



Securing your System Without Breaking your Business

Carol Woodbury, CISSP, CRISC
IBMCHAMPION 
IBM i Security SME and Senior Advisor
carol@kisco.com





© Kisco Systems LLC, All Rights Reserved.

1



Oh no! My Security Change Broke Something!



2

Removing Access



3

How Do You Safely Remove Access?

Answer: Authority Collection!

Examples:

- Determining what a developer is doing so *ALLOBJ can be removed
- Determining what profiles are accessing objects (e.g., database files, directories, etc) so *PUBLIC can be set to *EXCLUDE



4

Define Collection on Specific Libraries

Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

Type of authority collection . . .	<u>*USRPRF</u>	*USRPRF, *OBJAUTCOL
User profile	> <u>DEVELOPER</u>	Name
Library and ASP device:		
Library	> <u>PROD_LIB</u>	Name, *NONE, *ALL
ASP device	<u>*SYSBAS</u>	Name, *SYSBAS
Library		
ASP device	> <u>QSYS</u>	Name
	<u>*SYSBAS</u>	Name, *SYSBAS
Library		
ASP device	> <u>QSYS2</u>	Name
	<u>*SYSBAS</u>	Name, *SYSBAS
+ for more values		
Object	<u>*ALL</u>	Name, generic*, *ALL
+ for more values		
Object type	<u>*ALL</u>	*ALL, *CMD, *DTAARA...
+ for more values		

More...

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display

F24=More keys

5

Start the Collection – Navigator for i

Security

Security Configuration Info

Audit Journal

Authority Collection

Users

Objects

Authorization Lists

Manage authority collection for users

0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
CPU Utilization (Average)

Authority Collection for a User

User: developer Browse

Display Authority Collection Options

Summary

View Collection

Authorization Failure

Programs and Commands

Database Files

IFS Directories

Authority Collection Actions

Start Authority Collection

End Authority Collection

Start Authority Collection

User*: DEVELOPER

Libraries to include: PROD_LIB QSYS QSYS2 Browse

Objects to include: *ALL Browse

Object types: *ALL Browse

Include document library objects: None

Include IFS objects: None Browse

Delete previous collection? Yes

Details: Object information


Libraries to omit: None Browse

6

View Authority Required

```
160 SELECT DISTINCT authorization_name,
161     system_object_name,
162     system_object_schema,
163     system_object_type,
164     detailed_required_authority,
165     current_authority,
166     authority_source,
167     current_adopted_authority
168 FROM qsys2.authorization_collection
169 WHERE authorization_name = 'DEVELOPER'
170     AND current_adopted_authority IS null
171     AND check_any_authority = '0',
172 stop
```

Authorization Name	System Object Name	System Object Schema	System Object Type	Detailed Required Authority	Current Authority	Authority Source
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	AUTHORITY_SOURCE
DEVELOPER	DSPUSRPRF	QSYS	*CMD	*OBJOPR *READ *EXECUTE	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLES	PROD_LIB	*FILE	*READ	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLES	PROD_LIB	*FILE	*OBJOPR	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLES	PROD_LIB	*FILE	*OBJOPR *READ	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLES	PROD_LIB	*FILE	*OBJMGT *OBJOPR *READ *EXECUTE	*USE	AUTHORIZATION LIST ...
DEVELOPER	PAYABLES	PROD_LIB	*FILE	*OBJMGT *OBJOPR *READ *EXECUTE	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLEST	PROD_LIB	*FILE	*OWNER	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLEST	PROD_LIB	*FILE	*OBJOPR	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLEST	PROD_LIB	*FILE	*OBJMGT	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLEST	PROD_LIB	*FILE	*OBJEXIST	*ALL	USER *ALLOBJ
DEVELOPER	PAYABLEST	PROD_LIB	*FILE	*OBJEXIST *OBJOPR	*ALL	USER *ALLOBJ



7

Goals: *PUBIC *EXCLUDE, Reduce Private Autos


Edit Object Authority

Object : ALLOBJUSRS Owner : CWOODBURY
Library : CAROLNEW Primary group : *NONE
Object type : *FILE ASP device : *SYSBAS

Type changes to current authorities, press Enter.

Object secured by authorization list : *NONE

User	Group	Object Authority
*PUBIC		<u>*ALL</u>
CWOODBURY		<u>*ALL</u>
CWOODBURYT		<u>*CHANGE</u>
DEVELOPER		<u>*CHANGE</u>
SCOTT		<u>*ALL</u>
TIMMR		<u>*USE</u>



8

Configure Authority Collection for an Object

Configure collection for a file in a library:

```

Change Authority Collection (CHGAUTCOL)

Type choices, press Enter.

Object . . . . . /qsys.lib/yourlib.lib/yourobj.file_
Authority collection value . . . *objinf          *NONE, *OBJINF  ←
Include dependent objects . . . *NO            *NO, *LF
Directory subtree . . . . . *NONE              *NONE, *ALL
Symbolic link . . . . . *NO                    *NO, *YES
Delete collection . . . . . *NO                 *NO, *YES  ←

```

Start the collection:

```

                                Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

Type of authority collection . . > *OBJAUTCOL      *USRPRF, *OBJAUTCOL
Delete collection . . . . . *NO                  *NO, *YES, *ALL

```



9

Object Authority Collection – New Nav

The screenshot shows the 'Security' configuration page. Under 'Security Configuration Info', the 'Authority Collection' section is expanded, revealing 'Users' and 'Objects'. A red arrow points to the 'Objects' link. Below this, the 'Authorization List' section is partially visible, with the text 'Manage authority collection for objects'.

The screenshot shows a web interface for managing authority collections. At the top, the title is 'Authority Collection for Objects'. Below it, a red-bordered box contains the 'Authority collection status' section, which states 'Authority collection for objects is currently: On' and has 'Start' and 'Stop' buttons. Below this box is the 'Display Authority Collection Options' section with a blue 'View Collection' button. At the bottom is the 'Authority Collection Actions' section, which contains two buttons: 'Change Authority Collection' and 'Delete Authority Collection'. A red arrow points to the 'Change Authority Collection' button.

Change Authority Collection

Object:

/qsys.lib/carolnew.lib/allobjusr.sfile

Authority information should be collected for this object:

Yes

Include dependent objects:

No

Delete previous collection:

No

Directory subtree:

None

Symbolic link:

No

OK

Cancel



10

View Profiles Accessing ALLOBJUSRS *FILE

```
116 SELECT DISTINCT authorization_name,
117     system_object_name,
118     detailed_required_authority,
119     authority_source
120 FROM qsys2.authorization_collection_libraries
121 WHERE system_object_name = 'ALLOBJUSRS'
122     AND adopting_program_owner IS null
123     AND adopt_authority_used = 0
124     AND check_any_authority = '0'
125     AND authorization_name IS NOT null
126 order by authority_source;
```

Authorization Name	System Object Name	Detailed Required Authority	Authority Source
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	DETAILED_REQUIRED_AUTHORITY	AUTHORITY_SOURCE
SCOTT	ALLOBJUSRS	*OBJOPR *READ	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*OBJOPR *ADD	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*READ	USER *ALLOBJ
DEVELOPER	ALLOBJUSRS	*READ	USER PRIVATE
DEVELOPER	ALLOBJUSRS	*OBJOPR	USER PRIVATE
CWOODBURYT	ALLOBJUSRS	*READ	USER PRIVATE
CWOODBURYT	ALLOBJUSRS	*OBJOPR	USER PRIVATE

11

The Results

Display Authority Collection - Library objects

Actions

User

Object

Object Type


Authority Source

Detailed Current Authority

Detailed Required Authority

c	c	Filter	Filter	Filter	Filter
CWOODBURY	CAROLNEW/ALLOBJUSRS	*FILE	USER *ALLOBJ	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*ADD
CWOODBURY	CAROLNEW/ALLOBJUSRS	*FILE	USER *ALLOBJ	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ
CWOODBURY	CAROLNEW/ALLOBJUSRS	*FILE	USER *ALLOBJ	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ *DLT
CWOODBURY	CAROLNEW/ALLOBJUSRS	*FILE	USER *ALLOBJ	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ *ADD *DLT *UPD


12



Options for Allowing Access

- *PUBLIC authority (not recommended for objects containing data)
- *ALLOBJ special authority assigned to the user's or group's profile (also not recommended)
- User or group private authority to the object
- User or group authorized to an authorization list securing the object
- Adopted authority (only valid for objects in libraries)

13



Authority Search Order

*ALLOBJ
Private
Authorization List

*ALLOBJ
Primary Group
Private
Authorization List

Object or
Authorization List

Adopted

RCAC

USER

GROUP(S)

*PUBLIC or
*PUBLIC(*AUTL)

STOP

Repeats for each group until
sufficient authority is
accumulated or no more groups

Checked when no authority is
found for User or Group(s)

Checks program owner's authority
when authority is not sufficient – 'One
last chance'

Must have authority to the object
before RCAC permissions are
checked

14

Use Authorization Lists to Secure Files

- Easy to manage multiple files requiring the same authorities (whether *FILE or *STMF objects)
- Can adjust authorities to an authorization list – even if the objects it secures are locked
 - HUGE bonus for Db2 files!
- Attaching an *AUTL is a two-step process
 - GRTOBJAUT OBJ(PROD_LIB/OVERDUE) OBJTYPE(*FILE) AUTL(AR_AUTL)
 - GRTOBJAUT OBJ(PROD_LIB/OVERDUE) OBJTYPE(*FILE) USER(*PUBLIC) AUT(*AUTL)



15

Go About your Changes S L O W L Y

- Roll-out authority changes one at a time and test each one.
- *PUBLIC authority should be the last authority modified
- Proactively look for authority failures (AF audit journal entries or authority_check_successful field in the Authority Collection views)



16

For Example ...

Edit Authorization List

Object : AR_AUTL

Library : QSYS

Type changes to current authorities, press Enter.

Owner : CWOODBURY

Primary group . . . : *NONE

User	Object Authority	List Mgt
*PUBLIC	*CHANGE	—
CWOODBURY	*ALL	X
AIAGENT1	*CHANGE	—
DEVELOPER	*USE	—
SERVICE1	*USE	—
SRIEDMUELL	*USE	—

1. Add individual profile (SRIEDMUELL)


2. Add the DEVELOPER group (remove SRIEDMUELL)

3. Add SERVICE1 – test

4. Add AIAGENT1 – test

5. Change *PUBLIC to *EXCLUDE

Bottom



17

Utilize Function Usage



18

- Increased use by the OS in IBM i 7.5 and 7.6
- Provides a way to control (allow or restrict) actions
- Many options for not assigning a special authority (such as *ALLOBJ or *IOSYSCFG) when performing certain tasks
- For the list of all IBM-supplied functions and what they control, see the IBM i Security Reference manual, Appendix H



19

Dashboard

Home

Work Management

Configuration and Service

System

Monitors

My Work

Network

Security

Users and Groups

Performance

File System

Function Usage

Actions

Function ID

Description

Category

Default Usage

Filter

Filter

host

Filter

QIBM_LIST_ALL_OBJS

Return list of all objects from list interfaces

Host

DENIED

QIBM_LIST_ALL_OBJS_SQL

Return list of all objects from SQL services

Host

DENIED

QIBM_QZLS_NETSVR_SHARE

Allow object owner to modify IBM i Net Server share without *IOSYSCFG special authority.

Host

DENIED

QIBM_IOSYSCFG_VIEW

Allows the ability to view Input/Output system configuration information.

Host

DENIED

QIBM_RUN_UNDER_USER_NO_AUTH

Run under a user without verifying the authentication information for the user

Host

ALLOWED

QIBM_ACCESS_ALLOBJ_JOBLOG

If a user has *JOBCTL special authority, provide access to the job log of a job with *ALLOBJ special authority.

Host

DENIED

QIBM_ALLOBJ_TRACE_ANY_USER

Trace any user function

Host

DENIED



20

Find Profiles with a Special Authority

```
122 -- category: IBM i Services
123 -- description: Security - Review *ALLOBJ users
124 --
125 -- Which users have *ALLOBJ authority either directly
126 -- or via a Group or Supplemental profile?
127 -- To find profiles with other special authorities, replace all instances of *ALLOBJ with the other value, e.g., *IOSYSCFG
128 --
129 SELECT AUTHORIZATION_NAME,
130        STATUS,
131        NO_PASSWORD_INDICATOR,
132        PREVIOUS_SIGNON,
133        TEXT_DESCRIPTION
134 FROM QSYS2.USER_INFO
135 WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'
136      OR AUTHORIZATION_NAME IN (SELECT USER_PROFILE_NAME
137                                FROM QSYS2.GROUP_PROFILE_ENTRIES
138                                WHERE GROUP_PROFILE_NAME IN (SELECT AUTHORIZATION_NAME
139                                                              FROM QSYS2.USER_INFO
140                                                              WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'))
141 ORDER BY AUTHORIZATION_NAME;
```

Authorization Name	Status	No Password Indicator	Previous Signon	Text Description
AUTHORIZATION_NAME	STATUS	NO_PASSWORD_INDICATOR	PREVIOUS_SIGNON	TEXT_DESCRIPTION
CJWPUBLIC	*DISABLED	YES	-	Powerful profile not *EXCLUDE
COMMONBE	*DISABLED	NO	-	Common Belgium Users
CONNORAH	*DISABLED	NO	-	-
CWOODBURY	*ENABLED	NO	2026-04-13 10:57:51.000000	Carol Woodbury
CWOODBURYT	*ENABLED	NO	2025-08-25 19:07:03.000000	Menu user
DAVIDAJ	*DISABLED	NO	2025-02-26 10:00:59.000000	David Crow - AJS
DAWN	*DISABLED	NO	2025-05-13 11:35:11.000000	second dawn may profile for demo purposes

21

Granting “Function Usage” – Navigator for i

Configuration and Service

System

Monitors

My Work

Network

Security

Users and Groups

Performance

File System

Security

Security Configuration Info

Audit Journal

Authority Collection

Authorization Lists

Function Usage

Intrusion Detection

Cryptographic Coprocessors

CVE Information

Work with function usage, also known as the Application Administration support in the past

Function Usage

Actions

Function ID T1

Function Name T1

Default Usage T1

All Object Indicator T1

ALLOBJ

Filter

QIBM_ACCESS_ALLOBJ_JOBLOG

Access job log of *ALLOBJ job

DENIED

USED

QIBM_ALLOBJ_TRACE_ANY_USER

Trace any user

DENIED

USED

Filtered Rows: 2 | Total Rows: 245

Change Function Usage

Function ID

Description

Default Usage

QIBM_ACCESS_ALLOBJ_JOBLOG

If a user has *JOBCTL special authority, provide access to the job log of a job with *ALLOBJ special authority.

DENIED

Usage options for the selected function IDs

Default authority:

Denied

*ALLOBJ special authority:

Used

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

Profile(s):

Browse Profiles

Access Allowed

CWOODBURY

QPGMR

Access Denied

Add

Remove

OK

Cancel

22

Cleaning up Profiles



25

Cleaning up Inactive Profiles

- Look at the right date!
 - Last sign-on is not updated by all interfaces
 - Last used /S updated whenever a job runs as that profile
 - A Sign-on date with a blank Last used date indicates the profile hasn't been used on the current hardware



26

Group Profile - FYIs

- The “last used date” of a group profile is updated whenever one of its member profiles is “used”!
- The OS will never allow the deletion of a group profile that has
 - Members
 - Been granted primary group authority to an object



27

Listing Inactive Profiles with SQL

```
46 --
47 -- List User profiles that haven't been used in the last 3 months
48 --
49 SELECT user_name,
50        date(last_used_timestamp) as last_used,
51        timestamp(previous_signon, 0) as last_signon,
52        timestamp(creation_timestamp, 0) as create_time,
53        status,
54        text_description
55 FROM QSYS2.USER_INFO
56 WHERE (last_used_timestamp IS NULL
57        OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
58        AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS);
```

Authorization Name				Status	Text Description
USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	STATUS	TEXT_DESCRIPTION
#GNOTEST	-	-	2022-01-03 09:07:31	*ENABLED	-
AAATIM4	-	-	2021-07-07 09:01:55	*ENABLED	asdfasdf
AARONC	2020-03-11	2020-03-11 09:03:36	2019-05-06 14:17:45	*ENABLED	-
AATIM	-	-	2018-08-27 07:41:53	*ENABLED	Setsrggee
AATIM3	-	-	2022-10-21 13:18:20	*ENABLED	Test users
ACADMN01	2020-09-15	2020-09-15 16:15:08	2019-05-02 17:05:31	*ENABLED	Admin user for authority collection



Make sure you're looking at the right date. Last used, NOT last sign-on!

28

28

Managing Inactive Profiles with SQL

```
62 -- DISABLE User profiles that haven't been used in the last 3 months
63 -- To ensure a profile is not disabled, add it to an omission list (file QASECIDL) by running CHGACTPRFL (Change Active Profile List).
64 -- (The list ships populated with the IBM-supplied profiles.)
65 --
66 SELECT cup.*
67 FROM QSYS2.USER_INFO u,
68      TABLE (
69        SYSTOOLS.CHANGE_USER_PROFILE(P_USER_NAME => USER_NAME, P_STATUS => 'DISABLED', PREVIEW => 'YES')
70      ) cup
71 WHERE (u.user_name NOT IN (SELECT aidprf
72                            FROM QUSRSYS.QASECIDL))
73 AND ((last_used_timestamp IS NULL
74      OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
75      AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS));
76 stop;
```

USER_NAME	CHANGE_ATTEMPTED	CHANGE_SUCCESSFUL	CHGUSRPRF_COMMAND	FAILURE_MESSAGE
#GNOTEST	NO	-	QSYS/CHGUSRPRF USRPRF(#GNOTEST) STATUS('DISABLED')	-
AAATIM4	NO	-	QSYS/CHGUSRPRF USRPRF(AAATIM4) STATUS('DISABLED')	-
AARONC	NO	-	QSYS/CHGUSRPRF USRPRF(AARONC) STATUS('DISABLED')	-
AATIM	NO	-	QSYS/CHGUSRPRF USRPRF(AATIM) STATUS('DISABLED')	-
AATIM3	NO	-	QSYS/CHGUSRPRF USRPRF(AATIM3) STATUS('DISABLED')	-

Preview => 'YES' lists the profiles
Preview => 'NO' disables the profiles

<https://www.ibm.com/docs/en/i/7.6.0?topic=services-change-user-profile-table-function>

29

Hidden Gem – The Audit Journal



Using the Audit Journal

- Determining
 - If there are authority failures after restricting access or removing *ALLOBJ.
 - If anything's being created into '/' (root) or '/QOpenSys' prior to changing its authority
 - How a profile is being used
 - Connections made by service accounts prior to changing a default password or moving to a higher password level
 - Which encryption algorithms are in use prior to modifying QSSL*



31

Check for Authority Failures

```
133 -- Get more information on an authority failure (AF) that occurred during a specific timeframe
134 --
135 SELECT user_name,
136        program_library,
137        program_name,
138        violation_type_detail,
139        object_library,
140        object_name,
141        object_type,
142        path_name
143 FROM TABLE (
144     SYSTOOLS.AUDIT_JOURNAL_AF(
145         STARTING_TIMESTAMP => '2026-03-29 13:00:00',
146         ENDING_TIMESTAMP => '2026-03-29 14:59:59')
147 );
148 stop;
```

USER_NAME	PROGRAM_LIBRARY	PROGRAM_NAME	VIOLATION_TYPE_DETAIL	OBJECT_LIBRARY	OBJECT_NAME	OBJECT_TYPE	PATH_NAME
SERVICE1	QSYS	QCMD	Not authorized to object	QSYS	CJWGROUP	*USRPRF	-
SERVICE1	QSYS	QCMD	Not authorized to object	QSYS	CJWMFA	*USRPRF	-
SERVICE1	QSYS	QCMD	Not authorized to object	QSYS	CWOODBURY	*LIB	-

- Check for Authority Failures (AF) PRIOR to making any changes to understand current 'false positives'



32

Is Anything Being Created into '/' ?

132 --

133 -- description: Look for processes creating something into root in the last two weeks before setting *PUBLIC to DTAUT(*RX) OBJAUT(*NONE)

134 --

135 SELECT entry_timestamp,

136 user_name,

137 qualified_job_name,

138 program_library,

139 program_name,

140 path_name

141 FROM TABLE (

142 systools.audit_journal_co(STARTING_TIMESTAMP => CURRENT_TIMESTAMP - 14 DAYS)

143)

144 WHERE path_name NOT LIKE '/%/%';

145 stop;

146

ENTRY_TIMESTAMP	USER_NAME	QUALIFIED_JOB_NAME	PROGRAM_LIBRARY	PROGRAM_NAME	PATH_NAME
2026-03-24 11:26:15.346112	SRIEDMUJELL	565580/SRIEDMUJELL/QPADEV0009	QSYS	QCMD	/JOHN

- Must have *CREATE specified in QAUDLVL to get CO audit journal entries
- Use a WHERE clause to get to the entries you're looking for



What Jobs Did a Specific Profile Run?

163 --

164 -- What jobs did a specific profile run (in this example - CWOODBURY)?

165 --

166 SELECT entry_timestamp,

167 user_name,

168 qualified_job_name,

169 remote_address,

170 entry_type,

171 entry_type_detail,

172 job_type,

173 job_type_basic,

174 job_subtype

175 FROM TABLE (

176 systools.audit_journal_js(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)

177)

178 WHERE user_name = 'CWOODBURY'

179 ORDER BY entry_timestamp;

180 stop;

181

ENTRY_TIMESTAMP	USER_NAME	QUALIFIED_JOB_NAME	REMOTE_ADDRESS	ENTRY_TYPE	ENTRY_TYPE_DETAIL	JOB_TYP
2026-03-30 14:08:34.076208	CWOODBURY	652543/CWOODBURY/QPADEV0007	66.73.9.116	S	Start	INT
2026-03-30 14:11:15.927232	CWOODBURY	652543/CWOODBURY/QPADEV0007	66.73.9.116	B	Submit	BCH
2026-03-30 14:11:15.962176	CWOODBURY	652556/CWOODBURY/QHXHDLTU	-	S	Start	BCH
2026-03-30 14:11:15.973984	CWOODBURY	652556/CWOODBURY/QHXHDLTU	-	P	Attach prestart or batch immediate job	BCI

Requires *JOBDBA or *JOBDBAS in either QAUDLVL or at the user level (CHGUSRAUD)



Who's Making an ODBC Connection?

```
145 --
146 -- Find users of ODBC
147 --
148 SELECT DISTINCT user_name
149 FROM TABLE (
150     systools.audit_journal_GR(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
151 )
152 WHERE program_name LIKE 'QZDAS%';
153 stop;
```

USER_NAME
AECIESLA
HUTCHINSON
TIMMR
LRPOWELL
CWOODBURY
SCOTT
RMOELLER
SRIEDMUELL

Requires *SECURITY or *SECCFG in QAUDLVL

35

Connection Information

```
155 --
156 -- Find unsecured connections - specifically unsecured telnet (connections to port 23)
157 --
158 SELECT DISTINCT remote_address,
159     local_port
160 FROM TABLE (
161     systools.audit_journal_sk(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
162 )
163 WHERE local_port = '23';
164 stop;
```

REMOTE_ADDRESS	SECURE_VERSION	SECURE_PROPERTIES
207.90.244.25	TLSV1.3	TLS_AES_128_GCM_SHA256 RSA_SHA256
207.90.244.25	TLSV1.3	TLS_AES_128_GCM_SHA256 RSA_SHA256
45.79.181.251	TLSV1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 RSA_SHA256
85.217.149.36	TLSV1.3	TLS_AES_128_GCM_SHA256 RSA_SHA256

Requires *NETTELSVR
in QAUDLVL

Requires *NETSECURE
and *NETUDP in
QAUDLVL

36

Create a Data Mart to Keep Information Longer

```
-- Establish and update an Audit Journal Data Mart for the SK entry type
--
-- Create the SK data mart
CALL qsys2.manage_audit_journal_data_mart(
  journal_entry_type => 'SK',
  data_mart_library => 'YOUR_LIB',
  starting_timestamp => "FIRST",
  ending_timestamp => default,
  data_mart_action => 'CREATE');
stop;

-- Add new entries to the SK data mart
CALL qsys2.manage_audit_journal_data_mart(
  journal_entry_type => 'SK',
  data_mart_library => 'YOUR_LIB',
  starting_timestamp => "CONTINUE",
  ending_timestamp => default,
  data_mart_action => 'ADD');
stop;
```



37

Create a Data Mart to Collect Entries over Time

Manage Audit Journal Data Mart

System

Monitors

My Work

Network

Security

Security Configuration Info

MFA Configuration

Audit Journal

Manage Data Mart

Audit Journal Entries

Auditing Configuration

	Data Mart System Table Name	Data Mart Filter
	AF	
	PW	AUDIT_USER_NAME NOT LIKE '%ADM'
	PW	
DMARTLIBSK	AUDIT_JOURNAL_SK	ENTRY_TYPE IN ('C', 'S')
RPGPGM1	AUDIT_JOURNAL_LD	
SFDATEAMART	AUDIT_JOURNAL_GR	function_name like 'QIBM_RUN_UNDER
SFDATEAMART	AUDIT_JOURNAL_VP	share_type = 'FILE'

Manage

Delete

Detail View

Daily View

Weekly View

Schedule

Permissions



38

View the Audit Journal or the Data Mart

View Configuration

Use live data or the data mart

☐ Live Data

☒ Data Mart

Data Mart Library:

SF DATAMART

Select view

☒ Chart View

☐ Detail View

Select audit journal entries

☐

☒ Generic Record (GR)



Cleaning Up File Shares



Displaying File Shares is a Point in Time

The screenshot shows the IBM Navigator for i interface. The 'File Shares' section is active. A table lists various file shares. The 'ASHARE2ROOT' share is highlighted with a red triangle, indicating a Read/Write share to the root directory. A tooltip shows the 'File Shares' section is selected in the left sidebar.

Server Share Name	Path Name	Path Availability	Current Users	Permissions	Encryption Required	Authorization List
ASHARE2ROOT	/	Available	0	*RW	NO	
CAROLSHARE	/home/cjwdemo	Available	0	*RW	NO	CAROLSHARE
CLAIMIMAGE	/claimimage	Available	0	*R	NO	
COMMON	/COMMON	Available	0	*R	NO	
HOMELDB	/home/ldb	Available	0	*R	NO	
IFSLAB06	/ifslab06	Available	0	*RW	NO	
IFSLAB08	/ifslab08/reflab	Available	0	*R	NO	
IFSLAB10	/ifslab10	Available	0	*RW	NO	
IFSLAB12	/ifslab12	Available	0	*RW	NO	
File System		Available	0	*RW	NO	
Integrated File System		Available	0	*RW	NO	
File Shares		Available	0	*R	NO	

Worst possible scenario is to have a Read/Write share to root

41


*NETSMBSVR Action Audit Value (QAUDLVL)

7.6

Generates a **VP** audit entry documenting the use of a file share – including the name of the share!!!

```
303 --
304 -- description: New in IBM i 7.6!
305 --      Add *NETSMBSVR to QAUDLVL and look at the VP audit journal entries to see which shares are in use!
306 --
307 SELECT entry_timestamp,
308        audit_user_name,
309        share_name,
310        entry_type_detail,
311        share_authorization_list
312 FROM TABLE (
313     systools.audit_journal_vp(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
314 );|
315 stop;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	SHARE_NAME	ENTRY_TYPE_DETAIL	SHARE_AUTHORIZATION_LIST
2025-04-02 10:47:52.333616	CJW	*SERVER	Server or share connection established	-
2025-04-02 10:47:52.693216	CJW	ROOT	Server or share connection established	-
2025-04-02 11:20:12.253872	CJW	ROOT	Server or share connection ended	-
2025-04-02 11:20:12.337952	CJW	*SERVER	Server or share connection ended	-



kisco

42

Determining Who's Using a File Share – IBM i 7.4 and 7.5

Configure Authority Collection on the path being shared

```
272 -- To determine who's using a file share in IBM i 7.4 and 7.5, configure Authority Collection on the object being shared
273 -- This enhanced/simplified Authority Collection view added in IBM i 7.6 and IBM i 7.5 TR6
274 --
275 CL:CHGAUTCOL OBJ('/HOME/TESTNAV/') AUTCOLVAL(*OBJINF);
276 CL:STRAUTCOL TYPE(*OBJAUTCOL);
277 SELECT user_name, check_timestamp, path_name,
278        detailed_required_authority, detailed_current_authority
279 FROM qsys2.authority_collection_ifs
280 WHERE job_name LIKE 'QZLSFILE%' AND UPPER(path_name) LIKE '/HOME/TESTNAV/%';
281
282 stop;
```



43

Moving to a Higher Password Level



44

Moving to a Higher Password Level

7.5

System value	
0 / 1 are now the same	<p>Default</p> <p>Character set: A-Z, 0-9, \$, @, # and _</p> <p>Maximum length: 10</p> <p>LanMan password not stored at ANY level</p>
2	<p>Character set: Upper / lower case, all punctuation and special characters, numbers and spaces</p> <p>Maximum length: 128</p> <p>Encrypts with old and new algorithms to accommodate both levels 0/1, 2/3 and 4</p> <p>Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed</p>
3	<p>Same as level 2, gets rid of old encrypted password</p> <p>Level 4 password generated and retained</p>
4 has been added	<p>Stronger algorithm to store password hash. Only version stored is the one that works at level 4*</p> <p>*Note: Requires ACS 1.1.9.0 or higher!</p>



45

Password Hashes Stored at Each Level

Password hashes generated at QPWDVL 0/1	Password hashes generated at QPWDVL 2	Password hashes generated at QPWDVL 3	Password hash generated at QPWDVL 4
All uppercase All lowercase	> Password no longer folded for authentication	Used for authentication: Mixed case – Level 2/3	Level 4 version only
Regardless of what the user types (Car0L) the password is folded: CAR0L car0l	Used for authentication: Mixed case – Level 2/3 Hashes generated when password is changed: - Mixed case – Level 2/3 - All uppercase - All lowercase - Mixed case – Level 4	Hashes generated when password is changed: - Mixed case – Level 2/3 - Mixed case - Level 4	

- Move from 0/1 to 2, test then move to 3 (or 4)
- Cannot move directly from 0/1 to 4
- Cannot move from 4 to 0/1
- All changes require an IPL



46



47

Users

- After moving from QPWLVL 0/1 to 2, users must enter their password in either all lower case or all upper case until they perform a password change at the new level
- Many organizations force a password change (set PWDEXP to *YES) at the time of the IPL
 - Note: the system does NOT force this password change
- Best option is to push users to change their passwords BEFORE the password level change! New password hashes will be created and stored for the higher password levels and will be ready to go.
- Clearly communicate the new password composition requirements
 - Match your broader company-wide password requirements

48

Check Users Before Changing QPWLVL

```

286 -- Check which user profiles do not yet have a QPWLVL 3 (or 4) password stored
287 --
288 SELECT authorization_name, password_change_date, text_description
289     FROM qsys2.user_info_basic
290     WHERE no_password_indicator = 'NO'
291           AND password_level_2_3 = 'NO';
292
293 SELECT authorization_name, password_change_date, text_description
294     FROM qsys2.user_info_basic
295     WHERE no_password_indicator = 'NO'
296           AND password_level_4 = 'NO';
297 stop;
298 |

```

AUTHORIZATION_NAME	PASSWORD_CHANGE_DATE	TEXT_DESCRIPTION
--------------------	----------------------	------------------

CL command alternative: PRTUSRPRF TYPE(*PWLVL)



49

Other Considerations for Moving to a Higher Level

- Check connections that use a hard-coded user id / password
- If using replication software, move the target partition before the current source partition
- If using password management software, don't enforce new (stronger) rules until all partitions are at the higher level
- Save security data (SAVSECDTA) before QPWLVL 4
 - <https://www.ibm.com/docs/en/i/7.6.0?topic=changes-considerations-changing-qpwdlwl-from-2-3-4>



50

To Communicate or Not To Communicate...?



51

Getting the Project Approved

- After a breach
- Compliance requirements (New law or regulation)
- Audit requirement or finding
- You know vulnerabilities exist
 - Risk assessment (comparison against best practices)
 - Pen test (visual example of the vulnerability)

Describe the project in how it affects the business...
not in technical terms!!!



52

Use Outside Sources to Help with Management Understanding

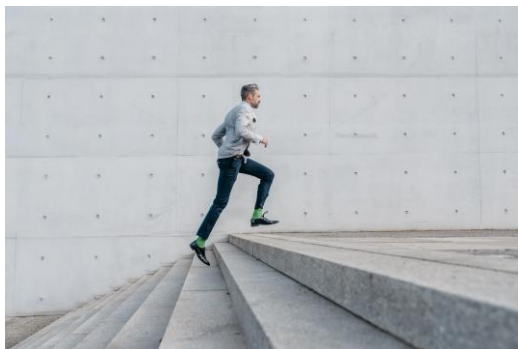
Examples:

- IBM / Ponemon Institute's Cost of a Data Breach
- Verizon Data Breach Investigations Report (DBIR)



53

Start Somewhere!!!



54

For More Information

IBM i Services- <https://www.ibm.com/support/pages/node/1119123>

Memo to Users – [7.5](#) and [7.6](#)

IBM i 7.6 Redbook - <https://www.redbooks.ibm.com/redpieces/pdfs/sg248588.pdf>

IBM i Security Reference – [PDF](#)

[IBM i Security Administration and Compliance](#), 3rd edition, by Carol Woodbury, 2020 available from Amazon or MCPress Bookstore

[Mastering IBM i Security](#) – A Step by Step Approach by Carol Woodbury, 2022 available from Amazon or MCPress Bookstore

Whitepaper: [Securing IBM i: A Dual Responsibility](#)

Articles by Steve Riedmueller and Carol Woodbury on [Kisco U](#) – free articles and tutorials, for example ...
<https://www.kisco.com/u/content/subscribe-to-ibm-notifications-for-ibm-i.html>

55



Questions?



Contact: carol@kisco.com

