



**helpsystems**

What's New and Great about  
IBM i Security –  
including V7R4


Carol Woodbury, CISSP, CRISC, PCIP  
VP Global Security Services  
carol.woodbury@helpsystems.com  
@carolwoodbury

IBM CHAMPION 

© HelpSystems LLC. All rights reserved.  
All trademarks and registered trademarks are the property of their respective owners.

www.helpsystems.com

1



## QLMTDEVSSN

- ▶ Limit active device sessions
  - ▶ Restrict users to active device sessions
    - 0 – Do not limit (existing value)
    - 1 – Limit user to one session (existing value)
    - 2 – 9 Limit users to x number of sessions
- ▶ User profile parameter (LMTDEVSSN) also supports new parameters

© HelpSystems LLC. All rights reserved.

**helpsystems**

2

## Save private authorities

Save Object (SAVOBJ)

Type choices, press Enter.

Private authorities	*NO	*NO, *YES
Storage	*KEEP	*KEEP, *FREE
Data compression	*DEV	*DEV, *NO, *YES, *LOW...
Data compaction	*DEV	*DEV, *NO
Libraries to omit	*NONE	Name, generic*, *NONE...
+ for more values		
Objects to omit:		
Object		Name, generic*, *USRSPC...
Library	*ALL	Name, generic*, *ALL
Object type	*ALL	*ALL, *ALRTBL, *BNDDIR...
+ for more values		

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

More...

© HelpSystems LLC. All rights reserved.

3

## Restore private authorities with objects

Restore Object (RSTOBJ)

Type choices, press Enter.

Option	*ALL	*ALL, *NEW, *OLD, *FREE
File member:		
File	*ALL	Name, *ALL
Member	*ALL	Name, generic*, *ALL, *NONE
+ for more values		
Data base member option	*MATCH	*MATCH, *ALL, *NEW, *OLD
Defer ID	*NONE	Name, *NONE
Spooled file data	*NEW	*NEW, *NONE
Private authorities	*NO	*NO, *YES
Start journaling	*YES	*YES, *NO
Date when saved		Date
Time when saved		Time
Allow object differences	*NONE	*NONE, *COMPATIBLE, *ALL...
+ for more values		

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

More...

Note: Must save the private authorities to be able to restore them ☺

© HelpSystems LLC. All rights reserved.

4

## Authority parm on CPYTOSTMF / CPYTOIMPF

Copy To Stream File (CPYTOSTMF)

Type choices, press Enter.

From file member or save file . . . . .

To stream file . . . . .

Stream file option . . . . .	*NONE	*NONE, *ADD, *REPLACE
Data conversion options . . . . .	*AUTO	*AUTO, *IBL, *NONE
Database file CCSID . . . . .	*FILE	1-65533, *FILE
Stream file CCSID . . . . .	*STMF	1-65533, *STMF, *PCASCII...
Conversion table . . . . .		
End of line characters . . . . .	*CRLF	*CRLF, *LF, *CR, *LFCR...
Authority . . . . .	*DFI	*DFI, *INDIR, *FILE...
Stream file code page . . . . .	*STMF	1-32767, *STMF, *PCASCII...

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

Bottom

5 © HelpSystems LLC. All rights reserved.

5

## Change the owner of all objects in a library

Change Owner (CHGOWN)

Type choices, press Enter.

Object . . . . . /qsys.lib/applib.lib/\*.file

New owner . . . . .	NEWOWNER	Name
Revoke current authority . . . . .	*YES	*NO, *YES
Directory subtree . . . . .	*NONE	*NONE, *ALL
Symbolic link . . . . .	*NO	*NO, *YES

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

Bottom

MA A 05/064

6 © HelpSystems LLC. All rights reserved.

6

## “Renaming” a user profile

- ▶ Copy the user profile
- ▶ Grant private authorities
  - ▶ GRTUSRAUT
- ▶ Transfer all owned objects to the new profile when deleting the old
- ▶ Add a new directory entry (if required)

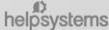
© HelpSystems LLC. All rights reserved.



7

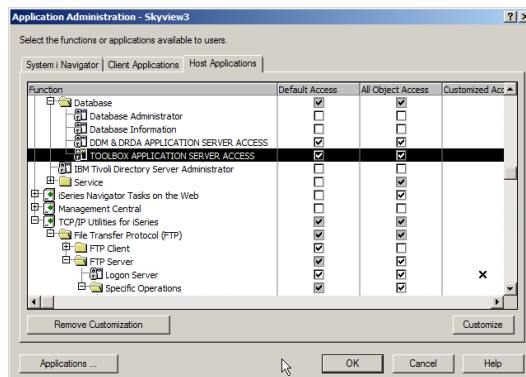
## V7R1 and Technology Releases



HelpSystems Corporate Overview. All rights reserved. 

8

## Application Administration (WRKFCNUSG)



New functions to manage:

- TOOLBOX APPLICATION SERVER ACCESS = ODBC and JDBC
- DDM / DRDA

© HelpSystems LLC. All rights reserved.

helpsystems

9

## Field procedures (FIELDPROC)

SQL programming enhancement:

- ▶ a FIELDPROC allows a user-written exit routine to be defined that will encrypt a field
  - ▶ No need to re-write an application to hold the encrypted field
    - ▶ Encrypted field is held 'internally'
  - ▶ Encryption is not provided by OS
    - ▶ Powertech Encryption for IBM i
      - <https://www.helpsystems.com/products/encryption-and-key-management-software-ibm-i>
- ▶ Values can be displayed as
  - ▶ Clear text
  - ▶ Masked support (for example - xxxx-xxxxxx-1003)
  - ▶ "Not authorized" (for example - zzzz-zzzzzzz-zzzzz)
- ▶ More organizations are choosing to encrypt at the field level

© HelpSystems LLC. All rights reserved.

helpsystems

10

## SQL Views in QSYS2

IBM i Service	Type of Service	IBM i 7.3	IBM i 7.2	IBM i 7.1
<b>PTF Services</b>				
QSYS2.GROUP_PTF_INFO	View	Base	Base	SP99701 Level 6
QSYS2.PTF_INFO	View	Enhanced in Base	Base	SP99701 Level 23
SYSTOOLS.GROUP_PTF_CURRENCY	View	Base	SP99702 Level 3	SP99701 Level 32
		Enhanced: SP99703 Level 2	Enhanced: SP99702 Level 14	Enhanced: SP99701 Level 41
SYSTOOLS.GROUP_PTF_DETAILS	View	Base	SP99702 Level 9	SP99701 Level 38
		Enhanced: SP99703 Level 3	Enhanced: SP99702 Level 14	
<b>Security Services</b>				
QSYS2.AUTHORITY_COLLECTION	View	Base	-	-

<https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/DB2%20for%20i%20-%20Services>

11 © HelpSystems LLC. All rights reserved.



11

## Access Client Solutions (ACS) – Run SQL Scripts

The screenshot shows the IBM Access Client Solutions (ACS) interface. The 'File' menu is open, highlighting the 'Insert from Examples...' option. The 'Examples' window is also open, showing a list of SQL scripts for various IBM i services, including 'QSYS2.AUTHORITY\_COLLECTION' and 'SYSTOOLS.GROUP\_PTF\_CURRENCY'.

12 © HelpSystems LLC. All rights reserved.



12

## View determining Group PTF currency

Untitled\* - Run SQL Scripts - R2D2(H02D0CBR)

```
1 select * from systools.group_ptf_currency
2
```

PTF_GROUP_CURRENCY	PTF_GROUP_ID	PTF_GROUP_TITLE	PTF_GROUP_LEVEL INSTALLED	PTF_GROUP_LEVEL AVAILABLE	PTF_GROUP_LAST UPDATED_BY IBM	PTF_GROUP
INSTALLED LEVEL IS CURRENT	SF99225	SF99225 730 IBM Open Source Solutions for i	6	6	11/06/2017	R730
UPDATE AVAILABLE	SF99703	SF99703 730 DB2 for IBM i	8	8	02/07/2018	R730
INSTALLED LEVEL IS CURRENT	SF99722	SF99722 730 IBM HTTP Server for i	13	13	12/27/2017	R730
UPDATE AVAILABLE	SF99724	SF99724 730 Backup Recovery Solutions	16	16	03/20/2018	R730
INSTALLED LEVEL IS CURRENT	SF99725	SF99725 730 Java	7	7	12/28/2017	R730
UPDATE AVAILABLE	SF99727	SF99727 730 Technology Refresh	3	3	03/15/2018	R730
UPDATE AVAILABLE	SF99728	SF99728 730 Group Security	19	19	03/20/2018	R730
UPDATE AVAILABLE	SF99729	SF99729 730 Group Hiper	48	48	03/20/2018	R730
UPDATE AVAILABLE	SF99730	Current Cumulative PTF Media Documentation	17283	18025	03/16/2018	R730
UPDATE AVAILABLE	SF99875	SF99875 730 Hardware and Related PTFs	13	13	03/20/2018	R730
INSTALLED LEVEL IS CURRENT	SF99876	SF99876 730 High Availability for IBM i	5	5	10/18/2017	R730

Done: 11 rows retrieved.

Messages | Global Variables and Special Registers | select \* from systools.group\_ptf\_currency |

Connected to relational database H02D0CBR on R2D2 as CJW - 216402/USER/QZDASOINIT using JDBC configuration Default.

13 © HelpSystems LLC. All rights reserved.

helpsystems

13

## V7R2 and Technology Releases

UP NEXT

HelpSystems Corporate Overview. All rights reserved. helpsystems

14

## Password rules (QPWDRULES)

- ▶ \*MAXLENnnn
  - ▶ \*MINLENnnn
  - ▶ \*MIXCASEnnn
  - ▶ \*REQANY3
  - ▶ \*SPCCHRLMTAJC
  - ▶ \*SPCCHRLMTFST
  - ▶ \*SPCCHRLMTLST
  - ▶ \*SPCCHRMAXn
  - ▶ \*SPCCHRMINn
- V7R2**
- ▶ \*ALLCRTCHG
- \*PWDSYSVAL or
  - ▶ \*CHRLMTAJC
  - ▶ \*CHRLMTREP
  - ▶ \*DGTLMATAJC
  - ▶ \*DGTLMTFST
  - ▶ \*DGTMLTLST
  - ▶ \*DGTMAXn
  - ▶ \*DGTMINn
  - ▶ \*LMTSAMPOS
  - ▶ \*LMTPRFNAME
  - ▶ \*LTRLMTAJC
  - ▶ \*LTRLMTFST
  - ▶ \*LTRLMTLST
  - ▶ \*LTRMAXn
  - ▶ \*LTRMINn



Hint: Once you start to use QPWDRULES, put all of the password composition rules in this value because others will be ignored

© HelpSystems LLC. All rights reserved.

helpsystems

15

## “Before” values added to these audit entries

- ▶ AD—Auditing value changes
- ▶ AU—Attribute changes
- ▶ CA—Authority changes
- ▶ CP—User profile changes (Note: only the previous special authority values have been added)
- ▶ DI—Directory server
- ▶ GR—Generic record (added changes to the function usage (Application Administration) settings)
- ▶ PA—Program adopt
- ▶ PG—Primary group changes
- ▶ RA—Restore object authority changes (added the name of the authorization list)
- ▶ RJ—Restore job description (added name that had been specified in the job description)
- ▶ RO—Ownership changes for restored objects
- ▶ RZ—Primary group changes for restored objects

© HelpSystems LLC. All rights reserved.

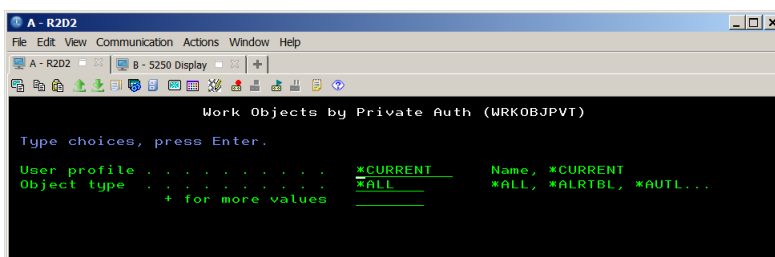
helpsystems

16



## Changes to commands

- ▶ The following commands now accept an object type so you can scope your search:
  - ▶ WRKOBJOWN – work with objects by owner
  - ▶ WRKOBJPGP – work with objects by primary group
  - ▶ WRKOBJPVT – work with objects by private authorities



© HelpSystems LLC. All rights reserved.

helpsystems

17

## RCAC – Row and column access control

- ▶ Rows: Using SQL, can put rules in place at the file level (outside of program logic) to limit which users can see which rows
  - ▶ Has the potential to eliminate logical files
- ▶ Columns: Using SQL, can put rules in place at the file level to determine who can see the full contents of a field in a column or a masked value

© HelpSystems LLC. All rights reserved.

helpsystems

18

## RCAC prerequisites

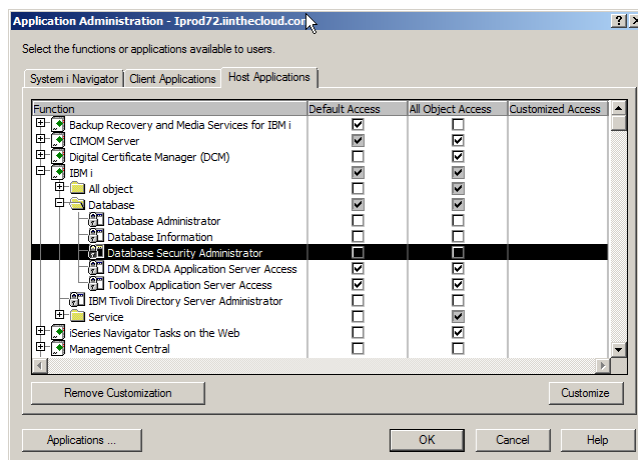
- ▶ Requires installation of BOSS option 47 IBM Advanced Data Security for i (no charge)
- ▶ To administer, someone needs to have the Security Administration function usage or QIBM\_DB\_SECADM privilege as defined in Application Administration.

© HelpSystems LLC. All rights reserved.



19

## DB administrator – App Admin



© HelpSystems LLC. All rights reserved.



20

## RCAC

- ▶ Object level security takes precedence. If you have permission as defined by RCAC you must first have object authority.
- ▶ Once activated, just like object security, it's in effect for every object access method – ftp, ODBC, queries, command such as UPDDTA and RUNQRY, etc

© HelpSystems LLC. All rights reserved.



23

## Adding a row permission

```
CREATE PERMISSION emp_info ON hr
FOR ROWS WHERE
(
  VERIFY_GROUP_FOR_USER (SESSION_USER,'MGR01') = 1
  AND dept = '001'
)
OR
(
  VERIFY_GROUP_FOR_USER (SESSION_USER,'MGR02') = 1
  AND dept = '002'
)
OR
(
  VERIFY_GROUP_FOR_USER (SESSION_USER,'DIRECTOR') = 1
)
OR
(
  CURRENT_USER = 'APP_OWN'
)

ENFORCED FOR ALL ACCESS
ENABLE;
COMMIT;
ALTER TABLE hr ACTIVATE ROW ACCESS CONTROL;
COMMIT;
```

VERIFY\_GROUP\_FOR\_USER is a new SQL function added in V7R2

SESSION\_USER = profile trying to access the file  
CURRENT\_USER = Owner of last program set to USRPRF(\*OWNER)

© HelpSystems LLC. All rights reserved.



24

## Row permission considerations

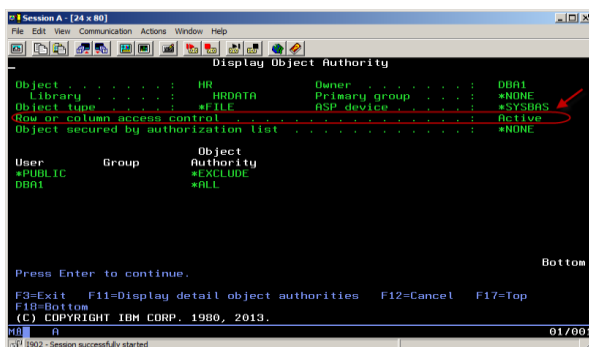
- ▶ The absence of authority prevents access to data
- ▶ Need to consider how production issues are debugged
  - ▶ If using a tool to elevate privileges, may need to grant privileges to the profile being adopted or swapped to so they can access the data
  - ▶ No indication that the data is sub-setted
- ▶ When copying files to QA or Dev systems, may need to grant additional row privileges for testing
- ▶ Need to make sure that users will still get correct data if data is already being filtered via a logical file or program logic

© HelpSystems LLC. All rights reserved.



25

## RCAC restrictions – no green screen management



```

Session A - [24 x 80]
File Edit View Communication Actions Window Help

Display Object Authority

Object      : HRDATA      Owner      : DBA1
Library     : HRDATA      Primary group : *NONE
Object type : *FILE       ASP device  : *SYSBAS
Row or column access control : Active
Object secured by authorization list : *NONE

User      Group      Object Authority
*PUBLIC   DBA1          *EXCLUDE
          DBA1          *ALL

Press Enter to continue.

F9=Exit  F11=Display detail object authorities  F12=Cancel  F17=Top
F18=Bottom
(C) COPYRIGHT IBM CORP., 1980, 2013.
DB  01/001
0002 - Session successfully started
  
```

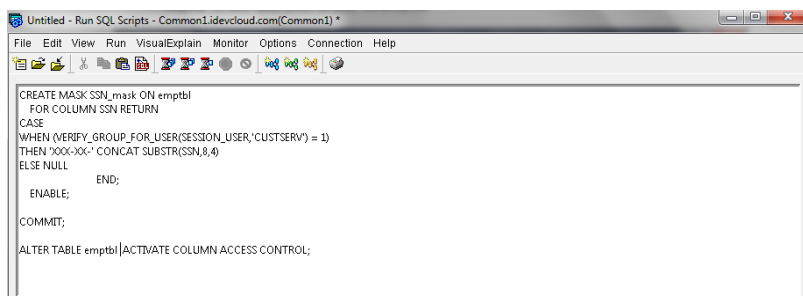
Or query new QSYS2/SYSCONTROLS catalog

© HelpSystems LLC. All rights reserved.



26

## Column masks



```

CREATE MASK SSN_mask ON emptytbl
FOR COLUMN SSN RETURN
CASE
WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER,'CUSTSERV') = 1)
THEN 'XXX-XX-XXXX' || CONCAT SUBSTR(SSN,8,4)
ELSE NULL
END;
ENABLE;
COMMIT;
ALTER TABLE emptytbl ACTIVATE COLUMN ACCESS CONTROL;

```

© HelpSystems LLC. All rights reserved.



27

## Column mask considerations

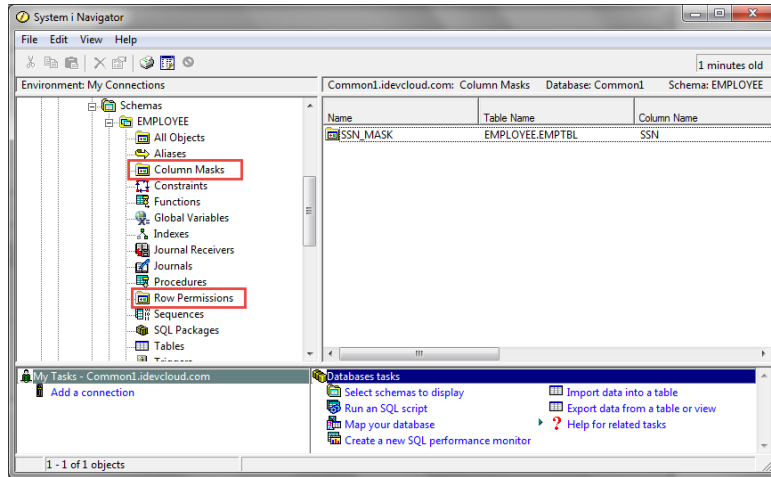
- ▶ Masking is NOT a replacement for encryption!
  - ▶ May be a good option for test systems if you don't already have a process to mask production data.
- ▶ Need to consider program logic – is a record read and then written back? If so, the masked data may be written, over-writing your data.
  - ▶ New check constraint support will help prevent this. See <http://www.mcpressonline.com/database/techtip-protecting-against-accidental-updates-with-masked-values.html>
- ▶ When restoring an RCAC-protected file to another system, data will not be accessible if BOSS option 47 isn't installed.

© HelpSystems LLC. All rights reserved.



28

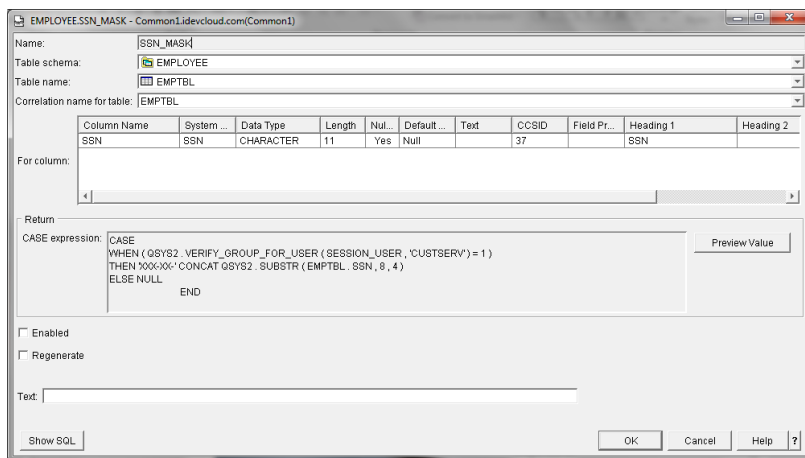
## Only administered through Navigator for i or ACS



© HelpSystems LLC. All rights reserved.

helpsystems


29



© HelpSystems LLC. All rights reserved.

helpsystems

30




## For more information on RCAC


---

- ▶ DB2 for i SQL Reference manual
  - ▶ [https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_71/db2/rbafz.pdf](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_71/db2/rbafz.pdf)
- ▶ Redpiece ★★★★★
  - ▶ <http://www.redbooks.ibm.com/abstracts/redp5110.html>

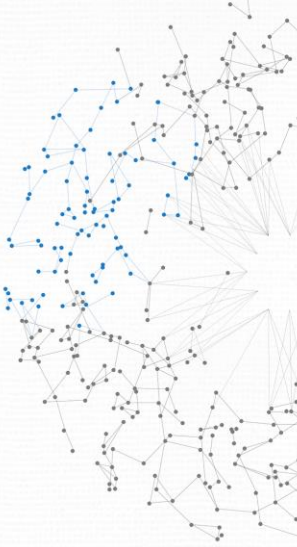
© HelpSystems LLC. All rights reserved.





31



## V7R3



 UP NEXT

HelpSystems Corporate Overview. All rights reserved. 

32

## V7R3 - Auditing enhancements

- ▶ CP – contains all user profile attributes except TEXT and AUT (\*PUBLIC authority) for both create and changes to a user profile
- ▶ QAUDLVL
  - ▶ \*NETSECURE (to audit secure network connections)
  - ▶ \*NETTELSVR (to audit telnet connections)
  - ▶ \*NETUDP (to audit UDP connections)
  - ▶ \*NETSCK is no longer considered a subset of \*NETCMN

© HelpSystems LLC. All rights reserved.



33

## V7R3 - DCM enhancements

- ▶ Digital Certificate Manager (DCM) allows you to assign up to 4 certificate to a server
  - ▶ Helps you move to use stronger encryption even if some connections require weaker protocols

© HelpSystems LLC. All rights reserved.



34



## V7R3 - Authority Collection by User

- ▶ By user, collects the objects accessed along with:
  - ▶ Current authority
  - ▶ Source of the authority
  - ▶ Specific authority required by the Operating System

© HelpSystems LLC. All rights reserved.



35

## 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

© HelpSystems LLC. All rights reserved.



36

## Start Authority Collection (STRAUTCOL)

```

Display Data
Position to line . . . . . Data width . . . . . : 72
....+....1....+....2....+....3....+....4....+....5....+....6....+....7...
Timestamp . . . . . User . . . . . Object . . . . . Library . . . . . Object
2018-04-03-13.16.18.619760 CJWTEST DEMO CJW *DTAARA
***** End of data *****

Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

User profile . . . . . cjwtest . . . . . Name
Library and ASP device: . . . . . Library . . . . . Name, *NONE, *ALL
2 . . . . . *SYSBAS . . . . . Name, *SYSBAS
ASP device . . . . . + for more values
Object . . . . . *ALL . . . . . Name, generic*, *ALL
+ for more values
Object type . . . . . *dtara . . . . . *ALL, *CMD, *DTAARA...
+ for more values
Include DLO . . . . . *NONE . . . . . *NONE, *ALL, *DOC, *FLR
+ for more values
Include file system objects . . . . . *NONE . . . . . *NONE, *ALL, *BLKSF...
+ for more values
Delete collection . . . . . *NO . . . . . *NO, *YES
Detail . . . . . *OBJINF . . . . . *OBJINF, *OBJJOB

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

MD 13/037

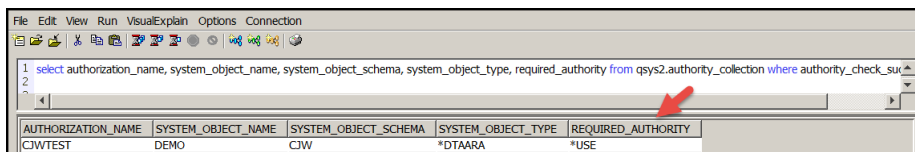
```

© HelpSystems LLC. All rights reserved.



37

## Querying the collection QSYS2.authority\_collection



```

1 select authorization_name, system_object_name, system_object_schema, system_object_type, required_authority from qsys2.authority_collection where authority_check_suc
2

```

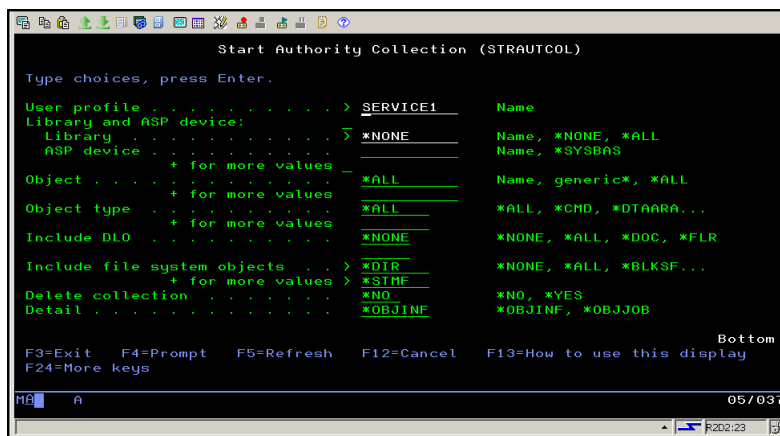
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	REQUIRED_AUTHORITY
CJWTEST	DEMO	CJW	*DTAARA	*USE

© HelpSystems LLC. All rights reserved.



38

## Start authority collection for SERVICE1 – IFS discovery

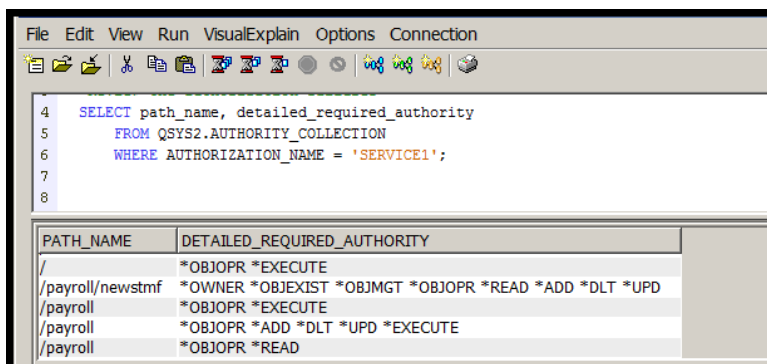


39 © HelpSystems LLC. All rights reserved.

helpsystems

39

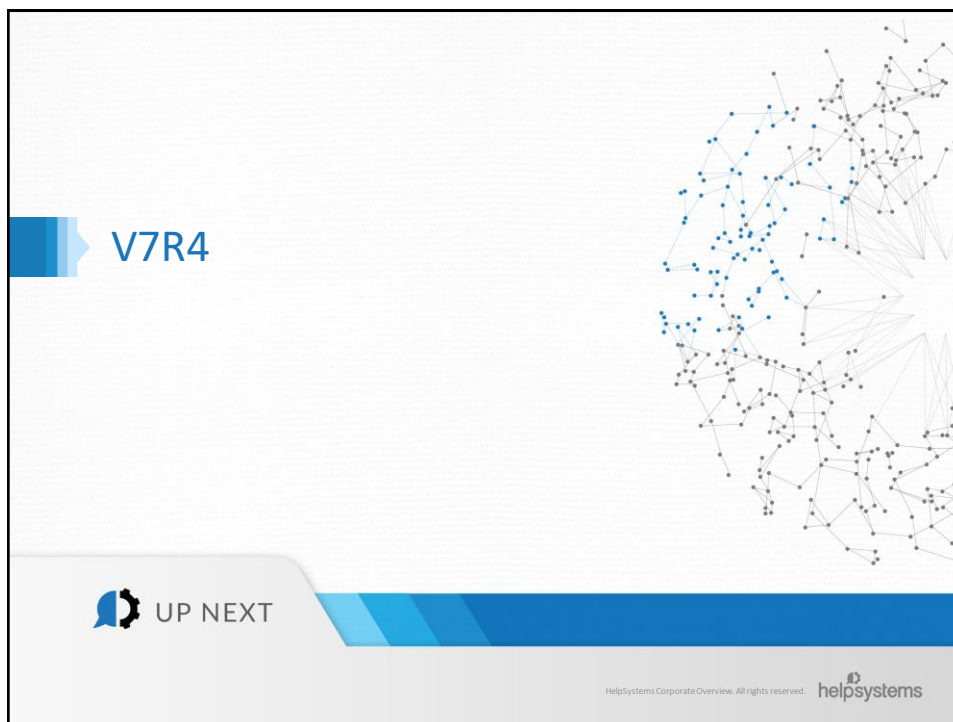
## Query the collection for SERVICE1



40 © HelpSystems LLC. All rights reserved.

helpsystems

40



41

A presentation slide titled 'V7R4 - Authority Collection by Object'. The title is preceded by a blue arrow icon. Below the title, a list of bullet points is shown, each preceded by a blue arrow icon. The first bullet point is 'By object, collects the users accessing the objects along with:', followed by three sub-bullets: 'Current authority', 'Source of the authority', and 'Specific authority required by the Operating System'. At the bottom left, the text '© HelpSystems LLC. All rights reserved.' is visible. At the bottom right, the 'helpsystems' logo is displayed. A blue horizontal bar runs across the bottom of the slide.

42

## Ways to use the Authority Collection – V7R

- Determine what profiles are accessing a specific object and the authority required

© HelpSystems LLC. All rights reserved.

helpsystems

43

## V7R4 - Configuring Authority Collection – Step 1

```

Change Authority Collection (CHGAUTCOL)

Type choices, press Enter.

Object . . . . . /qsus.lib/skyviewpmp.lib
Authority collection value . . . *objinf *NONE, *OBJINF
Include dependent objects . . . *NO *NO, *LF
Directory subtree . . . *ALL *NONE, *ALL
Symbolic link . . . *NO *NO, *YES
Delete collection . . . *NO *NO, *YES

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

Bottom

10/03/7

```

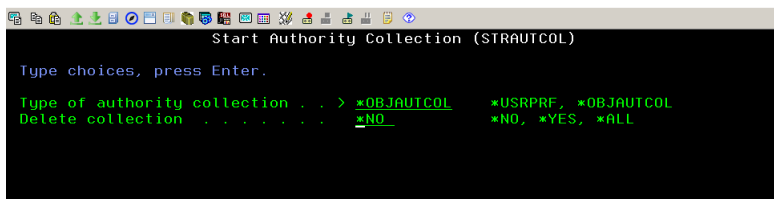
Running this enables authority collection for all objects in the SKYVIEWPMP library.

44 © HelpSystems LLC. All rights reserved.

helpsystems

44

## Configuring Authority Collection – Step 2



```

Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

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

Authority collection is now active for all objects configured using CHGAUTCOL.

## Authority Collection – More considerations

- ▶ You must have either \*ALLOBJ special authority or be authorized to the Database Security Administrator function (QIBM\_DB\_SECADM) to start the collection. You can administer this function via Application Administration (which is available as part of Navigator for i) or the Work with Function Usage (WRKFCNUSG) command.
- ▶ Limit User Function (Application Administration) settings are not recorded.
- ▶ For those features where authority to an object plus some special authority is required, the special authority requirement is not recorded.
- ▶ To display whether a collection is active and/or an authority collection repository exists for a user, run the DSPUSRPRF (Display User Profile) command and scroll to the end of the display. Use DSPOBJD to see when the collection is active for an object (V7R4.)
- ▶ While a user's collection setting is saved when running the SAVSECDTA (Save Security Data) command, the actual collection data is not. Likewise, saving an object does not save the collection (V7R4.)
- ▶ If an authority collection exists and the profile or object (V7R4) is deleted, its authority collection is also deleted.
- ▶ If you specify to collect authority for all objects in all libraries, some objects, such as operating system programs are omitted from the collection; however, objects, such as IBM-supplied commands will be included in the collection data
- ▶ See Chapter 10 of the *IBM i Security Reference* manual for more details.

## V7R4 - New SST Commands

```

File Edit View Communication Actions Window Help
-----
CMDSSST      System Service Tools Commands

Select one of the following:

Commands
1. Change SST Security Attributes      CHGSSSTSECA
2. Change Service Tools User ID       CHGSSSTUSR
3. Create Service Tools User ID       CRTSSTUSR
4. Delete Service Tools User ID       DLTSSTUSR
5. Display SST Security Attrs         DSPSSSTSECA
6. Display Service Tools User ID      DSPSSSTUSR
7. Start System Service Tools         STRSST

Selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F16=Major menu
(C) COPYRIGHT IBM CORP. 1980, 2018.
MLA B 21/007

```

47 © HelpSystems LLC. All rights reserved.

helpsystems

47

## V7R4 - CRTSSTUSR

```

Create Service Tools User ID (CRTSSTUSR)

Type choices, press Enter.

Requesting SST user ID . . . . . Character value
Requesting SST user ID pwd . . . . . Character value
Service tools user ID info:
  Password . . . . .
  Status . . . . . *ENABLED *ENABLED, *DISABLED
  Set password to expired . . . . . *NO *NO, *YES
  Text 'description' . . . . . *BLANK
Linked profile . . . . . *NONE Character value, *NONE

More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
MLA A MW 05/037

```

48 © HelpSystems LLC. All rights reserved.

helpsystems

48

## V7R4 - Encryption enhancements

- ▶ TLS1.3 is enabled!
- ▶ QSSLPCL:
  - ▶ \*OPSYS (default) = \*TLSv1.2 and \*TLSv1.3
  - ▶ \*TLSV1.0 and \*TLSV1.1 are removed from the default but can be added back in
  - ▶ \*SSLv2 can no longer be specified.

49

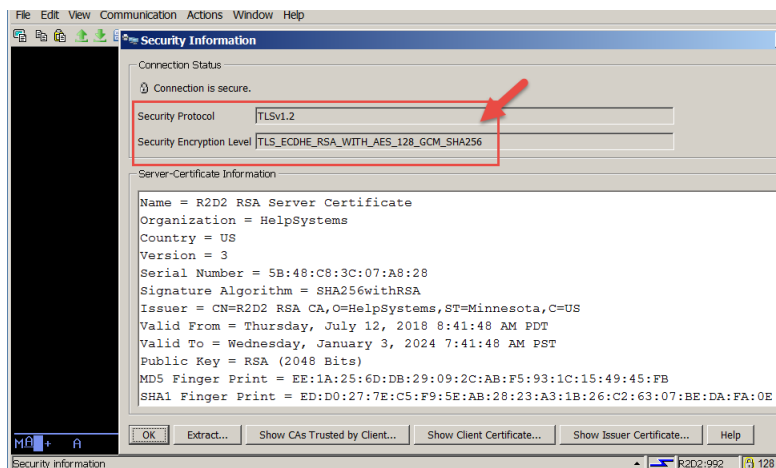
## V7R4 – Encryption enhancements continued

- ▶ QSSLCSL default cipher list is changed – now includes:
  - ▶ \*AES\_128\_GCM\_SHA256
  - ▶ \*AES\_256\_GCM\_SHA384
  - ▶ \*CHACHA20\_POLY1305\_SHA256
  - ▶ \*ECDHE\_ECDSA\_AES\_128\_GCM\_SHA256
  - ▶ \*ECDHE\_ECDSA\_AES\_256\_GCM\_SHA384
  - ▶ \*ECDHE\_RSA\_AES\_128\_GCM\_SHA256
  - ▶ \*ECDHE\_RSA\_AES\_256\_GCM\_SHA384
- ▶ Removed:
  - ▶ ECDSA\_SHA224
  - ▶ ECDSA\_SHA1
  - ▶ RSA\_SHA224
  - ▶ RSA\_SHA1
  - ▶ RSA\_MD5

50



## Hint: Check current encryption levels



51

## Check to see if Protocols / Ciphers are in Use

- ▶ Enable counters in SST to determine if protocols / ciphers are in use
  - ▶ <http://www-01.ibm.com/support/docview.wss?uid=nas8N1020451>
- ▶ Run a communication trace to determine what process is using the protocol / cipher
  - ▶ <http://www-01.ibm.com/support/docview.wss?uid=nas8N1020594>

52

## Coffee with Carol Webinars

- ▶ Making the Move from SSL to TLS
  - ▶ <https://www.helpsystems.com/resources/on-demand-webinars/making-move-ssl-tls11-and-tls12>
- ▶ Configuring ACS to use SSL/TLS
  - ▶ <https://www.helpsystems.com/resources/on-demand-webinars/configuring-acs-access-client-solutions-use-ssl-tls>
- ▶ Securely Deploying ACS
  - ▶ <https://www.helpsystems.com/resources/on-demand-webinars/securely-deploying-ibms-access-client-solutions-acs>

© HelpSystems LLC. All rights reserved.



53

## For more information

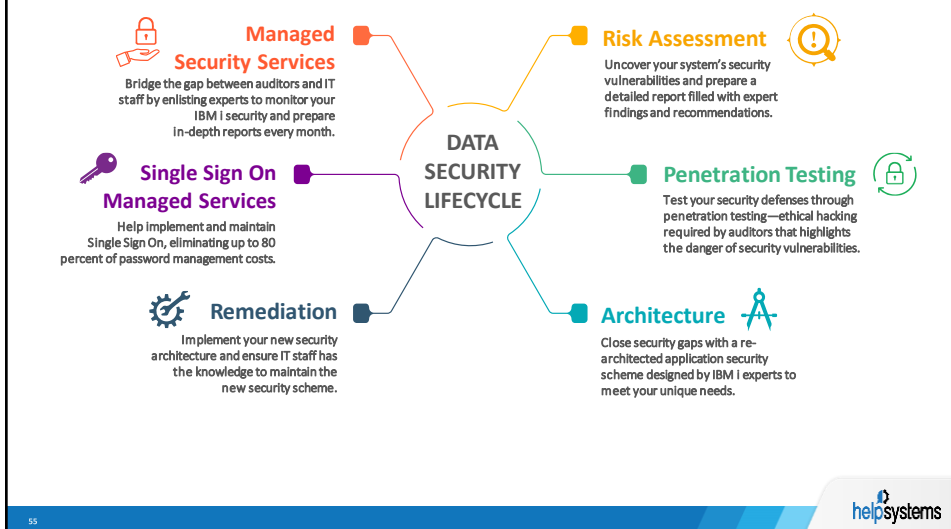
- ▶ IBM i Security Administration and Compliance, 2<sup>nd</sup> edition
  - ▶ [www.mc-store.com/5129.html](http://www.mc-store.com/5129.html)
- ▶ Technical updates
  - ▶ [www.ibm.com/developerworks/ibmi/techupdates](http://www.ibm.com/developerworks/ibmi/techupdates)
- ▶ IBM i Information Center
  - ▶ [http://www-01.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i/welcome](http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i/welcome)
- ▶ Security Reference manual
  - ▶ Chapter 9 – Auditing
  - ▶ Chapter 10 – Authority Collection

© HelpSystems LLC. All rights reserved.



54

## HelpSystems' Professional Security Services



55


## HelpSystems' Solution-based Approach



56


Questions?

---



[www.helpsystems.com](http://www.helpsystems.com)  
[www.helpsystems.com/professional-security-services](http://www.helpsystems.com/professional-security-services)  
800-328-1000 | [info@helpsystems.com](mailto:info@helpsystems.com)

© HelpSystems LLC. All rights reserved.



57