



and the IBM i Community presents: -

International i-Power 2020_(v)

June 10th and June 11th 2020

In support of our **NHS**



Scroll down to see the Fund-Ometer !!

Authority Collection Services

Steve Bradshaw

Technical Director of i-UG (COMMON UK)

Steve.Bradshaw@RowtonIT.com

Authority Collection Services

Today's agenda

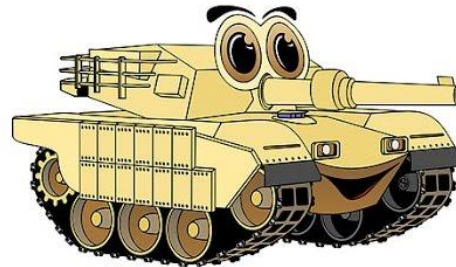
- What is the problem?
- What are Authority Collection Services?
- How do you use them?
- How do you get them?
- How much do they cost?
- What don't they do?

What is the problem?

IBM i is the most secure platform in the world right ?



=



Yes - but it has to be configured

And it has to be maintained

ProTip Check out 5733ARE to help you with maintenance

What is the problem?

- By default your system is not secured
- Too many users have *ALLOBJ authority
- Users gain authorities via Groups, Adoption & Swaps

Protip – Use IBM i Services to help you check

AUTHORIZATION_NAME	STATUS	NO_PASSWORD_INDICATOR	PREVIOUS_SIGNON	TEXT_DESCRIPTION
QLPAUTO	*ENABLED	NO	-	IBM-supplied User Profile
QLPINSTALL	*ENABLED	NO	-	IBM-supplied User Profile
QSECOFR	*ENABLED	YES	2015-09-20 13:05:04.000000	Security Officer
QSECOFR1	*ENABLED	YES	2015-09-20 14:29:08.000000	Security Officer
QSYS	*ENABLED	NO	-	Internal System User Profile
ROWTON	*ENABLED	YES	2015-09-20 13:56:51.000000	Rowton Support
SURPRISE	*ENABLED	YES	2015-09-20 14:29:52.000000	Has AllObj because Rowton is Group Profile
ZENDADMIN	*ENABLED	NO	-	Zend Server Administrator

IBM i Services give you a better answer

For example – Finding Users with the All Object Special Authority

PRTUSRPRF TYPE(*AUTINFO) SPCAUT(*ALLOBJ)

User	Group	*ALL	*AUD	SYS	*JOB	*SAV	*SEC	*SER	*SPL	User
Profile	Profiles	OBJ	IT	CFG	CTL	SYS	ADM	VICE	CTL	Class
QLPAUTO	*NONE	X		X	X	X	X			*SYSOPR
QLPINSTALL	*NONE	X		X	X	X	X			*SYSOPR
QSECOFR	*NONE	X	X	X	X	X	X	X	X	*SECOFR
QSECOFR1	*NONE	X	X	X	X	X	X	X	X	*SECOFR
QSYS	*NONE	X	X	X	X	X	X	X	X	*SECOFR
ROWTON	*NONE	X	X	X	X	X	X	X	X	*SECOFR
ZENDADMIN	*NONE	X	X	X	X	X	X	X	X	*SECOFR

Using IBM i Services we get a more complete answer

AUTHORIZATION_NAME	STATUS	NO_PASSWORD_INDICATOR	PREVIOUS_SIGNON	TEXT_DESCRIPTION
QLPAUTO	*ENABLED	NO	-	IBM-supplied User Profile
QLPINSTALL	*ENABLED	NO	-	IBM-supplied User Profile
QSECOFR	*ENABLED	YES	2015-09-20 13:05:04.000000	Security Officer
QSECOFR1	*ENABLED	YES	2015-09-20 14:29:08.000000	Security Officer
QSYS	*ENABLED	NO	-	Internal System User Profile
ROWTON	*ENABLED	YES	2015-09-20 13:56:51.000000	Rowton Support
SURPRISE	*ENABLED	YES	2015-09-20 14:29:52.000000	Has AllObj because Rowton is Group Profile
ZENDADMIN	*ENABLED	NO	-	Zend Server Administrator

User SURPRISE inherits the *ALLOBJ super power from its Group Profile ROWTON. It does not have *ALLOBJ specified in its own right so does not show up on the PRTUSRPRF. That doesn't stop this user from having full access to every object on the system!

What is the problem?

- What happen when there is a problem with authority?



- We Call Support

- Often, their default answer is to grant more authority

What is the problem?

- What happen when you apply a software patch / upgrade?



Often the new default authority after patching is too generous

Most ISV's are interested in making software work,
not making software secure

One size does NOT fit all!

- Not all users need the same level of access
- Some users need more authority than others
- How do you know which user needs what authority?
- How can you know what authority is really needed?



So what is the **Business** problem?

Figuring all this out takes time and money



Because of GDPR there is a bigger cost if you ignore security!

What is the challenge?

How can I improve my security without

BREAKING MY APPLICATION!!!

or

BREAKING THE BANK

(Spending too much)

What are Authority Collections?

It is an IBM supplied monitoring service which:

- Calculates what authority you have

- Watches what you do

- Works out what authority you actually needed

- Records the above information

- Reports it back to you

How do they work?

They work like Performance Collection Services:

- They run in the background

- They have a very small performance overhead

- You can start and stop them whenever you like

- You choose how much you want to monitor

- They can use up a lot of disk space

How do you use them?

Step 1 – Choose a User

Step 2 – Choose a library

Step 3 – Start the Authority Collection

Step 4 – Wait while the user does their job

Step 5 – Analyse the results

Step 6 – Repeat

(Monitor different time, user, application, etc)

How do you use them?

Example – Starting Authority Collection using 5250

```
Start Authority Collection (STRAUTCOL)

Type choices, press Enter.

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

How do you use them?

Example: Starting Authority Collection using Nav for i

The screenshot displays the IBM Navigator for i web interface. The top navigation bar includes the product name 'IBM® Navigator for i', the user 'Welcome qsecofr', the target system '192.168.2.206', and links for 'Help' and 'Logout'. The left sidebar contains a navigation tree with categories like 'Welcome', 'Dashboard', 'Search Task', and 'IBM i Management'. The 'Start Authority Collection' task is selected in the tree. The main content area shows a dialog box with the following fields:

- User:** Rowton
- Libraries to search:** Use entry from below (dropdown), Ritmor (text input), and a 'Browse' button.
- Objects to search:** All (dropdown), with a note 'All, Generic* or Name (up to 10)' and an empty text input field.
- Object types:** All (dropdown), with a note 'All, Types (up to 10)', a 'Browse' button, and an empty text input field.
- Include document library objects:** None (dropdown)
- Include file system objects:** None (dropdown), with a 'Browse' button and an empty text input field.
- Delete previous collection?:** No (dropdown)
- Details:** Object Information (dropdown)
- Libraries to omit:** None (dropdown), with a 'Browse' button and an empty text input field.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

How do you use them?

Example : Ending Authority Collection

```
End Authority Collection (ENDAUTCOL)

Type choices, press Enter.

User profile . . . . . > ROWTON      Name
```

The screenshot displays the IBM Navigator for i interface. On the left, the navigation pane shows the 'Manage Collections' task selected. On the right, the 'End Authority Collection' task is active, and a 'User Information' dialog box is open. The dialog box prompts the user to provide user information for the task, with the 'User name' field containing 'Rowton' and a 'Browse...' button next to it. The 'OK' and 'Cancel' buttons are also visible.

IBM® Navigator for i

Welcome qsecofr

- Welcome
- Dashboard

Search Task

IBM i Management

- Target Systems and Groups
- Favorites
- System
- Monitors
- Basic Operations
- Work Management
- Configuration and Service
- Network
- Integrated Server Administration
- Security
- Users and Groups
 - Users
- Groups
 - Create User
 - Create Group
 - User Properties
- Manage Collections
 - Start Authority Collection
 - End Authority Collection
 - Display Authority Collection
 - Delete Authority Collection

Welcome x Dashboard x End Authority Collection x

User Information

Please provide the user information for your task:

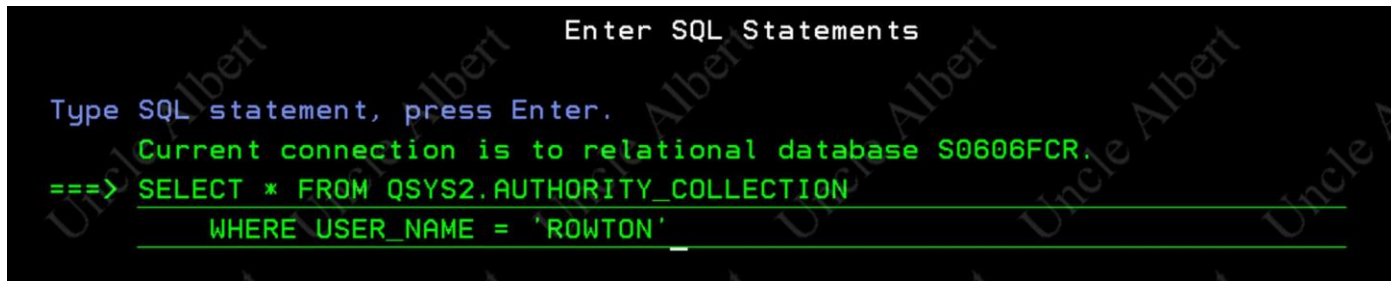
User name: Rowton Browse...

OK Cancel

How do you use them?

Example : Display Authority Collection

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME  
= 'ROWTON'
```

A screenshot of a terminal window with a black background and white text. The title bar at the top reads "Enter SQL Statements". The prompt "Type SQL statement, press Enter." is displayed. Below it, a status message says "Current connection is to relational database S0606FCR." The SQL query "SELECT * FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME = 'ROWTON'" is entered in green text, with a green cursor at the end of the second line.

```
Enter SQL Statements  
Type SQL statement, press Enter.  
Current connection is to relational database S0606FCR.  
===> SELECT * FROM QSYS2.AUTHORITY_COLLECTION  
      WHERE USER_NAME = 'ROWTON'
```

How do you use them?

This is not the best way!

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME  
= 'ROWTON'
```

Display Data

Position to line 3
Data width 2522
Shift to column

AUTHORIZATION_NAME	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBE
ROWTON	2016-12-19-16.14.49.615896	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.616068	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.616310	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.620269	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.616058	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.620193	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.616046	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.616032	WRKOUTQS	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968153	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968107	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968132	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968033	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968266	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.54.968119	RITMON	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.622410	RIT005FM	RITMON	*FILE	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.619940	RIT003	RITMON	*PGM	*SYSBAS	0
ROWTON	2016-12-19-16.14.49.619926	RIT003	RITMON	*PGM	*SYSBAS	0

More . . .

F3=Exit F12=Cancel F19=Left F20=Right F21=Split F22=Width 80

How do you use them?

Example : Display Authority Collection using Nav for i

The screenshot displays the IBM Navigator for i interface. The left-hand pane shows a tree view under 'IBM i Management' with the following items:

- Target Systems and Groups
- Favorites
- System
- Monitors
- Basic Operations
- Work Management
- Configuration and Service
- Network
- Integrated Server Administration
- Security
- Users and Groups
 - Users
 - Groups
 - Create User
 - Create Group
 - User Properties
- Manage Collections
 - Start Authority Collection
 - End Authority Collection
 - Display Authority Collection (highlighted)
 - Delete Authority Collection

The main pane on the right shows a window titled 'Display Authority Collection' with a 'User Information' dialog box. The dialog box contains the following text and controls:

User Information
Please provide the user information for your task:
User name:

How do you use them?

Nav for i is a much easier starting point!

IBM® Navigator for i Welcome qsecofr Target system: 192.168.2.206 Help | Logout

Welcome x Dashboard x Display Authority Collection x Display Authority Collection - Rowton x

Display Authority Collection - Rowton - 192.168.2.206

Actions Search

No filter applied

<input type="checkbox"/>	System Object Name	System Object Library	System Object Type	Required Authority	Current Authority	Authority Source	Adopted Authority Source	Current Adopted Authority	Authority Check Successful	Check Any Authority
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	x
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ	ADOPTED *ALLOBJ	*ALL	x	
<input type="checkbox"/>	Wrkoutqs	RITMON	*FILE	*ALL	*ALL	USER *ALLOBJ	ADOPTED *ALLOBJ	*ALL	x	x
<input type="checkbox"/>	Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	x
<input type="checkbox"/>	Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Ritmon	RITMON	*FILE	*USE	*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Ritmon	RITMON	*FILE	*ALL	*ALL	USER *ALLOBJ			x	x
<input type="checkbox"/>	Rit005fm	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit003	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit003	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit005	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit005	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit002	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit002	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit004	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
<input type="checkbox"/>	Rit004	RITMON	*PGM		*ALL	USER *ALLOBJ			x	

How do you use them?

Export your data for further Analysis

IBM® Navigator for i Welcome qsecofr

Welcome x Dashboard x Display Authority Collection x Display Authority Collection - Rowton x

Display Authority Collection - Rowton - 192.168.2.206

Actions

No filter applied

System Object Name	System Object Library	Object Type	Required Authority	Current Authority	Authority
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Wrkoutqs	RITMON		*ALL	U
<input checked="" type="checkbox"/>	Ritmon	RITMON	*ALL	*ALL	U
<input checked="" type="checkbox"/>	Ritmon	RITMON	*ALL	*ALL	U

Export All to CSV

How do you use them?

Use IBM i Services to review authority collection data

IBM i Service	Type of Service	IBM i 7.4	IBM i 7.3	IBM i 7.2
Security Services				
QSYS2.AUTHORITY_COLLECTION	View		Base	-
QSYS2.AUTHORITY_COLLECTION_DLO	View	Base	-	-
QSYS2.AUTHORITY_COLLECTION_FSOBJ	View	Base	-	-
QSYS2.AUTHORITY_COLLECTION_LIBRARIES	View	Base	-	-
QSYS2.AUTHORITY_COLLECTION_OBJECT	View	Base	-	-
QSYS2.AUTHORIZATION_LIST_INFO	View		SF99703 Level 4	SF99702 Level 16
QSYS2.AUTHORIZATION_LIST_USER_INFO	View		SF99703 Level 4	SF99702 Level 16
QSYS2.DRDA_AUTHENTICATION_ENTRY_INFO	View		Base	SF99702 Level 5
QSYS2.FUNCTION_INFO	View		Base	Base
QSYS2.FUNCTION_USAGE	View		Base	Base

How do you use them?

What information is collected?

User name

Group name

Current authority

Minimum authority required

Source of the current authority

Whether adopted authority was used

Source of adopted authority

Authorisation list name

And much more.....

In Summary

Put simply Authority Collections are a monitoring service that:

Checks what authority you have

Watches what you do

Works out what authority you actually needed

Records the above information

Reports it back to you

How much do they cost?

£0

Enhanced in IBM i 7.4

IBM i 7.4

You can not collect security data based on an object

All user based functions from 7.3 still supported

ProTip:

You can use a combination of user and object to get a better answer

What don't they do?

Authority Collections Services DO NOT do the following:

They do not apply the security changes

You still have to apply the security

They do not summarise the security you need

You get multiple entries per object

They do not clean up after themselves

You have to delete the authority collections

What should you do next?

I recommend you do the following:

Group your entire application into modules

Group your users into a small number of classes

Use Authority Collection Services for one module

Summarise what authority you need for each user class

Create a security schema that represents this authority

Apply this security schema to a module

Repeat for the next module

That sounds like a lot of work!

Summarise what authority you need for each user type

Create a security schema that represents this authority

Apply this security schema to your system

Monitor your system to check for deviations from schema

This can seem a little daunting – it is a lot of work!

**5733ARE Administration Runtime Expert is your friend
It will help you implement and monitor these authorities**

Something to Remember

Authority Collection Services output is to a database file

This means you can integrate, summarise and archive it

A few SQL Examples from IBM website

See all authority information for 'USER1'

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION  
WHERE USER_NAME = 'USER1'
```

View authority info for USER1 for object PAYROLL in library
PAYLIB

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION  
WHERE USER_NAME = 'USER1' AND  
SYSTEM_OBJECT_NAME = 'PAYROLL' AND SYSTEM_OBJECT_SCHEMA  
= 'PAYLIB'
```

Questions?





Thank you