


IBM i Security Cocktail with an SQL Chaser – Another Round, Please!



Carol Woodbury, CISSP, CRISC
IBM i Security SME and Senior
Advisor, Kisco Systems

IBMCHAMPION 
carol@kisco.com

© Copyright IBM Corporation 2025

Scott Forstie
Db2 for i Business Architect
forstie@us.ibm.com

April 2026

IBM i

1

Carol Loves SQL ...Why...?



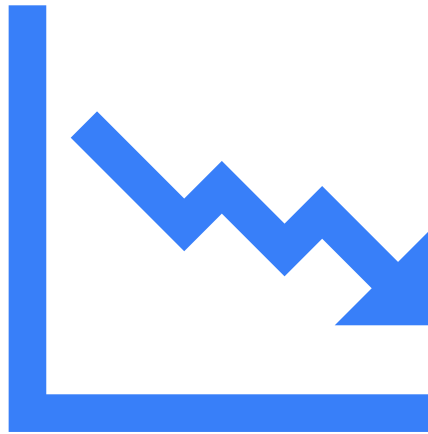
Image generated with Microsoft Copilot 1/26/2026

© Copyright IBM Corporation 2025

2

2

Why are We Talking about This?



To Reduce Risk!

3

© Copyright IBM Corporation 2025

3

In past presentations we've shown techniques for

- Discovering profiles with default passwords
- Managing inactive profiles
 - Discovering
 - Setting to *DISABLED
 - Deleting
- Reviewing profiles with special authorities either from the profile or group(s)
- Reviewing permissions on objects that don't meet your policy
- But what continues to be a mystery to many administrators...?

The IFS!

4

© Copyright IBM Corporation 2025

4

New Topic!

5

© Copyright IBM Corporation 2025

5

Let's Start at the Top – '/root' or '/'

Integrated File System

Actions

Navigate to: Path Name

Star Icon

Refresh Icon

Home Icon

Path Name

Type

Size

Owner

Last Modified

Filter

Filter

Filter

Filter

Filter

/

/QOpenS

/QDLS

/QSYS.LI

/QOPT

/QNTC

/dev

/home

/tmp

/etc

/usr

Permissions

Object: /

Type: *DIR

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			✓						

Total Rows: 3

Add

Change

Remove

☐ Propagate change to subtree

OK

Cancel

6

© Copyright IBM Corporation 2025

6

Addressing '/' (and '/QOpenSys')

- Ships with *PUBLIC authority set to the equivalent of *ALL
 - DTAAUT(*RWX) OBJAUT(*ALL)
- Recommended setting is the equivalent of *USE
 - DTAAUT(*RX) OBJAUT(*NONE)
- How do we get there without breaking anything?

7

© Copyright IBM Corporation 2025

7

Look in the Audit Journal!

```
--
-- Look for processes creating something into root in the last two weeks
-- before setting *PUBLIC to DTAAUT(*RX) OBJAUT(*NONE)
--
SELECT entry_timestamp,
       user_name,
       qualified_job_name,
       program_library,
       program_name,
       path_name
FROM TABLE (
    systools.audit_journal_co(STARTING_TIMESTAMP => CURRENT_TIMESTAMP - 14 DAYS)
)
WHERE path_name NOT LIKE '/%/';
stop;
```

▼ RESULTS					
ENTRY_TIMESTAMP	USER_NAME	QUALIFIED_JOB_NAME	PROGRAM_LIBRARY	PROGRAM_NAME	PATH_NAME
2026-04-07 16:18:44.214128	SCOTT	750484/QUSER_NC/QZDAS0INIT	QSYS	QZDAS0INIT	/library_names

8

© Copyright IBM Corporation 2025

8

Don't Forget '/QOpenSys'

```
--
-- Look for processes creating something into '/QOpenSys' in the last two weeks
-- before setting *PUBLIC to DTAAUT(*RX) OBJAUT(*NONE)
--
SELECT entry_timestamp,
       user_name,
       qualified_job_name,
       program_library,
       program_name,
       path_name
FROM TABLE (
    systools.audit_journal_co(STARTING_TIMESTAMP => CURRENT_TIMESTAMP - 14 DAYS)
)
WHERE path_name LIKE '/QOpenSys%'
      AND path_name NOT LIKE '/QOpenSys/%/%';
stop;
```

9

© Copyright IBM Corporation 2025

9

Next Task – Identify all Directories with Old Default *PUBLIC Authority

```
--
-- description: List the first-level directories under root that are set to *PUBLIC DTAAUT(*RWX) OBJAUT(*ALL)
--
WITH OBJS AS (
    SELECT PATH_NAME
    FROM TABLE (
        QSYS2.IFS_OBJECT_STATISTICS(START_PATH_NAME => '/',
                                   subtree_directories => 'NO',
                                   object_type_list => '*ALLDIR')
    )
)
SELECT *
FROM OBJS,
     TABLE (
        QSYS2.IFS_OBJECT_PRIVILEGES(PATH_NAME)
     )
WHERE data_authority = '*RWX'
      AND object_management = 'YES'      AND object_existence = 'YES'
      AND object_reference = 'YES'      AND object_alter = 'YES'
      and authorization_name = '*PUBLIC' and objs.path_name not in ('/');
```

See companion SQL script for the SQL

10

© Copyright IBM Corporation 2025

10

But Wait! Don't Jump Without Knowing the Consequences



11

© Copyright IBM Corporation 2025

11

Configure Authority Collection for a Directory

The screenshot displays the IBM Security Configuration interface. On the left, a navigation pane shows various system components, with 'Security' highlighted by a red arrow. The main pane shows the 'Security' section, with 'Authority Collection' expanded and 'Objects' selected, also indicated by a red arrow. A modal window titled 'Authority Collection for Objects' is open, showing the 'Change Authority Collection' options. The modal includes a 'Start' button, a 'Stop' button, and a 'View Collection' button. The 'Change Authority Collection' section contains a text input field for the 'Object' (containing '/payroll_upload'), and four dropdown menus for 'Authority information should be collected for this object:', 'Include dependent objects:', 'Delete previous collection:', and 'Directory subtree:'. The 'Authority Collection Actions' section is also visible, with a red arrow pointing to the 'Change Authority Collection' button.

12

© Copyright IBM Corporation 2025

12

Read the Results of the Authority Collection

```
-- After configuring Authority Collection, view the entries after a period of time
-- Use this new Authority Collection IFS view to get a better / more accurate
-- translation of IFS authority requirements
--
```



```
SELECT user_name, check_timestamp, path_name,
       detailed_required_authority, detailed_current_authority
FROM qsys2.authority_collection_ifs
WHERE UPPER(path_name) LIKE '/PAYROLL_UPLOAD%';
```

Authorization Name	Check Timestamp	Path Name	Detailed Required Authority	Detailed Current Authority
USER_NAME	CHECK_TIMESTAMP	PATH_NAME	DETAILED_REQUIRED_AUTHORITY	DETAILED_CURRENT_AUTHORITY
ADMIN06	2025-10-08 17:05:32.217798	/payroll_upload	*OBJMGT	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
LRPOWELL	2025-12-09 13:13:08.934442	/payroll_upload	*OBJMGT	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
JONGRKIM	2025-10-13 16:15:53.149330	/payroll_upload	*OBJMGT	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
ADMIN01	2025-10-08 16:40:44.236711	/payroll_upload	*OBJMGT	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
DEVELOPER	2024-03-28 18:09:10.622228	/payroll_upload	*R	*EXCLUDE
DAWNM	2024-01-17 10:18:55.562835	/payroll_upload	*OBJMGT	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
LDB	2023-08-12 09:14:33.333951	/payroll_upload	*X	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X

13

© Copyright IBM Corporation 2025

13

Manage the Permissions of the Secured Directory and its Objects

```
--
-- description: Find any objects under an IFS path that have the wrong value for owner or *PUBLIC
--
```

```
WITH ifs_auts AS (
  SELECT path_name
  FROM TABLE (
    qsys2.ifs_object_statistics(start_path_name => '/payroll_upload',
                               subtree_directories => 'YES', IGNORE_ERRORS => 'YES'))

  SELECT iop.*
  FROM ifs_auts,
  TABLE (qsys2.ifs_object_privileges(path_name)) iop
  WHERE owner <> 'PROD_OWNER'
  OR (authorization_name = '*PUBLIC'
  AND (data_authority <> '*EXCLUDE'
  OR object_management <> 'NO'
  OR object_existence <> 'NO'
  OR object_reference <> 'NO'
  OR object_alter <> 'NO'));
```

PATH_NAME	OBJECT_TYPE	OWNER	PRIMARY_GROUP	AUTHORIZATION_LIST	AUTHORIZATION_NAME	DATA_AUTHORITY	OBJECT_OPERATIONAL	OBJECT_MANAGEMENT
/payroll_upload	*DIR	CWOODBURY	-	-	*PUBLIC	*EXCLUDE	NO	NO
/payroll_upload	*DIR	CWOODBURY	-	-	CWOODBURY	*RWX	YES	YES
/payroll_upload	*DIR	CWOODBURY	-	-	QDIRSRV	*X	YES	NO

© Copyright IBM Corporation 2025

14

Find Old Stuff in Directories (and get rid of it!)

```
--
-- Find old objects in /home
--
SELECT path_name, object_type, object_owner,
       last_used_timestamp, create_timestamp, data_size
FROM TABLE (
    QSYS2.IFS_OBJECT_STATISTICS(START_PATH_NAME => '/home',
                                SUBTREE_DIRECTORIES => 'YES')
) AS oldifsstuff
WHERE last_used_timestamp < CURRENT DATE - 6 MONTHS ORDER BY data_size desc;
```

PATH_NAME	OBJECT_TYPE	OBJECT_OWNER	LAST_USED_TIMESTAMP	CREATE_TIMESTAMP	DATA_SIZE
/home/LRPOWELL/.cache/javasharedresources/C290M17F1A64P_...	*STMF	LRPOWELL	2025-05-12 00:00:00	2025-05-12 20:40:42	314,572,800
/home/DRIVEWAY/openjdk-11-11.0.6.10-99.ibm7.2.ppc64.rpm	*STMF	DRIVEWAY	2022-05-12 00:00:00	2020-05-01 16:28:00	235,512,609
/home/reverhart/XASetup13_0_07.msi	*STMF	CAROL	2022-05-12 00:00:00	2018-05-11 20:59:18	217,909,760
/home/DRIVEWAY/openjdk/openjdk-jdk11-11.0.1.13-99.ibm7.2.ppc...	*STMF	DRIVEWAY	2022-05-12 00:00:00	2020-06-15 10:39:57	207,412,712
/home/TIMOTHYC/rdi/.git/objects/pack/pack-6b9203ac5ce3f509e39...	*STMF	TIMOTHYC	2022-05-12 00:00:00	2021-01-27 13:02:16	195,270,112
/home/DRIVEWAY/openjdk/openjdk-11-ea-11.0.6.10-101.src.rpm	*STMF	DRIVEWAY	2022-05-12 00:00:00	2020-06-15 10:37:44	125,266,815
/home/DRIVEWAY/jwoehr/Qiskit/gcc/gcc-9.2.0.tar.gz	*STMF	DRIVEWAY	2022-05-12 00:00:00	2019-12-09 12:33:02	124,304,709

15

© Copyright IBM Corporation 2025

15

Find Old Stuff in Libraries

```
--
-- description: List objects in PROD_LIB not used in six months
--
SELECT objname, objtype, objattribute, objowner, objdefiner AS Creator, objlongname, objlongschema
, sql_object_type,
   objcreated, objtext, last_used_timestamp, days_used_count
FROM TABLE (
    qsys2.object_statistics('PROD_LIB', '*ALL')
) AS oldstuff
where last_used_timestamp < CURRENT DATE - 6 months and last_used_object = 'YES';
```

OBJNAME	OBJTYPE	OBJATTRIBUTE	OBJOWNER	CREATOR	OBJLONGNAME	OBJLONGSCHEMA	SQL_OBJECT_TYPE	OBJCREATED
AR	*PGM	CLP	CWOODBURY	CWOODBURY	AR	PROD_LIB	-	2020-08-10 12:23:01.000000
INLMENU	*PGM	CLP	QSECOFR	CWOODBURY	INLMENU	PROD_LIB	-	2020-08-10 12:23:01.000000
APOUTQ	*OUTQ		CWOODBURY	CWOODBURY	APOUTQ	PROD_LIB	-	2020-08-10 12:23:01.000000
PAYABLES	*FILE	PF	CWOODBURY	CWOODBURY	PAYABLES	PROD_LIB	TABLE	2020-08-10 12:23:01.000000
BALANCE	*QRYDFN	QRY	CWOODBURY	CWOODBURY	BALANCE	PROD_LIB	-	2020-08-10 12:23:01.000000

16

© Copyright IBM Corporation 2025

16

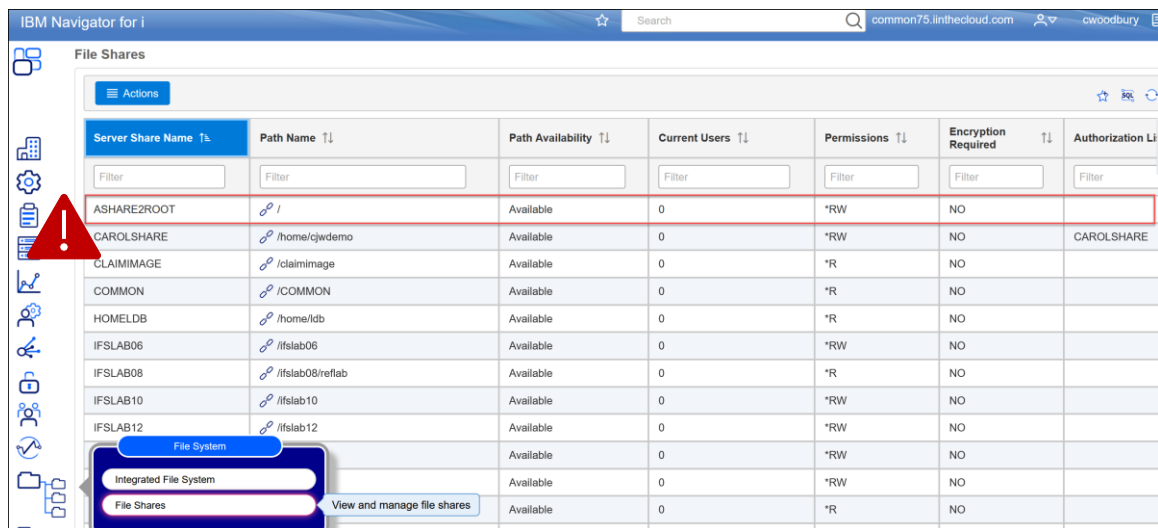
New Topic!

17

© Copyright IBM Corporation 2025

17

File Shares – the Entry Point of Malware – including Ransomware!



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



18

© Copyright IBM Corporation 2025

18

How Do I Remove a File Share if I Don't Know if it's in Use?



Image generated by Microsoft Copilot 2/23/2026

19

© Copyright IBM Corporation 2025

19

*NETSMBSVR Action Audit Value (QAUDLVL)

```
--
-- Add *NETSMBSVR to QAUDLVL and
-- look at the VP audit journal entries to see which shares are in use!
-- (New in IBM i 7.6)
--
```

```
SELECT entry_timestamp,
       audit_user_name,
       share_name,
       entry_type_detail,
       share_authorization_list
FROM TABLE(systools.audit_journal_vp());
```



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	-

VP (Network) journal entries

20

© Copyright IBM Corporation 2025

20

QSYS2.manage_audit_journal_data_mart

Delivered on June 14, 2024:
IBM i 7.4
and Higher

Create the data mart ... results in the creation of a file
audit_journal_VP in library VPDATAMART

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART (
  JOURNAL_ENTRY_TYPE => 'VP',
  DATA_MART_LIBRARY => 'VPDATAMART',
  STARTING_TIMESTAMP => '*FIRST',
  ENDING_TIMESTAMP   => DEFAULT,
  DATA_MART_ACTION  => 'CREATE'
  DATA_MART_FILTER   => ' share_type = ''FILE'' ');
```

21

© Copyright IBM Corporation 2025

21

QSYS2.manage_audit_journal_data_mart

Delivered on June 14, 2024:
IBM i 7.4
and Higher

At some later date, but before the audit journal receivers are
removed... Add any entries generated since the last run

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART (
  JOURNAL_ENTRY_TYPE => 'VP',
  DATA_MART_LIBRARY => 'VPDATAMART',
  STARTING_TIMESTAMP => '*CONTINUE',
  ENDING_TIMESTAMP   => NULL,
  DATA_MART_ACTION  => 'ADD'
);
```

22

© Copyright IBM Corporation 2025

22

Viewing the Entries from the Data Mart

```
--
-- See the Data Mart data
--
select * from vpdamart.audit_journal_VP;
-- OR
select * from vpdamart.aj_vp;
```

23

© Copyright IBM Corporation 2025

23

Audit Journal Data Marts in Navigator for i

The screenshot shows the IBM Navigator for i Security Configuration page. The left sidebar contains a navigation menu with icons for System, Monitors, My Work, Network, and Security. The Security icon is highlighted with a red arrow. The main content area is titled 'Security' and contains a 'Security Configuration Info' section. Under this section, there is a 'MFA Configuration' link and an expanded 'Audit Journal' section. The 'Audit Journal' section has three sub-items: 'Manage Data Mart' (highlighted with a red arrow), 'Audit Journal Entries', and 'Auditing Configuration'. The 'Manage Data Mart' link is also highlighted with a red arrow. The 'Manage Audit Journal Data Mart' window is open, displaying a table of data marts. The table has four columns: 'Data Mart Library', 'Data Mart', 'Data Mart System Table Name', and 'Data Mart Filter'. The table contains several rows, with the last row, 'SFDATAMART', 'AUDIT_JOURNAL_VP', 'AJ_VP', and 'share_type = FILE', highlighted in blue. A context menu is open over the highlighted row, showing options: 'Manage', 'Delete', 'Detail View', 'Daily View', 'Weekly View', 'Schedule', and 'Permissions'.

Data Mart Library	Data Mart	Data Mart System Table Name	Data Mart Filter
AECIESLA	AUDIT_JOURNAL_AF	AJ_AF	
RPGPMM1	AUDIT_JOURNAL_CA	AJ_CA	
SFDATAMART	AUDIT_JOURNAL_GR	AJ_GR	function_name like 'QIBM_RUN_UNDER
RPGPMM1	AUDIT_JOURNAL_LD	AJ_LD	
AECIESLA	AUDIT_JOURNAL_PW	AJ_PW	AUDIT_USER_NAME NOT LIKE '%ADM
DMARTLIB	AUDIT_JOURNAL_PW	AJ_PW	
SFDATAMART	AUDIT_JOURNAL_VP	AJ_VP	share_type = 'FILE'

24

© Copyright IBM Corporation 2025

24

Scheduling Options

Schedule

Data Mart Library:
SFDATAMART

Journal Entry Type:
Network Password Error (VP)

Action:
Append new data to the existing data mart

Append new data to the existing data mart
Delete the existing data mart and create a new one
Delete entries from the data mart table

02/20/2026 03:00 PM

Add Scheduled Job

Job name: Job Description

Command to run:
QSYS/RUNSQL SQL('CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART(JOURNAL_ENTRY_TYPE => "VP", DATA_MART_LIBRARY => "SFDATAMART", STARTING_TIMESTAMP => ""CONTINUE"')

Frequency: Once

Schedule date: Current date 02/23/2026

Schedule day:
☒ None
☐ All
☐ Specific days
Monday Tuesday Wednesday Thursday
Friday Saturday Sunday

Schedule time: Current time 05:12 PM

Save: No

Additional Parameters

OK Cancel

© Copyright IBM Corporation 2025

25

Prior to 7.6, Use Authority Collection to Discover File Share Use

--

-- Configure Authority Collection on the object being shared

-- View the results to determine who's using the share

--

```
SELECT user_name, check_timestamp, path_name,
       detailed_required_authority, detailed_current_authority
FROM   qsys2.authority_collection_fsobj
WHERE  job_name LIKE 'QZLSFILE%' AND
       UPPER(path_name) LIKE '/HOME/TESTNAV/%';
```

Authorization Name	Check Timestamp	Path Name	Detailed Required Authority	Detailed Current Authority
USER_NAME	CHECK_TIMESTAMP	PATH_NAME	DETAILED_REQUIRED_AUTHORITY	DETAILED_CURRENT_AUTHORITY
TIMMR	2025-05-07 08:59:31.375538	/home/testnav/dir090	*OBJOPR *EXECUTE	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJ
TIMMR	2025-05-07 08:59:31.375548	/home/testnav/dir090	*OBJOPR *READ	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJ
TIMMR	2025-05-07 08:59:29.036798	/home/testnav/dir010	*OBJOPR *EXECUTE	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJ
TIMMR	2025-05-07 08:59:29.036809	/home/testnav/dir010	*OBJOPR *READ	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJ

© Copyright IBM Corporation 2025

26

26

Use the New IFS Authority Collection View

```
--
-- Configure Authority Collection on the object being shared
-- View the results to determine who's using the share
--
```

```
SELECT user_name, check_timestamp, path_name,
       detailed_required_authority, detailed_current_authority
FROM qsys2.authority_collection_ifs
WHERE job_name LIKE 'QZLSFILE%' AND
       UPPER(path_name) LIKE '/HOME/TESTNAV/%';
```

Delivered via:
IBM i 7.6 SF99960 Level 1
and
IBM i 7.5 SF99950 Level 9

USER_NAME	CHECK_TIMESTAMP	PATH_NAME	DETAILED_REQUIRED_AUTHORITY	DETAILED_CURRENT_AUTHORITY
TIMMR	2025-05-07 08:59:31.375538	/home/testnav/dir090	*X	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
TIMMR	2025-05-07 08:59:31.375548	/home/testnav/dir090	*R	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
TIMMR	2025-05-07 08:59:29.036798	/home/testnav/dir010	*X	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X
TIMMR	2025-05-07 08:59:29.036809	/home/testnav/dir010	*R	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *R *W *X

27

© Copyright IBM Corporation 2025

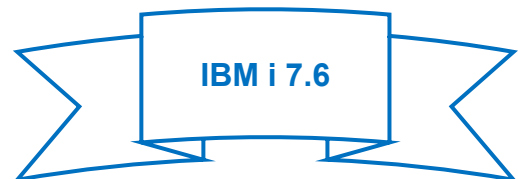
27

IBM i 7.6 Memo to Users (MTU) - *IOSYSCFG Comes ALIVE!!!

- Command and API Authority Changes (47)
- Some system values and network attributes require *IOSYSCFG or QIBM_IOSYSCFG_VIEW function usage to view or retrieve data (8)
- Network Command and API Authority Changes (27)
- CHGTELNA Command Authority Changes
- QTVRTVTELA API Authority Changes
- Authority requirements change for NetServer shares
- Authority change for tape commands and APIs (17)
- SQL services changed to require *IOSYSCFG or QIBM_IOSYSCFG_VIEW (14)
- Authority changes for Db2 Mirror SQL services (16)
- SQL CREATE ALIAS statement authority change

- IBM i 7.6 Memo to Users :

https://www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf



29

© Copyright IBM Corporation 2025

29

Determine which Profiles have *IOSYSCFG

```
--
--  description: Special Authority analysis
--
SELECT user_name, status, no_password_indicator, DATE(previous_signon) AS last_signon,
       DATE(last_used_timestamp) AS last_used, text_description
FROM qsys2.user_info
WHERE special_authorities LIKE '%*IOSYSCFG%' OR authorization_name IN (SELECT user_profile_name
                              FROM qsys2.group_profile_entries
                              WHERE group_profile_name IN (SELECT authorization_name
                                                            FROM qsys2.user_info
                                                            WHERE special_authorities LIKE '%*IOSYSCFG%')) ORDER BY user_name;
```

Authorization Name	Status	No Password Indicator			Text Description
USER_NAME	STATUS	NO_PASSWORD_INDICATOR	LAST_SIGNON	LAST_USED	TEXT_DESCRIPTION
CWOODBURY	*ENABLED	NO	2025-05-06	2025-05-06	Carol Woodbury
DAVID	*ENABLED	NO	2025-02-25	2025-02-25	David Crow AJS
DAVIDAJS	*DISABLED	NO	2023-01-24	2023-01-24	AJS test user for David
DAWN	*ENABLED	NO	2024-06-10	2024-06-10	second dawn may profile for demo pu...
DAWNM	*ENABLED	NO	2025-05-06	2025-05-06	Dawn May - Presenter and IBM i Perf...
DAWNSRV	*ENABLED	NO	2024-10-09	2024-10-09	-
DAWNTEST	*DISABLED	NO	2021-03-20	2021-03-20	test prestart job attribute changes

30

© Copyright IBM Corporation 2025

30

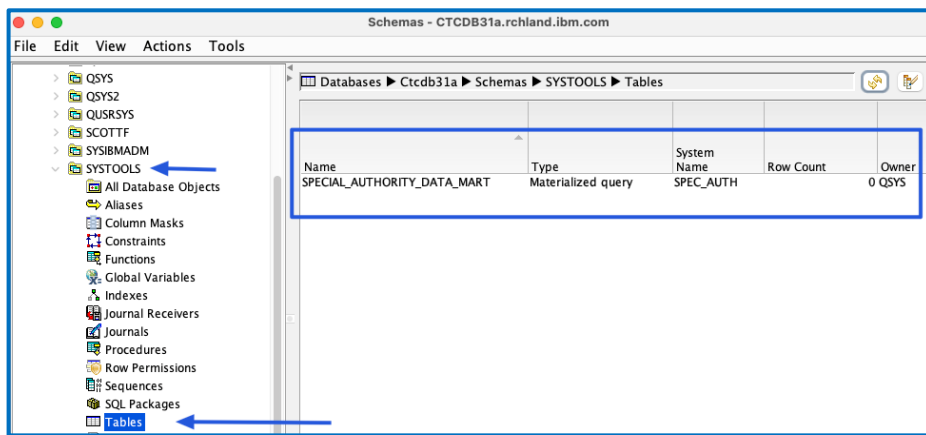
SPECIAL_AUTHORITY_DATA_MART

Contains information about special authorities for users

Implemented as a Materialized Query Table (MQT)

– Use REFRESH TABLE to populate the data

Added to
IBM i 7.4 and 7.5
in [June 2024](#)



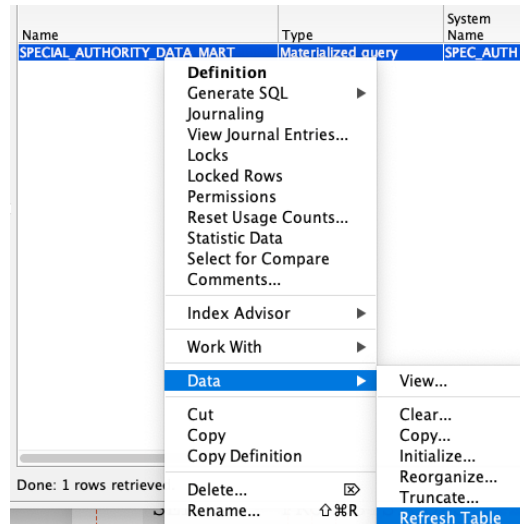
31

© Copyright IBM Corporation 2025

31

SPECIAL_AUTHORITY_DATA_MART

ACS – Schemas includes an action that is the same as executing REFRESH TABLE



32

© Copyright IBM Corporation 2025

32

Review Profiles with a Special Authority and the Source

```
--
-- Who has *IOSYSCFG special authority, and from what authority source?
-- (Using the data mart)
--
```

```
SELECT user_name, authority_source, group_profile_name,
       status, text_description, last_used_date
FROM systools.special_authority_data_mart
WHERE special_authority = '*IOSYSCFG'
ORDER BY user_name;
```

Authorization Name	Authority Source	Group Profile Name	Status	Text Description	Last Used Date
USER_NAME	AUTHORITY_SOURCE	GROUP_PROFILE_NAME	STATUS	TEXT_DESCRIPTION	LAST_USED_DATE
BRIANAJS	USER PROFILE	—	*ENABLED	AJS Test User cor Brian	2025-02-13
BRIANAJS	GROUP PROFILE	SUPERUSER	*ENABLED	AJS Test User cor Brian	2025-02-13
BSHAM	USER PROFILE	—	*ENABLED	Brock Shamblin	2025-03-18
CAROLSPC	GROUP PROFILE	CWOODBURY	*ENABLED	—	—
CAROLSPC	GROUP PROFILE	QSECOFR	*ENABLED	—	—

33

© Copyright IBM Corporation 2025

33

Revisiting MTU and QIBM_IOSYSCFG_VIEW function

- Command and API Authority Changes (47)
 - Some system values and network attributes require *IOSYSCFG or **QIBM_IOSYSCFG_VIEW function** usage to view or retrieve data (8)
 - Network Command and API Authority Changes (27)
 - CHGTELNA Command Authority Changes
 - QTVRTVTELA API Authority Changes
 - Authority requirements change for NetServer shares
 - Authority change for tape commands and APIs (17)
 - SQL services changed to require *IOSYSCFG or **QIBM_IOSYSCFG_VIEW (14)**
 - Authority changes for Db2 Mirror SQL services (16)
 - SQL CREATE ALIAS statement authority change
- IBM i 7.6 Memo to Users :
https://www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf

34

© Copyright IBM Corporation 2025

34

QIBM_IOSYSCFG_VIEW function

IBM i 7.6

The screenshot displays the IBM Navigator for i interface. On the left is a navigation pane with categories like Dashboard, Home, Work Management, Configuration and Service, System, Monitors, My Work, Network, and Security (highlighted with a red arrow). The main area shows 'Function Usage' with a list of functions including 'QIBM_IOSYSCFG_VIEW'. A modal window titled 'Change Function Usage' is open, showing details for 'QIBM_IOSYSCFG_VIEW'. It includes a table with columns: Function ID, Description, Default Usage, and All Object Indicator. Below the table are sections for 'Usage options for the selected function IDs' and 'Usage options for specified user and group profiles for the the selected function', each with dropdowns for Default authority and *ALLOBJ special authority, and buttons for Add, Remove, and Browse Profiles.

Function ID	Description	Default Usage	All Object Indicator
QIBM_IOSYSCFG_VIEW	Allows the ability to view Input/Output system configuration information.	DENIED	NOT USED

Total Rows: 1

Usage options for the selected function IDs

Default authority:

*ALLOBJ special authority:

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

Profile(s):

Access Allowed:

Access Denied:

Provides the ability to view network config information without granting full
 *IOSYSCFG access

© Copyright IBM Corporation 2025

35

QIBM_RUN_UNDER_USER_NO_AUTH function



IBM i 7.6

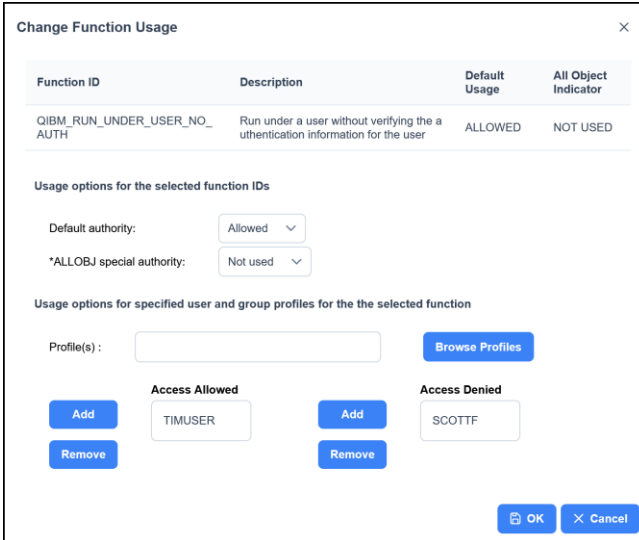
➔ **Protect profiles that can be exploited**

Examples:

- Submit a job to run as a different user
- Swap to a profile

How can this happen?

- Profile with *ALLOBJ but no other authorities
- Profile set to *PUBLIC *USE
- Group members with added *EXECUTE



Change Function Usage

Function ID	Description	Default Usage	All Object Indicator
QIBM_RUN_UNDER_USER_NO_AUTH	Run under a user without verifying the authentication information for the user	ALLOWED	NOT USED

Usage options for the selected function IDs

Default authority:

*ALLOBJ special authority:

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

Profile(s):

Access Allowed

Access Denied

36

© Copyright IBM Corporation 2025

36

Which Profiles Can Be Impersonated / Exploited?

```
--
-- Which users can be impersonated by anyone?
--
```

```
SELECT object_name AS user_name,
       object_authority
FROM   qsys2.object_privileges
WHERE  system_object_schema = 'QSYS'
       AND object_type = '*USRPRF'
       AND user_name = '*PUBLIC'
       AND object_authority <> '*EXCLUDE'
       AND object_name NOT IN ('QDBSHR', 'QDBSHRDO', 'QTMLPD');
```

	Object Authority
USER_NAME	OBJECT_AUTHORITY
CJWOH0H	*USE

37

© Copyright IBM Corporation 2025

37

How Do you Know if a Profile is Already Being Exploited?

New User Action Audit Value

- *AUTWARN (CHGUSRAUD)
 - Turn on the profile you wish to protect to determine if it's being used without authentication – for example, to submit a job or perform a profile swap
 - Note: No *AUTHENTICATION* as in without entering a user id and password
 - Implemented with the idea of protecting profiles that can't be enabled for MFA ... but can be used without MFA being in place
 - E.g., You have profiles with *ALLOBJ that you don't want to elevate to a profile with all special authorities
 - Audit value can only be specified at the user level – not in QAUDLVL



38

© Copyright IBM Corporation 2025

38

GR – Generic Record Audit Journal Entries

- Generated to show access / failure attempts of functions in Function Usage
- Will be generated once you modify any value from the default in Function usage (assuming either *SECURITY or *SECCFG is specified for QAUDLVL)

39

© Copyright IBM Corporation 2025

39

GR - *AUTWARN Audit Journal Entries

```
--
-- After adding *AUTWARN to the user auditing level,
-- determine whether and when the profile is currently being exploited
--
SELECT entry_timestamp, qualified_job_name,
       user_name, user_profile_name AS profile_exploited,
       function_registration_operation AS failure_or_warning,
       fail_operation
FROM TABLE(systools.audit_journal_gr())
WHERE function_name LIKE 'QIBM_RUN_UNDER%';
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	PROFILE_EXPLOITED	FAILURE_OR_WARNING	FAIL_OPERATION
2025-05-03 23:55:00.007440	789731/QSYS/QJOBSCD	QSYS	SCOTT	USAGE FAILURE	-
2025-05-03 23:55:00.008560	789731/QSYS/QJOBSCD	QSYS	SCOTT	USAGE FAILURE	-
2025-05-03 23:55:00.009600	789731/QSYS/QJOBSCD	QSYS	SCOTT	USAGE FAILURE	-
2025-05-04 00:00:01.000400	789731/QSYS/QJOBSCD	QSYS	SCOTT	USAGE FAILURE	-
2025-05-04 13:44:21.115296	832089/CWOODBURY/QPADEV01TZ	CWOODBURY	SERVICE1	USAGE WARNING	SBMJOB
2025-05-04 13:46:06.495632	789731/QSYS/QJOBSCD	QSYS	SERVICE1	USAGE WARNING	SBMJOB
2025-05-04 13:48:56.622880	832089/CWOODBURY/QPADEV01TZ	CWOODBURY	SERVICE1	USAGE WARNING	GETPH
2025-05-04 13:49:15.658432	832089/CWOODBURY/QPADEV01TZ	CWOODBURY	SERVICE1	USAGE WARNING	SBMJOB

40

© Copyright IBM Corporation 2025

40

Function Usage SQL

```
--
-- What's the default access for the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
SELECT default_usage, allobj_indicator, function_name_message_text
FROM qsys2.function_info WHERE function_id = 'QIBM_IOSYSCFG_VIEW';
```

Default Usage	Allobj Indicator	Function Name Message Text
DEFAULT_USAGE	ALLOBJ_INDICATOR	FUNCTION_NAME_MESSAGE_TEXT
DENIED	NOT USED	View Input/Output System Configuration

```
--
-- Who is allowed to use the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
select * from qsys2.function_usage where function_id = 'QIBM_IOSYSCFG_VIEW';
```

Function ID	User Name	Usage	User Type
FUNCTION_ID	USER_NAME	USAGE	USER_TYPE
QIBM_IOSYSCFG_VIEW	TIMUSER	ALLOWED	USER
QIBM_IOSYSCFG_VIEW	MGMT	ALLOWED	GROUP

41

© Copyright IBM Corporation 2025

41

For More Information

IBM i Services

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

IBM Tutorials

- <https://www.ibm.com/support/pages/ibm-i-tutorials-demos-and-sql-examples-0>

IBM i Security Reference – PDF

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_76/rzarl/sc415302.pdf?view=kc

- Chapters 2 and 3 – System Values
- Chapter 4 – User Profiles
- Chapter 9 – Auditing
- Chapter 10 – Authority Collection
- Appendix H – IBM-Supplied Function Usage definitions

IBM i MFA - https://www.ibm.com/docs/en/ssw_ibm_i_76/pdf/mfapdf.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 Carol Woodbury on mcpresonline.com and [KiscoU](#)

48

© Copyright IBM Corporation 2025

48

For More Information ...

What is IBM doing to help your team be successful with SQL?

1. ACS – Insert From Examples
SQL examples for all IBM i Services and more
2. SQL Tutor
SQL solutions for questions clients asked Scott
3. SQL Tutor
iSee Video blog series from Scott & Tim



<https://ibm.biz/Db2foriSQLTutor>

For example:

[Searching the IFS for objects with "log4j" in the name.sql](#)

The request from a client was to provide an SQL approach to search all of the IFS, finding any object that has "log4j" in its name, and producing an SQL table with the search results.

49

© Copyright IBM Corporation 2025

49

Bonus Topics!

50

© Copyright IBM Corporation 2025

50

Default Passwords and More

```
--
-- description: User profiles with default passwords
--
select USER_NAME, STATUS, PASSWORD_EXPIRATION_INTERVAL, SPECIAL_AUTHORITIES,
       GROUP_PROFILE_NAME, SUPPLEMENTAL_GROUP_LIST, LAST_USED_TIMESTAMP,
       CREATION_TIMESTAMP, USER_CREATOR, TEXT_DESCRIPTION
from qsys2.user_info
where USER_DEFAULT_PASSWORD = 'YES' order by status;
```

USER_NAME	STATUS	PASSWORD_EXPIRATION_INTERVAL		GROUP_PROFILE_NAME	SUPPLEMENTAL_GROUP_LIST	LAST_USED_TIMESTAMP
Authorization Name	Status	Password Expiration Interval	SPECIAL_AUTHORITIES	Group Profile Name	Supplemental Group List	Last Used Timestamp
IOAT	*DISABLED	0	<NULL>	*NONE	<NULL>	<NULL>
IREDD	*DISABLED	0	<NULL>	MYGROUP	<NULL>	<NULL>
IYSQL	*DISABLED	0	<NULL>	*NONE	<NULL>	2022-05-12 00:00:00.0
UIUSR03	*DISABLED	0	<NULL>	*NONE	<NULL>	<NULL>
YLAB	*DISABLED	0	<NULL>	*NONE	<NULL>	2022-04-23 00:00:00.0
SUPERUSER	*DISABLED	0	*ALLOBJ *SECADM *JOBCL...	*NONE	<NULL>	2022-05-15 00:00:00.0
LAB01	*DISABLED	-1	<NULL>	QPMR	<NULL>	2021-02-11 00:00:00.0

Profiles with non-expiring passwords (PWDEXPITV-*NOMAX), limited capability *NO, etc

51

© Copyright IBM Corporation 2025

51

Discover Inactive Profiles

```
--
-- description: User profiles that haven't been used in the last 3 months
--
SELECT user_name,
       date(last_used_timestamp) as last_used,
       timestamp(previous_signon, 0) as last_signon,
       timestamp(creation_timestamp, 0) as create_time, status, text_description
FROM QSYS2.USER_INFO
WHERE (last_used_timestamp IS NULL
       OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
       AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS);
```

USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	STATUS	TEXT_DESCRIPTION
FRANKDBA26	<NULL>	<NULL>	2019-11-06 04:40:09	*ENABLED	<NULL>
FRANKDBA27	<NULL>	<NULL>	2019-11-06 04:40:47	*ENABLED	<NULL>
FRANKDBA28	<NULL>	<NULL>	2019-11-06 04:40:35	*ENABLED	<NULL>
FRANKDBA99	11/06/2019	<NULL>	2019-11-05 15:28:54	*ENABLED	<NULL>

Done: 1,638 rows retrieved.

52

© Copyright IBM Corporation 2025

52

Managing Inactive Profiles with an SQL

```
--
-- description: DISABLE User profiles that haven't been used in the last 3 months
--
SELECT cup.*
FROM QSYS2.USER_INFO u,
     TABLE (SYSTOOLS.CHANGE_USER_PROFILE(
       P_USER_NAME => USER_NAME,
       P_STATUS    => '*DISABLED',
       P_TEXT      => 'Careful - do not re-enable',
       PREVIEW     => 'YES')) cup
WHERE (u.user_name not in (select aidprf from QUSRSYS.QASECIDL)) and ((last_used_timestamp IS NULL
OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS));
```

USER_NAME	CHANGE_ATTEMPTED	CHGUSRPRF_COMMAND	CHANGE_SUCCESSFUL
AMRA	NO	QSYS/CHGUSRPRF USRPRF(AMRA) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
BOBADMIN99	NO	QSYS/CHGUSRPRF USRPRF(BOBADMIN99) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
BRAD	NO	QSYS/CHGUSRPRF USRPRF(BRAD) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CAROL	NO	QSYS/CHGUSRPRF USRPRF(CAROL) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CAROLAUDIT	NO	QSYS/CHGUSRPRF USRPRF(CAROLAUDIT) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CONNOR4	NO	QSYS/CHGUSRPRF USRPRF(CONNOR4) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CUST_G99	NO	QSYS/CHGUSRPRF USRPRF(CUST_G99) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CWOODBURYT	NO	QSYS/CHGUSRPRF USRPRF(CWOODBURYT) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CWOODBURY2	NO	QSYS/CHGUSRPRF USRPRF(CWOODBURY2) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-

<https://www.ibm.com/docs/en/i/7.5?topic=services-change-user-profile-table-function>

53

© Copyright IBM Corporation 2025

53

Automating the Use of systools.change_user_profile

```
create or replace procedure coolstuff.user_dis()
SET OPTION USRPRF=*user, DYNUSRPRF=*user, commit=*none
begin
  create or replace table qtemp.just_do_it as
  (select cup.*
   from QSYS2.USER_INFO u, table (
     SYSTOOLS.CHANGE_USER_PROFILE(
       P_USER_NAME => USER_NAME, P_STATUS => '*DISABLED',
       P_TEXT => 'Careful - do not re-enable', PREVIEW => 'NO')
    ) cup
   where (u.user_name not in (select aidprf
                             from QUSRSYS.QASECIDL)) and
         ((last_used_timestamp is NULL or
          last_used_timestamp < current_timestamp - 3 months) and
          (creation_timestamp < current_timestamp - 3 months)))
  with data
  on replace delete rows;
end;

cl: ADDJOBSCDE JOB(USER_DIS) CMD(QSYS/RUNSQL SQL('call coolstuff.user_dis()'))
  COMMIT(*NONE) NAMING(*SQL) FRQ(*WEEKLY) SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME(235500);
```

54

© Copyright IBM Corporation 2025

54

Deleting User Profiles using SQL

```
--
-- description: Delete User profiles that are at least 6 months old and have not been
--              used in the last six months
--              Reassign ownership of any object to the user's primary group
--              If the user has no primary group, reassign object ownership to CAROL
--              If the user profile is in the "do not delete list", skip it
--
SELECT qsys2.qcmdexc('DLTUSRPRF USRPRF(' concat user_name concat ' ) '
                    concat 'OWNOBJOPT(*CHGOWN ' concat
                    case GROUP_PROFILE_NAME when '*NONE' then 'CAROL'
                    else GROUP_PROFILE_NAME end concat ' )' )
FROM QSYS2.USER_INFO u
WHERE (coalesce(last_used_timestamp, previous_signon, current_timestamp - 7 months)
      < CURRENT_TIMESTAMP - 6 MONTHS)
      AND (creation_timestamp < CURRENT_TIMESTAMP - 6 MONTHS)
      AND (user_creator not in ('*IBM', 'QLPINSTALL', 'QSYS', 'QSECOFR'))
      AND u.user_name not in (select aidprf from QUSRSYS.QASECIDL);
```

55

© Copyright IBM Corporation 2025

55

In Addition to Special Authorities, Review Group Profile Members

```
--
-- description: List the members of each group profile
--
SELECT *
FROM qsys2.group_profile_entries order by group_profile_name;
```

Group Profile Name	User Profile Name	User Text
GROUP_PROFILE_NAME	USER_PROFILE_NAME	USER_TEXT
QPGMR	WLAB19	User 19 for lab
QPGMR	WLAB20	User 20 for lab
QSECOFR	AOFROMGRP	Example of spcaut from user and ...
QSECOFR	CAROLSPC	-
QUSER	AOFROMGRP	Example of spcaut from user and ...
QWQADMGRP	AECIESLA	Ann Ciesla
QWQADMGRP	AECIESLA1	-
QWQADMGRP	CHOWLIN	Cecilia Howlin - Lab Presenter
QWQADMGRP	JOHNW	-
RCAC_G99	MARYSEC99	-

56

