

**Power  
Week**

# Université IBM i 2019



**22 et 23 mai**

IBM Client Center Paris

## **S53 - Sécurisez vos données sensibles grâce aux collectes de droits**

Dominique GAYTE

NoToS

[dgayte@notos.fr](mailto:dgayte@notos.fr) – 06 30 17 02 55



# NoToS

- Expertise autour de l'IBM i



- Sécurité
- PHP sur IBM i
- DB2 Web Query
- Développement de progiciels

lorena 

distant.backup 

monitor i 

power.gdpr 

power.sign 

power.spool 

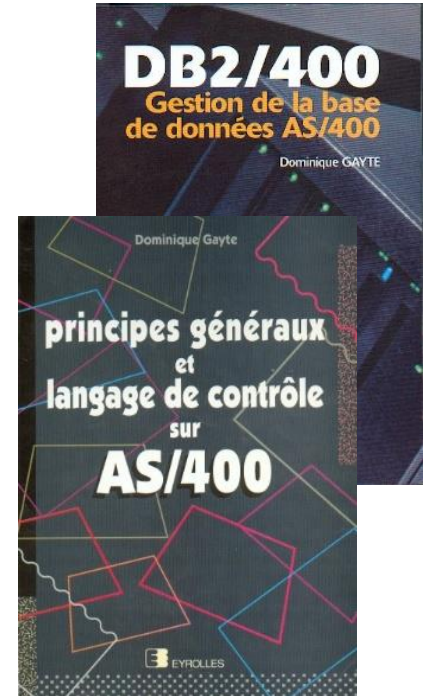
AD-ICT 

**ON S'ASSOC*i*E!**

**iDINFO**  
L'INGENIERIE DIGITALE

# Dominique GAYTE

- Intervenant « AS/400 » depuis 1990
  - Au nom d'IBM
  - Plus de 1 000 journées
- Sécurité
  - Audit
  - GDPR
  - Mise en œuvre : SSO, SSL, sécurisation de la base de données...
- Développements complexes
  - Sécurité
    - Points d'exit
  - API système
  - RPG IV
    - XML
    - Accès bases de données distantes



# Plan de la présentation

- Petits rappels sur la Sécurité
- La collecte de droits
  - Démarrage
  - Exploitation
- Utilisation avec SQL

**Power  
Week**

**Université IBM i**

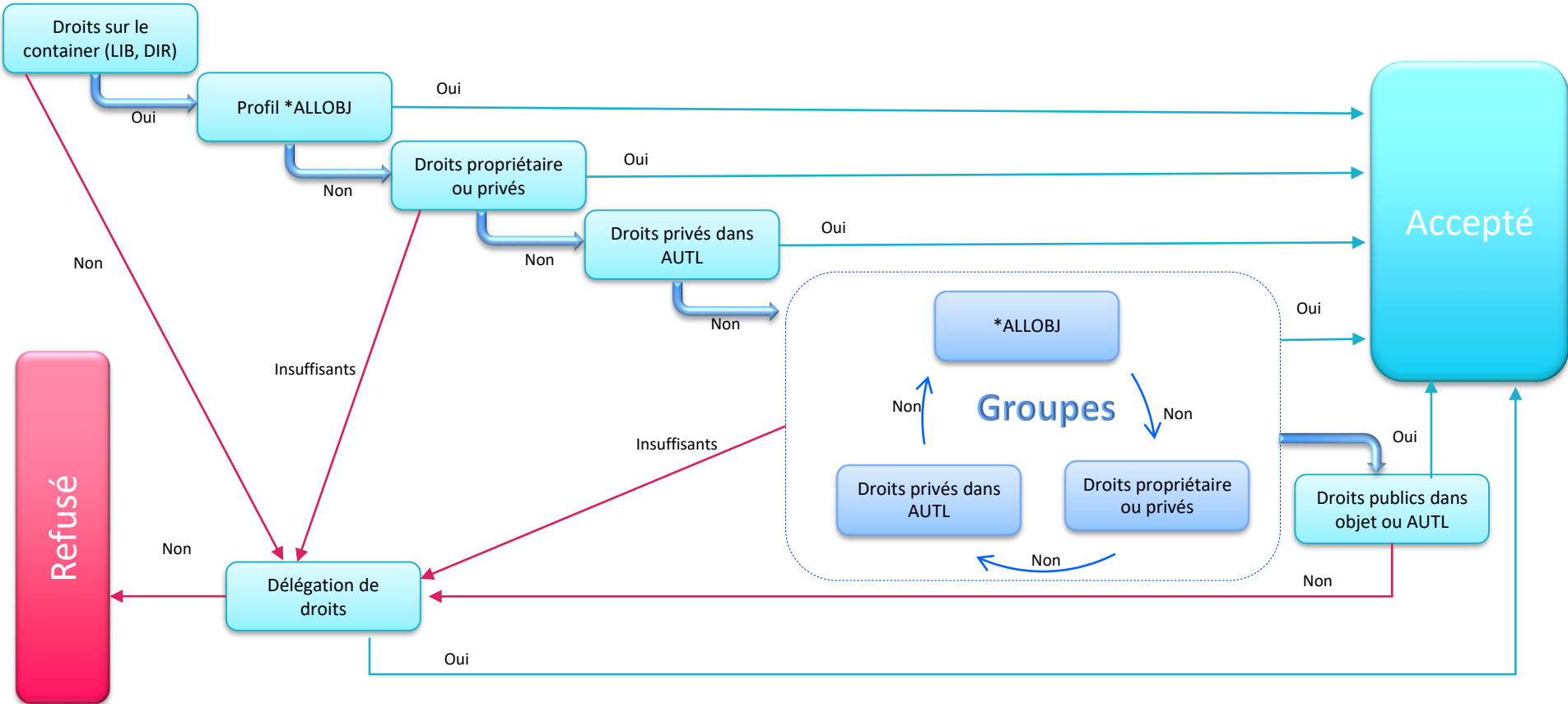
22 et 23 mai 2019

**IBM**

Petits rappels ...

# Vérification des droits (schématisique)

Accepté



# Règles

- Lorsqu'un droit est trouvé, bon ou mauvais, on sort
  - Sauf avec la délégation de droits qui est vérifiée ensuite
  - En vérifiant les droits du propriétaire du programme
- Les droits élémentaires ne sont pas cumulés
  - Sauf pour les groupes
  - \*EXCLUDE provoque la sortie

# Collectes de droits

*Authority Collection*



# Collectes de droits

- Fonction qui permet à l'administrateur de la Sécurité de mieux comprendre les mécanismes d'attributions des droits réellement mis en œuvre dans le cadre d'une application
- Utile pour n'octroyer que les droits nécessaires aux utilisateurs
- Intégré à l'IBM i (V7R3) (et au microcode)
- Capture d'informations lors de l'exécution des programmes par un profil utilisateur
- Affichage et analyse des données
- Déduction des plus petits droits nécessaires au bon fonctionnement des applications pour ce profil

# Ce qui est analysé

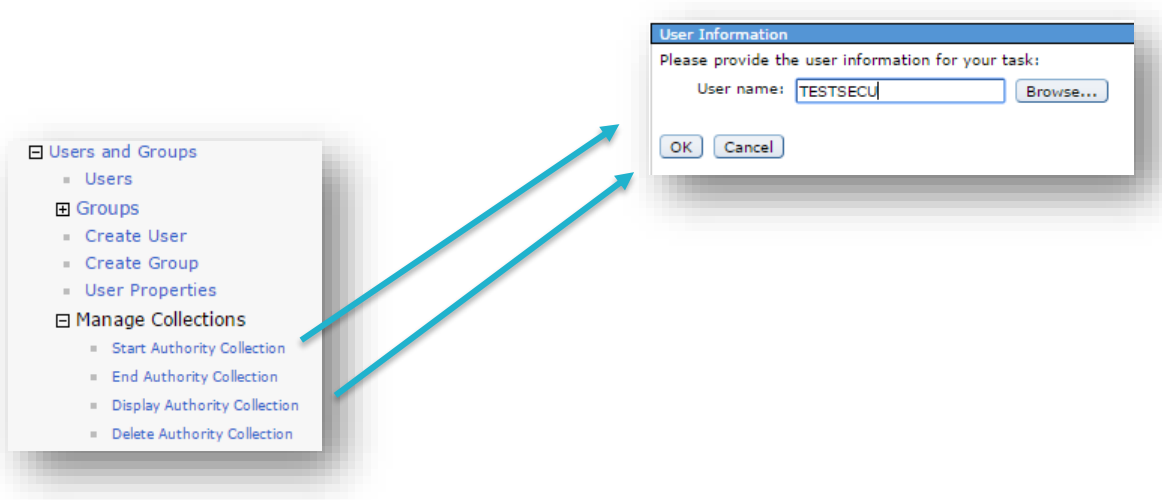
- Les droits utilisés quelle qu'en soit l'origine
  - Profil utilisateur
  - Groupes
  - Droits publics
  - Adoption de droits
- Sur tous types d'objets (et IFS)
- Une entrée est stockée dans la base données pour chaque vérification des droits
- Attention à la charge du système
  - Mise en œuvre pour un profil
  - Tests
  - Arrêt
  - Analyse

# Interfaces

- Navigator for i
- Commandes de l'IBM i
  - STRAUTCOL
  - ENDAUTCOL
  - DLTAUTCOL
  - DSPUSRPRF
  - DMPUSRPRF
  - RTVUSRPRF
- API
  - QSYRUSRI (ajouté à la fin du format USRI0300)
- SQL (Vues)
  - QSYS2.AUTHORITY\_COLLECTION
  - QSYS2.USER\_INFO

# Navigator for i

- Dans la gestion des utilisateurs
  - Manage Collections



# Démarrage d'une collecte

- STRAUTCOL ou QSYRUSRI ou Navigator for i

Démarrer la collecte des droits

Utilisateur : Neuneu

Bibliothèques de recherche : Utiliser l'entrée suivante Survol  
DGAYTE

Objets à rechercher : Utiliser l'entrée suivante Survol Tout, Générique\* ou Nom (jusqu'à 10)  
ENTETE

Types d'objet : Tout Survol Tout, Types (jusqu'à 10)

Inclure documents ou dossiers Néant

Inclure objets de système de fichiers Néant Survol

Supprimer la collecte précédente ? Non

Détails : Informations sur les objets

Bibliothèques à omettre : Néant Survol

OK Annulation

\*OBJINF : une fois par objet et type de droits (quel que soit le travail)  
\*OBJJOB : pour chaque travail (volume plus important)

# Affichage d'une collection

- Visualisation des droits utilisés pour accéder à l'objet

Gsm	GSM	*PGM	*USE	*CHANGE	PUBLIC
Securinit	Droits	*PGM		*CHANGE	PUBLIC
Securinit	Properties	*PGM		*CHANGE	PUBLIC
Bldettmp	GSM	*FILE			PUBLIC
Bldettmp	GSM	*FILE			PUBLIC
Bldettmp	GSM	*FILE			PUBLIC
Bldetmp	GSM	*FILE	*ALL		PUBLIC

Droits de Gsm.pgm - 192.168.1.10

Objet : /QSYS.LIB/GSM.LIB/GSM.PGM

Type : Programme Propriétaire : Dgaye Groupe principal : (Néant) Liste d'autorisation : (Néant)

Vue Droits : Minimum Go

Sélection	Nom	Utilisation	Modification	Droits absolus	Exclusion
<input checked="" type="checkbox"/>	(Public)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Dgaye	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Gsm Properties - 192.168.1.10

Object Information	Authorization name: TESTSECU
Authority Details	Check timestamp: 2016-05-04 11:38:18.892293
Stack Information	<b>Authority information</b>
Job Information	Authorization list:
File System Information	Authority check successful: 1
	Check any authority: 0
	Cached authority: 1
	Required authority: *USE
	Detailed required authority: *OBJOPR *READ *EXECUTE
	Current authority: *CHANGE
	Detailed current authority: *OBJOPR *READ *ADD *DLT *UPD *EXECUTE
	Authority source: PUBLIC
	Group name:
	Multiple groups used: 0
	<b>Authority adoption information</b>
	Adopt authority used: 0
	Current adopted authority:

# Propriétés

- Détail des droits nécessaires et des droits réellement disponibles
- Ci-dessous \*OBJOPR nécessaire et disponible via les droits publics de l'objet

**System object information**  
Name: SODETTMP  
Library: GSM  
Type: \*FILE

**Authority information**  
Authorization name: TESTSECU  
Check timestamp: 2016-05-04 11:38:18.973094

**Authority information**  
Authorization list:  
Authority check successful: 1  
Check any authority: 0  
Cached authority: 1  
Required authority:  
**Detailed required authority: \*OBJOPR**  
Current authority:  
Detailed current authority: \*OBJMGT \*OBJOPR READ \*ADD \*DLT \*UPD \*EXECUTE  
Authority source: **PUBLIC**  
Group name:  
Multiple groups used: 0

Utilisat	Groupe	sur objet	Opér	Gest	Exist	Modif	Réf
*PUBLIC		<u>USER DEF</u>	X	X	-	-	-
QSECOFR		<u>*ALL</u>	X	X	X	X	X

# Exemple 1

- Non autorisé par liste d'autorisation, droits publics

System Object Name	System Object Library	System Object Type	Required Authority	Current Authority	Authority Source	Adopted Authority Source	Current Adopted Authority	Authority Check Successful
Familles	GSM	*FILE			PUBLIC			x
Famden	GSM	*FILE			PUBLIC			x
Gsm	GSM	*PGM	*USE	*EXCLUDE	AUTHORIZATION LIST PUBLIC			
Gsm	GSM	*PGM		*EXCLUDE	AUTHORIZATION LIST PUBLIC			

## Authority information

Authorization list:

Authority check successful: 0

Check any authority: 0

Cached authority: 1

Required authority: \*USE

Detailed required authority: \*OBJOPR \*READ \*EXECUTE

Current authority: \*EXCLUDE

Detailed current authority: \*EXCLUDE

Authority source: AUTHORIZATION LIST PUBLIC

Group name:

Multiple groups used: 0

## Authority adoption information

Adopt authority used: 0



# Exemple 2

- Droits personnel \*EXCLUDE
- Autorisé grâce à la liste d'autorisation
- Héritage de \*ALLOBJ

System Object Name	System Object Library	System Object Type	Required Authority	Current Authority	Authority Source	Adopted Authority Source	Current Adopted Authority	Authority Check Successful
Familles	GSM	*FILE			PUBLIC			x
Famdsp	GSM	*FILE			PUBLIC			x
Gsm	GSM	*PGM	*USE	*EXCLUDE	AUTHORIZATION LIST PUBLIC			
Gsm	GSM	*PGM		*EXCLUDE	AUTHORIZATION LIST PUBLIC			
Gsm	GSM	*PGM	*USE	*EXCLUDE	AUTHORIZATION LIST PUBLIC			
Gsm	GSM	*PGM		*EXCLUDE	AUTHORIZATION LIST PUBLIC			
Gsm	GSM	*PGM	*USE	*USE	PUBLIC			x
Securinit	GSM	*PGM	*EXCLUDE	*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x
Securinit	GSM	*PGM	*EXCLUDE	*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x

**Authority Information**  
Authorization list: GSM  
Authority check successful: 1  
Check any authority: 0  
Cached authority: 0  
Required authority:  
Detailed required authority: \*OBJOPR  
Current authority: \*EXCLUDE  
Detailed current authority: \*EXCLUDE  
Authority source: AUTHORIZATION LIST PUBLIC  
Group name:  
Multiple groups used: 0

**Authority adoption information**  
Adopt authority used: 1  
Current adopted authority: \*ALL  
Detailed current adopted authority: \*OWNER \*OBJEXIST \*OBJMGT \*OBJALTER \*OBJREF \*OBJOPR \*READ \*ADD \*DLT \*UPD \*EXECUTE  
Adopted authority source: ADOPTED \*ALLOBJ

# Export des résultats

- En HTML ou CSV

```
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:23:03.475451"
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:23:03.475413"
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:23:03.475387"
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:23:03.475337"
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:23:03.474687"
Entete.DGAYTE *FILE,*ALL,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,x,"",2019-04-22 17:23:03.474520"
Entete.DGAYTE *FILE,*USE,PUBLIC,,,x,"",2019-04-22 17:23:03.474090"
Entete.DGAYTE *FILE,*USE,PUBLIC,,,x,"",2019-04-22 17:23:03.474079"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.466470"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.466200"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.466166"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.466137"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.466080"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:19:19.465367"
Entete.DGAYTE *FILE,*ALL,*USE,USER PRIVATE,ADOPTED *ALLOBJ,*ALL,x,x,"",2019-04-22 17:19:19.465171"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,,,x,"",2019-04-22 17:19:19.464715"
Entete.DGAYTE *FILE,*USE,USER PRIVATE,,,x,"",2019-04-22 17:19:19.464702"
Entete.DGAYTE *FILE,*EXCLUDE,USER PRIVATE,,,,"",2019-04-22 17:18:08.222091"
Entete.DGAYTE *FILE,*USE,PUBLIC,,,,"",2019-04-22 17:10:05.506969"
Entete.DGAYTE *FILE,*USE,PUBLIC,ADOPTED *ALLOBJ,*ALL,x,"",2019-04-22 17:10:05.506936"
```

Fermer

Nom d'objet système	Bibliothèque d'objets système	Type d'objet système	Droits requis	Droits en cours	Source de droits	Source de droits adoptés	Droits adoptés en cours	La vérification des droits a abouti	Vérification de tous les droits	Vérification d'horodatage
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:33:18.570436
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:33:18.570427
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC					2019-04-22 17:32:56.769688
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:31:59.000706
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:31:59.000698
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:26:48.595034
Entete	DGAYTE	*FILE		*EXCLUDE	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:26:48.595025
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475695
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475451
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475413
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475387
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475337
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:23:03.475337
Entete	DGAYTE	*FILE	*ALL	*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x	x	2019-04-22 17:23:03.474520
Entete	DGAYTE	*FILE		*USE	PUBLIC			x		2019-04-22 17:23:03.474090
Entete	DGAYTE	*FILE		*USE	PUBLIC			x		2019-04-22 17:23:03.474079
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.466470
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.466200
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.466166
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.466137
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.466080
Entete	DGAYTE	*FILE		*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:19:19.465367
Entete	DGAYTE	*FILE	*ALL	*USE	USER PRIVATE	ADOPTED *ALLOBJ	*ALL	x	x	2019-04-22 17:19:19.465171
Entete	DGAYTE	*FILE		*USE	USER PRIVATE			x		2019-04-22 17:19:19.464715
Entete	DGAYTE	*FILE		*USE	USER PRIVATE			x		2019-04-22 17:19:19.464702
Entete	DGAYTE	*FILE		*EXCLUDE	USER PRIVATE					2019-04-22 17:18:08.222091
Entete	DGAYTE	*FILE		*USE	PUBLIC					2019-04-22 17:10:05.506969
Entete	DGAYTE	*FILE		*USE	PUBLIC	ADOPTED *ALLOBJ	*ALL	x		2019-04-22 17:10:05.506936

# Ajout de colonnes

The screenshot shows a software interface with a menu and a dialog box. The menu is open, showing options like 'Droits', 'Colonnes...', 'Sauvegarde en tant que favori', 'Actualiser', 'Exporter', 'Imprimer', and 'Configurer les options'. The dialog box, titled 'Collecte des droits - Colonnes', has two panes. The left pane, 'Colonnes disponibles', contains a list of columns with checkboxes: Titre, Nom d'autorisation, Nom ASP, Numéro de l'ASP, Liste d'autorisation, Nom d'objet, Schéma d'objet, Type d'objet, Nom ASP objet, Numéro ASP objet, Droits adoptés utilisés, and Nom de programme d'adoption. The right pane, 'Colonnes en cours', contains a list of columns with checkboxes: Titre, Nom d'objet système, Bibliothèque d'objets système, Type d'objet système, Droits requis, Droits en cours, Source de droits, Source de droits adoptés, Droits adoptés en cours, La vérification des droits a abouti, Vérification de tous les droits, and Vérification d'horodatage. Between the panes are buttons for 'Ajout >', '< Retrait', 'Ajout global >>', 'Vers le haut', and 'Vers le bas'. The 'Ajout global >>' button is highlighted in blue.

# Utilisation de SQL pour exploiter les données

- Pour extraire les données à partir des vues
- QSYS2.AUTHORITY\_COLLECTION
- QSYS2.USER\_INFO

AUTHORIZATION_N...	AUTHORITY_COLLECTION_REPOSITORY_EXI...
TESTSECU	YES

# QSYS2.AUTHORITY\_COLLECTION

- Contient les informations sur les collectes de droits pour les objets
- [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_73/rzarl/rzarl\\_autcolview.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_73/rzarl/rzarl_autcolview.htm)
- Ce qui est affiché dans Navigator for i
- Liste des échecs pour le profil utilisateur TESTSECU

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION  
WHERE authorization_name = 'TESTSECU' AND  
authority_check_successful = 0;
```

AUTHORIZATION_NAME	CHECK_TIMESTAMP	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	ASP_NAME	ASP_NUMBER	OBJECT_NAME	OBJECT_SCHEMA	OBJECT_TYPE	AUTHORIZATION_LIST
TESTSECU	2019-04-22 17:52:41.438430	-	-	*DIR	-	--	-	-	-	-
TESTSECU	2019-04-22 17:10:05.506969	ENTETE	DGAYTE	*FILE	*SYSBAS	0	ENTETE	DGAYTE	TABLE	TESTSECU
TESTSECU	2019-04-22 17:18:08.222091	ENTETE	DGAYTE	*FILE	*SYSBAS	0	ENTETE	DGAYTE	TABLE	TESTSECU
TESTSECU	2019-04-22 17:32:56.769688	ENTETE	DGAYTE	*FILE	*SYSBAS	0	ENTETE	DGAYTE	TABLE	TESTSECU

# QSYS2.USER\_INFO

- Contient des informations au sujet d'un profil utilisateur
- Notamment s'il a des données concernant les collectes de droits
  - AUTHORITY\_COLLECTION\_ACTIVE : une collecte est en cours pour ce profil
    - Nom système AUTCOLACT
    - YES ou NO
  - AUTHORITY\_COLLECTION\_REPOSITORY\_EXISTS : des données de collecte sont disponibles
    - Nom système AUTCOLREP
    - YES ou NO

## QSYS2.USER\_INFO (2)

- Liste des utilisateurs ayant une collection

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

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

AUTHORIZATION_NAME	AUTHORITY_COLLECTION_REPOSITORY_EXISTS
TESTSECU	YES

# Exemple SQL 3

- Liste des documents de l'IFS pour lesquels il y a des données dans la collection

```
SELECT AUTHORIZATION_NAME, AUTHORITY_CHECK_SUCCESSFUL, CHECK_ANY_AUTHORITY,  
       REQUIRED_AUTHORITY, PATH_NAME, DETAILED_REQUIRED_AUTHORITY, CURRENT_AUTHORITY,  
       DETAILED_CURRENT_AUTHORITY, AUTHORITY_SOURCE  
FROM QSYS2.AUTHORITY_COLLECTION  
WHERE AUTHORIZATION_NAME = 'TESTSECU' AND SYSTEM_OBJECT_TYPE = '*STMF'
```

AUTHORIZATION_N...	AUT...	CHECK_AN...	REQUI...	PATH_NAME	DETAILED_REQUIRED_AUTHO...	CURRENT_AUTHO...	DETAILED_CURRENT_AUTHORITY
TESTSECU	1	0	-	/tmp/xmlhandler2.xml	*OBJOPR *READ	*ALL	*OBJEXIST *OBJMGT *OBJALTER *OBJRE



# Announce V7R4

- Possibilité de collecter de donnée sur un objet en particulier
- Avant, seulement possible à partir d'un utilisateur

Authority Collection support is enhanced to include the collection of authority information for specific objects. Previously, authority information could be collected only for users, where authority information was collected for all objects accessed by a specific user.



Dominique GAYTE

NoToS

[dgayte@notos.fr](mailto:dgayte@notos.fr) – 06 30 17 02 55