IBM i

Protect Your IBM i Objects and Data with Authority Collection

Thomas Barlen
Senior Managing Consultant – IBM Power System Security
IBM Technology Expert Labs

19th November 2024

IBM

Agenda

- Situation today
- Introduction to IBM i Authority Collection
- Practical examples

Agenda

- Situation today
- Introduction to IBM i Authority Collection
- Practical examples

Situation Today

- Customers run many applications on a single partition
  - No detailed knowledge of the applications… where is the data?
    - Data in DB2 or IFS … but where?
  - Once found, how do you lock down security without application breakage?
    - What is the “minimum” authority level that can be granted for the end user?
  - Many customers have little to no idea what interfaces an application uses so the authority requirements cannot be determined
  - Applications are shipped with excessive public authority (common problem) which leads to security exposures, such as **data theft** or data encryption via **Ransomware**

- The problem: customers don’t change permission settings leaving data exposed

Agenda

- Situation today
- Introduction to IBM i Authority Collection
- Practical examples

IBM i Authority Collection

- Initially introduced with IBM i V7.3
- Utility that captures pertinent data associated with an authority check
  - Included as part of the base IBM i OS
  - The collection covers all native IBM i file systems
  - Focus on capturing only unique instances of the authority check
  - Run-time performance, while the collection is active, will degrade 2-3%
  - Storage consideration for long running authority collection

- The collection includes key pieces of information… (including)

What authority is required for this authority check

Implementation

- The Authority collection is “user” based in the 7.3 release
  - Turn on the authority collection for a given user(s)
  - Collect authority information for the user
    - Cannot collect information on the group level but object access allowed via a group profile authority is collected
    - Adopted authority information collected
- Authority collection can be enabled on an object basis
  - Collect information for a given object
  - New attribute on every object specifies whether authority collection is enabled

7.3

7.4

```
                    Display Object Description - Full
_                                                          Library 1 of 1
 Object . . . . . :   BARLEN          Attribute . . . . . :   PROD
   Library  . . . . :     QSYS        Owner . . . . . . . :   BARLEN
 Library ASP device . :   *SYSBAS     Library ASP group . :   *SYSBAS
 Type . . . . . :   *LIB              Primary group . . . :   *NONE
   Authority collection value . . . . . :   *OBJINF
```

Running the collection – Start collection for user(s)

- Collection is started with the Start Authority Collection (STRAUTCOL) command

```
                    Start Authority Collection (STRAUTCOL)
Type choices, press Enter.
Type of authority collection . . > *USRPRF       *USRPRF, *OBJAUTCOL
User profile . . . . . . . . . . > BARLENT       Name
Library and ASP device:
  Library  . . . . . . . . . . . > PAYROLLO      Name, *NONE, *ALL
  ASP device . . . . . . . . . .   *SYSBAS       Name, *SYSBAS

  Library  . . . . . . . . . . . > PAYROLLD      Name
  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  . . . . . . . . . .   *NONE         *NONE, *ALL, *DOC, *FLR
Include file system objects  . .   *NONE         *NONE, *ALL, *BLKSF...
Delete collection  . . . . . . .   *NO           *NO, *YES
Detail . . . . . . . . . . . . .   *OBJINF       *OBJINF, *OBJJOB
```

Running the collection – Start collection for object(s)

- Authority collection for objects need to be started differently
  - First define the objects you want to collect authority information for

7.4+

```
                        Change Authority Collection (CHGAUTCOL)
Type choices, press Enter.
Object . . . . . . . . . . . . . . > '/qsys.lib/barlen.lib/*'

Authority collection value . . . > *OBJINF        *NONE, *OBJINF
Include dependent objects  . . . > *LF            *NO, *LF
Directory subtree  . . . . . . . .  *NONE         *NONE, *ALL
Symbolic link  . . . . . . . . . .  *NO           *NO, *YES
Delete collection  . . . . . . . .  *NO           *NO, *YES
```

  - Next start the collection

```
                      Start Authority Collection (STRAUTCOL)
Type choices, press Enter.

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

Running the collection - Stop

- Collection is ended with the End Authority Collection (ENDAUTCOL) command
  - Ending user-based collection:

```
                End Authority Collection (ENDAUTCOL)

Type choices, press Enter.
 Type of authority collection . .   *USRPRF      *USRPRF, *OBJAUTCOL
User profile . . . . . . . . . .   BARLENT       Name
```

  - Ending object-based collection:

```
                End Authority Collection (ENDAUTCOL)

Type choices, press Enter.
Type of authority collection . .   *OBJAUTCOL    *USRPRF, *OBJAUTCOL
```

Determine list of objects with enabled collection

7.4+

- It is not obvious which objects have turned on the authority collection attribute
- The following SQL statement can be used to list all object where the authority collection value has been set to *OBJINF
  - Note → this command can take a while to complete
    - It is better to remember what you have activated

QSYS

```
SELECT * FROM TABLE (QSYS2.OBJECT_STATISTICS('*ALLUSR ','*ALL') ) AS X
WHERE AUTHORITY_COLLECTION_VALUE = '*OBJINF'
```

OBJNAME	OBJTYPE	OBJOWNER	OBJDEFINER	OBJCREATED
STARTSYSBK	*PGM	BARLEN	BARLEN	2024-09-29-07.12.24.000000
STARTSYSL	*PGM	BARLEN	THOMAS2	2024-10-23-10.32.38.000000
SYSLOG1	*PGM	BARLEN	BARLEN	2024-08-09-11.53.48.000000
SYSLOG2	*PGM	BARLEN	BARLEN	2024-08-09-11.56.02.000000
SYSLOG3	*PGM	THOMAS2	THOMAS2	2024-11-02-11.19.13.000000
SYSLOG3S	*PGM	BARLEN	BARLEN	2024-04-26-10.50.24.000000

Determine list of objects with enabled collection

7.4+

- The following command and SQL statement can be used to list all object where the authority collection value has been set to *OBJINF for a given IFS directory

IFS

```
RTVDIRINF DIR(/) OMIT('/QSYS.LIB')
```

This will produce a QAEZDxxxxO file

- List the objects with the authority collection value set to *OBJINF

```
SELECT QEZOBJNAM, QEZOBJTYPE, QEZAUTCOL FROM QUSRSYS.QAEZDxxxxO
  WHERE QEZAUTCOL = '*OBJINF'
```

Check for active authority collections for users

- The following command and SQL statement can be used to check the status of user-based authority collections

```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
  QSYS2.USER_INFO
```

```
AUTHORIZATION_NAME  AUTHORITY_COLLECTION
                    _ACTIVE
    SECHARD                 NO
    SLOPR                   NO
    SSHGRP                  NO
    SYSLOG                  NO
    TBARLEN                 YES
    THOMAS                  NO
    THOMAS2FA               YES
```

- Just checking for active collections

```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
QSYS2.USER_INFO WHERE AUTHORITY_COLLECTION_ACTIVE='YES'
```

Check for existing user collection repositories

- The following command and SQL statement can be used to check the existence of user-based authority collection repositories

```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
QSYS2.USER_INFO WHERE AUTHORITY_COLLECTION_REPOSITORY_EXISTS='YES'
```

```
AUTHORIZATION_NAME  AUTHORITY_COLLECTION
                    _ACTIVE
    BARLEN                  NO
    THOMAS2FA               YES
```

Check for active authority collections for objects

7.4+

- The Display Security Attributes (DSPSECA) command can be used to check if object-based authority collection has been started on the system

```
                        Display Security Attributes
                                                          System:   SQ740
User ID number . . . . . . . . . . . . . . . :   716249
Group ID number  . . . . . . . . . . . . . . :   132655
Security level . . . . . . . . . . . . . . . :   50
Password level . . . . . . . . . . . . . . . :   0
Allow change of security related system
  values . . . . . . . . . . . . . . . . . . :   *NO
Allow add of digital certificates  . . . . . :   *YES
Allow service tools user ID with default
  and expired password to change its own
  password . . . . . . . . . . . . . . . . . :   *NO
Authority collection for objects active  . . :   *YES
```

Captured data analysis

- Collected data is stored in collections
  - The collected information contains the following:
    - Object name, Library name, ASP device, Object type
    - SQL name, SQL object type, SQL schema name
    - Path name and object name
    - Authorization list for the object
    - **Required authority**
    - **Current authority**
    - Authority source for the user that satisfies the authority request
    - Adopted authority indicator (adopt was used to satisfy the authority request), Current adopted authority, Adopted authority source, Adopting program name and indicator (adopting program that was used to satisfy the authority request), Adopting program library, Adopting program object type (*PGM or *SRVPGM), Adopting program owner
    - Stack info (most recent invocation and most recent user state invocation including procedure name and statement)
    - Job name, Job user, Job number
      - Current job user profile
      - Group profile and indicator (group profile that was used to satisfy the authority request)
  - Date and time of authority check

Captured data analysis (cont'd)

- Example of a query output for a user collection

```
SELECT AUTHORIZATION_NAME,OBJECT_NAME,SYSTEM_OBJECT_TYPE,
DETAILED_REQUIRED_AUTHORITY,
DETAILED_CURRENT_AUTHORITY,AUTHORITY_SOURCE
FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME = 'BARLENT'
```

```
AUTHORIZATION OBJECT_NAME SYSTEM_ DETAILED_REQUIRED_AUTHORITY    AUTHORITY_SOURCE
_NAME                     OBJECT_TYPE


    BARLENT   SALES         *FILE *OBJOPR                        USER PRIVATE
    BARLENT   SALES         *FILE *OBJOPR *READ                  USER PRIVATE
    BARLENT   SALESPGM      *PGM  *OBJOPR *READ *EXECUTE         PUBLIC
    BARLENT   SALESPGM      *PGM  *OBJOPR                        PUBLIC
```

Captured data analysis (cont'd)

7.4+

- Example of a query for an object collection
  - See who performed changes on file SALARIES in library PAYROLL

```
WITH emp_activity (username, cur_auth, req_auth) AS (
        SELECT "CURRENT_USER",
               detailed_current_authority,
               detailed_required_authority
            FROM qsys2.authority_collection_object as aco
            WHERE system_object_schema = 'PAYROLL'
                  AND system_object_name = 'SALARIES'
                  AND adopting_program_owner IS NULL
    )
    SELECT *
        FROM emp_activity
        WHERE req_auth LIKE '%UPD%'
              OR req_auth LIKE '%DLT%'
              OR req_auth LIKE '%ADD%';
```

Captured data analysis (cont'd)

7.4+

- Following collection objects are available when using object-based authority collections
  - AUTHORITY_COLLECTION_OBJECT
    View to look at information that was collected for libraries and objects in libraries during authority collection for objects.
  - AUTHORITY_COLLECTION_LIBRARIES
    View to look at information that was collected for all libraries and objects in libraries during authority collection for objects.
    - QSYS2.AUTHORITY_COLLECTION_OBJECT and QSYS2.AUTHORITY_COLLECTION_LIBRARIES return the same results
    - QSYS2.AUTHORITY_COLLECTION_OBJECT will perform better when the number of entries in the authority collection is large and you are looking for a specific object
    - QSYS2.AUTHORITY_COLLECTION_LIBRARIES will perform better when the number of entries in the authority collection is small or you are looking for all or most objects in the authority collection

Captured data analysis (cont'd)

7.4+

- AUTHORITY_COLLECTION_FSOBJ
  View to look at information that was collected for all file system objects in the "root" (/), QOpenSys, and user-defined file systems
- AUTHORITY_COLLECTION_DLO
  View to look at information that was collected for document library objects (DLO)

Deleting the collection

7.4+

- The authority collection can be deleted with the Delete Authority Collection (DLTAUTCOL) command
  - Deleting user-based collection:

```
                Delete Authority Collection (DLTAUTCOL)

Type choices, press Enter.
Type of authority collection . .   *USRPRF        *USRPRF, *OBJ
User profile . . . . . . . . . .   BARLENT        Name
```

  - Deleting object-based collection:

```
                Delete Authority Collection (DLTAUTCOL)

Type choices, press Enter.
Type of authority collection . .   *OBJ          *USRPRF, *OBJ
                                   *ALL
```

Agenda

- Situation today
- Introduction to IBM i Authority Collection
- Practical examples

Recommended authority collection process

- A typical approach to collect, analyze, and change object permissions is:

1. Define list of objects and set authority collection value to *OBJINF
2. Define application use cases
3. Start authority collection
4. Run all use cases to capture access attempts of all application functions
5. Stop authority collection
6. Analyze collected data, create groups/authorization lists, assign required permissions to groups, assign authorization lists to objects, remove previous permissions from objects (most likely public permissions)
7. Delete authority collection
8. Set authority collection value from *OBJINF to *NONE

Collected Data

Untitled* - Run SQL Scripts - I5osp4(I5osp4)

File Edit View Run VisualExplain Monitor Options Connection Tools Help

```
1 SELECT object_name, system_object_type,
2        authorization_name,
3        detailed_current_authority,
4        detailed_required_authority,
5        authority_source
6     FROM qsys2.authority_collection_object
7     WHERE system_object_schema = 'QZRDSYSLOG' order by object_name,authorization_name;
```

OBJECT_NAME	SYSTEM_OBJECT_TYPE	AUTHORIZATION_NAME	DETAILED_CURRENT_AUTHORITY	DETAILED_REQUIRED_AUTHORITY	AUTHORITY_SOURCE
AUDCFG	*FILE	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDCFG	*FILE	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
AUDLASTART	*DTAARA	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
AUDLASTART	*DTAARA	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
AUDLASTART	*DTAARA	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CFGJSCR	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGJSGLB	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGJSGLBD	*FILE	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CFGJSGLBP	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLENV	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
CFGSLENV	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLENVP	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLHST	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLHSTD	*FILE	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CFGSLHSTP	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*READ	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *ADD *DLT *UPD	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJMGT	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD	USER *ALLOBJ
CFGSLMQM	*CMD	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ
CFGSLMQMP	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSRM	*CMD	BARLEN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSRMP	*PGM	BARLEN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR *READ *EXECUTE	USER *ALLOBJ
CFGSRMP	*PGM	BARLEN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
CHKCNN	*PGM	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*EXECUTE	USER *ALLOBJ
CHKCNN	*PGM	QZRDSLOWN	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*OBJOPR	USER *ALLOBJ
CHKJOBSTS	*PGM	BARLEN	*OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	*EXECUTE	USER *ALLOBJ

Determining the right authority requirements

- From your authority collection get the required authority by object
- Example SQL:

```
SELECT AUTHORIZATION_NAME,
CAST(OBJECT_NAME AS VARCHAR(10)) as Object,
DETAILED_REQUIRED_AUTHORITY,
AUTHORITY_SOURCE, GROUP_NAME FROM QSYS2.AUTHORITY_COLLECTION_OBJECT
WHERE object_schema = 'PAYROLL' ORDER BY AUTHORIZATION_NAME,DETAILED_REQUIRED_AUTHORITY
```


```
SELECT AUTHORIZATION_NAME,
CAST(OBJECT_NAME AS VARCHAR(10)) as Object,
DETAILED_REQUIRED_AUTHORITY,
AUTHORITY_SOURCE, GROUP_NAME FROM QSYS2.AUTHORITY_COLLECTION_OBJECT
WHERE object_schema = 'PAYROLL' ORDER BY AUTHORIZATION_NAME,DETAILED_REQUIRED_AUTHORITY
```


AUTHORIZATION_NAME	OBJECT	DETAILED_REQUIRED_AUTHORITY	AUTHORITY_SOURCE	GROUP_NAME
BARLEN	EMPLOYEES	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ	-
BARLEN	SALARIES	*OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	USER *ALLOBJ	-
BARLEN	SALARIES	*OBJMGT *OBJOPR *READ *EXECUTE	USER *ALLOBJ	-
BARLEN	SALARIES	*OBJMGT *OBJOPR *READ *EXECUTE	USER *ALLOBJ	-
BARLEN	EMPLOYEES	*READ *ADD *DLT *UPD	USER *ALLOBJ	-
BARLEN	SALARIES	*READ *ADD *DLT *UPD	USER *ALLOBJ	-
THOMAS	SALARIES	*ADD	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OBJOPR	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*OWNER *OBJEXIST *OBJMGT *OBJALTER *OBJREF *OBJOPR *READ *ADD *DLT *UPD *EXECUTE	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*READ	GROUP PRIVATE	SSHGRP
THOMAS	SALARIES	*READ *UPD	GROUP PRIVATE	SSHGRP

Deciding what permission model to implement

- If required permission is *CHANGE or *ALL only for the business application, recommended to run application under adopted authorities
- If users have *CHANGE or *ALL but only need *USE, change the permission on the object
  - Recommended to use authorization lists with group profiles to assign required authority
- Generally do not grant more than what the maximum required authority is
- Pay special attention to remote access, i.e. ODBC, and external interfaces, such as data exchange, data import/export, etc.

Take-aways

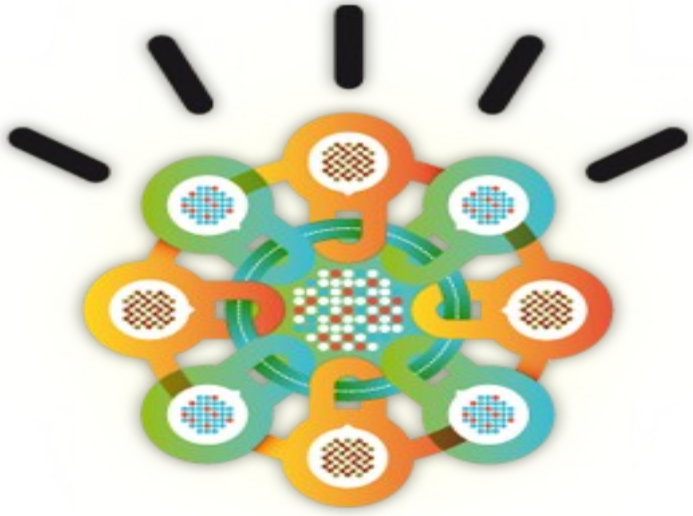
- Authority Collection is a great feature to better protect your application data and objects without breaking the functionality of the application
- Authority Collection is most useful with IBM i 7.4
- Authority Collection provides the information to implement access control on the least privilege principle
- Always consider the combination of available security features, such as adopted authorities, profile swapping, group profiles (role-based access), authorization lists

Thanks for your attention

Questions ?

Thomas Barlen
barlen@de.ibm.com
Senior Managing Consultant
IBM Power System Security
IBM Technology Expert Labs

IBM Technology Expert Labs Can Help!



- IBM Technology Expert Labs can offer consulting and security services:
  - IBM i, AIX, and Linux Security Assessment
  - IBM i Network Encryption (TLS)
  - IBM i Single Sign On Setup
  - IBM i Cryptography
  - AIX RBAC and Trusted Execution Services
  - IBM PowerSC Implementation Services
  - AIX and Linux LDAP Integration Services
- IBM Technology Expert also has several security tools:
  - IBM i Privilege Elevation (Firecall)
  - IBM i Password Validation and Password Sync
  - IBM i Advanced Authentication (2FA – RFC 6238)
  - IBM i Compliance and Reporting Tool with Event Monitoring
  - IBM i Certificate Expiration Manager
  - IBM i Syslog Reporting Manager
  - IBM i Software Firewall (Exit Point Tool)
  - And many more security related tools
- Visit ibm.biz/IBMiSecurity
- to learn more about all of these offerings!

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.