IBM i Security Auswertungen

Februar 2023

IT-Power Services GmbH

Klaus Haderer

Überblick

- Security Tools
- IBM Navigator for i
- IBM i Services (SQL)
- Security Exit Points

Überblick

Security Tools	IBM Navigator for i	IBM i Services	Security Exit Points
5250 – Green Screen	Webinterface – Browser	ACS – Run SQL Scripts / STRSQL	System Exit Point
Menü / Command based	Graphical User Interface (GUI)	SQL Tool	Selbst entwickelte Programme
Interaktiv / Batch	Interaktiv	Interaktiv / Batch	
Automatisierung möglich	-	Automatisierung möglich	
Anzeige und Änderung	Anzeige und Änderung	Anzeige	
Report SPLF (teilweise Outfile)	Client Format (CSV,XLS,ODS,…)	Client Format (CSV,XLS,ODS,…)	
-	Zertifikat Management, EIM, Fileshares, …	Nur lesender Zugriff	

Voraussetzungen

- Als Referenz Betriebssystemversion wurde V7R4 verwendet
  - Auswertungsmöglichkeiten hängen auch vom installierten TR und PTF Level ab
  - Wichtig!! Immer eine aktuelle ACS Version verwenden

- Das Audit Journal muss eingerichtet sein,
  z.B. mit folgenden Einstellungen
  - QAUDCTL: *OBJAUD, *AUDLVL, *NOQTEMP
  - QAUDLVL: *CREATE, *DELETE, *OBJMGT, *SAVRST, *SECURITY, *SPLFDTA, *PRTDTA, *AUTFAIL, *PGMFAIL, *JOBDTA, *NETCMN, *NETTELSVR

- Die in Screens gezeigten Settings sind IBM Default und entsprechen nicht den Recommended Settings

Security Tools

Security Tools

- Das Security Tools Menu stellt eine Vielzahl an Optionen zur Verfügung um die System Security zu managen und zu überwachen
- Erreichbar über 5250 mittels GO MENU(SECTOOLS)
- In den folgenden Slides sind diese in Erfahrungswerte kategorisiert

☆☆☆ Basic

★☆☆ Medium

★★☆ Advanced

Security Tools

Benutzer Profile

Auflistung aller Benutzer mit Default Passwort (User=Passwort)
1. Analyze default passwords

Möglichkeit nicht verwendete Benutzer auszuwerten und zu deaktivieren
2. Display active profile list
3. Change active profile list
4. Analyze profile activity

Möglichkeit Benutzer zeitlich befristet zu aktivieren
5. Display activation schedule
6. Change activation schedule entry

Möglichkeit Benutzer an einem gewissen Tag zu deaktivieren/löschen
7. Display expiration schedule
8. Change expiration schedule entry

Auswertung detailierter Informationen je Benutzer
Owned Objects, Private Authorities, Authorized Objects, Primary Group Authorities
9. Print profile internals

Security Tools

Auditing

Möglichkeit die Audit-Journal relevanten Systemwerte zu ändern

10. Change security auditing
11. Display security auditing
12. Copy audit journal entries

System Security

NICHT ausführen, ändern Systemeinstellungen auf eine Art und Weise dass es zu Problemen führen wird!!!

60. Configure system security
61. Revoke public authority to objects

Überprüft die Integrität von Objekten eines bestimmten Eigentümers (z.B. Q*)

62. Check object integrity

Security Tools

Reporting

Auswertung welche Programme die Rechte eines anderen Benutzers nutzen (z.B. QSECOFR).
Auch Auswertung der Änderungen möglich
21. Adopting objects

Auswertung der Audit Journal Einträge
22. Audit journal entries

Auflistung aller Authorization Lists und ihrer Berechtigungen
23. Authorization list authorities

Private und public Berechtigung auf Befehle pro Bibliothek
24. Command authority
25. Command private authority

Security Tools

Reporting

Berechtigung auf alle Objekte der Kommunikationsdefinitonen
26. Communications security

Berechtigung auf alle Objekte der Kommunikationsdefinitonen
26. Communications security

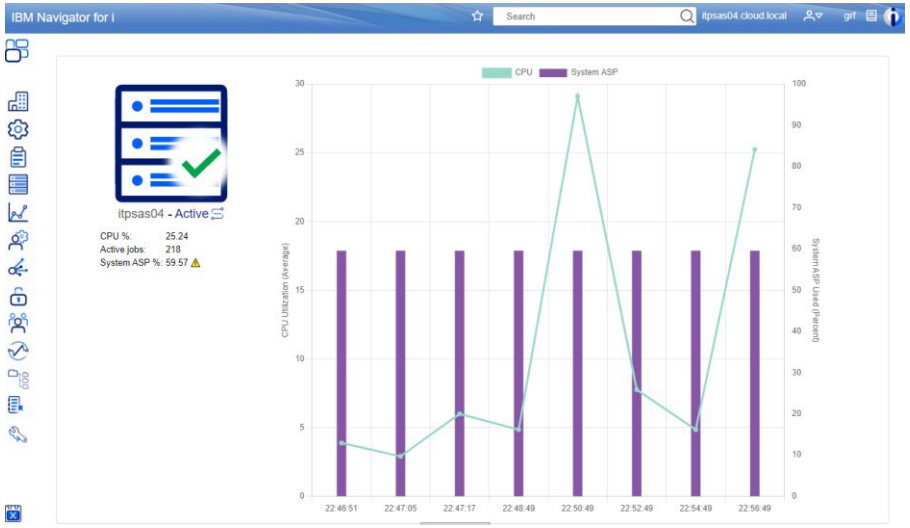
Auswertung der public Berechtigungen auf Benutzerprofile
42. User profile authority

Berechtigungsauswertung für unterschiedliche Objektarten
27. Directory authority 28. Directory private authority 29. Document authority
30. Document private authority 31. File authority 32. File private authority
33. Folder authority 34. Folder private authority 35. Job description authority
36. Library authority 37. Library private authority 38. Object authority
39. Private authority 40. Program authority 41. Program private authority
43. User profile private authority 44. Job and output queue authority 45. Subsystem authority
46. System security attributes 47. Trigger programs 48. User objects
49. User profile information

IBM Navigator for i

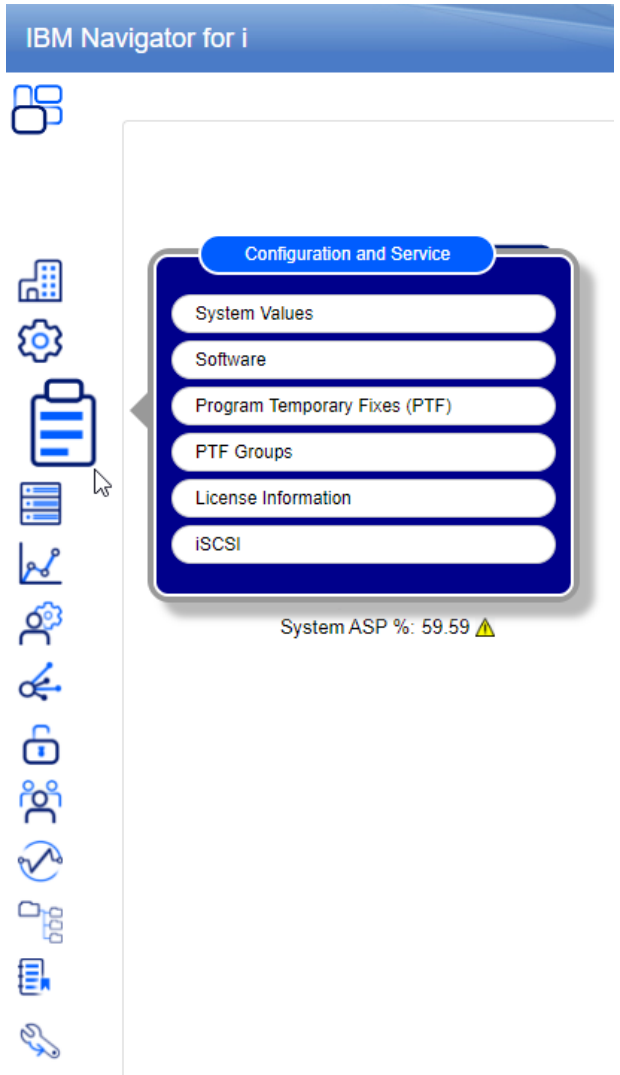
IBM Navigator for i

- Bietet ein modernes web based Interface
- Managen und Monitoring einer oder mehrere IBM i Instanzen
- Neue Version wurde 09/2021 released
- Verfügbar über die HTTP Group PTF für V7R3, V7R4 und V7R5
- Läuft im QHTTPSVR Subsystem im ADMIN1 Server Job
- Default URL ist http://hostname:2002/Navigator
  oder https://hostname:2003/Navigator

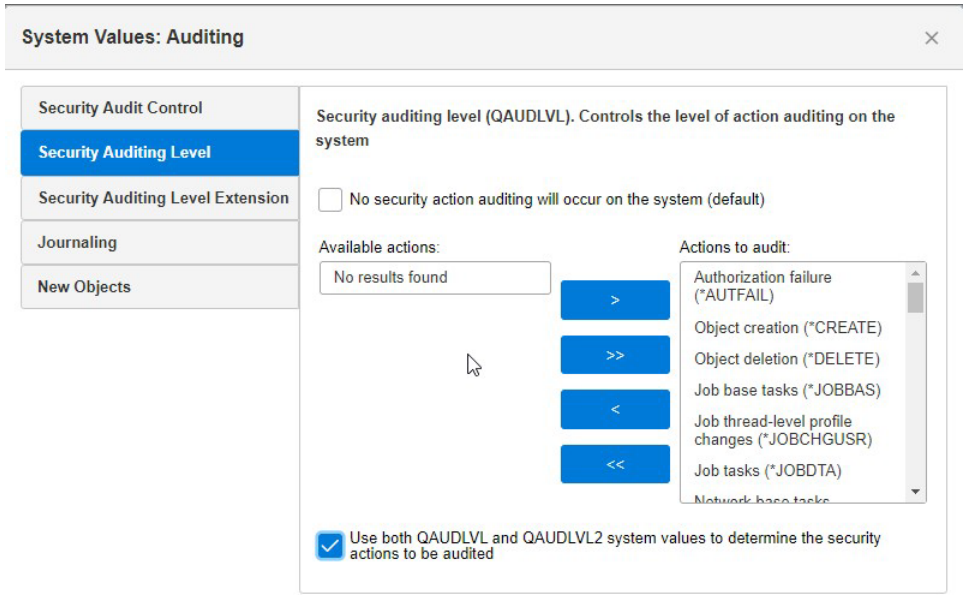


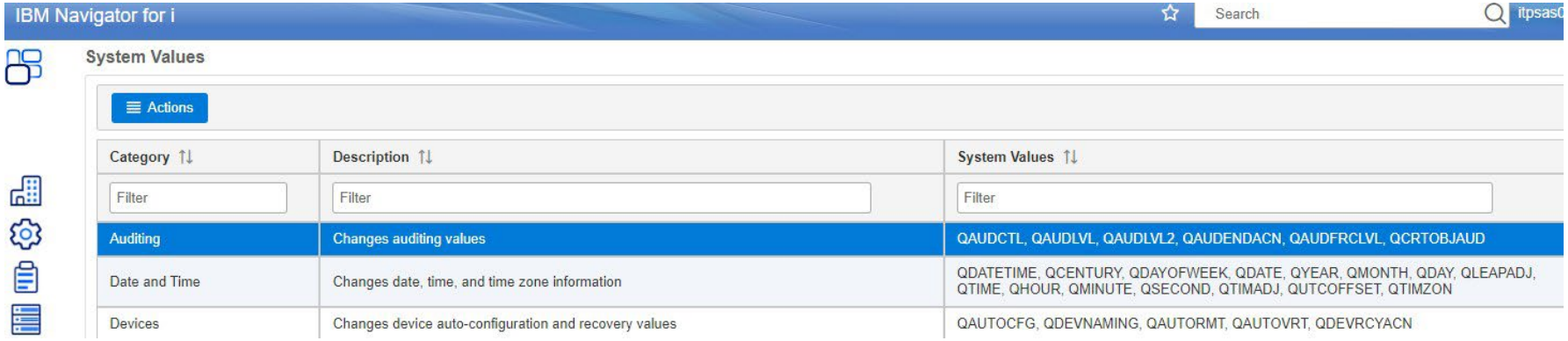

```
                          Work with Active Jobs
                                                          02/23/23  22:2
J %:       .0      Elapsed time:    00:00:00     Active jobs:    208
                     Current
t  Subsystem/Job     User        Type   CPU %   Function         Status
   QHTTPSVR          QSYS        SBS       .0                    DEQW
     ADMIN           QTMHHTTP    BCH       .0  PGM-QZHBMAIN      SIGW
     ADMIN           QTMHHTTP    BCI       .0  PGM-QZSRLOG       SIGW
     ADMIN           QTMHHTTP    BCI       .0  PGM-QZSRHTTP      SIGW
     ADMIN1          QWEBADMIN   BCI       .0  JVM-/QIBM/Prod    THDW
     ADMIN3          QWEBADMIN   BCI       .0  JVM-/QIBM/Prod    THDW
     ADMIN4          QWEBADMIN   BCI       .0  JVM-/QIBM/Prod    THDW
     ADMIN5          QLWISVR     BCI       .0  JVM-/QIBM/Prod    THDW
```

IBM Navigator for i



- Unterteilt in Funktionsbereiche und Kategorien
- Zusammenhängende Settings sind in einem Menü dargestellt
- Meist verwendete Ansichten können als Favoriten gespeichert werden
- Absicherung durch Definition von Zugriffskontrollen dringend empfohlen
- Nachfolgende Slides bieten einen Überblick über die einzelnen Darstellungsmöglichkeiten





Security Configuration Information

- Zentrale Stelle für die meisten Security Relevanten Einstellungen
- Anzeige der gesetzten Werte sowie detailierter Informationen
- Betroffene System Values werden im jeweiligen Menü aufgelistet
- Über die Hauptpunkte kann direkt zu den jeweiligen Einstellungen navigiert werden

Security Configuration Information

Actions

Name	Current Value	Description	Values
Filter	Filter	Filter	Filter
Security Level	40	Security Level (20, 30, 40, 50) (QSECURITY)	20=Password security only, 30=Password and operating system integrity, 50=Password, obje
Pending Security Level		The security level that the system will use after the next IPL	Blank=No change, 20=Password security only, object, and operating system integrity, 50=Pas integrity
Password Level	3	Password Level (0, 1, 2, 3, 4) (QPWDLVL)	0=User profile passwords with a length of 1-10 passwords with a length of 1-10 characters are length of 1-128 characters are supported, 3=U characters are supported *, 4=User profile pas supported *
Pending Password Level		The password level that the system will use after the next IPL	Blank=No change, 0=User profile passwords w 1=User profile passwords with a length of 1-10 passwords with a length of 1-128 characters ar length of 1-128 characters are supported *, 4= characters are supported *
Password Change Block	*NONE	The current setting for the block password change (QPWDCHGBLK) system value	*NONE, 1-99 Hours
Password Expiration Interval	*NOMAX	The current setting for the password expiration interval (QPWDEXPITV) system value	*NOMAX, 1-366 Days
Password Expiration Warning	7	The current setting for the password expiration warning (QPWDEXPWRN) system value	1-99 Days

« ‹ 1 › » 100

Total Rows: 43

Password Rules	*PWDSYSVAL	The current setting for the password rules (QPWDRULES) system value Change	Any of these: *PWDSYSVAL, *ALLCRTCHG, *CHRLMTAJC, *CHRLMTREP, *DGTLMTAJC, *DGTLMTFST, *DGTLMTLST, *DGTMAXn, *DGTMINn, *LMTSAMPOS, *LMTPRFNAME, *LTRLMTAJC, *LTRLMTFST, *LTRLMTLST, *LTRMAXn, *LTRMINn, *MAXLENnnn, *MINLENnnn, *MIXCASEn, *REQANY3, *SPCCHRLMTAJC, *SPCCHRLMTFST, *SPCCHRLMTLST, *SPCCHRMAXn, *SPCCHRMINn
Password	Changes password expiration and validation	Properties	QPWDLVL, QPWDCHGBLK, QPWDVLDPGM, QPWDMINLEN, QPWDMAXLEN, QPWDRQDDGT, QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDRQDDIF, QPWDPOSDIF, QPWDRULES, QPWDEXPITV, QPWDEXPWRN

System Values: Password

General
Validation 1
Validation 2
Expiration

Password level (current):
Long passwords using an unlimited character set (3) *

Password level (at next restart) (QPWDLVL):
- Short passwords using a limited character set (0)
- Short passwords using a limited character set (1)
- Long passwords using an unlimited character set (2)
- Long passwords using an unlimited character set (3)
- Long passwords using an unlimited character set (4)

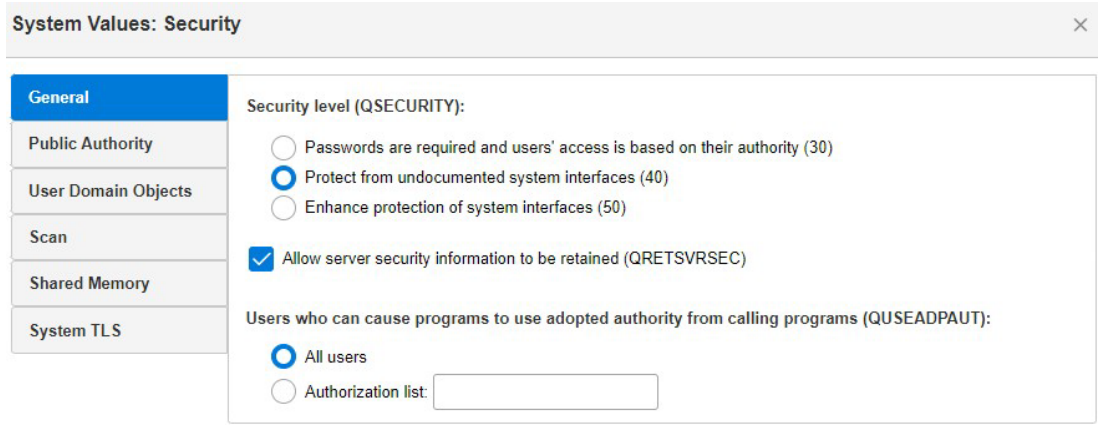
Minimum time between password changes (QPWDCHGBLK):
- None
- Hours (1-99): 1 - 99

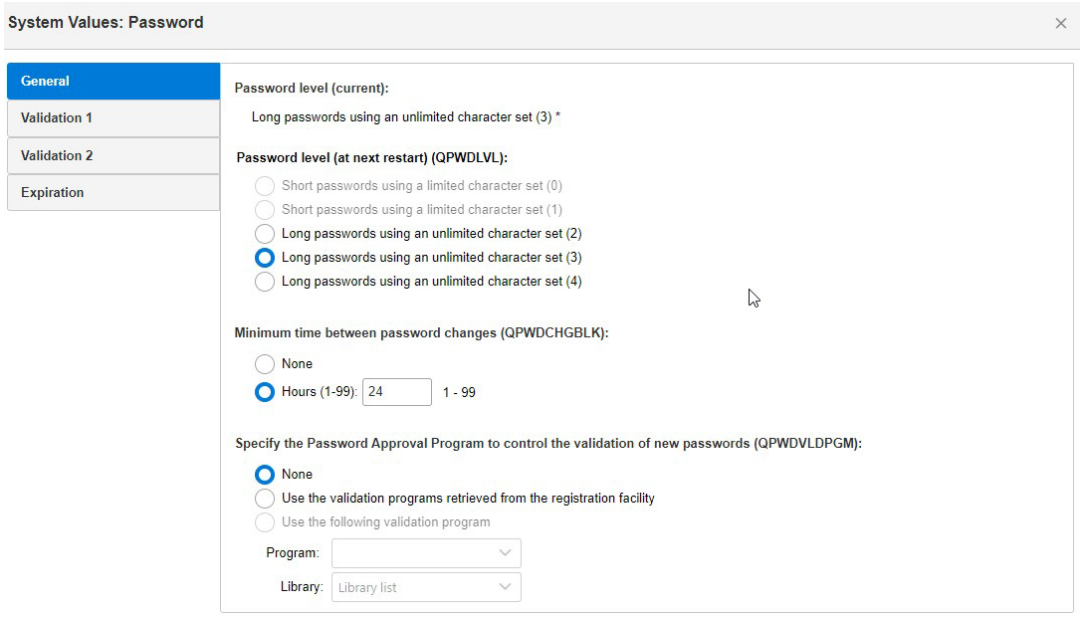
Specify the Password Approval Program to control the validation of new passwords (QPWDVLDPGM):
- None
- Use the validation programs retrieved from the registration facility
- Use the following validation program

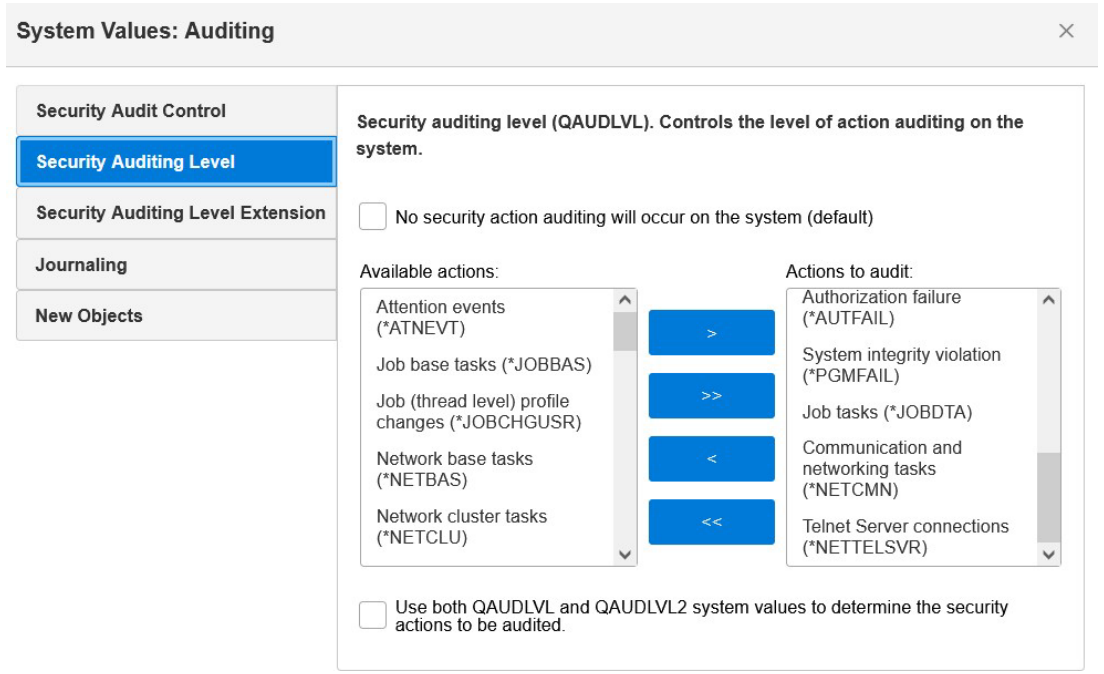
Program:
Library: Library list

System Values

- Beispiel System Values
- Anzeige in Kategorien unterteilt
- Logische Gruppierung zusammenhängender Werte
- Zusätzliche Informationen

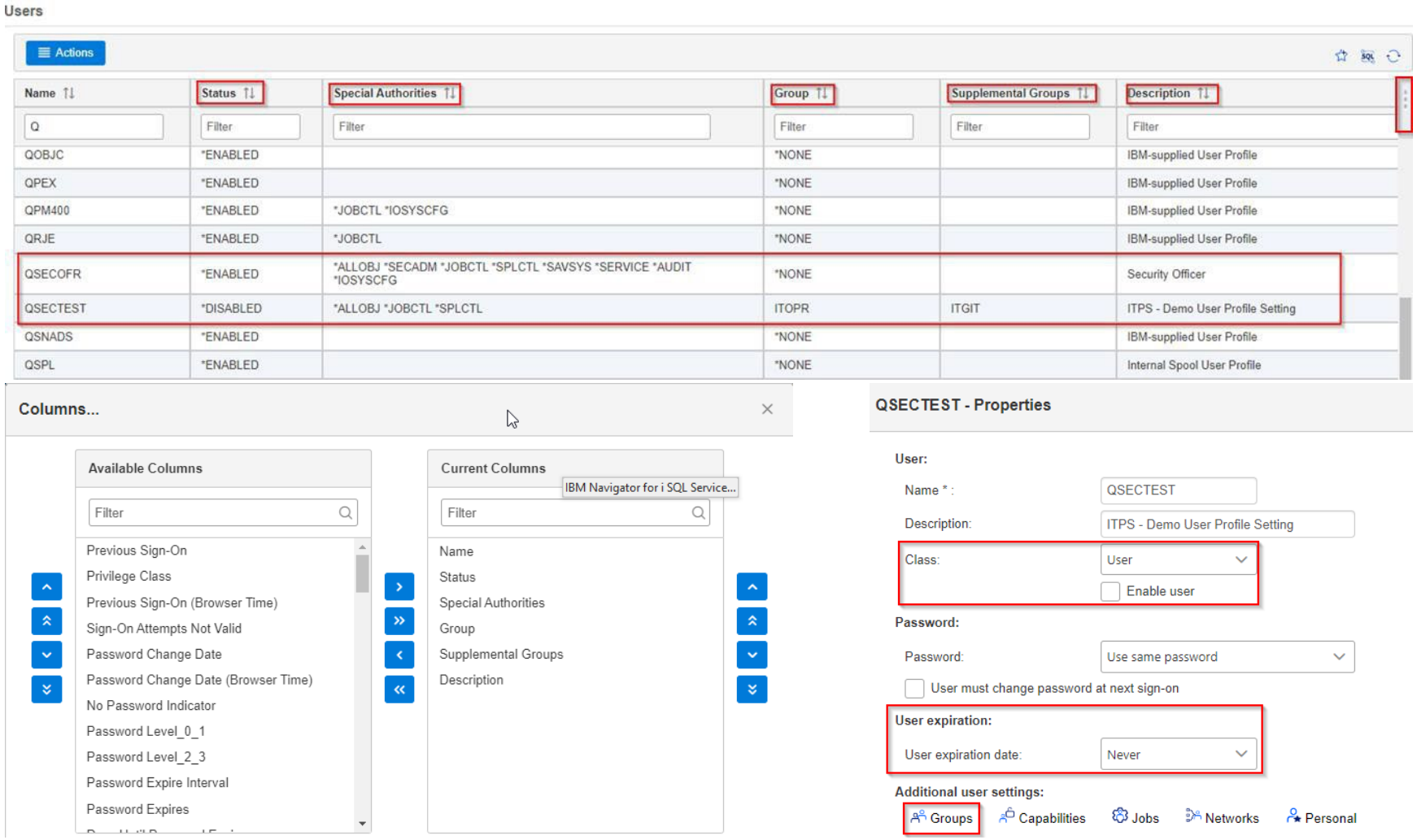






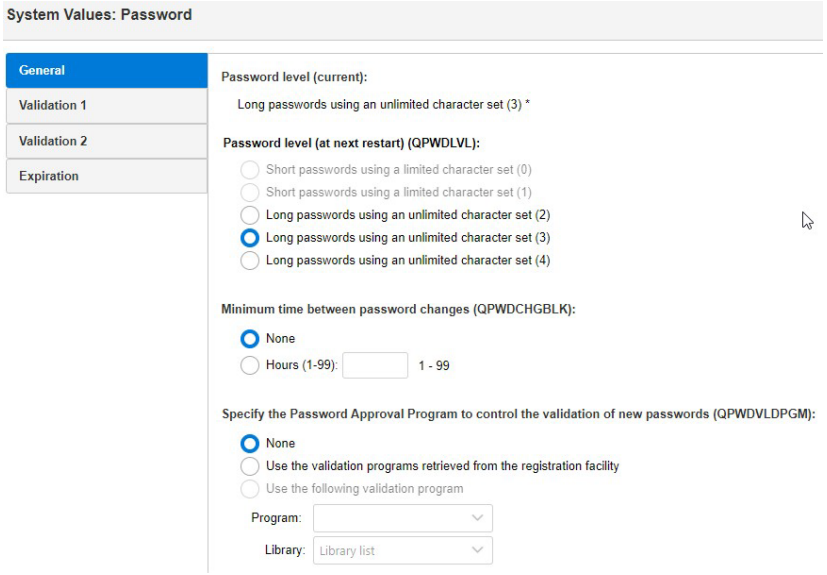
User Profile Information

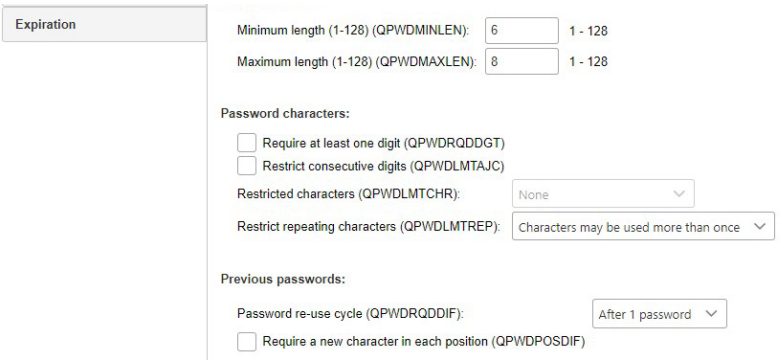
- Beispiel User Profile
- Standard View zeigt Basis Information
- Über die Auswahl der Columns können zusätzliche Spalten eingeblendet werden (z.B. Previous Sign On, Password Indicator, …)
- Filtern nach Kriterien möglich (z.B. Status *ENABLED, Special Authorities *ALLOBJ)
- Es können auch direkt Änderungen vorgenommen werden
- Ähnliche Darstellung für Gruppen Profile

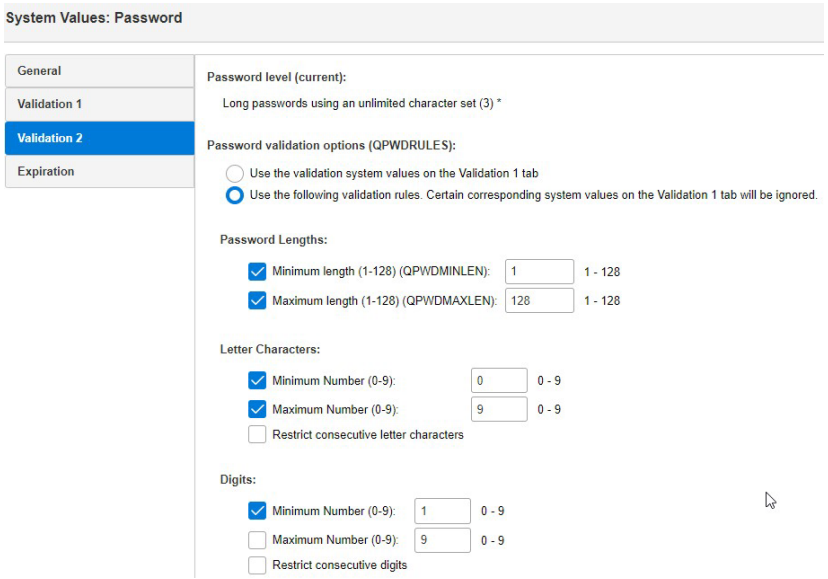


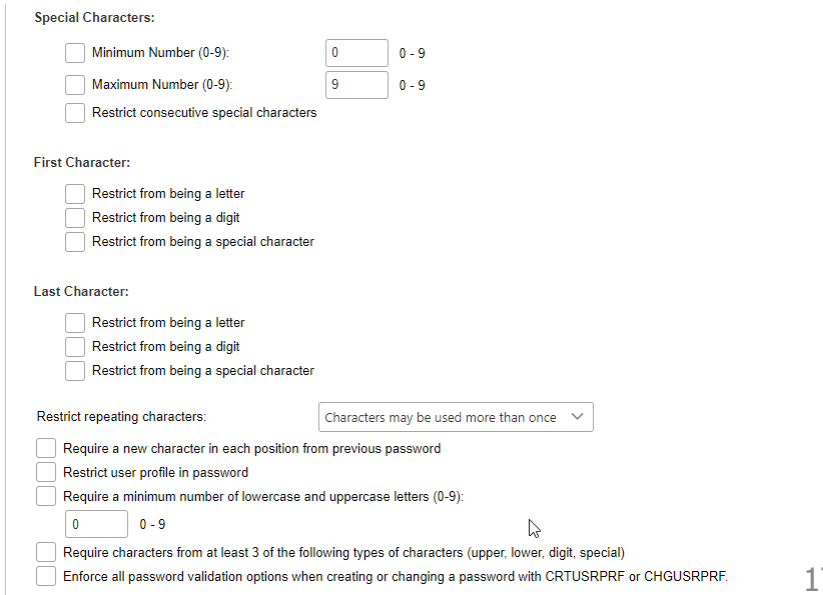
Passwort Rules

- Beispiel Passwort Rules
- Unterschiedliche Settings werden an zentraler Stelle zusammengefasst
- Zusätzliche Informationen
- Default/Min/Max Werte
- Einfache Änderung









File Shares

- Beispiel File Shares
- Auflistung aller definierten File Shares
- Definierte Share Berechtigung
- Definierte IFS Berechtigung je User
- Export der Liste in CSV Format

File Shares

Actions

Server Share Name	Path Name	Path Availability	Permissions	Authorization List	Description	Current Users	Encryption Required
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
ROOT	/	Available	*RW		Root File Share Read/Write	0	NO
QDIRSRV	/QIBM/ProdData/OS400/DirSrv	Available	*RW		OS/400 -- Directory Services	0	NO
PRODDATA	/QIBM/ProdData	Available	*R			0	NO
HOME	/home	Available	*RW			0	NO

File Shares

Actions

--- Item Actions ---
New File Share (Based on)...
Properties
Stop Sharing...
Permissions
--- List Actions ---
New File Share...
Export Selected
Export All
Refresh
Select All
Deselect All
--- Shares Actions ---
Disabled User IDs
IBM i NetServer Status

Permissions

Object:
/QIBM/ProdData

Type:
Owner: QSYS
Primary group: (None)
Authorization list (AUTL): (None)

Owner... | Primary group... | Authorization list...

Name	Read	Write	Execute	Management	Existence	Alter	Reference	Exclude	From AUTL
*PUBLIC	✓		✓						
QSYS	✓	✓	✓	✓	✓	✓	✓		
QDIRSRV			✓						

AutoSave Off | Search

File Home Insert Draw Page Layout Formulas Data Review View Automate Developer Help Power Pivot

B12

	A	B	C	D	E	F
1	Server Share Name	Path Name	Path Availability	Permissio	Authorization List	Description
2	QDIRSRV	/QIBM/ProdData/OS400/DirSrv	Available	*RW		OS/400 -- Directory Services
3	PRODDATA	/QIBM/ProdData	Available	*R		
4	HOME	/home	Available	*RW		
5						

Function Usage

- Beispiel FTP Server
- Regelt den Zugriff auf IBM i Applikationen und Funktionen z.B. FTP, ODBC, … aber auch IBM Navigator for i

Function Usage

Actions

Function ID	Function Name	Default Usage	All Object Indicator	Profiles Allowed / Denied	Description
QTMF_SERVER	Filter	Filter	Filter	Filter	Filter
QIBM_QTMF_SERVER_REQ_0	Logon Server	ALLOWED	NOT USED	YES	Permission to logon to the FTP Server. Must be allowed to use other server operations.
QIBM_QTMF_SERVER_REQ_1	Create Directory/Library	ALLOWED	NOT USED	NO	Use of server subcommand MKD to create directories.
QIBM_QTMF_SERVER_REQ_2	Delete Directory/Library	ALLOWED	NOT USED	NO	Use of server subcommand RMD to delete directories.
QIBM_QTMF_SERVER_REQ_3	Change Directory	ALLOWED	NOT USED	NO	Use of server subcommand CWD to change current directory.
QIBM_QTMF_SERVER_REQ_4	List Files	ALLOWED	NOT USED	NO	Use of server subcommands LIST and NLST.
QIBM_QTMF_SERVER_REQ_5	Delete Files	ALLOWED	NOT USED	NO	Use of server subcommand DELE to delete files.
QIBM_QTMF_SERVER_REQ_6	Send Files	ALLOWED	NOT USED	NO	Use of server subcommand RETR to send files to client.
QIBM_QTMF_SERVER_REQ_7	Receive Files	ALLOWED	NOT USED	NO	Use of server subcommands STOR, STOU, and APPE to receive files from client.
QIBM_QTMF_SERVER_REQ_8	Rename Files	ALLOWED	NOT USED	NO	Use of server subcommands RNFR, RNTO to rename files.
QIBM_QTMF_SERVER_REQ_9	CL Commands	ALLOWED	NOT USED	NO	Use of server subcommand RCMD to execute CL commands.
QIBM_QTMF_SERVER_REQ_10	Clear Command Channel	DENIED	NOT USED	NO	Use of Server subcommand CCC to end encryption of the control connection.

Change Function Usage

Function ID	Description	Default Usage	All Object Indicator
QIBM_QTMF_SERVER_REQ_0	Permission to logon to the FTP Server. Must be allowed to use other server operations.	ALLOWED	NOT USED

Total Rows: 1

Usage options for the selected function IDs

Default authority: Allowed

*ALLOBJ special authority: Not used

Usage options for specified user and group profiles for the the selected function

Profile(s) :

Browse Profiles

Access Allowed: Add, Remove

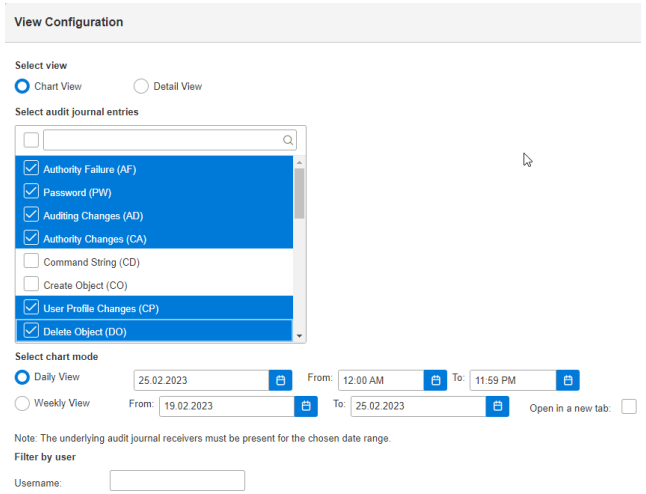
Access Denied: Add, Remove

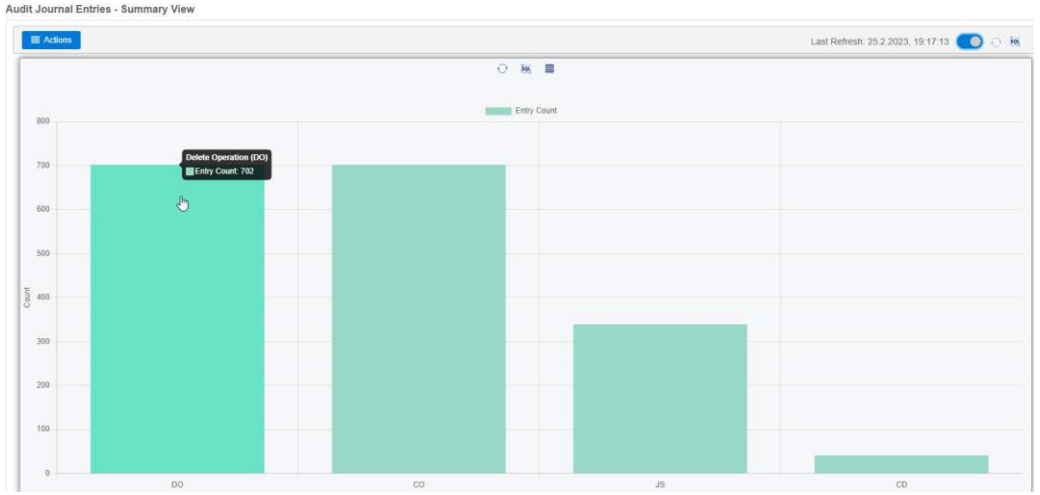
No results found

No results found

Audit Journal Auswertung

- Beispiel Audit Journal
- Unterschiedliche Views (Chart/Detail)
- Möglichkeit zu Filtern
- Informationen zu Journal Codes und Entry Types
- Klick auf Balken des Chart View öffnet direkt die Details
- Automatischer Refresh





Command String (CD) Detail View

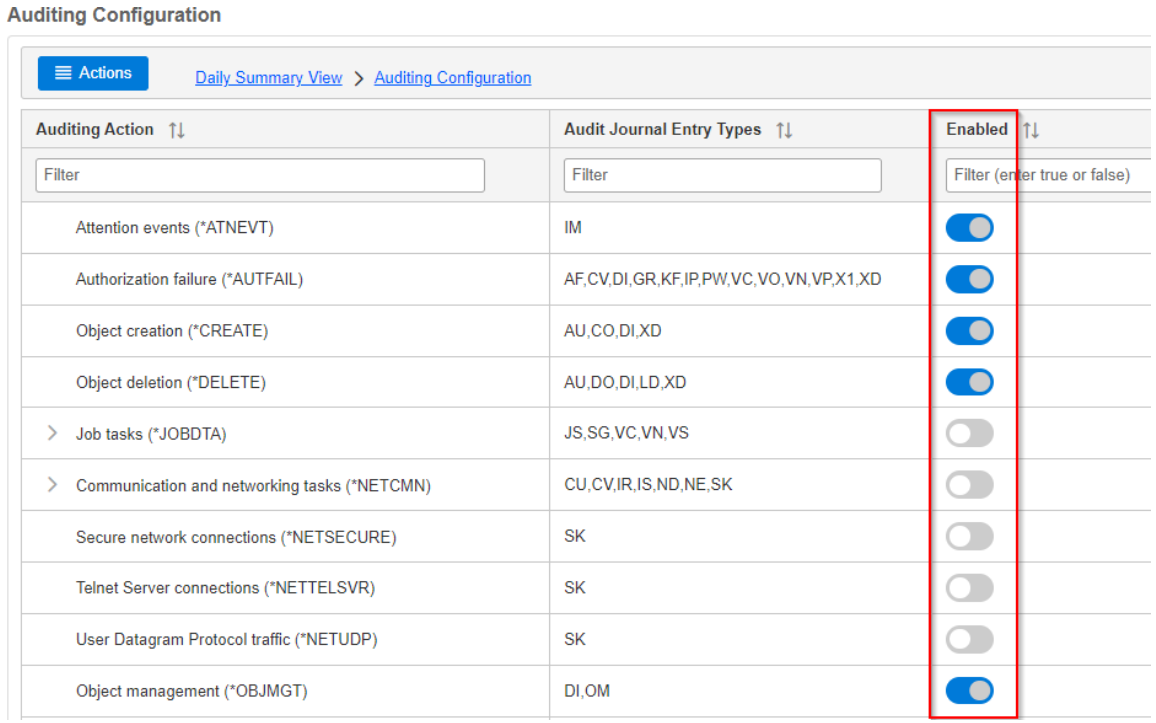
Actions

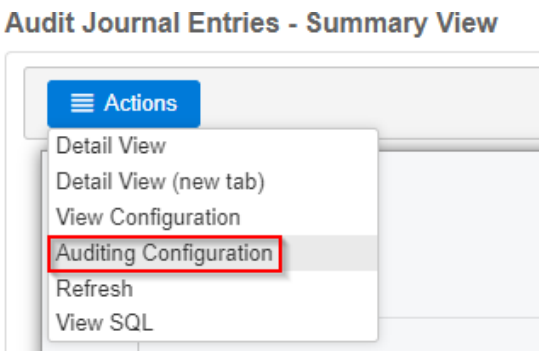
Filters

Timestamp	User Name	Qualified Job Name	Program Library	Program Name	Command String
Filter	Filter	Filter	Filter	Filter	Filter
2023-02-25 09:57:23.445136	[redacted]	419975/QUSER/QZRCSRVS	QSYS	QZRCSRVS	CHGJOB JOB(169742/QUSER/QZDASSINIT) INQMSGRPY(*DFT)
2023-02-25 10:26:41.163536	[redacted]	419979/QUSER/QZRCSRVS	QSYS	QZRCSRVS	QSYS/CHGAUT OBJ('/QIBM/UserData/OS/WebTrustStore/WebTrustStore') USER(QWEBADMIN) DTAAUT(*RW) OBJAUT(*ALL) SUBTREE(*ALL) SYMLNK(*YES)
2023-02-25 10:40:17.114416	[redacted]	419978/QUSER/QZRCSRVS	QSYS	QZRCSRVS	QSYS/CHGAUT OBJ('/QIBM/UserData/OS400/Navigator/preferences/') USER(*PUBLIC) DTAAUT(*WX) OBJAUT(*ALL) SUBTREE(*ALL) SYMLNK(*YES)
2023-02-25 10:59:30.722368	[redacted]	419978/QUSER/QZRCSRVS	QSYS	QZRCSRVS	QSYS/CHGAUT OBJ('/QIBM/UserData/OS400/Navigator/preferences/') USER(*PUBLIC) DTAAUT(*WX) OBJAUT(*ALL) SUBTREE(*ALL) SYMLNK(*YES)

ACHTUNG: Änderung Systemeinstellungen

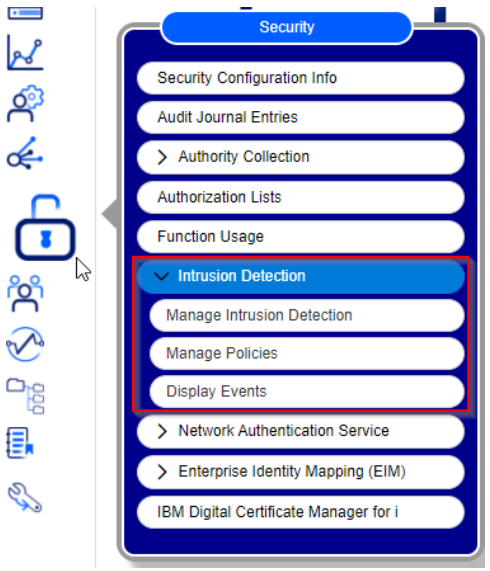
- **ACHTUNG**
- „Unbeabsichtigte" Änderungen von systemweiten Einstellungen sind leicht möglich
- z.B. beim Menü Audit Journal Entries ändert die Option Auditing Configuration direkt die betreffenden System Values
- Regler nach rechts/links aktiviert/deaktiviert direkt den betreffenden Wert
- Eine eigene Bestätigung „Sind Sie sicher?" gibt es nicht





Intrusion Detection System (IDS) – V7R5

- Überwachung des TCP/IP Netzwerks
  - Intrusion Events: nicht berechtigte Versuche in das System einzudringen
  - Extrusion Events: System wird als Source für Angriffe auf andere Systeme verwendet
- Definition über Policies
- Protokollierung im Audit Journal
- Anzeige via IBM Navigator for i
- Verständigung via QSYSOPR oder E-Mail



Event Details

Detected by policy:	QIBM_Scan
Date and time:	Sat Feb 25 15:16:02 CET 2023
Intrusion type:	Scan
Direction:	Inbound
Protocol:	6 (TCP - Transmission Control Protocol)
Local IP address:	127.0.0.1
Local port:	5989
Remote IP address:	127.0.0.1
Remote port:	24885
IDS packet throttling active:	No
Number of discarded packets:	0
TCP/IP stack:	Production stack
Audit sequence number:	1696

Suspected packet:

```
450000400000400040060000 7f0000017f0000016135176 54d38742000000000b00
2ffff000000000204ffd7010303060101080aee2094340000000001010402
```

Intrusion Detection Policies

Actions

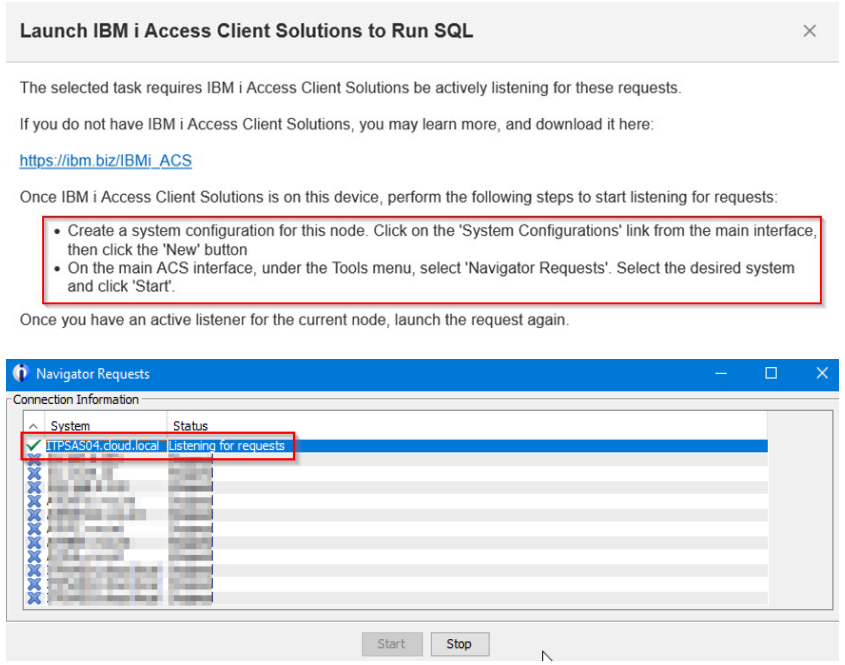
Policy Name	Policy Type	Status	Local IP Addresses	Local Ports	Remote IP Addresses	Remote Ports	Description
QIBM_Address_Poisoning	Attack (Address Poisoning)	Enabled	All	All	All	All	IBM-supplied default address poisoning attack policy
QIBM_Flood	Attack (Flood)	Enabled	All	All	All	All	IBM-supplied default flood attack policy
QIBM_Fraggle	Attack (Fraggle)	Enabled	All	All	All	All	IBM-supplied default Fraggle attack policy
QIBM_ICMP_Redirect	Attack (ICMP Redirect)	Enabled	All	All	All	All	IBM-supplied default ICMP redirect attack policy
QIBM_IP_Fragment	Attack (IP Fragment)	Enabled	All	All	All	All	IBM-supplied default IP fragment attack policy
QIBM_Malformed_Packet	Attack (Malformed Packet)	Enabled	All	All	All	All	IBM-supplied default malformed packet attack policy

Intrusion Detection Events- Last 1 Days

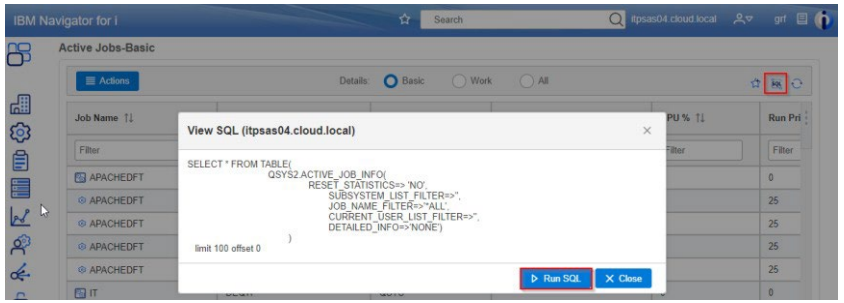
Actions

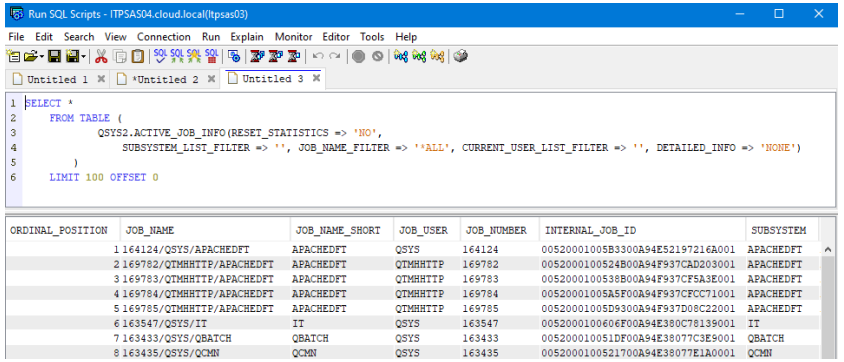
Date and Time	Type	Direction	Local IP Address	Local Port	Remote IP Address	Remote Port
Sat Feb 25 15:16:02 CET 2023	Scan	Inbound	127.0.0.1	5989	127.0.0.1	24885
Sat Feb 25 15:16:02 CET 2023	Scan	Outbound	127.0.0.1	24885	127.0.0.1	5989
Sat Feb 25 15:16:02 CET 2023	Scan	Inbound	127.0.0.1	5989	127.0.0.1	26867
Sat Feb 25 15:16:02 CET 2023	Scan	Outbound	127.0.0.1	26867	127.0.0.1	5989

IBM i Services (SQL) evaluieren



- Informationen im Webinterface direkt als SQL-Statement ausführen
- Navigator Requests in IBM i Access Client Solutions starten
- Über den SQL-Button im Webinterface Run SQL drücken
- Im Run SQL Scripts Fenster wird das SQL-Statement automatisch eingefügt
- Filter werden übernommen, Spaltenauswahl nicht
- Alternativ kann das Statement auch direkt über copy/paste übernommen werden





IBM i Services (SQL)

IBM i Services (SQL)

- Zugriff auf viele System Services mittels system-provided SQL views, procedures und functions
- SQL Interface um auf System Informationen zuzugreifen
- Keine Notwendigkeit mehr Programme zu entwickeln (System API's)
- Werden laufend von der IBM weiterentwickelt
- Je nach OS und PTF Level sind unterschiedliche Services verfügbar

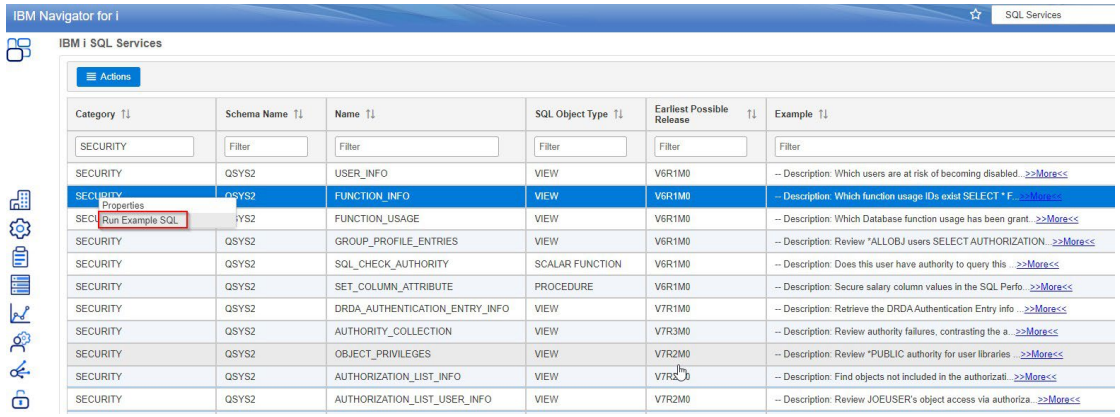
- Liste der Services
  - online unter IBM i Services (SQL)
  - Via IBM Navigator for i

IBM i Services (SQL)

Content

You are in: IBM i Technology Updates > Db2 for i - Technology Updates > IBM i Services (SQL)

IBM i Service	Type of Service	IBM i 7.5	IBM i 7.4	IBM i 7.3	IBM i 7
Application Services					
QSYS2.ACTIVATION_GROUP_INFO()	Table function	Base	SF99704 Level 20	SF99703 Level 28	Not Suppo
QSYS2.ADD_USER_INDEX_ENTRY()	Procedure	Base	SF99704 Level 20	Not Supported	Not Suppo
QSYS2.ADD_USER_INDEX_ENTRY_BINARY()	Procedure	Base	SF99704 Level 20	Not Supported	Not Suppo
QSYS2.BINDING_DIRECTORY_INFO	View	Base	SF99704 Level 20	SF99703 Level 28	Not Suppo
QSYS2.BOUND_MODULE_INFO	View	Base	SF99704 Level 4	SF99703 Level 16	Not Suppo
QSYS2.BOUND_SRVPGM_INFO	View	Base	SF99704 Level 4	SF99703 Level 16	Not Suppo



System Values

- View QSYS2.SYSTEM_VALUE_INFO liefert den Namen und Wert aller Systemvalues des Systems
- OS: WRKSYSVAL SYSVAL(*ALL)
- API: QWCRSVAL

```sql
-- List all Systemvalues
SELECT SYSTEM_VALUE_NAME AS "NAME",
       COALESCE(CURRENT_CHARACTER_VALUE,CHAR(CURRENT_NUMERIC_VALUE)) AS "VALUE"
FROM QSYS2.SYSTEM_VALUE_INFO
ORDER BY SYSTEM_VALUE_NAME;
```

NAME	VALUE
QABNORMSW	0
QACGLVL	*NONE
QACTJOB	200
QADLACTJ	30
QADLSPLA	2048
QADLTOTJ	30
QALWJOBITP	0
QALWOBJRST	*ALL
QALWUSRDMN	*ALL
QASTLVL	*BASIC
QATNPGM	QEZMAIN QSYS

Security Information

- View QSYS2.SECURITY_INFO liefert eine Zeile mit Informationen zur IBM i Security Konfiguration
- OS: DSPSECA, DSPSECAUD
- API: QSYRTVSA

- Dieses Beispiel zeigt die laufende Weiterentwicklung von IBM

For complete detail, visit this IBM Documentation page: SECURITY_INFO view

Enhanced with IBM i 7.5 SF99950 Level 1:

- Add ALLOW_PASSWORD_EXIT_PROGRAM_ADD_REMOVE column

Enhanced with IBM i 7.4 SF99704 Level 15 and IBM i 7.3 SF99703 Level 26:

- Add the following columns:
  VERIFY_OBJECT_RESTORE, ALLOW_OBJECT_RESTORE, USE_ADOPTED_AUTHORITY, ALLOW_USER_DOMAIN,
  LIMIT_SECOFR_ACCESS, INACTIVE_JOB_TIMEOUT, INACTIVE_JOB_MESSAGE_QUEUE,
  DISCONNECTED_JOB_INTERVAL, AUTOCONFIGURE_DEVICES, and
  AUTOCONFIGURE_REMOTE_CONTROLLERS

```
1  -- List Security Information
2  SELECT *
3  FROM QSYS2.SECURITY_INFO;
4
5
```

SECURITY_LEVEL	PENDING_SECURITY_LEVEL	PASSWORD_LEVEL	PENDING_PASSWORD_LEVEL	AUDIT_JOURNAL_EXISTS
40	-	3	-	YES

User Information

- Views QSYS2.USER_INFO und QSYS2.GROUP_PROFILE_ENTRIES liefern detailierte Informationen zu Benutzer und Gruppen Profilen
- Informationen einzelner Services können leicht miteinander kombiniert werden
- Filtern auf bestimmte Werte z.B. *ALLOBJ,*SECADM,*AUDIT Special Authorities ist möglich
- Sowohl Einträge des GroupProfiles sowie SupplementalGroupProfiles können berücksichtigt werden
- OS: WRKUSRPRF USRPRF(*ALL)
- API: QSYSUSRI

```sql
-- User Informationen
SELECT *
FROM QSYS2.USER_INFO;

-- Group Profile Information
SELECT *
FROM QSYS2.GROUP_PROFILE_ENTRIES;
```

AUTHORIZATION_NAME	PREVIOUS_SIGNON	STATUS	PASSWORD_CHANGE_DATE	NO_PASSWORD_INDICATOR
QPM400	-	*ENABLED	2019-06-05 17:01:02.000000	YES
QRJE	-	*ENABLED	2019-06-05 17:01:01.000000	YES
QSECOFR	2023-02-20 01:11:33.000000	*ENABLED	2019-06-05 19:19:31.000000	NO
QSNADS	-	*ENABLED	2019-06-05 17:01:01.000000	YES
QSPL	-	*ENABLED	2019-06-05 17:01:01.000000	YES
QSPLJOB	-	*ENABLED	2019-06-05 17:01:01.000000	YES

GROUP_PROFILE_NAME	USER_PROFILE_NAME	USER_TEXT
ITAPP	ITPS[redacted]	IT-PS [redacted] *ALLOBJ Profile
ITGIT	[redacted]	IT-PS [redacted]
ITOPR	FERIALI	IT-PS Ferialpraktikanten
ITOPR	[redacted]	IT-PS [redacted]

AUTHORIZATION_NAME	GROUP_PROFILE_NAME	USR_SPECIAL_AUTHORITIES								GRP_SPECIAL_AUTHORITIES						
[redacted]	QWQADMGRP	*ALLOBJ	*SECADM	*JOBCTL	*SPLCTL	*SAVSYS	*SERVICE	*AUDIT	*IOSYSCFG	-						
[redacted]	ITOPR	*ALLOBJ	*SECADM	*JOBCTL	*SPLCTL	*SAVSYS	*SERVICE	*AUDIT	*IOSYSCFG	*ALLOBJ	*SECADM	*JOBCTL	*SPLCTL	*SAVSYS	*SERVICE	*AUD
QLPAR		*ALLOBJ	*SECADM	*JOBCTL	*SPLCTL	*SAVSYS	*SERVICE	*AUDIT	*IOSYSCFG	-						
QLPAUTO		*ALLOBJ	*SECADM	*JOBCTL	*SAVSYS	*IOSYSCFG				-						
QLPINSTALL		*ALLOBJ	*SECADM	*JOBCTL	*SAVSYS	*IOSYSCFG				-						
QSECOFR		*ALLOBJ	*SECADM	*JOBCTL	*SPLCTL	*SAVSYS	*SERVICE	*AUDIT	*IOSYSCFG	-						

User Profile mit PUBLIC Berechtigung

- Table Function QSYS2.OBJECT_PRIVILEGES liefert eine Zeile für jeden authorisierten User des betreffenden Objektes
- Andere SQL-Syntax im Vergleich zu Views
- Grundsätzlich sind alle Objekt Type der IBM i unterstützt
- Neben AuthorizationLists werden auch Primary Group sowie Objekt- und Datenberechtigungen angezeigt
- OS: DSPOBJAUT

```
1  -- UserProfiles - Public Authority (basic)
2
3  SELECT *
4  FROM TABLE(QSYS2.OBJECT_PRIVILEGES('QSYS','QDBSHR','*USRPRF'));
5
```

AUTHORIZATION_USER	OBJECT_AUTHORITY	AUTHORIZATION_LIST	PRIMARY_GROUP	OWNER	OBJECT_OWNER	OBJECT_OPERATIONAL	OBJECT_MANAGEMENT	OBJECT_EXISTENCE	DATA_READ	DATA_UPDATE
*PUBLIC	USER DEFINED	-	-	QSYS	NO	NO	NO	NO	NO	NO
QSYS	*ALL	-	-	QSYS	YES	YES	YES	YES	YES	YES
QDBSHR	*CHANGE	-	-	QSYS	NO	YES	NO	NO	YES	YES

Audit Journal Auswertung (Security)

- Table Function QSYS2.DISPLAY_JOURNAL liefert Informationen zu Journal Einträgen
- Filtern nach Journal Code und Type z.B:

```
T AF Authority Failure
T CA Authority Changes
T CP User Profile changed, created or restored
…
```

- Abhängig von den Einstellungen der Audit Relevanten Systemvalues
- OS: DSPJRN JRN(QAUDJRN)
- API: QjoRetrieveJournalEntries

```sql
-- Audit Journal Auswertung
SELECT ENTRY_TIMESTAMP
       ,JOURNAL_CODE
       ,JOURNAL_ENTRY_TYPE
       ,JOB_NAME
       ,JOB_USER
       ,JOB_NUMBER
       ,PROGRAM_NAME
       ,PROGRAM_LIBRARY
       ,CAST(ENTRY_DATA AS VARCHAR(30)) as ENTRY_DATA
FROM TABLE (QSYS2.DISPLAY_JOURNAL('QSYS', 'QAUDJRN',                              -- Journal library and name
                                  STARTING_TIMESTAMP => CURRENT TIMESTAMP - 24 HOURS  -- Time period
                                 ));

```

ENTRY_TIMESTAMP	JOURNAL_CODE	JOURNAL_ENTRY_TYPE	JOB_NAME	JOB_USER	JOB_NUMBER	PROGRAM_NAME	PROGRAM_LIBRARY	ENTRY_DATA
2023-02-24 17:22:27.760864	T	CP	QPADEV000D	[redacted]	037338	QCMD	QSYS	A[redacted] QSYS *USRPRF C
2023-02-24 17:18:18.191360	T	CP	QPADEV000D	[redacted]	037338	QCMD	QSYS	A[redacted] QSYS *USRPRF C
2023-02-24 17:00:03.674208	T	CA	AMQZLAA0	QMQM	031476	LIBMQMAS_R	QMQM	A*N *N *STMF Q
2023-02-24 17:00:03.674176	T	CA	AMQZLAA0	QMQM	031476	LIBMQMAS_R	QMQM	A*N *N *STMF Q
2023-02-24 17:00:03.674128	T	CA	AMQZLAA0	QMQM	031476	LIBMQMAS_R	QMQM	A*N *N *STMF *
2023-02-24 17:00:03.572736	T	CA	AMQZLAA0	QMQM	031476	LIBMQMCS_R	QMQM	A*N *N *STMF Q

Audit Journal Auswertung (IP-Verbindungen)

- Mit demselben Service QSYS2.DISPLAY_JOURNAL können auch Remote Verbindungen zur IBM I ausgewertet werden
- Vorraussetzung ist auch hier das die betreffenden Einträge mittels Audit Journal protokolliert werden

ENTRY_TIMESTAMP	LOCAL_IP	LOCAL_PORT	REMOTE_IP	REMOTE_PORT	REMOTE_ADDRESS	JOB_NAME	JOB_USER	CURRENT_USER	CONNECTIONSTATUS
2023-02-24 17:13:03.429504	192.168.	9476	10.	48651	10.	QZSOSGND	QUSER	QUSER	Accept
2023-02-24 17:13:03.800624	192.168.	9476	10.	48652	10.	QZSOSGND	QUSER	QUSER	Accept
2023-02-24 17:13:04.174272	192.168.	9471	10.	48653	10.	QZDASRVSD	QUSER	QUSER	Accept
2023-02-24 17:13:04.629968	192.168.	9475	10.	48654	10.	QZRCSRVSD	QUSER	QUSER	Accept
2023-02-24 17:15:06.198880	192.168.	443	192.168.	51558	192.168.		QTMHHTTP	QTMHHTTP	Accept
2023-02-24 17:15:11.205696	192.168.	80	192.168.	51585	192.168.		QTMHHTTP	QTMHHTTP	Accept
2023-02-24 17:15:18.199280	192.168.	443	192.168.	51610	192.168.		QTMHHTTP	QTMHHTTP	Accept
2023-02-24 17:15:23.208896	192.168.	80	192.168.	51632	192.168.		QTMHHTTP	QTMHHTTP	Accept
2023-02-24 17:17:36.207472	192.168.	443	192.168.	52270	192.168.		QTMHHTTP	QTMHHTTP	Accept
2023-02-24 17:17:41.202896	192.168.	80	192.168.	52286	192.168.		QTMHHTTP	QTMHHTTP	Accept

TCP Service Connection Information

- View QSYS2.NETSTAT_INFO liefert Information zu IPv4 und IPv6 Netzwerkverbindungen
- z.B. Analyse offener und nicht verwendeter Ports (ssh,smtp,ldap,…)
- OS: NETSTAT OPTION(*CNN)

```
1 -- TCP Service Information
2 SELECT *
3 FROM QSYS2.NETSTAT_INFO;
4
```

CONNECTION_TYPE	LOCAL_ADDRESS	LOCAL_PORT	LOCAL_PORT_NAME	PROTOCOL	TCP_STATE	BIND_USER
IPV4	0.0.0.0	21	ftp-control	TCP	LISTEN	QTCP
IPV4	0.0.0.0	22	ssh	TCP	LISTEN	QSECOFR
IPV4	0.0.0.0	23	telnet	TCP	LISTEN	QTCP
IPV4	0.0.0.0	25	smtp	TCP	LISTEN	QTCP
IPV4	0.0.0.0	80	www-http	TCP	LISTEN	QTMHHTTP
IPV4	0.0.0.0	137	netbios-ns	TCP	LISTEN	QSYS
IPV4	0.0.0.0	139	netbios-ssn	TCP	LISTEN	QSYS
IPV4	0.0.0.0	389	ldap	TCP	LISTEN	QDIRSRV
IPV4	127.0.0.1	427	-	TCP	LISTEN	QSYS
IPV4	0.0.0.0	445	cifs	TCP	LISTEN	QSYS
IPV4	0.0.0.0	446	drda	TCP	LISTEN	QUSER
IPV4	0.0.0.0	447	ddm	TCP	LISTEN	QUSER
IPV4	0.0.0.0	448	ddm-ssl	TCP	LISTEN	QUSER
IPV4	0.0.0.0	449	as-svrmap	TCP	LISTEN	QUSER
IPV4	0.0.0.0	515	lpd	TCP	LISTEN	QTCP
IPV4	0.0.0.0	636	ldaps	TCP	LISTEN	QDIRSRV
IPV4	0.0.0.0	657	rmc	TCP	LISTEN	QSYS
IPV4	0.0.0.0	990	ftps-control	TCP	LISTEN	QTCP
IPV4	0.0.0.0	992	telnet-ssl	TCP	LISTEN	QTCP
IPV4	0.0.0.0	2002	as-admin1-http	TCP	LISTEN	QWEBADMIN
IPV4	0.0.0.0	2006	as-admin3-http	TCP	LISTEN	QWEBADMIN

CONNECTION_TYPE	LOCAL_ADDRESS	LOCAL_PORT	LOCAL_PORT_NAME	PROTOCOL	TCP_STATE	BIND_USER
IPV4	10.	992	telnet-ssl	TCP	ESTABLISHED	QTCP
IPV4	127.0.0.1	7327	-	TCP	ESTABLISHED	QSECOFR
IPV4	127.0.0.1	8473	as-file	TCP	ESTABLISHED	QUSER
IPV4	127.0.0.1	8475	as-rmtcmd	TCP	ESTABLISHED	QUSER
IPV4	10.	9471	as-database-s	TCP	ESTABLISHED	QUSER
IPV4	10.	9471	as-database-s	TCP	ESTABLISHED	QUSER
IPV4	10.	9471	as-database-s	TCP	ESTABLISHED	QUSER
IPV4	10.	9475	as-rmtcmd-s	TCP	ESTABLISHED	QUSER
IPV4	10.	9475	as-rmtcmd-s	TCP	ESTABLISHED	QUSER
IPV4	10.	9475	as-rmtcmd-s	TCP	ESTABLISHED	QUSER

NetServer - Laufwerkfreigaben

- View QSYS2.SERVER_SHARE_INFO und
  Table Function QSYS2.IFS_OBJECT_PRIVILEGES
- In Kombination ergeben beide Services einen vollständigen Überblick über die vorhanden Laufwerkfreigaben sowie deren IFS Berechtigung
- IBM I Navigator / WRKLNK
- API: QZLSLSTI, QZLSOLST

```
1  -- NetServer
2  WITH NFS AS
3  (
4      SELECT *
5      FROM QSYS2.SERVER_SHARE_INFO
6      WHERE SHARE_TYPE = 'FILE'
7  )
8      SELECT NFS.SERVER_SHARE_NAME
9             ,NFS.PATH_NAME
10            ,NFS.PERMISSIONS
11            ,AUTHORIZATION_NAME
12            ,DATA_AUTHORITY
13            ,NFS.TEXT_DESCRIPTION
14     FROM NFS,
15     LATERAL (
16                 SELECT *
17                 FROM TABLE
18                 (QSYS2.IFS_OBJECT_PRIVILEGES(PATH_NAME => PATH_NAME))
19             );
```

SERVER_SHARE_NAME	PATH_NAME	PERMISSIONS	AUTHORIZATION_NAME	DATA_AUTHORITY	TEXT_DESCRIPTION
QDIRSRV	/QIBM/ProdData/OS400/DirSrv	*RW	*PUBLIC	*RX	OS/400 -- Directory Services
QDIRSRV	/QIBM/ProdData/OS400/DirSrv	*RW	QSYS	*RWX	OS/400 -- Directory Services
QDIRSRV	/QIBM/ProdData/OS400/DirSrv	*RW	QDIRSRV	*RWX	OS/400 -- Directory Services
PRODDATA	/QIBM/ProdData	*R	*PUBLIC	*RX	-
PRODDATA	/QIBM/ProdData	*R	QSYS	*RWX	-
PRODDATA	/QIBM/ProdData	*R	QDIRSRV	*X	-
HOME	/home	*RW	*PUBLIC	*RWX	-
HOME	/home	*RW	QSYS	*RWX	-

SSHD-Konfiguration

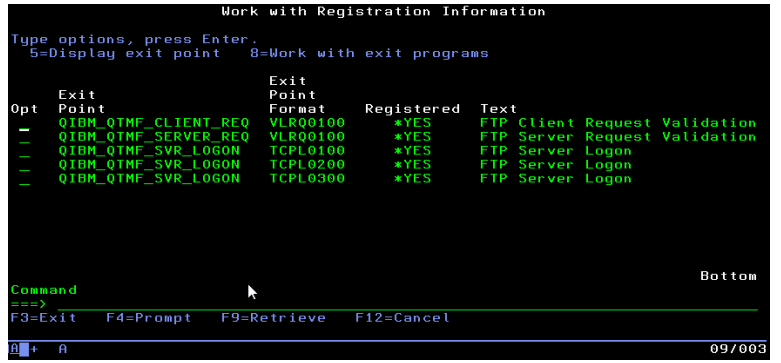
- Table Function QSYS2.IFS_READ liest den Inhalt von Streamfiles im Integrated File System
- WRKLNK

```sql
-- SSHD-Konfiguration
SELECT *
FROM TABLE(QSYS2.IFS_READ(
    PATH_NAME => '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config',
    END_OF_LINE => 'LF'));
```

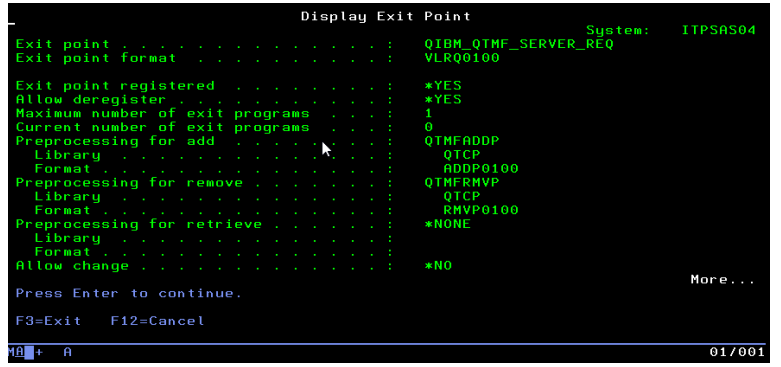
LINE
#$OpenBSD: sshd_config,v 1.75 2007/03/19 01:01:29 djm Exp $
This is the sshd server system-wide configuration file. See
sshd_config(5) for more information.
This sshd was compiled with PATH=/QOpenSys/usr/bin:/usr/ccs/bin:/QOpenSys/usr/bin/X11:/usr/sbin:.:/us...
The strategy used for options in the default sshd_config shipped with
OpenSSH is to specify options with their default value where
possible, but leave them commented. Uncommented options change a
default value.
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

Security Exit Points

Security Exit Points



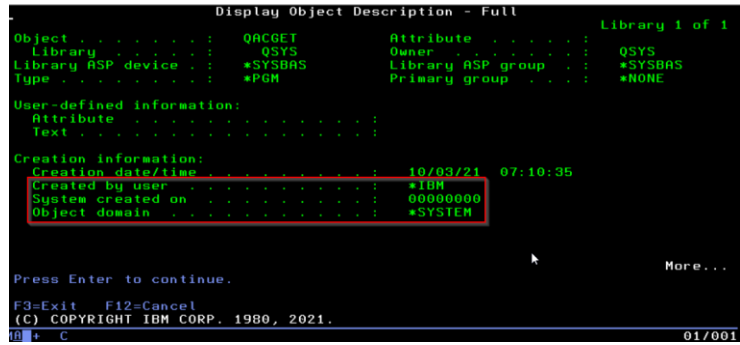
- IBM i stellt für einige System Funktionen Exit Points zur Verfügung
- Bieten die Möglichkeit selbst entwickelte Programme auszuführen
- Erweitertes Logging (in eigenen Tabellen)
  sowie zusätzliche Überprüfungen (z.B. Zugriff auf Objekt Ebene)
  bis zur Validierung des Zugriffes (Blocken/Erlauben) sind möglich
- z.B. Ausführung eines Exit Programms das jedes mal ausgeführt wird wenn eine FTP Verbindung aufgebaut wird
- Nachstehende eine Liste der Security relevanten Exit Points:
  - Zahlreiche TCP/IP Server (FTP, TELNET, REXEC, …)
  - ODBC Verbindungen
  - Remote Sign On
  - Client requests via ACS (Virtual Printer, File Transfer, Message Queue, Remote SQL …)
  - Distributed Data Management (DDM)
  - Password Validation
  - User Profile Changes



- Details und weiterführende Informationen - [Using security exit programs - IBM Documentation]

Fragen

- Passwort Default nicht auf User=Passwort
  - Mit der Definition der Password Rules und forcen der Einstellungen mittels Systemvalue QPWDRULES -> *ALLCRTCHG kann verhindert werden das Defaultpassworte = User gesetzt werden
- Identifizieren von Programmen die Original von der IBM ausgeliefert werden
  - Mittels Objektbeschreibung verifizieren das Object Domain auf *SYSTEM und Created by User auf *IBM gesetzt sind DSPOBJD OBJ(QSYS/QACGET) OBJTYPE(*PGM) DETAIL(*FULL)



The System is NOT Old….

It´s what you have choosen to do with the system that defines it's ´age'

www.it-ps.at

Klaus Haderer
Geschäftsführer
+43-664-3906530
klaus.haderer@it-ps.at

IT-Power Services GmbH
Modecenterstraße 14, 1030 Wien