Université IBM i

7 novembre 2023

IBM Innovation Studio Paris

S23 – Administration moderne de la sécurité IBM i avec les services SQL

16:00 / 17:00

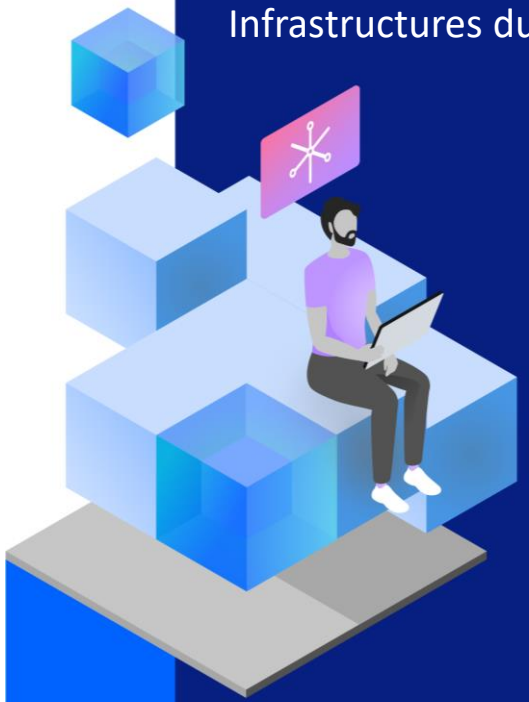
Dominique GAYTE
i.gayte.it
dominique@gayte.it

infrasdufutur

#ibmi
#uii2023
#infrastructuredufuturIBM23

IBM

Infrastructures du futur

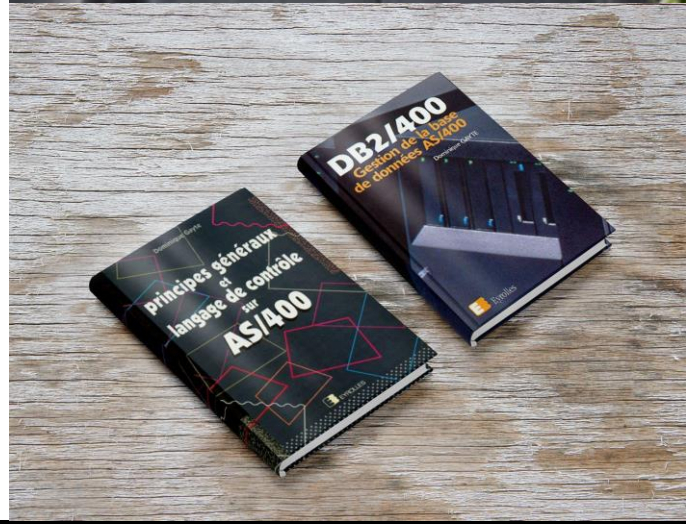


7 et 8 novembre 2023

Dominique GAYTE

I.GAYTE.IT
IBM i Security Softwares & Services

- Intervenant « AS/400 » depuis 1990
- Sécurité
  - Audit
  - Formation
  - Mise en œuvre : SSO, SSL, sécurisation de la BD, RGPD…
- Développements complexes
  - Sécurité : Points d'exit (Power.exit), AD-iCT
  - API système
  - RPG IV : XML, Accès bases de données distantes
- Auteur des livres ci-contre



Dominique GAYTE - suite

- Evènement Sécurité IBM i
  - https://i.gayte.it/category/securiti/
  - https://www.youtube.com/@igayteit

Securit.i
Événement Sécurité IBM i

- Distingué par IBM comme IBM Champion 2023
- Décerné aux experts reconnus par IBM

SQL services for Security

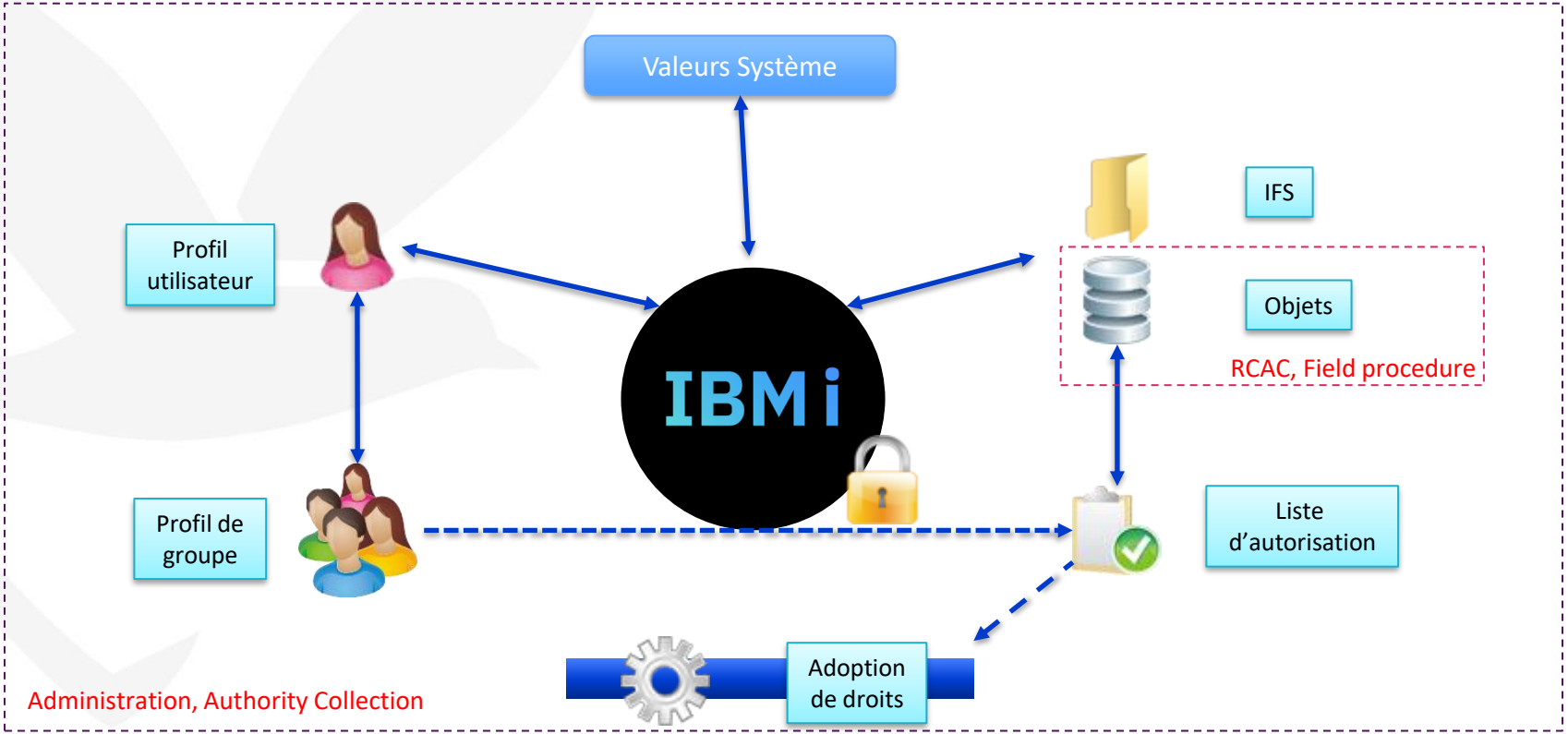
- Depuis la V5R4, dépendent de la version de l'IBM i
- https://www.ibm.com/support/pages/node/1119123

Security Services					
QSYS2.AUTHORITY_COLLECTION	View	Base	Base	Base	Not Supported
QSYS2.AUTHORITY_COLLECTION_DLO	View	Base	Base	Not Supported	Not Supported
QSYS2.AUTHORITY_COLLECTION_FSOBJ	View	Base	Base	Not Supported	Not Supported
QSYS2.AUTHORITY_COLLECTION_LIBRARIES	View	Base	Base	Not Supported	Not Supported
QSYS2.AUTHORITY_COLLECTION_OBJECT	View	Base	Base	Not Supported	Not Supported
QSYS2.AUTHORIZATION_LIST_INFO	View	Base	Base	SF99703 Level 4	SF99702 Level 16
QSYS2.AUTHORIZATION_LIST_USER_INFO	View	Base	Base	SF99703 Level 4	SF99702 Level 16
QSYS2.CERTIFICATE_INFO()	Table function	Base	SF99704 Level 7 Enhanced: SF99704 Level 13	SF99703 Level 18 Enhanced: SF99703 Level 24	Not Supported
QSYS2.CHECK_PASSWORD()	Table function	Base	Not Supported	Not Supported	Not Supported

Droits

- Il faut disposer des droits nécessaires pour exécuter les requêtes
- Dépend de l'objet (vue, table, fonction) et des colonnes sollicitées
- La Sécurité est bien préservée en utilisant SQL par rapport aux commandes de l'OS

Organisation de base de la Sécurité



IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Valeurs système

Vue SYSTEM_VALUE_INFO

- Informations sur les valeurs système
- Quelques nouveautés annoncées récemment
  - DB2 for IBM i - IBM i 7.5 SF99950 Level 5 ou IBM i 7.4 SF99704 Level 26
  - Colonnes supplémentaires : TEXT_DESCRIPTION, CATEGORY, CHANGEABLE, and SHIPPED_DEFAULT_VALUE

```
SELECT *      FROM QSYS2.SYSTEM_VALUE_INFO;

SELECT *      FROM QSYS2.SYSTEM_VALUE_INFO
    WHERE SYSTEM_VALUE <> SHIPPED_DEFAULT_VALUE;
```

Vue SECURITY_INFO

- Toutes les valeurs systèmes relatives à la Sécurité
- Une seule ligne est renvoyée

```
SELECT * FROM QSYS2.SECURITY_INFO;
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Profils utilisateur

Profils utilisateur

- Vue QSYS2.USER_INFO
- Vue QSYS2.USER_INFO_BASIC
  - Meilleures performances
  - Pas en V7R2

Mot de passe par défaut

- Les mots de passe par défaut sont identiques au profil
- USER_DEFAULT_PASSWORD = 'YES'
- Il ne devrait pas y en avoir !

```
SELECT AUTHORIZATION_NAME, USER_DEFAULT_PASSWORD
    FROM qsys2.USER_INFO_BASIC
    WHERE USER_DEFAULT_PASSWORD = 'YES';
```

Niveau de mot de passe

- Vérification du niveau de mot de passe
- Indispensable pour préparer le passage de la valeur système QPWDLVL
  - 0 ou 1 => 2 ou 3
  - 2 ou 3 => 4 (V7R5)
- Colonnes
  - PASSWORD_LEVEL_0_1
  - PASSWORD_LEVEL_2_3
  - PASSWORD_LEVEL_4 (V7R5)

```
SELECT AUTHORIZATION_NAME, PASSWORD_LEVEL_0_1,
PASSWORD_LEVEL_2_3, NO_PASSWORD_INDICATOR
    FROM QSYS2.USER_INFO;
```

Droits spéciaux

- Colonne SPECIAL_AUTHORITIES
- Liste de 8 droits maximum (VARCHAR(88))
  - 10 caractères
  - Un espace

```
-- Droits spéciaux de tous les profils
SELECT AUTHORIZATION_NAME, SPECIAL_AUTHORITIES, STATUS
    FROM QSYS2.USER_INFO;
--Liste des profils *ALLOBJ
SELECT AUTHORIZATION_NAME, SPECIAL_AUTHORITIES, STATUS
    FROM QSYS2.USER_INFO
    WHERE SPECIAL_AUTHORITIES LIKE '*ALLOBJ%';
```

Profils de groupe

- Vue QSYS2.GROUP_PROFILE_ENTRIES
- Contient la liste de tous les profils qui appartiennent à un groupe

Table 1. GROUP_PROFILE_ENTRIES view

Column Name	System Column Name	Data Type	Description
GROUP_PROFILE_NAME	GROUPNAME	VARCHAR(128)	Group profile name
USER_PROFILE_NAME	USERNAME	VARCHAR(128)	User profile name
USER_TEXT	USER_TEXT	VARCHAR(50) Nullable	User profile text description.

- Pour voir si le profil est *ALLOBJ par son groupe…

QSYS2.GROUP_PROFILE_ENTRIES

- Exemples

```
--Liste des profils qui appartiennent à un groupe
SELECT USER_PROFILE_NAME,
       GROUP_PROFILE_NAME
    FROM QSYS2.GROUP_PROFILE_ENTRIES;
--Liste des profils de groupe
SELECT GROUP_PROFILE_NAME
    FROM QSYS2.GROUP_PROFILE_ENTRIES
    GROUP BY GROUP_PROFILE_NAME;
```

QSYS2.GROUP_PROFILE_ENTRIES (2)

- Groupes *ALLOBJ

```
--Liste des groupes *ALLOBJ
--Avec Common Table Expression (CTE)
WITH Groupes (Groupe) as (SELECT GROUP_PROFILE_NAME
    FROM QSYS2.GROUP_PROFILE_ENTRIES
    GROUP BY GROUP_PROFILE_NAME)
SELECT P.AUTHORIZATION_NAME,
       P.SPECIAL_AUTHORITIES
    FROM Groupes G INNER JOIN QSYS2.USER_INFO P
    ON G.Groupe = P.AUTHORIZATION_NAME
    WHERE P.SPECIAL_AUTHORITIES LIKE '*ALLOBJ%';
```

QSYS2.GROUP_PROFILE_ENTRIES (3)

- Liste de tous les profils qui héritent de *ALLOBJ par le groupe

```
WITH Groupes (Groupe) AS ( SELECT GROUP_PROFILE_NAME
             FROM QSYS2.GROUP_PROFILE_ENTRIES
             GROUP BY GROUP_PROFILE_NAME ),
     GroupesALLOBJ (GroupeAll) AS (SELECT P.AUTHORIZATION_NAME
             FROM Groupes G INNER JOIN QSYS2.USER_INFO P
                      ON G.Groupe = P.AUTHORIZATION_NAME
             WHERE P.SPECIAL_AUTHORITIES LIKE '*ALLOBJ%' )
SELECT USER_PROFILE_NAME, GROUP_PROFILE_NAME
        FROM QSYS2.GROUP_PROFILE_ENTRIES
        WHERE GROUP_PROFILE_NAME IN (
              SELECT GroupeAll FROM GroupesALLOBJ);
```

Autre exemple sur les groupes

- *Authors: Carol Woodbury & Scott Forstie*

```
SELECT user_name, special_authorities, group_profile_name,
       supplemental_group_list, text_description
    FROM QSYS2.USER_INFO
    WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'
         OR AUTHORIZATION_NAME IN (SELECT USER_PROFILE_NAME
          FROM QSYS2.GROUP_PROFILE_ENTRIES
          WHERE GROUP_PROFILE_NAME IN (SELECT AUTHORIZATION_NAME
                 FROM QSYS2.USER_INFO
                 WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'))
    ORDER BY AUTHORIZATION_NAME;
```

Et encore…

- Profils désactivés
  - STATUS
- Profils inutilisés depuis x jours
  - LAST_USED_TIMESTAMP et PREVIOUS_SIGNON
- Possibilités restreintes
  - LIMIT_CAPABILITIES (*YES, *NO)
- Créateur du profil (pour identifier les profils « systèmes »)
  - USER_CREATOR : *IBM (ou QSYS) pour les profils standards
- Profils désactivés dans NetServer
  - NETSERVER_DISABLED (YES, NO)
- …

Question ?

Modification d'un profil

- SYSTOOLS.CHANGE_USER_PROFILE

```
-- LMTCPB à *YES pour le profil TESTSECU. En mode test
SELECT AUTHORIZATION_NAME, LIMIT_CAPABILITIES FROM qsys2.USER_INFO
WHERE AUTHORIZATION_NAME = 'TESTSECU';

SELECT * FROM
              TABLE(SYSTOOLS.CHANGE_USER_PROFILE(
                P_USER_NAME  => 'TESTSECU',
                P_LIMIT_CAPABILITIES     => '*YES',
                PREVIEW => 'YES' --En mode test montre la commande
                    --PREVIEW      => 'NO' --En mode réel
                    ));
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Objets

Vue QSYS2.OBJECT_PRIVILEGES

- Droits sur un objet
  - Privés
  - Publics

```
--Objets de la bibliothèque PROD ayant des droits publics <>
d'*EXCLUDE
SELECT *
    FROM qsys2.object_privileges
    WHERE system_object_schema = 'PROD'
        AND authorization_name = '*PUBLIC'
        AND object_authority <> '*EXCLUDE';
```

Fonction table OBJECT_PRIVILEGES()

- Liste des droits privés et public pour un objet

```
--Pour un objet, liste des droits privés et publics
--Syntaxe 1
SELECT * FROM TABLE(
QSYS2.OBJECT_PRIVILEGES('ZSTRICT', 'INSTALL', '*DTAARA'));
--Syntaxe 2
SELECT * FROM TABLE (QSYS2.OBJECT_PRIVILEGES(
SYSTEM_OBJECT_SCHEMA =>'ZSTRICT',
SYSTEM_OBJECT_NAME   => 'INSTALL',
OBJECT_TYPE          => '*DTAARA'));
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

IFS

Fonction Table QSYS2.IFS_OBJECT_STATISTICS

- Liste les dossiers et documents de l'IFS à partir d'un niveau de l'arborescence

```
--Liste des dossiers et documents et leur taille, contenus dans
la racine
SELECT PATH_NAME, OBJECT_TYPE, DATA_SIZE
  FROM TABLE (QSYS2.IFS_OBJECT_STATISTICS(START_PATH_NAME => '/',
        SUBTREE_DIRECTORIES => 'NO'));
--Liste des dossiers et documents avec scan des sous répertoires
SELECT PATH_NAME, OBJECT_TYPE, DATA_SIZE, ALLOCATED_SIZE
    FROM TABLE (QSYS2.IFS_OBJECT_STATISTICS(
       START_PATH_NAME => '/STR-iCT/elk',
       SUBTREE_DIRECTORIES => 'YES'));
```

Fonction table QSYS2.IFS_OBJECT_PRIVILEGES()

- Comparable à OBJECT_PRIVILEGES()
- Renvoie une ligne par droit (privé ou public)

```
--IFS : liste des droits pour le dossier /STR-iCT et tout ce
qu'il contient
WITH DOSSIER (Chemin) AS (SELECT PATH_NAME FROM TABLE
(QSYS2.IFS_OBJECT_STATISTICS(START_PATH_NAME => '/STR-iCT')))
SELECT * FROM DOSSIER D,
TABLE(QSYS2.IFS_OBJECT_PRIVILEGES(D.Chemin)) P;
```

Vue QSYS2.SERVER_SHARE_INFO

- Renvoie des informations sur les partages

```
--Liste des partages
SELECT * FROM QSYS2.SERVER_SHARE_INFO;
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Liste d'autorisations

QSYS2.AUTHORIZATION_LIST_USER_INFO

- Renvoie la liste des AUTL et les droits qu'elles portent

```
--Liste des AUTL
SELECT AUTHORIZATION_LIST
   FROM QSYS2.AUTHORIZATION_LIST_USER_INFO
   GROUP BY  AUTHORIZATION_LIST
   ORDER by 1;
-- Droits portés par une AUTL
SELECT *
   FROM QSYS2.AUTHORIZATION_LIST_USER_INFO
   WHERE AUTHORIZATION_LIST = 'TESTSECU';
```

QSYS2.AUTHORIZATION_LIST_INFO

- Renvoie la liste des objets (et IFS) protégés par une liste d'autorisation

```
--Liste des objets et IFS sécurisés par une AUTL
SELECT * FROM QSYS2.AUTHORIZATION_LIST_INFO WHERE
AUTHORIZATION_LIST = 'ADICT';
--Liste des documents et dossiers de l'IFS sécurisés par une AUTL
SELECT * FROM QSYS2.AUTHORIZATION_LIST_INFO WHERE
AUTHORIZATION_LIST = 'ADICT'
AND SYSTEM_OBJECT_NAME is null;
```

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Réseau

QSYS2.NETSTAT_INFO

- Équivalent NETSTAT(*CNN)

Fonction table SYSTOOLS.PING

- Ping

```
--Ping
SELECT * FROM
TABLE(SYSTOOLS.PING('www.ibm.com'));
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

Et encore…

Authority Collection

- Gestion des Authority Collection
- QSYS2.AUTHORITY_COLLECTION_xxx

PTFs

- Nombreuses vues et fonction table sur les PTFs
- Vue GROUP_PTF_INFO : groupes PTFs

```
--Groupe PTFs WRKPTFGRP
SELECT * FROM QSYS2.GROUP_PTF_INFO;

-- Comparaison PTFs de la partition avec préconisées par IBM

SELECT *
    FROM SYSTOOLS.GROUP_PTF_CURRENCY
    ORDER BY PTF_GROUP_LEVEL_AVAILABLE -
PTF_GROUP_LEVEL_INSTALLED DESC;
```

Journalisation

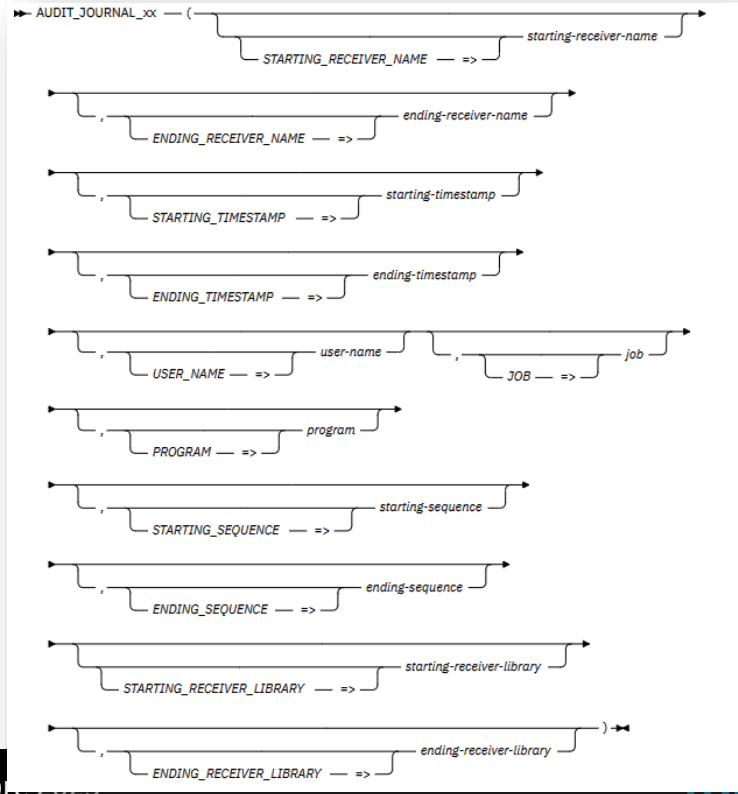
- SQL Service sur les journaux
- Fonction table QSYS2.DISPLAY_JOURNAL()

QSYS2.DISPLAY_JOURNAL()

```
--QAUDJRN nombre problèmes de mot de passe
SELECT count(*) FROM TABLE (
        QSYS2.DISPLAY_JOURNAL( 'QSYS', 'QAUDJRN')
WHERE  JOURNAL_ENTRY_TYPES =>'PW');
--QAUDJRN liste problèmes de mot de passe
SELECT  ENTRY_TIMESTAMP, JOURNAL_CODE, JOURNAL_ENTRY_TYPE,
 REMOTE_PORT, REMOTE_ADDRESS
   FROM TABLE (QSYS2.DISPLAY_JOURNAL(
   JOURNAL_LIBRARY  =>'QSYS',
   JOURNAL_NAME     =>'QAUDJRN',
   STARTING_RECEIVER_NAME  => '*CURRENT',
   JOURNAL_ENTRY_TYPES => 'PW'));
```

Fonction table SYSTOOLS.AUDIT_JOURNAL_xx

- Des fonctions spécifiques pour traiter le journal d'audit
- AUDIT_JOURNAL_xx
  - Ou xx est le type d'entrée (AF, PW…)



Fonction table QSYS2.CERTIFICATE_INFO

- Vérification des certificats

```
--Vérification de date des certificats
SELECT CERTIFICATE_LABEL, VALIDITY_START, VALIDITY_END
  FROM TABLE (QSYS2.CERTIFICATE_INFO(
     CERTIFICATE_STORE_PASSWORD  => 'MonPWD',
     CERTIFICATE_STORE  => '*SYSTEM'));
```

CERTIFICATE_LABEL	VALIDITY_START	VALIDITY_END
STR-iCT_Postgre	2023-02-14 18:00:58	2024-02-14 18:00:58
AUBRAC	2022-10-17 14:37:26	2023-10-18 14:37:26
LOCAL_CERTIFICATE_AUTHORITY_21A3E2V1(1)	2022-10-17 14:33:02	2042-10-13 14:33:02

Et aussi…

- Sécurisation des objets en SQL
  - GRANT & REVOKE
- RCAC
  - Limitation de l'accès aux données
  - Sélection de lignes en fonction du profil/groupe
  - Obfuscation d'une colonne (XX-XXXXXX-5246)
- Field procédure
  - Programme d'exit appelé à chaque action sur la colonne
  - Permet le cryptage au niveau base de données

44