Authority Collection Services

Steve Bradshaw

Technical Director of i-UG (COMMON UK)

Steve.Bradshaw@RowtonIT.com

Authority Collection Services

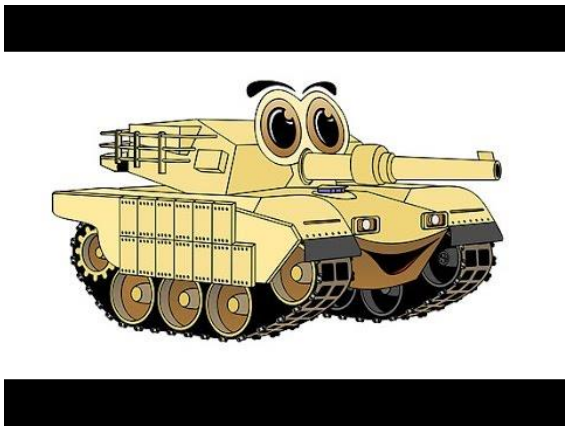
Todays agenda

- 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 Profile	Group Profiles	*ALL OBJ	*AUD IT	SYS CFG	*JOB CTL	*SAV SYS	*SEC ADM	*SER VICE	*SPL CTL	User 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

Graphics by pixabay.com

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

Graphics by pixabay.com

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

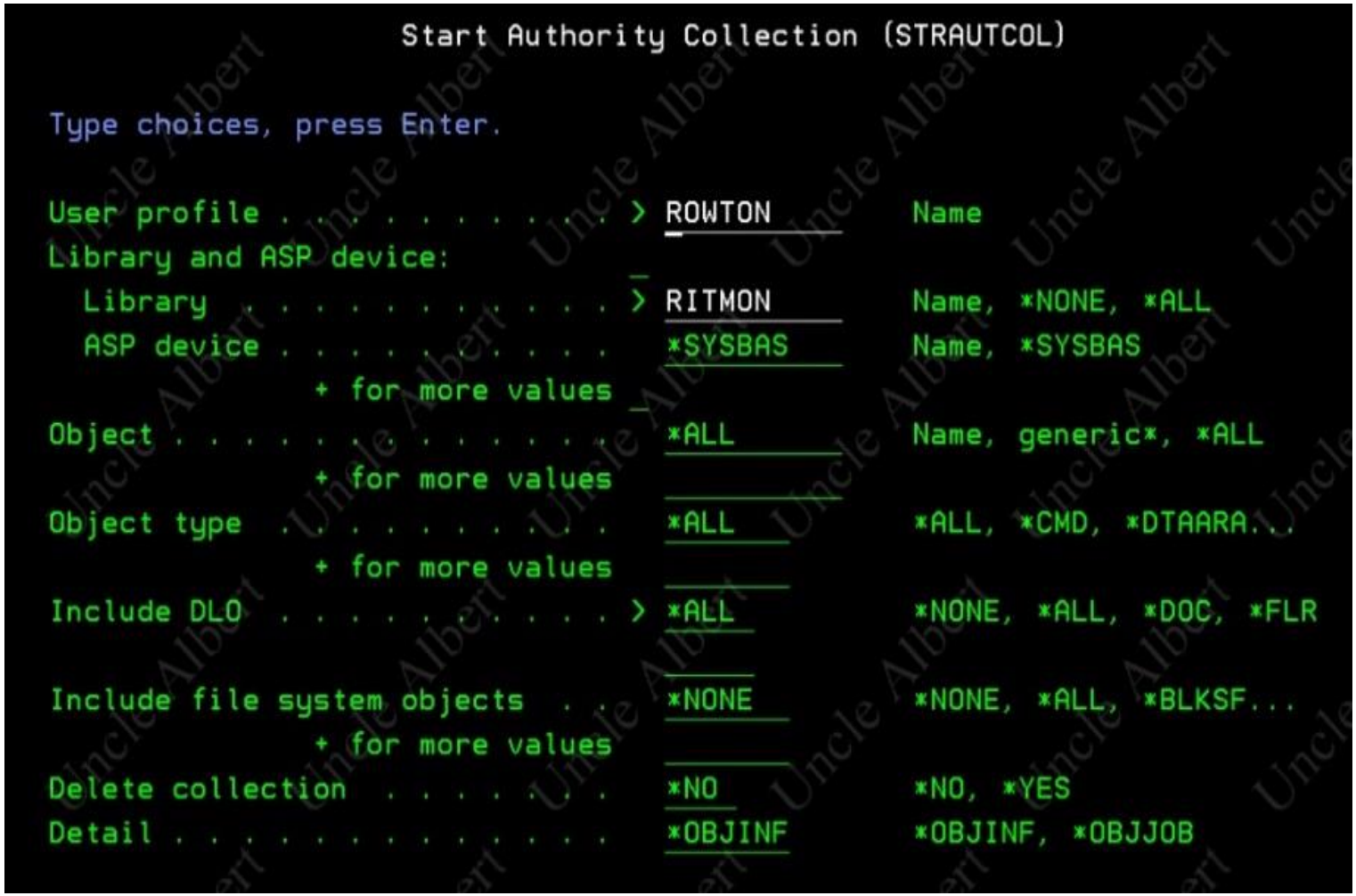
Step 4 – Wait while the user does their job

Step 5 – Analyse the results

Step 6 – Repeat
(Monitor different time, user, application, etc)

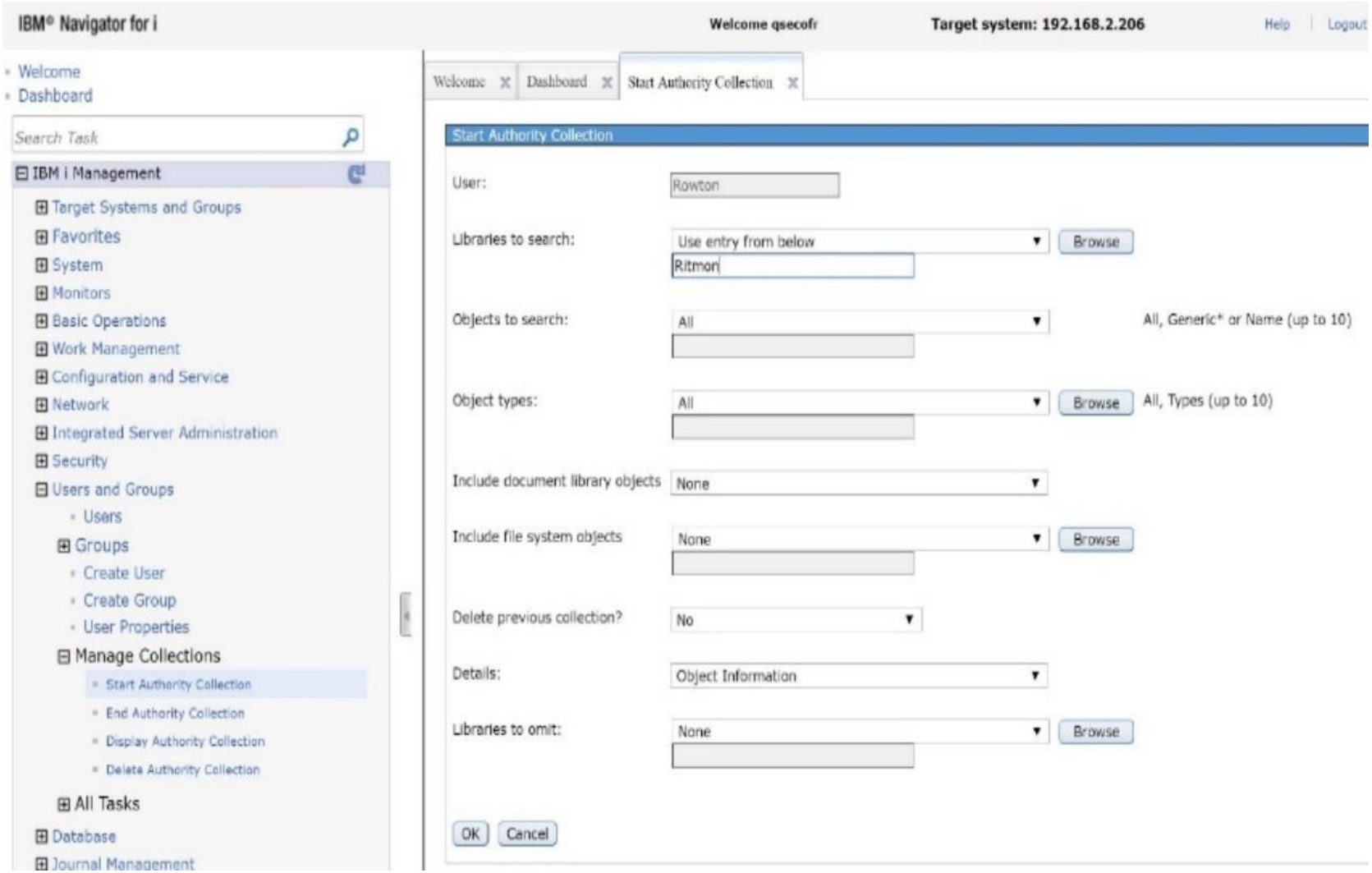
How do you use them?

Example – Starting Authority Collection using 5250



How do you use them?

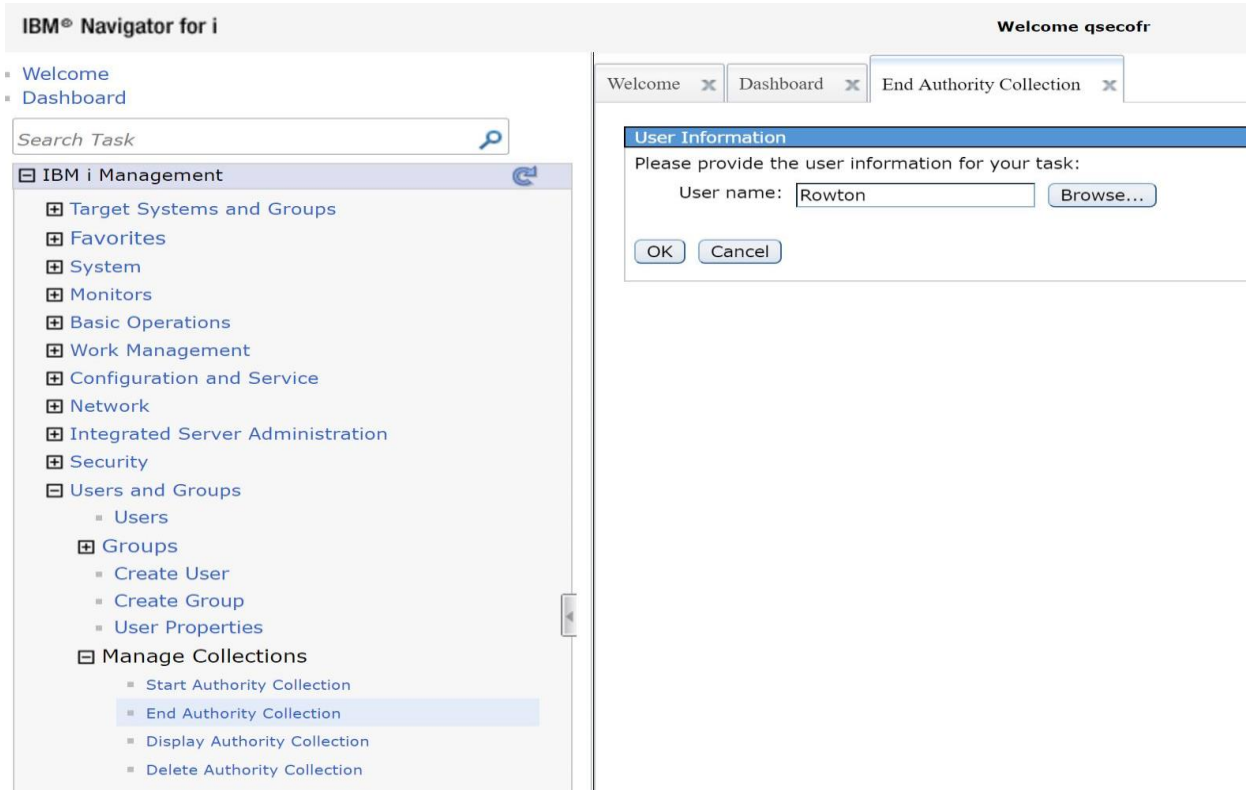
Example: Starting Authority Collection using Nav for i



How do you use them?

Example : Ending Authority Collection

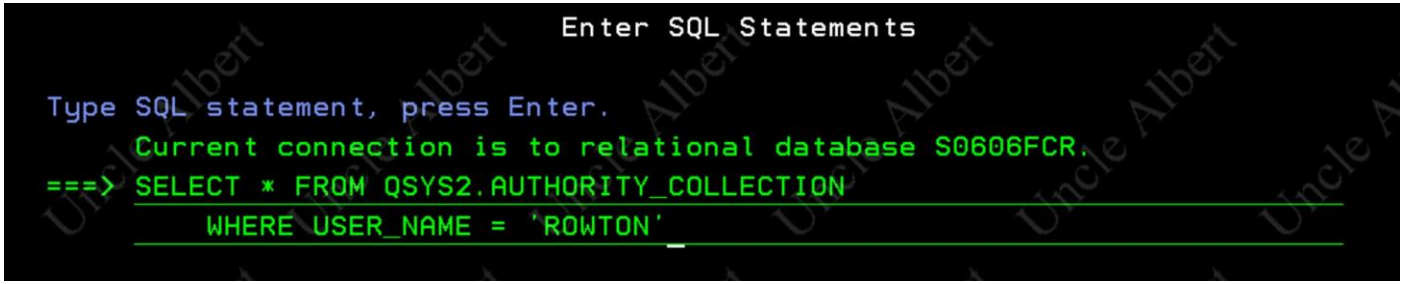
```
                End Authority Collection (ENDAUTCOL)

Type choices, press Enter.

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



How do you use them?

Example : Display Authority Collection

SELECT * FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME = ‘ROWTON’



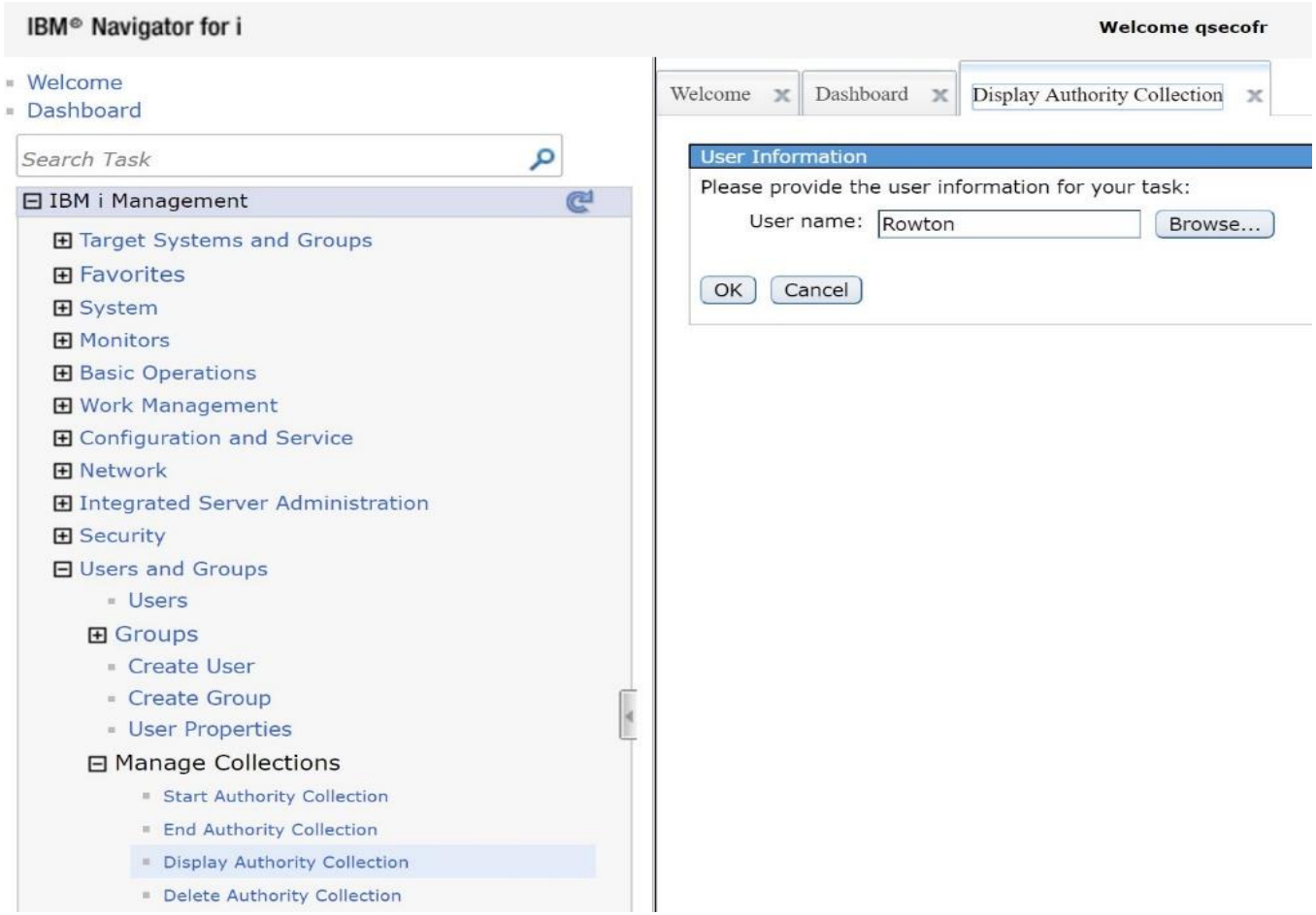
How do you use them?

This is not the best way!

SELECT * FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME = ‘ROWTON’

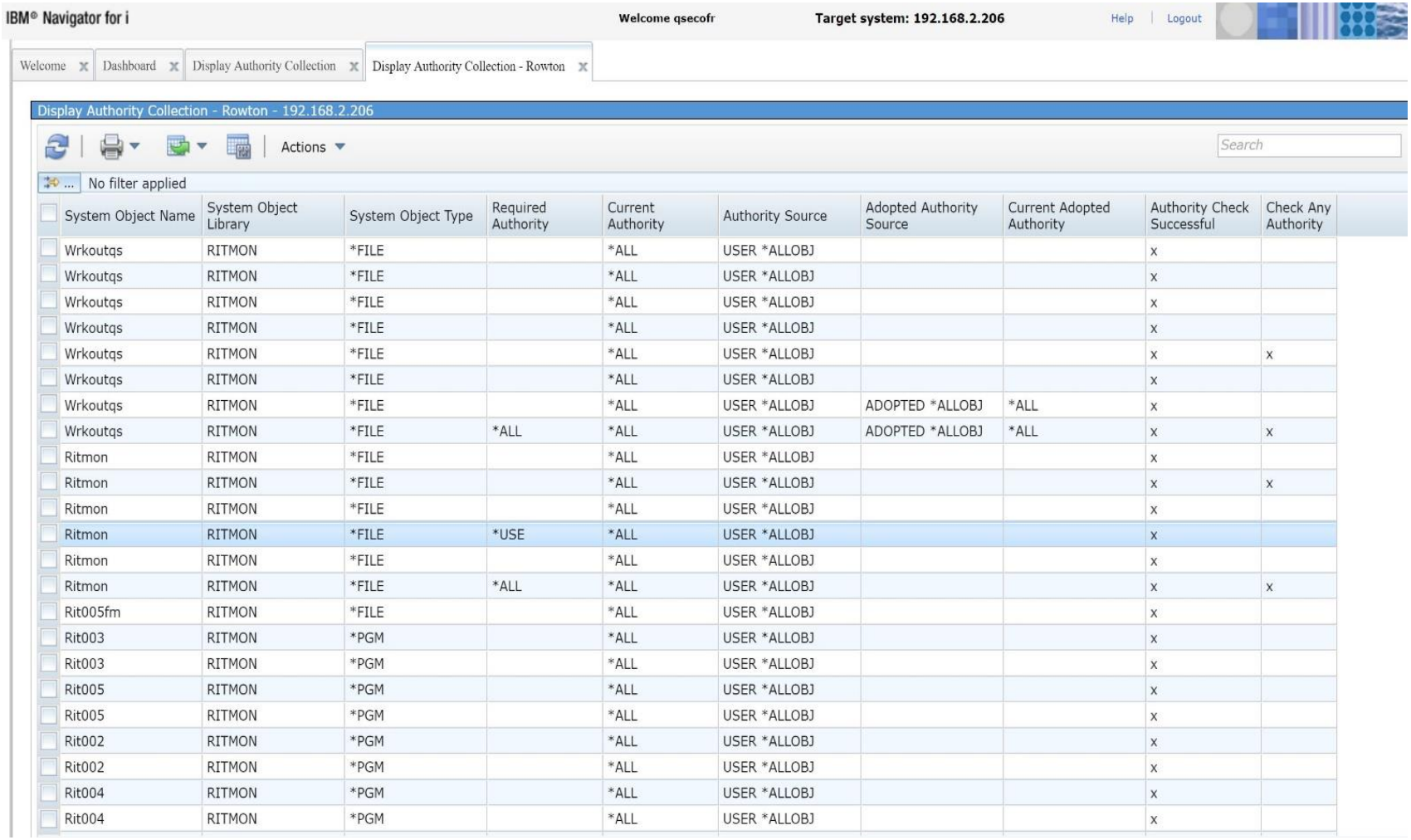
How do you use them?

Example : Display Authority Collection using Nav for i



How do you use them?

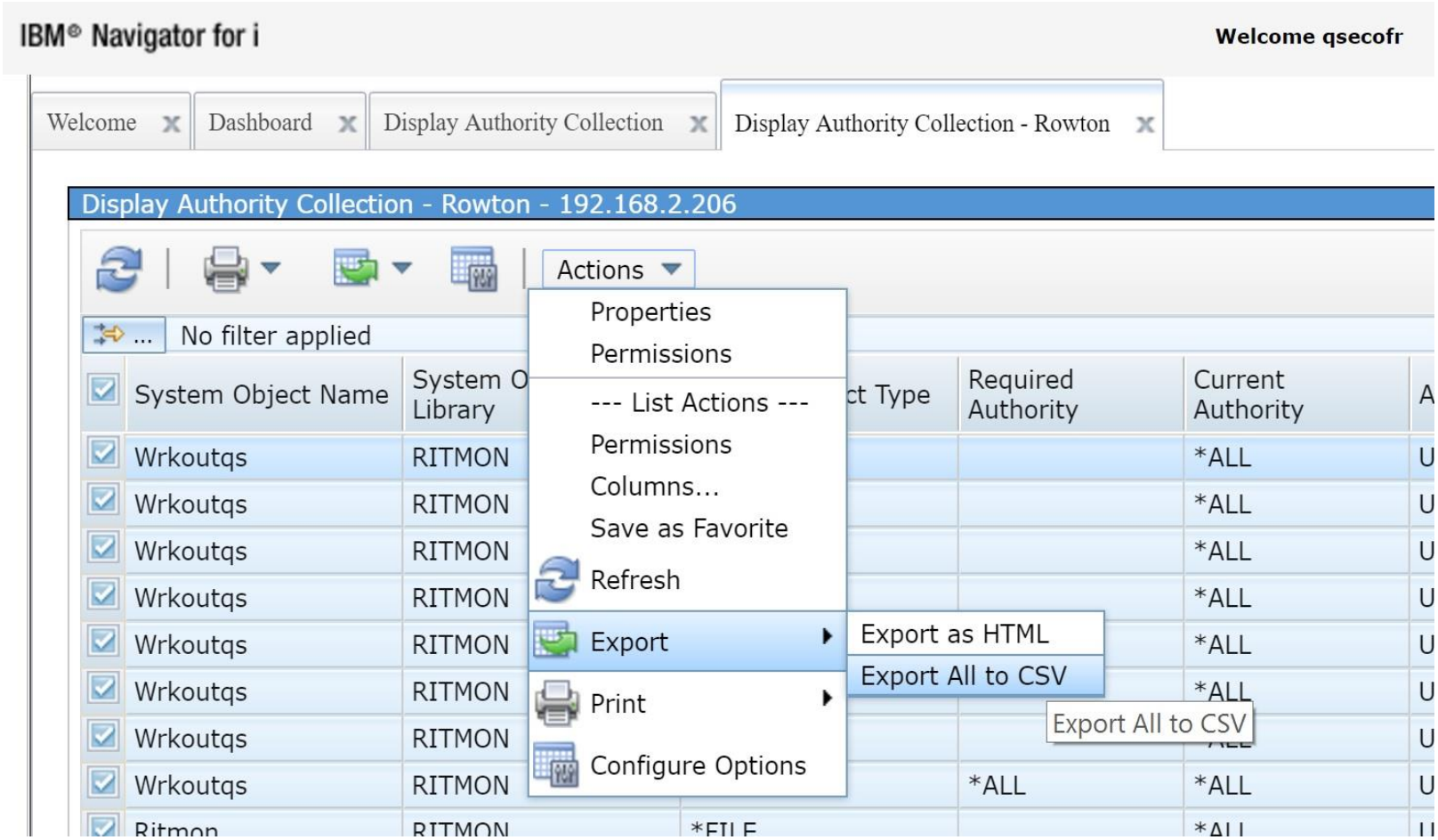
Nav for i is a much easier starting point!



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
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	x
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Wrkoutqs	RITMON	*FILE		*ALL	USER *ALLOBJ	ADOPTED *ALLOBJ	*ALL	x	
Wrkoutqs	RITMON	*FILE	*ALL	*ALL	USER *ALLOBJ	ADOPTED *ALLOBJ	*ALL	x	x
Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	x
Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Ritmon	RITMON	*FILE	*USE	*ALL	USER *ALLOBJ			x	
Ritmon	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Ritmon	RITMON	*FILE	*ALL	*ALL	USER *ALLOBJ			x	x
Rit005fm	RITMON	*FILE		*ALL	USER *ALLOBJ			x	
Rit003	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit003	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit005	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit005	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit002	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit002	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit004	RITMON	*PGM		*ALL	USER *ALLOBJ			x	
Rit004	RITMON	*PGM		*ALL	USER *ALLOBJ			x	

How do you use them?

Export your data for further Analysis



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?

- Image source blog.rankdone.com

Thank you