



Managing IBM i Security Using IBM i Services

Carol Woodbury, CISSP, CRISC, PCIP

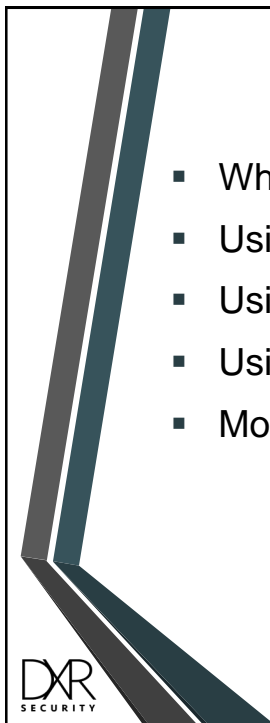
IBMCHAMPION 

carol@dxrsecurity.com

© DXRSecurity, All Rights Reserved.




1



Agenda

- What are these Services and Why use them?
- Using Services in ACS
- Using Services in a CL program
- Using Services in ARE
- More information



2

IBM i Services



3

What and Why

- SQL views which provide access to IBM i data using SQL rather than running a command or writing to an API otherwise writing a 'traditional' program
- Typically faster access
- Easy access to data via languages such as python
- Provides information in a 'better' format



4

Don't Run Away!

- Just because these are SQL-based – don't be frightened and think you can't use them if you aren't familiar with SQL!



5

IBM i Service Webpage

Security Services				
OSYS2.AUTHORITY_COLLECTION	View	Base	Base	Not Supported
OSYS2.AUTHORITY_COLLECTION_DLO	View	Base	Not Supported	Not Supported
OSYS2.AUTHORITY_COLLECTION_ESOBJ	View	Base	Not Supported	Not Supported
OSYS2.AUTHORITY_COLLECTION_LIBRARIES	View	Base	Not Supported	Not Supported
OSYS2.AUTHORITY_COLLECTION_OBJECT	View	Base	Not Supported	Not Supported
OSYS2.AUTHORIZATION_LIST_INFO	View	Base	SF99703 Level 4	SF99702 Level 16
OSYS2.AUTHORIZATION_LIST_USER_INFO	View	Base	SF99703 Level 4	SF99702 Level 16
OSYS2.CERTIFICATE_INFO	Table function	SF99704 Level 7	SF99703 Level 18	Not Supported
OSYS2.DRDA_AUTHENTICATION_ENTRY_INFO	View	Base	Base	SF99702 Level 5
OSYS2.FUNCTION_INFO	View	Base	Base	Base
OSYS2.FUNCTION_USAGE	View	Base	Base	Base
OSYS2.GROUP_PROFILE_ENTRIES	View	Base	Base	Base

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



6

Detailed Description of the Service

The screenshot shows a web-based documentation page for the 'OBJECT_PRIVILEGES table function'. On the left is a 'Table of Contents' sidebar with 'OBJECT_PRIVILEGES table function' selected. The main content area includes:

- Last updated:** 2020-10-06
- Description:** The OBJECT_PRIVILEGES table function returns a row for every user authorized to the specified object, along with their associated object and data authorities.
- Information returned:** The information returned is similar to the information available through the Display Object Authority (DSPOBJAUT) CL command.
- Authorization:** All authorized users are returned for an object when at least one of the following is true:
 - The caller has *OBJMGT authority.
 - The caller is the owner of the object.
 - The object is an authorization list.
 - The caller is authorized to the Database Security Administrator function of IBM i. The Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_DB_SECADM, can be used to change the list of users allowed to use the function.
- Otherwise:** Only authorizations for the caller are returned.

Example

Return authority information for the file APPLIB/EMPLOYEE.

```
SELECT *
FROM TABLE(QSYS2.OBJECT_PRIVILEGES('APPLIB', 'EMPLOYEE', '*FILE'));
```

7

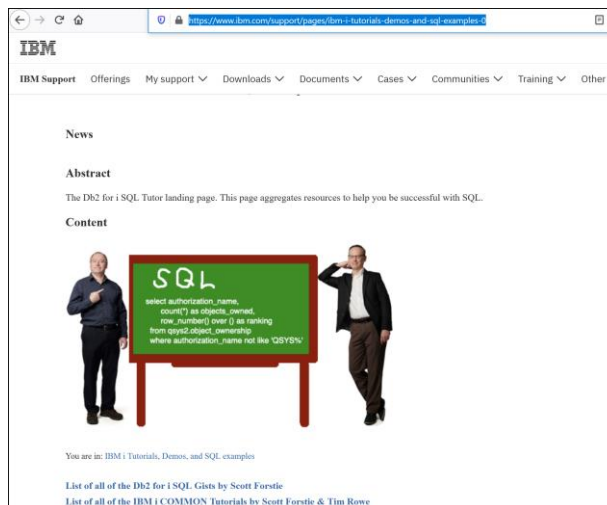
Access Client Solutions (ACS) – Run SQL Scripts

The screenshots illustrate the steps to run SQL scripts in ACS:

- ACS Main Window:** Shows the 'Run SQL Scripts' option under the 'Database' menu, highlighted with a red arrow.
- File Menu:** Shows the 'Examples' option under the 'File' menu, highlighted with a red arrow.
- Examples List:** Shows a list of SQL examples, with 'Security - Authority Collection' selected and highlighted with a red arrow.

8

Resources from IBM (Scott Forstie and Tim Rowe)



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



Core of IBM i Security

Users
User profile settings

Object authorities
Access to libraries,
directories and their
objects

System Values
Security-relevant global settings



User Profiles

- QSYS2.user_info
 - DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) and QSYRUSRI
 - SELECT * from qsys2.user_info;
- Benefits:
 - *Immediately* current regardless of new, changed or deleted profile
 - Select any fields based on any criteria (e.g., special authorities, groups, limited capabilities, last used date, default password)



11

QSYS2.user_info – Default Passwords

- ANZDFTPWD

```

Display Spooled File
File . . . . . : QPSECPWD          Page/Line  1/1
Control . . . . : _____      Columns    1 - 78
Find . . . . .
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
                                     User profiles with default passwords.
5770SS1 V7R4M0 190621
Action taken against profiles . . . . . : *NONE
User
Profile      STATUS      PWDEXP      Text
  
```

- SELECT authorization_name, password_expiration_interval, special_authorities, group_profile_name, supplemental_group_list, last_used_timestamp, status, text_description from **qsys2.user_info** where user_default_password = 'YES' order by status;



12

QSYS2.user_info – Special Authorities

```

11 SELECT authorization_name, special_authorities,
12 group_profile_name, supplemental_group_list, text_description FROM QSYS2.USER_INFO
13 WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'
14 OR AUTHORIZATION_NAME IN (
15 SELECT USER_PROFILE_NAME
16 FROM QSYS2.GROUP_PROFILE_ENTRIES
17 WHERE GROUP_PROFILE_NAME IN (
18 SELECT AUTHORIZATION_NAME
19 FROM QSYS2.USER_INFO
20 WHERE SPECIAL_AUTHORITIES like '%*ALLOBJ%'
21 )
22 )
23 ORDER BY AUTHORIZATION_NAME;

```

Authorization Name	Special Authorities	Group Profile Name	Supplemental Group List	Text Description
AUTHORIZATION_NAME	SPECIAL_AUTHORITIES	GROUP_PROFILE_NAME	SUPPLEMENTAL_GROUP_LI	TEXT_DESCRIPTION
AARONC	*ALLOBJ *SECADM *JOBCTL...	*NONE	-	-
ACADMN01	*ALLOBJ *SECADM	*NONE	-	Admin user for aut



13

QSYS2.user_info – Use Your Imagination!

- Get a list of profiles to disable or delete
 - Last used -> Creation date -> Restore date
- Profiles not owned by xx user profile
- Profiles with Authority Collection active and/or collection exists
- Action auditing values enabled at the profile
- Profiles that are limited capability *NO or *PARTIAL

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzajq/rzajqviewuserinfo.htm



14

QSYS2.group_profile_entries

- DSPAUTUSR SEQ(*GRPPRF)

```
25 -- Groups
26 select * from qsys2.group_profile_entries;
```

GROUP_PROFILE_NAME	USER_PROFILE_NAME	USER_TEXT
ACGRPPRF	ACUSER01	Test user for authority collection

- DSPUSRPRF PYLAB *GRPMBR

```
25 -- Groups
26 select * from qsys2.group_profile_entries
27 where group_profile_name = 'PYLAB';
```

GROUP_PROFILE_NAME	USER_PROFILE_NAME	USER_TEXT
PYLAB	PYUSR01	-
PYLAB	PYUSR02	-



15

Object Authority Services

- QSYS2.object_privileges (DSPOBJAUT)

```
-- Permissions
-- Ownership
select * from qsys2.object_privileges where
system_object_schema = 'CWOODBURY' and
owner <> 'CWOODBURY';

-- *PUBLIC authority
select * from qsys2.object_privileges where
system_object_schema = 'CWOODBURY' and
authorization_name = '*PUBLIC' and
object_authority <> '*EXCLUDE';
```

- QSYS2.ifs_object_privileges (DSPAUT)
- QSYS2.object_ownership (WRKOBJOWN / QSYLOBJA)



16

QSYS2.authorization_list_user_info (DSPAUTL)

The screenshot shows a SQL client window titled "Untitled* - Run SQL Scripts - COMMON1.frankeni.com(localhost)". The query entered is:

```

8
9 select *
10 from qsys2.authorization_list_user_info where authorization_list = 'AR_AU TL'
11 ;

```

The results are displayed in a table with the following columns: AUTHORIZATION_LIST, AUTHORIZATION_NAME, OBJECT AUTHORITY, AUTHORIZATION_LIST_MANAGEMENT, OWNER, OBJECT OPERATIONAL, OBJECT_MANAGEMENT, OBJECT_EXISTENCE, OBJECT_ALTER, OBJECT_REFERENCE, DATA_READ, DATA_ADD, DATA_UPDATE, DATA_DELETE, DATA_EXECUTE.

AUTHORIZATION_LIST	AUTHORIZATION_NAME	OBJECT AUTHORITY	AUTHORIZATION_LIST_MANAGEMENT	OWNER	OBJECT OPERATIONAL	OBJECT_MANAGEMENT	OBJECT_EXISTENCE	OBJECT_ALTER	OBJECT_REFERENCE	DATA_READ	DATA_ADD	DATA_UPDATE	DATA_DELETE	DATA_EXECUTE
AR_AU TL	*PUBLIC	*EXCLUDE	NO	CWOODBURY	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
AR_AU TL	CWOODBURY	*ALL	YES	CWOODBURY	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
AR_AU TL	AR_APP OWN	*CHANGE	NO	CWOODBURY	YES	NO	NO	NO	NO	YES	YES	YES	YES	YES
AR_AU TL	GRF ACCTNG	*USE	NO	CWOODBURY	YES	NO	NO	NO	NO	YES	NO	NO	NO	YES
AR_AU TL	JOHNV	*USE	NO	CWOODBURY	YES	NO	NO	NO	NO	YES	NO	NO	NO	YES
AR_AU TL	AR_DTA OWN	*ALL	NO	CWOODBURY	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
AR_AU TL	ERINT	*CHANGE	NO	CWOODBURY	YES	NO	NO	NO	NO	YES	YES	YES	YES	YES



17

QSYS2.authorization_list_info (DSPAUTLOBJ)

The screenshot shows a SQL client window titled "Untitled* - Run SQL Scripts - COMMON1.frankeni.com(localhost)". The query entered is:

```

1 select authorization_list, object_schema, object_name, system_object_type, object_owner, path_name
2 from qsys2.authorization_list_info where authorization_list = 'AR_AU TL';
3
4

```

The results are displayed in a table with the following columns: AUTHORIZATION_LIST, OBJECT_SCHEMA, OBJECT_NAME, SYSTEM_OBJECT_TYPE, OBJECT_OWNER, PATH_NAME.

AUTHORIZATION_LIST	OBJECT_SCHEMA	OBJECT_NAME	SYSTEM_OBJECT_TYPE	OBJECT_OWNER	PATH_NAME
AR_AU TL	PROD LIB	AP	*PGM	CWOODBURY	-
AR_AU TL	PROD LIB	AR	*PGM	CWOODBURY	-
AR_AU TL	PROD LIB	FINANCE	*PGM	CWOODBURY	-
AR_AU TL	PROD LIB	INIMENU	*PGM	CWOODBURY	-
AR_AU TL	PROD LIB	REPORTS	*PGM	CWOODBURY	-
AR_AU TL	PROD LIB	APUTQ	*OUTQ	CWOODBURY	-
AR_AU TL	PROD LIB	OVERDUE	*FILE	CWOODBURY	-
AR_AU TL	PROD LIB	PAYABLES	*FILE	CWOODBURY	-
AR_AU TL	PROD LIB	RECEIVABLE	*FILE	CWOODBURY	-
AR_AU TL	PROD LIB	BALANCE	*QRYDFN	CWOODBURY	-
AR_AU TL	PROD LIB	CHECKS	*QRYDFN	CWOODBURY	-
AR_AU TL	PROD LIB	DAILYRUN	*QRYDFN	CWOODBURY	-
AR_AU TL	PROD LIB	MONTHEND	*QRYDFN	CWOODBURY	-
AR_AU TL	PROD LIB	YEAREND	*QRYDFN	CWOODBURY	-
AR_AU TL	-	-	*DIR	CWOODBURY	/FTP to Bank



18

System Values

- QSYS2.system_value_info
- Equivalent of QWCRSVAL API

```
1 select * from qsys2.system_value_info where system_value_name like 'QPWD*';
```

System Value Name	Current Numeric Value	Current Character Value
SYSTEM_VALUE_NAME	CURRENT_NUMERIC_VALUE	CURRENT_CHARACTER_VALUE
QPWDQDIF	- 0	
QPWDLMTA3C	- 0	
QPWDLMTREP	- 0	
QPWDQSDIF	- 0	
QPWDQDDCT	- 0	
QPWDMINLEN	6 -	
QPWDMAXLEN	8 -	
QPWDLMTCHR	- *NONE	
QPWDVLPGM	- *NONE	
QPWDXPITV	- 000200	
QPWDLVL	3 -	
QPWDRULES	- *PWDSYSVAL	
QPWDCHGBK	- *NONE	
QPWDXFWRN	7 -	



Authority Collection



Ways to Use the Authority Collection – V7R3

- Determine the authority required for service accounts to work with database files. Simply turn on the authority collection for the service account, examine the entries, and determine the authority required. Undoubtedly it will not require *ALLOBJ!
- Determine where authority is coming from
- Debug authority failures



21

Determining What Authorities a Profile Needs

```

Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

Type of authority collection . . . > *USRPRF      *USRPRF, *OBJAUTCOL
User profile . . . . . winsvr                Name
Library and ASP device:
  Library . . . . . carolnew_                Name, *NONE, *ALL
  ASP device . . . . .                      Name, *SYSBAS
Object . . . . . *ALL                      Name, generic*, *ALL
Object type . . . . . *ALL                  *ALL, *CMD, *DTAARA...
Include DLO . . . . . *NONE                *NONE, *ALL, *DOC, *FLR
Include file system objects . . . *NONE    *NONE, *ALL, *BLKSF...
Delete collection . . . . . *NO            *NO, *YES, *ALL
Detail . . . . . *OBJINF                    *OBJINF, *OBJJOB

```

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys



22

Analyzing the Profile's Collection

```

1 select authorization_name,system_object_name, system_object_type,
2 detailed_required_authority,current_authority, authority_source
3 from qsys2.authority_collection
4 where authorization_name = 'WINSVR'
5 and adopting_program_owner IS NULL;

```

Authorization Name	System Object Name	System Object Type	Detailed Required Authority	Current Authority	Authority Source
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_TYPE	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	AUTHORITY_SOURCE
WINSVR	MAINT00001	*PGM	*OBJOPR *READ *EXECUTE	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*ADD	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*READ	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*READ *DLT	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*OBJOPR	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*OBJOPR	*ALL	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*FILE	*OWNER *OBJEXIST *OBJMG...	*ALL	USER *ALLOBJ



23

V7R4 - Authority Collection *by Object*

- By object, collects the users accessing the objects along with:
 - Current authority
 - Source of the authority
 - Specific authority required by the Operating System



24

```

1 select distinct authorization_name, system_object_name,
2 detailed_required_authority, authority_source
3 from qsys2.authority_collection_libraries
4 where system_object_name = 'ALLOBJUSRS' and
5 adopting_program_owner IS NOT NULL
6 and adopt_authority_used = 0
7 and authorization_name IS NOT NULL;

```

Authorization Name	System Object Name	Detailed Required Authority	Authority Source
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	DETAILED_REQUIRED_AUTHORITY	AUTHORITY_SOURCE
WINSVR	ALLOBJUSRS	*OBJOPR	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*OBJOPR *READ	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*OBJOPR	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *REA...	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*READ *ADD *DLT *UPD	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*ADD	USER *ALLOBJ
WINSVR	ALLOBJUSRS	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CWOODBURY	ALLOBJUSRS	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *REA...	USER *ALLOBJ



25

Configure Authority Collection on the Directory

```

Change Authority Collection (CHGAUTCOL)

Type choices, press Enter.

Object . . . . . '/home/cjwdemo'
Authority collection value . . . *objinf *NONE, *OBJJNF
Include dependent objects . . . *NO *NO, *LF
Directory subtree . . . . . *NONE *NONE, *ALL
Symbolic link . . . . . *NO *NO, *YES
Delete collection . . . . . *NO *NO, *YES

```

Notes:

Object authority collection is already started so no need to run the STRAUTCOL command

Not starting the collection for '/home' – only /home/cjwdemo



26

```

71 -- Authority Collection - directory
72 select distinct authorization_name, path_name,
73 detailed_required_authority, authority_source
74 from qsys2.authority_collection_fsobj
75 where path_name = '/home/cjwdemo' and
76 adopting_program_owner IS NULL and
77 adopt_authority_used = 0 and
78 authorization_name IS NOT NULL;
79

```

Authorization Name	Path Name		Authority Source
AUTHORIZATION_NAME	PATH_NAME	DETAILED_REQUIRED_AUTHORITY	AUTHORITY_SOURCE
TESTER1	/home/cjwdemo	*OBJOPR *READ	GROUP *ALLOBJ
WINSVR	/home/cjwdemo	*OBJOPR *EXECUTE	USER *ALLOBJ
TESTER1	/home/cjwdemo	*OBJOPR *EXECUTE	GROUP *ALLOBJ
WINSVR	/home/cjwdemo	*OBJOPR *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ

Notice – no information for '/home'



27

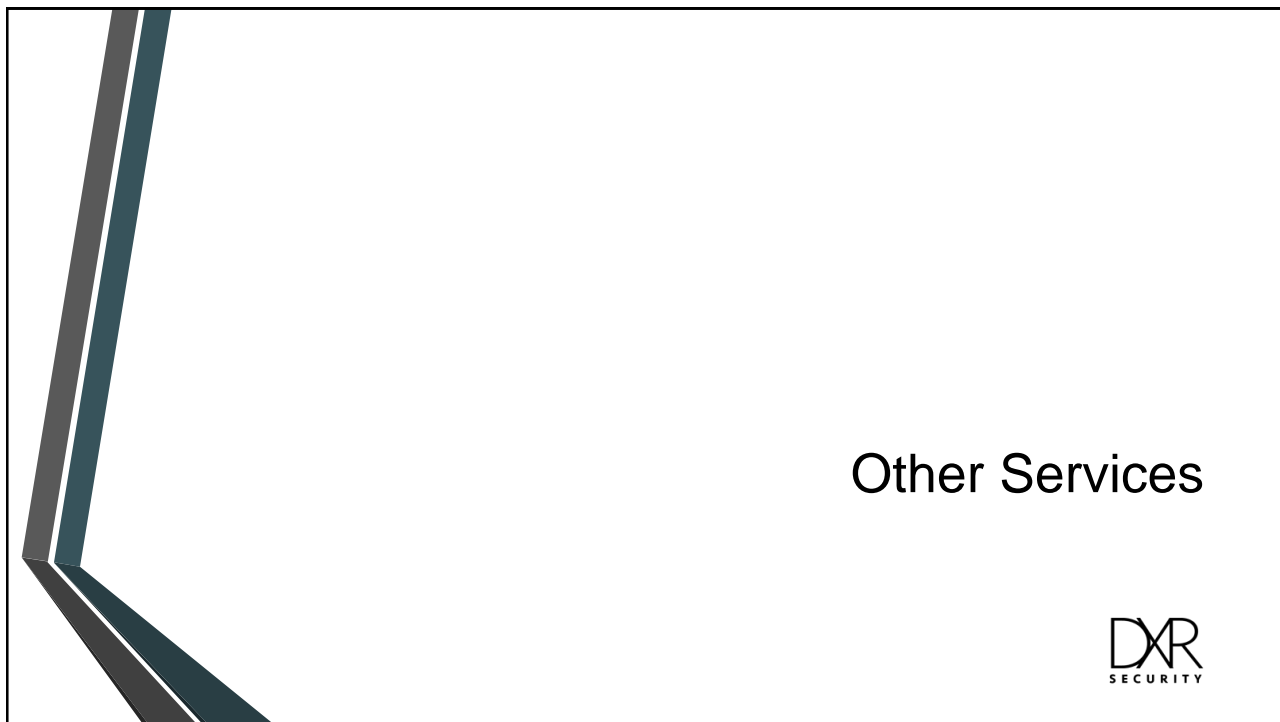
Object Authority Collection Views

- QSYS2.AUTHORITY_COLLECTION_OBJECT
 - Use when the number of entries in the authority collection is large and you are looking for a specific object or objects in a specific library
- QSYS2.AUTHORITY_COLLECTION_LIBRARIES
 - Use when the number of entries in the authority collection is small or you are looking for all or most objects in the authority collection.
- QSYS2.AUTHORITY_COLLECTION_FSOBJ (IFS objects)
- QSYS2.AUTHORITY_COLLECTION_DLO

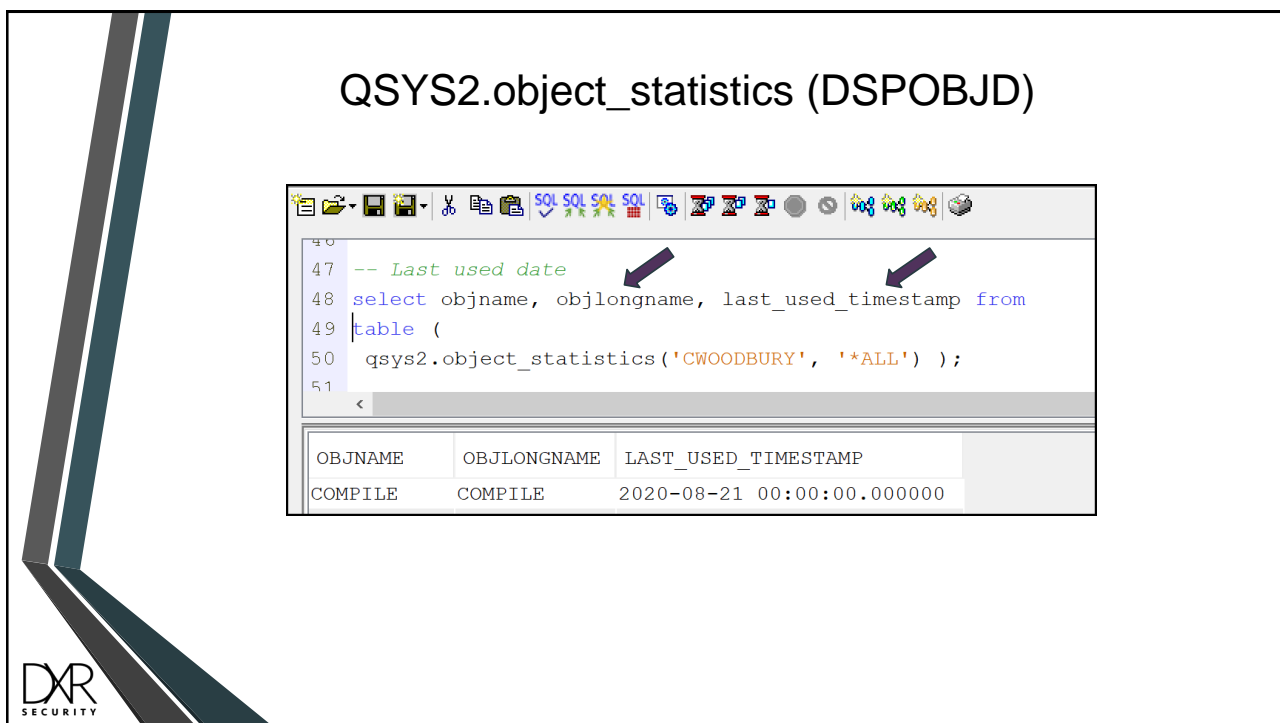


28

28



29



30

QSYS2.ifs_object_statistics

```

3 select path_name, object_type, data_size, object_owner, create_timestamp, access_timestamp
4
5 from table (
6   qsys2.ifs_object_statistics(
7     start_path_name => '/',
8     subtree_directories => 'YES',
9     object_type_list => '**ALLSTMF')
10  where path_name like '%testdemo.jpg%';
11
12

```

PATH_NAME	OBJECT_TYPE	DATA_SIZE	OBJECT_OWNER	CREATE_TIMESTAMP	ACCESS_TIMESTAMP
/FTP to Bank/testdemo.jpg	*STMF	21213	CWOODBURY	2020-07-10 13:26:27	2020-07-10 13:32:56



31

Adopted Authority

- QSYS2.program_info (DSPPGM / DSPPGMADP)

```

44 -- Adopted authority
45 select * from qsys2.program_info where owner = 'QSECOFR' and user_profile = '*OWNER';
46

```

PROGRAM_LIBRARY	PROGRAM_NAME	PROGRAM_TYPE	OBJECT_TYPE	CREATE_TIMESTAMP	TEXT_DESCRIPTION
EMSANDBOX	USERENV	ILE	*PGM	2014-07-11 01:24:01	Set up user environment for EMSANDBO
PROD_LIB	INLMENU	OPM	*PGM	2020-08-10 12:23:01	-
PROFOUNDUI	PUI LICR	ILE	*PGM	2018-03-05 11:25:07	-

- QSYS2.sql_check_authority

- Flips Dynamic User Profile attribute from *OWNER to *USER (or vice versa)



32

SYSTOOLS.group_PTF_currency

```

40
41 -- Group PTFs
42 select * from systools.group_PTF_currency;

```

PTF_GROUP_CURRENCY	PTF_GROUP_ID	PTF_GROUP_TITLE	Group Level	PTF
INSTALLED LEVEL IS CURRENT	SF99653	SF99653 740 Db2 Web Query for i V2.2.1	ED	9
UPDATE AVAILABLE	SF99661	SF99661 740 WebSphere App Server V8.5		1
UPDATE AVAILABLE	SF99662	SF99662 740 IBM HTTP Server for i		7
UPDATE AVAILABLE	SF99663	SF99663 740 Performance Tools		3
UPDATE AVAILABLE	SF99664	SF99664 740 Backup Recovery Solutions		15



33

QSYS2.server_share_info

```

1 select * from qsys2.server_share_info where share_type = 'FILE';

```

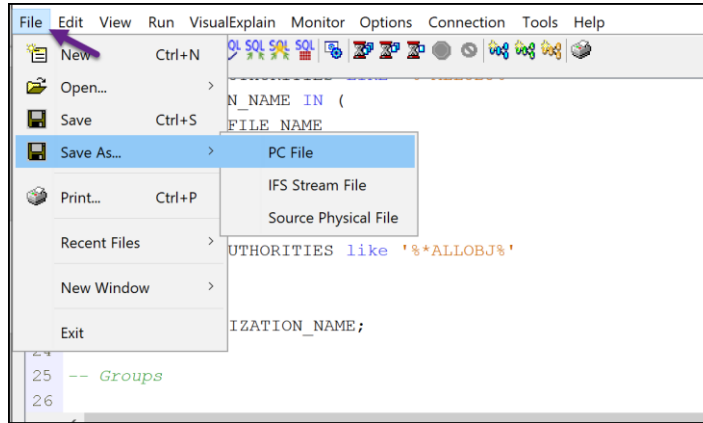
SERVER_SHARE_NAME	SHARE_TYPE	Text Description	ENCRYPTION_REQUIRED	Path Name	Permissions	Current Connections
QDIRSRV	FILE	OS/400 -- Directory Ser...	NO	/QIBM/ProdData/OS400/DirSrv	*RW	0
CHOWLIN	FILE	-	NO	/chowlin	*RW	0
CLAIMIMAGE	FILE	IFS lab	NO	/claimimage	*R	0
LABXL	FILE	-	NO	/LABXL	*RW	0
LABPX	FILE	-	NO	/LABPX	*RW	0
WALABRO	FILE	System i Access for Web...	NO	/walab	*R	0

- Just released 10/06/2020!!!
 - V7R4: SF99704 Level 10
 - V7R3: SF99703 Level 22



34

Save Your Work!



35

Using Services in a CL PGM



36

Two Options

- RUNSQL – added V7R1
 - Runs SQL statements from within a CL program
 - https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/sqj/rbafyrnsql.htm
 - <https://www.rpgpgm.com/2014/03/run-sql-statements-in-your-cl.html> (Simon Hutchinson)
- RUNSQLSTM
 - Runs SQL statements defined in a source file
 - https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/cl/runsqlstm.htm
- BOTH have the restriction that you can't run SELECT ←



37

RUNSQL

```

PGM
DCLF  FILE(QTEMP/LIBRARY) ALWVARLEN(*YES) ALWNULL(*YES)
DCL  VAR(&LIBNAME) TYPE(*CHAR) LEN(10)
CHGJOB CCSID(37) /* Set CCSID (from 65535) */
DLTF  FILE(QTEMP/LIBRARY)
MONMSG MSGID(CPF2105)
RUNSQL  SQL('CREATE TABLE QTEMP.LIBRARY AS +
           (SELECT SYSTEM_OBJECT_NAME, OBJECT_TYPE, OBJECT_AUTHORITY, AUTHORIZATION_NAME, TEXT_DESCRIPTION +
           FROM QSYS2.OBJECT_PRIVILEGES +
           WHERE OBJECT_TYPE = "LIB" AND AUTHORIZATION_NAME = "PUBLIC" AND OBJECT_AUTHORITY <> "EXCLUDE") +
           WITH DATA) COMMIT(*NONE) NAMING(*SQL)
MONMSG MSGID(SQL9010) EXEC(GOTO CMDLBL(DONE))
OVRPRTF FILE(QPQUPRFIL) MAXRCDS(*NOMAX) SPLFNAME(LIBAUT) OVRSCOPE(*CALLLVL) /* Name spooled file - LIBAUT */
RUNQRY QRYFILE((QTEMP/LIBRARY)) OUTTYPE(*PRINTER) FORMSIZE(*RUNOPT 378) /* Print report */
DONE:
ENDPGM

```



38

Administration Runtime Expert (ARE)



39

Administration Runtime Expert (ARE)


- Check various system settings across multiple partitions
 - Authorities, User profile configurations, System value settings
 - PTFs
 - Network configuration
 - ... and more – including the ability to customize your own
- You create a template of what you want checked
 - Run via ARE scheduler or ad hoc
- Reports can be emailed
- Can also 'fix' or push out changes



40

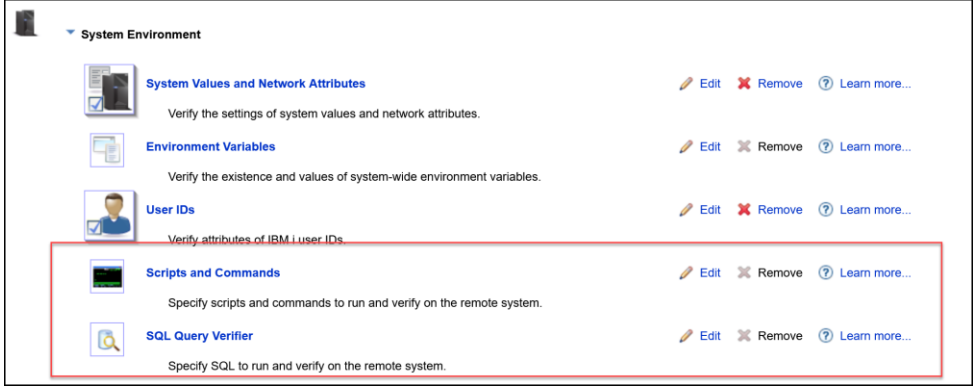
Security-relevant features

- File and directory authorities
- System values
- User profile configuration




41

Customize what is Checked



The screenshot shows a configuration window titled "System Environment" with a list of items to be checked. Each item has a checkbox, a description, and action buttons (Edit, Remove, Learn more...).

Item	Description	Actions
<input checked="" type="checkbox"/> System Values and Network Attributes	Verify the settings of system values and network attributes.	Edit Remove Learn more...
<input checked="" type="checkbox"/> Environment Variables	Verify the existence and values of system-wide environment variables.	Edit Remove Learn more...
<input checked="" type="checkbox"/> User IDs	Verify attributes of IBM I user IDs.	Edit Remove Learn more...
<input checked="" type="checkbox"/> Scripts and Commands	Specify scripts and commands to run and verify on the remote system.	Edit Remove Learn more...
<input checked="" type="checkbox"/> SQL Query Verifier	Specify SQL to run and verify on the remote system.	Edit Remove Learn more...



42

Summary

- SQL isn't that difficult!
- MANY examples exist to help you
 - Scott Forstie's github gists <https://gist.github.com/forstie>
- Views often provide information more easily, is up-to-date and often performs better
- Views allow you to gather information from multiple partitions without having to physically sign on
- CL programs running SQL can be added to your favorite job scheduler



43

Who knows the places you might go?



44

For More Information

IBM i Services page

- <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 Application Runtime Environment support page


- <https://www.ibm.com/support/pages/ibm-administration-runtime-expert-i>

IBM i Security Reference – PDF

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzarl/sc415302.pdf?view=kc

- Chapter 10 – Authority Collection

IBM i Security Administration and Compliance, 3rd edition, by Carol Woodbury, 2020.



45

45

Questions?



Contact: carol@DXRSecurity.com



46

46