wurden.

```
                Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .                          Name, *JOBD
Auszuführender Befehl  . . . . . > PRTUSROBJ LIB(QSYS) CHGRPTONLY(*NO)

Häufigkeit . . . . . .                        *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . .   *CURRENT       Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . .     *NONE          *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . .   *CURRENT       Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPUO                                  Seite/Zeile 1/1
Steuerung . . . .   _                                         Spalten     1 - 130
Suchen  . . . . .   _____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerobjekte (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    26.10.14  20:23:24 CET
 Angegebene Bibliothek  . . . . :   QSYS
 Bibliothek   Objekt       Art        ASP-Einh.    Attribut    Eigner       Beschreibung
 QSYS         QLIC         *PGM       *SYSBAS      CLP         QSECOFR
 QSYS         QQFENDSVR    *PGM       *SYSBAS
 QSYS         QACGJRN      *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0001   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0002   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0003   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0004   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0005   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0006   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0007   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0008   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0009   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0010   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0011   *JRNRCV    *SYSBAS                  RENGEL
 QSYS         QACGJR0012   *JRNRCV    *SYSBAS                  RENGEL
                                                                                  Weitere ...
```

Auswahl 68: Benutzerprofilinformationen (PRTUSRPRF)

9.14.1.13
Seite 45

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht mit Informationen über alle Benutzerprofile im System erstellt. In den Bericht können Berechtigungs-, Umgebungs-, Kennwort- oder alle Informationen (*ALL) über ausgewählte Benutzerprofile aufgenommen werden.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . . . . . . . . .            Name, *JOBD
Auszuführender Befehl  . . . . . > PRTUSRPRF TYPE(*ALL) SELECT(*SPCAUT)

Häufigkeit . . . . . . . . . . .              *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . . . .  *CURRENT    Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . . . . .  *NONE       *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . . . .  *CURRENT    Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECUSR                                    Seite/Zeile 1/1
Steuerung . . . .   _______                                     Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerprofilinformationen                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:24:54 CET
 Berichtsart  . . . . . . . . . :   *AUTINFO
 Auswählen nach . . . . . . . . :   *SPCAUT
 Sonderberechtigungen . . . . . :   *ALL
                        -----------Sonderberechtigungen-------------                        Art
                                    *IO                                    Gruppen-        der
 Benutzer-   Gruppen-    *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Benutzer-          berech-    Gruppen-   Möglichk.
 profil      profile      OBJ   IT    CFG  CTL   SYS   ADM  VICE  CTL   klasse    Eigner   tigung     berecht.   einschr.
 #SYSLOAD    *NONE        X     X     X    X     X     X    X     X     *SECOFR   *USRPRF  *NONE      *PRIVATE   *NO
 ARPEGGIO                                                  *USER     *USRPRF  *NONE      *PRIVATE   *YES
             DB           X     X     X    X     X     X    X     X
             FORGOT
 CODESCOPE   *NONE                                         *PGMR     *USRPRF  *NONE      *PRIVATE   *NO
 DB          *NONE        X     X     X    X     X     X    X     X     *SECOFR   *USRPRF  *NONE      *PRIVATE   *NO
 DISKSCOPE                X           X          X     X          *SECOFR   *GRPPRF  *NONE      *PRIVATE   *NO
             QSECOFR      X     X     X    X     X     X    X     X
 FILESCOPE   *NONE                                         *PGMR     *USRPRF  *NONE      *PRIVATE   *NO
 FORGOT      *NONE                                         *USER     *USRPRF  *NONE      *PRIVATE   *YES
                                                                                                    Weitere ...
```

9.14.1.13
Seite 46

Auswahl 69: Interne Benutzerprofildaten (PRTPRFINT)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der einen Bericht mit internen Informationen über die Anzahl der Einträge in einem Benutzerprofilobjekt (*USRPRF) druckt. Die Anzahl der Einträge in einem Profil bestimmt dessen Größe. Der Befehl PRTPRFINF (Interne Profildaten drucken) stellt anhand der Anzahl Einträge fest, wie „voll“ ein Benutzerprofilobjekt (*USRPRF) ist. Weitere Einzelheiten finden Sie in den Hilfetexten zum Befehl PRTPRFINT.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

Auswahl eingeben und Eingabetaste drücken.

Jobname  . . . . . .              Name, *JOBD
Auszuführender Befehl  . . . . . > PRTPRFINT

Häufigkeit . . . . . .            *ONCE, *WEEKLY, *MONTHLY
Geplantes Datum  . . . . . .      Datum, *CURRENT, *MONTHSTR...
Geplanter Tag  . . . . . .        *NONE      *NONE, *ALL, *MON, *TUE...
     + für weitere Werte
Geplante Uhrzeit . . . . . .      *CURRENT   Zeit, *CURRENT
```

```
Datei . . . . . :   QPSECPPI                                  Seite/Zeile 1/1
Steuerung . . . .                                             Spalten     1 - 130
Suchen  . . . . .
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Interne Benutzerprofildaten                    Seite     1
5770SS1 V7R2M0  140418                                          RAZLEE    26.10.14  20:25:33 CET
 Auswählen nach . . . . . :   *USRPRF
 Benutzerprofil . . . . . :   *ALL
                             Prozentsatz an    Prozentsatz an    Prozentsatz an    Prozentsatz an
 Benutzer-        Voll       Einträgen für     Einträgen mit     Einträgen für     Primärgruppen-
 profil       (Prozentsatz)  Eigene Objekte    pers. Berecht.    berecht. Ben.       einträgen
 #SYSLOAD          0,00           0,00              0,00              0,00              0,00
 ARPEGGIO          0,00           0,00              0,00              0,00              0,00
 CODESCOPE         0,00           0,00              0,00              0,00              0,00
 DB                0,00           0,00              0,00              0,00              0,00
 DISKSCOPE         0,00           0,00              0,00              0,00              0,00
 FILESCOPE         0,00           0,00              0,00              0,00              0,00
 FORGOT            0,00           0,00              0,00              0,00              0,00
 QANZAGENT         0,00           0,00              0,00              0,00              0,00
 QAUTPROF          0,00           0,00              0,00              0,00              0,00
 QBRMS             0,00           0,00              0,00              0,00              0,00
 QCLUMGT           0,00           0,00              0,00              0,00              0,00
 QCLUSTER          0,00           0,00              0,00              0,00              0,00
                                                                                  Weitere ...
```

9.14.1.13
Seite 47

Auswahl 70: Objektintegrität prüfen (CHKOBJITG)

Für diese Auswahl entscheiden Sie sich, um einen Stapeljob zu planen, der alle Objekte überprüft, die Eigentum eines angegebenen Benutzerprofils sind. Auf diese Weise kann festgestellt werden, ob Objekte geändert wurden und dadurch ein Verstoß gegen die Objektintegrität vorliegt. Ist dies der Fall, werden Objektname, Bibliothek, Objektart, Objekteigner und Art des Verstoßes in einer Datenbankdatei protokolliert.

Das oder die Benutzerprofile, deren Objekte auf Verstöße gegen die Integrität überprüft werden, müssen angegeben werden. Der qualifizierte Name der Datenbankdatei, an die die Ausgabe weitergeleitet wird, muss ebenfalls angegeben werden.

```
                  Jobplanungseintrag hinzufügen (ADDJOBSCDE)

 Auswahl eingeben und Eingabetaste drücken.

 Jobname  . . . . . .                 Name, *JOBD
 Auszuführender Befehl  . . . . . > CHKOBJITG USRPRF(*ALL) OUTFILE(QTEMP/OBJ) CH
KDMN(*YES) CHKPGMMOD(*YES)
                                                                               
                                                                               
                                                                               
                                                                               
                                                                               
 Häufigkeit . . . . . .              *ONCE, *WEEKLY, *MONTHLY
 Geplantes Datum  . . . . . .  *CURRENT    Datum, *CURRENT, *MONTHSTR...
 Geplanter Tag  . . . . . .    *NONE       *NONE, *ALL, *MON, *TUE...
      + für weitere Werte
 Geplante Uhrzeit . . . . . .  *CURRENT    Zeit, *CURRENT
```

```
                                  Bericht anzeigen
                                                          Breite des Berichts . :   10263
Anfang auf Zeile . . . . . .                                Anfang in Spalte . . . . . .
Zeile  ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....
       ANZEIGE-     ANZEIGE-  ANZEIGE-  SYSTEM   NAMENS-   OBJEKT     BIBLIOTHEK  ART      EIGNER     VERSTOSS    ANZEIGER FÜR
       JAHRHUNDERT  DATUM     ZEIT                ANZEIGER                                                    ABGESCHNITTEN

000001      1        102614    210033   RAZLEE       0     AUGRPTR    TEMP        *PGM     RENGEL     NOTTRANS
000002      1        102614    210033   RAZLEE       0     GSSPCPRT   SMZODTA     *PGM     RENGEL     NOTTRANS
000003      1        102614    210033   RAZLEE       0     GSSPCPRT   SMZJDTA     *PGM     RENGEL     NOTTRANS
000004      1        102614    210033   RAZLEE       0     RZMENU     QGPL        *PGM     RENGEL     NOTTRANS
****** ******** Ende des Berichts ********
```

9.14.1.13

Seite 48

9.14.1.14 Objekte mit Berechtigungsübernahmen drucken

Mit dem Befehl PRTADPOBJ (Objekte mit Berechtigungsübernahme drucken) kann ein Bericht zu allen Objekten gedruckt werden, die die Sonderberechtigungen und die persönlichen Berechtigungen des angegebenen Benutzerprofils übernehmen. Auf diese Weise kann der Sicherheitsstandard des Systems bei der Programmübernahme geprüft werden.

Einschränkungen:

- Um diesen Befehl zu verwenden, muss der Benutzer über die Berechtigung *ALLOBJ oder *AUDIT verfügen.
- Das im Befehl angegebene Benutzerprofil ist für die Dauer der Befehlsausführung gesperrt. Die Sperre verhindert beispielsweise, dass der Eigner von Objekten dieses Profils geändert wird. Ist dieses Profil der Eigner vieler Objekte, könnte das Profil für eine längere Zeit gesperrt sein.

Mit diesem Befehl werden zwei Berichte für ein Benutzerprofil gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Objekte, die die Berechtigungen des Benutzerprofils übernehmen. Der zweite Bericht (Änderungen) enthält die Objekte, die bei der letzten Ausführung des Befehls PRTADPOBJ noch nicht zu den Objekten mit Berechtigungsübernahme für dieses Benutzerprofil gehörten. Wurde der Befehl zuvor noch nicht für das Benutzerprofil ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar zuvor bereits für das Benutzerprofil ausgeführt, sind aber zwischenzeitlich keine weiteren Objekte mit Berechtigungsübernahme hinzugekommen, so wird ein Änderungsbericht gedruckt, der keine Objekte enthält.

In den Berichten sind folgende Informationen enthalten:

- der Name des Benutzerprofils
- die Sonderberechtigungen des Benutzerprofils
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jedes Objekt, das die Berechtigungen des Benutzerprofils übernimmt. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Objekts
  - die Objektart
  - die Berechtigung *PUBLIC für das Objekt. Ist das Objekt oder die Bibliothek des Objekts zum Zeitpunkt der Berichterstellung gesperrt, wird der Wert auf *LOCKED gesetzt.

9.14.1.14
Seite 2

– den Namen der Bibliothek, in der sich das Objekt befindet
– die Berechtigung *PUBLIC für die Bibliothek. Ist die Bibliothek zum Zeitpunkt der Berichterstellung gesperrt, wird der Wert auf *LOCKED gesetzt.
– einen Hinweis darauf, ob für das Objekt persönliche Berechtigungen vorhanden sind ('J' oder 'N'). Ist das Objekt oder die Bibliothek zum Zeitpunkt der Berichterstellung gesperrt, wird kein Wert angegeben.

Anmerkung:

Gibt es keine Objekte, die die Berechtigungen eines Benutzerprofils übernehmen, wird für diesen Benutzer kein Bericht gedruckt. Gibt es für keines der im Befehl angegebenen Benutzerprofile Objekte, die die Berechtigungen des Benutzerprofils übernehmen, werden keine Berichte erstellt.

Die Datei QSECADPOLD in der Bibliothek QUSRSYS enthält Informationen zur letzten Ausführung des Befehls PRTADPOBJ für ein Benutzerprofil. In der Datei ist für jedes Benutzerprofil, das bereits zuvor in dem Befehl angegeben wurde, eine Teildatei enthalten, der derselbe Name wie dem Benutzerprofil zugeordnet ist. Die Systemdatei QADPGMAD in der Bibliothek QSYS mit dem Formatnamen QSYPGMAD ist die Modelldatei für die Datei QSECADPOLD.

```
Datei . . . . . :   QPSECADP                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit Berechtigungsübernahme (Gesamt)                              Seite     1
5770SS1 V7R2M0  140418                                                    RAZLEE    26.10.14  21:10:02 CET
 Benutzerprofil . . . . . :   RENGEL
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 --------------Objekt---------------     --------------Bibliothek--------------
                            Allgem.                                  Allgem.      Persönl.
 Name           Art         Berecht.     Name           ASP-Einh.    Berecht.     Berecht.
 GSSPCPRT       *PGM        *USE         SMZJDTA        *SYSBAS      *EXCLUDE       J
 GSSPCPRT       *PGM        *USE         SMZODTA        *SYSBAS      *EXCLUDE       J
 AUGRPTR        *PGM        *USE         TEMP           *SYSBAS      *CHANGE        J
                                  Objekte mit Berechtigungsübernahme (Änderungen)                      Seite     2
5770SS1 V7R2M0  140418                                                    RAZLEE    26.10.14  21:10:02 CET
 Benutzerprofil . . . . . :   RENGEL
 Sonderberechtigungen . . . . . :   *ALLOBJ     *AUDIT      *IOSYSCFG   *JOBCTL
                                    *SAVSYS     *SECADM     *SERVICE    *SPLCTL
 Letzter Änderungsbericht . . . :   10.26.14  09:54:43
 --------------Objekt---------------     --------------Bibliothek--------------
                            Allgem.                                  Allgem.      Persönl.
                                                                                              Weitere ...
```

9.14.1.15 Protokolljournaleinträge

Mit dem Befehl DSPAUDJRNE (Protokolljournaleinträge anzeigen) können Sicherheitsjournal-Protokollberichte erstellt werden. Die Berichte basieren auf den im Befehl angegebenen Protokolleintragsarten und dem angegebenen Benutzerprofil. Die Berichte können auf bestimmte Zeitrahmen beschränkt und es kann nach abgehängten Journalempfängern gesucht werden. Die Berichte werden auf der aktiven Anzeige oder in eine Spooldatei ausgegeben.

Die Protokolleinträge, für die Berichte ausgeführt werden können, sind nur eine Teilmenge der Protokolleinträge, die generiert werden können. Informationen über die möglichen Protokolleintragsarten enthält Kapitel 9 des Handbuchs System i Security Reference, IBM Form SC41-5302.

Einschränkung:

Der Benutzer muss über die Sonderberechtigung (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

Journaleintragsarten (ENTTYP)
Die Journaleintragsarten, die in den Bericht aufgenommen werden sollen.

Für diesen Parameter können 30 Werte angegeben werden:

- AF
  Berechtigungsfehler
- CA
  Berechtigungsänderungen
- CD
  Befehlszeichenfolgen
- CO
  Objekterstellungen
- CP
  Änderungen des Benutzerprofils
- CU
  Clusterverwaltungsoperationen
- CV
  Verbindungsprüfung
- DO
  Objektlöschungen
- EV
  Umgebungsvariablenoperationen

9.14.1.15
Seite 2

- GR
  Generischer Datensatz
- IP
  Interprozesskommunikation
- JS
  Aktionen für Jobs
- ND
  Unzulässige Verzeichnissuchfilter
- NE
  Unzulässige Sitzungsendpunktfilter
- OM
  Versetzen oder Umbenennen von Objekten
- OR
  Zurückspeichern von Objekten
- OW
  Änderungen des Objekteignerrechts
- PG
  Änderungen einer Primärgruppe für ein Objekt
- PO
  Druckausgaben
- PS
  Profilumschaltung
- PW
  Ungültige Kennwörter
- SF
  Aktionen für Spooldateien
- SO
  Benutzerdatenaktionen für die Serversicherheit
- SV
  Änderungen von Systemwerten
- VO
  Aktionen für Prüflisten
- YC
  Änderungen von DLO-Objekten

9.14.1.15
Seite 3

- YR
  Lesen von DLO-Objekten
- ZC
  Objektänderungen
- ZR
  Lesen von Objekten

```
Datei . . . . . :   QPQUPRFIL                                          Seite/Zeile 1/29
Steuerung . . . .   ________                                           Spalten     1 - 130
Suchen  . . . . .   ________________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                                    ABFRAGENAME  . . . . QSECCO
                                                    BIBLIOTHEKSNAME  . . QSYS
                                                    DATEI        BIBLIOTHEK   TEILDATEI    FORMAT
                                                    QASYCOJ4     QTEMP        QASYCOJ4     QASYCOJ4
                                                    DATUM  . . . . . . . 26.10.14
                                                    UHRZEIT  . . . . . . 21:19:21
26.10.14  21:19:21
  Eintragsart Benutzer-  Objekt-    Bibliotheks- Objekt-  Büro-      DLO-         Ordner-
              profil     name       name         art     benutzer-  Name         pfad
                                                         name
Zeitmarke
CO      N      #SYSLOAD   OBJD        #SYSLOAD    *FILE
2014-10-26-20.58.08.914688
CO      N      #SYSLOAD   PRB         #SYSLOAD    *FILE
2014-10-26-20.58.21.270320
CO      N      RZKHANGO   FB400RUN    QGPL        *DTAARA
2014-10-26-21.00.16.509104
CO      N      RZKHANGO   SESSLIST    FB400D      *FILE
2014-10-26-21.00.26.087920
                                                                                Weitere ...
```

9.14.1.15

Seite 4

9.14.1.16 Persönliche Berechtigung drucken

Mit dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken) kann ein Bericht gedruckt werden, der alle persönlichen Berechtigungen für eine bestimmte Objektart in einer angegebenen Bibliothek, einem angegebenen Ordner oder Verzeichnis enthält. In dem Bericht werden alle Objekte der angegebenen Art und die jeweils berechtigten Benutzer aufgeführt. Auf diese Weise kann geprüft werden, welche Benutzer welche Berechtigungen für die einzelnen Objekte haben.

Mit diesem Befehl werden drei Berichte für die ausgewählten Objekte gedruckt. Der erste Bericht (Gesamt) enthält alle persönlichen Berechtigungen für die einzelnen Objekte.

Der zweite Bericht (Änderungen) enthält alle Neuzugänge/Änderungen, wenn der Befehl PRTVTAUT zuvor für die angegebenen Objekte in der Bibliothek oder im Ordner ausgeführt wurde. Dazu gehören alle neuen Objekte der ausgewählten Art sowie neue und geänderte Berechtigungen für die bereits vorhandenen Objekte. Wurde der Befehl PRTVTAUT zuvor noch nicht für die angegebenen Objekte in der Bibliothek oder dem Ordner ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, aber haben zwischenzeitlich keine Änderungen stattgefunden, wird ein Änderungsbericht ohne Objekte gedruckt.

Der dritte Bericht (Löschungen) enthält alle Benutzer, deren persönliche Berechtigungen für die angegebenen Objekte seit der letzten Ausführung des Befehls PRTPVTAUT gelöscht wurden. In dem Löschbericht werden sowohl alle gelöschten Objekte als auch alle gelöschten Benutzer mit persönlicher Berechtigung aufgeführt. Wurde der Befehl PRTPVTAUT zuvor noch nicht ausgeführt, wird kein Löschbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, aber wurde zwischenzeitlich keine Löschoperation für die Objekte ausgeführt, wird ein Löschbericht ohne Objekte gedruckt.

9.14.1.16
Seite 2

In den Berichten sind folgende Informationen enthalten:

- die im Befehl angegebene Objektart (sofern sie nicht *AUTL lautet)
- Datum und Uhrzeit der letzten Berichterstellung (nicht im Gesamtbericht)
- der Name der im Befehl angegebenen Bibliothek (sofern die Objektart nicht *AUTL, *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)
- die Berechtigung *PUBLIC für die Bibliothek (sofern die Objektart nicht *AUTL, *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)
- der Name des Ordners mit den Dokumenten oder dem Ordner (wenn die Objektart *DOC oder *FLR lautet)
- der Name des Verzeichnisses, in dem sich die Objekte befinden (sofern die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK lautet)
- die Berechtigung *PUBLIC für das Verzeichnis (wenn die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK lautet)
- ein Eintrag für jeden Benutzer, der für die Objekte in der Liste berechtigt ist. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Objekts (nur beim ersten Benutzer)
  - den Eigner des Objekts (nur beim ersten Benutzer)
  - die Primärgruppe des Objekts (nur beim ersten Benutzer)
  - Den Namen der Berechtigungsliste, die das Objekt sichert (nur beim ersten Benutzer, sofern die Objektart nicht *AUTL lautet).
  - die Sicherheitsstufe des Dokuments oder des Ordners (nur beim ersten Benutzer, sofern die Objektart *DOC oder *FLR lautet)
  - den Namen des Benutzers, der für das Objekt berechtigt ist
  - den Sonderwert für die Berechtigung, die der Benutzer für das Objekt besitzt (zum Beispiel *ALL oder *CHANGE)
  - eine Angabe für die individuellen Berechtigungen, die der Benutzer für das Objekt besitzt ('X' oder ' ') (sofern die Objektart nicht *DOC oder *FLR lautet)

Die Datei QPBXXXXXXX ('XXXXXXX' ist die im Befehl angegebene Objektart) in Bibliothek QUSRSYS enthält Informationen, die die vorherige Ausführung des Befehls PRTPVTAUT betreffen. Sofern die Objektart nicht *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet, enthält diese Datei für jede zuvor im Befehl angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Bei Objektarten, für die keine Bibliotheksangabe erforderlich ist (zum Beispiel *USRPRF), lautet der Bibliotheksname QSYS. Die Systemdatei QAOBJAUT in Bibliothek QSYS mit dem Formatnamen QSYDSAUT dient als Modell für die Datei.

Lautet die Objektart *FLR, enthält die erste Teildatei die Informationen, die die vorherige Angabe von *FLR in dem Befehl betreffen. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO dient als Modell für die Datei.

Lautet die Objektart *DOC, enthält die Datei eine Teildatei für jeden Ordner, der zuvor in dem Befehl angegeben wurde. Der Name der Teildatei stimmt mit dem Systemnamen des Ordners überein. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO dient als Modell für die Datei.

Ist die Objektart *FILE und wurde für den Parameter AUTTYPE der Wert *FIELD oder *ALL angegeben, wird der Befehl DSPOBJAUT (Objektberechtigung anzeigen) für jede Datei ausgeführt, der Berechtigungen auf Feldebene zugeordnet sind. Für jede dieser Dateien wird eine Spooldatei mit dem Namen QPOBJAUT erstellt, die alle Berechtigungsdaten auf Feldebene für die Datei enthält. Unterstützung für Änderungsberichte steht jedoch für Berechtigungsdaten auf Feldebene für diese Dateien nicht zur Verfügung.

Lautet die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK, enthält die Datei eine Teildatei für jedes Verzeichnis, das zuvor im Parameter „Verzeichnis“ (DIR) angegeben wurde. Die Teildateinamen basieren auf der Reihenfolge, in der die Verzeichnisse verarbeitet werden. Die Namen der Teildateien folgen der Namenskonvention x000000001, x000000002 usw. Das erste Zeichen des Teildateinamens ist entweder N oder Y. Dieses Zeichen zeigt an, ob die Unterverzeichnisse bei der Erfassung der Daten durchsucht wurden. N bedeutet, dass die Unterverzeichnisse nicht durchsucht wurden, Y bedeutet, dass sie durchsucht wurden. Sobald einem Verzeichnis ein Teildateiname zugeordnet wurde, wird der numerische Teil des Präfixes für alle oben aufgeführten Objektarten verwendet. Die Systemdatei QASECDIR in Bibliothek QSYS mit dem Formatnamen QSECDIR dient als Modell für die Datei.

9.14.1.16

Seite 4

Anmerkung:

Die Datei QASECGFIPV in Bibliothek QUSRSYS enthält die Datei-ID-Werte für jedes verarbeitete Verzeichnis sowie den Nxxxxxxxxx-Teildateinamen, der ihm zugeordnet wurde. Die Systemdatei QASECGFI in Bibliothek QSYS mit dem Formatnamen QSECGFI dient als Modell für QASECGFIPV.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    27.10.14  07:41:42 CET
 Berecht.-                Primär-                Berech-   List  ----------Objekt----------  ----------Daten-----------
 liste       Eigner       gruppe      Benutzer   tigung    verw  Opr  Ver  Exist  Änd.  Ref  Les.  Hin  Akt  Lös  Ausf.
 ADPAUT      QSECOFR      *NONE       *PUBLIC    *CHANGE         X                            X     X    X    X     X
                                      QSECOFR    *ALL      X     X    X     X     X     X    X     X    X    X     X
 QIWSADM     QSECOFR      *NONE       *PUBLIC    *USE            X                            X                      X
                                      QSECOFR    *ALL      X     X    X     X     X     X    X     X    X    X     X
 QLWISVR     QSYS         *NONE       *PUBLIC    *EXCLUDE
                                      QSYS       *ALL      X     X    X     X     X     X    X     X    X    X     X
                                      QTMHHTTP   *USE            X                            X                      X
 QOPTSEC     QSYS         *NONE       *PUBLIC    *CHANGE         X                            X     X    X    X     X
                                      QSYS       *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPMCCDATA   QSYS         *NONE       *PUBLIC    *EXCLUDE
                                      QSYS       *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPMCCFCN    QSYS         *NONE       *PUBLIC    *EXCLUDE
                                      QSYS       *ALL      X     X    X     X     X     X    X     X    X    X     X
 QPQSPLJOB   QSYS         *NONE       *PUBLIC    *EXCLUDE
                                      QSYS       *ALL      X     X    X     X     X     X    X     X    X    X     X
                                                                                                              Weitere ...
```

9.14.1.17 Befehlsberechtigung drucken

Mit dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken) kann ein Bericht gedruckt werden, der die angegebenen Objekte enthält, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Von den *PGM-Objekten werden nur die vom Benutzer aufrufbaren Programme (das Programm ist entweder eine Benutzerdomäne oder die Systemsicherheitsstufe – Systemwert QSECURITY ist kleiner/gleich 30), deren allgemeine Berechtigung nicht *EXCLUDE lautet, in den Bericht aufgenommen. Auf diese Weise kann geprüft werden, welche Objekte für jeden Systembenutzer zugänglich sind.

Mit diesem Befehl werden zwei Berichte gedruckt. Der erste Bericht (Gesamt) enthält sämtliche angegebenen Objekte, deren allgemeine Berechtigung nicht *EXCLUDE lautet. Der zweite Bericht (Änderungen) enthält die Objekte, die jetzt nicht über die allgemeine Berechtigung *EXCLUDE verfügen, denen diese jedoch zugeordnet war, als der Befehl PRTPUBAUT zuvor ausgeführt wurde, oder die zum Zeitpunkt der vorherigen Befehlsausführung noch nicht vorhanden waren. Wurde der Befehl zuvor noch nicht für die angegebenen Objekte und die Bibliothek oder den Ordner ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine weiteren Objekte ohne *EXCLUDE-Berechtigung hinzugekommen, wird ein Änderungsbericht gedruckt, der keine Objekte enthält.

In den Berichten sind folgende Informationen enthalten:

- die im Befehl angegebene Objektart (sofern sie nicht *DOC oder *FLR lautet)
- der Name der im Befehl angegebenen Bibliothek (sofern die Objektart nicht *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)
- der Name des Ordners, in dem sich die Dokumente befinden (sofern die Objektart nicht *DOC lautet)
- der Name des Verzeichnisses, in dem sich die Objekte befinden (sofern die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK lautet)
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jedes Objekt, dessen allgemeine Berechtigung (*PUBLIC) nicht *EXCLUDE lautet. Jeder Eintrag enthält folgende Informationen:
  - den Namen der Bibliothek, in der sich das Objekt befindet (sofern die Objektart nicht *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)

9.14.1.17
Seite 2

- den Namen des Ordners, in dem sich das Objekt befindet (sofern die Objektart nicht *FLR lautet)
- den Namen des Objekts
- den Eigner des Objekts
- die Berechtigungsliste, die das Objekt schützt
- den Sonderwert für die Berechtigung *PUBLIC (zum Beispiel *ALL oder *CHANGE)
- die Sicherheitsstufe des Dokuments oder des Ordners (sofern die Objektart nicht *DOC oder *FLR lautet)
- eine Angabe für die einzelnen Berechtigungen, die *PUBLIC für das Programm hat ('X' oder ' ') (sofern die Objektart nicht *DOC oder *FLR lautet)

Die Datei QPBXXXXXXX ('XXXXXXX' ist die im Befehl angegebene Objektart) in Bibliothek QUSRSYS enthält Informationen, die die vorherige Ausführung des Befehls PRTPUBAUT betreffen. Sofern die Objektart nicht *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet, enthält diese Datei für jede zuvor im Befehl angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Wurde für den Bibliotheksnamen ein Sonderwert angegeben (zum Beispiel *USRLIBL), wird der '*' im Teildateinamen durch ein 'Q' ersetzt. Bei Objektarten, für die keine Bibliotheksangabe erforderlich ist (zum Beispiel *USRPRF), lautet der Bibliotheksname QSYS. Die Systemdatei QAOBJAUT in Bibliothek QSYS mit dem Formatnamen QSYDSAUT dient als Modell für die Datei.

Lautet die Objektart *FLR, enthält die erste Teildatei die Informationen, die die vorherige Angabe von *FLR in dem Befehl betreffen. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO dient als Modell für die Datei.

Lautet die Objektart *DOC, enthält die Datei eine Teildatei für jeden Ordner, der zuvor in dem Befehl angegeben wurde. Der Name der Teildatei stimmt mit dem Systemnamen des Ordners überein. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO dient als Modell für die Datei.

Lautet die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK, enthält die Datei eine Teildatei für jedes Verzeichnis, das zuvor im Parameter „Verzeichnis“ (DIR) angegeben wurde. Die Teildateinamen basieren auf der Reihenfolge, in der die Verzeichnisse verarbeitet werden. Die Namen der Teildateien folgen der Namenskonvention x000000001, x000000002 usw. Das erste Zeichen des Teildateinamens ist entweder N oder Y. Dieses Zeichen weist darauf hin, ob die Unterverzeichnisse bei der Erfassung der Daten durchsucht wurden. N bedeutet, dass die Unterverzeichnisse nicht durchsucht wurden, Y bedeutet, dass sie durchsucht wurden. Sobald einem Verzeichnis ein Teildateiname zugeordnet wurde, wird der numerische Teil des Präfixes für alle oben aufgeführten Objektarten verwendet. Die Systemdatei QASECDIR in Bibliothek QSYS mit dem Formatnamen QSECDIR dient als Modell für die Datei.

Anmerkung:

Die Datei QASECGFIPB in Bibliothek QUSRSYS enthält die Datei-ID-Werte für jedes verarbeitete Verzeichnis sowie den Nxxxxxxxxx-Teildateinamen, der ihm zugeordnet wurde. Die Systemdatei QASECGFI in Bibliothek QSYS mit dem Formatnamen QSECGFI dient als Modell für QASECGFIPB.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   _____                                                   Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                          RAZLEE    27.10.14  18:57:28 CET
 Objektart  . . . . . . . . . . :   *CMD
 Angegebene Bibliothek  . . . . :   QGPL
                                                 Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausführ.
 QGPL        ADDCSWND    *SYSBAS     RENGEL      *NONE       *CHANGE   X                          X     X    X    X      X
 QGPL        AJB         *SYSBAS     RENGEL      *NONE       *USE      X                          X                       X
 QGPL        AJZ         *SYSBAS     RENGEL      *NONE       *USE      X                          X                       X
 QGPL        APYRLOBJ    *SYSBAS     RENGEL      *NONE       *USE      X                          X                       X
 QGPL        AUINITDFT   *SYSBAS     SECURITY7P  *NONE       *USE      X                          X                       X
 QGPL        AVOBJITG    *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        AVPGMCRT    *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        AVSCNDIR    *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        AVSNDM      *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        AVSNDSNMP   *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        AVSNDTWT    *SYSBAS     RAZLEEILOF  *NONE       *USE      X                          X                       X
 QGPL        CACVTH      *SYSBAS     SECURITY7P  *NONE       *USE      X                          X                       X
 QGPL        CFGCS       *SYSBAS     RENGEL      *NONE       *CHANGE   X                          X     X    X    X      X
                                                                                                                  Weitere ...
```

9.14.1.17

Seite 4

9.14.1.18 Persönliche Befehlsberechtigung drucken

Mit dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken) kann ein Bericht gedruckt werden, der alle persönlichen Berechtigungen für eine bestimmte Objektart in einer angegebenen Bibliothek, einem angegebenen Ordner oder Verzeichnis enthält. In dem Bericht werden alle Objekte der angegebenen Art und die jeweils berechtigten Benutzer aufgeführt. Auf diese Weise kann geprüft werden, welche Benutzer welche Berechtigungen für die einzelnen Objekte haben.

Mit diesem Befehl werden drei Berichte für die ausgewählten Objekte gedruckt. Der erste Bericht (Gesamt) enthält alle persönlichen Berechtigungen für die einzelnen Objekte.

Der zweite Bericht (Änderungen) enthält alle Neuzugänge/Änderungen, wenn der Befehl PRTVTAUT zuvor für die angegebenen Objekte in der Bibliothek oder im Ordner ausgeführt wurde. Dazu gehören alle neuen Objekte der ausgewählten Art sowie neue und geänderte Berechtigungen für die bereits vorhandenen Objekte. Wurde der Befehl PRTVTAUT zuvor noch nicht für die angegebenen Objekte in der Bibliothek oder dem Ordner ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, aber haben zwischenzeitlich keine Änderungen stattgefunden, wird ein Änderungsbericht ohne Objekte gedruckt.

Der dritte Bericht (Löschungen) enthält alle Benutzer, deren persönliche Berechtigungen für die angegebenen Objekte seit der letzten Ausführung des Befehls PRTPVTAUT gelöscht wurden. In dem Löschbericht werden sowohl alle gelöschten Objekte als auch alle gelöschten Benutzer mit persönlicher Berechtigung aufgeführt. Wurde der Befehl PRTPVTAUT zuvor noch nicht ausgeführt, wird kein Löschbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, aber wurde zwischenzeitlich keine Löschoperation für die Objekte ausgeführt, wird ein Löschbericht ohne Objekte gedruckt.

In den Berichten sind folgende Informationen enthalten:

- die im Befehl angegebene Objektart (sofern sie nicht *AUTL lautet)
- Datum und Uhrzeit der letzten Berichterstellung (nicht im Gesamtbericht)
- der Name der im Befehl angegebenen Bibliothek (sofern die Objektart nicht *AUTL, *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)
- die Berechtigung *PUBLIC für die Bibliothek (sofern die Objektart nicht *AUTL, *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet)

9.14.1.18
Seite 2

- der Name des Ordners mit den Dokumenten oder dem Ordner (wenn die Objektart *DOC oder *FLR lautet)
- der Name des Verzeichnisses, in dem sich die Objekte befinden (sofern die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK lautet)
- die Berechtigung *PUBLIC für das Verzeichnis (wenn die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK lautet)
- ein Eintrag für jeden Benutzer, der für die Objekte in der Liste berechtigt ist. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Objekts (nur beim ersten Benutzer)
  - den Eigner des Objekts (nur beim ersten Benutzer)
  - die Primärgruppe des Objekts (nur beim ersten Benutzer)
  - den Namen der Berechtigungsliste, die das Objekt sichert (nur beim ersten Benutzer, sofern die Objektart nicht *AUTL lautet)
  - die Sicherheitsstufe des Dokuments oder des Ordners (nur beim ersten Benutzer, sofern die Objektart *DOC oder *FLR lautet)
  - den Namen des Benutzers, der für das Objekt berechtigt ist
  - den Sonderwert für die Berechtigung, die der Benutzer für das Objekt besitzt (zum Beispiel *ALL oder *CHANGE)
  - eine Angabe für die individuellen Berechtigungen, die der Benutzer für das Objekt besitzt ('X' oder ' ') (sofern die Objektart nicht *DOC oder *FLR lautet)

Die Datei QPBXXXXXXX ('XXXXXXX' ist die im Befehl angegebene Objektart) in Bibliothek QUSRSYS enthält Informationen, die die vorherige Ausführung des Befehls PRTPVTAUT betreffen. Sofern die Objektart nicht *BLKSF, *DIR, *DOC, *FLR, *SOCKET, *STMF oder *SYMLNK lautet, enthält diese Datei für jede zuvor im Befehl angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Bei Objektarten, für die keine Bibliotheksangabe erforderlich ist (zum Beispiel *USRPRF), lautet der Bibliotheksname QSYS. Die Systemdatei QAOBJAUT in Bibliothek QSYS mit dem Formatnamen QSYDSAUT dient als Modell für die Datei.

Lautet die Objektart *FLR, enthält die erste Teildatei die Informationen, die die vorherige Angabe von *FLR in dem Befehl betreffen. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO dient als Modell für die Datei.

Lautet die Objektart *DOC, enthält die Datei eine Teildatei für jeden Ordner, der zuvor in dem Befehl angegeben wurde. Der Name der Teildatei stimmt mit dem Systemnamen des Ordners überein. Die Systemdatei QASECDLO in Bibliothek QSYS mit dem Formatnamen QSECDLO ist die Objektart *FILE. Wurde für den Parameter AUTTYPE der Wert *FIELD oder *ALL angegeben, wird der Befehl DSPOBJAUT (Objektberechtigung anzeigen) für jede Datei ausgeführt, der Berechtigungen auf Feldebene zugeordnet sind. Für jede dieser Dateien wird eine Spooldatei mit dem Namen QPOBJAUT erstellt, die alle Berechtigungsdaten auf Feldebene für die Datei enthält. Unterstützung für Änderungsberichte steht jedoch für Berechtigungsdaten auf Feldebene für diese Dateien nicht zur Verfügung.

Lautet die Objektart *BLKSF, *DIR, *SOCKET, *STMF oder *SYMLNK, enthält die Datei eine Teildatei für jedes Verzeichnis, das zuvor im Parameter „Verzeichnis“ (DIR) angegeben wurde. Die Teildateinamen basieren auf der Reihenfolge, in der die Verzeichnisse verarbeitet werden. Die Namen der Teildateien folgen der Namenskonvention x000000001, x000000002 usw. Das erste Zeichen des Teildateinamens ist entweder N oder Y. Dieses Zeichen weist darauf hin, ob die Unterverzeichnisse bei der Erfassung der Daten durchsucht wurden. N bedeutet, dass die Unterverzeichnisse nicht durchsucht wurden, Y bedeutet, dass sie durchsucht wurden. Sobald einem Verzeichnis ein Teildateiname zugeordnet wurde, wird der numerische Teil des Präfixes für alle oben aufgeführten Objektarten verwendet. Die Systemdatei QASECDIR in Bibliothek QSYS mit dem Formatnamen QSECDIR dient als Modell für die Datei.

9.14.1.18

Seite 4

Anmerkung:

Die Datei QASECGFIPV in Bibliothek QUSRSYS enthält die Datei-ID-Werte für jedes verarbeitete Verzeichnis sowie den Nxxxxxxxxx-Teildateinamen, der ihm zugeordnet wurde. Die Systemdatei QASECGFI in Bibliothek QSYS mit dem Formatnamen QSECGFI dient als Modell für QASECGFIPV.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                    RAZLEE    28.10.14  09:30:58 CET
 Bibliothek . . . . . . . . . . :   QGPL
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *CMD
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                        Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner     gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 ADDCSWND    RENGEL     *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X    X
                                                RENGEL     *ALL      X    X    X      X      X    X     X    X    X    X
                                                QPGMR      *ALL      X    X    X      X      X    X     X    X    X    X
 AJB         RENGEL     *NONE       *NONE       *PUBLIC    *USE      X                             X                       X
                                                RENGEL     *ALL      X    X    X      X      X    X     X    X    X    X
                                                QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 AJZ         RENGEL     *NONE       *NONE       *PUBLIC    *USE      X                             X                       X
                                                RENGEL     *ALL      X    X    X      X      X    X     X    X    X    X
                                                QSYS       *ALL      X    X    X      X      X    X     X    X    X    X
 APYRLOBJ    RENGEL     *NONE       *NONE       *PUBLIC    *USE      X                             X                       X
                                                RENGEL     *ALL      X    X    X      X      X    X     X    X    X    X
                                                                                                                  Weitere ...
```

9.14.1.19 DFV-Datenschutz drucken

Mit dem Befehl PRTCMNSEC (DFV-Datenschutzbericht drucken) kann ein Bericht gedruckt werden, der die Sicherheitsattribute der auf dem System vorhandenen *DEVD-, *CTLD- und *LIND-Objekte enthält. Auf diese Weise kann die Sicherheit der DFV-Konfiguration geprüft werden.

Mit dem Befehl PRTCMNSEC werden zwei Spool-Ausgabedateien erstellt, die DFV-Datenschutzinformationen enthalten. Die erste Spooldatei enthält einen Bericht, der vom CL-Befehl DSPCFGL (Konfigurationsliste anzeigen) erstellt wurde. Er beinhaltet die momentan in der fernen APPN-Konfigurationsliste QAPPNRMT enthaltenen Einträge. Wenn die Konfigurationsliste QAPPNRMT nicht auf dem System vorhanden ist, wird kein Bericht gedruckt. Die zweite Spooldatei enthält einen Bericht mit den Sicherheitsattributen der im System vorhandenen *DEVD-, *CTLD- und *LIND-Objekte.

Einschränkung:

Der Benutzer benötigt die Sonderberechtigungen *ALLOBJ und *IOSYSCFG oder *AUDIT, um diesen Befehl verwenden zu können.

Die Spool-Ausgabedatei mit den *DEVD-, *CTLD- und *LIND-Objekten enthält zwei Berichte. Der erste Bericht (Gesamt) enthält sämtliche DFV-Objekte sowie die Sicherheitsattribute der einzelnen Objekte. Der zweite Bericht (Änderungen) enthält die DFV-Objekte, die seit der letzten Ausführung des Befehls PRTCMNSEC geändert wurden. Wurde der Befehl zuvor noch nicht ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, aber zwischenzeitlich kein DFV-Objekt geändert, wird ein Änderungsbericht gedruckt, der keine Objekte enthält.

Der erste Bericht enthält die Einträge aus dem fernen APPN-Konfigurationslistenobjekt QAPPNRMT. Wenn die Konfigurationsliste QAPPNRMT nicht vorhanden ist, wird kein Bericht gedruckt.

Der zweite Bericht enthält die unten angegebenen Informationen für die Objektarten *DEVD, *CTLD und *LIND. Felder, die leer oder auf Null gesetzt sind, sind für das entsprechende Objekt nicht zutreffend.

9.14.1.19
Seite 2

Objektart *DEVD
In den Berichten sind folgende Informationen enthalten:

- die Objektart
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jedes *DEVD-Objekt im System
  - der Name des DFV-Objekts
  - die Objektart des DFV-Objekts
  - die Einheitenkategorie des DFV-Objekts
  - der für das DFV-Objekt angegebene Wert für die Standortsicherheit
  - eine Angabe darüber, ob ein Standortkennwort für das DFV-Objekt vorhanden ist
  - der für das DFV-Objekt angegebene Wert für die APPN-Fähigkeit
  - der für das DFV-Objekt angegebene Wert für Einzelsitzung
  - der für das DFV-Objekt angegebene Wert für vordefinierte Sitzung
  - der für das DFV-Objekt angegebene Wert für den SNUF-Programmstart

Objektart *CTLD
In den Berichten sind folgende Informationen enthalten:

- die Objektart
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jedes *CTLD-Objekt im System
  - der Name des DFV-Objekts
  - die Objektart des DFV-Objekts
  - die Steuereinheitenkategorie des DFV-Objekts
  - der für das DFV-Objekt angegebene Wert für automatisches Erstellen
  - der für das DFV-Objekt angegebene Wert für die Steuereinheit mit Wählleitung
  - der für das DFV-Objekt angegebene Wert für die Anrufrichtung
  - der für das DFV-Objekt angegebene Wert für die APPN-Fähigkeit
  - der für das DFV-Objekt angegebene Wert für CP-Sitzungen
  - der für das DFV-Objekt angegebene Wert für den Unterbrechungszeitgeber

- der für das DFV-Objekt angegebene Wert für automatisches Löschen (in Minuten)
- der für das DFV-Objekt angegebene Wert für den Einheitennamen

Objektart *LIND
In den Berichten sind folgende Informationen enthalten:

- die Objektart
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jedes *LIND-Objekt im System
  - der Name des DFV-Objekts
  - die Objektart des DFV-Objekts
  - die Leitungskategorie des DFV-Objekts
  - der für das DFV-Objekt angegebene Wert für automatisches Erstellen
  - der für das DFV-Objekt angegebene Wert für automatisches Löschen (in Minuten)
  - der für das DFV-Objekt angegebene Wert für automatischen Rückruf
  - der für das DFV-Objekt angegebene Wert für automatisches Anwählen

Die Datei QSECCMNOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTCMNSEC betreffen. Die Systemdatei QASECCMN in Bibliothek QSYS mit dem Formatnamen QSECCMN dient als Modelldatei für QSECCMNOLD.

```
Datei . . . . . :   QPSECCMN                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                    DFV-Informationen (Gesamt)                                        Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    28.10.14  11:02:46 CET
 Objektart  . . . . . . . . . . :   *DEVD

                          Einheiten-     Sicherer     Standort-                    Einzelne     Vordefin.     SNUF-Progr.
 Objektname     Objektart kategorie      Standort     kennwort      APPN-fähig     Sitzung       Sitzung       Start
 #2345          *DEVD     *DSP
 A              *DEVD     *DSP
 ALEXS2         *DEVD     *DSP
 BLINKI         *DEVD     *DSP
 DSP01          *DEVD     *DSP
 GGS01          *DEVD     *DSP
 GGS1           *DEVD     *DSP
 GMGS01         *DEVD     *DSP
 LINETTCP       *DEVD     *NET
 OPT03          *DEVD     *OPT
 OPT04          *DEVD     *OPT
 OPT99          *DEVD     *OPT
 PCHOLLE1       *DEVD     *DSP
 PCHOLLE2       *DEVD     *DSP

                                                                                                  Weitere ...
```

9.14.1.19

Seite 4

9.14.1.20 Verzeichnisberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                      RAZLEE    28.10.14  17:41:37 CET
 Objektart  . . . . . . . . . . :   *DIR
 Verzeichnis  . . . . . . . . . :   /iSecurity
                                    Berecht.-    Daten-     ---------Objekt----------   ---------------Daten----------------
 Objekt                  Eigner     liste        berecht.   Ver   Exist   Änder   Ref   Opr   Lese   Hin   Akt   Dlt   Ausf.
 SMS                     RENGEL     *NONE        *RX                                    X     X                          X
 report output           SECURITY1P *NONE        *RX                                    X     X                          X
 DB-Gate                 RAZLEEILOF *NONE        *RX                                    X     X                          X
 IBI                     RENGEL     *NONE        *RX                                    X     X                          X
 tmp                     RAZLEEILOF *NONE        *RX                                    X     X                          X
 Capture                 RENGEL     *NONE        *RX                                    X     X                          X
                         Objekte mit allgemeiner Berechtigung (Änderungen)                                      Seite     2
5770SS1 V7R2M0  140418                                                      RAZLEE    28.10.14  17:41:37 CET
 Objektart  . . . . . . . . . . :   *DIR
 Verzeichnis  . . . . . . . . . :   /iSecurity
 Letzter Änderungsbericht . . . :   26.10.14  10:40:33
                                    Berecht.-    Daten-     ---------Objekt----------   ---------------Daten----------------
 Objekt                  Eigner     liste        berecht.   Ver   Exist   Änder   Ref   Opr   Lese   Hin   Akt   Dlt   Ausf.
                                                                                                                 Weitere ...
```

9.14.1.20

Seite 2

9.14.1.21 Persönliche Verzeichnisberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  08:50:18 CET
 Verzeichnis  . . . . . . . . . . :   /iSecurity
 Berechtigung *PUBLIC . . . . . :   *RX
 Objektart  . . . . . . . . . . . :   *DIR
                                    Primär-      Berecht.-                  Daten-      -----------Objekt-----------
 Objekt                  Eigner     gruppe       liste       Benutzer       berecht.    Ver    Exist    Änder    Ref
 SMS                     RENGEL     *NONE        *NONE       *PUBLIC        *RX
                                                             RENGEL         *RWX         X       X        X       X
 report output           SECURITY1P *NONE        *NONE       *PUBLIC        *RX
                                                             SECURITY1P     *RWX         X       X        X       X
 DB-Gate                 RAZLEEILOF *NONE        *NONE       *PUBLIC        *RX
                                                             RAZLEEILOF     *RWX         X       X        X       X
 IBI                     RENGEL     *NONE        *NONE       *PUBLIC        *RX
                                                             RENGEL         *RWX         X       X        X       X
 tmp                     RAZLEEILOF *NONE        *NONE       *PUBLIC        *RX
                                                             RAZLEEILOF     *RWX         X       X        X       X
 Capture                 RENGEL     *NONE        *NONE       *PUBLIC        *RX
                                                             RENGEL         *RWX         X       X        X       X
                                                                                                          Weitere ...
```

9.14.1.21

Seite 2

9.14.1.22 Dokumentberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   _                                                       Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                          RAZLEE    01.11.14  09:00:51 CET
 In Ordner  . . . . . . . . . . . :   PS
                                Berecht.-      Berech-        Sicherheits-
 Dokument         Eigner        Liste          tigung         stufe
   (Es sind keine DLO-Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                                Objekte mit allgemeiner Berechtigung (Änderungen)                              Seite     2
5770SS1 V7R2M0  140418                                                          RAZLEE    01.11.14  09:00:51 CET
 In Ordner  . . . . . . . . . . . :   PS
                                Berecht.-      Berech-        Sicherheits-
 Dokument         Eigner        Liste          tigung         stufe
   (Es sind keine DLO-Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                                     * * * * *  E N D E   D E R   L I S T E  * * * * *
```

9.14.1.22

Seite 2

9.14.1.23 Persönliche Dokumentberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Persönliche Berechtigungen drucken (Gesamt)                                    Seite     1
5770SS1 V7R2M0  140418                                                    RAZLEE    01.11.14  09:01:20 CET
 Objektart  . . . . . . . . . . :   *DOC
                               Primär-        Berecht.-                                  Berech-
 DLO             Eigner        gruppe         liste          Sicherheitsstufe     Benutzer   tigung
   (Es sind keine DLO-Objekte zum Auflisten vorhanden.)
                               Persönliche Berechtigungen drucken (Änderungen)                                Seite     2
5770SS1 V7R2M0  140418                                                    RAZLEE    01.11.14  09:01:20 CET
 Objektart  . . . . . . . . . . :   *DOC
                               Primär-        Berecht.-                                  Berech-
 DLO             Eigner        gruppe         liste          Sicherheitsstufe     Benutzer   tigung
   (Es sind keine DLO-Objekte zum Auflisten vorhanden.)
                               Persönliche Berechtigungen drucken (Löschungen)                                Seite     3
5770SS1 V7R2M0  140418                                                    RAZLEE    01.11.14  09:01:20 CET
 Objektart  . . . . . . . . . . :   *DOC
                               Primär-        Berecht.-                                  Berech-
 DLO             Eigner        gruppe         liste          Sicherheitsstufe     Benutzer   tigung
   (Es sind keine DLO-Objekte zum Auflisten vorhanden.)
                                    * * * * *  E N D E  D E R  L I S T E  * * * * *
                                                                                                      Ende
```

9.14.1.23

Seite 2

9.14.1.24 Dateiberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   _                                                       Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:01:51 CET
 Objektart  . . . . . . . . . . :   *FILE
 Angegebene Bibliothek  . . . . :   RLG
                                                  Berecht.-  Berech-   ----------Objekt-----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner       liste      tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 RLG         DADOCCLA    *SYSBAS     QSECOFR      *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         DEMOPF      *SYSBAS     RAZOFR       *NONE      *ALL      X    X     X      X     X    X     X    X    X      X
 RLG         DEMOPF_MM   *SYSBAS     RAZLEEFR     *NONE      *ALL      X    X     X      X     X    X     X    X    X      X
 RLG         DEMOPFJRN1  *SYSBAS     RENGEL       *NONE      *ALL      X    X     X      X     X    X     X    X    X      X
 RLG         DEMOPFJRN2  *SYSBAS     RENGEL       *NONE      *ALL      X    X     X      X     X    X     X    X    X      X
 RLG         DEMOPF1     *SYSBAS     RENGEL       *NONE      *ALL      X    X     X      X     X    X     X    X    X      X
 RLG         PRINTERFIL  *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         QCLPSRC     *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         RLG         *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         TEST        *SYSBAS     RENGEL       *NONE      *USE      X                             X                       X
 RLG         TESTSRC     *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         TEST1SRC    *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
 RLG         TEST2SRC    *SYSBAS     RENGEL       *NONE      *CHANGE   X                             X     X    X    X      X
                                                                                                                  Weitere ...
```

9.14.1.24

Seite 2

9.14.1.25 Persönliche Dateiberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _______                                           Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen (Gesamt)                                    Seite     1
5770SS1 V7R2M0  140418                                                          RAZLEE    01.11.14  09:02:49 CET
 Bibliothek . . . . . . . . . . :   RLG
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *FILE
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                          Primär-     Berecht.-                Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner      gruppe      liste       Benutzer     tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 AUCMXI      RENGEL      *NONE       SECURITY1P  *PUBLIC      *EXCLUDE
                                                 RENGEL       *ALL      X    X     X      X     X    X     X    X    X     X
                                                 SECURITY2P   *ALL      X    X     X      X     X    X     X    X    X     X
 DADOCCLA    QSECOFR     *NONE       *NONE       *PUBLIC      *CHANGE   X                              X     X    X    X     X
                                                 QSECOFR      *ALL      X    X     X      X     X    X     X    X    X     X
 DEMOPF      RAZOFR      *NONE       *NONE       *PUBLIC      *ALL      X    X     X      X     X    X     X    X    X     X
                                                 RAZOFR       *ALL      X    X     X      X     X    X     X    X    X     X
                                                 QPGMR        *ALL      X    X     X      X     X    X     X    X    X     X
 DEMOPF_MM   RAZLEEFR    *NONE       *NONE       *PUBLIC      *ALL      X    X     X      X     X    X     X    X    X     X
                                                 RAZLEEFR     *ALL      X    X     X      X     X    X     X    X    X     X
                                                 QPGMR        *ALL      X    X     X      X     X    X     X    X    X     X
                                                                                                                  Weitere ...
```

9.14.1.25

Seite 2

9.14.1.26 Ordnerberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    01.11.14  09:03:18 CET
                         Berecht.-   Berech-     Sicherheits-
 Ordner        Eigner    liste       tigung      stufe          In Ordner
 QDIADOCS      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2924      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2928      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2932      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2939      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2940      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QFOS2942      QSYS      *NONE       *CHANGE     *NONE          *NONE
 QIWSADM       QSECOFR   QIWSADM     *USE        *NONE          *NONE
 MODEL         QSECOFR   QIWSADM     *USE        *NONE          QIWSADM
 USER          QSECOFR   QIWSADM     *USE        *NONE          QIWSADM
                         Objekte mit allgemeiner Berechtigung (Änderungen)                Seite     2
5770SS1 V7R2M0  140418                                                RAZLEE    01.11.14  09:03:18 CET
 Letzter Änderungsbericht . . . :   26.10.14  20:00:25
                         Berecht.-   Berech-     Sicherheits-
 Ordner        Eigner    liste       tigung      stufe          In Ordner
                                                                                  Weitere ...
```

9.14.1.26

Seite 2

9.14.1.27 Persönliche Ordnerberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _                                                       Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen drucken (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:03:42 CET
 Objektart  . . . . . . . . . . :   *FLR
 In Ordner  . . . . . . . . . . :   *NONE
                                Primär-        Berecht.-                                        Berech-
 DLO            Eigner          gruppe         liste          Sicherheitsstufe    Benutzer      tigung
 PS             QSPLJOB         *NONE          *NONE          *NONE               QSPLJOB       *ALL
                                                                                   *PUBLIC       *EXCLUDE
 QDIADOCS       QSYS            *NONE          *NONE          *NONE               QSYS          *ALL
                                                                                   *PUBLIC       *CHANGE
 QFOSDIA        QSECOFR         *NONE          *NONE          *NONE               QSECOFR       *ALL
                                                                                   *PUBLIC       *EXCLUDE
 QFOS2924       QSYS            *NONE          *NONE          *NONE               QSYS          *ALL
                                                                                   *PUBLIC       *CHANGE
 QFOS2928       QSYS            *NONE          *NONE          *NONE               QSYS          *ALL
                                                                                   *PUBLIC       *CHANGE
 QFOS2932       QSYS            *NONE          *NONE          *NONE               QSYS          *ALL
                                                                                   *PUBLIC       *CHANGE
 QFOS2939       QSYS            *NONE          *NONE          *NONE               QSYS          *ALL
                                                                                                  Weitere ...
```

9.14.1.27

Seite 2

9.14.1.28 Jobbeschreibungsberechtigung drucken

Mit dem Befehl PRTJOBDAUT (Jobbeschreibungsberechtigung drucken) kann ein Bericht gedruckt werden, der die Jobbeschreibungen einer Bibliothek enthält, deren allgemeine Berechtigung nicht *EXCLUDE lautet und in denen ein Benutzername als Jobbeschreibung angegeben ist. Auf diese Weise kann geprüft werden, welche Jobbeschreibungen, die für sämtliche Systembenutzer zugänglich sind, der Benutzer unter einem anderen Benutzerprofil ausführen kann.

Mit diesem Befehl werden zwei Berichte für eine Bibliothek gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Subsystembeschreibungen, für die ein Standardbenutzer im Subsystemeintrag angegeben ist. Der zweite Bericht (Änderungen) enthält die Jobbeschreibungen, die jetzt nicht über die allgemeine Berechtigung *EXCLUDE verfügen oder für die ein Benutzername angegeben ist, der entweder über die allgemeine Berechtigung *EXCLUDE verfügt hat, für den kein Benutzername angegeben war, oder der nicht vorhanden war, als der Befehl PRTJOBDAUT zuvor für die Bibliothek ausgeführt wurde. Wurde der Befehl zuvor noch nicht für die Bibliothek ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine weiteren Subsystembeschreibungen mit einem Standardbenutzer hinzugekommen, wird ein Änderungsbericht gedruckt, der keine Subsystembeschreibungen enthält. Änderungen, die die Sonderberechtigungen eines Benutzerprofils betreffen, führen nicht zu einem Änderungsbericht.

In den Berichten sind folgende Informationen enthalten:

- der Name der im Befehl angegebenen Bibliothek
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jede Jobbeschreibung, deren allgemeine Berechtigung (*PUBLIC) *EXCLUDE lautet und für die ein Benutzername angegeben ist. Jeder Eintrag enthält folgende Informationen:
  - den Namen der Bibliothek, in der sich die Jobbeschreibung befindet
  - den Namen der Jobbeschreibung
  - den Eigner der Jobbeschreibung
  - den Namen des in der Jobbeschreibung angegebenen Benutzerprofils
  - die dem Benutzerprofil zugeordneten Sonderberechtigungen. Es werden alle Sonderberechtigungen aufgeführt, die bei Verwendung der Jobbeschreibung verfügbar sind. Es sind sowohl die Sonderberechtigungen des Benutzers als auch die seiner Gruppenprofile (falls zutreffend) enthalten.

9.14.1.28
Seite 2

Die Datei QSECJBDOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTJOBDAUT für eine Bibliothek betreffen. Diese Datei enthält für jede zuvor innerhalb des Befehls angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Wurde für den Bibliotheksnamen ein Sonderwert angegeben (zum Beispiel *USRLIBL), wird der '*' im Teildateinamen durch ein 'Q' ersetzt. Die Systemdatei QAOBJAUT in Bibliothek QSYS mit dem Formatnamen QSYSDSAUT dient als Modelldatei für QSECJBDOLD.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECJOBD                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                  Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Jobbeschreibungen mit Zugriffsberechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:08:54 CET
 Angegebene Bibliothek  . . . . :   QGPL
                                                          ----------------Sonderberechtigungen-----------------
             Job-                                Benutzer-    *ALL   *AUD   *IOSYS   *JOB   *SAV   *SEC   *SER   *SPL
 Bibliothek  beschreib.  ASP-Einh.   Eigner      profil        OBJ    IT      CFG     CTL    SYS    ADM   VICE    CTL
 QGPL        QCTXFORM    *SYSBAS     QSYS        QUSER
 QGPL        QSPLAFPW    *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLDBR     *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLDKTR    *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLDKTW    *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLPRTW    *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLRMTW    *SYSBAS     QSPL        QSPLJOB
 QGPL        QSPLSTRWTR  *SYSBAS     QSPL        QSPLJOB
                         * * * * *  E N D E  D E R  L I S T E  * * * * *
```

9.14.1.29 Bibliotheksberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                          Objekte mit allgemeiner Berechtigung (Gesamt)                    Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    01.11.14  09:09:24 CET
 Objektart  . . . . . . . . . . . :   *LIB
 Angegebene Bibliothek  . . . . :   QSYS
                                                Berecht.-   Berech-   ----------Objekt-----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        #CGULIB     *SYSBAS     QSYS        *NONE       *USE       X                          X                        X
 QSYS        #COBLIB     *SYSBAS     QSYS        *NONE       *USE       X                          X                        X
 QSYS        #DFULIB     *SYSBAS     QSYS        *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        #DSULIB     *SYSBAS     QSYS        *NONE       *USE       X                          X                        X
 QSYS        #LIBRARY    *SYSBAS     QSYS        *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        #RPGLIB     *SYSBAS     QSYS        *NONE       *USE       X                          X                        X
 QSYS        #SEULIB     *SYSBAS     QSYS        *NONE       *USE       X                          X                        X
 QSYS        ALEX        *SYSBAS     RAZLEEILOF  *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        ALEX2       *SYSBAS     RAZLEEILOF  *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        ARD         *SYSBAS     RAZLEEILOF  *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        ARD2        *SYSBAS     RAZLEEILOF  *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        ARPEGGIOL   *SYSBAS     ARPEGGIO    *NONE       *CHANGE    X                          X     X    X    X     X
 QSYS        ARPZIP      *SYSBAS     RAZLEEILIL  *NONE       *CHANGE    X                          X     X    X    X     X
                                                                                                                  Weitere ...
```

9.14.1.29

Seite 2

9.14.1.30 Persönliche Bibliotheksberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                RAZLEE    01.11.14  09:14:47 CET
 Bibliothek . . . . . . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . . . . . . :   *LIB
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                       Primär-     Berecht.-              Berech-   ----------Objekt----------  ----------Daten----------
 Objekt      Eigner    gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #CGULIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                              X                      X
                                               QSYS       *ALL      X    X     X      X     X    X     X    X    X     X
 #COBLIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                              X                      X
                                               QSYS       *ALL      X    X     X      X     X    X     X    X    X     X
 #DFULIB     QSYS      *NONE       *NONE       *PUBLIC    *CHANGE   X                              X     X    X    X     X
                                               QSYS       *ALL      X    X     X      X     X    X     X    X    X     X
 #DSULIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                              X                      X
                                               QSYS       *ALL      X    X     X      X     X    X     X    X    X     X
 #LIBRARY    QSYS      *NONE       *NONE       *PUBLIC    *CHANGE   X                              X     X    X    X     X
                                               QSYS       *ALL      X    X     X      X     X    X     X    X    X     X
 #RPGLIB     QSYS      *NONE       *NONE       *PUBLIC    *USE      X                              X                      X
                                                                                                                Weitere ...
```

9.14.1.30

Seite 2

9.14.1.31 Objektberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   ________                                                Spalten     1 - 130
Suchen  . . . . .   ________________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                          RAZLEE    01.11.14  09:15:41 CET
 Objektart  . . . . . . . . . . :   *FILE
 Angegebene Bibliothek  . . . . :   RLG
                                                    Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.   Eigner         liste       tigung     Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 RLG         DADOCCLA    *SYSBAS     QSECOFR       *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         DEMOPF      *SYSBAS     RAZOFR        *NONE       *ALL       X    X     X      X     X      X     X    X    X      X
 RLG         DEMOPF_MM   *SYSBAS     RAZLEEFR      *NONE       *ALL       X    X     X      X     X      X     X    X    X      X
 RLG         DEMOPFJRN1  *SYSBAS     RENGEL        *NONE       *ALL       X    X     X      X     X      X     X    X    X      X
 RLG         DEMOPFJRN2  *SYSBAS     RENGEL        *NONE       *ALL       X    X     X      X     X      X     X    X    X      X
 RLG         DEMOPF1     *SYSBAS     RENGEL        *NONE       *ALL       X    X     X      X     X      X     X    X    X      X
 RLG         PRINTERFIL  *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         QCLPSRC     *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         RLG         *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         TEST        *SYSBAS     RENGEL        *NONE       *USE       X                                 X                      X
 RLG         TESTSRC     *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         TEST1SRC    *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
 RLG         TEST2SRC    *SYSBAS     RENGEL        *NONE       *CHANGE    X                                 X     X    X    X      X
                                                                                                                          Weitere ...
```

9.14.1.31

Seite 2

9.14.1.32 Persönliche Berechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Persönliche Berechtigungen (Gesamt)                                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:16:08 CET
 Bibliothek . . . . . . . . . . :   RLG
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *FILE
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                       Primär-     Berecht.-              Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner    gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 AUCMXI      RENGEL    *NONE       SECURITY1P  *PUBLIC    *EXCLUDE
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
                                               SECURITY2P *ALL      X    X     X      X     X    X     X    X    X     X
 DADOCCLA    QSECOFR   *NONE       *NONE       *PUBLIC    *CHANGE   X                                 X    X    X     X
                                               QSECOFR    *ALL      X    X     X      X     X    X     X    X    X     X
 DEMOPF      RAZOFR    *NONE       *NONE       *PUBLIC    *ALL      X    X     X      X     X    X     X    X    X     X
                                               RAZOFR     *ALL      X    X     X      X     X    X     X    X    X     X
                                               QPGMR      *ALL      X    X     X      X     X    X     X    X    X     X
 DEMOPF_MM   RAZLEEFR  *NONE       *NONE       *PUBLIC    *ALL      X    X     X      X     X    X     X    X    X     X
                                               RAZLEEFR   *ALL      X    X     X      X     X    X     X    X    X     X
                                               QPGMR      *ALL      X    X     X      X     X    X     X    X    X     X
                                                                                                                Weitere ...
```

9.14.1.32

Seite 2

9.14.1.33 Programmberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Objekte mit allgemeiner Berechtigung (Gesamt)                              Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:16:36 CET
 Objektart  . . . . . . . . . . :   *PGM
 Angegebene Bibliothek  . . . . :   RLG
                                                  Berecht.-   Berech-   ----------Objekt----------  ----------Daten----------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 RLG         RE_AUD      *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
 RLG         RE_AUD_     *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
 RLG         RE_AUD__    *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
 RLG         RE_AUD_MMA  *SYSBAS     RAZLEEFR    *NONE       *CHANGE    X                          X     X    X    X      X
 RLG         RE_CPT001   *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
 RLG         RE_OBJ      *SYSBAS     RENGEL      *NONE       *CHANGE    X                          X     X    X    X      X
                                  * * * * *  E N D E  D E R  L I S T E  * * * * *
                                                                                                                    Ende
```

9.14.1.33

Seite 2

9.14.1.34 Persönliche Programmberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                                Seite/Zeile 1/1
Steuerung . . . .   _______                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Persönliche Berechtigungen (Gesamt)                                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  09:16:58 CET
 Bibliothek . . . . . . . . . . :   RLG
   Berechtigung *PUBLIC . . . . :     *CHANGE
 Objektart  . . . . . . . . . . :   *PGM
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                       Primär-     Berecht.-              Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner    gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 RE_AUD      RENGEL    *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X     X
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
 RE_AUD_     RENGEL    *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X     X
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
 RE_AUD__    RENGEL    *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X     X
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
 RE_AUD_MMA  RAZLEEFR  *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X     X
                                               RAZLEEFR   *ALL      X    X     X      X     X    X     X    X    X     X
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
 RE_CPT001   RENGEL    *NONE       *NONE       *PUBLIC    *CHANGE   X                             X     X    X    X     X
                                               RENGEL     *ALL      X    X     X      X     X    X     X    X    X     X
                                                                                                                Weitere ...
```

9.14.1.34

Seite 2

9.14.1.35 Benutzerprofilberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPUBAUT (Objekte mit allgemeiner Berechtigung drucken).

```
Datei . . . . . :   QPSECPUB                                                Seite/Zeile 1/1
Steuerung . . . .   _                                                       Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Objekte mit allgemeiner Berechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                                RAZLEE    01.11.14  09:17:31 CET
 Objektart  . . . . . . . . . . :   *USRPRF
 Angegebene Bibliothek  . . . . :   QSYS
                                                Berecht.-   Berech-   ----------Objekt----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
 QSYS        QDBSHR      *SYSBAS     QSYS                    USER DEF                                      X         X
 QSYS        QDBSHRDO    *SYSBAS     QSYS                    USER DEF                                      X         X
 QSYS        QTMPLPD     *SYSBAS     QSYS                    USER DEF   X
                              Objekte mit allgemeiner Berechtigung (Änderungen)                                Seite     2
5770SS1 V7R2M0  140418                                                                RAZLEE    01.11.14  09:17:31 CET
 Objektart  . . . . . . . . . . :   *USRPRF
 Angegebene Bibliothek  . . . . :   QSYS
 Letzter Änderungsbericht . . . :   10.26.14  20:14:10
                                                Berecht.-   Berech-   ----------Objekt----------  -----------Daten------------
 Bibliothek  Objekt      ASP-Einh.   Eigner      liste       tigung    Opr  Mgt  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausfüh.
   (Es sind keine Objekte mit allgemeiner Berechtigung zum Auflisten vorhanden.)
                                    * * * * *   E N D E   D E R   L I S T E   * * * * *

                                                                                                              Ende
```

9.14.1.35

Seite 2

9.14.1.36 Persönliche Benutzerprofilberechtigung drucken

Die Beschreibung des Befehls finden Sie weiter vorne unter dem Befehl PRTPVTAUT (Persönliche Berechtigung drucken).

```
Datei . . . . . :   QPSECPVT                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Persönliche Berechtigungen (Gesamt)                          Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    01.11.14  09:17:55 CET
 Bibliothek . . . . . . . . . . :   QSYS
   Berechtigung *PUBLIC . . . . :     *USE
 Objektart  . . . . . . . . . . :   *USRPRF
 ASP-Einheit  . . . . . . . . . :   *SYSBAS
                        Primär-     Berecht.-              Berech-   ----------Objekt-----------  ----------Daten-----------
 Objekt      Eigner     gruppe      liste       Benutzer   tigung    Opr  Ver  Exist  Änder  Ref  Lese  Hin  Akt  Lös  Ausf.
 #SYSLOAD    QSECOFR    *NONE                   *PUBLIC    *EXCLUDE
                                                QSECOFR    *ALL       X    X     X      X     X     X     X    X    X     X
                                                #SYSLOAD   USER DEF   X    X                       X     X    X    X     X
 ARPEGGIO    RAZLEEILIL *NONE                   *PUBLIC    *EXCLUDE
                                                RAZLEEILIL *ALL       X    X     X      X     X     X     X    X    X     X
                                                ARPEGGIO   USER DEF   X    X                       X     X    X    X     X
 CODESCOPE   RENGEL     *NONE                   *PUBLIC    *EXCLUDE
                                                RENGEL     *ALL       X    X     X      X     X     X     X    X    X     X
                                                CODESCOPE  USER DEF   X    X                       X     X    X    X     X
 DB          RAZLEEIL   *NONE                   *PUBLIC    *EXCLUDE
                                                RAZLEEIL   *ALL       X    X     X      X     X     X     X    X    X     X
                                                                                                                Weitere ...
```

9.14.1.36

Seite 2

9.14.1.37 Job- und Ausgabewarteschlangenberechtigung drucken

Mit dem Befehl PRTQAUT (Warteschlangenberechtigung drucken) kann ein Bericht mit den Ausgabe- und Jobwarteschlangenberechtigungen für die Objekte in der angegebenen Bibliothek gedruckt werden. Auf diese Weise kann geprüft werden, welche Berechtigungsattribute den Ausgabe- und Jobwarteschlangenobjekten zugeordnet sind.

Mit diesem Befehl werden zwei Berichte für eine Bibliothek gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Ausgabe- und Jobwarteschlangen in der angegebenen Bibliothek. Der zweite Bericht (Änderungen) enthält die Ausgabe- und Jobwarteschlangen, die seit der letzten Ausführung des Befehls PRTQAUT für die Bibliothek geändert oder deren Berechtigungsattribute geändert wurden. Wurde der Befehl zuvor noch nicht für die Bibliothek ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine Änderungen erfolgt, wird ein Änderungsbericht gedruckt, der keine Warteschlangen enthält.

In den Berichten sind folgende Informationen enthalten:

- der Name der im Befehl angegebenen Bibliothek
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jede im System vorhandene Ausgabe- und Jobwarteschlange. Jeder Eintrag enthält folgende Informationen:
  - den Namen der Bibliothek, in der sich die Warteschlange befindet
  - den Namen der Warteschlange
  - die Objektart der Warteschlange
  - den Eigner der Warteschlange
  - die allgemeine Berechtigung für die Warteschlange
  - den DSPDTA-Wert (Jede Datei anzeigen) der Ausgabewarteschlange; für Jobwarteschlangenobjekte wird dieses Feld auf *NONE gesetzt
  - den OPRCTL-Wert (Vom Bediener gesteuert) der Warteschlange
  - der AUTOCHK-Wert (Berechtigung prüfen) der Warteschlange

9.14.1.37
Seite 2

Die Datei QSECQOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTQAUT betreffen. Diese Datei enthält für jede zuvor innerhalb des Befehls angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Wurde für den Bibliotheksnamen ein Sonderwert angegeben (zum Beispiel *USRLIBL), wird der '*' im Teildateinamen durch ein 'Q' ersetzt. Die Systemdatei QASECQF in Bibliothek QSYS mit dem Formatnamen QSECQF dient als Modelldatei für QSECQOLD.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECQ                                          Seite/Zeile 1/1
Steuerung . . . .   _                                               Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Warteschlangenberechtigung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                    RAZLEE    01.11.14  09:21:18 CET
 Angegebene Bibliothek  . . . . :   *ALL

                                                    Berech-
 Bibliothek     Objekt          Art          Eigner  tigung     DSPDTA     OPRCTL     AUTCHK
 #SYSLOADX      OUTPUT          *OUTQ        QSECOFR *EXCLUDE   *NO        *YES       *OWNER
 #SYSLOADX      #SYSLOADQ       *JOBQ        QSECOFR *EXCLUDE   *NONE      *NO        *DTAAUT
 FB400          FBACKUPQ        *JOBQ        QSECOFR *USE       *NONE      *YES       *OWNER
 QDP4           QZSNDPR         *JOBQ        QSYS    *USE       *NONE      *YES       *OWNER
 QGPL           QDKT            *OUTQ        QPGMR   *USE       *NO        *YES       *OWNER
 QGPL           QPFROUTQ        *OUTQ        QSYS    *CHANGE    *YES       *YES       *OWNER
 QGPL           QPRINT          *OUTQ        QPGMR   *USE       *NO        *YES       *OWNER
 QGPL           QPRINTS         *OUTQ        QPGMR   *USE       *NO        *YES       *OWNER
 QGPL           QPRINT2         *OUTQ        QPGMR   *USE       *NO        *YES       *OWNER
 QGPL           QBASE           *JOBQ        QPGMR   *USE       *NONE      *YES       *OWNER
 QGPL           QBATCH          *JOBQ        QPGMR   *USE       *NONE      *YES       *OWNER
 QGPL           QFNC            *JOBQ        QFNC    *USE       *NONE      *YES       *OWNER
 QGPL           QINTER          *JOBQ        QPGMR   *USE       *NONE      *YES       *OWNER
 QGPL           QPGMR           *JOBQ        QPGMR   *USE       *NONE      *YES       *OWNER
                                                                                        Weitere ...
```

9.14.1.38 Subsystemberechtigung drucken

Mit dem Befehl PRTSBSDAUT (Berechtigung für Subsystembeschreibung drucken) kann ein Bericht mit den Subsystembeschreibungen in einer Bibliothek gedruckt werden, für die ein Standardbenutzer im Subsystemeintrag angegeben ist. Auf diese Weise kann geprüft werden, welche Subsystembeschreibungen auf dem System unter einem Standardbenutzerprofil verarbeitet werden können.

Mit diesem Befehl werden zwei Berichte für eine Bibliothek gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Subsystembeschreibungen, für die ein Standardbenutzer im Subsystemeintrag angegeben ist. Der zweite Bericht (Änderungen) enthält die Subsystembeschreibungen, die seit der letzten Ausführung des Befehls PRTSBSDAUT für die Bibliothek geändert wurden und jetzt einen Subsystemeintrag mit einem Standardbenutzer enthalten. Wurde der Befehl zuvor noch nicht für die Bibliothek ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine weiteren Subsystembeschreibungen mit einem Standardbenutzer hinzugekommen, wird ein Änderungsbericht gedruckt, der keine Subsystembeschreibungen enthält. Änderungen, die die Sonderberechtigungen eines Benutzerprofils betreffen, führen nicht zu einem Änderungsbericht.

In den Berichten sind folgende Informationen enthalten:

- der Name der im Befehl angegebenen Bibliothek
- Datum und Uhrzeit der letzten Berichterstellung (nur im Änderungsbericht)
- ein Eintrag für jede Subsystembeschreibung, für die ein Standardbenutzer im Subsystemeintrag angegeben ist. Jeder Eintrag enthält folgende Informationen:
  - den Namen der Bibliothek, in der sich die Subsystembeschreibung befindet
  - den Namen der Subsystembeschreibung
  - den Eigner der Subsystembeschreibung
  - den Namen des im Subsystemeintrag angegebenen Standardbenutzerprofils
  - die dem Benutzerprofil zugeordneten Sonderberechtigungen. Es werden alle Sonderberechtigungen aufgeführt, die bei Verwendung des Subsystemeintrags verfügbar waren. Es sind sowohl die Sonderberechtigungen des Benutzers als auch die seiner Gruppenprofile (falls zutreffend) enthalten.

9.14.1.38
Seite 2

Die Datei QSECSBDOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTSBSDAUT betreffen. Diese Datei enthält für jede zuvor innerhalb des Befehls angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Wurde für den Bibliotheksnamen ein Sonderwert angegeben (zum Beispiel *USRLIBL), wird der ‚*' im Teildateinamen durch ein ‚Q' ersetzt. Die Systemdatei QASECSBF in Bibliothek QSYS mit dem Formatnamen QSECSBF dient als Modelldatei für QSECSBDOLD.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECSBSD                                                  Seite/Zeile 1/1
Steuerung . . . .   _______                                                    Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                Subsystembeschreibung (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  11:26:26 CET
 Angegebene Bibliothek  . . . . :   QSYS

                                                 Standard-    ----------------Sonderberechtigungen-----------------
 Subsystem-   Subsystem-                Subsystem-  benutzer-    *ALL   *AUD   *IOSYS   *JOB   *SAV   *SEC   *SER   *SPL
 bibliothek   name          ASP-Einh.   eigner      profil       OBJ    IT     CFG     CTL    SYS    ADM   VICE    CTL
 QSYS         QCMN          *SYSBAS     QSYS        QIJS
 QSYS         QCMN          *SYSBAS     QSYS        QUSER
 QSYS         QSYSWRK       *SYSBAS     QSYS        QUSER
 QSYS         QSYSWRK       *SYSBAS     QSYS        QPM400                       X       X
 QSYS         QSYSWRK       *SYSBAS     QSYS        QIJS
 QSYS         QSYSWRK       *SYSBAS     QSYS        QPM400                       X       X
                                        * * * * *  E N D E   D E R   L I S T E  * * * * *
```

9.14.1.39 Systemsicherheitsattribute drucken

Mit dem Befehl PRTSYSSECA (Systemsicherheitsattribute drucken) wird ein Bericht mit sicherheitsrelevanten Systemwerten und Netzwerkattributen in eine Spooldatei ausgegeben. Der Bericht enthält den Systemwert oder den Namen des Netzwerkattributs, den aktuellen Wert und den empfohlenen Wert.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECATTR                                          Seite/Zeile 1/1
Steuerung . . . .   _____                                              Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Systemsicherheitsattribute                                    Seite     1
5770SS1 V7R2M0  140418                                                  RAZLEE    01.11.14  11:28:03 CET
 Systemwert
 Name                Aktueller Wert                          Empfohlener Wert
    QALWOBJRST       *ALL                                    *NONE
    QALWUSRDMN       *ALL                                    QTEMP
    QATNPGM          QEZMAIN   QSYS                          *NONE
    QAUDCTL          *AUDLVL   *OBJAUD   *NOQTEMP            *AUDLVL   *OBJAUD   *NOQTEMP
    QAUDENDACN       *NOTIFY                                 *NOTIFY
    QAUDFRCLVL       *SYS                                    *SYS
    QAUDLVL          *ATNEVT   *AUTFAIL  *CREATE   *DELETE   *AUDLVL2
                     *JOBDTA   *OBJMGT   *PGMADP   *PGMFAIL
                     *SAVRST   *SECURITY *SERVICE  *SPLFDTA
                     *SYSMGT
    QAUDLVL2         *NONE                                   *AUTFAIL  *CREATE   *DELETE   *SAVRST
                                                             *SECURITY
    QAUTOCFG         1                                       0
    QAUTORMT         1                                       0
    QAUTOVRT         512                                     0
                                                                                          Weitere ...
```

9.14.1.39

Seite 2

9.14.1.40 Auslöserprogramme drucken

Mit dem Befehl PRTTRGPGM (Auslöserprogramme drucken) werden die Programme aufgelistet, die als Auslöserprogramme für die in der angegebenen Bibliothek enthaltenen Dateien definiert wurden.

Mit diesem Befehl werden zwei Berichte für eine Bibliothek gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Auslöserprogramme, die Dateien in der angegebenen Bibliothek zugeordnet sind. Der zweite Bericht (Änderungen) enthält die Auslöserprogramme, die seit der letzten Ausführung des Befehls PRTTRGPGM für die Bibliothek hinzugekommen sind. Wurde der Befehl zuvor noch nicht für die Bibliothek ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine Auslöserprogramme hinzugekommen, wird ein Änderungsbericht gedruckt, der keine Objekte enthält. Eine Änderung der Zeit, des Ereignisses und der Bedingung für ein Auslöserprogramm führen nicht zu einem Änderungsbericht.

Die Datei QSECTRGOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTTRGPGM betreffen. Diese Datei enthält für jede zuvor im Befehl angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Die Systemdatei QAFDTRG in Bibliothek QSYS mit dem Formatnamen QWHFDTRG dient als Modelldatei für QSECTRGOLD.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

```
Datei . . . . . :   QPSECTRG                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                              Auslöserprogramm (Gesamtbericht)                                  Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    01.11.14  11:30:44 CET
 Angegebene Bibliothek  . . . . :   QSYS

                                                                                                 Wiederh.
                                  ---------------------------------------Auslöser---------------------------------------  Änd.
 Bibliothek Datei      ASP-Einh.   Name                 Art  Bibliothek Programm   Uhrzeit     Ereignis    Bedingung     zulass.
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach        Einfügen                  Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach        Aktual.     Ändern        Ja
 QSYS       QADBCCST   *SYSBAS     Q__QSYS_QADBCCST__ > *SYS QSYS       QDBXESND   Nach        Löschen                   Ja
 QSYS       QADBFCST   *SYSBAS     Q__QSYS_QADBFCST__ > *SYS QSYS       QDBXESND   Nach        Einfügen                  Ja
 QSYS       QADBFCST   *SYSBAS     Q__QSYS_QADBFCST__ > *SYS QSYS       QDBXESND   Nach        Aktual.     Ändern        Ja
 QSYS       QADBFCST   *SYSBAS     Q__QSYS_QADBFCST__ > *SYS QSYS       QDBXESND   Nach        Löschen                   Ja
 QSYS       QADBFDEP   *SYSBAS     Q__QSYS_QADBFDEP__ > *SYS QSYS       QDBXESND   Nach        Einfügen                  Ja
 QSYS       QADBFDEP   *SYSBAS     Q__QSYS_QADBFDEP__ > *SYS QSYS       QDBXESND   Nach        Aktual.     Ändern        Ja
 QSYS       QADBFDEP   *SYSBAS     Q__QSYS_QADBFDEP__ > *SYS QSYS       QDBXESND   Nach        Löschen                   Ja
 QSYS       QADBIFLD   *SYSBAS     Q__QSYS_QADBIFLD__ > *SYS QSYS       QDBXESND   Nach        Einfügen                  Ja
 QSYS       QADBIFLD   *SYSBAS     Q__QSYS_QADBIFLD__ > *SYS QSYS       QDBXESND   Nach        Aktual.     Ändern        Ja
 QSYS       QADBIFLD   *SYSBAS     Q__QSYS_QADBIFLD__ > *SYS QSYS       QDBXESND   Nach        Löschen                   Ja
 QSYS       QADBKFLD   *SYSBAS     Q__QSYS_QADBKFLD__ > *SYS QSYS       QDBXESND   Nach        Einfügen                  Ja
                                                                                                 Weitere ...
```

9.14.1.40

Seite 2

9.14.1.41 Benutzerobjekte drucken

Mit dem Befehl PRTUSROBJ (Benutzerobjekte drucken) kann ein Bericht gedruckt werden, der die Objekte in einer Bibliothek enthält, die nicht von IBM erstellt wurden. Es handelt sich dabei um die Objekte, deren Erstellerattribut nicht *IBM oder QLPINSTALL lautet. Auf diese Weise kann geprüft werden, welche vom Benutzer erstellten Objekte sich in Bibliotheken befinden, die für die ausschließliche Benutzung von IBM-Objekten vorgesehen sind. Dieser Befehl kann beispielsweise für die Bibliothek QSYS ausgeführt werden, um festzustellen, ob sie Objekte enthält, die nicht vom IBM erstellt wurden (Benutzerobjekte).

Anmerkung:

Einige der von IBM erstellten Objekte werden dennoch in diesem Bericht enthalten sein. Dies sind beispielsweise Objekte, die von einem PTF-Exitprogramm erstellt wurden. Objekte, deren Erstellerattribut „*IBM“ oder „QLPINSTALL“ lautet, werden nicht in diesen Bericht aufgenommen.

Mit diesem Befehl werden zwei Berichte für eine Bibliothek gedruckt. Der erste Bericht (Gesamt) enthält sämtliche Objekte, die nicht von IBM erstellt wurden. Der zweite Bericht (Änderungen) enthält die Objekte, die seit der letzten Ausführung des Befehls PRTUSROBJ für die Bibliothek hinzugekommen sind. Wurde der Befehl zuvor noch nicht für die Bibliothek ausgeführt, wird kein Änderungsbericht erstellt. Wurde der Befehl zwar bereits zuvor ausgeführt, sind aber zwischenzeitlich keine Objekte hinzugekommen, wird ein Änderungsbericht gedruckt, der keine Objekte enthält.

Die Datei QSECPUOOLD in Bibliothek QUSRSYS enthält Informationen, die die letzte Ausführung des Befehls PRTUSROBJ betreffen. Diese Datei enthält für jede zuvor im Befehl angegebene Bibliothek eine Teildatei gleichen Namens wie die Bibliothek. Die Systemdatei QADSPOBJ in Bibliothek QSYS mit dem Formatnamen QLIDOBJD dient als Modelldatei für QSECPUOOLD.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

9.14.1.41 Seite 2

```
Datei . . . . . :   QPSECPUO                                          Seite/Zeile 1/1
Steuerung . . . .   _                                                 Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerobjekte (Gesamt)                                  Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    01.11.14  11:33:03 CET
 Angegebene Bibliothek  . . . . :   RLG
 Bibliothek   Objekt       Art        ASP-Einh.    Attribut    Eigner       Beschreibung
 RLG          RE_AUD       *PGM       *SYSBAS      CLP         RENGEL       Changes for Audit
 RLG          RE_AUD_      *PGM       *SYSBAS      CLP         RENGEL       Changes for Audit
 RLG          RE_AUD__     *PGM       *SYSBAS      CLP         RENGEL       Changes for Audit
 RLG          RE_AUD_MMA   *PGM       *SYSBAS      CLP         RAZLEEFR     Changes for Audit
 RLG          RE_CPT001    *PGM       *SYSBAS      CLP         RENGEL       Changes for Audit
 RLG          RE_OBJ       *PGM       *SYSBAS      CLP         RENGEL       Objekt in RLG löschen und erstellen
 RLG          TEST         *DTAQ      *SYSBAS                  RAZLEEFR
 RLG          TEST1        *DTAQ      *SYSBAS                  RAZLEEFR
 RLG          AUCMXI       *FILE      *SYSBAS      PF          RENGEL
 RLG          DADOCCLA     *FILE      *SYSBAS      PF          QSECOFR      DirectArc - Document Classes
 RLG          DEMOPF       *FILE      *SYSBAS      PF          RAZOFR       Demo file  1
 RLG          DEMOPF_MM    *FILE      *SYSBAS      PF          RAZLEEFR     Demo file
 RLG          DEMOPFJRN1   *FILE      *SYSBAS      PF          RENGEL       Demo file  1
 RLG          DEMOPFJRN2   *FILE      *SYSBAS      PF          RENGEL       Demo file  2
 RLG          DEMOPF1      *FILE      *SYSBAS      PF          RENGEL       Demo file  1
                                                                                  Weitere ...
```

9.14.1.42 Benutzerprofilinformationen drucken

Mit dem Befehl PRTUSRPRF (Benutzerprofil drucken) kann ein Bericht gedruckt werden, der Informationen über die auf dem System vorhandenen Benutzerprofile enthält. Es können vier verschiedene Berichte gedruckt werden. Ein Bericht mit Informationen über Berechtigungen, einer mit Informationen über Umgebungen, einer mit Informationen über Kennwörter und einer mit Informationen über Kennwortstufen.

Der Bericht mit den Berechtigungsinformationen enthält folgende Angaben:

- die Art des Berichts
- die Auswahlkriterien für die Benutzerprofile
- die Sonderberechtigungen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *SPCAUT lautet)
- die Benutzerklassen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *USRCLS lautet)
- einen Eintrag für jedes ausgewählte Benutzerprofil. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Benutzerprofils
  - die Namen der Gruppenprofile des Benutzers. Sind dem Benutzerprofil keine Gruppenprofile zugeordnet, enthält dieses Feld den Wert ‚*NONE'. Andernfalls folgt auf den Benutzerprofileintrag ein weiterer Eintrag für die einzelnen Gruppenprofile mit dem jeweiligen Namen und den Sonderberechtigungen.
  - eine Angabe für die Sonderberechtigungen des Benutzerprofils (‚X' oder , ,)
  - die Benutzerklasse für das Benutzerprofil
  - ob es sich bei dem Benutzer- oder Gruppenprofil um einen Eigner von Objekten handelt, die von diesem Benutzerprofil erstellt wurden
  - die Berechtigung, die das Gruppenprofil für neu erstellte Objekte besitzt (wenn der Eignerwert *USRPRF lautet)
  - den Wert für „Möglichkeiten einschränken" des Benutzerprofils

9.14.1.42
Seite 2

Der Bericht mit den Umgebungsinformationen enthält folgende Angaben:

- die Art des Berichts
- die Auswahlkriterien für die Benutzerprofile
- die Sonderberechtigungen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *SPCAUT lautet)
- die Benutzerklassen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *USRCLS lautet)
- einen Eintrag für jedes ausgewählte Benutzerprofil. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Benutzerprofils
  - den Namen der aktuellen Benutzerbibliothek
  - den Namen des Startmenüs für den Benutzer und den Namen der Bibliothek für das Menü
  - den Namen des Startprogramms für den Benutzer und den Namen der Bibliothek für das Programm
  - den Namen der Jobbeschreibung für den Benutzer und den Namen der Bibliothek für die Jobbeschreibung
  - den Namen der Nachrichtenwarteschlange für den Benutzer und den Namen der Bibliothek für die Nachrichtenwarteschlange
  - den Namen des Abrufprogramms für den Benutzer und den Namen der Bibliothek für das Programm

Der Bericht mit den Kennwortinformationen enthält folgende Angaben:

9.14.1.42
Seite 3

- die Art des Berichts
- die Auswahlkriterien für die Benutzerprofile
- die Sonderberechtigungen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *SPCAUT lautet)
- die Benutzerklassen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *USRCLS lautet)
- der Wert für den Systemwert QPWDEXPITV (als Referenz, wenn die Verfallszeit für das Benutzerkennwort *SYSVAL lautet)
- einen Eintrag für jedes ausgewählte Benutzerprofil. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Benutzerprofils
  - den Status des Benutzerprofils
  - die Anzahl der ungültigen Anmeldeversuche
  - die Angabe für ‚kein Kennwort' (‚X', wenn der Benutzer kein Kennwort hat, , „ wenn er eins hat)
  - ob das Kennwort lokal verwaltet wird
  - das Datum der letzten Anmeldung des Benutzers
  - das Datum, zu dem das Benutzerkennwort zuletzt geändert wurde
  - die Verfallszeit des Benutzerkennworts
  - ob das Benutzerkennwort verfallen soll

9.14.1.42
Seite 4

Der Bericht mit den Informationen über die Kennwortstufen wird verwendet, um festzustellen, ob das System für die Änderung von Kennwortstufen bereit ist:

- die Art des Berichts
- die Auswahlkriterien für die Benutzerprofile
- die Sonderberechtigungen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *SPCAUT lautet)
- die Benutzerklassen, nach denen die Auswahl erfolgte (wenn ‚Auswählen nach' *USRCLS lautet)
- einen Eintrag für jedes ausgewählte Benutzerprofil. Jeder Eintrag enthält folgende Informationen:
  - den Namen des Benutzerprofils
  - die Anzeige ‚Kennwort vorhanden für Stufe 0 oder 1' (‚*YES', wenn der Benutzer über ein Kennwort verfügt, ‚*NO', wenn der Benutzer kein Kennwort hat, oder ‚*UNKNOWN', wenn keine Informationen über das Kennwort verfügbar sind)
  - die Anzeige ‚Kennwort vorhanden für Stufe 2 oder 3' (‚*YES', ‚*NO' oder ‚*UNKNOWN')
  - die Anzeige ‚Kennwort vorhanden für NetServer' für Windows 95/98 NetServer-Kennwörter (‚*YES', ‚*NO' oder ‚*UNKNOWN')

Anmerkung:

Mit dem Befehl DSPSECA (Sicherheitsattribute anzeigen) werden die aktuellen und anstehenden Kennwortstufen für das System angezeigt. Die Kennwortstufe kann geändert werden, indem der Systemwert QPWDLVL geändert wird.

Einschränkung:

Der Benutzer muss über die Sonderberechtigungen (*ALLOBJ) und (*AUDIT) verfügen, um diesen Befehl ausführen zu können.

9.14.1.42
Seite 5

```
Datei . . . . . :   QPSECUSR                                                Seite/Zeile 1/1
Steuerung . . . .   _____                                                   Spalten     1 - 130
Suchen  . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                                  Benutzerprofilinformationen                                  Seite     1
5770SS1 V7R2M0  140418                                                 RAZLEE    01.11.14  11:41:26 CET
 Berichtsart  . . . . . . . . . :   *AUTINFO
 Auswählen nach . . . . . . . . :   *SPCAUT
 Sonderberechtigungen . . . . . :   *ALL
                       -----------Sonderberechtigungen------------                          Art
                                  *IO                                                       der
 Benutzer-   Gruppen-    *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Benutzer-          Gruppen-  Möglichk.
 profil      profile      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  klasse    Eigner  tigung    berecht.  einschr.
 #SYSLOAD    *NONE        X     X    X     X     X     X    X      X    *SECOFR   *USRPRF *NONE     *PRIVATE  *NO
 ARPEGGIO                                                              *USER     *USRPRF *NONE     *PRIVATE  *YES
             DB           X     X    X     X     X     X    X      X
             FORGOT
 CODESCOPE   *NONE                                                     *PGMR     *USRPRF *NONE     *PRIVATE  *NO
 DB          *NONE        X     X    X     X     X     X    X      X    *SECOFR   *USRPRF *NONE     *PRIVATE  *NO
 DISKSCOPE                X                X           X    X           *SECOFR   *GRPPRF *NONE     *PRIVATE  *NO
             QSECOFR      X     X    X     X     X     X    X      X
 FILESCOPE   *NONE                                                     *PGMR     *USRPRF *NONE     *PRIVATE  *NO
 FORGOT      *NONE                                                     *USER     *USRPRF *NONE     *PRIVATE  *YES
```

9.14.1.42

Seite 6

9.14.2 Systemsicherheit konfigurieren

Dieser Befehl aktiviert die Systemsicherheitseinrichtungen, indem er die Sicherheitsprotokollierung aktiviert und Systemwerte sowie vom System bereitgestellte Benutzerprofile ändert. Den Befehl sollte nur ausgeführt werden, wenn bekannt ist, welche Einrichtungen er aktiviert.

Um festzustellen, welche Sicherheitseinrichtungen aktiviert werden, setzen Sie den Befehl RTVCLSRC (CL-Quelle auffinden) für das Programm QSECCFGS ab und prüfen die erstellte Quellendatei.

Es folgt ein Überblick darüber, was ggf. mit diesem Befehl geändert wird:

- Systemwert QALWOBJRST von *ALL in *NONE geändert
- Systemwert QAUDCTL von *AUDLVL in *AUDLVL*OBJAUD*NOQTEMP geändert
- Systemwert QAUDLVL von *SECCFG*SECRUN in *AUTFAIL *CREATE*-DELETE geändert
- *SECURITY *SAVRST geändert
- Systemwert QAUTOCFG von 1 in 0 geändert
- Systemwert QAUTOVRT von 32767 in 0 geändert
- Systemwert QDSCJOBITV von 0000000240 in 0000000120 geändert
- Systemwert QDSPSGNINF von 0 in 1 geändert
- Systemwert QINACTITV von *NONE in 0000000060 geändert
- Systemwert QLMTDEVSSN von 0 in 1 geändert
- Systemwert QLMTSECOFR von 0 in 1 geändert
- Systemwert QSECURITY von 40 in 50 geändert
- Systemwert QVFYOBJRST von 1 in 3 geändert
- Systemwert QFRCCVNRST von 1 in 4 geändert
- Systemwert QPWDEXPITV von *NOMAX in 000060 geändert
- Systemwert QPWDPOSDIF von 0 in 1 geändert
- Systemwert QPWDLMTCHR wird auf Kennwortstufe 2 ignoriert
- Systemwert QPWDLMTCHR von *NONE in AEIOU§$# geändert
- Systemwert QPWDLMTAJC von 0 in 1 geändert
- Systemwert QPWDLMTREP von 0 in 2 geändert
- Systemwert QPWDRQDDGT von 0 in 1 geändert
- Systemwert QPWDRQDDIF von 0 in 1 geändert
- Systemwert QPWDCHGBLK von *NONE in 0000000003 geändert

9.14.2
Seite 2

- Systemwert QPWDEXPWRN von 7 in 14 geändert
- Benutzerprofil QSYSOPR geändert
- Benutzerprofil QPGMR geändert
- Benutzerprofil QUSER geändert
- Benutzerprofil QSRV geändert
- Benutzerprofil QSRVBAS geändert

9.14.3 Allgemeine Objektberechtigung entziehen

Dieser Befehl schränkt die Verwendung von Befehlen und Programmen ein, indem er die allgemeine Berechtigung in *EXCLUDE ändert. Führen Sie den Befehl nur aus, wenn bekannt ist, für welche Befehle und Programme er die allgemeine Berechtigung festlegt.

Um festzustellen, welche Befehls- und Programmberechtigungen geändert werden, setzen Sie den Befehl RTVCLSRC (CL-Quelle abrufen) für das Programm QSECRVKP ab und prüfen die erstellte Quellendatei.

Ein Blick ins Programm zeigt, was an Rechten geändert wird:

```
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDAJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDCFGLE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDCMNE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDCFGLE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDCMNE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGAJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGCFGLE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGCMNE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ADDWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
```

9.14.3
Seite 2

```
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGCTLAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGDEVAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGCTLAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGDEVAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
+
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGSBSD) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CPYCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTCTLAPPC) OBJTYPE(*CMD) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGSBSD) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CHGWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CPYCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTCTLAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTDEVAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTSBSD) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ENDRMTSPT) OBJTYPE(*CMD) -
```

```
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVAJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVCFGLE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTDEVAPPC) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/CRTSBSD) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/ENDRMTSPT) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVAJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVCFGLE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVCMNE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVCMNE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVJOBQE) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVPJE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVRTGE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RMVWSE) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTLIB) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTOBJ) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36F) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36FLR) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36LIBM) OBJTYPE(*CMD) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTLIB) OBJTYPE(*CMD) USER(*PUBLIC) -
```

9.14.3
Seite 4

```
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTOBJ) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36F) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36FLR) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/RSTS36LIBM) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRRMTSPT) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRSBS) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRSBS) OBJTYPE(*CMD) USER(QPGMR) -
AUT(*USE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/WRKCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QTIENDSUP) OBJTYPE(*PGM) USER(*PUBLIC) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRRMTSPT) OBJTYPE(*CMD) -
USER(*PUBLIC) AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRSBS) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/STRSBS) OBJTYPE(*CMD) USER(QPGMR) -
AUT(*USE)
QSYS/GRTOBJAUT OBJ(&LIBRARY/WRKCFGL) OBJTYPE(*CMD) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QTIENDSUP) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QTISTRSUP) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QWTCTLTR) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QWTSETTR) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QY2FTML) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/CALL PGM(QSYS/QSYRTVUA) PARM(&RCVVAR X'0000023C' &RTNREC -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QTISTRSUP) OBJTYPE(*PGM) USER(*PUBLIC)
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QWTCTLTR) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QWTSETTR) OBJTYPE(*PGM) USER(*PUBLIC) -
AUT(*EXCLUDE)
QSYS/GRTOBJAUT OBJ(QSYS/QY2FTML) OBJTYPE(*PGM) USER(*PUBLIC) -
```

```
AUT(*EXCLUDE)
QSYS/CALL PGM(QSYS/QSYRTVUA) PARM(&RCVVAR X'0000023C' &RTNREC -
X'00000037' 'RTUA0100' '/' X'00000001' &ERRCOD)
QSYS/IF COND(%SST(&RCVVAR 12 8) ¬= '*EXCLUDE') THEN(DO)
QSYS/CHGAUT OBJ(/) USER(*PUBLIC) DTAAUT(*RX) OBJAUT(*NONE)
```

9.14.3
Seite 6

9.14.4 Objektintegrität prüfen

Mit dem Befehl CHKOBJITG (Objektintegrität prüfen) werden die Objekte des angegebenen Benutzerprofils, die Objekte, die mit dem angegeben Pfadnamen übereinstimmen, oder alle Objekte des Systems überprüft, um festzustellen, ob eine Integritätsverletzung an einem Objekt aufgetreten ist. Eine Integritätsverletzung tritt unter folgenden Bedingungen auf:

- Ein Befehl wurde geändert.
- Ein Objekt hat eine digitale Signatur, die ungültig ist.
- Ein Objekt hat ein falsches Domänenattribut für seine Objektart.
- Ein Programm- oder Modulobjekt wurde geändert.
- Die Attribute einer Bibliothek wurden geändert.
- Bei der Dateisystemprüfung wurde in einem Objekt ein Fehler festgestellt.

Kam es zu einer Integritätsverletzung, werden der Objektname, der Bibliotheks- oder Pfadname, die Objektart, der Objekteigner und die Fehlerart in einer Datenbankdatei protokolliert.

Folgende Arten von Integritätsverletzungen können auftreten:

- ALTERED – Das Objekt wurde geändert.
- BADSIG – Das Objekt hat eine digitale Signatur, die ungültig ist.
- DMN – Die Domäne ist für die Objektart nicht korrekt.
- PGMMOD – Das ausführbare Objekt wurde geändert.
- BADLIBUPDA – Das Attribut für Bibliothekszugriffsschutz ist falsch gesetzt.
- SCANFSFAIL – Das Objekt wurde von einem prüfungsbezogenen Exitprogramm geprüft, und bei der letzten Prüfanforderung wurde ein Fehler bei dem Objekt festgestellt.

Wenn eine Verletzung für ein LIC-Modul protokolliert wird, besteht der Objektname aus einem acht Zeichen umfassenden RU-Namen, wobei der RU-Name ein ersetzbarer Einheitenname des LIC-Moduls, der Bibliotheksname leer und die Objektart *LIC ist. Wenn eine derartige Verletzung auftritt, sollte der IBM-Ansprechpartner benachrichtigt werden.

Es werden neben den Integritätsverletzungen auch solche Objekte in der Datenbankdatei protokolliert, die keine digitale Signatur haben, aber signiert sein können, Objekte, die nicht überprüft werden können, und Objekte, deren Format verändert werden muss, damit sie auf der vorliegenden Maschinenimplementierung verwendet werden können.

9.14.4
Seite 2

Folgende Arten von Integritätsverletzungen können auftreten:

- NOSIG – Das Objekt kann signiert werden, hat aber keine digitale Signatur.
- NOTCHECKED – Das Objekt kann nicht überprüft werden, da es sich im Debug-Modus befindet, mit geleertem Speicher gesichert oder komprimiert ist.
- NOTTRANS – Das Objekt wurde nicht in das aktuelle Format umgesetzt oder ist nicht mit dem aktuellen Releasestand kompatibel.

Anmerkung:

Objekte, die komprimiert oder beschädigt sind, mit leerem Speicher gesichert sind oder sich im Debug-Modus befinden, können nicht überprüft werden.

Anmerkung:

IBM-Befehle, die von einem Release vor V5R2 dupliziert wurden, werden als Verletzungen der Art ALTERED protokolliert. Diese Befehle sollten jedes Mal, wenn ein neues Release geladen wird, gelöscht und mit dem Befehl CRTDUPOBJ (Doppeltes Objekt erstellen) neu erstellt werden.

Einschränkungen:

Für die Prüfung der Objektintegrität ist die Sonderberechtigung für Protokollierung *AUDIT erforderlich.

Hinweis:

Der Befehl CHKOBJITG läuft möglicherweise aus folgenden Gründen sehr lange:

- Das für den Parameter USRPRF angegebene Benutzerprofil besitzt viele Objekte.
- *ALL ist für den Parameter USRPRF angegeben.
- *SYSTEM ist für den Parameter OBJ angegeben.
- Viele Objekte stimmen mit dem Muster des Pfadnamens, das im Parameter OBJ angegeben ist, überein.

9.15 Zeilen und Spaltenberechtigungen (RCAC)

Sie alle kennen die Rechtevergabe auf einzelne Objekte des IBM i-Servers. Objektberechtigungen gibt es schon genauso lange wie es die AS/400 gibt. Allerdings können wir mit Mitteln des Betriebssystems nur die Rechte auf das Objekt insgesamt erteilen oder entziehen. Man kann also sagen: Mit Objektberechtigungen kann zwar der Zugriff auf das Objekt mit seinen Daten eingeschränkt werden, nicht aber auf Datenbereiche.

Nun gibt es aber Szenarien, in denen der Zugriff genauer gesteuert werden muss, als dies durch einfaches Gewähren, Widerrufen oder Ablehnen von Berechtigungen für Daten möglich ist. Nehmen wir das beliebte Beispiel der Personalabteilungen. Vielleicht dürfen nicht alle Mitarbeiter der Personalabteilung alle Informationen eines jeweiligen Mitarbeiters lesen. Bisher wurde dieses Problem in erster Linie über entsprechende Prüfungen im Programmcode eingeschränkt. Sobald aber der Zugriff auf die Daten über ein anderes Interface (SQL, IBM i Navigator, ODBC, JDBC, QUERY/400) erfolgt, sind die Daten ungeschützt. Natürlich ist es möglich, die sensiblen Daten in einer eigenständigen Datei zu speichern, aber dadurch wird der Datenzugriff unnötig kompliziert und auch das Datenbankdesign wird unübersichtlicher. Die Personalabteilung ist stets das Paradebeispiel, das genannt wird, um die Problematik zu verdeutlichen, aber es gibt auch andere Beispiele:

Vertriebsmitarbeiter sollen lediglich auf die ihnen zugeordneten Kunden zugreifen und auch nur ihre eigenen Daten auswerten dürfen. Mandantenfähigkeit musste bislang häufig über separate Bibliotheken realisiert werden, um sicherzustellen, dass Mitarbeiter nicht firmenübergreifend Informationen abrufen können. Wenn Sie ein klein wenig überlegen, fallen Ihnen sicherlich viele weitere Beispiele ein.

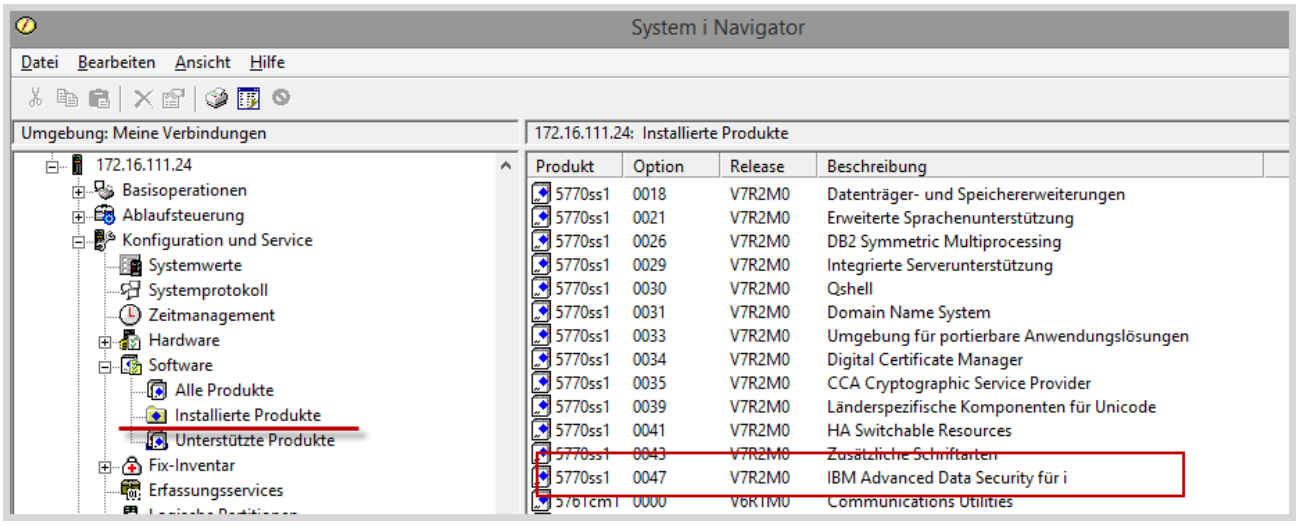
Die oben geschilderten Szenarien können mit Release i7.2 jetzt gelöst werden. Denn im Release i7.2 ist es möglich, Zeilen- und Spaltenberechtigungen für Tabellen zu vergeben. Selbst Benutzer mit der Sonderberechtigung *ALLOBJ können diese Berechtigungen nicht unterlaufen und sehen nur noch die für sie explizit berechtigten Zeilen und Spalten. Diese neuen Berechtigungen werden unter dem Oberbegriff Row and Column Access (RCAC) zusammengefasst.

9.15
Seite 2

9.15.1 Zeilen-/Spaltenberechtigungen (RCAC) – Voraussetzungen

Bevor Sie allerdings mit den neuen Berechtigungsbefehlen arbeiten können, müssen ein paar Voraussetzungen erfüllt sein:

1. Achten Sie darauf, dass Option 47 – IBM Advanced Data Security for i – auf dem Server installiert ist:

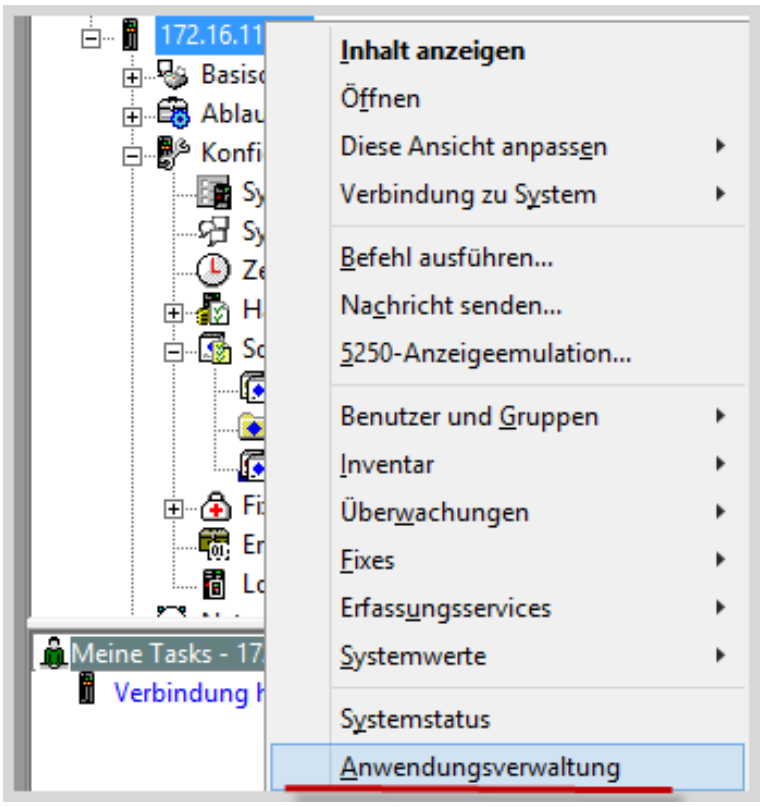


9.15.1
Seite 2

2. Alle Benutzer, die Zeilen- und Objektberechtigungen vergeben sollen, müssen dafür explizit in der Anwendungsverwaltung registriert werden. Die Sonderberechtigungen *SECADM und *ALLOBJ reichen dieses Mal als Legitimierung nicht aus.

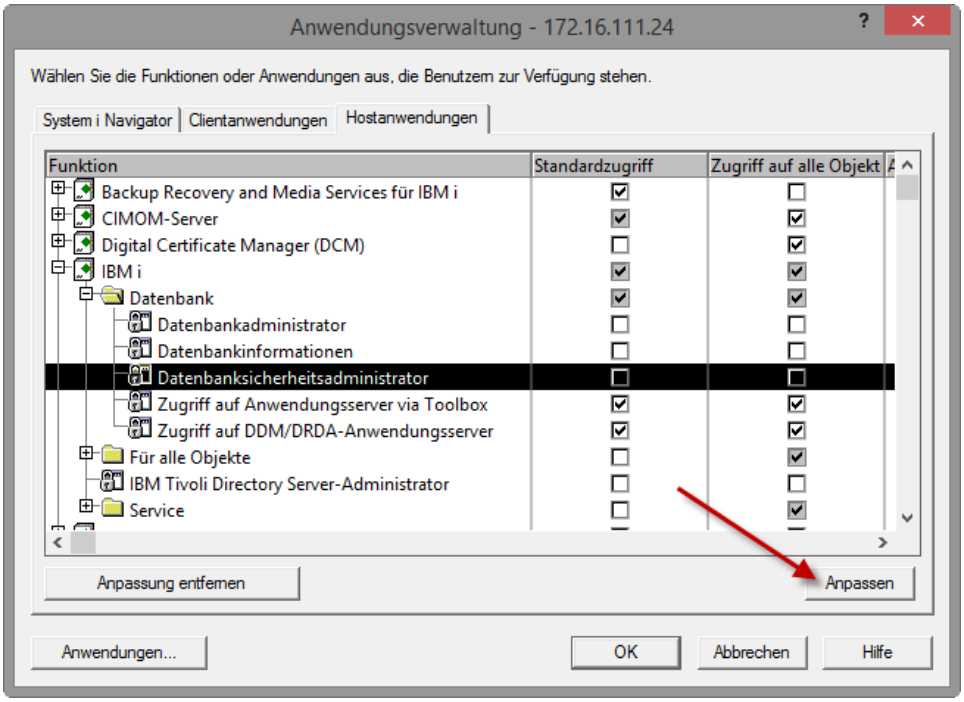
   Um die Registrierung vorzunehmen, haben Sie zwei Möglichkeiten:

   a) Im IBM i System Navigator
   Dafür öffnen Sie das Kontextmenü der Serververbindung und wählen den Menüpunkt „Anwendungsverwaltung“ – wie in der nachfolgenden Abbildung gezeigt:



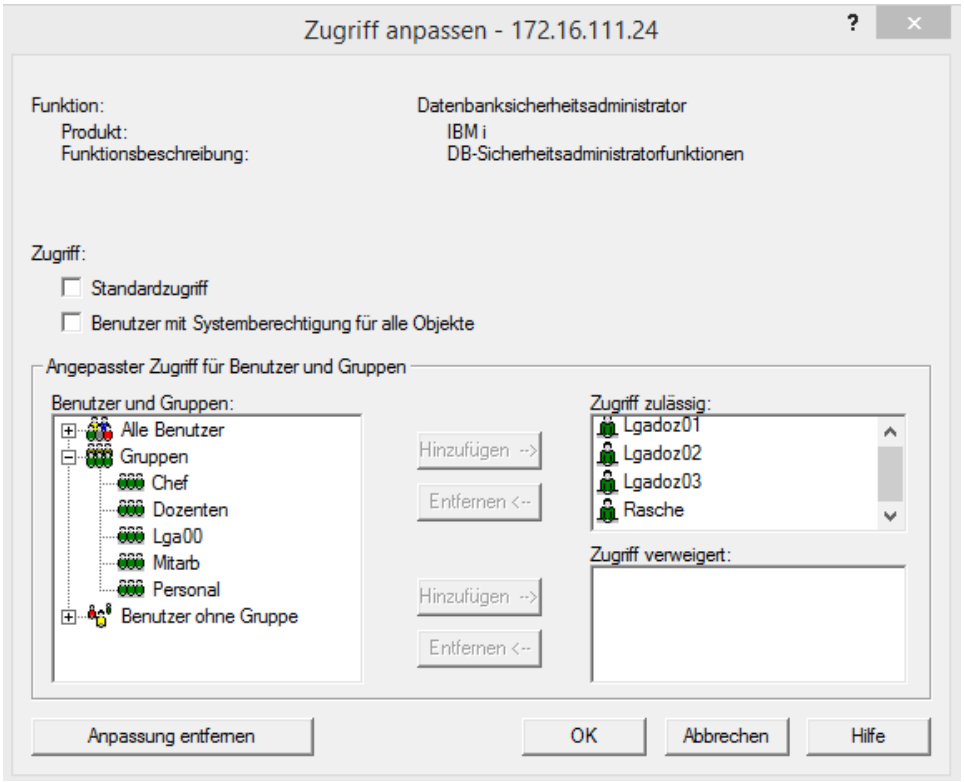
Anwendungsverwaltung öffnen

Nachdem Sie sich ggf. auf dem zentralen System angemeldet haben, wählen Sie im Dialog den Eintrag „Hostanwendungen“. Markieren Sie dort den Eintrag „Datenbanksicherheitsadministrator“:



Anwendungsverwaltung – Hostanwendungen

Klicken Sie anschließend auf den Button „Anpassen“. Nun folgt ein weiterer Dialog, der Ihnen die Auswahl von Gruppenprofilen oder einzelnen Benutzerprofilen ermöglicht:



Anwendungsverwaltung – Zugriff anpassen

Alle Benutzergruppen oder Benutzerprofile, die Sie hier auswählen, dürfen anschließend mit den neuen Berechtigungsbefehlen arbeiten.

Alternativ können Sie diese Berechtigungen natürlich auch mit entsprechenden CL-Befehlen erteilen:

```
                          Work with Function Usage

Type options, press Enter.
  2=Change usage   5=Display usage

Opt  Function ID                    Function Name
     QIBM_DIRSRV_ADMIN              IBM Tivoli Directory Server Administrator
     QIBM_ACCESS_ALLOBJ_JOBLOG      Access job log of *ALLOBJ job
     QIBM_ALLOBJ_TRACE_ANY_USER     Trace any user
     QIBM_WATCH_ANY_JOB             Watch any job
     QIBM_DB_DDMDRDA                DDM & DRDA Application Server Access
     QIBM_DB_SECADM                 Database Security Administrator
     QIBM_DB_SQLADM                 Database Administrator
```

Mit Funktionsnutzung arbeiten – WRKFCNUSG

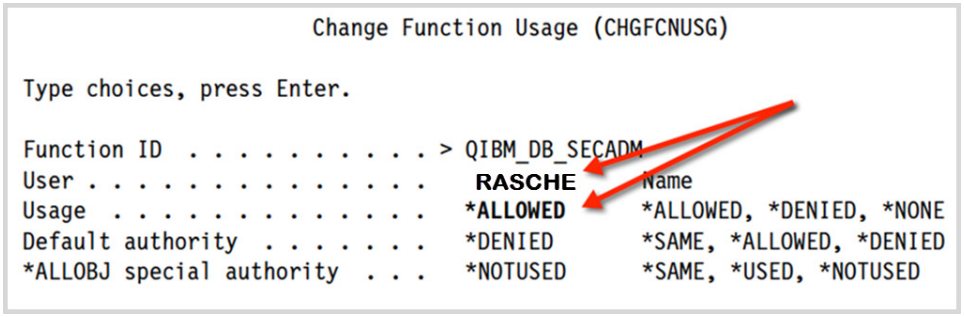
Mit Option 5 können Sie sich die aktuellen Einstellungen anzeigen lassen (DSPFCNUSG):

```
                          Display Function Usage

 Function ID  . . . . . :   QIBM_DB_SECADM
 Function name  . . . . . :   Database Security Administrator

 Description  . . . . . :   Database Security Administrator Functions


 Product  . . . . . :   QIBM_BASE_OPERATING_SYSTEM
 Group  . . . . . :   QIBM_DB

 Default authority  . . . . . :   *DENIED
 *ALLOBJ special authority  . . . . . :   *NOTUSED

 User        Type          Usage       User        Type          Usage
 DEVELOPER1  User          *DENIED
 DEVELOPER2  User          *DENIED
```

Funktionsnutzung anzeigen – DSPFCNUSG

In der Abbildung oben können Sie auch erkennen, warum die *ALLOBJ-Berechtigung nicht ausreicht, um die neuen Berechtigungsbefehle zu verwenden.

Wählen Sie die Option 2 im Ausgangsbildschirm „Mit Funktionsnutzung arbeiten (WRKFCNUSG)“ oder den Befehl CHGFCNUSG, so können Sie anschließend entsprechende Änderungen vornehmen:



Funktionsnutzung ändern – CHGFCNUSG

9.15.1
Seite 6

9.15.2 Zeilenberechtigung erteilen

Sind die Voraussetzungen erfüllt, können Zeilenberechtigungen mit dem SQL-Befehl

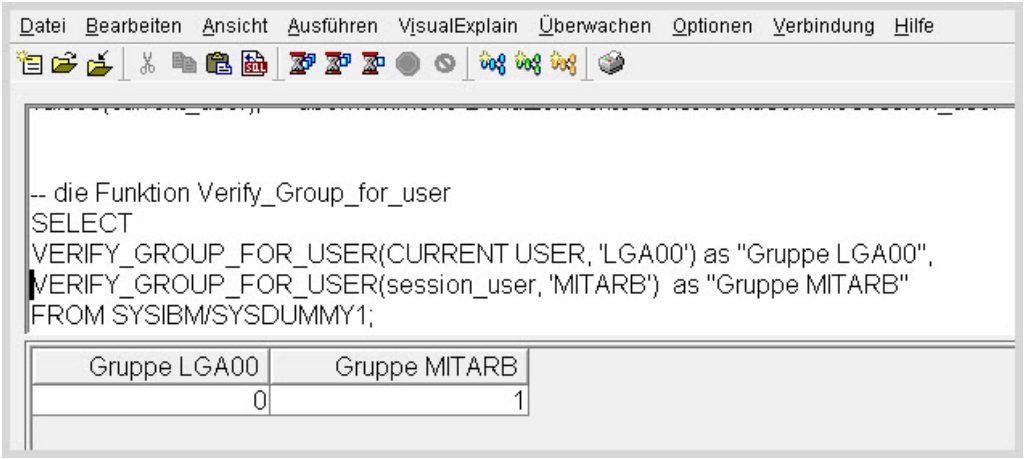
```
CREATE OR REPLACE PERMISSION
```

erteilt werden. Erfreulich ist, dass IBM für diesen Erstellungsbefehl sofort die REPLACE-Option integriert hat. Dies erspart uns bei Änderungen den Befehl DROP PERMISSION.

Für die Erteilung der Berechtigungen benötigen wir spezielle Register. Sie erinnern sich an deren Bedeutung?

Register	Bedeutung
USER oder SESSION_USER	Beinhaltet den Namen des aktuellen Benutzerprofils, welches den Thread anfordert.
SYSTEM_USER	Beinhaltet den Namen des Benutzerprofils, welches die Verbindung aufgebaut hat (häufig QUSER).
CURRENT USER oder CURRENT_USER	Beinhaltet gewöhnlich – wie das Register USER – den aktuellen Benutzer, der die Thread-Anforderung ausgelöst hat. Nur wenn es sich um Programme oder Umgebungen mit übernommenen Benutzerrechten (adopted authority) handelt, enthält das Register den Benutzerprofilnamen, von dem die Rechte übernommen wurden.

Außerdem benötigen wir gleich die skalare Funktion VERIFY_GROUP_FOR_USER. Diese Funktion prüft, ob das aktuelle Benutzerprofil Mitglied einer bestimmten Benutzergruppe ist:



Wirkungsweise der Funktion VERIFY_GROUP_FOR_USER

9.15.2
Seite 2

In der Abbildung oben können Sie erkennen, dass die Funktion den Wert 1 liefert, wenn die Bedingung wahr ist. Im Übrigen ist es mit der Funktion natürlich auch möglich, einfach den Namen eines Benutzerprofils zu prüfen:

```
SELECT

VERIFY_GROUP_FOR_USER(session_user, 'RASCHE') as "Gruppe MITARB"

FROM SYSIBM/SYSDUMMY1;
```

Auch diese Abfrage gibt den Wert 1 zurück, obwohl das Profil RASCHE kein Gruppenprofil ist. Und Sie können auch mehr als einen Profilnamen als Vergleichswert verwenden:

```
SELECT

VERIFY_GROUP_FOR_USER(session_user, 'LGA00', 'RASCHE') as "Gruppe MITARB"

FROM SYSIBM/SYSDUMMY1;
```

Der aktuelle Benutzer muss entweder mit dem Profil RASCHE angemeldet sein oder zur Gruppe LGA00 gehören.

Nun haben wir auch SQL-seitig die Voraussetzungen geklärt und können entsprechende Zeilenberechtigungen mit dem Befehl CREATE PERMISSION aufbauen. Stellen Sie sich dafür das folgende Szenario vor:

Es gibt zwei Gruppenprofile:

- MITARB beinhaltet alle Mitarbeiter der Firma
- PERSONAL enthält die Mitarbeiter der Personalabteilung

Und es gibt natürlich die Tabelle PERSONAL – unter anderem mit folgenden Informationen:

PERSONALNU...	VORNAME	NACHNAME	MONATSGEHALT	BANKVERBINDUNGIB...
000010	CHRISTINE	HAAS	5078.00	BRLADE21
000020	MICHAEL	MAYER	14000.00	BRLADE21
000030	SALLY	KWAN-CHANG	12800.00	BRLADE21
000050	JOHN	MEYER LUDWIG	11050.00	BRLADE21
000060	IRVING	STERN	10000.00	BRLADE21
000070	EVA	PULASKI	11200.00	BRLADE21
000090	EILEEN	HENDERSON	8900.00	BRLADE21

Die Tabelle PERSONAL

```
CREATE OR REPLACE PERMISSION

ZEILENZUGRIFF_PERSONALDATEN                                          1

ON PERSONAL                                                          2
FOR ROWS WHERE
  (VERIFY_GROUP_FOR_USER(SESSION_USER, 'MITARB') = 1                 3
  AND UPPER(NACHNAME) = SESSION_USER)
OR
  (VERIFY_GROUP_FOR_USER(SESSION_USER, 'PERSONAL') = 1)              4
ENFORCED FOR ALL ACCESS                                              5
ENABLE ; -- Deaktivierung DISABLE                                    6
```

Schauen wir uns das Statement etwas genauer an:

1. Nach dem eigentlichen Befehl erfolgt ein beliebiger Name, das heißt, die Berechtigung wird benannt. Dies erleichtert später die Identifizierung der diversen Berechtigungen.
2. Anschließend wird die Tabelle benannt.
3. Und schließlich folgt die eigentliche Bedingung. Im Beispiel muss der jeweilige Benutzer zur Gruppe MITARB gehören und die anzuzeigenden Datensätze müssen dem Namen des Benutzers entsprechen, das heißt, jeder Mitarbeiter darf seinen eigenen Personalstammsatz sehen, aber nicht den der Kollegen.
4. In der zweiten Bedingung bestimmen wir, dass alle Personen, die zur Gruppe Personal gehören, Zugriff auf alle Tabellenzeilen haben.
5. Diese Regeln gelten für die gesamte Tabelle und alle Tabellenzeilen und sollen aktiviert werden.
6. Um die Regeln jetzt endgültig zu implementieren, müssen wir noch die Tabelle aktualisieren:

```
ALTER TABLE PERSONAL ACTIVATE ROW ACCESS CONTROL;

ALTER TABLE PERSONAL DEACTIVATE ROW ACCESS CONTROL;
```

Anschließend greifen die Zeilenberechtigungen. Ein An- oder Abmelden der Benutzer ist dafür nicht erforderlich:

PERSONALNU...	VORNAME	NACHNAME	MONATSGE...	BANKVERBI...	KONTOVE...
000010	CHRISTINE	HAAS	5078.00	BRLADE21	...
000020	MICHAEL	MAYER	14000.00	BRLADE21	...
000030	SALLY	KWAN-CHANG	12800.00	BRLADE21	...
000050	JOHN	MEYER LUDWIG	11050.00	BRLADE21	...
000060	IRVING	STERN	10000.00	BRLADE21	...
000070	EVA	PULASKI	11200.00	BRLADE21	...
000090	EILEEN	HENDERSON	8900.00	BRLADE21	...
000100	THEODORE	SPENSER	20000.00	BRLADE21	...
000110	VINCENZO	LUCCHESSI	3500.00	BRLADE21	...

Anzeige für Mitarbeiter der Personalabteilung

PERSONALNU...	VORNAME	NACHNAME	MONATSGE...	BANKVERBINDUNGIB...	KONTOVERBINDUNG...
993400	Carmen	Rasche	3500.00	BRLADE21	DE000000000

Anzeige für einfache Mitarbeiter

Diese Einschränkungen lassen sich nicht umgehen, auch dann nicht, wenn die Tabelle nativ im RPG-Programm verarbeitet wird oder Sie über eine SQL-View auf die Daten zugreifen. Der Zeilenschutz ist immer wirksam.

Schauen wir uns ein zweites Beispiel an:

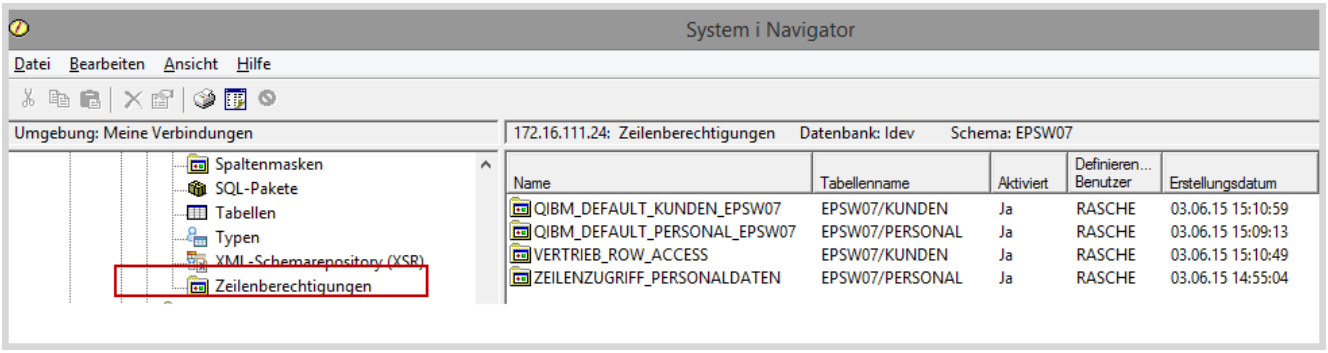
Wir wollen sicherstellen, dass die Vertriebsmitarbeiter nur auf die eigenen Kunden zugreifen können. Dazu erteilen wir die entsprechende Zeilenberechtigung für die Tabelle KUNDEN:

```
CREATE OR REPLACE PERMISSION
VERTRIEB_ROW_ACCESS
ON KUNDEN
FOR ROWS WHERE
VERIFY_GROUP_FOR_USER(SESSION_USER, 'MITARB') = 1
AND KUNDEN_GEBIET =
                        (SELECT VERKAUFSGEBIET
                         FROM VERTRIEBSMITARBEITER
                         JOIN PERSONAL USING(PERSONALNUMMER)
                   WHERE UPPER(NACHNAME) = SESSION_USER)
OR
VERIFY_GROUP_FOR_USER(SESSION_USER, 'CHEF') = 1
ENFORCED FOR ALL ACCESS
ENABLE;
```

Dieses Mal ist die Bedingung sehr viel komplexer aufgebaut. Es wird geprüft, ob das beim Kunden hinterlegte Gebiet dem zugeordneten Verkaufsgebiet des Verkäufers entspricht. Zu diesem Zweck müssen die Tabellen VERTRIEBS-MITARBEITER und PERSONAL verknüpft werden, da das Verkaufsgebiet und der Name des Mitarbeiters in unterschiedlichen Tabellen gespeichert sind.

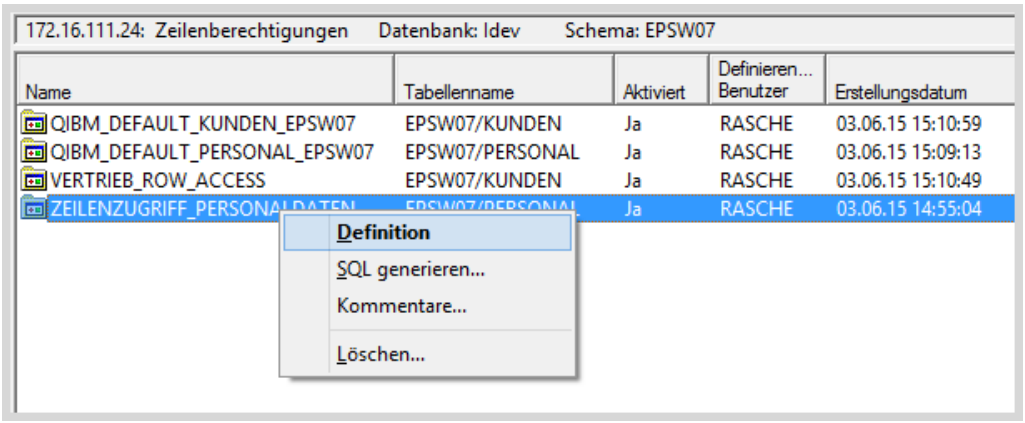
9.15.3 Zeilenberechtigungen anzeigen

Welche Zeilenberechtigungen erteilt sind und ob diese aktiviert oder deaktiviert sind, können Sie sehr schnell im IBM i Navigator überprüfen. Öffnen Sie hierfür die „DATENBANK“ und das Schema mit den betroffenen Tabellen:



Zeilenberechtigungen anzeigen

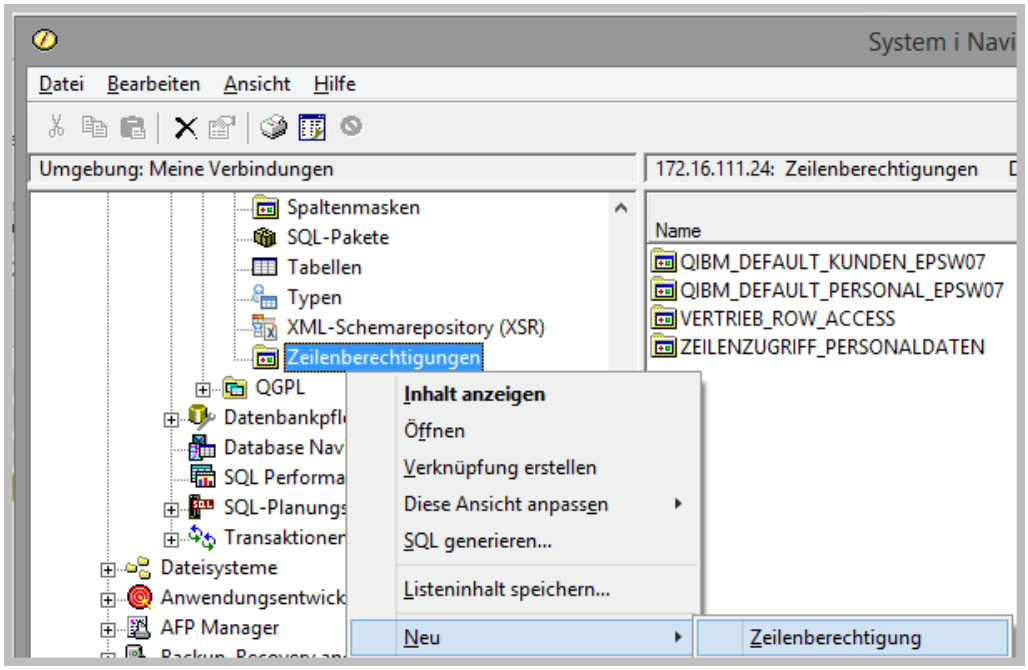
Von hier aus ist es sehr einfach möglich, Berechtigungen zu löschen, das zugehörige SQL-Statement zu generieren oder die Definition anzuzeigen:



Zeilenberechtigungen bearbeiten

9.15.3
Seite 2

Und wenn Sie sich das Kontextmenü der ZEILENBERECHTIGUNGEN ansehen, werden Sie feststellen, dass Sie die Zeilenberechtigungen auch problemlos über die grafische Oberfläche erstellen können:



Zeilenberechtigungen mit dem Navigator erstellen (1)

Zeilenberechtigungen mit dem Navigator erstellen (2)

9.15.4 Spaltenberechtigungen erstellen

Sie können aber nicht nur Berechtigungen für die Zeilen einer Tabelle erteilen, sondern auch die Anzeige von einzelnen Spalten steuern. Mit dem neuen SQL-Befehl CREATE OR REPLACE MASK können Spalteninhalte maskiert werden. Auf diesem Weg können sensible Daten durch die hinterlegten Regeln unsichtbar gemacht werden.

Um die Wirkung wiederum anhand der Gehaltsspalte der Tabelle PERSONAL zu demonstrieren, deaktiviere ich zunächst die zuvor hinterlegte Zeilenberechtigung:

```
ALTER TABLE PERSONAL DEACTIVATE ROW ACCESS CONTROL;
```

```
CREATE OR REPLACE MASK GEHALTS_MASKE
ON PERSONAL
FOR COLUMN MONATSGEHALT
RETURN
CASE WHEN UPPER(NACHNAME) = SESSION_USER
       THEN MONATSGEHALT
       WHEN VERIFY_GROUP_FOR_USER(SESSION_USER, 'PERSONAL' ) = 1
       THEN MONATSGEHALT
ELSE 0
END
ENABLE;
```

Wie zuvor vergeben wir zunächst wieder einen Namen für die Spaltenberechtigung und bestimmen die Tabelle. Danach geben wir bekannt, für welche Spalte die Berechtigung gesetzt werden soll. In meinem Beispiel verwende ich wieder die Spalte Monatsgehalt.

Mit der Klausel RETURN legen wir fest, wie der Inhalt der Spalte MONATSGEHALT dargestellt werden soll. Hierbei ist die Anweisung CASE behilflich. Der einzelne Mitarbeiter darf sein eigenes Gehalt sehen, allerdings nicht die Gehälter der Kollegen. Die Mitarbeiter der Personalabteilung erhalten Zugriff auf die Gehälter aller Mitarbeiter, und alle anderen Benutzer sehen anstelle des Gehalts den Wert 0.

Damit die Regel implementiert wird, müssen wir auch dieses Mal wieder den ALTER TABLE-Befehl verwenden. Achten Sie darauf, dass Sie jetzt COLUMN ACCESS aktivieren und nicht wie zuvor ROW ACCESS CONTROL:

```
ALTER TABLE PERSONAL ACTIVATE COLUMN ACCESS CONTROL;;
```

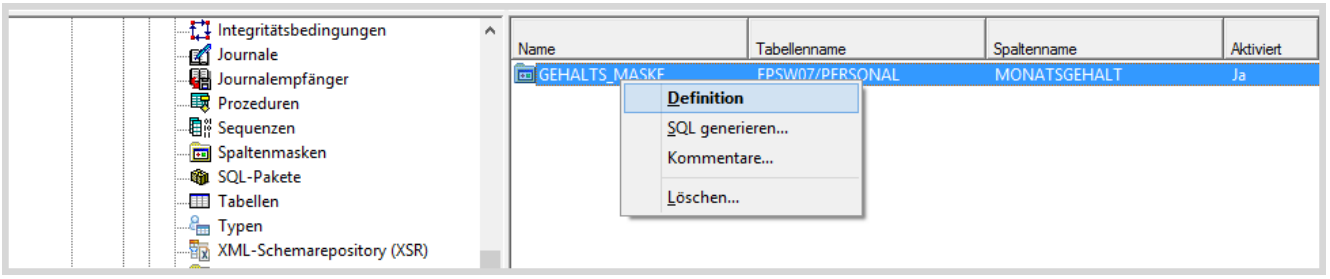
9.15.4
Seite 2

Bevor oder spätestens kurz nachdem Sie die Spaltenberechtigungen aktiviert haben, müssen Sie außerdem noch die Funktionen (UDF) und Trigger, die auf die jetzt maskierten Spalten zugreifen, neu erstellen und das Schlüsselwort SECURED oder NOT SECURED als Eigenschaft hinzufügen:

```
CREATE FUNCTION xxxxx (
                 INDAT DECIMAL(8, 0)
                 )

       RETURNS DATE
       LANGUAGE SQL
       SPECIFIC xxxxxx
       NOT DETERMINISTIC
       READS SQL DATA
       CALLED ON NULL INPUT

       SECURED -- NOT SECURED

       SET OPTION
```

9.15.5 Spaltenberechtigungen anzeigen

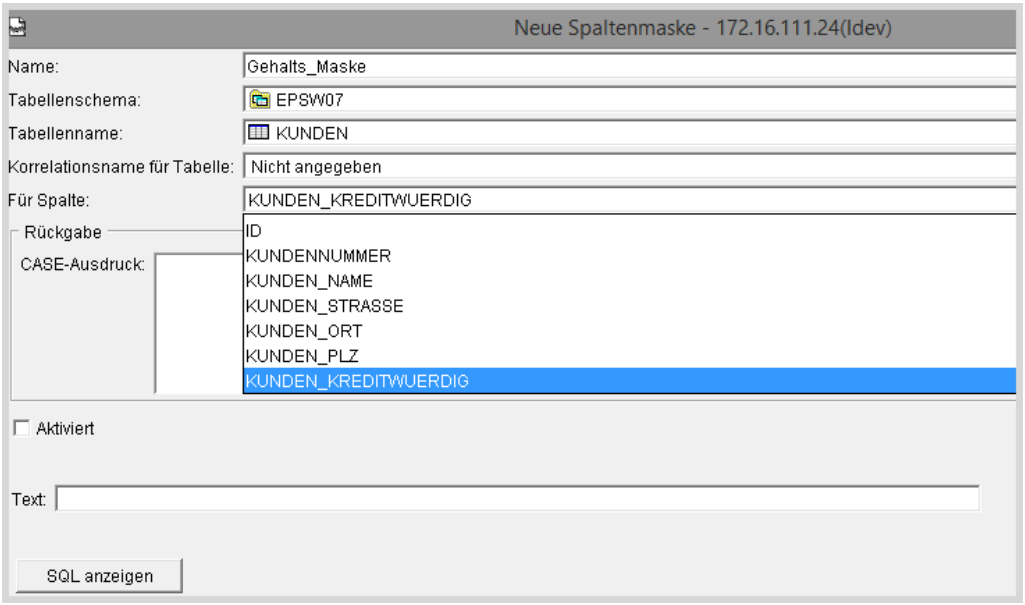
Welche Spaltenberechtigungen erteilt sind und ob diese aktiviert oder deaktiviert sind, können Sie wieder sehr schnell im IBM i Navigator überprüfen. Öffnen Sie hierfür die „DATENBANK“ und das Schema mit den betroffenen Tabellen:



Spaltenberechtigungen anzeigen

Ebenso wie bei den Zeilenberechtigungen können Sie die bestehenden Spaltenmasken löschen, das zugehörige SQL-Statement generieren oder die Definition anzeigen.

Und wenn Sie sich das Kontextmenü der Spaltenmasken ansehen, werden Sie feststellen, dass Sie die Spaltenmasken auch problemlos über die grafische Oberfläche erstellen können:



Spaltenberechtigungen im Navigator erstellen

Im grafischen Interface werden Sie dabei gut unterstützt, etwa indem die Spalten der ausgewählten Tabelle angezeigt werden.

9.15.5
Seite 2

9.15.6 Beschränkungen und Fallen beim Einsatz von RCAC

Um sicherzustellen, dass die Row and Column Access Control (RCAC) bei jedem Zugriff auf Datenbankobjekte und damit auch auf die Daten aktiviert wird, werden die Row-Permissions (Zeilenberechtigungen) und Column-Masks (Spaltenmasken) direkt in die physischen Dateien/SQL-Tabellen integriert und vorrangig bearbeitet. Der eigentliche Datenzugriff – unabhängig davon, welche Methode für den Zugriff verwendet wird (native I/O, SQL, Query/400, JDBC etc.) – erfolgt auf die durch die RCAC-Zugriffsberechtigungen vorselektierten und ggf. maskierten Daten.

RCAC-Zugriffskontrolle kann jedoch nur dann verwendet werden, wenn die Datenzugriffe mit Hilfe der SQL Query Engine (SQE) erfolgen.

Für SQL-Zugriffe ist das soweit klar, aber was, wenn die Zugriffe mit Methoden erfolgen, bei denen kein SQL im Spiel ist, etwa mit native I/O, Query/400 oder UPDDTA?

Damit die RCAC-Berechtigung auch für Nicht-SQL-Zugriffe verwendet werden kann, werden seit Einführung von Release 7.2 alle Zugriffe auf die Datenbankdaten per Default mit der SQE ausgeführt.

Es gibt jedoch einige wenige Datenbankobjekte, zum Beispiel multiformatlogische Dateien, auf die (aktuell) nicht mit der SQE zugegriffen werden kann. Folglich ist der Einsatz von RCAC-Zugriffsberechtigungen in diesen Fällen nicht möglich.

Im Klartext bedeutet die Verwendung der SQE in Verbindung mit RCAC-Zugriffsberechtigungen auch für Nicht-SQL-Zugriffe, dass die Daten von der SQE vorselektiert bereitgestellt werden. Erst im Anschluss wird die eigentliche Aktion ausgeführt, zum Beispiel die Verarbeitung einer DDS-beschriebenen logischen Datei mit Hilfe des RPG-OpCodes READE.

Da der Query Optimizer, der CQE (Classic Query Engine) und der SQE Optimizer in einigen Bereichen komplett anders arbeiten, kann es insbesondere bei der intensiven Nutzung von QUERY/400 oder OPNQRYF nach dem Umstieg auf Release 7.2 zu Performance-Problemen kommen. Um diesen Problemen entgegenzuwirken, besteht die Möglichkeit, mit Hilfe der Auswahl SQE_NATIVE_ACCESS in der Abfrage-Optionsdatei QAQQINI beispielsweise QUERY/400-Abfragen auch weiterhin von der CQE (Classic Query Engine) auszuführen zu lassen. Diese Lösung sollte allerdings nur als Übergangslösung betrachtet und auch nur so lange eingesetzt werden, bis die Abfragen analysiert und die für die SQE notwendigen Zugriffswege bereitgestellt wurden.

Sofern in einem Job die Option SQE_NATIVE_ACCESS in der Abfrage-Optionsdatei auf *NO gesetzt wurde, kann RCAC nicht eingesetzt werden. Sofern RCAC für Tabellen aktiviert wurde, können die an die CQE zurückgegebenen Abfragen nicht (mehr) ausgeführt werden.

Zudem muss ein besonderes Augenmerk auf die in Programmen und Anwendungen verwendete CL-Befehle geworfen werden. Dies gilt insbesondere für Befehle, über die Daten kopiert oder dupliziert werden, wie z. B. CPYF (Datei kopieren) oder CRTDUPOBJ (doppeltes Objekt erstellen). Aktivierte RCAC kann in diesen Fällen nicht nur zu unerwarteten Ergebnissen, sondern sogar zu Datenverlust führen.

9.15.6.1 Zugriffe, die bei aktivierter RCAC nicht mehr oder anders funktionieren

Distributed Files (verteilte Dateien) sowie programmbeschriebene Dateien können bei aktiver RCAC nicht verarbeitet werden. RCAC kann für solche SQL-Tabellen bzw. physische Dateien problemlos, d. h. ohne Warnung oder Fehlermeldung, implementiert werden.

Die Fehlermeldung CPD43A4 (= Zeilen- oder spaltenbezogene Zugriffsteuerung ist für die Abfrage nicht gültig) erfolgt erst beim Dateizugriff durch eine der folgenden Zugriffsmethoden:

- Verwendung von multiformatlogischen Dateien, wenn auf mehr als ein Format zugegriffen wird.
- Sofern direkt auf die physische Datei/Tabelle, für die RCAC implementiert wurde, zugegriffen wird oder der Zugriff über eine logische Datei mit nur einem Format erfolgt, kann die Verarbeitung auch bei aktivierter RCAC korrekt ausgeführt werden.
- Dabei spielt es keine Rolle, ob für die Tabelle/physische Datei logische Dateien mit mehreren Formaten definiert wurden.
- Zugriff auf Dateien mit ICU 2.6.1 Sortierreihenfolge
- Zugriff auf physische Dateien/Tabellen mit Read-Triggern

Anmerkung:

Vor Einführung der RCAC sollten für multiformatlogische Dateien ICU2-Sortierreihenfolgen und Read-Trigger-Alternativen (zum Beispiel SQL-Views und/oder embedded SQL) ermittelt und implementiert werden.

9.15.6.1

Seite 2

9.15.6.2 Zugriffsmethoden auf Datenbankendaten ohne SQL

Beginnend mit Release V5R2 hat IBM die Query Engine, über die die Datenzugriffe via SQL gesteuert werden, umgeschrieben. Zusätzlich zur klassischen Query Engine (CQE) wurde die SQL Query Engine (SQE) eingeführt. Seit Release V5R2 wurde für den Zugriff über SQL nach und nach mehr Funktionalität von der klassischen Query Engine auf die neue Query Engine übertragen. Mit Release 7.1 war der Übergang von der CQE auf die SQE abgeschlossen.

Datenbankzugriffe erfolgen jedoch nicht nur mittels SQL, es stehen vielmehr noch eine Reihe weiterer Zugriffsmöglichkeiten zur Verfügung. Zu diesen Methoden und Interfaces gehören

- Query/400.
- der Befehl Open Query File (OPNQRYF),
- der Befehl Run Query (RUNQRY),
- das QQQQRY API (Application Programming Interface),
- der Befehl UPDDTA (Daten mit temporärem Programm fortschreiben) und
- native I/O in RPG und COBOL.

Row and Column Access Control (RCAC), die mit Release 7.2 eingeführt wurde und über die der Zugriff auf Datenbankdateien gezielt gesteuert werden kann, wurde nur in die SQE eingebaut.

Da die RCAC-Zugriffsbeschränkungen jedoch nicht nur für SQL-Zugriffe, sondern für jede mögliche Zugriffsmethode gelten müssen, ist es erforderlich, dass die Datenzugriffe über die Nicht-SQL-Interfaces ebenfalls von der SQE ausgeführt werden bzw. dass die zu verarbeitenden Daten von der SQE bereitgestellt werden.

9.15.6.2

Seite 2

9.15.6.3 RCAC mit native I/O

Bei einem nativen I/O-Zugriff gibt der Programmierer den Zugriffsweg (physische/logische Datei oder SQL-Index) vor, mit dessen Hilfe die Daten gelesen werden. Da die Dateien fix (in RPG zum Beispiel in den F-Bestimmungen) angegeben werden, war die Implementierung der zusätzlichen Zugriffskontrolle nicht weiter problematisch.

Sofern Zeilenberechtigungen (Row-Permissions) oder Spaltenmasken (Column Masks) für die physischen Dateien bzw. SQL-Tabellen aktiviert wurden, werden die Daten zunächst gefiltert und nur die selektierten Daten verarbeitet. RCAC wird in Form von WHERE-Bedingungen, die direkt mit den physischen Dateien/Tabellen verlinkt werden implementiert. Der eigentliche Zugriff erfolgt dann auf die vorselektierten Daten. Dabei spielt es keine Rolle, ob der Zugriff direkt auf die Tabelle/physische Datei oder mit Hilfe von logischen Dateien, Views oder SQL-Indices erfolgt.

Vor Aktivierung der RCAC sollte jedoch in Programmen, in denen mit native I/O auf die Daten zugegriffen wird, Folgendes überprüft werden:

- Welche Daten müssen verarbeitet werden?

  Führt die Ausführung des Programms durch einen Benutzer mit eingeschränkten Rechten eventuell zu Datenverlust?

  Beispiel: Zum Monatsabschluss müssen alle Bewegungsdaten, die älter als drei Monate sind, gesichert und im Anschluss gelöscht werden. Wird das Programm von einem Benutzer mit eingeschränkten Zugriffsrechten ausgeführt, kann nur (noch) ein Teil der Daten gesichert und gelöscht werden.
  Dabei wird jedoch weder eine Warnung noch eine Fehlermeldung ausgegeben.

9.15.6.3
Seite 2

- Mit welchen Ausführungsrechten wurden die (Service-)Programme erstellt?

  Hat der Benutzer, sofern das (Service-)Programm mit Benutzerprofil *USER erstellt wurde, Zugriff auf alle Daten, die verarbeitet werden müssen?

  Beispiel: Der Benutzer, der den Monatsabschluss aufruft, hat nur eingeschränkte Zugriffsrechte.
  Daten werden unter Umständen nur noch unvollständig verarbeitet.

  Hat der Benutzer, sofern das (Service-)Programm mit dem Benutzerprofil *OWNER erstellt wurde, Zugriff auf die Daten, für die er berechtigt ist?

  Beispiel: Der Programmierer, der das Programm erstellt, hat zwar Zugriff auf alle Datenbankobjekte, so auch auf den Personalstamm. Er hat jedoch keine Zugriffsberechtigung auf die Personaldaten.
  Daten werden unter Umständen nur noch unvollständig verarbeitet.

  Erhält der Benutzer, sofern das (Service-)Programm mit dem Benutzerprofil OWNER erstellt wurde, Zugriff auf Daten, für die er nicht berechtigt ist?

  Beispiel: Das Benutzerprofil, das Eigner des Programms ist, hat Zugriff auf alle Daten und alle Objekte.
  Die Benutzer, die das Programm in einem mandantenfähigen System ausführen, sind jedoch jeweils nur für bestimmte Mandanten berechtigt.
  Trotz aktivierter RCAC könnten die Benutzer auf Daten zugreifen, für die sie nicht berechtigt sind.

Anmerkung:

Bevor RCAC aktiviert wird, sollte überprüft werden, ob die Benutzer während der Ausführung der (Service-)Programme Zugriff auf alle zu verarbeitenden Daten haben.

Insbesondere die übertragenen Rechte müssen geprüft werden.

9.15.6.4 RCAC und OPNQRYF und Query/400

Methoden wie Query/400 und OPNQRYF funktionieren ähnlich wie SQL, das heißt, ein Optimizer ermittelt, ob und welche Zugriffswege verwendet werden.

Die Entscheidung, ob und welche Zugriffswege verwendet werden, wird jedoch bei den Optimizern der CQE und der SQE auf Basis von unterschiedlichen Regeln getroffen.

Die unterschiedlichen Optimierungsmethoden der beiden Optimizer können dazu führen, dass unterschiedliche Zugriffswege gewählt werden, was zum einen zu einer unterschiedlichen Sortierung der Ergebnisse und zum anderen auch zu Performance-Problemen führen kann.

Um Performance-Problemen vorzubeugen bzw. um zu ermöglichen, dass Query/400 und OPNQRYF so performant wie bisher ausgeführt werden können, wurde die Option SQE_NATIVE_ACCESS in die Abfrage-Optionsdatei QAQQINI eingefügt. Standardmäßig ist diese Option auf *YES gesetzt, das heißt, die Ausführung der Datenbankenzugriffe erfolgt mit Hilfe der SQE.

Wird diese Option auf *NO gesetzt, so werden die nicht nativen Interfaces wie bisher über die CQE ausgeführt.

Anmerkung:

Die Abfrage-Optionsdatei (QAQQINI) kann mittels CRTDUPOBJ (Doppeltes Objekt erstellen) in eine beliebige Bibliothek kopiert und in dieser Bibliothek modifiziert werden.

Mit Hilfe des CL-Befehls CHGQRYA (Abfrageattribute ändern) kann über die Option QRYOPTLIB (Bibliothek für Abfrageoptionsdatei) die (kopierte) Abfrage-Optionsdatei auf Jobebene gesetzt werden.

Sofern allerdings die Option SQE_NATIVE_ACCESS in einem Job auf *NO gesetzt wird, können keine Tabellen/physische Dateien mit aktiver RCAC verarbeitet werden.

Sämtliche Zugriffe auf Tabellen/physische Dateien mit aktiver RCAC werden abgebrochen.

9.15.6.4
Seite 2

Anmerkung:

Vor Implementierung der RCAC sollte man zunächst sicherstellen, dass alle Datenzugriffe unabhängig von der Zugriffsmethode mit Hilfe der SQE performant ausgeführt werden.

Gegebenenfalls müssen an dieser Stelle für die performante Ausführung von Query/400-Abfragen zunächst neue Zugriffswege (vorzugsweise SQL-Indices) angelegt werden.

Programme, die noch OPNQRYF verwenden, müssen/sollten auf embedded SQL umgestellt werden.

9.15.6.5 Kopieren, Duplizieren und (Zurück)Sichern – offene Fragen

Nachdem alle Eventualitäten geklärt sind und alle Datenbankzugriffe performant über die SQE ausgeführt werden können, kann die Implementierung von Zugriffsberechtigungen über RCAC ins Auge gefasst werden.

RCAC-Zugriffsberechtigungen werden in Form von zusätzlichen WHERE-Bedingungen direkt in den Tabellen/physischen Dateien verankert. Beim Zugriff auf die Daten in den zugrundeliegenden Tabellen/physischem Dateien werden diese zusätzlichen WHERE-Bedingungen vorrangig ausgeführt.

Der Benutzer kann somit nur auf die Daten zugreifen, für die er berechtigt ist. Dabei spielt es keine Rolle, ob der Zugriff über native I/O, SQL oder CL-Befehle wie CPYF erfolgt. Die RCAC-Zugriffsberechtigungen greifen, unabhängig davon, ob direkt auf die Tabelle/physische Datei oder indirekt über DDS-beschriebene logische Dateien, SQL-Views oder -Indices auf die Daten zugegriffen wird.

Das Prinzip ist soweit klar, dennoch werfen die Definition und Implementierung der RCAC-Zugriffsberechtigungen noch eine Reihe weiterer Fragen auf:

- Was geschieht beim Schreiben von Daten bzw. beim Übertragen von Daten aus einer Tabelle in eine andere Tabelle bei aktiver RCAC-Zugriffsberechtigung?

  Was passiert, wenn beim Kopieren von Daten für die Ausgangs- und Zieltabellen abweichende RCAC-Zugriffsberechtigungen hinterlegt wurden oder RCAC-Zugriffsberechtigungen lediglich in einer der beiden Tabellen/physischen Dateien implementiert wurden?

- Was geschieht, wenn beim Kopieren zugleich ein neues Objekt oder sogar ein Duplikat des Objekts erzeugt wird, etwa über die Befehle CRTDUPOBJ (Doppeltes Objekt erstellen) bzw. CPYF (Datei kopieren) oder mit dem SQL-Befehl CREATE TABLE in Verbindung mit einem SELECT-Statement?

  Werden alle Datensätze oder nur die Datensätze, für die der Benutzer berechtigt ist, in die neue Tabelle übertragen?

  Werden die RCAC-Berechtigungen aus der Ausgangsdatei auch in der neuen Zieldatei implementiert und aktiviert?

9.15.6.5
Seite 2

- Was geschieht beim Kopieren von Datensätzen, wenn für die Ausgangsdatei RCAC-Spaltenberechtigungen hinterlegt sind und der Benutzer, der die Datensätze kopiert, nicht alle Spalteninhalte sehen darf?

  Werden die Maskenwerte oder die Originalwerte übertragen?

- Was geschieht, wenn ein Datensatz mit native I/O geschrieben oder geändert wird, der Benutzer für bestimmte Spaltenwerte nicht berechtigt ist und folglich auch im Programm, sowie beim Debuggen des Programms lediglich auf die Maskenwerte zugreifen kann?

  Werden in diesem Fall die Originalwerte durch die Maskenwerte überschrieben oder bleiben die Originalwerte unverändert?

  Werden die in der Ausgangsdatei implementierten RCAC-Spaltenberechtigungen auf das neue Objekt übertragen?

- Was geschieht beim Sichern und Zurücksichern von Tabellen/physischen Dateien mit den RCAC-Zugriffsberechtigungen?

  Macht es einen Unterschied, ob die Bibliothek oder das Objekt mit dem gleichen oder einem anderen Namen zurückgesichert wird?

  Was geschieht beim Zurücksichern mit RCAC-Zugriffsberechtigungen, in denen auf andere Datenbankobjekte entweder im gleichen oder in einem anderen Schema zugegriffen wird?

  Was geschieht beim Umbenennen einer Tabelle mit den RCAC-Zugriffsberechtigungen?

9.15.6.5.1 Kopieren von Daten zwischen Tabellen mit RCAC-Zeilenberechtigung

Beim Kopieren oder Übertragen von Datensätzen mit SQL, native I/O oder dem CL-Befehl CPYF (Datei kopieren) kommt es darauf an, welche RCAC-Zugriffsregeln in der Ausgangsdatei implementiert wurden und für welche Datensätze der Anwender berechtigt ist.

Wenn der Benutzer, der die Daten dupliziert, aufgrund der RCAC-Zugriffsberechtigung nur auf einen Teil der Datensätze zugreifen darf, kann er auch nur diese Zeilen auf das neue Objekt übertragen.

Um die Daten in die Zieldatei einfügen zu können, dürfen auf der Zieldatei entweder keine Zugriffsberechtigungen liegen oder die Zugriffsberechtigungen müssen so definiert sein, dass der Anwender für die Daten, die er zu kopieren versucht, auch in der Zieldatei berechtigt ist.

Anmerkungen:

Beim Kopieren von Daten (zum Beispiel mit CPYF) werden nur die Datensätze übertragen, für die der Benutzer berechtigt ist.

9.15.6.5.1

Seite 2

9.15.6.5.1.1 Kopieren aus Tabelle mit RCAC-Zugriffsberechtigung mit Neuanlage der Zieltabelle

Sofern beim Kopieren der Daten gleichzeitig eine neue Tabelle angelegt wird – etwa durch die Option CRTFILE (Datei erstellen) im Befehl CPYF (Datei anlegen) oder durch den SQL-Befehl CREATE TABLE in Verbindung mit einem SELECT-Statement – so wird lediglich die Tabelle/physische Datei generiert.

Die in der Ausgangsdatei implementierten RCAC-Zugriffsberechtigungen werden jedoch nicht übernommen.

Da in der Zieldatei keine RCAC-Zugriffsberechtigungen implementiert werden und um einem unberechtigten Zugriff entgegenzuwirken, werden nur die Datensätze, für die der Benutzer in der Ausgangsdatei berechtigt ist, in die neue Tabelle/physische Datei übertragen.

Beispiel:
Für die Tabelle MYADDRESS wurde eine Row-Permission (Zeilenberechtigung) implementiert, durch die Benutzer HAUSER nur Zugriff auf Adressen in Deutschland im Postleitzahlenbereich zwischen 50000 und 79999 hat. Dadurch kann Benutzer HAUSER in unserem Beispiel lediglich auf fünf Datensätze der Tabelle MYADDRESS zugreifen.

In der Tabelle MYADDRESS sind jedoch insgesamt 72 Datensätze vorhanden.

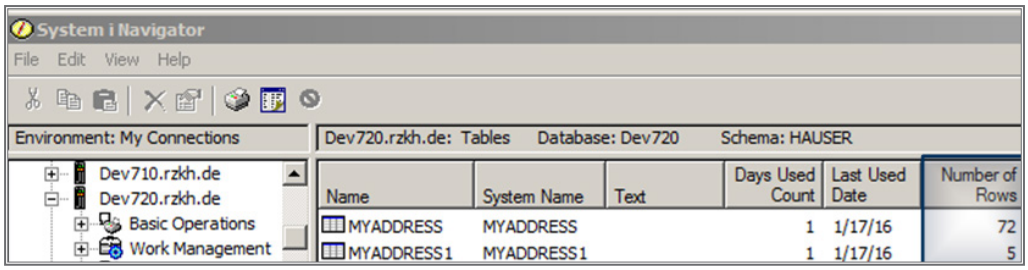
Benutzer HAUSER erstellt nun mit dem folgenden CL-Befehl die Tabelle MYADDRESS1:

```
CPYF    FROMFILE(HAUSER/MYADDRESS)
        TOFILE(HAUSER/MYADDRESS1)
        CRTFILE(*YES)
```

Datensätze aus Tabelle mit RCAC-Zugriffsberechtigung via CPYF in neue Datei kopieren

9.15.6.5.1.1
Seite 2

Da der Benutzer jedoch nur die Zugriffsberechtigung für die fünf Datensätze im Postleitzahlenbereich zwischen 50000 und 79999 hat, werden in die neue Tabelle MYADDRESS1 tatsächlich auch nur diese fünf Datensätze übertragen, wie die folgende Abbildung (Auszug aus IBM i Navigator) zeigt:



IBM i Navigator – Tabelle – Neue Tabelle nach CPYF

So gut und wichtig die RCAC-Kontrolle auch ist, so kann deren Implementierung auch zu Problemen und unerwarteten Ergebnissen bis hin zu Datenverlust führen, wie das folgende Beispiel zeigt.

Beispiel:
Jeweils am Monatsanfang werden alle Datensätze aus der Bewegungsdatei, die älter als drei Monate sind, in eine neue Tabelle übertragen und anschließend gesichert. Nach dem Sichern der kopierten Daten werden die ursprünglichen und jetzt gesicherten Daten aus der Bewegungsdatei entfernt.

Das Programm wird jeweils am Monatsanfang über einen Job-Schedular-Eintrag aktiviert und von Benutzer USER01 ausgeführt.

Nach Implementierung der RCAC-Zugriffsberechtigungen darf der Benutzer USER01 nur noch auf Datensätze von MANDANT01 zugreifen. Da der Benutzer USER01 sich unter anderem auch die Bewegungsdaten anzeigen lassen muss, wurde eine entsprechende Row-Permission (Zeilenberechtigung) auch in der Bewegungsdatei implementiert.

Wird nun das Programm am Monatsanfang durch den Job-Schedular unter dem Benutzerprofil USER01 aktiviert, werden aufgrund der RCAC-Zugriffsberechtigungen in der Bewegungsdatei lediglich die Bewegungssätze von MANDANT01 in die neue Tabelle übertragen und gesichert und nicht wie bisher – und vielleicht erwartet – die Daten von allen Mandanten.

Eine Warnung oder Fehlermeldung wird nicht ausgegeben, da die Daten, für die der Benutzer USER01 berechtigt ist, problemlos kopiert werden können. Sofern sich der Benutzer USER01 im Anschluss alle Datensätze der Bewegungsdatei anzeigen lässt, wird er keine alten Datensätze finden. Da er für die Daten von anderen Mandanten nicht berechtigt ist, stellt er nicht fest, dass in der Tabelle weiterhin alte Datensätze von anderen Mandanten vorhanden sind.

Sofern das Programm nicht mehrfach von entsprechend berechtigten Benutzern aufgerufen wird, bleiben die Bewegungsdaten der anderen Mandanten ungesichert.

Einige Zeit später könnte ein entsprechend berechtigter Benutzer feststellen, dass in der Bewegungsdatei noch alte Mandantendaten vorhanden sind. Eine Prüfung ergibt, dass die Sicherung erfolgreich ausgeführt wurde, das heißt, laut Protokoll wurde eine entsprechende Sicherungsdatei erstellt und gesichert. In der Annahme, dass das anschließende Löschen nicht stattgefunden habe, löscht der Benutzer daher alle alten Mandantendaten, ohne dass sie zuvor tatsächlich gesichert worden wären.

Anmerkung:

Beim Kopieren von Daten mit dem CL-Befehl CPYF (Datei kopieren) oder mit dem auf einem SELECT-Statement basierenden Befehl CREATE TABLE werden nur die Daten kopiert, für die der ausführende Benutzer berechtigt ist.

Diese Regel gilt auch dann, wenn ein neues Objekt erstellt wird. Die RCAC-Zugriffsberechtigungen werden nicht auf das neue Objekt übertragen.

Im Extremfall kann eine inkorrekte Implementierung der Zugriffsberechtigungen zu Datenverlust führen.

9.15.6.5.1.1

Seite 4

9.15.6.5.1.2 Kopieren von Daten zwischen Tabellen mit RCAC-Zugriffskontrolle

In den meisten Fällen werden jedoch beim Kopieren von Daten keine neuen Tabellen erstellt, sondern lediglich die Daten von einer Tabelle/physischen Datei in eine andere Tabelle/physische Datei transferiert.

Sofern für die Ausgangsdatei entsprechende RCAC-Zugriffskontrollen implementiert sind, werden nur die Datensätze übertragen, für die der Benutzer berechtigt ist. Sind in der Ausgangsdatei keine RCAC-Zugriffskontrollen hinterlegt, werden alle (selektierten) Datensätze in die Zieldatei übernommen.

Sofern für die Zieldatei entsprechende RCAC-Zugriffskontrollen implementiert sind, wird beim Schreiben in die Tabelle/physische Datei geprüft, ob der Benutzer für diese Daten berechtigt ist. Fehlt dem Benutzer die Berechtigung für die Daten, die er schreiben möchte, wird der Befehl mit der Fehlermeldung „INSERT oder UPDATE entspricht nicht den Zeilenberechtigungen." (SQLCODE=20471 / SQLSTATE=22542) abgebrochen.

Sehen wir uns an einem Beispiel an, zu welchen Folgen abweichende oder nicht implementierte RCAC-Zugriffskontrollen beim Kopieren von Daten führen können.

Beispiel:
Benutzer USER01 ruft ein weiteres Reorganisationsprogramm auf, um alle erledigten Aufträge aus den Auftragsdateien, dem Auftragskopf und der Auftragsposition in die entsprechenden History-Dateien zu übernehmen.

Innerhalb dieses Reorganisationsprogramms werden die Auftragsdaten über das folgende SQL-Statement in die History-Datei geschrieben:

```
Insert into OrderHistory (OrdHdrCol1, OrdHdrCol2, ... OrdHdrColN)
       (Select OrdHdrCol1, OrdHdrCol2 ...OrdHdrColN
          From OrderHdr
          Where OrdHdrStatus = 'ERL');
```

Daten mittels SQL in eine andere Tabelle mit RCAC-Zugriffskontrolle übernehmen

9.15.6.5.1.2
Seite 2

- Sofern in beiden Tabellen, ORDERHDR und ORDERHISTORY, RCAC-Zugriffsberechtigungen hinterlegt sind, die den Benutzer USER01 auf die Daten/Aufträge von MANDANT01 beschränken, werden alle erledigten Aufträge von MANDANT01 aus dem Auftragskopf in die Auftrags-History-Datei übertragen.

  Erledigte Aufträge von anderen Mandanten werden aufgrund der Zugriffsbeschränkungen nicht übertragen und bleiben in den Auftragsdateien. Die Übernahme dieser Aufträge muss von einem anderen Benutzer mit entsprechenden Zugriffsberechtigungen ausgeführt werden.

  Lässt sich USER01 nun alle Datensätze in der ORDERHISTORY-Datei anzeigen, so bekommt er lediglich die Datensätze von MANDANT01 zu sehen.

- In der Auftragskopfdatei wurden Zugriffsberechtigungen hinterlegt, die den Zugriff von USER01 auf MANDANT01 beschränken.
  In der History-Datei wurden jedoch keine RCAC-Zugriffskontrollen implementiert.

  Wird der SQL-Befehl von USER01 ausgeführt, so werden alle erledigten Aufträge von MANDANT01 übertragen.

  Erledigte Aufträge von anderen Mandanten müssen von einem anderen Benutzer mit entsprechender Zugriffsberechtigung übertragen werden.

  Lässt sich USER01 alle Datensätze aus der History-Datei anzeigen, so bekommt er aufgrund der nicht implementierten RCAC-Zugriffskontrollen auch die Aufträge der anderen Mandanten zu sehen.

- In der Auftragskopfdatei wurden entweder keine RCAC-Zugriffsberechtigungen oder aber Zugriffsberechtigungen hinterlegt, die USER01 für mehr als einen Mandanten berechtigen. Die RCAC-Zugriffsberechtigungen in der History-Datei beschränken den Benutzer USER01 jedoch auf MANDANT01.

  Bei der Ausführung des SQL-Statements wird versucht, nicht nur die Datensätze von MANDANT01, sondern auch alle Datensätze der anderen Mandanten in die History-Datei zu schreiben.

  Die RCAC-Zugriffskontrolle in der History-Datei bricht an dieser Stelle die Ausführung des INSERT-Statements mit der Fehlermeldung „INSERT oder UPDATE entspricht nicht den Zeilenberechtigungen.“ (SQLCODE=20471 / SQLSTATE=22542) ab.

Anmerkung:

Sofern für Ausgangs- und/oder Zieldatei RCAC-Zugriffsberechtigungen implementiert sind, kann eine abweichende Definition dazu führen, dass der Befehl abgebrochen wird und keine Daten kopiert werden.

Im Extremfall kann aber auch hier eine inkorrekte Implementierung zu Datenverlust führen.

Werden Daten dupliziert, sollte sichergestellt werden, dass in der Ausgangs- und Zieldatei identische Row-Permissions (Zeilenberechtigungen) hinterlegt sind.

9.15.6.5.1.2

Seite 4

9.15.6.5.2 Ändern von Daten mit aktivierten Spaltenmasken

Ein weiteres Problem kann in Verbindung von Updates oder Insert von Datensätzen mit maskierten Spaltenwerten auftreten.

Dies ist insbesondere wichtig, wenn Datensätze mit native I/O geschrieben oder modifiziert werden. Das Problem kann jedoch auch dann auftreten, wenn komplette Datensätze beispielsweise mit SQL oder auch mit dem CL-Befehl CPYF (Datei kopieren) kopiert werden und der Benutzer für bestimmte Spalteninhalte nicht berechtigt ist.

Beispiel:
Benutzer USER01 darf die Adresse im Personalstamm verändern, hat jedoch keine Berechtigung, das Geburtsdatum der Mitarbeiter zu sehen, das sich in einer anderen Spalte im gleichen Datensatz der gleichen Tabelle befindet,.

Das Geburtsdatum der Mitarbeiter wird für USER01 mit dem 01.01.0001 maskiert und entsprechend angezeigt. Selbst beim Debuggen kann der Benutzer USER01 nur den maskieren Wert sehen, nicht jedoch den Originalwert.

Der Benutzer USER01 ändert nach dem Umzug eines Mitarbeiters dessen Adresse über ein Dialogprogramm. Das Programm, das von Benutzer USER01 ausgeführt wird, liest und schreibt den geänderten Datensatz mit native I/O fort.

Vor dem Update bzw. vor dem Einlesen des Datensatzes in das Dialogprogramm der Tabelle ist in der Spalte „Geburtstag“ das echte Geburtsdatum hinterlegt. Beim Einlesen des Datensatzes nun wird das eigentliche Geburtsdatum maskiert und der Maskenwert in den Daten-Buffer ausgegeben. Das Geburtsdatum wird innerhalb des Dialogprogramms nicht verändert. Beim Update ist folglich (noch) der maskierte Wert und nicht der Originalwert im Daten-Buffer enthalten. Das echte Geburtsdatum sollte jedoch beim Update der Adresse nicht verändert, also nicht durch den Maskenwert überschrieben werden.

9.15.6.5.2
Seite 2

Die Überschreibung der Originalwerte durch die Maskenwerte kann auf zwei Arten verhindert werden:

- Check Constraints/Prüfbeschränkung
- Before Insert/Update Trigger

Anmerkung:

Um zu verhindern, dass die Originalspaltenwerte von einem nicht berechtigten Benutzer durch einen Maskenwert überschrieben werden, sollten für alle Spalten mit Spaltenberechtigungen **Check-Constraints** mit **ON-INSERT- / ON-UPDATE-VIOLATION-Klauseln** angelegt werden.

Alternativ kann das Überschreiben der Originalwerte durch **SECURED-BEFORE-INSERT-Trigger / -BEFORE-UPDATE-Trigger** verhindert werden.

9.15.6.5.2.1 Überschreibungen durch Masken mit Check-Contraints verhindern

Um Überschreibungen von Daten durch maskierte Werte zu verhindern, können für Check-Constraints (Prüfintegritäten) zukünftig die folgenden Klauseln hinterlegt werden:

- ON INSERT VIOLATION
  Wird beim Einfügen eines Datensatzes für die Spalte der Maskenwert angegeben, und wurde für diese Maske ein Check-Constraint (Prüfintegrität) mit einer ON-INSERT-VIOLATION-Klausel hinterlegt, so wird anstatt des Maskenwerts der Default-Wert für die Spalte übernommen.
- ON UPDATE VIOLATION
  Sofern für die maskierte Spalte ein Check-Constraint (Prüfintegrität) mit einer ON-UPDATE-VIOLATION-Klausel hinterlegt ist, wird beim Fortschreiben des Datensatzes der übergebene Maskenwert durch den ursprünglichen Spaltenwert ersetzt.

Das folgende Beispiel zeigt die Definition eines Check-Constraint (Prüfintegrität) für die Spalte BIRTHDAY in der Tabelle EMPLOYEE, bei der sowohl die ON-INSERT-VIOLATION-Option als auch die ON-UPDATE-VIOLATION-Option gesetzt wurde.

```
Alter Table EMPLOYEE
       Add Check(BIRTHDAY <> '0001-01-01')
           On Insert Violation Set BIRTHDAY = DEFAULT
           On Update Violation Preserve BIRTHDAY
```

Prüfintegrität/Check Constraint mit ON-INSERT-/UPDATE-VIOLATION -Klausel

9.15.6.5.2.1

Seite 2

9.15.6.5.2.2 Überschreibung durch Masken mit Before-Trigger verhindern

Anstatt Überschreibungen mit Hilfe von Check-Constraints (Prüfintegritäten) zu verhindern, können Maskenwerte auch mit Hilfe von BEFORE-INSERT-Triggern und/oder BEFORE-UPDATE-Triggern ersetzt werden.

Das folgende Beispiel zeigt den SQL-Code für einen BEFORE-Trigger, in dem sowohl die Ereignisse INSERT als auch UPDATE behandelt werden. Wird ein Datensatz mit dem maskierten Geburtstag eingefügt, so wird der Default-Spaltenwert gesetzt. Wird ein Datensatz geändert und der Geburtstag mit dem Maskenwert übergeben, so wird der ursprüngliche Spaltenwert übernommen.

```
Create or Replace Trigger YourSchema.REPLACE_MASK_BIRTHDAY
       Before Insert Or Update On YourSchema.EMPLOYEE
       Referencing New Row as N
                   Old Row as O
       For Each Row
       Mode DB2ROW
        Secured
       When (N.BIRTHDAY = '0001-01-01')
   Begin
     If Inserting Then Set N.BIRTHDAY = Default;
     ElseIf Updating Then Set N.BIRTHDAY = o.BIRTHDAY;
     End If;
   End;
```

Before-Insert/Update-Trigger zum Setzen von Spaltenwerten

Beim Erstellen jeglicher Art von Triggern für Tabellen/physische Dateien, bei denen RCAC-Zugriffsberechtigungen aktiviert wurden, ist noch zu beachten, dass die Trigger-Programme nur dann generiert werden können, wenn das Attribut **SECURED** angegeben wurde.

Durch das Attribut SECURED wird in der Trigger-Definition sichergestellt, dass kein Datenmissbrauch erfolgen kann.

Beispiel:
Ein Programmierer, der einen Trigger erstellen kann, ist nicht notwendigerweise für den Datenzugriff auf die Tabelle bzw. die originalen Spaltenwerte berechtigt.

Ein Trigger-Programm wird durch den Datenbank-Manager aktiviert. Der Benutzer, der mit der entsprechenden Berechtigung die Datenmanipulation vornimmt, ist in der Regel nicht der Programmierer selbst.

9.15.6.5.2.2
Seite 2

Der Programmierer könnte in dem Trigger-Programm dafür sorgen, dass die Daten, für die zwar der Benutzer, jedoch nicht der Programmierer berechtigt ist, gesichert, heruntergeladen, verschickt, publiziert oder auf andere Art missbraucht werden.

Wird das Attribut SECURED bei Erstellung eines Triggers auf eine Tabelle/physische Datei mit aktiver RCAC nicht angegeben, so wird der Trigger nicht erstellt.

Wird das Attribut SECURED angegeben und ist der Programmierer dabei nicht für den Datenzugriff berechtigt, so wird der Trigger ebenfalls nicht erstellt.

Anmerkung:

Das Attribut **SECURED** muss in alle User Defined Functions (UDFs) und Trigger integriert werden, über die auf Tabellen mit aktivierter RCAC zugegriffen wird. Das Attribut SECURED muss auch für alle Trigger angegeben werden, die mit Tabellen mit aktivierter RCAC verlinkt sind.

9.15.6.6 Programmausführung mit Benutzerprofil *USRPRF=*OWNER

Bei der Aktivierung und Implementierung von RCAC muss man auch berücksichtigen, dass der Großteil der Abfragen und Datenmanipulationen nicht interaktiv, sondern innerhalb von Programmen, Prozeduren und Funktionen erfolgt.

Vielfach wurden solche Programme mit der Option Benutzerprofil USRPRF=*OWNER umgewandelt, um (Objekt-)Berechtigungsproblemen aus dem Weg zu gehen. Damit erhält der Benutzer während der Programmausführung die gleichen (Objekt-)Berechtigungen wie der Programmeigner.

Insbesondere in Umgebungen, in denen Datenbankobjekte mit SQL und SQL-Namenskonventionen (*SQL Naming) erstellt werden, wird diese Technik sehr oft verwendet. Bei Datenbankobjekten, die mit SQL-Namenskonventionen erstellt werden, wird die Objektberechtigung für die Allgemeinheit (=*PUBLIC) auf *EXLUDE gesetzt, so dass einzelne Benutzer oder Benutzergruppen, die nicht Eigner des Objekts sind, explizit für den Zugriff berechtigt werden müssen.

Diese Regeln gelten jedoch nicht für den Zugriff auf die Daten. Die Berechtigungsprüfungen für den Zugriff auf Daten können erst dann erfolgen, wenn der Benutzer auf das Objekt zugreifen kann.

Bei den Zugriffsberechtigungen auf Daten kommt es vor allem innerhalb von Programmen darauf an, wie die RCAC-Zugriffskontrolle implementiert bzw. welches Spezialregister (Special Register) für die Berechtigungsprüfung verwendet wurde.

Wurde bei der Implementierung der RCAC-Zugriffskontrolle das Spezialregister SESSION_USER angegeben, so wird die Zugriffsberechtigung zur Laufzeit für den tatsächlichen Benutzer ermittelt. Dies gilt auch dann, wenn das Programm mit Benutzerprofil USRPRF=*OWNER erstellt wurde. Der Benutzer erhält dadurch zwar die gleichen (Objekt-)Berechtigungen wie der Programmeigner, kann jedoch nur auf die Daten zugreifen, für die er selber berechtigt ist.

Wurde bei der Implementierung der RCAC-Zugriffskontrollen dagegen das Spezialregister CURRENT_USER verwendet, so wird die Zugriffsberechtigung innerhalb von Programmen für den übernommenen Benutzer geprüft.

Sofern das Programm mit dem Default-Wert für die Option Benutzerprofil USRPRF=*USER umgewandelt wurde, wird der tatsächliche Benutzer geprüft.

9.15.6.6
Seite 2

Wurde das Programm jedoch mit der Option Benutzerprofil USRPRF=*OWNER umgewandelt, so greift der Benutzer während der Programmausführung auf die Daten zu, für die der Programmeigner berechtigt ist.

Beispiel:
Angenommen, der Eigner des Reorganisationsprogramms, das die Bewegungssätze kopiert, hat die Berechtigung für alle Datensätze.

Das Reorganisationsprogramm wurde außerdem mit der Option Benutzerprofil USRPRF=*OWNER umgewandelt, und in der RCAC-Zugriffsberechtigung wird die Berechtigung über das Spezialregister CURRENT_USER geprüft.

In diesem Fall könnte der Benutzer USER01 das Reorganisationsprogramm aufrufen und alle Bewegungsdaten für alle Mandanten reorganisieren, obwohl er persönlich eigentlich nur für die Daten von MANDANT01 berechtigt ist.

Anmerkung:

Übernommene Berechtigungen für Programme via Benutzerprofil **USRPRF=*OWNER** gelten nur für **Objektberechtigungen.**

Zugriffsberechtigungen auf Daten werden mit Hilfe der verwendeten Spezialregister (SESSION_USER oder **CURRENT_USER**) in den RCAC-Zugriffskontrollen gehandelt.

Je nach Implementierung kann ein Benutzer aufgrund der übertragenen Rechte innerhalb eines Programms Daten verarbeiten, für die er bei einem direkten Zugriff auf die Tabelle nicht berechtigt ist.

9.15.6.6.1 Duplikate erstellen

Vielfach wird der Befehl CRTDUPOBJ (Doppeltes Objekt erstellen) als Alternative zum Erstellen von Tabellen über den CL-Befehl CPYF angesehen.

Beim Kopieren von Daten aus physischen Dateien oder SQL-Tabellen mit aktiver RCAC-Berechtigung werden nur diejenigen Daten übernommen, für die der Benutzer berechtigt ist. Dies ist auch der Fall, wenn eine neue Tabelle, in die die Daten kopiert werden, erstellt wird. Die Row-Permissions (Zeilenberechtigungen) und Column-Masks (Spaltenmasken) werden nicht übernommen.

Was geschieht nun, wenn eine physische Datei oder eine SQL-Tabelle mit aktiven RCAC-Berechtigungen dupliziert wird?

Werden wie auch beim Kopieren über den Befehl CPYF (Datei kopieren) nur die Datensätze übernommen, für die der Benutzer berechtigt ist?

Was geschieht mit den RCAC-Berechtigungen? Werden diese für das neue Objekt übernommen oder nicht?

9.15.6.6.1

Seite 2

9.15.6.6.1.1 CL-Befehl CRTDUPOBJ (Doppeltes Objekt erstellen)

Mit Hilfe des Befehls CRTDUPOBJ (Doppeltes Objekt erstellen) kann ein komplettes Duplikat einer Tabelle/physischen Datei erstellt werden.

Um auch die RCAC-Zugriffsberechtigungen übernehmen zu können, wurde der Befehl CRTDUPOBJ (Doppeltes Objekt erstellen) um die Option ACCCTL (Doppelte Zugriffssteuerung) erweitert.

Der Default-Wert für die Option ACCCTL ist auf *ALL eingestellt, was bewirkt, dass die implementierten Row-Permissions (Zeilenberechtigungen) und Column-Masks (Spaltenmasken) auf das neue Objekt übertragen werden.

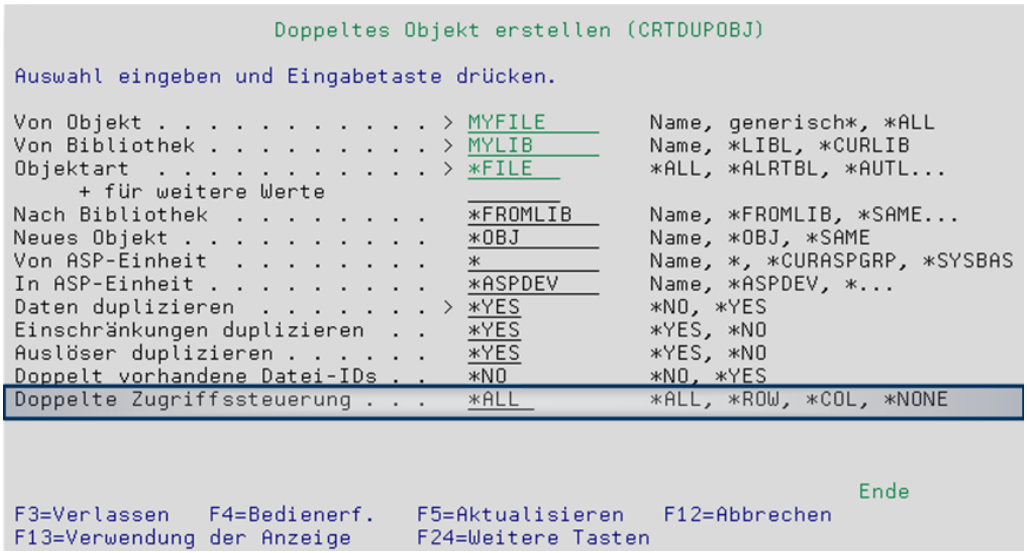
Sofern keine Daten kopiert werden, das heißt, die Option DATA (= Daten duplizieren) ist mit *NO angegeben, ist es auch möglich, wahlweise entweder keine RCAC-Berechtigungen, nur die Zeilen- oder nur die Spaltenberechtigungen für das neue Objekt zu übernehmen.

Sobald jedoch Daten übertragen werden, muss die Option ACCCTL (Doppelte Zugriffssteuerung) unbedingt auf *ALL gesetzt werden, ansonsten kann das Objekt nicht erstellt werden. Diese Angabe ist erforderlich, weil beim Duplizieren der Daten alle Datensätze kopiert werden, unabhängig davon, ob der Benutzer für den Zugriff auf alle Daten berechtigt ist oder nicht. Beim Befehl CRTDUPOBJ werden nicht nur alle Zeilen kopiert, sondern auch die tatsächlichen Spaltenwerte und keine maskierten Werte, auch wenn der Benutzer beim direkten Zugriff auf die Tabelle einen Teil der Spaltenwerte nicht sehen kann.

Da die Regeln für die RCAC-Zugriffsberechtigunen ebenfalls dupliziert werden, ist der Benutzer auch nach Erstellung des Duplikats nicht in der Lage, auf die kopierten Daten – Zeilen wie Spaltenwerte –, für die er nicht explizit berechtigt ist, zuzugreifen.

9.15.6.6.1.1
Seite 2

Die folgende Abbildung zeigt den CL-Befehl CRTDUPOBJ (Doppeltes Objekt erstellen) mit der neuen Option ACCCTL (Doppelte Zugriffssteuerung):



Erweiterung im CL-Befehl CRTDUPOBJ (Doppeltes Objekt erstellen)

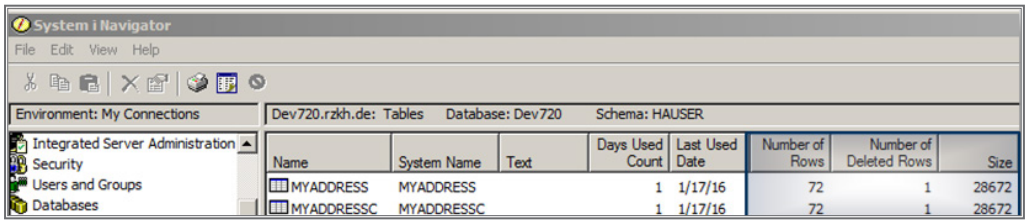
Beispiel:
Mit dem folgenden CL-Befehl wird von Benutzer HAUSER ein absolutes Duplikat der Tabelle MYADDRESS erzeugt.

```
CRTDUPOBJ  OBJ(MYADDRESS)
           FROMLIB(HAUSER)
           OBJTYPE(*FILE)
           TOLIB(HAUSER)
           NEWOBJ(MYADDRESSC)
           DATA(*YES)
           ACCCTL(*ALL)
```

CRTDUPOBJ – Duplikat mit RCAC-Zugriffsberechtigungen erzeugen

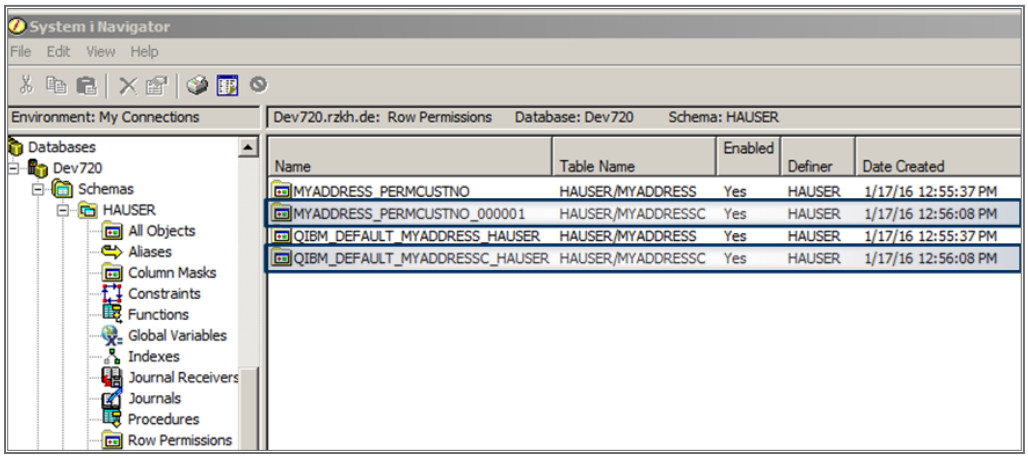
Benutzer HAUSER ist lediglich für die Datensätze im Postleitzahlenbereich zwischen 50000 und 79999 berechtigt und kann dadurch nur auf fünf Datensätze in der Tabelle MYADDRESS zugreifen. Beim Erstellen der Tabelle über CPYF würden nur genau diese fünf Datensätze in das neue Objekt übernommen werden. (Vgl.: Abbildung: IBM i Navigator – Tabelle – Neue Tabelle nach CPYF)

Nach Ausführung des Befehls CRTDUPOBJ zeigt ein Blick auf die Tabellenübersicht im IBM i Navigator (siehe nächste Abbildung), dass das Duplikat die gleiche Anzahl Zeilen und exakt die gleiche Größe wie die Ausgangsdatei hat.



IBM i-Navigator – Tabellenübersicht nach CRTDUPOBJ

In der folgenden Abbildung werden die Row-Permissions (Zeilenberechtigungen) angezeigt, die für die Originaldatei MYADDRESS und die Kopie MYADDRESSC definiert sind. Für beide Tabellen wurden die gleichen RCAC-Zugriffskontrollen implementiert.



IBM i-Navigator – Row-Permissions nach CRTDUPOBJ

Anmerkung:

Anders als bei den Kopierbefehlen, zum Beispiel CPYF (Datei kopieren), wird bei Ausführung des CL-Befehls CRTDUPBOJ ein **komplettes Duplikat** erstellt.

Alle Datensätze werden kopiert, unabhängig davon, ob der Benutzer der den Befehl ausführt, für alle Daten berechtigt ist.

Die Angabe der Option **ACCCTL=*ALL** im Befehl CRTDUPOBJ ist beim Kopieren von Daten zwingend erforderlich. Durch die Angabe der Option ACCCTL=*ALL werden die RCAC-Zugriffsberechtigungen für das neue Objekt übernommen.

9.15.6.6.1.1
Seite 4

Wird in den zugeordneten RCAC-Zugriffsberechtigungen auf andere Datenbankobjekte entweder in der gleichen oder einer anderen Bibliothek/Schema zugegriffen, werden beim Implementieren der RCAC-Zugriffsberechtigungen die vollqualifizierten Objektnamen ermittelt und integriert.

Beim Kopieren wird ein Duplikat der Zugriffsberechtigungen erzeugt und die vollqualifizierten Objektnamen innerhalb der RCAC-Zugriffsberechtigungen werden unverändert übernommen. Das kann zur Folge haben, dass die kopierten Zugriffsberechtigungen nicht auf die gewünschten Objekte verweisen.

Beispiel:
Wird zum Beispiel eine Tabelle in eine Testbibliothek kopiert, sollten auch die Prüfungen innerhalb der RCAC-Zugriffsberechtigungen auf Objekte in dieser Testbibliothek erfolgen.

Bei Ausführung des CRTDUPOBJ-Befehls werden die vollqualifizierten Objektangaben in den RCAC-Zugriffsberechtigungen nicht geändert. Die kopierten RCAC-Zugriffsberechtigungen greifen damit auf die gleichen Objekte wie die ursprünglichen RCAC-Zugriffsberechtigungen zu.

Anmerkung:

Nach dem Erzeugen eines Duplikats sollte man die RCAC-Zugriffsberechtigungen für das Duplikat neu erstellen, um sicherzugehen, dass auf die erwarteten Datenbankenobjekte zugegriffen wird.

9.15.6.6.1.2 Der CL-Befehl CPYLIB (Bibliothek kopieren)

Dem Befehl CPYLIB (Bibliothek kopieren) wurde ebenfalls die Option ACCCTL (doppelte Zugriffssteuerung) hinzugefügt. Der Default-Wert für diese Option im Befehl CPYLIB ist *ALL. Damit werden alle RCAC-Zugriffsberechtigungen, die für die Tabellen/physischen Dateien in der Originalbibliothek definiert sind, auch für die Datenbankobjekte in der neuen Bibliothek implementiert und aktiviert.

Wie für den Befehl CRTDUPOBJ (doppeltes Objekt erstellen) gilt: Werden Datenbankdaten kopiert (Option Daten duplizieren = *YES), so muss die Option ACCCTL (doppelte Zugriffssteuerung) mit *ALL angegeben werden. Anderenfalls wird eine Fehlermeldung ausgegeben und die Bibliothek wird nicht dupliziert.

Durch die Duplizierung einer Datei über Zugriffssteuerungen wird der Bibliotheksname von Dateien, auf die in den zeilen- oder spaltenbezogenen Zugriffssteuerungen verwiesen wird, nicht geändert.

Anmerkung:

Nach dem Duplizieren der Bibliothek sollten die RCAC-Zugriffsberechtigungen auf Tabellen innerhalb der Bibliothek neu erstellt werden, um sicherzustellen, dass die RCAC-Zugriffsberechtigungen auf die richtigen Objekte zugreifen.

9.15.6.6.1.2

Seite 2

9.15.6.6.7 Sichern und Zurücksichern von Tabellen mit RCAC-Zugriffsberechtigungen

Da Row-Permissions (Zeilenberechtigungen) und Column-Masks (Spaltenmasken) direkt in das Datenbankobjekt integriert werden, werden sie automatisch zusammen mit dem Objekt gesichert und auch wieder zurückgespeichert.

Solange in den RCAC-Definitionen auf keine anderen Datenbankobjekte außer die Tabelle selbst zugegriffen wird, gibt es mit dem Sichern und Zurücksichern der Tabellen keinerlei Probleme, auch dann nicht, wenn in eine andere Bibliothek zurückgesichert wird.

Problematischer wird es, wenn in den RCAC-Zugriffsberechtigungen auf andere Datenbankobjekte zugegriffen wird – entweder im gleichen oder einem anderen Schema.

Beim Implementieren der RCAC-Zugriffsberechtigungen werden die Schemata ermittelt, in denen sich die Objekte befinden. Die verwendeten Objekte werden vollqualifiziert in der RCAC-Zugriffsdefinition hinterlegt. Nach dem Zurücksichern kann es sein, dass die in der RCAC-Zugriffsberechtigung vollqualifiziert hinterlegten Objekte entweder nicht existieren oder dass es sich bei den Objekten nicht um die Objekte handelt, auf die zugegriffen werden soll.

Wird zum Beispiel eine Bibliothek unter einem anderen Namen zurückgeladen, so werden zwar die Objekte in die neue Bibliothek integriert, die in der RCAC-Zugriffsdefinition hinterlegten qualifizierten Objektnamen jedoch nicht angepasst.

Anmerkung:

Nach dem Zurücksichern kann es sein, dass es sich bei den in den RCAC-Zugriffsberechtigungen vollqualifizierten Objekten nicht um die Objekte handelt, auf die zugegriffen werden soll.

Aus diesem Grund sollten nach dem Zurücksichern die RCAC-Zugriffsberechtigungen erneut implementiert werden, um sicherzustellen, dass auf die richtigen Objekte zugegriffen wird.

9.15.6.6.7

Seite 2

9.15.7 Schlussfolgerung

Mit Hilfe von RCAC-Zugriffsberechtigungen können die Daten in Tabellen/physischen Dateien effizient vor unerlaubtem Zugriff geschützt werden.

Da die RCAC-Zugriffsberechtigungen direkt in der Datenbank hinterlegt bzw. mit den Tabellen/physischen Dateien verlinkt werden, ist kein zusätzlicher Programmieraufwand erforderlich. Weder die Daten noch die Programme müssen für die Implementierung der RCAC-Zugriffskontrollen geändert werden. Da die Zugriffsbeschränkungen als zusätzliche Schicht zwischen den echten Daten und den ausgegebenen Daten implementiert werden, spielt es keine Rolle, mit welcher Methode (native I/O, JDBC, Query/400 etc.) auf die Daten zugegriffen wird.

Da die RCAC-Zugriffsregeln an einer zentralen Stelle (in der Tabelle/physischen Datei) implementiert werden und damit Auswirkungen auf alle Zugriffe, Programme, Prozeduren, Auswertungen, Downloads etc. haben, ist eine genaue Analyse der vorhandenen Abläufe, Programme, Auswertungen und Downloads erforderlich. Dem schließen sich dann eine detaillierte Planung, penible Realisierung und ausgiebige Tests an.

Einmal erfolgreich implementiert, kann der Source-Code, der zur Sicherstellung der Datenintegrität erforderlich war, aus vielen Programmen und Prozeduren, die unter Umständen in unterschiedlichen Programmiersprachen geschrieben sind, entfernt werden.

Änderungen/Erweiterungen der Zugriffsberechtigungen werden zukünftig nicht mehr innerhalb der Programme, sondern direkt in der Datenbank implementiert. Damit kann der Programmier- und Wartungsaufwand für bestehende und neue Programme beträchtlich reduziert werden. Die Gefahr, dass neue Regeln nicht in allen Programmen und Prozeduren, die außerdem noch in unterschiedlichen Programmiersprachen geschrieben wurden, implementiert werden, besteht somit zukünftig nicht mehr.

9.15.7
Seite 2

9.16 Sicherheitseinstellungen im System i Navigator (Windows)

Viele sicherheitsrelevante Einstellungen lassen sich nicht nur über den Green Screen vornehmen. Unter anderem gibt es für diese Zwecke auch den System i Navigator als Teil der IBM iSeries Access-Lösung, die unter Windows (32- und 64-Bit-Version) läuft.

Interessant zu wissen ist, dass Sie für die Administration keine Client-Lizenzen benötigen, sondern diese Funktionen kostenfrei zur Verfügung stehen. Nur wenn Sie die Client-Emulation aus den IBM Personal Communications verwenden, brauchen Sie die Lizenz für das IBM i-Lizenzprogramm 5770XE1.

Sollten Sie noch keinen System i Navigator installiert haben, hilft nur eine DVD von IBM weiter, die im Auslieferumfang von neuen Systemen enthalten ist. Ich habe noch keinen offiziellen Download auf IBM-Seiten gefunden, eventuell kann ein befreundetes Unternehmen oder ein Dienstleister weiterhelfen, wenn Sie die DVD nicht haben.

Releasevoraussetzungen für IBM i
IBM i Access für Windows unterstützt bestimmte Versionen und Releases des Systems.

IBM i Access für Windows 7.1 (5770-XE1) kann nur auf Systemen mit IBM i 6.1 oder höher installiert werden. Wenn Sie die Installation auf einem System vornehmen, das diese Voraussetzung nicht erfüllt, müssen Sie die Anweisungen im Dokument *„IBM i und zugehörige Software installieren, aktualisieren und Upgrade durchführen“* ausführen, bevor Sie 5770-XE1 installieren können.

Außerdem müssen Sie möglicherweise für andere Systeme, zu denen Ihr PC Verbindungen herstellt, Upgrades vornehmen, nachdem IBM i Access für Windows auf Ihrem PC installiert wurde. IBM unterstützt nur PC-Verbindungen zu IBM i-Systemen mit V5R4 oder höher. Falls diese Systeme diese Voraussetzung nicht erfüllen, müssen Sie dort ein Upgrade des Betriebssystems IBM i vornehmen. Gehen Sie hierbei entsprechend der Anweisungen im Dokument *„IBM i und zugehörige Software installieren, aktualisieren und Upgrade vornehmen“* vor.

PC einrichten

Nach der Installation und Konfiguration von IBM i Access für Windows unter IBM i müssen Sie IBM i Access für Windows auf dem/den anderen PC/s installieren und konfigurieren.

Anmerkung:

Installationen, Service-Pack-Aktualisierungen sowie Upgrades auf neue Releases können nur von Benutzern mit einer Administratorberechtigung vorgenommen werden. Über die Windows-Funktion *„Geplante Tasks mit Fernzugriff"* können Sie auch Benutzern ohne Administratorberechtigung die Durchführung von Installationen, Service-Pack-Aktualisierungen und Upgrades ermöglichen. Alternativ können Sie auch die Richtlinie *„AlwaysInstallElevated"* festlegen. Dies ist eine der Windows Installer-Richtlinien, mit denen Sie das Verhalten des Windows Installer auf den Client-Computern steuern können.

Am besten Sie schauen sich das Dokument zur Installation von System i Access in der Knowledgebase von IBM an, die wichtige Hinweise für die Installation enthält:

http://www-01.ibm.com/support/knowledgecenter/api/content/nl/de/ssw_ibm_i_71/rzaij/rzaij.pdf

System i Access und der Navigator sind nur eingeschränkt nutzbar, wenn Sie die Basisinstallation am PC durchgeführt haben. Der Grund dafür ist, dass Sie vor dem eigentlichen Einsatz erst noch die jeweils aktuellen Service Packs benötigen, die Sie über die Downloadseite für IBM i Access Servicepacks beziehen können.

Release 7.1 war übrigens das letzte Release für IBM® i Access for Windows (5770-XE1). Die meisten der in Release 7.1 von IBM i Access for Windows enthaltenen Funktionen sind allerdings auch in den neueren Produkten verfügbar, Die 5250-Anzeigen- und Druckeremulation, Datenübertragung, 5250-Konsole, virtuelle Steuerkonsole sowie die Möglichkeit zum Herunterladen von Spool-Dateien auf den Desktop sind daher nun auch Bestandteil von IBM i Access Client Solutions (5733-XJ1). Und Datenbanktreiber und Provider wie ODBC, .Net und OLE DB sind im Windows Application Package (5733-XJ1) von IBM i Access Client Solutions enthalten.

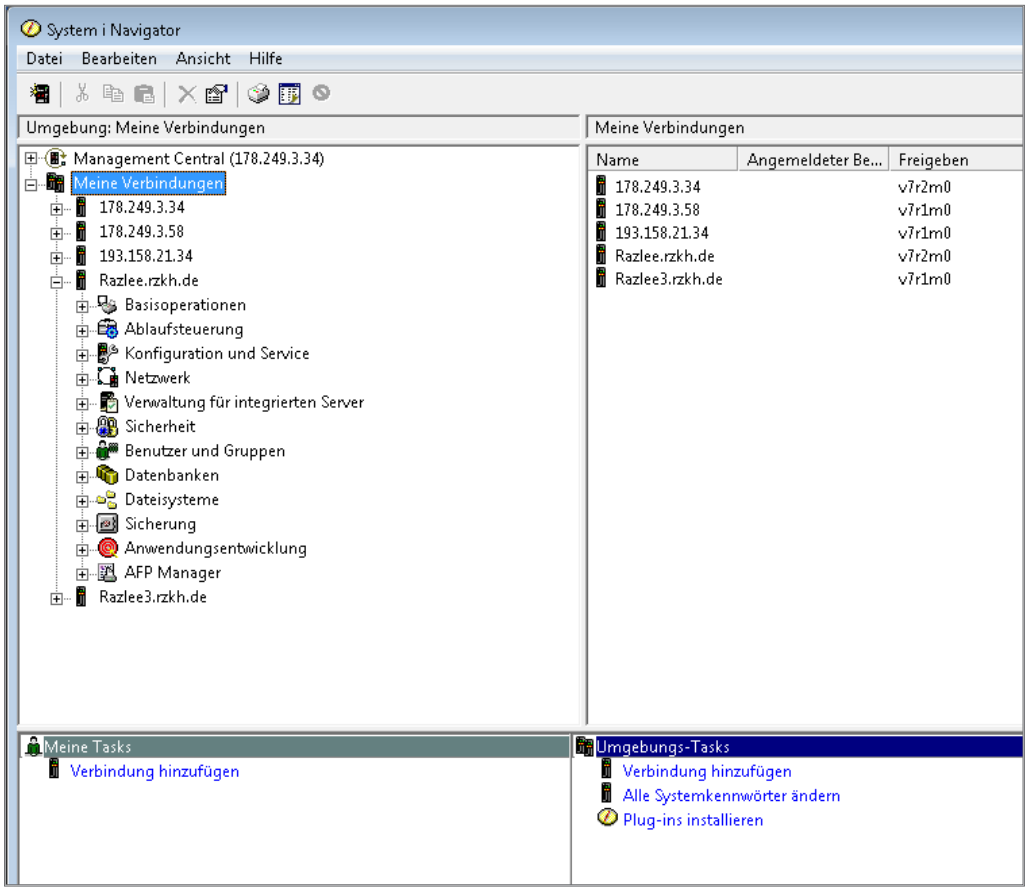
Die meisten Funktionen von System i Navigator sind auch im webbasierten Gegenstück, dem IBM Navigator for i (SS1-Option 3) verfügbar. Bei Funktionen von System i Navigator, die nicht in IBM Navigator for i integriert wurden, wie etwa die Ausführung von SQL-Script, Visual Explain und Management Central, ist die 7.1-Version von System i Navigator mit dem IBM i Release 7.2 kompatibel.

9.16.1 System i Navigator

Der System i Navigator ist eine leistungsstarke grafische Oberfläche, die es Ihnen erlaubt, ohne großen Aufwand mit dem System i-Produkt zu arbeiten. Mit jedem neuen Release wird die grafische Oberfläche des System i-Produkts erweitert.

Um mit System i Navigator arbeiten zu können müssen Sie zunächst über eine Systemverbindung verfügen. Für das Hinzufügen einer Systemverbindung stehen mehrere Möglichkeiten zur Verfügung. Darüber hinaus müssen Sie Ihre Umgebung konfigurieren. Umgebungen sind Container Ihrer direkten Systemverbindungen. Unter „*Verbindung hinzufügen*“ finden Sie weitere Informationen.

Im rechten Fensterbereich von System i Navigator sind die Systeme aufgelistet, zu denen bereits eine Verbindung besteht. Wenn Sie ein System und die Funktionsbereiche erweitern, wird der linke Fensterbereich dahingehend aktualisiert, dass alle Objekte dieses Funktionsbereichs angezeigt werden. Sie können mit der rechten Maustaste auf Objekte im rechten und im linken Fensterbereich klicken, um Aktionen auszuführen.



Verbindung hinzufügen

9.16.1
Seite 2

Eine neue Systemverbindung kann auf mehrere Arten hinzugefügt werden. Gehen Sie wie folgt vor, um eine Systemverbindung über die Menüleiste hinzuzufügen:

1. Wählen Sie „*Verbindung zu Systemen*“ im Menü „*Datei*“ aus.
2. Wählen Sie die Option „*Verbindung hinzufügen*“ aus.
3. Folgen Sie den Anweisungen des Assistenten, um eine Verbindung hinzuzufügen.

Gehen Sie wie folgt vor, um eine Systemverbindung über Ihre Umgebung in der Verzeichnisstruktur hinzuzufügen:

1. Klicken Sie mit der rechten Maustaste auf „*Meine Verbindungen*“ (Ihre aktive Umgebung) bzw. auf den Namen, den Sie für Ihre Umgebung festgelegt haben.
2. Wählen Sie „*Verbindung zu Systemen*“ ➜ „*Verbindung hinzufügen*“ aus.
3. Folgen Sie den Anweisungen des Assistenten, um eine Verbindung hinzuzufügen.

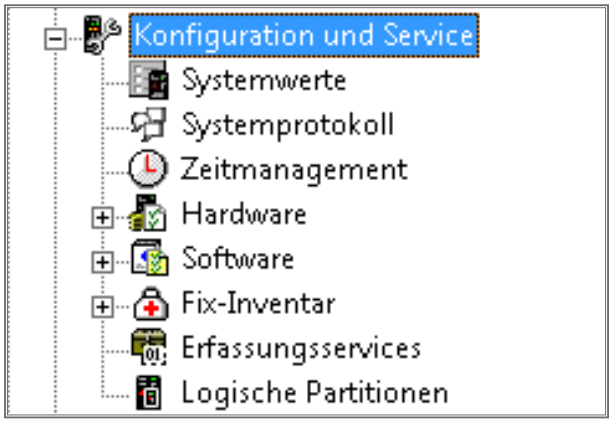
Gehen Sie wie folgt vor, um eine Serververbindung mit Hilfe der Liste „*Umgebungen*“ hinzuzufügen:

1. Klicken Sie mit der rechten Maustaste auf „*Meine Verbindungen*“ (Ihre aktive Umgebung) bzw. auf den Namen, den Sie für Ihre Umgebung festgelegt haben.
2. Wählen Sie „*Verbindung zu Systemen*“ ➜ „*Umgebungen*“ aus.
3. Wählen Sie die Umgebung aus, der Sie eine Verbindung hinzufügen möchten.
4. Wählen Sie die Option „*System hinzufügen*“ aus.
5. Folgen Sie den Anweisungen des Assistenten, um eine Verbindung hinzuzufügen.

9.16.2 Konfiguration und Services

Klappen Sie diesen Zweig auf und Sie finden hier bereits einige der vorher angesprochenen Sicherheitseinstellungen.

„*Konfiguration und Service*“ stellt Funktionen zur Verfügung, die die Verwaltung der Hardware und Software auf Ihrem System erleichtern.



Hier können Sie die Systemwerte anzeigen und ändern, die die Betriebsumgebung auf dem gesamten System beeinflussen. Sie können Zeitzonen für jedes System oder jede logische Partition verwalten und mit Hilfe des Zeitmanagements Ihre Systemzeit mit einer externen Zeitquelle synchronisieren.

Sie können sich außerdem eine vollständige Liste der Hardware- und/oder Softwareressourcen auf Ihrem System anzeigen lassen, einschließlich des Betriebsstatus aller Hardwareressourcen bzw. des jeweiligen Releasestands der Software sowie welche Optionen eventuell bereits installiert sind.

Sie können die Fixinventarliste aufrufen, um sich alle Fixes, Fixgruppen oder Produkte anzeigen zu lassen, die Fixes enthalten. Für jeden Fix können Sie sich zudem Informationen wie die ID, das zugehörige Produkt, den Releasestand oder den Typ anzeigen lassen. In der Fixinventarliste haben Sie des Weiteren die Auswahl zwischen mehreren Assistenten für die Verwaltung der Fixes und Fixgruppen.

Mit Hilfe der Erfassungsservices können Sie Leistungsdaten eines Systems oder mehrerer Systeme erfassen. Danach können Sie Datenbankdateien mit Teilmengen dieser Daten erstellen, um sie später ggf. mit Performance Management Agent zu analysieren.

Last but not least können Sie Systeme mit sekundären logischen Partitionen verwalten.

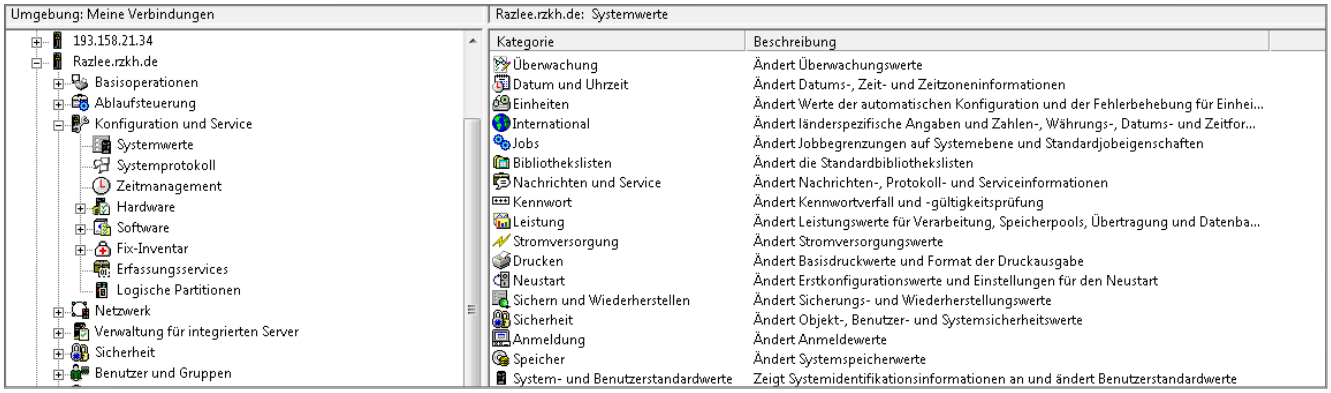
9.16.2
Seite 2

9.16.2.1 Systemwerte

Systemwerte sind informelle Steuerungselemente zur Justierung und Verwaltung der Betriebsumgebung eines Systems. Ein Benutzer kann die Systemwerte ändern, etwa um seine Arbeitsumgebung zu definieren. Systemdatum und Bibliotheksliste sind Beispiele dafür. Systemwerte sind keine Objekte und können daher nicht als Parameterwerte (wie beispielsweise bei CL-Variablen) übergeben werden.

Vorteile von Systemwerten
Systemwerte enthalten also Spezifikationen, mit denen Sie den Gesamtbetrieb Ihres Systems steuern bzw. ändern können. So können Sie beispielsweise als Systemwert für das Datumsformat JJ/MM/TT, MM/TT/JJ, TT/MM/JJ oder Julianisch angeben.

Gliederung der Systemwerte
Die Systemwerte sind in folgende Kategorien unterteilt:



- Überwachung
- Datum und Zeit
- Einheiten
- International
- Jobs
- Bibliothekslisten
- Nachrichten und Service
- Kennwort
- Leistung
- Stromversorgung
- Drucken
- Neustart
- Sichern und Wiederherstellen
- Sicherheit
- Anmeldung
- Speicher
- System- und Benutzerstandardwerte

9.16.2.1
Seite 2

Wann wird ein Systemwert wirksam?
Systemwerte bzw. Systemwertänderungen werden zu unterschiedlichen Zeitpunkten wirksam, sprich nicht alle Systemwertänderungen werden sofort nach ihrer Änderung vom System übernommen. Bei einigen Werten, wie zum Beispiel der Sicherheitsstufe (QSECURITY), werden Änderungen erst beim nächsten Neustart des Systems wirksam. Informationen darüber, wann ein bestimmter Systemwert wirksam wird, finden Sie im Hilfetext zu diesem Systemwert.

Wer kann mit einem Systemwert arbeiten?
Sonderberechtigungen legen fest, ob ein Benutzer Systemfunktionen – also zum Beispiel Systemwerte – ändern bzw. ausführen darf. Welche Sonderberechtigung für einen bestimmten Systemwert erforderlich ist, können Sie dem Hilfetext für den jeweiligen Systemwert entnehmen.

Sonderberechtigungsarten:

- Berechtigung für alle Objekte (*ALLOBJ)
  Der Benutzer ist berechtigt, alle Operationen für Objekte auszuführen.
- Überwachungsberechtigung (*AUDIT)
  Der Benutzer kann die Überwachungsmerkmale für das System, für Objekte und für Systembenutzer definieren.
- Systemkonfigurationsberechtigung (*IOSYSCFG)
  Der Benutzer kann Ein- und Ausgabeeinheiten auf dem System konfigurieren.
- Jobsteuerberechtigung (*JOBCTL)
  Der Benutzer kann Stapeljobs und die Druckausgabe auf dem System steuern.
- Systemsicherungsberechtigung (*SAVSYS)
  Der Benutzer kann Objekte sichern und wiederherstellen.
- Sicherheitsadministratorberechtigung (*SECADM)
  Der Benutzer kann Benutzerprofile auf dem System bearbeiten.
- Serviceberechtigung (*SERVICE)
  Der Benutzer kann Software-Servicefunktionen auf dem System ausführen.
- Spool-Steuerungsberechtigung (*SPLCTL)
  Der Benutzer besitzt uneingeschränkte Steuerungsberechtigung für Stapeljobs und Ausgabewarteschlangen auf dem System.

9.16.2.1.1 Sperrfunktion für sicherheitsrelevante Systemwerte

Die meisten Sicherheitssystemwerte können nur von einem Benutzer mit Sicherheitsadministratorberechtigung (*SECADM) und Sonderberechtigung für alle Objekte (*ALLOBJ) geändert werden. Die Systemservicetools (SST) und die dedizierten Servicetools (DST) enthalten eine Option zum Sperren dieser Sicherheitssystemwerte. Damit können Sie auch verhindern, dass Benutzer sicherheitsrelevante Einstellungen ändern.

Der Standardwert ist *„Ja“*. Bei dieser Einstellung können die Benutzer sicherheitsbezogene Systemwerte ändern.

Die folgende Tabelle bezeichnet die Systemwerte, für die diese Option relevant ist (es werden jeweils der Name im System i Navigator sowie der Name für die zeichenorientierte Schnittstelle angegeben):

Sperrbare Systemwerte	
Systemwerte für die Überwachung	
Aktionsüberwachung aktivieren	QAUDLVL, QAUDLVL2
Objektüberwachung aktivieren	QAUDCTL
Aktion bei Protokolljournalfehler	QAUDENACN
Standardüberwachung für neu erstellte Objekte	QCRTOBJAUD
Maximale Journaleinträge vor dem Schreiben in Zusatzspeicher	QAUDFRCLVL
Einheitensystemwerte	
Lokale Steuereinheiten und Einheiten	QAUTOCFG
Durchgriffseinheiten und Telnet	QAUTOVRT
Zu treffende Maßnahme bei Einheitenfehler	QDEVRCYACN
Ferne Steuereinheiten und Einheiten	QAUTORMT
Jobsystemwerte	
Zeitlimitintervall	QDSCJOBITV
Wenn Job Zeitlimit erreicht	QINACTMSGQ
Unterbrechen von Jobs zulassen, um benutzerdefinierte Exitprogramme auszuführen	QALWJOBITP
Kennwortsystemwerte	
Kennwortverfall	QPWDEXPITV
Aufeinanderfolgende Ziffern ausschließen	QPWDLMTAJC
Ausgeschlossene Zeichen	QPWDLMTCHR
Zeichenwiederholung ausschließen	QPWDLMTREP
Kennwortstufe	QPWDLVL
Maximale Kennwortlänge	QPWDMAXLEN
Mindestkennwortlänge	QPWDMINLEN

9.16.2.1.1
Seite 2

Neues Zeichen an jeder Position erforderlich	QPWDPOSDIF
Mindestens eine Ziffer erforderlich	QPWDRQDDGT
Zyklus für erneute Kennwortverwendung	QPWDRQDDIF
Kennwortprüfprogramm	QPWDVLDPGM
Optionen für Kennwortprüfung	QPWDRULES
Warnintervall für Kennwortverfall	QPWDEXPWRN
Mindestzeit zwischen Kennwortänderungen	QPWDCHGBLK
Systemwerte für Nachrichten und Service	
Fernen Service für System zulassen	QRMTSRVATR
Systemwerte für Sicherung und Wiederherstellung	
Objektkennungen beim Wiederherstellen prüfen	QVFYOBJRST
Objekte während der Wiederherstellung umsetzen	QFRCCVNRST
Wiederherstellung von sicherheitssensitiven Objekten zulassen	QALWOBJRST
Zugriffspfade speichern	QSAVACCPTH
Sicherheitssystemwerte	
Sicherheitsstufe	QSECURITY
Aufbewahrung von Systemsicherheitsinformationen zulassen	QRETSVRSEC
Benutzer, die mit Programmen mit übernommener Berechtigung arbeiten können	QUSEADPAUT
Standardberechtigung für neu erstellte Objekte im Dateisystem QSYS.LIB	QCRTAUT
Verwendung von gemeinsamem oder adressiertem Speicher mit Schreibberechtigung zulassen	QSHRMEMCTL
Diese Objekte zulassen in ...	QALWUSRDMN
Registrierte Exitprogramme zum Überprüfen der Dateisysteme Root (/) und QOpenSys sowie von benutzerdefinierten Dateisystemen verwenden	QSCANFS
Steuerung der Überprüfung	QSCANFSCTL
SSL-Protokolle (Secure Sockets Layer)	QSSLPCL
SSL-Chiffrierverfahren	QSSLCSLCTL
Chiffrierspezifikationsliste	QSSLCSL
Anmeldesystemwerte	
Ferne Anmeldung	QRMTSIGN
Anmeldeinformationen anzeigen	QDSPSGNINF
Privilegierte Benutzer auf spezifische Einheitensitzung beschränken	QLMTSECOFR
Für jeden Benutzer nur eine Einheitensitzung zulassen	QLMTDEVSSN
Inkorrekte Anmeldeversuche	QMAXSIGN
Wenn Maximalwert erreicht ist	QMAXSGNACN

Wenn Sie „*Nein*“ für die Option „*Ändern sicherheitsbezogener Systemwerte*“ setzen, können die Benutzer keine Änderungen an sicherheitsbezogenen Systemwerten vornehmen. Wenn Sie für diese Option „*Nein*“ setzen, können Benutzer mit entsprechender Berechtigung Änderungen an sicherheitsbezogenen Systemwerten vornehmen. Selbst wenn die sicherheitsbezogenen Systemwerte nicht gesperrt sind, benötigen Sie die Sicherheitsadministratorberechtigung (*SECADM) und die Sonderberechtigung für alle Objekte (*ALLOBJ), um sie ändern zu können.

9.16.2.1.1

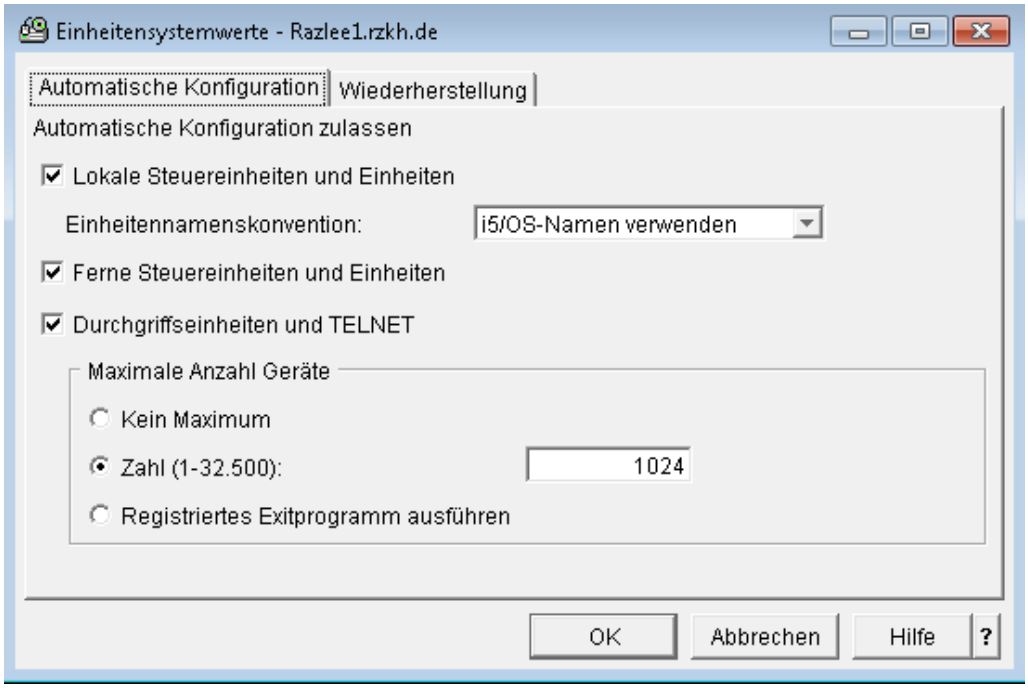
Seite 4

9.16.2.1.2 Einheiten

Übersicht über Einheitensystemwerte

Mit Hilfe der Einheitensystemwerte können Sie Konfigurations- und Wiederherstellungssystemwerte steuern. Die Einheitensystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- Automatische Konfiguration
- Wiederherstellung



9.16.2.1.2
Seite 2

Einheitensystemwerte – automatische Konfiguration
Auf der Seite „*Automatische Konfiguration*“ können Sie Steuerelemente für die automatische Konfiguration verschiedener Objekte angeben. Dazu werden Einheiten und Steuereinheiten benannt und erstellt. Die Objekte werden außerdem angehängt.

Weitere ausführliche Hilfeinformationen können Sie zu folgendem Element dieses Fensters aufrufen:

- Automatische Konfiguration zulassen

Automatische Konfiguration zulassen – Optionen

Lokale Steuereinheiten und Einheiten:
Gibt an, ob Einheiten und Steuereinheiten, die dem System hinzugefügt werden, automatisch konfiguriert werden. Weitere Informationen dazu, welche Steuereinheiten und Einheiten konfiguriert werden, finden Sie in Kapitel 1 unter „*Einheitenkonfiguration*“, IBM Form SC42-2050.

Wird diese Option nicht ausgewählt, müssen Sie neue lokale Steuereinheiten bzw. Einheiten, die Sie dem System hinzufügen wollen, manuell konfigurieren.

Wird diese Option ausgewählt, ist die automatische Konfiguration aktiviert. Das System konfiguriert dann automatisch alle neuen lokalen Steuereinheiten bzw. Einheiten, die dem System hinzugefügt werden. Zudem erhält der Systembediener eine Nachricht, die die Änderungen an der Systemkonfiguration ausweist.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QAUTOCFG

Einheitennamenskonvention:
Gibt die Namenskonvention an, die für die automatische Erstellung von Einheitenbeschreibungen durch das System verwendet wird. Die entsprechenden Namen werden bei der Erstellung von Einheitenbeschreibungen für lokale Steuereinheiten oder Einheiten verwendet, die Ihrem System hinzugefügt werden.

Mögliche Werte:

- i5/OS-Namen verwenden
  i5/OSTM entsprechende Namenskonventionen verwenden
- System/36-Namen verwenden
  dem System/36 entsprechende Namenskonventionen verwenden
- Einheitenadresse verwenden
  Einheitennamen von der Einheitenadresse ableiten

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheits-administrator (*SECADM)
Standardwert:	i5/OS-Namen verwenden
Änderungen werden wirksam:	bei der nächsten Einheitenkonfiguration; vorhandene konfigurierte Einheitennamen werden nicht geändert.
Sperrbar:	nein
Systemwert:	QDEVNAMING

Ferne Steuereinheiten und Einheiten:
Gibt an, ob mit dem System verbundene ferne Steuereinheiten und Einheiten automatisch konfigurieren werden. Wird diese Option nicht ausgewählt, müssen Sie neue ferne Steuereinheiten sowie Einheiten, die mit dem System verbunden werden, manuell konfigurieren.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheits-administrator (*SECADM)
Standardwert:	ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QAUTORMT

Durchgriffseinheiten und TELNET:
Gibt die Anzahl virtueller Einheiten an, die automatisch konfiguriert werden sollen.

Wenn Sie keine Einheiten automatisch konfigurieren wollen, dürfen Sie diese Option nicht auswählen. Es werden dann auch keine Einheiten automatisch gelöscht, etwa um die Summe auf den angegebenen Grenzwert für diesen Systemwert zu senken. Das heißt, wenn Sie den Wert verringern, löscht das System auch keine virtuellen Einheiten.

9.16.2.1.2
Seite 4

Vor dem Erstellen von Einheiten für Telnet- oder für Durchgriffssitzungen, für die der Client keinen Anforderungsnamen angibt, wird dieser Systemwert überprüft, um sicherzustellen, dass mit der neuen Einheit nicht die für diesen Systemwert festgelegte Einheitenanzahl überschritten wird. Wenn durch die Erstellung einer weiteren Beschreibung einer virtuellen Einheit das in diesem Systemwert angegebene Maximum überschritten wird, wird die Einheit für Telnet bzw. den Durchgriff entsprechend nicht erstellt. Bei Anforderung einer Einheit für eine Durchgriffssitzung wird jedoch die Begrenzung dieses Systemwerts vor dem Erstellen einer Einheitenbeschreibung nicht überprüft, wenn der Client den Namen der eingehenden Anforderung (Startdatensatz) angegeben hat.

Das System löscht virtuelle Einheiten nur dann, wenn sie beschädigt sind oder wenn eine Einheit erneut erstellt werden muss, um ihren Typ zu ändern.

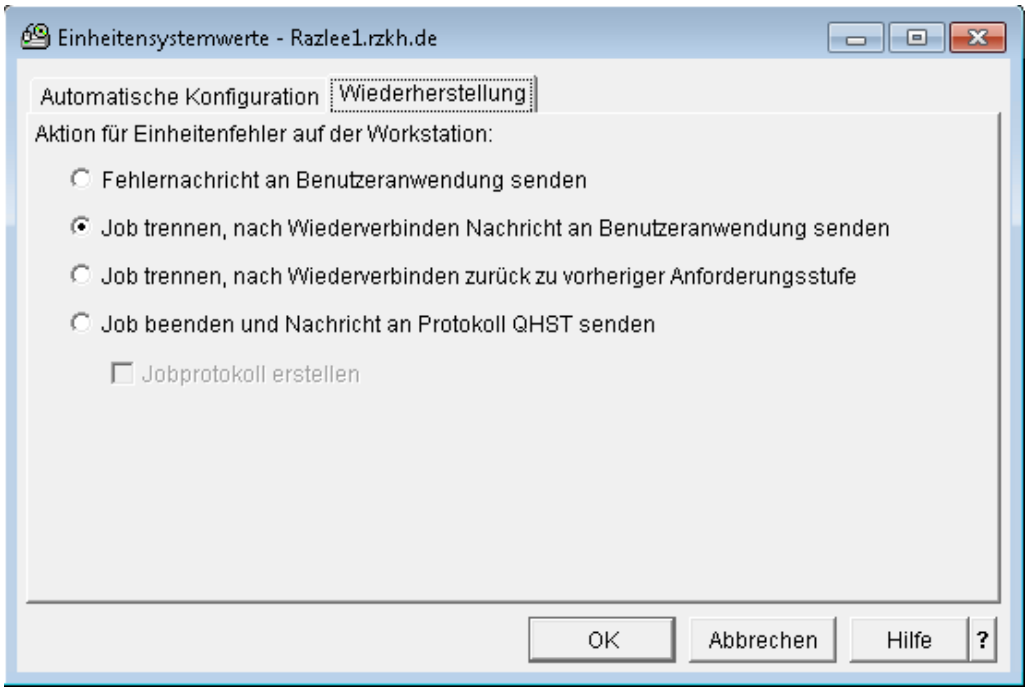
Wenn Sie *„Durchgriffseinheit und TELNET“* auswählen, geben Sie eine der folgenden Optionen an, um die maximale Anzahl konfigurierbarer Einheiten anzugeben:

- Kein Maximum
  Eine unbegrenzte Anzahl virtueller Einheiten kann automatisch konfiguriert werden.
- Zahl (1 bis 32.500)
  Die maximale Anzahl Einheiten, die automatisch konfiguriert werden kann.
  Gültige Werte sind 1 bis 32.500.
- Registriertes Exitprogramm ausführen
  Das für den Ausstiegspunkt *„Virtual Device Selection“* (QIBM_QPA_DEVSEL) registrierte Programm wird aufgerufen, wenn eine virtuelle Einheit vom System ausgewählt oder automatisch erstellt werden muss. Wenn das für den Ausstiegspunkt registrierte Programm nicht existiert oder einen Fehler zurückgibt, behandelt das System die Situation so, als wäre die Auswahl dieses Systemwerts aufgehoben (das heißt, das automatische Konfigurieren virtueller Einheiten ist nicht zulässig).

Wenn der Wert *„Registriertes Exitprogramm ausführen“* lautet, wird das Programm jedes Mal aufgerufen, wenn von einer Durchgriffs- oder einer Telnet-Sitzung eine virtuelle Einheit angefordert wird.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheits-administrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QAUTOVRT



9.16.2.1.2
Seite 6

Einheitensystemwerte – Wiederherstellung
Bei der Übertragung (Ein-/Ausgabe) zwischen Datenstation und System kann ein Einheitenfehler auftreten. Auf der Seite „*Wiederherstellung*“ können Sie die Aktion angeben, die für diesen Fall durchgeführt werden soll.

Weitere ausführliche Hilfeinformationen können Sie zu folgendem Element dieses Fensters aufrufen:

- Aktion für Einheitenfehler auf der Datenstation

Aktion für Einheitenfehler auf der Datenstation
Gibt an, welche Aktion ausgeführt wird, wenn auf der Datenstation eines interaktiven Jobs ein Ein-/Ausgabefehler auftritt.

Die Aktion zur Wiederherstellung einer Einheit wird erst dann ausgeführt, wenn die nächste Ein-/Ausgabeoperation durch den Job erfolgt. In einer LAN- oder WAN-Umgebung kann auf diese Weise eine Einheit die Verbindung trennen und eine andere eine Verbindung herstellen, bevor die nächsten Ein-/Ausgabeoperationen für den Job auftreten. Der Ein-/Ausgabefehler des Jobs kann behoben werden, und der Job kann auf der zweiten Einheit fortgesetzt werden. Um dies zu vermeiden, sollten Sie die Auswahl „*Job trennen, nach Wiederverbinden zurück zu vorheriger Anforderungsstufe*“ oder „*Job beenden und Nachricht an Protokoll QHST senden*“ angeben. Aktionen zur Wiederherstellung von Einheiten werden sofort ausgeführt, wenn ein Ein-/Ausgabefehler (zum Beispiel Ausschalten) auftritt.

Gültige Werte sind:

- Fehlernachricht an Benutzeranwendung senden
  Sendet die E/A-Fehlernachricht an das Anwendungsprogramm des Benutzers. Das Anwendungsprogramm führt dann die Fehlerbehebung durch.
- Job trennen, nach Wiederverbinden Nachricht an Benutzeranwendung senden
  Trennt die Verbindung des Jobs. Wenn sich der Benutzer wieder anmeldet, wird eine Fehlernachricht an das Anwendungsprogramm gesendet.
- Job trennen, nach Wiederverbinden zurück zu vorheriger Anforderungsstufe
  Trennt die Verbindung des Jobs. Wenn sich der Benutzer wieder anmeldet, wird eine Abbruchanforderungsfunktion ausgeführt, um die Steuerung des Jobs an die letzte Anforderungsstufe zurückzugeben.
- Job beenden und Nachricht an Protokoll QHST senden
  Beendet den Job. Eine Nachricht wird an das Protokoll QHST gesendet, die angibt, dass der Job aufgrund eines Einheitenfehlers beendet wurde.

Wählen Sie „*Jobprotokoll erstellen*“ aus, wenn die Nachricht an das Jobprotokoll und an das Protokoll QHST gesendet werden soll.

Damit die Auswirkung des beendeten Jobs auf die Systemleistung so gering wie möglich ausfällt, wird die Priorität des Jobs um 10 verringert, die Zeitscheibe wird auf 100 Millisekunden festgelegt und für das Löschattribut (purge) wird „*Ja*“ angegeben.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Job trennen, nach Wiederverbinden Nachricht an Benutzeranwendung senden
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QDEVRCYACN

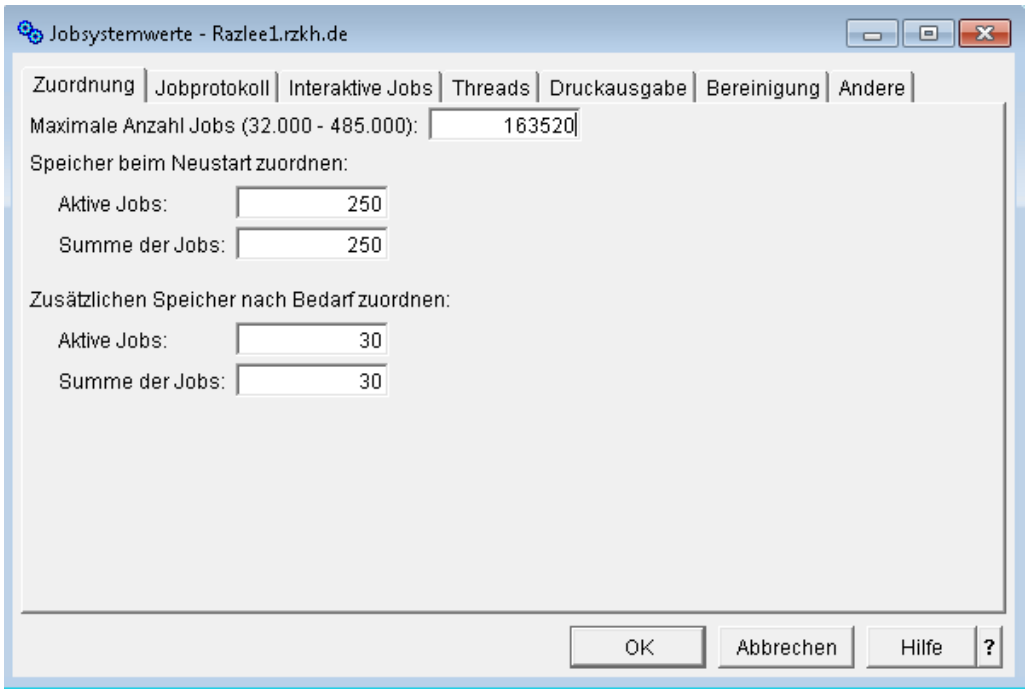
9.16.2.1.2

Seite 8

9.16.2.1.3 Übersicht über Jobsystemwerte

Mit Hilfe der Jobsystemwerte können Sie die Leistung von Jobs auf einem System steuern. Sie können beispielsweise das Zeitlimitintervall sowie die Größe der Jobnachrichtenwarteschlange festlegen und angeben, was geschehen soll, wenn ein Job nicht sicher für Threads ist ... und vieles mehr. Die Jobsystemwerte sind in Gruppen unterteilt. Ausführliche Hilfe zu bestimmten Systemwerten finden Sie für folgende Gruppen:

- Zuordnung
- Jobprotokoll
- Interaktive Jobs
- Threads
- Druckausgabe
- Bereinigung (Diese Seite ist nur in Systemen verfügbar, auf denen OS/400 V5R3 oder i5/OS ausgeführt wird.)
- Andere (Diese Seite ist nur in Systemen verfügbar, auf denen i5/OS ausgeführt wird.)



9.16.2.1.3
Seite 2

Jobsystemwerte – Zuordnung
Auf der Seite „*Zuordnung*“ können Sie die Speichergröße, die beim Neustart zugeordnet wird, sowie die Größe des zusätzlichen Speichers angeben. Auf diese Weise kann Ihr System verschiedene Funktionen mit Hochleistung ausführen.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Maximale Jobs
- Speicher beim Neustart zuordnen
- Zusätzlichen Speicher nach Bedarf zuordnen

Maximale Jobs
Gibt die maximale Anzahl Jobs an, die auf dem System zulässig ist. Wird dieser Maximalwert erreicht, können Sie keine weiteren Jobs auf dem System übergeben oder starten. Mit diesem Systemwert können Sie zudem den für Jobtabellen verwendeten Speicher begrenzen. Gültige Werte sind 32.000 bis 485.000.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	163.520
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QMAXJOB

Speicher beim Neustart zuordnen

Aktive Jobs:
Gibt die Anfangsanzahl aktiver Jobs an, für die Zusatzspeicher beim Neustart des Systems zugeordnet wird. Ein aktiver Job ist ein gestarteter Job, der noch nicht beendet ist. Zusatzspeicher ergänzt den Speicher, der mit dem Systemwert für die Summe der Jobs zugeordnet wird.

Sie können hier also einen neuen Wert festlegen, der aktiven Jobs zugeordnet werden soll. Dieser Wert sollte der geschätzten Anzahl Jobs entsprechen, die an einem normalen Tag mit normaler Auslastung aktiv ist. Um die Anzahl der zuzuordnenden aktiven Jobs zu bestimmen, rufen Sie die Anzahl aktiver Jobs zu einem Zeitpunkt mit normaler Auslastung auf Ihrem System ab.

Gehen Sie wie folgt vor, um sich mit Hilfe von System i Navigator die Anzahl aktiver Jobs auf Ihrem System anzeigen zu lassen:

1. Wählen Sie in System i Navigator den Eintrag für Ihr System aus.
2. Klicken Sie mit der rechten Maustaste auf „*Ablaufsteuerung*“, und wählen Sie „*Systemstatus*“ aus.
3. Klicken Sie im Dialog „*Systemstatus*“ auf „*Jobs*“.
4. Das Feld „*Aktive Jobs*“ gibt Auskunft über die Anzahl der aktiven Jobs.

Gehen Sie wie folgt vor, um sich mit Hilfe von IBM Systems Director Navigator for i5/OS die Anzahl aktiver Jobs auf Ihrem System anzeigen zu lassen:

1. Wählen Sie „*Leistung*“ aus Ihrem IBM Systems Director Navigator for i5/OS-Fenster aus.
2. Wählen Sie „*Systemstatus*“ aus.
3. Klicken Sie im Dialog „*Systemstatus*“ auf „*Jobs*“.
4. Das Feld „*Aktive Jobs*“ gibt Auskunft über die Anzahl der aktiven Jobs.

Diese Zahl liefert Ihnen einen geschätzten Wert für die Anzahl Jobs, die beim Neustart zugeordnet werden sollen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	20
Änderungen werden wirksam:	beim nächsten Neustart des Systems
Sperrbar:	nein
Systemwert:	QACTJOB

9.16.2.1.3
Seite 4

Summe der Jobs:

Gibt die Mindestanzahl Jobs an, für die Speicher zugeordnet wird, wenn Sie das System erneut starten. Die Anzahl Jobs ist die vom System jederzeit unterstützte Anzahl. Hierzu gehören Jobs in Jobwarteschlangen, aktive Jobs (einschließlich Systemjobs) und Jobs mit Ausgabe in Ausgabewarteschlangen.

Wird dieser Wert so definiert, dass der erforderliche Speicher den momentan zugeordneten Speicher überschreitet, wird zusätzlicher Speicher zugeordnet. Wird dieser Wert so definiert, dass der erforderliche Speicher geringer ist als der momentan verfügbare Speicher, passiert nichts.

Um die Gesamtzahl der Jobs im System zu ermitteln, klicken Sie in System i Navigator mit der rechten Maustaste auf Ihr System und wählen die Option „*Systemstatus*“ aus. Alternativ können Sie im IBM Systems Director Navigator for i5/OS „*System*“ und dann „*Systemstatus*“ auswählen.

Die Gesamtzahl der Jobs im System sollte in vernünftigen Grenzen gehalten werden, da sie sich zeitlich auf den Neustart und einige interne Suchen auswirkt. Dazu gehört auch das regelmäßige Entfernen von Jobs, die nur über Jobprotokolle verfügen. Im Handbuch für CL-Programmierung finden sich Erläuterungen zu Jobprotokollen und dazu, wie sie für normal beendete Jobs entfernt werden. Solange ein Job über mindestens eine zugeordnete Druckausgabedatei verfügt, bleibt er im System bekannt und wird im angezeigten Systemstatuswert berücksichtigt.

Sie können auch über den Systemwert „*Druckausgabe nach Ende der Jobs freigeben*“ die Wiederverwendung von Jobstrukturen steuern. Dadurch erhalten Sie ein höheres Maß an Kontrolle über die Anzahl der jeweils in Verarbeitung befindlichen Jobs.

Sie müssen diesen Wert so hoch definieren, dass er möglichst nicht durch die Gesamtsumme der Jobs überschritten wird.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	30
Änderungen werden wirksam:	beim nächsten Neustart des Systems
Sperrbar:	nein
Systemwert:	QTOTJOB

Zusätzlichen Speicher nach Bedarf zuordnen

Aktive Jobs:
Gibt die zusätzliche Anzahl aktiver Jobs an, für die Zusatzspeicher zugeordnet werden soll, wenn die Anfangsanzahl aktiver Jobs schon beim Neustart erreicht ist. Ein aktiver Job ist ein gestarteter Job, der noch nicht beendet ist. Zusatzspeicher wird zugeordnet, sobald die Anzahl aktiver Jobs den bereits zugeordneten Speicher überschreitet.

Für diesen Systemwert wird die Einstellung „*10*“ empfohlen. Wird hierfür ein Wert nahe 1 definiert, kann das häufige Unterbrechungen verursachen, wenn viele zusätzliche Jobs benötigt werden. Die Zahl darf aber auch nicht zu hoch sein, da die erforderliche Zeit für das Hinzufügen des zusätzlichen Speichers so gering wie möglich gehalten werden sollte.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Empfohlene Einstellung:	10
Standardwert:	10
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QADLACTJ

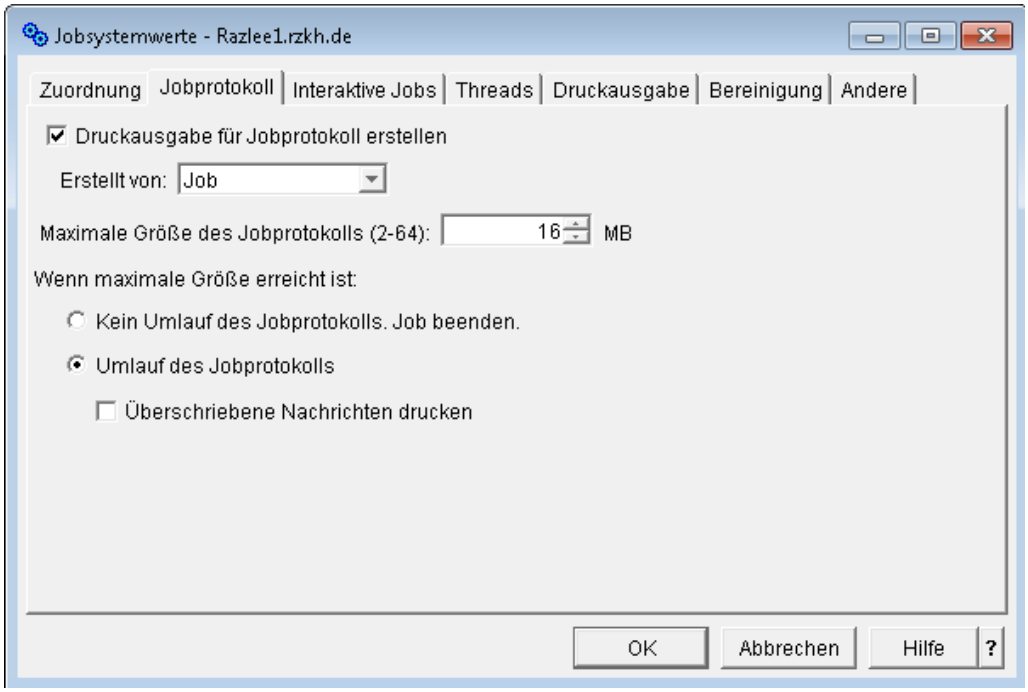
9.16.2.1.3
Seite 6

Summe der Jobs:
Gibt die zusätzliche Anzahl Jobs an, für die Zusatzspeicher zugeordnet werden soll, wenn die Anfangsanzahl der Jobs beim Neustart bereits erreicht ist. Zusatzspeicher wird zugeordnet, sobald die Anzahl der Jobs die Anzahl überschreitet, für die bereits Speicher zugeordnet wurde.

Für diesen Systemwert wird die Einstellung *„10“* empfohlen. Wird hierfür ein Wert nahe 1 definiert, verursacht das häufige Unterbrechungen, wenn viele zusätzliche Jobs benötigt werden. Die Zahl darf aber auch nicht zu hoch sein, da die erforderliche Zeit für das Hinzufügen des zusätzlichen Speichers so gering wie möglich gehalten werden sollte.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Empfohlene Einstellung:	10
Standardwert:	10
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QADLTOTJ



Jobsystemwerte – Jobprotokoll

Auf der Seite *„Jobprotokoll“* können Sie sich die maximale Größe des Jobprotokolls anzeigen lassen und einstellen, wie das Jobprotokoll erstellt wird und welche Aktionen bei Erreichen des Maximalwerts ausgeführt werden sollen.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Druckausgabe für Jobprotokoll erstellen (Nur für Betriebssysteme mit i5/OS V5R4 oder höher verfügbar.)
- Maximale Größe des Jobprotokolls (2 bis 64 MB)
- Wenn maximale Größe erreicht ist

Druckausgabe für Jobprotokoll erstellen
Gibt an, ob das Betriebssystem eine Druckausgabe erstellt, die die Jobprotokollinformationen für einen Job bei dessen Beendigung enthält. Die Druckausgabe des Jobprotokolls kann die mit dem Job ausgeführten Befehle sowie die zugehörigen Nachrichten enthalten.

Diese Option ist nur für Betriebssysteme mit i5/OS V5R4 oder höher verfügbar.

Diese Systemwerteinstellung hat keinen Einfluss auf die Druckausgabe für Jobprotokolle, die generiert werden, wenn die Nachrichtenwarteschlange voll ist und das Jobmerkmal angibt, dass überschriebene Nachrichten gedruckt werden sollen. Sobald eine Nachrichtenwarteschlange voll ist, ignoriert das Betriebssystem diese Systemwerteinstellung und eine Druckausgabe wird automatisch vom Job erstellt. Dieser Systemwert gilt für alle Jobs, die sich nicht in der Ausgabewarteschlange befinden. Jobs in der Ausgabewarteschlange sind bereits beendet.

Ist diese Option nicht ausgewählt, wird nicht automatisch eine Druckausgabe für ein Jobprotokoll erstellt. Dadurch wird der Umfang der durch unnötige Jobprotokolle verbrauchten Prozessor- und Speicherressourcen reduziert.

Ist diese Option ausgewählt, wird automatisch eine Druckausgabe für ein Jobprotokoll erstellt. Sie können die Druckausgabe zu Prüfzwecken und für die Fehlerbehebung verwenden. Außerdem müssen Sie angeben, wodurch die Druckausgabe des Jobprotokolls erstellt wird, durch den Job selbst oder durch den Jobprotokollserver. Wählen Sie eine der folgenden Angaben im Feld *„Erstellt von:“* aus:

Job:
Gibt an, dass der Job die Druckausgabe des Jobprotokolls generiert. Kann der Job die Druckausgabe nicht selbst generieren, wird sie vom Jobprotokollserver generiert. Wird das System zum Beispiel ausgeschaltet, bevor ein Job die Druckausgabe erstellt, wird sie vom Jobprotokollserver erstellt.

Jobprotokollserver:
Gibt an, dass der Jobprotokollserver die Druckausgabe generiert.

Denken Sie außerdem daran, dass Sie nicht mehr benötigte Jobprotokolle und Druckausgaben löschen müssen. Weitere Informationen finden Sie in „*Jobprotokolle löschen*".

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	Jobsteuerberechtigung (*JOBCTL)
Empfohlene Einstellung:	durch Jobprotokollserver ausgewählt und generiert
Standardwert:	durch Job ausgewählt und generiert
Änderungen werden wirksam:	Sofort, bereits gestartete Jobs sind jedoch nicht betroffen.
Sperrbar:	nein
Systemwert:	QLOGOUTPUT

Maximale Größe des Jobprotokolls (2 bis 64 MB)
Gibt die maximale Größe der Jobnachrichtenwarteschlange in Megabyte an. Wird dieser Maximalwert für eine Jobnachrichtenwarteschlange erreicht, wird diese Warteschlange als voll betrachtet, und die für „*Wenn maximale Größe erreicht ist*" angegebene Aktion ausgeführt. Gültige Werte sind 2 bis 64 MB.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	16
Änderungen werden wirksam:	Sofort, bereits gestartete Jobs sind jedoch nicht betroffen.
Sperrbar:	nein
Systemwert:	QJOBMSGQMX

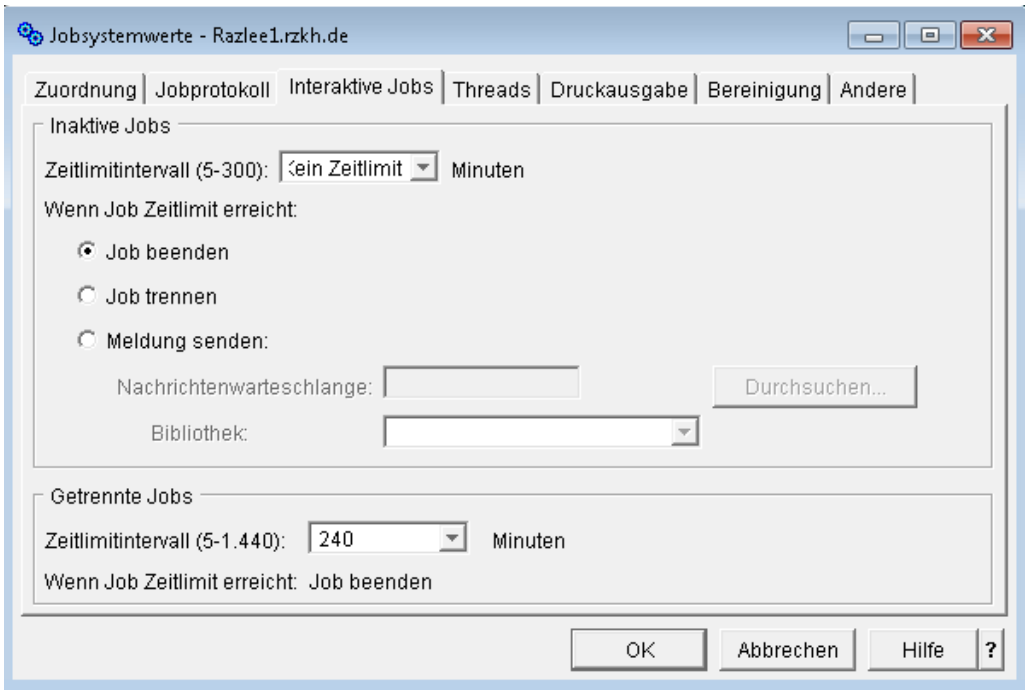
Wenn maximale Größe erreicht ist
Gibt an, wie das System die Jobnachrichtenwarteschlange bearbeiten soll, wenn diese voll ist. Der angegebene Wert im Feld „*Maximale Größe des Jobprotokolls*“ gibt an, wann eine Jobnachrichtenwarteschlange als voll betrachtet wird.

Gültige Werte sind:

- Kein Umlauf des Jobprotokolls. Job beenden.
  Es soll kein Umlauf der Jobnachrichtenwarteschlange stattfinden. Der Job wird beendet, wenn die maximale Größe des Jobprotokolls erreicht ist.
- Umlauf des Jobprotokolls.
  Es soll ein Umlauf der Nachrichtenwarteschlange stattfinden. Sie können die Nachrichten, die durch den Umlauf überschrieben werden, auch mit der Auswahl „*Überschriebene Nachrichten drucken*“ ausdrucken.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	kein Umlauf des Jobprotokolls; Job beenden
Änderungen werden wirksam:	Sofort, bereits gestartete Jobs sind jedoch nicht betroffen.
Sperrbar:	nein
Systemwert:	QJOBMSGQFL



9.16.2.1.3
Seite 10

Jobsystemwerte – Interaktive Jobs
Auf der Seite „*Interaktive Jobs*“ können Sie die Aktion angeben, die durchgeführt werden soll, wenn Jobs ihr Zeitlimit erreicht haben. Außerdem können Sie den Zeitraum für eine Operation angeben, wann also ein Job sein Zeitlimit erreicht hat. Sie können Informationen sowohl zu inaktiven als auch zu Jobs angeben, deren Verbindung getrennt wurde.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Inaktive Jobs
- Getrennte Jobs

Inaktive Jobs
Geben Sie mit Hilfe der Option „*Zeitlimitintervall*“ an, wie viele Minuten ein Job die Möglichkeit haben soll, eine Operation auszuführen, bevor er als inaktiv markiert wird, und mit Hilfe der Option „*Wenn Job Zeitlimit erreicht*“ die Aktion, die durchgeführt werden soll, wenn ein inaktiver Job ein Zeitlimit überschreitet.

Zeitlimitintervall:
Gibt das Zeitlimitintervall für inaktive Jobs in Minuten an. Wenn dieses Zeitlimit erreicht wird, führt das System für inaktive, interaktive Jobs Aktionen durch. Dieser Systemwert bestimmt, wann eine Aktion für einen inaktiven Job ausgeführt wird. Ausgenommen sind lokale Jobs, für die gegenwärtig eine Anmeldung an einem fernen System vorliegt. Beispiel: Eine Datenstation ist direkt an System A angeschlossen und auf System A ist ein bestimmter Systemwert aktiviert. Wenn Sie mit Hilfe von Durchgriff oder Telnet eine Anmeldung bei System B vornehmen, ist der auf System A definierte Zeitlimitwert für diese Datenstation nicht wirksam.

Gültige Werte sind:

- Kein Zeitlimit
  Das System prüft nicht, ob inaktive interaktive Jobs vorhanden sind.
- 5 bis 300
  Die Anzahl Minuten, die ein Job inaktiv sein darf, bevor eine Aktion stattfindet.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	kein Zeitlimit
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QINACTITV

Wenn Job Zeitlimit erreicht:
Gibt die Aktion an, die das System durchführt, wenn ein interaktiver Job über einen bestimmten Zeitraum inaktiv war. Der interaktive Job kann beendet oder getrennt werden, oder es wird eine Nachricht an eine bestimmte Nachrichtenwarteschlange gesendet.

Gültige Werte sind:

- Job beenden
  Der interaktive Job sowie alle zugeordneten sekundären Jobs und Gruppenjobs werden beendet. Sind in einem Subsystem viele inaktive Jobs vorhanden, die gleichzeitig beendet werden sollen, kann die interaktive Antwortzeit dieses Subsystems verlangsamt werden. Um diese Auswirkung gering zu halten, ändert das System einige Jobattribute für jeden zu beendenden Job. Die Jobpriorität wird um 10 verringert, die Zeitscheibe wird auf 100 Millisekunden festgelegt und für das Löschattribut (purge) wird „*Ja*“ angegeben.
- Job trennen
  Die Verbindung des interaktiven Jobs sowie aller zugeordneten sekundären Jobs und Gruppenjobs wird getrennt. Wird diese Aktion angegeben und kann der Job nicht getrennt werden, wird „*Job beenden*“ verwendet.
- Nachricht senden
  Die Nachricht CPI 1126 wird an die angegebene Nachrichtenwarteschlange gesendet. Ist die angegebene Nachrichtenwarteschlange nicht vorhanden oder beschädigt, werden die Nachrichten an die Nachrichtenwarteschlange für Systembediener gesendet.

  Alle Nachrichten in der durch diesen Systemwert angegebenen Nachrichtenwarteschlange werden während des Neustarts gelöscht. Wenn Sie die Nachrichtenwarteschlange eines Benutzers diesem Systemwert zuordnen, verliert dieser Benutzer bei jedem Neustart des Systems alle Nachrichten in seiner Nachrichtenwarteschlange.

9.16.2.1.3
Seite 12

- Nachrichtenwarteschlange
  Geben Sie den Namen einer Nachrichtenwarteschlange an oder wählen Sie mit der Schaltfläche „*Durchsuchen*“ eine Nachrichtenwarteschlange aus. Die Nachrichtenwarteschlange muss im Systemplattenpool (auch Zusatzspeicherpool genannt) oder in einem Basisbenutzerplattenpool vorhanden sein.
- Bibliothek
  Gibt die Bibliothek an, in der sich die Nachrichtenwarteschlange befindet. Sie können einen Bibliotheksnamen bestehend aus maximal 10 Zeichen angeben oder eine der folgenden Optionen auswählen.
  - Bibliotheksliste verwenden
    Alle Bibliotheken in der Bibliotheksliste der aktuellen Sitzung auf dem System werden durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich die Nachrichtenwarteschlange befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Bibliotheksliste verwenden*“. Wenn die Nachrichtenwarteschlange nicht gefunden wird, wird der Wert „*Bibliotheksliste verwenden*“ angezeigt.
  - Aktuelle Bibliothek verwenden
    Die aktuelle Bibliothek, die der aktuellen Sitzung auf dem System zugeordnet ist, wird durchsucht. Wenn keine aktuelle Bibliothek angegeben wurde, wird QGPL durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich die Nachrichtenwarteschlange befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Aktuelle Bibliothek verwenden*“. Wenn die Nachrichtenwarteschlange nicht gefunden wird, wird der Wert „*Aktuelle Bibliothek verwenden*“ angezeigt.
  - Bibliotheksname
    Gibt den Namen der Bibliothek an, die die Nachrichtenwarteschlange enthält.

Wichtige Informationen zu diesem Systemwert:

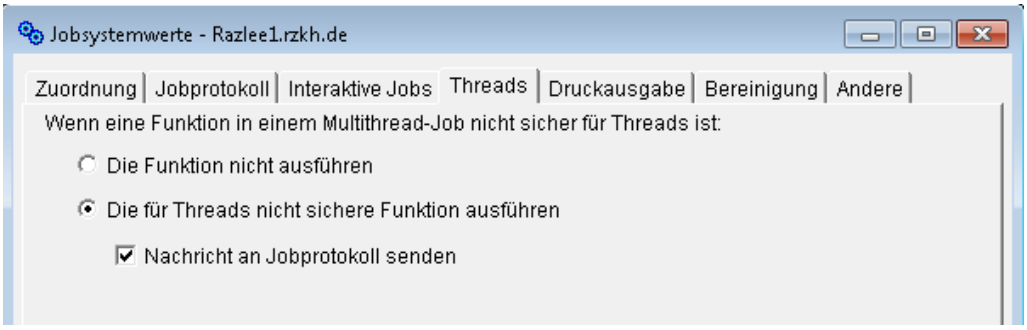
Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Job beenden
Änderungen werden wirksam:	sofort
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QINACTMSGQ

Getrennte Jobs:
Gibt an, wie lange ein getrennter Job inaktiv sein darf, bevor er beendet wird, und welche Aktion ausgeführt wird, wenn ein Job das Zeitlimit erreicht hat. Das Feld „*Wenn Job Zeitlimit erreicht*“ ist schreibgeschützt.

Zeitlimitintervall:
Gibt den Zeitraum in Minuten an, über den ein interaktiver Job getrennt sein darf, bevor er beendet wird. Die Verbindung eines interaktiven Jobs kann mit dem Befehl DSCJOB (Disconnect Job) getrennt werden, wenn der Job während des angegebenen Zeitintervalls inaktiv war oder wenn ein E/A-Fehler an der Datenstation des interaktiven Jobs auftritt.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	240
Änderungen werden wirksam:	sofort
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QDSCJOBITV



9.16.2.1.3
Seite 14

Jobsystemwerte – Threads
Auf der Seite „*Threads*“ können Sie die Aktion angeben, die ausgeführt werden soll, wenn eine Funktion, die möglicherweise nicht threadsicher ist, von einem mit mehreren Threads ausgeführten Job aufgerufen wird.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Wenn eine Funktion in einem Multithread-Job nicht sicher für Threads ist

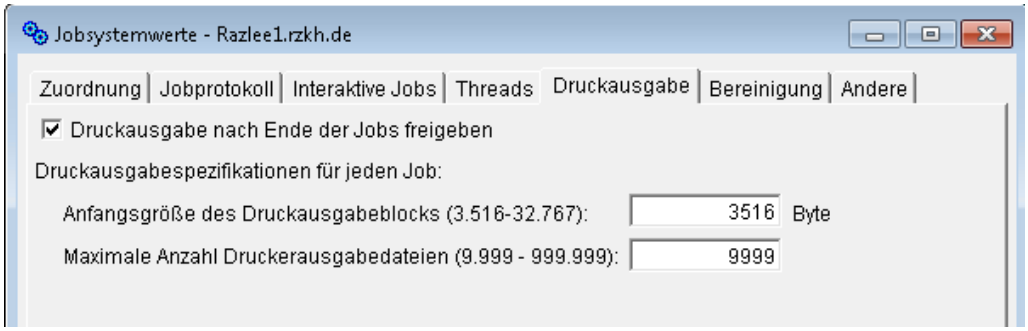
Wenn eine Funktion in einem Multithread-Job nicht sicher für Threads ist
Gibt die Aktion an, die ausgeführt werden soll, wenn eine Funktion, die möglicherweise nicht threadsicher ist, von einem mit mehreren Threads ausgeführten Job aufgerufen wird. Beispiele für Funktionen, die diesen Systemwert unterstützen, sind CL-Befehle und Ausstiegspunkte, die Benutzer-Exitprogramme ausführen, die über die Registrierungsfunktion des Exitprogramms registriert sind.

Gültige Werte sind:

- Die Funktion nicht ausführen
  Wenn eine Funktion nicht sicher für Threads ist, wird sie nicht ausgeführt. Dieser Wert sollte auf Systemen verwendet werden, in denen Multithread-Jobs im Produktionsmodus ausgeführt werden, sowie auf allen Systemen, bei denen Datenintegrität von besonderer Bedeutung ist.
- Die für Threads nicht sichere Funktion ausführen
  Eine für Threads nicht sichere Funktion wird ausgeführt. Dieser Wert sollte nicht auf Systemen verwendet werden, in denen Multithread-Jobs im Produktionsmodus ausgeführt werden; außerdem nicht auf Systemen, bei denen Datenintegrität von besonderer Bedeutung ist. Mit dieser Option können Sie zudem angeben, ob eine Nachricht an das Jobprotokoll gesendet wird. Wählen Sie hierfür folgende Option aus:
- Nachricht an Jobprotokoll senden
  Wählen Sie diese Option aus, um die für Threads nicht sichere Funktion auszuführen und eine Informationsnachricht an das Jobprotokoll zu senden

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	die für Threads nicht sichere Funktion ausführen und Nachricht an Jobprotokoll senden
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QMLTTHDACN



Jobsystemwerte – Druckausgabe
Auf der Seite „*Druckausgabe*“ geben Sie an, ob die Druckausgabe (Spooldateien) zusammen mit einem Job aufbewahrt werden oder von diesem Job abgehängt werden soll. Sie können hier auch bestimmte Druckausgabespezifikationen festlegen, beispielsweise die Mindest- und Höchstgrenze für die Größe von Druckausgabedateien.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Druckausgabe nach Ende der Jobs freigeben (nur für Betriebssysteme mit OS/400 V5R3 oder i5/OS verfügbar)
- Druckausgabespezifikationen für jeden Job

Druckausgabe nach Ende der Jobs freigeben
Gibt an, ob die Druckausgabe zusammen mit einem Job aufbewahrt werden oder von diesem Job abgehängt werden soll.

Das Aufbewahren der Druckausgabe zusammen mit den betreffenden Jobs ermöglicht das Anzeigen der Druckausgabe durch Auswahl der Option „*Druckausgabe*“ auch nach Beendigung des dazugehörigen Jobs. Die beendeten Jobs werden für die Erreichung der im Systemwert „*Maximale Anzahl Jobs*“ definierten Höchstanzahl weiterhin mitgezählt. Der Jobstatus wird zu „*Beendet...*“ (OUTQ), wenn der Job abgeschlossen ist.

9.16.2.1.3
Seite 16

Das Abhängen (Freigeben) der Druckausgabe von einem Job bedeutet, dass der Job nach seiner Beendigung aus dem System entfernt wird. Das verringert die Auslastung von Systemressourcen, da Jobstrukturen nach dem Ende der betreffenden Jobs erneut gestartet und wiederverwendet werden können. Da der Job aus dem System entfernt wird, können die Schnittstellen des Jobs nicht mehr zur Steuerung der dazugehörigen Druckausgabe verwendet werden. Diese Option führt allerdings nicht dazu, dass die Druckausgabe gelöscht wird. Wenn Sie die Druckausgabe eines Jobs anzeigen möchten, der aus dem System entfernt wurde, öffnen Sie System i Navigator und wählen die Option „*Basisoperationen*“ aus, anschließend gehen Sie in „*Druckausgabe*“. Die Druckausgabe wird in die Warteschlange eingereiht. Im IBM Systems Director Navigator for i5/OS wählen Sie „*Basisoperationen*“ aus und gehen anschließend in die „*Druckausgabe*“.

Wenn Sie die Druckausgabe mit den Jobs behalten möchten und sich die Druckausgabe in unabhängigen Plattenpools (auch Zusatzspeicherpool genannt) befindet, müssen Sie sich folgender Einschränkung bewusst sein: Die Druckausgabe in unabhängigen Plattenpools ist vom Job getrennt. Der unabhängige Plattenpool kann zum Beispiel abgehängt und in ein anderes System versetzt werden. Während der Job noch vorhanden ist und der Plattenpool noch abgehängt und auf demselben System wie der Job vorhanden ist, können Sie mit dem Job arbeiten und die Druckausgabe anzeigen. Die Druckausgabe in unabhängigen Plattenpools alleine ist jedoch noch keine Garantie für das kontinuierliche Vorhandensein des Jobs. Wenn sich die einzige Druckausgabe, die einem Job zugeordnet ist, in einem unabhängigen Plattenpool befindet, wird die Druckausgabe vom Job abgehängt und der Job aus dem System entfernt.

Wird ein Job abgeschlossen, enthält er drei Druckausgabedateien: File1, File2 und File3. Wenn der Benutzer es wünscht, werden File1 und File2 gelöscht, File3 bleibt jedoch weiterhin vorhanden. Da sich File3 in einem unabhängigen Plattenpool befindet, wird der Job von der Druckausgabe File3 abgehängt. Die Druckausgabe für diesen Job ist weiterhin verfügbar, aber der Job wird aus dem System entfernt.

Dieser Systemwert ist nur in Systemen verfügbar, auf denen OS/400 V5R3 oder i5/OS ausgeführt wird.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	Sofort, bereits gestartete Jobs sind jedoch nicht betroffen.
Sperrbar:	nein
Systemwert:	QSPLFACN

Druckausgabespezifikationen für jeden Job
Gibt die Anfangsgröße und die maximale Größe der Druckausgabe an. Mit diesen zwei Werten können Sie die Anzahl der zulässigen Druckausgabedateien steuern.

Anfangsgröße des Druckausgabeblocks (3.516 – 32.767 Byte):
Gibt die Anfangsgröße des Spool-Steuerblocks für einen Job an. (Für jeden Job im System gibt es einen Spool-Steuerblock.) Der Spool-Steuerblock zeichnet Informationen zu Inline-Spool-Dateien und Spool-Ausgabedateien auf. Dieser Wert betrifft hauptsächlich den Zusatzspeicher und wirkt sich kaum auf die Gesamtleistung des Systems aus. Der Zusatzspeicher wird für jeden im System bekannten Job reserviert.

Der zugeordnete Bereich besteht aus Standardsteuerdaten sowie einer separaten Gruppe von Steuerdaten für jede Inline-Spool-Datei. Der Standardwert ist 3.516 Byte, was ca. acht Inline-Spool-Dateien pro Job gestattet. Benötigen Ihre Jobs normalerweise mehr als acht Inline-Dateien und spielen zusätzlich 4 KB pro Job für Sie keine Rolle, sind 8.192 Byte eine gute Auswahl. Dadurch sind ungefähr 59 Inline-Spool-Dateien pro Job möglich.

Wichtige Informationen zu diesem Systemwert:

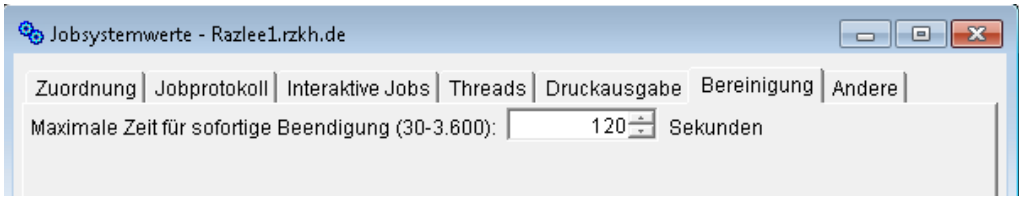
Nützliche Hinweise zu diesem Systemwert	
Sonderberechtigung:	keine
Standardwert:	3.516
Änderungen werden wirksam:	beim nächsten Neustart des Systems
Sperrbar:	nein
Systemwert:	QJOBSPLA

9.16.2.1.3
Seite 18

Maximale Anzahl Druckausgabedateien (9.999 bis 999.999):
Die maximale Anzahl Druckausgabedateien (Spool-Dateien), die pro Job erstellt werden kann. Wenn dieser Wert verringert wird, werden keine Druckausgabedateien gelöscht. Daher kann ein Job mehr als diese maximale Anzahl Druckausgabedateien besitzen. Die überzähligen Druckausgabedateien können aus einer Zeit stammen, als der Systemwert noch höher war. Geben Sie einen Wert im Bereich von 9.999 bis 999.999 an.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	9.999
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QMAXSPLF



Jobsystemwerte – Bereinigung
Auf der Seite „*Bereinigung*“ können Sie die maximal zulässige Zeit für die sofortige Beendigung eines Jobs angeben.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

- Maximale Zeit für sofortige Beendigung (30 bis 3.600 Sek.)

Maximale Zeit für sofortige Beendigung (30 bis 3.600 Sek.)
Gibt die Höchstdauer (in Sekunden) für die Anwendungsbereinigung während der sofortigen Beendigung eines Jobs an. Hierbei handelt es sich sowohl um die maximal zulässige Bereinigungszeit als auch um die Mindestdauer, die erforderlich ist, um festzustellen, ob die Signalverarbeitungsprozedur (SIGTERM) ein Problem entdeckt hat. Die Signalverarbeitungsprozedur wird von der Anwendung im Job definiert und gibt an, wie die eingehenden Signale verarbeitet werden. Nur Jobs, die Anwendungen mit Signalverarbeitungsprozeduren ausführen, verwenden diesen Systemwert.

Wenn ein Job beendet wird und über eine Signalverarbeitungsprozedur für das asynchrone Signal SIGTERM verfügt, wird das Signal SIGTERM für diesen Job generiert. Wenn die Signalverarbeitungsprozedur für das Signal SIGTERM die Steuerung erhält, kann die Prozedur die Aktionen ausführen, die erforderlich sind, um unerwünschte Ergebnisse wie zum Beispiel die teilweise Aktualisierung von Anwendungsdaten zu vermeiden. Wenn die Signalroutine SIGTERM nicht innerhalb der angegebenen Zeitdauer abgeschlossen wird, beendet das System den Job.

Wenn ein Job sofort beendet wird, wird die Höchstdauer für die Signalroutine durch diesen Systemwert festgelegt. Das Zeitlimit für diesen Systemwert wird verwendet, wenn entweder ein Job beendet wird oder wenn alle Jobs in einem Subsystem beendet werden oder wenn alle Jobs in allen Subsystemen beendet werden. Zwei Minuten nach der ersten Beendigungsanforderung kann der Systembediener mit dem Befehl ENDJOB (End Job) und mit OPTION(*IMMED) den Wert QENDJOBLMT überschreiben und einzelne Jobs sofort beenden. Verwenden Sie diesen Befehl nur, wenn ein Job seine Bereinigung aufgrund von Sperr- oder Wartebedingungen nicht durchführen kann.

Damit die Zeit für die Anwendungsbereinigung und die Jobendeverarbeitung des Systems ausreicht, müssen Sie unter Umständen die maximal zulässige Zeit für den Systemabschluss im Systemwert QPWRDWNLMT in der Systemwertekategorie *„Neustart“* anpassen. Wenn Sie für den Systemwert *„Maximale Zeit für sofortige Beendigung“* einen Wert festlegen, der den Wert für *„Maximale Zeit für unmittelbaren Systemabschluss“* überschreitet, wird eine Warnung angezeigt. Wenn ein Systemabschluss durchgeführt wird, müssen alle Jobs innerhalb des Zeitrahmens beendet werden, der durch den Systemwert *„Maximale Zeit für unmittelbaren Systemabschluss“* festgelegt ist, damit der Systemabschluss gesteuert abgeschlossen wird.

Gültige Werte liegen zwischen 30 und 3.600 Sekunden (1 Stunde).

Wichtige Informationen zu diesem Systemwert:

Nützliche Hinweise zu diesem Systemwert	
Sonderberechtigung:	keine
Standardwert:	120
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QENDJOBLMT

9.16.2.1.3
Seite 20

Jobsystemwerte – Andere
Auf der Seite „*Andere*“ können Sie angeben, ob Jobs unterbrochen werden können, um benutzerdefinierte Exitprogramme auszuführen.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

- Unterbrechen von Jobs zulassen, um benutzerdefinierte Exitprogramme auszuführen

Unterbrechen von Jobs zulassen, um benutzerdefinierte Exitprogramme auszuführen
Gibt an, wie das Betriebssystem auf vom Benutzer eingeleitete Anforderungen reagiert, einen Job zu unterbrechen. Mit dieser Funktion können Sie einem Exitprogramm die Möglichkeit bieten, einen Job zu unterbrechen, für den das Programm ausgeführt werden soll. Nur Jobs mit einem aktiven Status können unterbrochen werden.

Ist diese Option nicht ausgewählt, gestattet das Betriebssystem keine Unterbrechung von Jobs, um benutzerdefinierte Exitprogramme auszuführen.

Ist diese Option ausgewählt, gestattet das Betriebssystem eine Unterbrechung von Jobs, um benutzerdefinierte Exitprogramme auszuführen. Für momentan aktive Jobs können Sie mit der API QWCCJITP (Jobunterbrechungsstatus ändern) angeben, ob der Job unterbrochen werden kann, um benutzerdefinierte Exitprogramme auszuführen.

Ist diese Option ausgewählt, steht Ihnen folgende Möglichkeit zur Verfügung:

Alle neuen aktiven Jobs können unterbrochen werden
Wählen Sie diese Option aus, wenn es möglich sein soll, alle Jobs, die aktiv werden, zu unterbrechen. Andernfalls werden alle Jobs, die aktiv werden, standardmäßig als nicht unterbrechbar gekennzeichnet.

Wenn es nicht möglich sein soll, alle Jobs, die aktiv werden, zu unterbrechen, dürfen Sie diese Option nicht auswählen. Dann können Sie über die Eigenschaften bestimmter Jobs einzelne Jobs (anstelle von allen) angeben, die unterbrochen werden können.

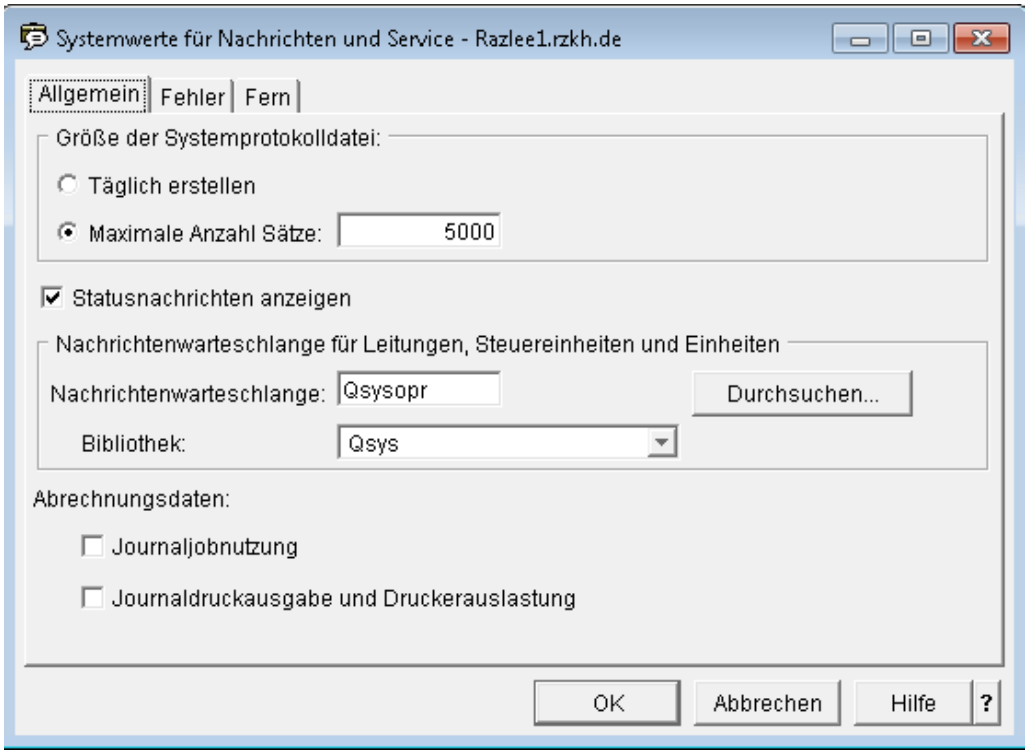
Wichtige Informationen zu diesem Systemwert:

Nützliche Hinweise zu diesem Systemwert	
Sonderberechtigung:	alle Objekte (*ALLOBJ) oder Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	Sofort, bereits gestartete Jobs sind jedoch nicht betroffen.
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QALWJOBITP

9.16.2.1.4 Nachrichten und Service

Übersicht über Nachrichten- und Servicesystemwerte
Mit Hilfe der Nachrichten- und Servicesystemwerte können Sie Nachrichten steuern und festlegen, wie diese auf Ihrem System protokolliert werden. Die Nachrichten- und Servicesystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- Allgemein
- Fehler
- Fern



Systemwerte für Nachrichten und Service – Allgemein

Auf der Seite „Allgemein" können Sie sich Nachrichtenoptionen anzeigen lassen oder diese ändern. Mit den zur Verfügung stehenden Optionen können Sie die Anzahl der Sätze im Systemprotokoll steuern, festlegen, dass Statusnachrichten angezeigt werden und die gewünschte Nachrichtenwarteschlange sowie Abrechnungsdaten angeben.

9.16.2.1.4
Seite 2

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Maximale Sätze in Systemprotokoll (nur für Betriebssysteme mit OS/400 V5R3 oder früher verfügbar)
- Größe der Systemprotokolldatei (nur für Betriebssysteme mit i5/OS V5R4 oder höher verfügbar)
- Statusnachrichten anzeigen
- Nachrichtenwarteschlange für Leitungen, Steuereinheiten und Einheiten
- Abrechnungsdaten

Maximale Sätze in Systemprotokoll
Gibt die maximale Anzahl Sätze für jede Version des Systemprotokolls an. Geben Sie einen Wert von 1 bis 65.535 an. Wenn eine Version voll ist (Maximum erreicht), wird eine neue Version erstellt. Sie können die volle (alte) Version sichern und dann aus dem System löschen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	5.000
Änderungen werden wirksam:	bei der nächsten Systemprotokollerstellung
Sperrbar:	nein
Systemwert:	QHSTLOGSIZ

Größe der Systemprotokolldatei
Gibt an, wann eine neue Version des Systemprotokolls erstellt werden soll. Sie haben die Auswahl zwischen der täglichen Erstellung eines neuen Protokolls oder der Erstellung eines neuen Protokolls nach Erreichen der maximalen Anzahl Sätze. In beiden Fällen wird eine neue Version erstellt, wenn eine Version voll ist (Maximum erreicht). Sie können die volle (alte) Version sichern und dann aus dem System löschen.
Weitere Informationen zur Arbeit mit Systemprotokollen in System i Navigator finden Sie in „*Systemprotokolle löschen*".

Folgende Optionen sind möglich:

Täglich erstellen
Wählen Sie diese Option aus, wenn täglich eine neue Version des Systemprotokolls erstellt werden soll. Erreicht ein Systemprotokoll das Maximum von 10.000.000 Sätzen, wird ein zusätzliches Systemprotokoll für diesen Tag erstellt. Daher kann es täglich mehrere Systemprotokolle geben.

Maximale Anzahl Sätze
Wählen Sie diese Option aus, wenn ein neues Systemprotokoll nur dann erstellt werden soll, wenn die maximale Anzahl Protokollsätze erreicht ist. Wenn Sie diese Option auswählen, müssen Sie einen Wert für die maximale Anzahl Sätze angeben. Gültige Werte sind 1 bis 10.000.000.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	5.000
Änderungen werden wirksam:	bei der nächsten Systemprotokollerstellung
Sperrbar:	nein
Systemwert:	QHSTLOGSIZ

Statusnachrichten anzeigen
Gibt an, ob Nachrichten in Zeile 24 der zeichenorientierten Schnittstelle angezeigt werden.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	ausgewählt
Änderungen werden wirksam:	sofort, bereits gestartete Jobs sind jedoch nicht betroffen
Sperrbar:	nein
Systemwert:	QSTSMSG

9.16.2.1.4
Seite 4

Nachrichtenwarteschlange für Leitungen, Steuereinheiten und Einheiten
Gibt die Nachrichtenwarteschlange an, die das System für Nachrichten bezüglich Leitungen, Steuereinheiten und Einheiten verwendet. Geben Sie Folgendes an:

Nachrichtenwarteschlange
Geben Sie entweder einen Namen aus maximal zehn Zeichen für eine Nachrichtenwarteschlange ein, oder wählen Sie mit der Schaltfläche „*Durchsuchen*“ eine Nachrichtenwarteschlange aus.

Bibliothek
Gibt den Namen der Bibliothek an, welche die Nachrichtenwarteschlange enthält. Sie können einen Bibliotheksnamen aus maximal 10 Zeichen angeben oder eine der folgenden Optionen auswählen:

Bibliotheksliste verwenden
Alle Bibliotheken in der Bibliotheksliste der aktuellen Sitzung auf dem System werden durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich die Nachrichtenwarteschlange befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Bibliotheksliste verwenden*“. Wenn die Nachrichtenwarteschlange nicht gefunden wird, wird der Wert „*Bibliotheksliste verwenden*“ angezeigt.

Aktuelle Bibliothek verwenden
Die aktuelle Bibliothek, die der aktuellen Sitzung auf dem System zugeordnet ist, wird durchsucht. Wenn keine aktuelle Bibliothek angegeben wurde, wird QGPL durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich die Nachrichtenwarteschlange befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Aktuelle Bibliothek verwenden*“. Wenn die Nachrichtenwarteschlange nicht gefunden wird, wird der Wert „*Aktuelle Bibliothek*“ verwenden angezeigt.

Bibliotheksname
Gibt den Namen der Bibliothek an, die die Nachrichtenwarteschlange enthält.

Mit diesem Systemwert können Sie die Standardnachrichtenwarteschlange angeben, die das System für Nachrichten bezüglich Leitungen, Steuereinheiten und Einheiten verwendet. Für ein optimales Gesamtsystemverhalten sollte die für diesen Systemwert angegebene Nachrichtenwarteschlange mit den folgenden Attributen erstellt werden:

Force (FORCE): *NO
Allow Alerts (ALWALR): *NO
Size (SIZE): (8,32,*NOMAX)
Wrap (MSGQFULL): *WRAP

Das System stellt eine Nachrichtenwarteschlange (QSYS/QCFGMSGQ) mit den oben aufgeführten Kenndaten zur Verfügung.

Folgende Leitungsbeschreibungstypen unterstützen diesen Systemwert: Token Ring, Ethernet, DDI, X.25, Frame Relay.

Folgende Steuereinheitenbeschreibungstypen unterstützen diesen Systemwert: APPC, SNA Host, Async, Lokale Datenstation, Ferne Datenstation, Virtuelle Datenstation.

Folgende Einheitenbeschreibungstypen unterstützen diesen Systemwert: APPC, Drucker, Verschlüsselt.

Der vorgegebene Wert lautet QSYS/QSYSOPR, wodurch die Übertragungsnachrichten an die Nachrichtenwarteschlange für Systembediener gesendet werden.

Die Nachrichtenwarteschlange muss im Systemplattenpool (auch Zusatzspeicherpool genannt) oder in einem Basisbenutzerplattenpool vorhanden sein.

Wichtige Informationen zu diesem Systemwert:

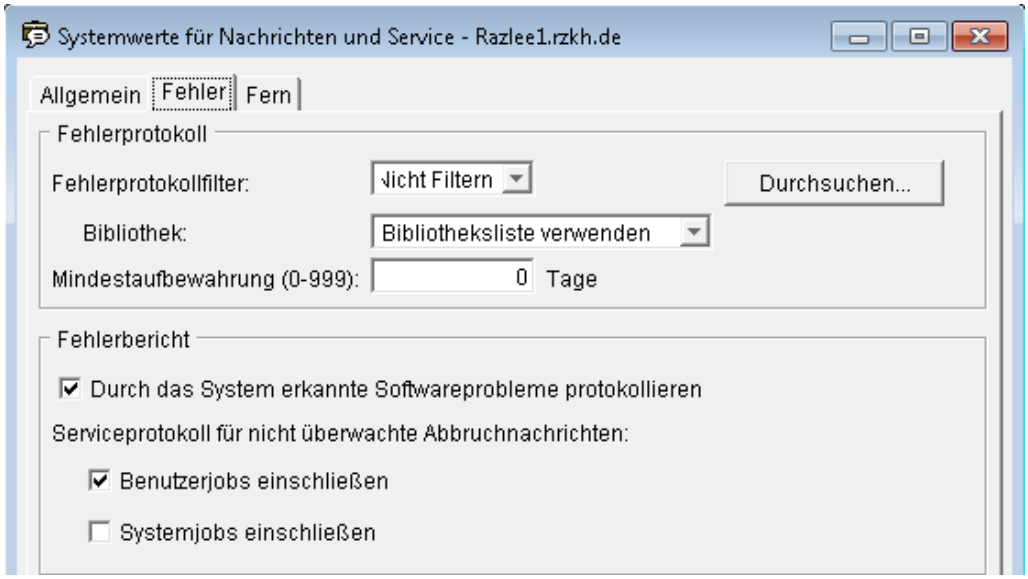
Kurzübersicht	
Sonderberechtigung:	Systemkonfiguration (*IOSYSCFG)
Standardwert:	Nachrichtenwarteschlange – QSYSOPR; Bibliothek – QSYS
Änderungen werden wirksam:	beim Anhängen der Leitungs-, Steuereinheiten- oder Einheitenbeschreibung. Daher müssen Sie bei einer Änderung dieses Systemwerts nach dem Anhängen einer Leitungs-, Steuereinheiten- oder Einheitenbeschreibung das Konfigurationsobjekt abhängen und dann wieder anhängen, damit der neue Wert verwendet wird.
Sperrbar:	nein
Systemwert:	QCFGMSGQ

9.16.2.1.4
Seite 6

Auslastungsdaten
Gibt den Typ der Auslastungsdaten an, den das System in ein Journal schreiben soll. Wird keine Option ausgewählt, werden keine Auslastungsdaten journalisiert. Sie können auswählen, ob Jobauslastungsdaten oder Druckausgabe- und Druckerauslastungsdaten in ein Journal geschrieben werden sollen. Wenn eine der Optionen ausgewählt ist, muss das Systemauslastungsjournal (QACGJRN) in der Bibliothek QSYS vorhanden sein. Ist das nicht der Fall, wird die Änderung zurückgewiesen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	beim Start des nächsten Jobs
Sperrbar:	nein
Systemwert:	QACGLVL



Systemwerte für Nachrichten und Service – Fehler
Auf der Seite „Fehler“ können Sie sich Optionen für das Fehlerprotokoll und den Fehlerbericht anzeigen lassen und diese ggf. ändern.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Fehlerprotokoll
- Fehlerbericht

Fehlerprotokoll
Im Feld „Fehlerprotokoll“ können Sie den Namen des Fehlerprotokollfilters, den Sie verwenden möchten, angeben sowie den Mindestzeitraum in Tagen, über den ein Eintrag im Fehlerprotokoll aufbewahrt werden soll.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	Fehlerprotokollfilter – keine Filterung; Mindestsicherungszeitraum – 30 Tage
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QPRBFTR und QPRBHLDITV

Sie können folgende Optionen für das Fehlerprotokoll angeben:

Fehlerprotokollfilter
Gibt den Namen des Fehlerprotokollfilters an, den der Serviceaktivitätenmanager für die Fehlerverarbeitung verwendet. Der Filter muss im Systemplattenpool (auch Zusatzspeicherpool genannt) oder in einem Basisbenutzerplattenpool vorhanden sein. Mit der Schaltfläche „*Durchsuchen*“ können Sie nach einem Fehlerprotokollfilter suchen.

Bibliothek
Gibt den Namen der Bibliothek an, die den Fehlerprotokollfilter enthält. Geben Sie einen Bibliotheksnamen aus maximal 10 Zeichen an oder wählen Sie eine der folgenden Optionen aus:

Bibliotheksliste verwenden
Alle Bibliotheken in der Bibliotheksliste der aktuellen Sitzung auf dem System werden durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich der Fehlerprotokollfilter „*Schriftart*“ befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Bibliotheksliste verwenden*“. Wenn der Fehlerprotokollfilter nicht gefunden wird, wird der Wert „*Bibliotheksliste verwenden*“ angezeigt.

9.16.2.1.4
Seite 8

Aktuelle Bibliothek verwenden
Die aktuelle Bibliothek, die der aktuellen Sitzung auf dem System zugeordnet ist, wird durchsucht. Wenn keine aktuelle Bibliothek angegeben wurde, wird QGPL durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich der Fehlerprotokollfilter „*Schriftart*" befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Aktuelle Bibliothek verwenden*". Wenn der Fehlerprotokollfilter nicht gefunden wird, wird der Wert „*Aktuelle Bibliothek verwenden*" angezeigt.

Bibliotheksname
Gibt den Namen der Bibliothek an, die den Fehlerprotokollfilter enthält.

Mindestaufbewahrung (0–999)
Geben Sie den Mindestzeitraum in Tagen an, über den ein Fehlerprotokolleintrag im Fehlerprotokoll aufbewahrt wird. Das Zeitintervall startet, sobald der Fehler im Protokoll eingeht. Der Bereich für diesen Systemwert ist 0 bis 999 Tage. Nach diesem Zeitintervall kann der Fehlerprotokolleintrag durch Ausführen eines Befehls gelöscht werden. Geben Sie DLTPRB in die Befehlszeile ein.

Fehlerbericht
Gibt Optionen für Fehlerprotokoll und Fehlerbericht an.

Sie können mindestens eine der folgenden Optionen auswählen:

Durch das System erkannte Softwareprobleme protokollieren
Dieser Wert legt fest, ob Softwarefehler durch das System protokolliert werden sollen. Das Fehlerprotokoll ist der Speicherort für Informationen zu Fehlern, die in der Software Ihres Systems auftreten.

Wenn Sie das Protokollieren von Softwarefehlern, die das System feststellt, auswählen, wird ein Fehler bewertet, um festzustellen, ob er ohne Bedingungen protokolliert werden soll oder ob die Entscheidung über das Protokollieren des Fehlers an die richtlinienbasierte Serviceüberwachung weitergegeben werden soll.

Wenn der Fehler ohne Bedingungen protokolliert werden soll, wird eine PAR-Nachricht (PAR = Problem Alert Record) an die Nachrichtenwarteschlange für Systembediener (QSYSOPR) gesendet und im Fehlerprotokoll wird ein Eintrag erstellt. Stellt die Berichtskomponente Fehlerdaten zur Verfügung, wird eine Spooldatei für die Daten erstellt. Der Name der Spooldatei befindet sich in den Fehlerprotokolleinträgen.

Soll der Fehler bedingt protokolliert werden, wird die Entscheidung über die Protokollierung des Fehlers durch die richtlinienbasierte Serviceüberwachung getroffen. Lautet die Entscheidung, den Fehler zu protokollieren, wird ein Eintrag im Fehlerprotokoll erstellt. Die Fehlerdaten werden in einer Fehlerdatenbibliothek gespeichert und der Problemsatzeintrag wird durch den Namen der Bibliothek aktualisiert.

Sollen durch das System erkannte Softwarefehler nicht protokolliert werden, findet keine Aufzeichnung im Protokoll statt, wenn ein Softwarefehler auftritt.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QSFWERRLOG

9.16.2.1.4
Seite 10

Serviceprotokoll für nicht überwachte Abbruchnachrichten
Dieser Wert definiert, ob Servicespeicherauszüge für nicht überwachte Abbruchnachrichten erstellt werden sollen. Wenn diese Servicespeicherauszüge erstellt werden sollen, können Sie angeben, dass Benutzerjobs und/oder Systemjobs berücksichtigt werden.

Wenn Sie Servicespeicherauszüge für ungewöhnliche Fehler – einschließlich nicht überwachten Abbruchnachrichten – erstellen und aufbewahren, helfen Sie IBM bei der Fehlerdiagnose im Falle eines ungewöhnlichen Fehlers. Beispiele für Systemjobs:

- System-Arbiter
- Subsystemüberwachungen
- Services der logischen Einheit (LU)
- Spool-Eingabe- und -Ausgabeprogramme
- Job zum Starten von Steuerprogrammfunktionen

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	ausgewählte Benutzerjobs einschließen
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QSRVDMP

Systemwerte für Nachrichten und Service – Fern
Auf der Seite „Fern“ können Sie angeben, ob ferner Service für ein System möglich sein soll. Durch fernen Service können Sie ein System von einem anderen Standort aus bedienen.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

- Fernen Service für System zulassen

Fernen Service für System zulassen
Gibt an, ob eine Fernanalyse des Systems zugelassen wird.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QRMTSRVATR

9.16.2.1.4

Seite 12

9.16.2.1.5 System- und Benutzerstandardwerte

Mit Hilfe der System- und Benutzerstandardsystemwerte für die Systemsteuerung können Sie sich spezifische Informationen zu Ihrem System anzeigen lassen oder diese steuern. Die System- und Benutzerstandardsystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- System
- Benutzer

System- und Benutzerstandardsystemwerte – System
Auf der Seite „System“ können Sie sich die Identifikationsdaten Ihres Systems anzeigen lassen.

Weitere ausfsührliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Modellnummer
- Seriennummer
- Prozessor-Feature-Code
- Konsolname

9.16.2.1.5
Seite 2

Modellnummer
Gibt vier Buchstaben oder Ziffern zur Identifizierung des Systemmodells an. Dieser Wert kann in benutzerdefinierten Programmen angezeigt oder abgerufen werden. Der Systemwert für die Modellnummer ist für jede Partition im System gleich. Diesen Wert können Sie nicht bearbeiten.

Die Modellnummer hat folgendes Format. Hierbei steht xx für die spezifische Modellnummer.

- **5xx:** gibt eServer bzw. i5-Server an
- **7xx:** gibt AS/400-Server an
- **8xx:** gibt iSeries- oder IBM System i5-Produkte an

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Standardwert:	maschinenabhängig
Änderungen werden wirksam:	Dieser Systemwert ist schreibgeschützt. Diesen Systemwert können Sie daher nicht ändern.
Sperrbar:	nein
Systemwert:	QMODEL

Seriennummer
Die Seriennummer dient der Kennzeichnung bzw. Identifikation. Diese Nummer richtet sich nach der Version, dem Release sowie dem Modell des installierten Systems. Die Seriennummer des Systems ist für jede Partition im System gleich. Beispiel einer Seriennummer: 1001003. Diesen Wert können Sie nicht bearbeiten.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Standardwert:	maschinenabhängig
Änderungen werden wirksam:	Dieser Systemwert ist schreibgeschützt. Diesen Systemwert können Sie daher nicht ändern.
Sperrbar:	nein
Systemwert:	QSRLNBR

Prozessor-Feature-Code
Dieser Wert gibt die Stufe des Prozessor-Feature-Codes des Systems an. Die Zahl bezeichnet den Prozessor, also denjenigen Teil des Computers, der für die eigentliche Datenverarbeitung im System zuständig ist. Der Systemwert für das Prozessor-Feature ist für jede Partition im System gleich. Diesen Wert können Sie nicht bearbeiten.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Standardwert:	maschinenabhängig
Änderungen werden wirksam:	Dieser Systemwert ist schreibgeschützt. Diesen Systemwert können Sie daher nicht ändern.
Sperrbar:	nein
Systemwert:	QPRCFEAT

Konsolname
Gibt den Namen derjenigen Bildschirmeinheit an, welche die Konsole ist. Das System ändert diesen Wert, wenn die Konsole angehängt wird. Diesen Wert können Sie nicht bearbeiten.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Standardwert:	QCONSOLE
Änderungen werden wirksam:	Dieser Systemwert ist schreibgeschützt. Diesen Systemwert können Sie daher nicht ändern.
Sperrbar:	nein
Systemwert:	QCONSOLE

9.16.2.1.5
Seite 4

System- und Benutzerstandardsystemwerte – Benutzer
Auf der Seite „Benutzer“ können Sie die Standardwerte für die Benutzer auf Ihrem System angeben.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Unterstützungsstufe
- Abrufprogramm
- Standardbenutzerumgebung
- Eingabepufferfunktion verwenden

Unterstützungsstufe
Gibt die Unterstützungsstufe an, die den Benutzern des Systems zur Verfügung steht. Mit diesem Wert können Sie die Stufe der Anzeigen, die den Benutzern des Systems zur Verfügung stehen, anpassen. Anzeigen für unerfahrene Benutzer stellen eine höhere Unterstützungsstufe zur Verfügung als Anzeigen für erfahrene Benutzer.

Mögliche Werte:

- Basis
  Eine Basisunterstützungsstufe für Systemanzeigen ist verfügbar.
- Erweitert
  Eine Zwischenunterstützungsstufe für Systemanzeigen ist verfügbar.
- Voll erweitert
  Eine erweiterte Unterstützungsstufe für Systemanzeigen ist verfügbar.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	Basis
Änderungen werden wirksam:	bei der nächsten Anmeldung eines Benutzers im System
Sperrbar:	nein
Systemwert:	QASTLVL

Abrufprogramm
Gibt das Programm an, das aufgerufen werden soll, wenn Sie die Abruftaste drücken.

Mögliche Werte:

- Oberfläche für Anwendungen verwenden
  Das Hauptmenü der Oberfläche für Anwendungen wird angezeigt, wenn Sie die Abruftaste drücken.
- Keine
  Kein Abrufprogramm wird aufgerufen, wenn sie die Abruftaste drücken.
- Programmname
  Geben Sie das Programm an, das aufgerufen werden soll, wenn sie die Abruftaste drücken, oder wählen Sie mit der Schaltfläche „Durchsuchen" ein Programm aus. Das Programm muss im Systemplattenpool (auch Zusatzspeicherpool genannt) oder in einem Basisbenutzerplattenpool vorhanden sein.

Bibliothek
Gibt den Namen der Bibliothek an, in der sich das Abrufprogramm befindet. Geben Sie einen Bibliotheksnamen aus maximal 10 Zeichen an oder wählen Sie eine der folgenden Optionen aus:

Bibliotheksliste verwenden
Alle Bibliotheken in der Bibliotheksliste der aktuellen Sitzung auf dem System werden durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich das Programm befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Bibliotheksliste verwenden*". Wenn das Programm nicht gefunden wird, wird der Wert „*Bibliotheksliste verwenden*" angezeigt.

Aktuelle Bibliothek verwenden
Die aktuelle Bibliothek, die der aktuellen Sitzung auf dem System zugeordnet ist, wird durchsucht. Wenn keine aktuelle Bibliothek angegeben wurde, wird QGPL durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich das Programm befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director Navigator for i5/OS wird der Bibliotheksname angezeigt und nicht „*Aktuelle Bibliothek verwenden*". Wenn das Programm nicht gefunden wird, wird der Wert „*Aktuelle Bibliothek verwenden*" angezeigt.

Bibliotheksname
Gibt den Namen der Bibliothek an, die das Programm enthält.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Oberfläche für Anwendungen verwenden
Änderungen werden wirksam:	bei der nächsten Anmeldung eines Benutzers im System
Sperrbar:	nein
Systemwert:	QATNPGM

Standardbenutzerumgebung
Gibt die für alle Benutzer verwendete Standardsystemumgebung an.

Mögliche Werte sind:

i5/OS
Geben Sie die i5/OS-Systemumgebung bei der Anmeldung an.

System/36
Geben Sie die System/36-Umgebung bei der Anmeldung an.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	i5/OS
Änderungen werden wirksam:	bei der nächsten Anmeldung eines Benutzers im System
Sperrbar:	nein
Systemwert:	QSPCENV

Eingabepufferfunktion verwenden
Gibt an, ob die Eingabepufferfunktion und die Pufferoption für die Abruftaste verwendet werden sollen. Die Eingabepufferfunktion sorgt dafür, dass sich das System einige Tastenanschläge ‚merkt'.

Angenommen, Sie drücken beispielsweise regelmäßig die Optionstaste 2 und müssen dann einige Sekunden warten, bis die nächste Anzeige aufgebaut ist, in der Sie Optionstaste 4 drücken möchten. Dank der Eingabepufferfunktion können Sie die Optionstasten 2 und 4 unmittelbar nacheinander drücken, ohne die nächste Bildschirmanzeige abwarten zu müssen. Wenn schließlich die nächste Anzeige geöffnet wird, weiß das System bereits, dass Option 4 angegeben wurde.

Wird die Eingabepufferfunktion ausgewählt, können Sie auch „*Puffern der Abruftaste verwenden*" auswählen.

Puffern der Abruftaste verwenden
Gibt an, ob die Option zum Puffern der Abruftaste aktiviert wird oder nicht. Wenn diese Option aktiviert ist, ‚merkt' sich das System, dass die Abruftaste gedrückt wurde.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Eingabepufferfunktion verwenden
Änderungen werden wirksam:	bei der nächsten Anmeldung eines Benutzers im System
Sperrbar:	nein
Systemwert:	QKBDBUF

9.16.2.1.5

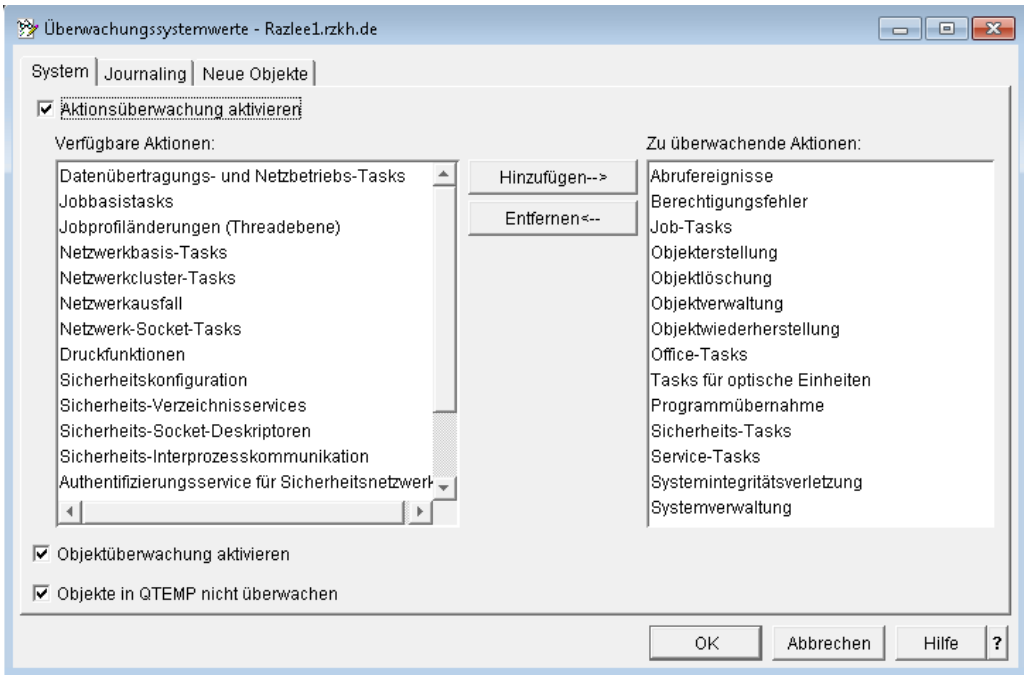
Seite 8

9.16.2.1.6 Überwachung (Audit)

Mit Hilfe der Überwachungssystemwerte können Sie die Überwachung – das von IBM zur Verfügung gestellte Audit auf dem System steuern. Die Überwachungssystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- System
- Neue Objekte
- Journaling

Zum Anzeigen der Überwachungssystemwerte benötigen Sie die Sonderberechtigung für alle Objekte (*ALLOBJ) oder Überwachungsberechtigung (*AUDIT). Ist keine geeignete Berechtigung vorhanden, ist die Kategorie Überwachung der Systemwerte nicht verfügbar



Die Überwachung wird für alle Benutzer des Systems ausgeführt. Verwenden Sie die Schaltflächen „*Hinzufügen*“ und „*Entfernen*“, um anzugeben, welche Aktionen überwacht werden sollen.

Verfügbare Aktionen
Diese Liste enthält alle Aktionen, die überwacht werden können. Wählen Sie eine Aktion aus und klicken Sie auf „Hinzufügen“, um sie in die Liste „Zu überwachende Aktionen“ zu verschieben.

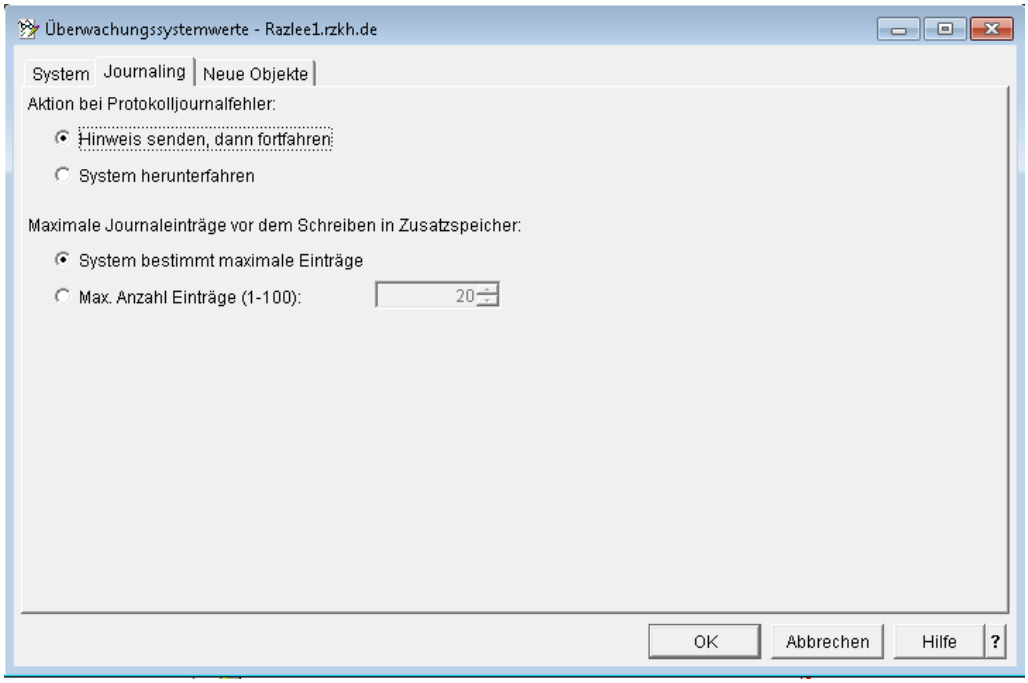
Zu überwachende Aktionen
Diese Liste enthält alle Aktionen, die überwacht werden sollen. Um eine Aktion aus der Liste zu entfernen, wählen Sie die entsprechende Aktion in der Liste „*Zu überwachende Aktionen*“ aus, und klicken auf „*Entfernen*“.

9.16.2.1.6
Seite 2

Wählen Sie einen der folgenden Einträge aus, um weitere Informationen zu jeder Aktion aufzurufen:

- Abrufereignisse Berechtigungsfehler
- Tasks für optische Einheiten –Tasks für Datenübertragung und Netzbetrieb
- Druckfunktionen Job-Tasks
- Programmübernahme – Objekterstellung
- Sicherheits-Tasks – Objektlöschung
- Service-Tasks – Objektverwaltung
- Spoolverwaltung – Objektwiederherstellung
- Systemintegritätsverletzung – Netzwerkbasis-Tasks
- Netzwerkcluster-Tasks – Netzwerkausfall
- Netzwerk-Socket-Tasks – Sicherheitskonfiguration
- Sicherheits-Directory Service – Sicherheits-Interprozesskommunikation
- Authentifizierungsservice für Sicherheitsnetzwerk – Sicherheits-Runtime-Tasks
- Sicherheits-Socket-Deskriptoren – Sicherheitsüberprüfung
- Sicherheitsüberprüfungs-Tasks – Systemverwaltung
- Jobbasis-Tasks– Jobprofiländerungen (Thread-Ebene)
- OfficeVision-Tasks

Getätigte Änderungen werden direkt in den Systemwert QAUDLVL bzw. QAUDLVL2 übernommen.



Geben Sie hier die Aktion an, die durchgeführt werden soll, wenn das System keine Überwachungs-(Audit)einträge schreiben kann und Audit aktiv ist. Wenn die Sicherheitsrichtlinie für Ihr System vorschreibt, dass keine Verarbeitung ohne Überwachung stattfinden darf, müssen Sie „*System herunterfahren*“ aktivieren. Für die meisten Systeme wird der Wert „*Hinweis senden, dann fortfahren*“ empfohlen. Dieser Systemwert betrifft nur Überwachungseinträge, die das Betriebssystem an das Sicherheitsprotokolljournal (QAUDJRN) sendet.

Mögliche Werte sind:

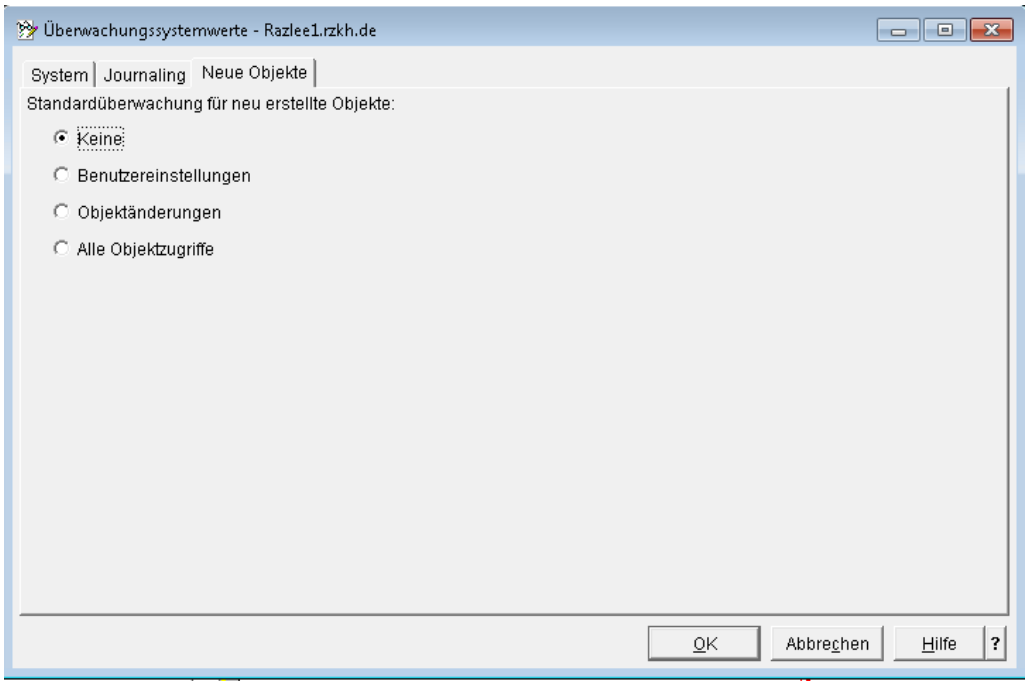
Hinweis senden, dann fortfahren
An die Nachrichtenwarteschlange des Systembedieners wird stündlich eine Nachricht gesendet, bis die Überwachung aktiviert wird.

System herunterfahren
Das System wird beendet, wenn der Versuch fehlschlägt, Überwachungsdaten an das Sicherheitsprotokoll zu senden. Wenn das System wieder eingeschaltet wird, befindet es sich im Status des eingeschränkten Betriebs. Der Systemwert „*Standardüberwachung für neu erstellte Objekte*“ wird auf „*keine*“ eingestellt, um die Überwachung zu deaktivieren. Beim nächsten Neustart muss der Benutzer, der sich am System anmeldet, mindestens über die Sonderberechtigungen *AUDIT (Überwachen) und *ALLOBJ (Berechtigung für alle Objekte) verfügen.

9.16.2.1.6
Seite 4

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	Überwachen (*AUDIT)
Empfohlene Einstellung:	Hinweis senden, dann fortfahren
Standardwert:	Hinweis senden, dann fortfahren
Änderungen werden wirksam:	sofort
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QAUDENDACN



Auf der Seite „Neue Objekte“ können Sie den Standardwert für die Überwachung von neu erstellten Objekten angeben. Der ausgewählte Wert richtet sich nach Ihren Überwachungsanforderungen.

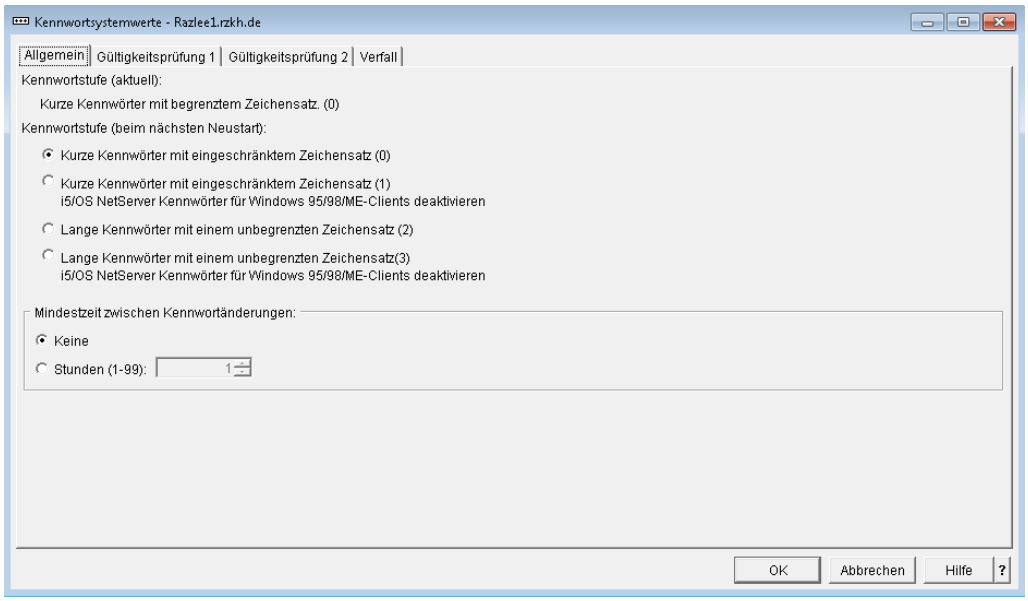
Zum Anzeigen der Überwachungssystemwerte benötigen Sie die Sonderberechtigung für alle Objekte (*ALLOBJ) oder Überwachungsberechtigung (*AUDIT). Ist keine geeignete Berechtigung vorhanden, ist die Kategorie Überwachung der Systemwerte nicht verfügbar

9.16.2.1.7 Kennwortsystemwerte

Auf der Seite „Allgemein“ können Sie die Kennwortstufe beim nächsten Neustart angeben.

Weitere ausführliche Hilfeinformationen können Sie zu folgenden Elementen dieses Fensters aufrufen:

- Kennwortstufe (aktuell)
- Kennwortstufe (beim nächsten Neustart)
- Mindestzeit zwischen Kennwortänderungen



„*Kennwortstufe (beim nächsten Neustart)*“ gibt die Stufe der Kennwortunterstützung auf dem System an.

Die Kennwortstufe des Systems kann so definiert werden, dass Benutzerprofilkennwörter mit 1 bis 10 Zeichen oder mit 1 bis 128 Zeichen verwendet werden können, oder auch so, dass eine Passphrase als Kennwortwert möglich ist. Der Begriff „Passphrase“ beschreibt einen Kennwortwert, der sehr lang sein kann und wenige (oder keine) Einschränkungen bezüglich der verwendeten Zeichen aufweist. In einer Passphrase sind Leerzeichen zwischen Buchstaben zulässig, wodurch ein Kennwortwert möglich ist, das einen Satz oder ein Satzfragment darstellt. Die einzige Einschränkung für eine Passphrase ist, dass sie nicht mit einem Stern (*) beginnen darf; abschließende Leerzeichen werden entfernt.

Eine Umstellung der Kennwortstufe des Systems von 1- bis 10-stelligen Kennwörtern auf 1- bis 128-stellige Kennwörter muss sorgfältig geplant werden. Überträgt Ihr System mit anderen Systemen in einem Netzwerk Daten, müssen alle Systeme die längeren Kennwörter akzeptieren.

9.16.2.1.7
Seite 2

Weitere Informationen, die vor einer Änderung dieses Systemwerts berücksichtigt werden müssen, finden Sie unter „Sicherheit“ im i5/OS Information Center. Wählen Sie „Verwandte Themen“ aus und anschließend das Handbuch „Security Reference“.

Folgende Optionen sind möglich:

Kurze Kennwörter mit begrenztem Zeichensatz. (0)
Das System unterstützt Benutzerprofilkennwörter mit einer Länge von 1 bis 10 Zeichen. Zulässige Zeichen sind die Buchstaben A bis Z, die Ziffern 0 bis 9 sowie die Sonderzeichen # (Nummernzeichen), $ (Dollarzeichen), @ (kommerzielles A) und _ (Unterstrich).

Dieser Wert sollte verwendet werden, wenn Ihr System mit anderen Systemen in einem Netzwerk Daten überträgt und wenn in diesen Systemen die Kennwortstufe 0 aktiviert ist oder ein Betriebssystemrelease vor V5R1M0 ausgeführt wird. Der Wert sollte außerdem verwendet werden, wenn Ihr System mit einem anderen System, in dem die Kennwortlänge auf 1 bis 10 Zeichen beschränkt ist, Daten austauscht.

Dieser Wert muss verwendet werden, wenn Ihr System mit der i5/OS-Unterstützung für Windows-Netzwerkumgebung (i5/OS NetServer) Daten überträgt und hierbei Kennwörter mit einer Länge von 1 bis 10 Zeichen verwendet.

Wird für die Kennwortstufe des Systems dieser Wert definiert, erstellt das Betriebssystem das verschlüsselte Kennwort für die Kennwortstufen 2 und 3. Die auf Stufe 0 verwendeten Kennwortzeichen sind die gleichen, die auch auf Stufe 2 und 3 verfügbar sind.

Kurze Kennwörter mit begrenztem Zeichensatz. Deaktivieren Sie i5/OS NetServer-Kennwörter für Windows 95/98/ME-Clients. (1)
Dieser Wert entspricht der Unterstützung für Kennwortstufe 0 mit folgender Ausnahme: i5/OS NetServer-Kennwörter für Windows 95/98/ME-Clients werden aus dem System entfernt. Wenn Sie Client-Unterstützung für i5/OS NetServer verwenden, können Sie diese Kennwortstufe (1) nicht verwenden.

NetServer für Windows 95/98/ME stellt keine Verbindung zum System her, wenn die Kennwortstufe 1 oder 3 lautet. NetServer-Kennwörter werden aus Sicherheitsgründen (die Kennwörter sind leicht zu entschlüsseln), das heißt auf Grund der unzureichenden Verschlüsselung von NetServer-Kennwörtern auf diesen Kennwortstufen aus dem System entfernt.

Lange Kennwörter mit einem unbegrenzten Zeichensatz. (2)
Dieser Wert unterstützt Benutzerprofilkennwörter mit 1 bis 128 Zeichen. Groß- und Kleinbuchstaben sind zulässig. Kennwörter dürfen beliebige Zeichen enthalten. Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden.

Diese Stufe wird als Kompatibilitätsstufe betrachtet. Wenn Sie sich bei einem System anmelden, dient das angegebene Kennwort zur Überprüfung der Berechtigung sowie für weitere kennwortbezogene Tests. Diese Stufe ermöglicht eine Rückkehr zu Kennwortstufe 0 oder 1, vorausgesetzt ein Kennwort erfüllt die Längen- und Syntaxbedingungen der Kennwortstufe 0 bzw. 1.

Diese Stufe kann verwendet werden, wenn Ihr System mit der i5/OS-Unterstützung für Windows-Netzwerkumgebung (i5/OS NetServer) Daten überträgt und wenn Ihr Kennwort 1 bis 14 Zeichen lang ist.

Diese Stufe können Sie nicht verwenden, wenn Ihr System mit folgenden Systemen kommuniziert:

- anderen Systemen in einem Netzwerk, in denen entweder die Kennwortstufe 0 oder 1 oder ein Betriebssystemrelease vor V5R1M0 aktiviert ist;
- einem anderen System, in dem die Kennwortlänge auf 1 bis 10 Zeichen beschränkt ist;
- Computern, die Client Access Version 5 Release 1 (V5R1) oder frühere Versionen verwenden.

Lange Kennwörter mit einem unbegrenzten Zeichensatz. Deaktivieren Sie i5/OS NetServer-Kennwörter für Windows 95/98/ME-Clients. (3)
Diese Stufe unterstützt Benutzerprofilkennwörter mit 1 bis 128 Zeichen. Groß- und Kleinbuchstaben sind zulässig. Kennwörter dürfen beliebige Zeichen enthalten und die Groß-/Kleinschreibung muss beachtet werden.

Bevor Sie die Kennwortstufe 3 angeben, lesen Sie Folgendes: Security Reference im i5/OS Information Center. Eine Zurückstufung von Kennwortstufe 3 auf Stufe 0 oder 1 ist nicht zulässig.

Diese Stufe können Sie nicht verwenden, wenn Ihr System mit folgenden Systemen kommuniziert:

- anderen Systemen in einem Netzwerk, in denen entweder die Kennwortstufe 0 oder 1 oder ein Betriebssystemrelease vor V5R1M0 aktiviert ist;
- einem anderen System, in dem die Kennwortlänge auf 1 bis 10 Zeichen beschränkt ist;
- Computern, die Client Access Version 5 Release 1 (V5R1) oder frühere Versionen verwenden
  oder wenn
- i5/OS-Unterstützung für eine Windows-Netzwerkumgebung (i5/OS NetServer) besteht.

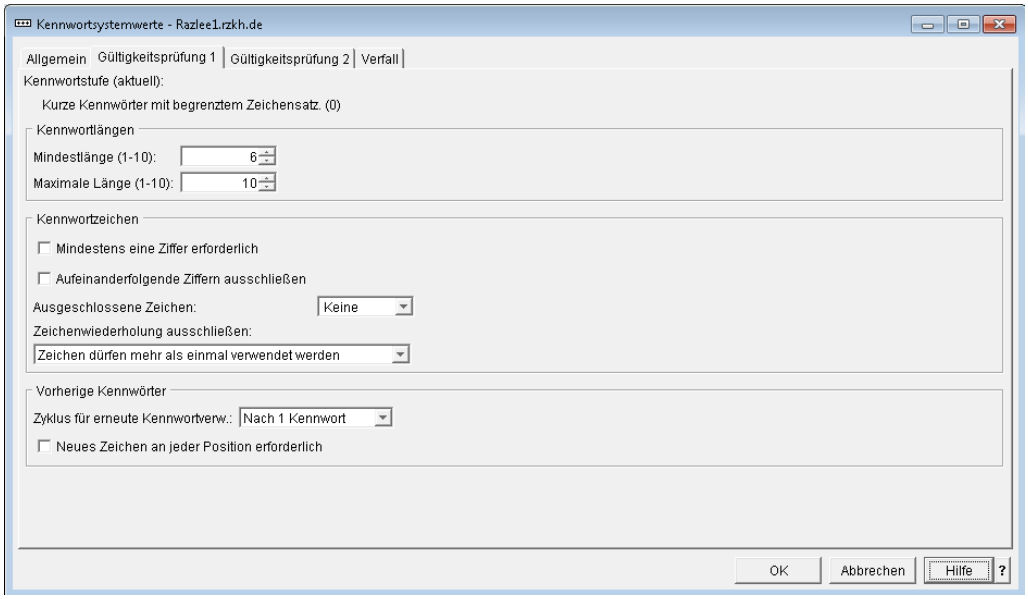
9.16.2.1.7
Seite 4

NetServer für Windows 95/98/ME stellt keine Verbindung zum System her, wenn die Kennwortstufe 1 oder 3 lautet. NetServer-Kennwörter werden aus Sicherheitsgründen (die Kennwörter sind leicht zu entschlüsseln), das heißt auf Grund der unzureichenden Verschlüsselung von NetServer-Kennwörtern, auf diesen Kennwortstufen aus dem System entfernt.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	kurze Kennwörter mit begrenztem Zeichensatz (0)
Änderungen werden wirksam:	beim nächsten Neustart des Systems
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QPWDLVL
Besondere Hinweise:	Eine Umstellung des Systemwerts für die Kennwortstufe von 3 auf 0 oder 1 ist nicht möglich. Der Systemwert für die Kennwortstufe muss hierbei zunächst von 3 nach 2 und dann nach 0 oder 1 umgestellt werden. Grund dieser Einschränkung ist, dass alle Kennwörter, die auf Kennwortstufe 0 oder 1 verwendet werden, aus dem System entfernt werden, wenn Sie die Kennwortstufe 3 festlegen. Solange sich das System auf Kennwortstufe 2 befindet, müssen Sie Ihre Benutzerprofile ändern und Ihnen ein Kennwort zuordnen, das auf Kennwortstufe 0 oder 1 (maximal 10 Zeichen pro Kennwort) gültig ist. Dann können Sie von Kennwortstufe 2 nach Stufe 0 oder 1 wechseln. Andernfalls haben die Benutzer keine Möglichkeit, sich an Ihrem System anzumelden. Weitere Informationen zur Überprüfung von Benutzerprofilen, um sicherzustellen, dass deren Kennwörter auch für die Kennwortstufe gültig sind, zu der Sie wechseln möchten, finden Sie unter *„Kennwort prüfen bei Änderung der Kennwortstufen“*.

Vorherige Kennwörter



Zyklus für erneute Kennwortverwendung

Gibt an, wie viele der vorherigen Kennwörter daraufhin geprüft werden, ob eine Übereinstimmung mit dem neuen Kennwort vorliegt. Diese Option bietet zusätzliche Sicherheit, da Benutzer bereits früher verwendete Kennwörter nicht mehr angeben können. Außerdem verhindert diese Option, dass ein Benutzer, dessen Kennwort verfallen ist, das Kennwort ändert und unmittelbar darauf wieder durch das alte Kennwort ersetzt.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Empfohlene Einstellung:	nach 10 oder mehr Kennwörtern
Standardwert:	nach einem Kennwort
Änderungen werden wirksam:	sofort
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QPWDRQDDIF

9.16.2.1.7
Seite 6

Kurzübersicht	
Besondere Hinweise:	Wählen Sie einen Wert von mindestens 10 aus, um die wiederholte Verwendung von Kennwörtern zu verhindern. Es wird empfohlen, eine Kombination aus den Werten *„Kennwortverfall"* und *„Zyklus für erneute Kennwortverwendung"* zu verwenden, um zu gewährleisten, dass die Wiederverwendung eines Kennworts für mindestens sechs Monate ausgeschlossen ist. Wählen Sie zum Beispiel *„30 Tage"* für *„Kennwortverfall"* (Tage nach letzter Änderung) und *„Nach 10 Kennwörtern"* für *„Zyklus für erneute Kennwortverwendung"* aus. Hierdurch kann ein normaler Benutzer, der sein Kennwort nach einer vom System ausgegebenen Warnung ändert, ein schon einmal verwendetes Kennwort für einen Zeitraum von ca. neun Monaten nicht wiederholen.

Neben der Angabe, wie viele vorherige Kennwörter auf Wiederholung geprüft werden, können Sie auch angeben, ob an jeder Position ein neues Zeichen erforderlich ist.

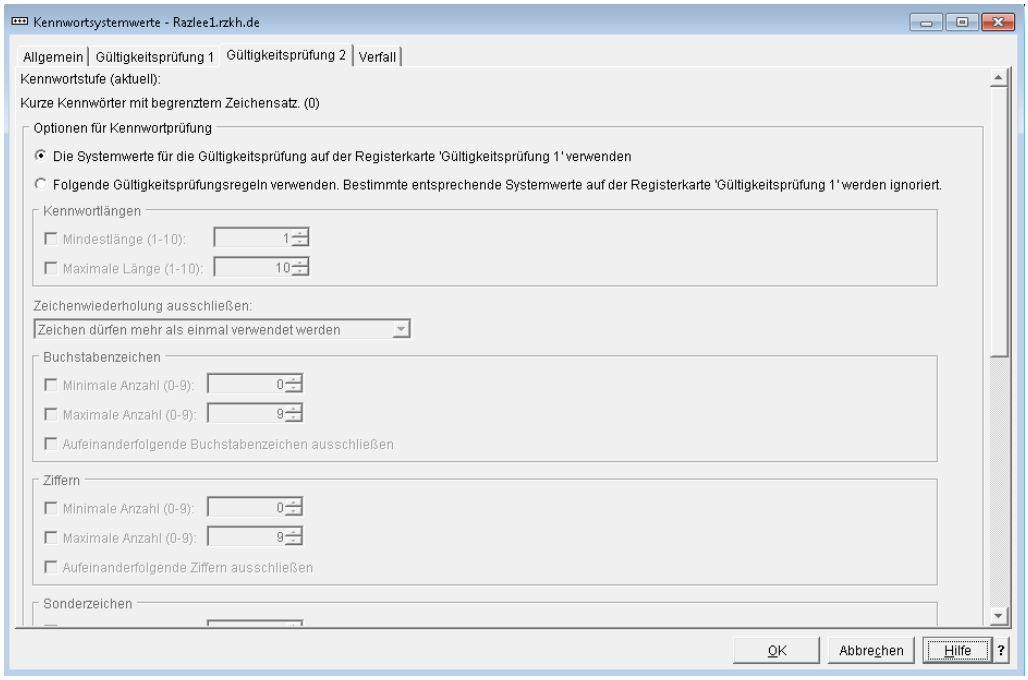
Neues Zeichen an jeder Position erforderlich
Gibt an, dass Sie in einem neuen Kennwort nicht das gleiche Zeichen an gleicher Stelle verwenden dürfen. Auf diese Weise wird verhindert, dass ein Benutzer ein Zeichen an einer Position in einem Kennwort angibt, an der sich das Zeichen bereits im vorherigen Kennwort befand. Das neue Kennwort DJS2 könnte zum Beispiel nicht verwendet werden, wenn das vorherige Kennwort DJS1 war (D, J und S sind an derselben Position).

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Sperrbar:	ja (klicken für weitere Details)
Änderungen werden wirksam:	sofort
Systemwert:	QPWDPOSDIF
Besondere Hinweise:	Auf Kennwortstufe 2 und 3 wird bei der Prüfung auf Zeichenwiederholungen die Groß-/Kleinschreibung berücksichtigt. Das heißt, ein Kleinbuchstabe und der entsprechende Großbuchstabe sind nicht identisch. Dieser Systemwert wird vom System ignoriert, wenn Sie die Verwendung der Werte auf der Registerkarte *„Gültigkeitsprüfung 2"* auswählen (Systemwert QPWDRULES).

9.16.2.1.7
Seite 8

Optionen für Kennwortprüfung



Gibt die Regeln an, mit denen überprüft wird, ob ein Kennwort korrekt ist. Eine Änderung dieses Systemwerts wird bei der nächsten Kennwortänderung wirksam.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	die Systemwerte für die Gültigkeitsprüfung auf der Registerkarte *„Gültigkeitsprüfung 1“* verwenden
Änderungen werden wirksam:	sofort – bei der nächsten Kennwortänderung
Sperrbar:	ja (klicken für weitere Details)
Systemwert:	QPWDRULES
Besondere Hinweise:	Wenn Sie die Verwendung der Gültigkeitsprüfungswerte auf dieser Registerkarte auswählen, werden bestimmte Werte auf der Registerkarte *„Gültigkeitsprüfung 1“* vom System ignoriert.

Mögliche Werte sind:

Die Systemwerte für die Gültigkeitsprüfung auf der Registerkarte „Gültigkeitsprüfung 1“ verwenden
Dieser Systemwert wird ignoriert und die anderen Systemwerte für Kennwörter werden verwendet, um zu überprüfen, ob ein Kennwort korrekt ist.

Folgende Gültigkeitsprüfungsregeln verwenden
Eine Änderung von Werten auf dieser Registerkarte führt dazu, dass bestimmte entsprechende Systemwerte auf der Registerkarte „Gültigkeitsprüfung 1“ vom System ignoriert werden.

Kennwortlängen

Mindestlänge (*MINLENnnn)
Gibt die Mindestanzahl der Zeichen für ein Kennwort an. Die gültigen Werte sind abhängig von der Kennwortstufe Ihres Systems. Wird Kennwortstufe 0 oder 1 angezeigt, lauten die gültigen Werte für die Mindestlänge 1 bis 10. Wird Kennwortstufe 2 oder 3 angezeigt, lauten die gültigen Werte für die Mindestlänge 1 bis 128.

Zum Ändern der Kennwortstufe wählen Sie die Seite „Allgemein“ und dann eine Stufe aus. Die auf dieser Seite vorgenommenen Änderungen werden beim nächsten Neustart des Systems wirksam.

Maximale Länge (*MAXLENnnn)
Gibt die maximale Anzahl der Zeichen für ein Kennwort an. Die gültigen Werte sind abhängig von der Kennwortstufe Ihres Systems. Wird Kennwortstufe 0 oder 1 angezeigt, lauten die gültigen Werte für die maximale Länge 1 bis 10. Wird Kennwortstufe 2 oder 3 angezeigt, lauten die gültigen Werte für die maximale Länge 1 bis 128.

Zum Ändern der Kennwortstufe wählen Sie die Seite „Allgemein“ und dann eine Stufe aus. Die auf dieser Seite vorgenommenen Änderungen werden beim nächsten Neustart des Systems wirksam.

9.16.2.1.7
Seite 10

Zeichenwiederholung ausschließen
Gibt an, ob Zeichenwiederholungen in einem Kennwort zulässig sind. Diese Option bietet zusätzliche Sicherheit, da Benutzer dann keine leicht zu erratenden Kennwörter (wie beispielweise Kennwörter, die aus der mehrfachen Wiederholung eines Zeichens bestehen) verwenden können.

Mögliche Werte sind:

Zeichen dürfen mehr als einmal verwendet werden
In einem Kennwort dürfen identische Zeichen mehr als einmal verwendet werden.

*Zeichen dürfen nicht mehr als einmal verwendet werden (*CHRLMTREP)*
In einem Kennwort darf ein Zeichen jeweils nur einmal verwendet werden.

*Zeichen dürfen nicht aufeinanderfolgend verwendet werden (*CHRLMTAJC)*
In einem Kennwort darf ein Zeichen mehrmals verwendet werden, aber nicht aufeinanderfolgend.

Buchstabenzeichen

Minimale Anzahl (*LTRMINn)
Gibt die minimale Anzahl der Buchstaben an, die im Kennwort enthalten sein muss.

Maximale Anzahl (*LTRMAXn)
Gibt die maximale Anzahl der Buchstaben an, die im Kennwort enthalten sein darf.

Aufeinanderfolgende Buchstabenzeichen ausschließen (*LTRLMTAJC)
Das Kennwort darf keine zwei oder mehr benachbarte (aufeinanderfolgende) Buchstabenzeichen enthalten.

Ziffern

Minimale Anzahl (*DGTMINn)
Gibt die minimale Anzahl Ziffern an, die im Kennwort enthalten sein muss.

Maximale Anzahl (*DGTMAXn)
Gibt die maximale Anzahl Ziffern an, die im Kennwort enthalten sein darf.

Aufeinanderfolgende Ziffern ausschließen (*DGTLMTAJC)
Das Kennwort darf keine zwei oder mehr benachbarte (aufeinanderfolgende) Ziffern enthalten.

Sonderzeichen

Minimale Anzahl (*SPCCHRMINn)
Gibt die minimale Anzahl Sonderzeichen an, die im Kennwort enthalten sein muss.

Maximale Anzahl (*SPCCHRMAXn)
Gibt die maximale Anzahl Sonderzeichen an, die im Kennwort enthalten sein darf.

Aufeinanderfolgende Sonderzeichen ausschließen (*SPCCHRLMTAJC)
Das Kennwort darf keine zwei oder mehr benachbarte (aufeinanderfolgende) Sonderzeichen enthalten.

Erstes Zeichen

Buchstaben ausschließen (*LTRLMTFST)
Das erste Zeichen des Kennworts darf kein Buchstabe sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Ziffern ausschließen*“ und „*Sonderzeichen ausschließen*“ angegeben werden. Wird das System mit der Kennwortstufe 0 oder 1 ausgeführt, kann nicht sowohl „*Buchstaben ausschließen*“ als auch „Sonderzeichen ausschließen“ angegeben werden.

Ziffern ausschließen (*DGTLMTFST)
Das erste Zeichen des Kennworts darf keine Ziffer sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Buchstaben ausschließen*“ und „*Sonderzeichen ausschließen*“ angegeben werden.

Sonderzeichen ausschließen (*SPCCHRLMTFST)
Das erste Zeichen des Kennworts darf kein Sonderzeichen sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Ziffern ausschließen*“ und „*Buchstaben ausschließen*“ angegeben werden. Wird das System mit der Kennwortstufe 0 oder 1 ausgeführt, kann nicht sowohl „*Buchstaben ausschließen*“ als auch „*Sonderzeichen ausschließen*“ angegeben werden.

9.16.2.1.7
Seite 12

Letztes Zeichen

Buchstaben ausschließen (*LTRLMTLST)
Das letzte Zeichen des Kennworts darf kein Buchstabe sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Ziffern ausschließen*“ und „*Sonderzeichen ausschließen*“ angegeben werden.

Ziffern ausschließen (*DGTLMTLST)
Das letzte Zeichen des Kennworts darf keine Ziffer sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Buchstaben ausschließen*“ und „*Sonderzeichen ausschließen*“ angegeben werden.

Sonderzeichen ausschließen (*SPCCHRLMTLST)
Das letzte Zeichen des Kennworts darf kein Sonderzeichen sein. Dieser Wert kann nicht angegeben werden, wenn auch „*Ziffern ausschließen*“ und „*Buchstaben ausschließen*“ angegeben werden.

Neues Zeichen an jeder Position des vorherigen Kennworts erforderlich (*LMTSAMPOS)
In einem Kennwort darf an einer Position nicht dasselbe Zeichen wie an derselben Position im vorherigen Kennwort verwendet werden.

Benutzerprofil im Kennwort ausschließen (*LMTPFRNAME)
Der Kennwortwert in Großbuchstaben darf nicht den vollständigen Namen des Benutzerprofils in aufeinanderfolgenden Positionen enthalten.

Minimale Anzahl Klein- und Großbuchstaben erforderlich (*MIXCASEn)
Das Kennwort muss mindestens n Großbuchstaben und n Kleinbuchstaben enthalten. Dieser Wert wird zurückgewiesen, wenn das System mit der Kennwortstufe 0 oder 1 ausgeführt wird, weil Kennwörter in Großbuchstaben angegeben werden müssen. Zum Ändern der Kennwortstufe wählen Sie die Seite „Allgemein“ und dann eine Stufe aus. Die auf dieser Seite vorgenommenen Änderungen werden beim nächsten Neustart des Systems wirksam.

Zeichen von mindestens drei der folgenden Zeichentypen erforderlich (*REQANY3)
Das Kennwort muss Zeichen von mindestens drei der folgenden vier Zeichentypen enthalten.

Gültige Werte:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Kennwortsystemwerte – Verfall
Auf der Seite „Verfall“ können Sie angeben, ob ein Kennwort in regelmäßigen Abständen geändert werden muss.

9.16.2.1.7

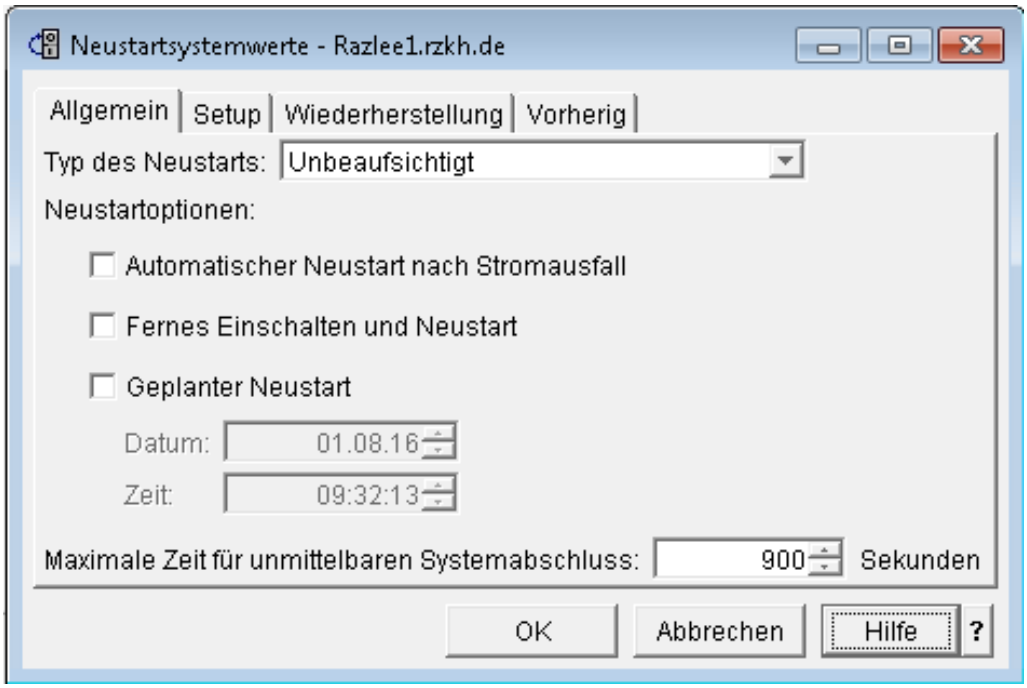
Seite 14

9.16.2.1.8 Neustart

Neustartsystemwerte – Allgemein
Auf der Seite „Allgemein“ können Sie sich den aktuell gültigen Typ des Neustarts für Ihr System anzeigen lassen und diesen ggf. ändern. Der Typ des Neustarts sowie die eingestellten Neustartoptionen führen zusammen den von Ihnen gewünschten Neustart im Falle eines Stromausfalls aus.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Typ des Neustarts
- Neustartoptionen
- Maximale Zeit für unmittelbaren Systemabschluss



Neustartoptionen
Gibt die Optionen für den Neustart Ihres Systems an.

Automatischer Neustart nach Stromausfall
Gibt an, dass das System automatisch erneut gestartet wird, sobald die Stromversorgung nach einem Stromausfall wiederhergestellt ist.

Auf partitionierten AS/400 7xx- und iSeries 8xx-Systemen kann diese Option nur auf der primären Partition ausgewählt werden. Verwenden Sie zum Auswählen dieser Option auf der primären Partition System i Navigator. Ob eine sekundäre Partition zur gleichen Zeit wie die primäre Partition neu gestartet wird, hängt von der ausgewählten Neustartoption für die sekundäre Partition ab.

9.16.2.1.8
Seite 2

Auf partitionierten System i-Produkten muss dieser Systemwert über die ASM-Schnittstelle (Advanced System Management) des Serviceprozessors geändert werden. Wenn Sie versuchen, diesen Wert über die Standardsystemwertschnittstellen zu ändern, tritt ein Fehler mit einer Fehlernachricht auf, die auf einen Serviceprozessorfehler verweist. Die Partitionen werden nur erneut gestartet, wenn das System erneut gestartet wird. Voraussetzung dafür ist, dass der automatische Neustart der Partition aktiviert ist. Der automatische Neustart ist für Partitionen aktiviert, die eingeschaltet sind. Der automatische Neustart kann aber auch für Partitionen aktiviert sein, die ausgeschaltet sind.

Anmerkung:

Der automatische Netzstromneustart ist für Partitionen gedrückt, die auf Grund eines Fehlers in der Stromversorgung ausgeschaltet werden.

Auf nicht partitionierten System i-Produkten kann dieser Wert auch mit System i Navigator definiert werden.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QPWRRSTIPL

Fernes Einschalten und Neustart
Gibt an, ob ein fernes Einschalten und ein ferner Neustart über eine Telefonleitung erfolgen können.

Auf partitionierten AS/400 7xx- und iSeries 8xx-Systemen kann diese Option nur auf der primären Partition ausgewählt werden. Verwenden Sie zum Auswählen dieser Option auf der primären Partition System i Navigator. Ob eine sekundäre Partition zur gleichen Zeit wie die primäre Partition neu gestartet wird, hängt von der ausgewählten Neustartoption für die sekundäre Partition ab.

Auf partitionierten System i-Produkten muss dieser Systemwert über die ASM-Schnittstelle (Advanced System Management) des Serviceprozessors geändert werden. Wenn Sie versuchen, diesen Wert über die Standardsystemwertschnittstellen zu ändern, tritt ein Fehler mit einer Fehlernachricht auf, die auf einen Serviceprozessorfehler verweist. Ob ein Neustart der Partitionen beim Neustart des Systems erfolgt, hängt von der Neustartoption ab, die für die jeweilige Partition im Profil der Hardware-Management-Konsole ausgewählt wurde.

Auf nicht partitionierten System i-Produkten kann dieser Wert auch mit System i Navigator definiert werden.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QRMTIPL
Besondere Hinweise:	Ein beliebiger Telefonanruf verursacht einen Neustart des Systems.

9.16.2.1.8
Seite 4

Geplanter Neustart
Gibt Datum und Uhrzeit für einen automatischen Neustart an.

Diesen Systemwert können Sie für jede Partition unabhängig definieren. Mit Hilfe von Partitionen können Ressourcen in einem einzelnen physischen System verteilt werden, so dass es wie zwei oder mehr unabhängige Systeme funktioniert. Wird die primäre Partition zu dem Zeitpunkt, zu dem ein automatischer Neustart in einer sekundären Partition erfolgen soll, ausgeschaltet, so findet der Neustart nicht statt. Wenn die primäre Partition erneut gestartet wird, wird auch die sekundäre Partition erneut gestartet, wenn das Datum und die Uhrzeit des Neustarts überschritten sind. Die sekundäre Partition wird nicht erneut gestartet, wenn sie mit der Neustartaktion „Anhalten" konfiguriert wurde.

Dieser Systemwert besteht aus zwei Teilen, Datum und Uhrzeit.

Datum
Gibt das Datum an, zu dem ein automatischer Neustart auf dem System erfolgt. Das Datum darf höchstens 11 Monate nach dem aktuellen Datum liegen.

Zeit
Gibt die Uhrzeit am angegebenen Datum an, zu der ein automatischer Neustart auf dem System erfolgt. Die angegebene Uhrzeit muss mindestens fünf Minuten nach der aktuellen Uhrzeit liegen.

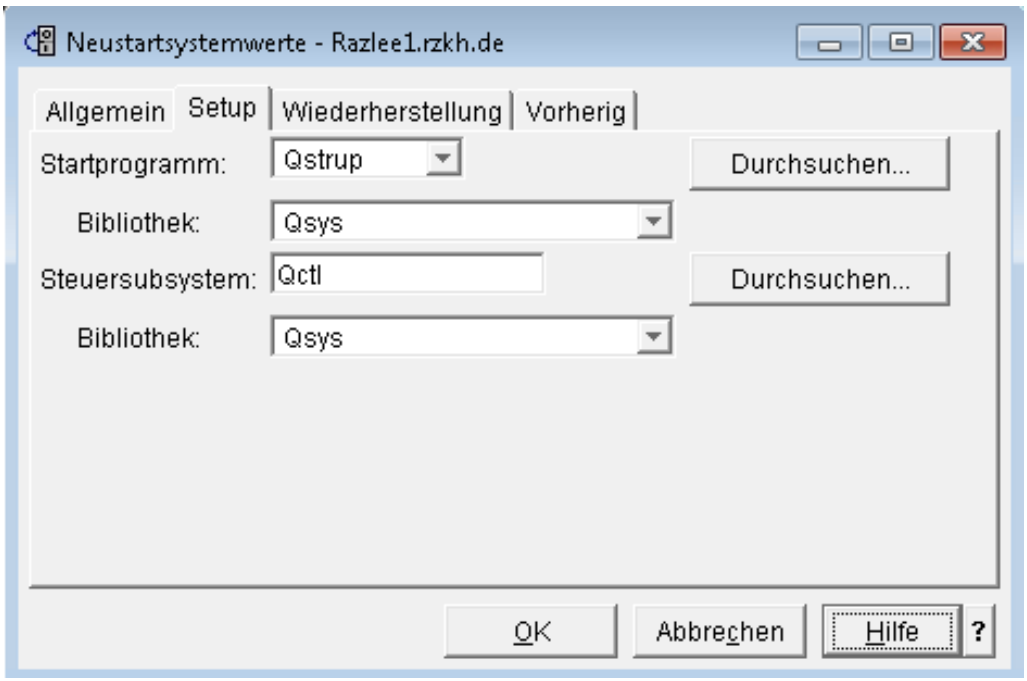
Wenn das Datum und die Uhrzeit zum Zeitpunkt des Systemabschlusses bereits verstrichen sind oder wenn das System aktiv ist, wenn das Datum und die Uhrzeit erreicht werden, wird kein Neustart durchgeführt. Nach dem geplanten Neustart wird der Systemwert so geändert, dass keine weiteren Neustarts terminiert werden. Diese Änderung erfolgt nur, wenn der geplante Neustart durchgeführt wird.

Wenn das System die Sommerzeit beachtet, können Sie Datum und Zeit nicht auf einen Zeitpunkt innerhalb der Stunde ändern, die durch die Sommerzeitumstellung betroffen ist. Wenn die Systemuhr zum Beispiel zur Umstellung auf die Sommerzeit am 6. April von 2:00 Uhr auf 3:00 Uhr springt, können Sie die Uhrzeit nicht auf einen Wert zwischen 2:00 Uhr und 3:00 Uhr am 6. April einstellen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QIPLDATTIM

Neustartsystemwerte – Setup



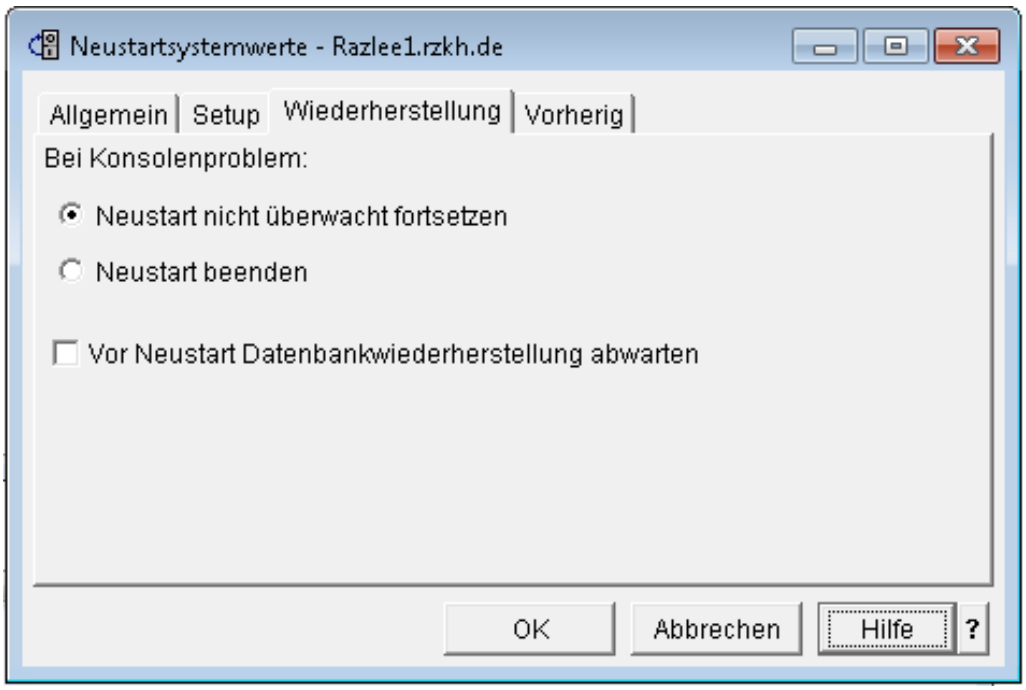
Auf der Seite „Setup“ können Sie sich anzeigen lassen oder angeben, mit welchem Programm das System gestartet wird. Auf dieser Seite können Sie außerdem das Steuersubsystem auswählen. Das Steuersubsystem ist das erste bei einem Neustart des Systems gestartete Subsystem.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Startprogramm
- Steuersubsystem

9.16.2.1.8
Seite 6

Neustartsystemwerte – Wiederherstellung

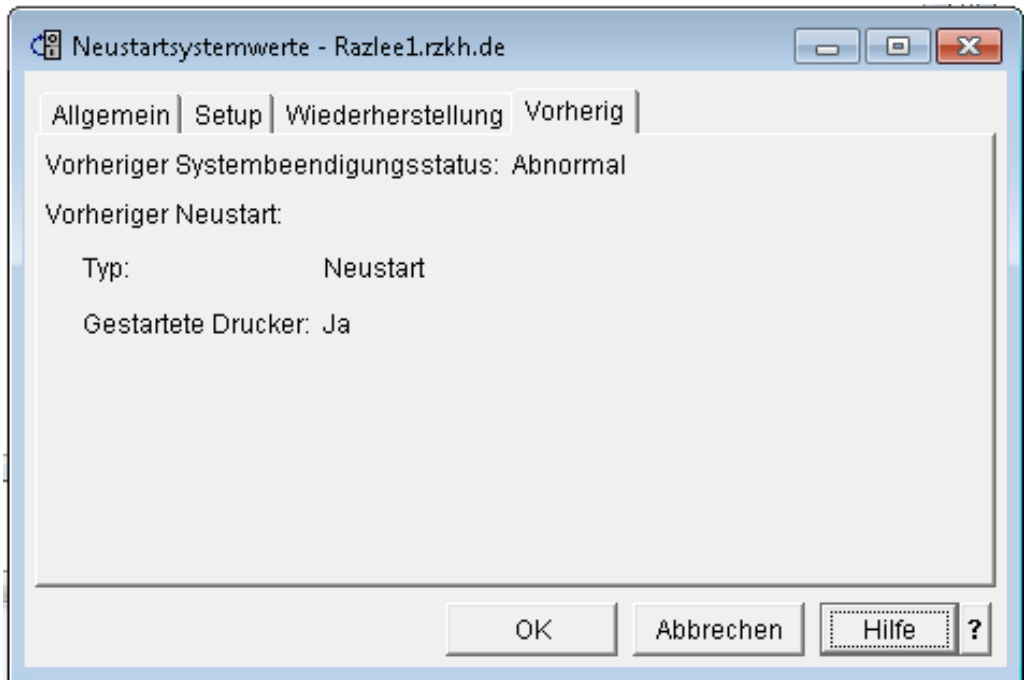


Auf der Seite „Wiederherstellung“ können Sie sich die Aktion anzeigen lassen oder ggf. ändern, die ausgeführt werden soll, wenn während des Neustarts ein Fehler auftritt.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Konsolproblem
- Vor Neustart Datenbankwiederherstellung abwarten

Neustartsystemwerte – Vorherig



Auf der Seite „Vorherig“ können Sie sich Informationen zum vorherigen Beendigungsstatus eines Systems und zum vorherigen Neustart anzeigen lassen.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Vorheriger Systembeendigungsstatus
- Vorheriger Neustart

9.16.2.1.8

Seite 8

9.16.2.1.9 Sicherheitswerte

Mit Hilfe der Sicherheitssystemwerte können Sie Sicherheitsmaßnahmen auf Ihrem System steuern. Die Sicherheitssystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- Allgemein
- Allgemeine Berechtigung
- Objekte der Benutzerdomäne
- Überprüfung (Diese Seite ist nur in Systemen verfügbar, auf denen OS/400 V5R3 oder i5/OS ausgeführt wird.)

Gemeinsam benutzter Speicher

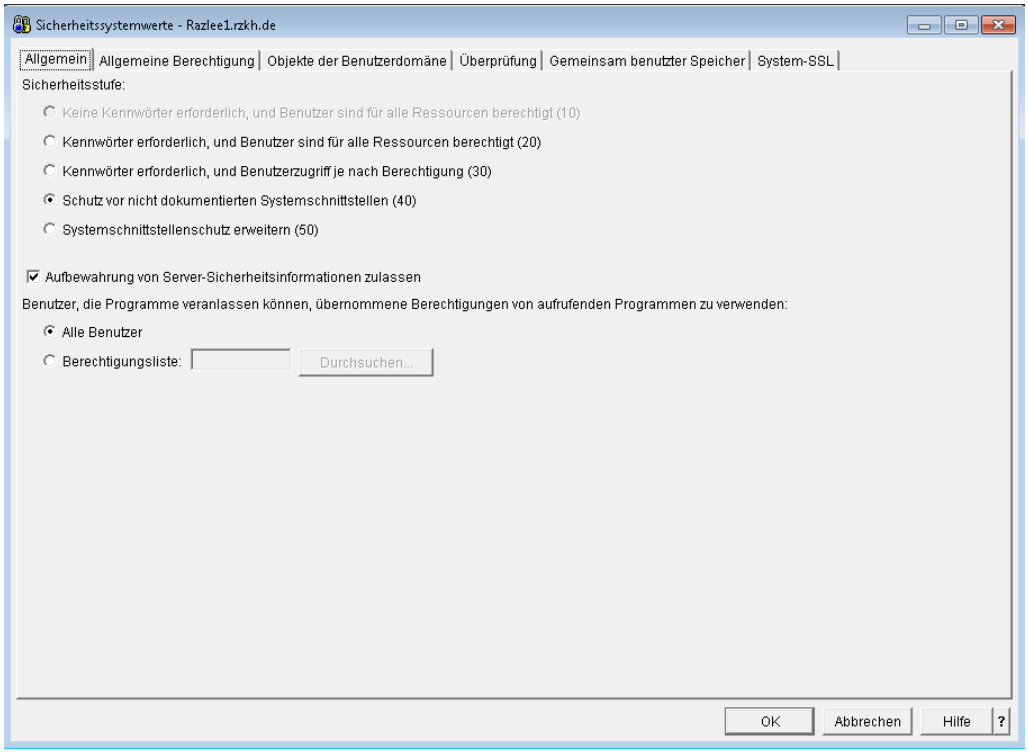
Anmerkung:

Wenn Sie noch mehr Kontrolle über sicherheitsbezogene Systemwerte benötigen, bieten die Systemservicetools (SST) und die dedizierten Servicetools (DST) eine Option zum Sperren sicherheitsbezogener Systemwerte. Damit können Sie verhindern, dass Benutzer sicherheitsrelevante Einstellungen ändern.

9.16.2.1.9

Seite 2

Sicherheitssystemwerte – Allgemein



Auf der Seite „Allgemein“ können Sie die Sicherheitsstufe für Ihr System und zusätzliche Systemsicherheitsinformationen angeben.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Sicherheitsstufe
- Aufbewahrung von Serversicherheitsinformationen zulassen
- Benutzer, die Programme veranlassen können, übernommene Berechtigungen von aufrufenden Programmen zu verwenden

Sicherheitssystemwerte – Allgemeine Berechtigung

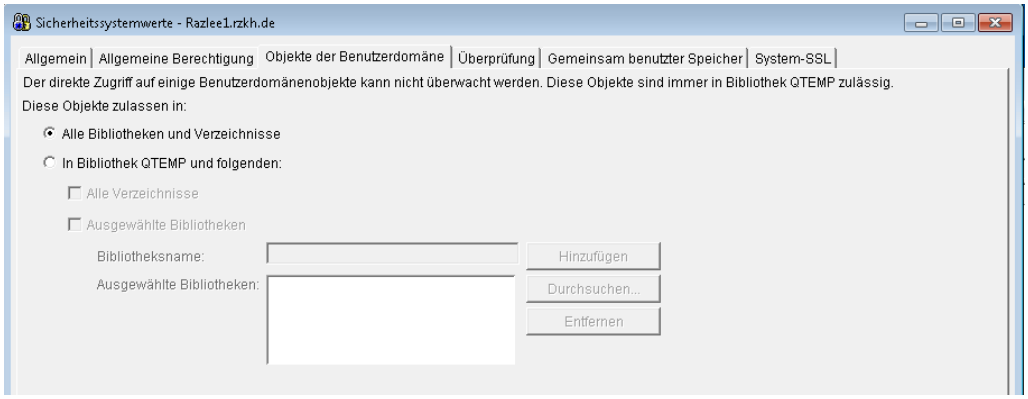
Auf der Seite „Allgemeine Berechtigung“ können Sie die allgemeine Standardberechtigung für jedes neu erstellte Objekt angeben. Sie können für jedes Objekt die verfügbare Zugriffsart für alle Systembenutzer festlegen, die über keine andere Berechtigung für das Objekt verfügen. Die allgemeine Berechtigung bietet guten Datenschutz bei guter Leistung.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

- Standardberechtigung für neu erstellte Objekte im Dateisystem QSYS.LIB

9.16.2.1.9
Seite 4

Sicherheitssystemwerte – Benutzerdomänenobjekte



Auf der Seite „Benutzerdomänenobjekte“ können Sie angeben, wo (außer in der Bibliothek QTEMP) sich nicht überwachbare Objekte befinden dürfen.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

Diese Objekte zulassen in
Wählen Sie aus, wo Benutzerdomänenobjekte, die nicht überwacht werden können, zulässig sind. Gelten in Ihrem System hohe Sicherheitsanforderungen, sollten Sie nur die Benutzerdomänenobjekte des Typs *USRSPC, *USRIDX und *USRQ in QTEMP angeben. Hierbei handelt es sich um die Benutzerdomänenobjektarten, die nicht überwachbar sind. Gültige Werte sind „Alle Bibliotheken und Verzeichnisse“ und „In Bibliothek QTEMP und folgenden“.

Alle Bibliotheken und Verzeichnisse
Überwachbare Objekte sind in allen Bibliotheken und Verzeichnissen zulässig. Das System verfügt über Mehrdateiensysteme. Bibliotheken gehören zum Dateisystem QSYS und Verzeichnisse gehören zu einem Dateisystem namens POSIX. Verzeichnisse werden als dem Dateisystem „Root“ oder „QOpenSys“ zugehörig betrachtet.

In Bibliothek QTEMP und folgenden
Sie können angeben, wo sich nicht überwachbare Objekte (außer in der Bibliothek QTEMP) befinden dürfen. Sie können eine der folgenden Optionen auswählen:

Alle Verzeichnisse
Nicht überwachbare Objekte sind in allen Verzeichnissen (außer der Bibliothek QTEMP) zulässig.

Ausgewählte Bibliotheken
Sie können Bibliotheken angeben, in denen Objekte zulässig sein sollen, die nicht überwachbar sind. Dieser Systemwert gibt bestimmte Bibliotheken an, die möglicherweise Benutzerdomänenversionen von Benutzerobjekten enthalten. Sie können bis zu 50 Bibliotheken auflisten. Wenn Sie eine Bibliotheksnamensliste angeben, treten in Anwendungen, die gegenwärtig mit Benutzerobjekten von Benutzerdomänen arbeiten, möglicherweise Fehler auf, wenn diese Anwendungen Objekte in Bibliotheken verwenden, die in der Liste nicht angegeben sind.

Bibliotheksname
Gibt den Namen der Bibliothek an, die hinzugefügt werden soll. Sie können einen Bibliotheksnamen angeben oder mit der Schaltfläche „Durchsuchen“ eine Bibliothek auswählen.

Ausgewählte Bibliotheken
Gibt die Bibliotheken an, in denen nicht überwachbare Objekte enthalten sein dürfen.

Gehen Sie wie folgt vor, um eine Bibliothek hinzuzufügen:

1. Geben Sie den Namen der Bibliothek im Feld „Bibliotheksname“ an oder wählen Sie mit der Schaltfläche „Durchsuchen“ eine Bibliothek aus.
2. Klicken Sie auf „Hinzufügen“.

Gehen Sie wie folgt vor, um eine Bibliothek zu entfernen:

1. Wählen Sie mindestens eine Bibliothek aus der Liste „Ausgewählte Bibliotheken“ aus.
2. Klicken Sie auf „Entfernen“.

Anmerkung:

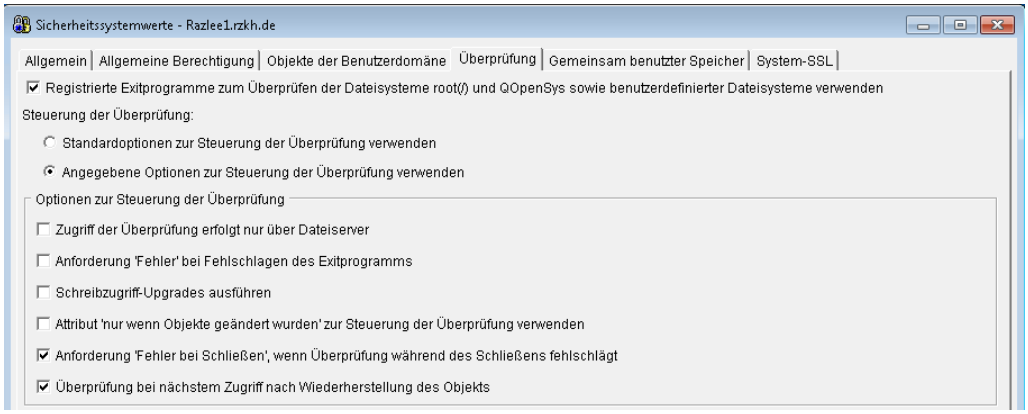
Um eine eventuelles Sicherheitsrisiko zu reduzieren, erstellen Sie die Bibliothek im Systemplattenpool, in einem Basisbenutzerplattenpool oder in allen unabhängigen Plattenpools, bevor sie sie zu diesem Systemwert hinzufügen. Geben Sie der Bibliothek die allgemeine Berechtigung *EXCLUDE.

9.16.2.1.9
Seite 6

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	alle Bibliotheken und Verzeichnisse
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QALWUSRDMN
Besondere Hinweise:	Alle ausgewählten Bibliotheken sollten allgemeine Ausschlussberechtigung haben. Wenn Sie eine Anwendung ausführen, die Benutzerdomänenobjekte des Typs *USRIDX, *USRQ und *USRSPC benötigen, muss ihre Bibliothek in diese Liste aufgenommen werden. Diese Liste muss die Bibliothek QRCL enthalten, damit Benutzerdomänenobjekte während der Verarbeitung des Befehls RCLSTG (Reclaim Storage) wiederhergestellt werden können. Ist die Bibliothek während der Verarbeitung des Befehls RCLSTG nicht richtig definiert, werden Benutzerdomänenobjekte gelöscht.

Steuerung der Überprüfung



Gibt die Optionen für die Überprüfung an. Diese Optionen steuern die Überprüfung des Integrated File System auf dem System, wenn Exitprogramme bei einem der überprüfungsbezogenen Ausstiegspunkte des Integrated File System registriert sind.

Standardoptionen zur Steuerung der Überprüfung verwenden
Gibt an, dass das System folgende Überprüfungsoptionen verwendet, wenn die registrierten Exitprogramme aufgerufen werden:

- Schreibzugriff-Upgrades ausführen
- Anforderung „Fehler bei Schließen“, wenn Überprüfung während des Schließens fehlschlägt
- Überprüfung bei nächstem Zugriff nach Wiederherstellung des Objekts

Angegebene Optionen zur Steuerung der Überprüfung verwenden Ermöglicht Ihnen auszuwählen, welche Überprüfungsoptionen das System verwenden soll, wenn die registrierten Exitprogramme aufgerufen werden. Wählen Sie eine der folgenden „Optionen zur Steuerung der Überprüfung“ aus:

Zugriff der Überprüfung erfolgt nur über Dateiserver
Wenn Sie diese Option auswählen, werden nur Systemzugriffe von Dateiservern aus überprüft. Dazu zählen auch Zugriffe über Network File System (NFS) und andere Dateiservermethoden. Native oder direkte Verbindungen zum System werden jedoch nicht überprüft. Wenn diese Option nicht ausgewählt ist, wird jede Art von Zugriff überprüft. Dabei ist es unerheblich, ob der Zugriff direkt auf das System oder über einen Dateiserver erfolgt.

9.16.2.1.9
Seite 8

Anforderung „Fehler“ bei Fehlschlagen des Exitprogramms
Wenn Sie diese Option auswählen, legen Sie fest, dass die Anforderung oder Operation fehlschlägt, die den Aufruf des Exitprogramms ausgelöst hat, wenn beim Aufrufen des Exitprogramms Fehler auftreten.
Mögliche Fehler: Das Programm wurde nicht gefunden oder das Programm ist nicht ordnungsgemäß codiert, um die Anforderung des Exitprogramms verarbeiten zu können. Wenn dies der Fall ist, erhält die angeforderte Operation die Meldung, dass die Überprüfung des Objekts fehlgeschlagen ist. Wenn diese Option nicht ausgewählt ist, überspringt das System das fehlgeschlagene Programm und behandelt das Objekt so, als wäre es nicht von diesem Exitprogramm überprüft worden.

Schreibzugriff-Upgrades ausführen
Wenn Sie diese Option auswählen, geben Sie an, dass das System ein Zugriffsupdate des Überprüfungsdeskriptors durchführen darf, der an das Exitprogramm zum Einschließen des Schreibzugriffs übergeben wurde, falls dies möglich ist. Verwenden Sie diese Option, wenn das Exitprogramm in der Lage sein soll, Objekte zu berichtigen oder zu ändern, auch wenn diese nur mit Lesezugriff geöffnet wurden. Wenn diese Option nicht ausgewählt ist, stellt das System den Zugriff nicht auf Schreibzugriff um.

Attribut „Nur wenn Objekte geändert wurden“ zur Steuerung der Überprüfung verwenden
Wenn Sie diese Option auswählen, verwendet das System die Angabe des Attributs „Nur Objektänderung“, um das Objekt nur dann zu überprüfen, wenn es geändert wurde (und nicht auch weil die Prüfsoftware eine Aktualisierung ausweist). Wenn diese Option nicht angegeben wurde, wird das Attribut „Nur Objektänderung“ nicht verwendet und das Objekt wird durchsucht, nachdem es geändert wurde und die Prüfsoftware eine Aktualisierung ausweist.

Anforderung „Fehler bei Schließen“, wenn Überprüfung während des Schließens fehlschlägt
Ist diese Option ausgewählt, schlägt die Anforderung zum Schließen fehl, wenn die Überprüfung eines Objekts während der Schließverarbeitung fehlschlägt. Diese Option gilt nur für Schließanforderungen.

Ist diese Option nicht ausgewählt, schlägt eine Schließanforderung nicht fehl, wenn die Überprüfung eines Objekts fehlschlägt. Die Schließanforderung schlägt auch dann nicht fehl, wenn die Option „Anforderung ‚Fehler‘ bei Fehlschlagen des Exitprogramms“ ausgewählt ist.

Wenn zum Beispiel die Option „Anforderung ‚Fehler' bei Fehlschlagen des Exitprogramms" ausgewählt ist, und die Option „Anforderung „Fehler bei Schließen", wenn Überprüfung während des Schließens fehlschlägt" nicht ausgewählt ist, sendet das System keinen Fehlerhinweis, auch wenn die Überprüfung eines Objekts während der Schließverarbeitung fehlgeschlagen ist. Das Objekt erhält aber eine Markierung, aus der hervorgeht, dass seine Überprüfung fehlgeschlagen ist.

Überprüfung bei nächstem Zugriff nach Wiederherstellung des Objekts Wenn Sie diese Option auswählen, werden Objekte mindestens einmal nach der Wiederherstellung überprüft; dies erfolgt unabhängig vom Objektüberprüfungsattribut. Wenn das Objektüberprüfungsattribut angibt, dass das Objekt nicht überprüft wird, wird das Objekt einmal direkt nach seiner Wiederherstellung überprüft. Wenn das Objektüberprüfungsattribut angibt, dass das Objekt nur überprüft wird, wenn es seit der letzten Überprüfung geändert worden ist, wird das Objekt nach seiner Wiederherstellung überprüft, weil die Wiederherstellung als Änderung des Objekts angesehen wird.

Wenn diese Option nicht ausgewählt ist, werden die Objekte nicht überprüft, weil sie wiederhergestellt wurden. Die Überprüfung hängt von den Überprüfungsattributen jedes Objekts ab.

In der Regel ist es sinnvoll, wiederhergestellte Objekte mindestens einmal zu überprüfen. Sie sollten diese Option jedoch nicht auswählen, wenn Sie wissen, dass die Objekte, die wiederhergestellt werden, vor dem Speichern überprüft wurden oder dass sie aus einer sicheren Quelle stammen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Standardoptionen zur Steuerung der Überprüfung verwenden
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QSCANFSCTL

9.16.2.1.9
Seite 10

Sicherheitssystemwerte – Gemeinsam benutzter Speicher

Auf der Seite „Gemeinsam benutzter Speicher“ können Sie angeben, ob der Zugriff auf gemeinsam benutzten Speicher und auf Datenstromdateien im adressierbaren Speicher zulässig ist.

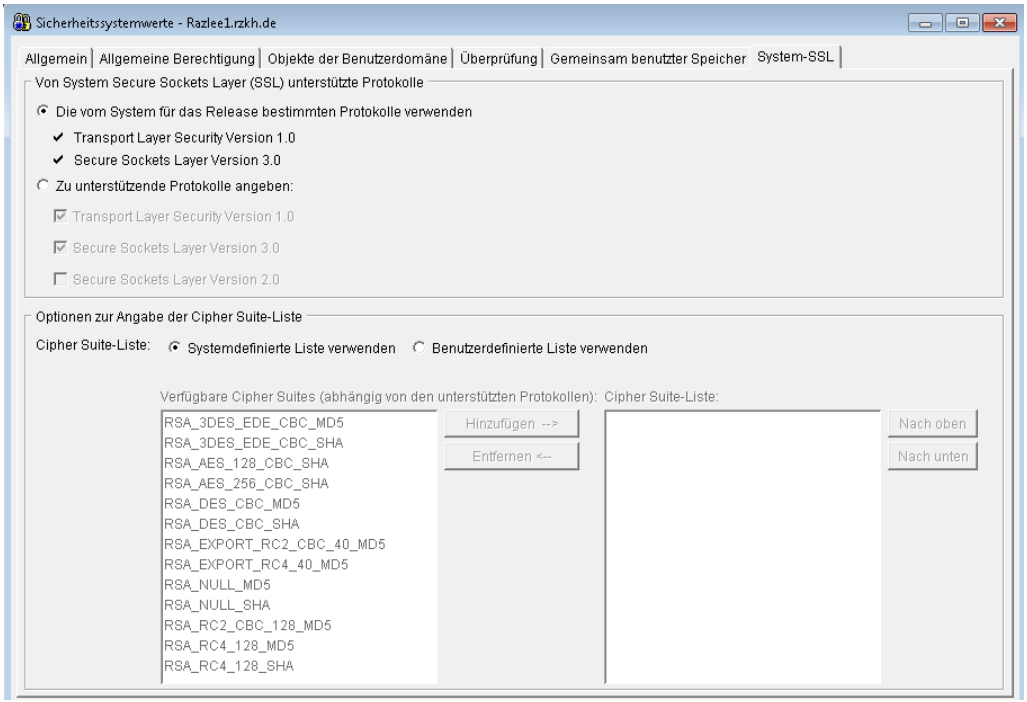
Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

Verwendung von gemeinsamem oder adressiertem Speicher mit Schreibberechtigung zulassen
Gibt an, ob Benutzer gemeinsam benutzten Speicher oder Datenstromdateien im adressierbaren Speicher verwenden können. Wählen Sie aus, ob der Zugriff auf den gemeinsam benutzten Speicher oder die Verwendung von Datenstromdateien im adressierbaren Speicher zulässig ist. Mit dieser Option können Benutzer APIs im gemeinsam benutzten Speicher (zum Beispiel shmat() – Shared Memory Attach API) und Objekte im adressierbaren Speicher mit Datenstromdateien (zum Beispiel mmap() – Memory Map a File API) verwenden. Der Zugriff auf den gemeinsam benutzten Speicher und auf Datenstromdateien im adressierbaren Speicher wird in Umgebungen empfohlen, in denen Zeiger von Programmen, die in verschiedenen Jobs ausgeführt werden, gemeinsam benutzt werden. Diese Einstellung wird jedoch in Umgebungen mit hohen Sicherheitsanforderungen nicht empfohlen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QSHRMEMCTL

Von System Secure Sockets Layer (SSL) unterstützte Protokolle



Gibt die von System-SSL unterstützten SSL-Protokollversionen an.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	Systemkonfiguration (*IOSYSCFG), alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	die vom System für das Release bestimmten Protokolle verwenden
Änderungen werden wirksam:	sofort für alle nachfolgenden SSL-Sitzungen des Systems
Sperrbar:	ja
Systemwert:	QSSLPCL

9.16.2.1.9

Seite 12

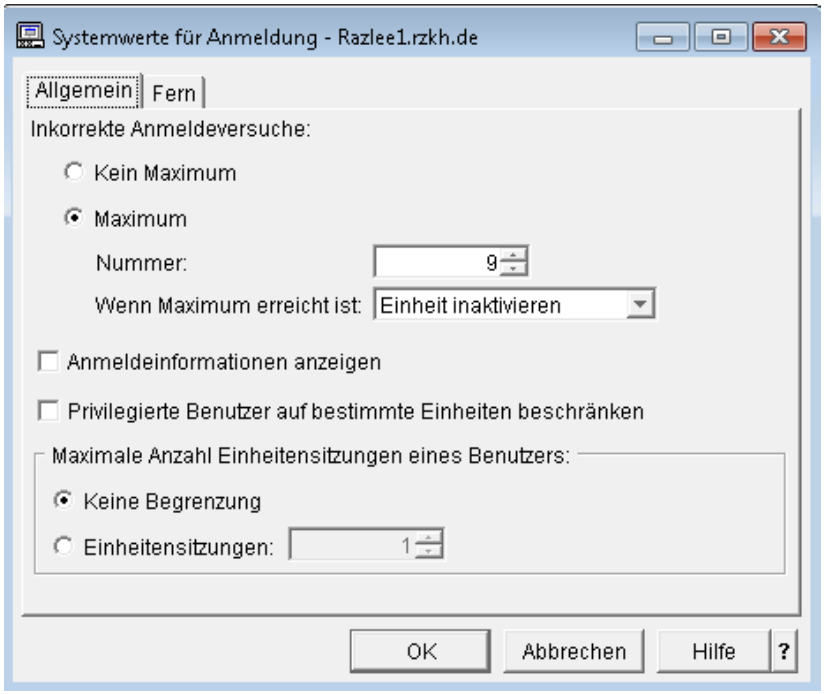
9.16.2.1.10 Anmeldung

Übersicht über Anmeldesystemwerte

Mit Hilfe der Anmeldesystemwerte können Sie sich Anmeldeinformationen anzeigen lassen oder diese steuern. Sie können die Anzahl der ungültigen Anmeldeversuche festlegen, um die Sicherheit Ihres Systems zu erhöhen. Die Anmeldesystemwerte sind in Gruppen unterteilt. Sie können ausführliche Hilfe zu bestimmten Systemwerten innerhalb der folgenden Gruppen finden:

- Allgemein
- Fern

Systemwerte für Anmeldung – Allgemein



Auf der Seite „Allgemein“ können Sie sich die zulässige Anzahl Anmeldeversuche eines Benutzers anzeigen lassen oder diese Anzahl ändern. Außerdem können Sie angeben, dass die Anmeldeinformationen nach der Anmeldung des Benutzers angezeigt werden. Auf dieser Seite können Sie außerdem die Benutzerberechtigungen und die Anzahl der Einheitensitzungen einschränken.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Ungültige Anmeldeversuche
- Anmeldeinformationen anzeigen
- Privilegierte Benutzer auf bestimmte Einheiten beschränken
- Für jeden Benutzer nur eine Einheitensitzung zulassen
- Maximale Anzahl Einheitensitzungen eines Benutzers

9.16.2.1.10
Seite 2

Ungültige Anmeldeversuche
Gibt an, wie viele ungültige Anmeldeversuche ein Benutzer ausführen darf und welche Aktion bei Erreichen der maximal zulässigen Anzahl Anmeldeversuche durchgeführt werden soll. Es wird eine Nachricht an die Systemnachrichtenwarteschlange gesendet, falls vorhanden. Andernfalls wird die Nachricht an den Systembediener gesendet. Ein Anmeldeversuch ist ungültig, sobald eine der folgenden Bedingungen zutrifft:

- Eine Benutzer-ID ist ungültig.
- Ein Kennwort ist ungültig.
- Das Benutzerprofil hat keine Berechtigung für die Einheit, von der die Benutzer-ID eingegeben wurde.

Ein Anmeldeversuch wird nicht als ungültiger Versuch betrachtet, wenn eine der folgenden Bedingungen vorliegt:

- Kennwörter sind erforderlich und das Benutzerprofil gibt kein erforderliches Kennwort an. Der Benutzer empfängt eine Nachricht, die darauf hinweist, das dem Benutzerprofil kein Kennwort zugeordnet ist.
- Die Programm- oder Menünamen sind ungültig.
- Das Benutzerprofil ist nicht vorhanden, und das System ist mit Sicherheitsstufe 10 konfiguriert.

Die angegebene aktuelle Bibliothek wird nicht gefunden.

Mögliche Werte sind:

Kein Maximum
Für die Anzahl der Anmeldeversuche gibt es keinen Maximalwert.

Maximale Anzahl
Maximal zulässige Anzahl der Anmeldeversuche.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	3
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QMAXSIGN

Wenn Sie eine maximal zulässige Anzahl aufeinanderfolgender Anmeldeversuche angeben, können Sie auch festlegen, wie das System reagiert, wenn dieser Grenzwert erreicht wird.

Mögliche Werte sind:

Einheit deaktivieren
Die Einheit wird abgehängt, wenn der Grenzwert erreicht wird. Befindet sich das Steuersubsystem im Status des eingeschränkten Betriebs (so dass nur eine Einheit darin verwendet werden kann) und wird die Einheit abgehängt, wird das System beendet und Lampen an der Steuerkonsole leuchten auf, um anzuzeigen, dass Sie das System erneut starten müssen.

Benutzer deaktivieren
Das Benutzerprofil wird deaktiviert, wenn der Grenzwert erreicht wird. Wenn ein Profil deaktiviert wird, muss es zunächst wieder aktiviert werden, damit sich der Benutzer anmelden kann.

Benutzer und Einheit deaktivieren
Die Einheit wird abgehängt und das Benutzerprofil deaktiviert, sobald der Grenzwert erreicht wird.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Benutzer und Einheit deaktivieren
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QMAXSGNACN

Anmeldeinformationen anzeigen
Dieser Systemwert legt fest, ob der Benutzer eine Informationsanzeige bei der Anmeldung sieht, die das Datum und die Uhrzeit der letzten Anmeldung sowie die Anzahl der ungültigen Anmeldeversuche seit der letzten Anmeldung enthält.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QDSPSGNINF

9.16.2.1.10
Seite 4

Privilegierte Benutzer auf bestimmte Einheiten beschränken
Gibt an, ob Benutzer mit einer Berechtigung für alle Objekte (*ALLOBJ) und einer Serviceberechtigung (*SERVICE) eine explizite Berechtigung für bestimmte Datenstationen benötigen.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QLMTSECOFR

Für jeden Benutzer nur eine Einheitensitzung zulassen

Gibt an, ob sich ein Benutzer an mehreren Datenstationen anmelden kann. Dies verhindert nicht die Verwendung von Gruppenjobs oder das Übergeben einer Systemanfrage an der Datenstation.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QLMTDEVSSN

Maximale Anzahl Einheitensitzungen eines Benutzers
Gibt an, ob sich ein Benutzer an mehreren Datenstationen anmelden kann. Dies verhindert nicht die Verwendung von Gruppenjobs oder das Übergeben einer Systemanfrage an der Datenstation.

Mögliche Werte sind:

Keine Begrenzung:
Gibt an, dass ein Benutzer auf eine Workstation beschränkt ist.

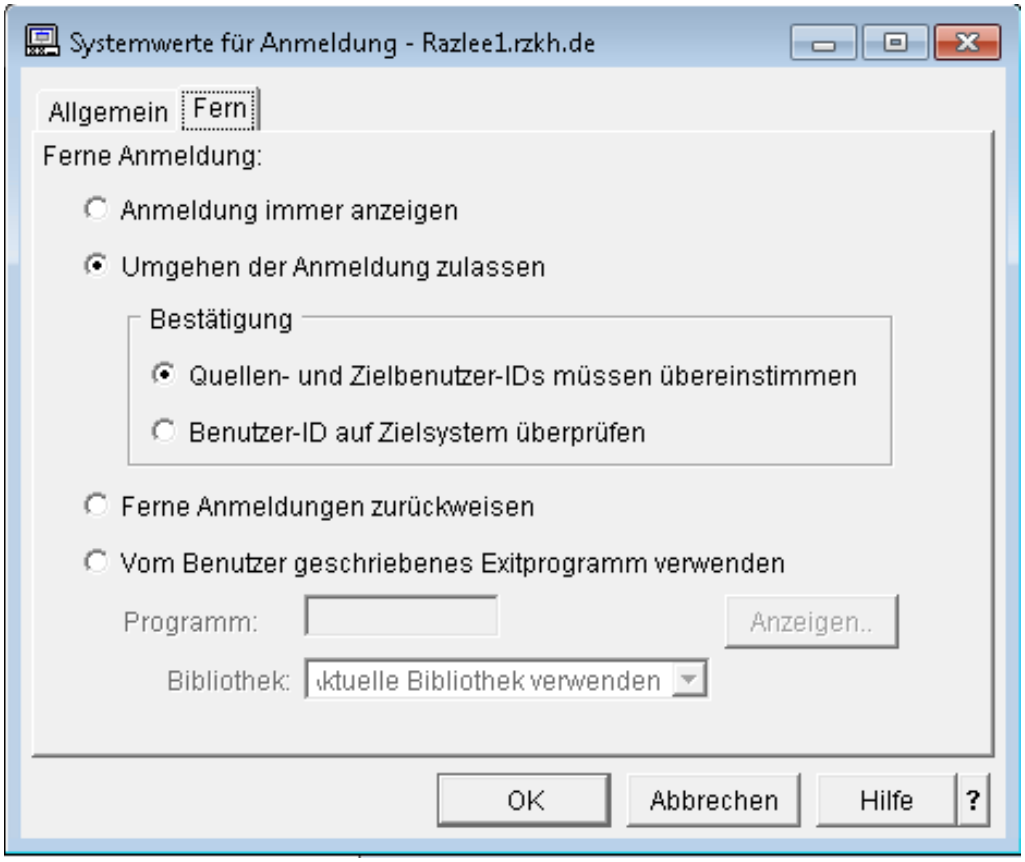
Einheitensitzungen:
Geben Sie eine Zahl im Bereich von 1 bis 9 an.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	keine Begrenzung
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QLMTDEVSSN

9.16.2.1.10
Seite 6

Anmeldesystemwerte – Fern



Auf der Seite „Fern“ können Sie angeben, wie das System Anforderungen für ferne Anmeldung behandeln soll.

Weitere ausführliche Hilfeinformationen können Sie zum folgenden Element dieses Fensters aufrufen:

- Ferne Anmeldung

Ferne Anmeldung
Gibt Optionen für die ferne Anmeldung an. Folgende Optionen sind möglich:

Anmeldung immer anzeigen
Alle fernen Anmeldesitzungen müssen die normale Anmeldeverarbeitung durchlaufen.

Übergehen der Anmeldung zulassen
Das System gestattet dem Benutzer, die Anmeldung zu übergehen.

Überprüfung
Wenn Sie die Anmeldung übergehen möchten, können Sie auch angeben, dass die Quellen- und Zielbenutzer-IDs überprüft oder die Benutzer-IDs nur auf dem Zielsystem überprüft werden. Die Anmeldung wird zwar umgangen, aber die Benutzer-ID wird überprüft, bevor Zugriff auf das System gewährt wird.

Quellen- und Zielbenutzer-IDs müssen übereinstimmen
Bei 5250-Datensichtgerätsdurchgriff oder Datenstationsfunktionen können Sie die Fernanmeldungsanzeige übergehen, wenn Quellen- und Zielbenutzerprofilnamen identisch sind.

Benutzer-ID auf Zielsystem prüfen
Das System gestattet dem Benutzer, die Anmeldeanzeige zu übergehen, nachdem überprüft wurde, ob der Benutzer Zugriffsberechtigung für das System besitzt.

Ferne Anmeldungen zurückweisen
Gestattet keine ferne Anmeldung für 5250-Datensichtgerätsdurchgriff und Datenstationsfunktion. Wenn diese Option ausgewählt wird, kann sich der Benutzer weiterhin über Telnet am System anmelden. Diese Sitzungen durchlaufen die normale Anmeldeverarbeitung. Wollen Sie alle Telnet-Anforderungen an das System zurückweisen, müssen Sie den Telnet-Server beenden.

Benutzerdefiniertes Exitprogramm
Sie können ein Programm und eine Bibliothek angeben, um zu entscheiden, welche fernen Sitzungen zulässig sind und welche Benutzerprofile von welchen Standorten aus automatisch angemeldet werden können. Das Programm muss im Systemplattenpool (auch Zusatzspeicherpool genannt) oder in einem Basisbenutzerplattenpool vorhanden sein.

Programm
Geben Sie einen Namen aus bis zu zehn Zeichen für das Programm an oder wählen Sie mit der Schaltfläche „Durchsuchen“ ein Programm aus.

Bibliothek
Gibt den Namen der Bibliothek an, die das Programm enthält. Geben Sie einen Bibliotheksnamen aus maximal 10 Zeichen an oder wählen Sie eine der folgenden Optionen aus:

Bibliotheksliste verwenden
Alle Bibliotheken in der Bibliotheksliste auf dem System werden durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich das Programm befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director wird der Bibliotheksname angezeigt und nicht „Bibliotheksliste verwenden“. Wenn das Programm nicht gefunden wird, wird der Wert „Bibliotheksliste verwenden“ angezeigt.

9.16.2.1.10
Seite 8

Aktuelle Bibliothek verwenden
Die aktuelle Bibliothek, die der aktuellen Sitzung auf dem System zugeordnet ist, wird durchsucht. Wenn keine aktuelle Bibliothek angegeben wurde, wird QGPL durchsucht. Wenn Sie diese Option auswählen, wird im Bibliotheksfeld automatisch die Bibliothek angegeben, in der sich das Programm befindet. Beim nächsten Öffnen von System i Navigator oder IBM Systems Director wird der Bibliotheksname angezeigt und nicht „Aktuelle Bibliothek verwenden". Wenn das Programm nicht gefunden wird, wird der Wert „Aktuelle Bibliothek verwenden" angezeigt.

Bibliotheksname
Gibt den Namen der Bibliothek an, die das Programm enthält.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	nicht ausgewählt
Änderungen werden wirksam:	sofort
Sperrbar:	ja
Systemwert:	QRMTSIGN

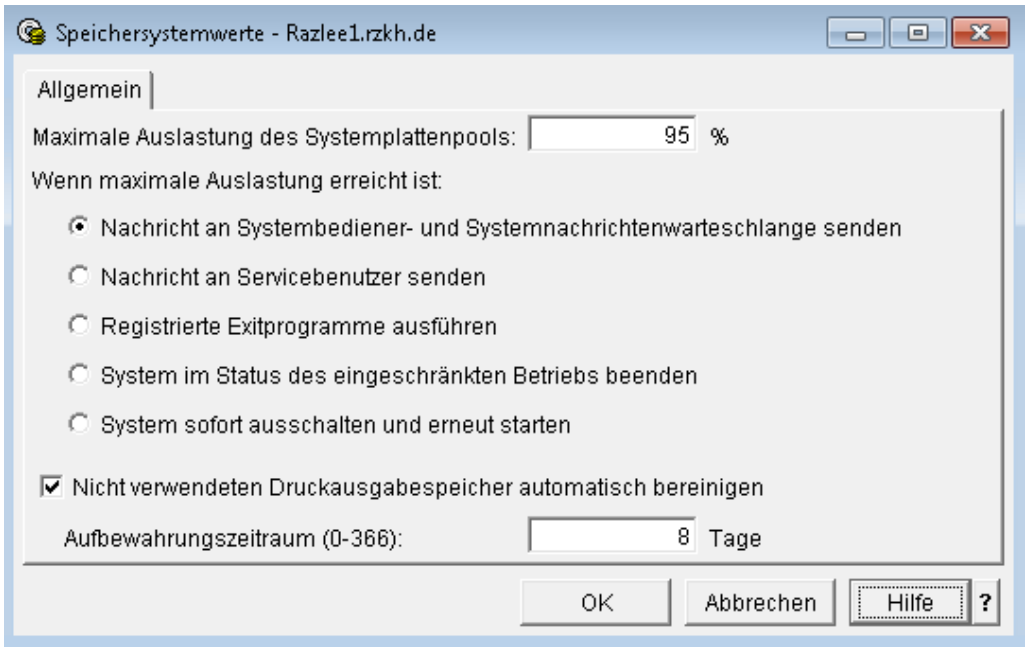
9.16.2.1.11 System- und Benutzerstandardwerte

Speichersystemwerte – Allgemein
Auf der Seite „Allgemein“ können Sie sich die Speicherauslastung sowie die Aktion, die ausgeführt werden soll, wenn die Maximalauslastung erreicht wird, anzeigen lassen oder diese ändern.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Maximale Auslastung des Systemplattenpools
- Wenn maximale Auslastung erreicht ist
- Nicht verwendeten Druckausgabespeicher automatisch bereinigen

Maximale Auslastung des Systemplattenpools



Gibt den zulässigen maximalen Prozentsatz des belegten Speichers im Systemplattenpool (auch Zusatzspeicherpool genannt) an.

Wenn das Maximum erreicht wird, erfolgt die Aktion, die im Systemwert „Wenn maximale Auslastung erreicht ist“ angegeben wurde.

9.16.2.1.11
Seite 2

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	95 %
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QSTGLOWLMT

Wenn maximale Auslastung erreicht ist
Gibt die Aktion an, die ausgeführt werden soll, wenn der verfügbare Speicher im Systemplattenpool (auch Zusatzspeicherpool genannt) die maximale Auslastung für den Zusatzspeicher erreicht hat. Auswahlmöglichkeiten:

Nachricht an Systembediener- und Systemnachrichtenwarteschlange senden
Nachricht CPI099C wird an die Systemnachrichten- und Systembedienerwarteschlange gesendet. Diese Nachricht wird auch bei den anderen Aktionen gesendet.

Nachricht an Servicebenutzer senden
Nachricht CPI099B wird an den Benutzer, der in den Serviceattributen als Empfänger von kritischen Nachrichten angegeben ist, gesendet. Nur an einer Datenstation angemeldete Benutzer werden benachrichtigt.

Registrierte Exitprogramme ausführen
Ein Job zum Aufrufen von Exitprogrammen, die für den Ausstiegspunkt QIBM_QWC_QSTGLOWACN (Untergrenze für Zusatzspeicher) registriert sind, wird übergeben.

Wenn sich das System im Status des eingeschränkten Betriebs befindet, erfolgt keine Aktion.

Wenn Sie diese Aktion auswählen und der verfügbare Hauptspeicher erreicht die Grenze für maximale Auslastung, so können Sie kein Subsystem starten, solange sich das System im Status des eingeschränkten Betriebs befindet.

System im Status des eingeschränkten Betriebs beenden
Das System wird im Status des eingeschränkten Betriebs beendet.

Wenn sich das System im Status des eingeschränkten Betriebs befindet, erfolgt keine Aktion.

Wenn Sie diese Aktion auswählen und der verfügbare Hauptspeicher erreicht die Grenze für maximale Auslastung, so können Sie kein Subsystem starten, solange sich das System im Status des eingeschränkten Betriebs befindet.

System sofort ausschalten und erneut starten
Das System wird sofort ausgeschaltet und erneut gestartet.

Wenn sich das System sich im Status des eingeschränkten Betriebs befindet, erfolgt keine Aktion.

Wenn Sie diese Aktion auswählen und der verfügbare Hauptspeicher erreicht die Grenze für maximale Auslastung, so können Sie kein Subsystem starten, solange sich das System im Status des eingeschränkten Betriebs befindet.

Erreicht der verfügbare Speicher das Maximum während eines Neustarts und lautet die Aktion nicht „Nachricht an Systembediener- und Systemnachrichtenwarteschlange senden“, so wird das System im Status des eingeschränkten Betriebs gestartet.

Wenn folgende Bedingungen zutreffen:
- der verfügbare Speicher liegt unter dem Grenzwert
- die Aktion ist „Registrierte Exitprogramme ausführen, System im Status des eingeschränkten Betriebs beenden“ oder „System sofort ausschalten und erneut starten“,
- das System ist im Status des eingeschränkten Betriebs,

so können Sie erst dann ein Subsystem starten, wenn:
- der verfügbare Speicher verkleinert wird,
- als Aktion eine der beiden ersten Optionen oben angegeben wird.

Wenn Folgendes auftritt, erfolgt keine Aktion:
- Der verfügbare Speicher sinkt unter den Grenzwert.
- Das System befindet sich im Status des eingeschränkten Betriebs.
- Die Aktion ist eine der letzten drei Optionen (siehe oben).

Die Aktion wird alle 30 Minuten wiederholt, wenn der verfügbare Speicher weiterhin das Maximum überschreitet.

Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	alle Objekte (*ALLOBJ) und Sicherheitsadministrator (*SECADM)
Standardwert:	Nachricht an Systembediener und Nachrichtenwarteschlange senden
Änderungen werden wirksam:	wenn der verfügbare Speicher das Maximum erreicht. Hat der verfügbare Speicher bereits das Maximum erreicht, wird die Aktion bei der nächsten Speicherzuordnung aus dem Systemplattenpool durchgeführt.
Sperrbar:	nein
Systemwert:	QSTGLOWACN

Nicht verwendeten Druckausgabespeicher automatisch bereinigen
Dieser Wert ermöglicht das automatische Entfernen leerer Spool-Datenbankteildateien. Nehmen Sie diese Auswahl vor, wenn Sie eine maximale Aufbewahrungsstufe wünschen.

Mögliche Werte sind:

0
Alle leeren Teildateien werden gelöscht. Der Wert verursacht zusätzlichen Systemaufwand beim Erstellen von Spool-Dateien. Daraus kann sich eine starke Verschlechterung der Systemleistung ergeben.

1 – 366
Gibt den Aufbewahrungszeitraum (in Tagen) für leere Spool-Datenbankteildateien zur neuen Verwendung von Spool-Dateien an. Sind die Teildateien nach der angegebenen Anzahl Tage noch immer leer, werden sie vom System gelöscht.

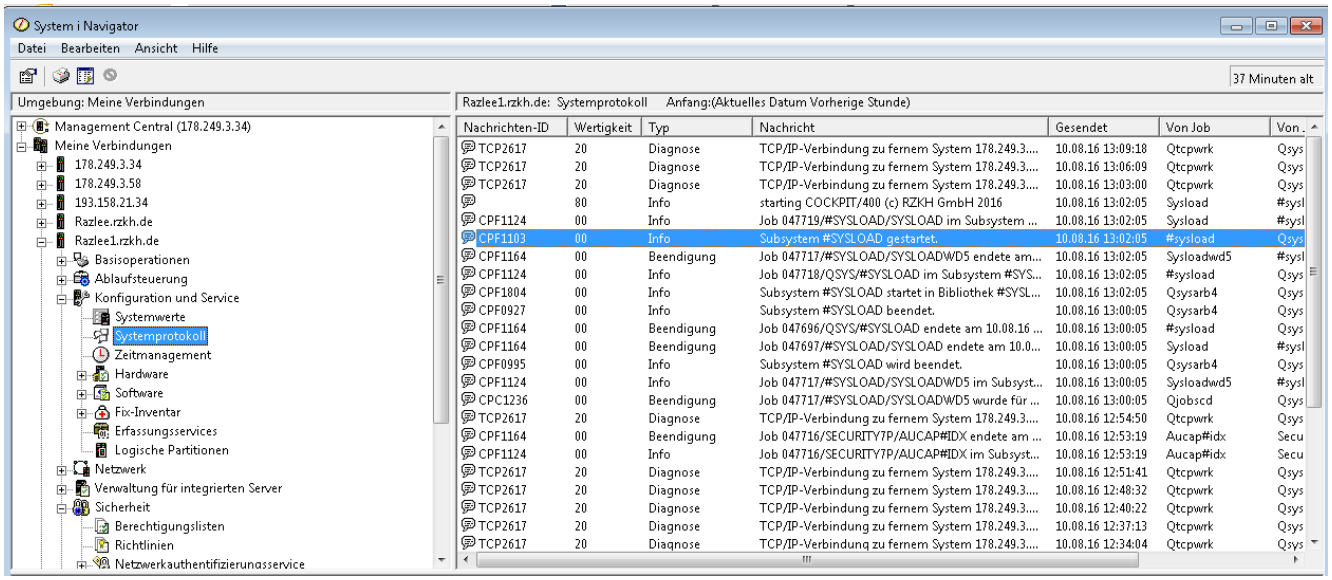
Wichtige Informationen zu diesem Systemwert:

Kurzübersicht	
Sonderberechtigung:	keine
Standardwert:	ausgewählt – 8 Tage
Änderungen werden wirksam:	sofort
Sperrbar:	nein
Systemwert:	QRCLSPLSTG

9.16.2.1.12 Systemprotokoll

Systemprotokoll

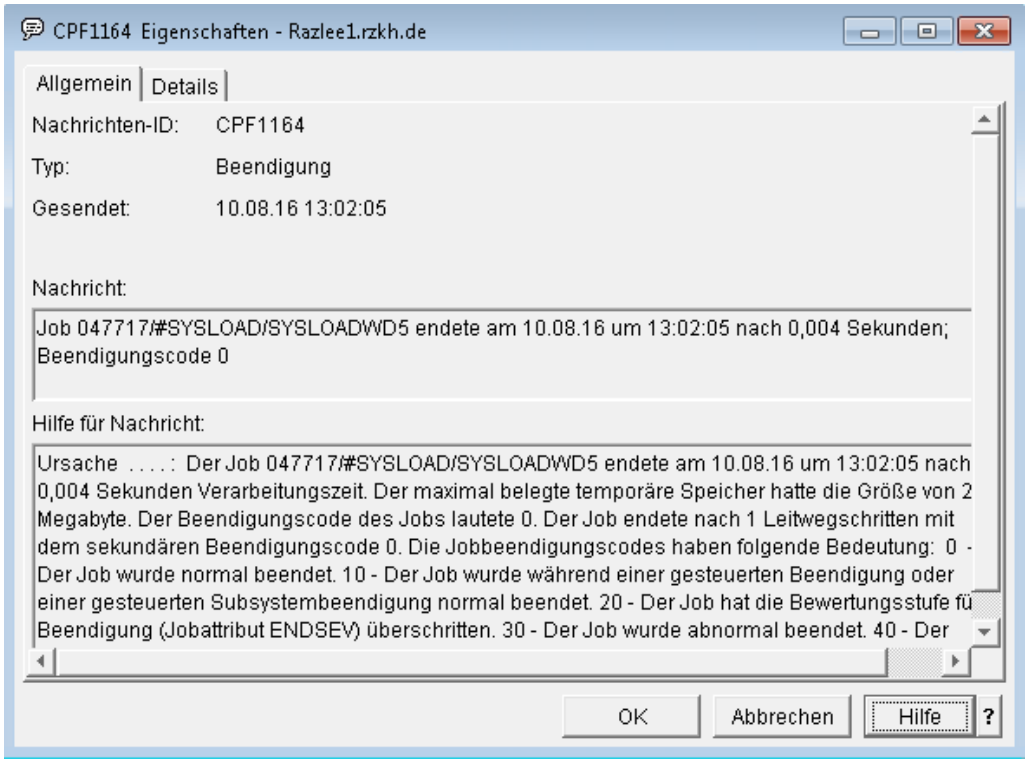
Mit Systemprotokollen können Sie die Systemaktivität überwachen und steuern. Wenn Sie ein präzises Systemprotokoll verwalten, können Sie bestimmte Systemaktivitäten überwachen, die Sie bei der Problemanalyse unterstützen. Systemprotokolle unterscheiden sich von Jobprotokollen. Jobprotokolle zeichnen die sequenziellen Ereignisse eines Jobs auf. Systemprotokolle zeichnen dagegen bestimmte Betriebs- und Statusnachrichten auf, die alle Jobs des Systems betreffen.



Weitere Informationen finden Sie unter „Systemprotokolle“ im i5/OS Information Center.

9.16.2.1.12
Seite 2

Allgemein



Auf der Seite „Nachrichteneigenschaften – Allgemein“ können Sie sich die Basiseigenschaften einer Nachricht anzeigen lassen. Zu diesen gehören unter anderen die ID der Nachricht, der Typ der Nachricht, Sendedatum und -uhrzeit der Nachricht, der Text der Nachricht und die Hilfe, die zur Nachricht verfügbar ist.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Nachrichten-ID/Von Benutzer
- Typ
- Gesendet
- Nachricht
- Hilfe für Nachricht

Nachrichten-ID/Von Benutzer
Zeigt die Nachrichten-ID (siebenstellige Kennung) für eine vordefinierte Nachricht an (zum Beispiel CPF1E99). Für eine nicht vordefinierte Nachricht zeigt dieses Feld den Namen des Benutzers an, der die Nachricht gesendet hat, wenn auf dem System i5/OS, OS/400 V5R3 oder eine aktuellere Version ausgeführt wird.

Wenn auf dem System eine frühere Version von OS/400 ausgeführt wird, gilt Folgendes:
- Der Name des neuen Jobbenutzers wird angezeigt.
- Wenn System i Navigator zum Senden der Nachricht verwendet wurde, lautet der Name des Jobbenutzers „QUSER".

Typ
Zeigt den Typ der Nachricht an. Es gibt folgende Typen:

Abschluss
Teilt Ihnen mit, dass die Arbeit abgeschlossen ist.

Diagnose
Gibt Fehler in einer Systemfunktion, einer Anwendung oder in Eingabedaten an.

Abbruch
Meldet eine Bedingung, die das Beenden eines Programms verursacht hat, bevor die angeforderte Funktion abgeschlossen war.

Informationen
Übergibt Informationen an einen Benutzer. Diese Nachricht muss nicht beantwortet werden. Eine Informationsnachricht kann von einem anderen Benutzer (beispielsweise „Besprechung geplant für 13:30 Uhr"), vom Systembediener (beispielsweise „System wird Sonntag um 7:00 Uhr ausgeschaltet") oder vom System gesendet werden.

Der Empfänger der Informationsnachricht kann durch eine weitere Informationsnachricht antworten, die an den Absender der ersten Nachricht zurückgesendet wird.

Anfrage
Erfordert eine Antwort von dem Benutzer, der die Nachricht empfängt. Sie könnten beispielsweise eine Anfragenachricht senden, in der um eine Auskunft gebeten wird (zum Beispiel „Joe, hast Du noch Teilenr. 45206 und 34133 auf Lager?").

Anmerkung:

Eine Anfragenachricht muss nicht unbedingt beantwortet werden. Die Nachricht kann gelöscht werden, bevor sie beantwortet wird. In diesem Fall sendet das Betriebssystem eine Standardantwort.

9.16.2.1.12
Seite 4

Hinweis
Beschreibt eine Bedingung, für die ein Programm eine Antwort vom aufrufenden Programm benötigt oder für die automatisch eine Antwort an das Programm gesendet wird.

Antwort
Eine Antwort auf eine Anfragenachricht. Für Antwortnachrichten gibt es folgende Subtypen:

Antwort, nicht auf Gültigkeit geprüft
Es wurde nicht überprüft ob die Antwortnachricht eine gültige Antwort ist. Antwortnachrichten werden nur auf ihre Gültigkeit überprüft, wenn sie vordefinierten Nachrichten zugeordnet sind, die sich in einer Nachrichtendatei befinden, die Antwortspezifikationen enthält.

Antwort, bereits auf Gültigkeit geprüft
Die Antwortnachricht wurde mit den Antwortspezifikationen verglichen, die in der Nachrichtenbeschreibung für die Anfragenachricht definiert sind, die dieser Antwort zugeordnet ist. Der Antwortwert ist mit den Spezifikationen identisch.

Antwort, Nachrichtstandardwert verwendet
Die Antwortnachricht ist die Standardantwort, die in der Nachrichtenbeschreibung für die Anfragenachricht angegeben ist, die dieser Antwort zugeordnet ist.

Antwort, Systemstandardwert verwendet
Die Antwortnachricht ist die Systemstandardantwort. Die Systemstandardantwort wird verwendet, wenn eine Standardantwort erforderlich ist und eine der folgenden Voraussetzungen zutrifft:

- Die zugeordnete Anfragenachricht ist keine vordefinierte Nachricht.
- Die zugeordnete Anfragenachricht ist eine vordefiniert Nachricht; in ihrer Nachrichtenbeschreibung ist keine Standardantwort angegeben.

Antwort, aus Systemantwortliste
Die Antwortnachricht stammt aus der Systemantwortliste. Der Job, der die Antwort gesendet hat, war für die Verwendung der Systemantwortliste konfiguriert, und die Nachrichten-ID der zugeordneten Anfragenachricht war mit einem Eintrag in der Systemantwortliste identisch.

Antwort, von Exitprogramm
Ein Antworten verarbeitendes Exitprogramm hat einen Antwortwert durch diesen Antwortwert ersetzt. Das Exitprogramm war für die Ausführung durch den Systemausstiegspunkt QIBM_QMH_REPLY_INQ konfiguriert, der in der Systemregistrierungsfunktion eingetragen ist.

Anforderung
Fordert eine Funktion vom empfangenden Programm an.

Kopie des Absenders
Eine Kopie der ursprünglichen Anfragenachricht, die zum Zurücksenden der Antwort an den Absender der ursprünglichen Anfragenachricht verwendet wird.

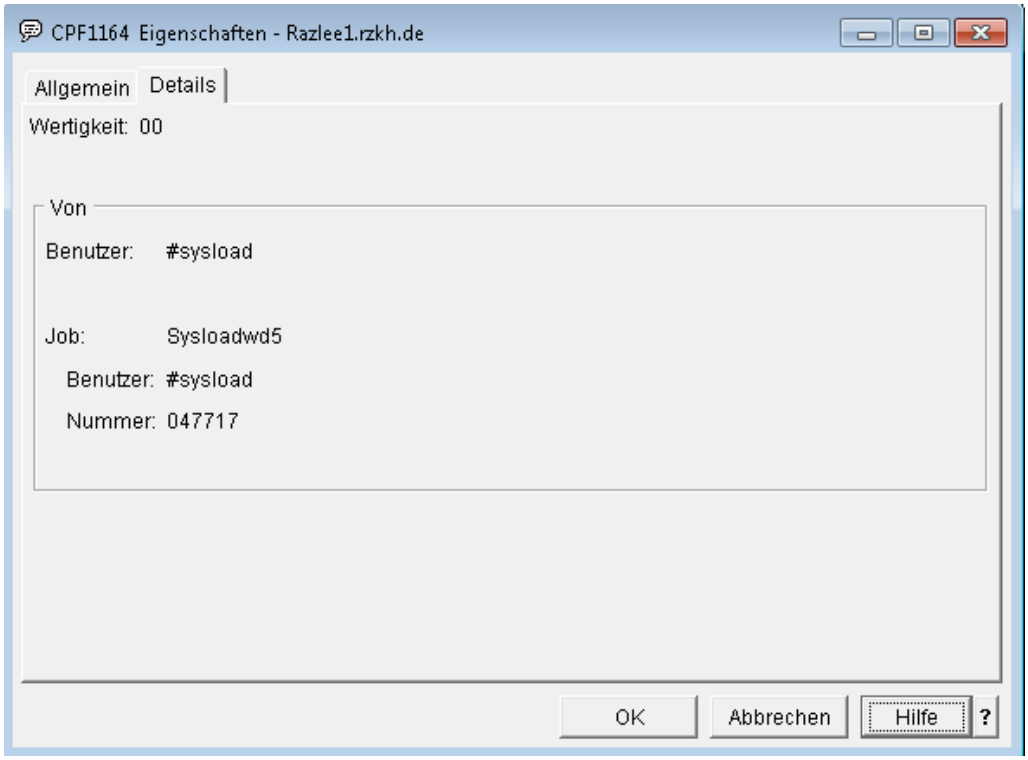
Gesendet
Zeigt an, an welchem Datum und zu welcher Uhrzeit die Nachricht gesendet wurde.

Nachricht
Zeigt den Nachrichtentext an. Für Anfragenachrichten und Senderkopien wird der Name des Benutzers angezeigt, an den die Anfragenachricht gesendet wurde. Der Name wird am Anfang des Nachrichtentexts unter ===>*benutzername* angezeigt, wobei *benutzername* den Benutzer bezeichnet, an den die Anfragenachricht gesendet wurde.

Gültige Antwortwerte werden bei einer vordefinierten Anfragenachricht am Ende des Texts angezeigt. Eine Erläuterung dieser möglichen Optionen wird im Feld „Hilfe für Nachricht“ angezeigt (wird nur für vordefinierte Nachrichten angezeigt).

9.16.2.1.12
Seite 6

Details



Auf der Seite „Nachrichteneigenschaften – Details“ können Sie zusätzliche Details zur Systemprotokollnachricht anzeigen. Zu diesen Details gehören die Wertigkeit der Nachricht und die Informationen zur Identifizierung des Benutzers und des Jobs, von denen die Nachricht gesendet wurde.

Weitere ausführliche Hilfeinformationen können Sie zu den folgenden Elementen dieses Fensters aufrufen:

- Wertigkeit
- Von

Wertigkeit
Zeigt den Wert aus zwei Ziffern für die Wertigkeit der Nachricht an. Je höher der Wert, desto größer die Wertigkeit oder die Bedeutung der Bedingung.

Von
Zeigt Informationen an, die den Benutzer und den Job angeben, von denen die Nachricht gesendet wurde.

Die Informationen umfassen folgende Daten:

Benutzer
Zeigt den Namen des Benutzers an, der die Nachricht gesendet hat, wenn auf dem System i5/OS, OS/400 V5R3 oder eine aktuellere Version ausgeführt wird.

Wenn auf dem System eine frühere Version von OS/400 ausgeführt wird:

- Der Name des neuen Jobbenutzers wird angezeigt.
- Wenn System i Navigator zum Senden der Nachricht verwendet wurde, lautet der Name des Jobbenutzers „QUSER“.

Job
Zeigt den Namen des Jobs an, der die Nachricht gesendet hat. Jeder Job besitzt einen qualifizierten Jobnamen, der aus dem Jobbenutzer, der Jobnummer und dem Jobnamen besteht.

Benutzer
Zeigt den Namen des Benutzerprofils an, unter dem der Job ausgeführt wurde, der die Nachricht gesendet hat.

Nummer
Zeigt die Nummer des Jobs an, der die Nachricht gesendet hat. Die Jobnummer ist eine eindeutige Nummer aus sechs Ziffern, die jedem Job vom System zugeordnet wird.

9.16.2.1.12

Seite 8