

# Université IBM i 2018

16 et 17 mai

IBM Client Center Paris



## S37 - SQL pour le responsable de la sécurité IBM i

Dominique GAYTE

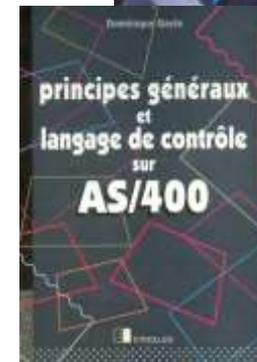
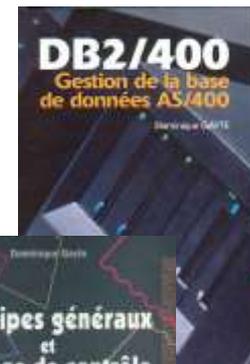
NoToS

*dgayte@notos.fr – www.notos.fr*



# NoToS

- Expertise autour de l'IBM i
  - Regard moderne
  - Sécurité
  - Service
    - Formation, audit, développement...
- PHP sur IBM i avec Zend
  - Modernisation
  - Web Services...
- Développement de progiciels
  - Modernisation à valeur ajoutée des IBM i



# Plan de la présentation

- Rappel sur SQL et IBM i
- Sécuriser en utilisant SQL
  - Déclarations SQL
  - RCAC
  - Field Procedure
- IBM i Services
  - Exemples

A background of a complex network graph with numerous nodes and connecting lines, rendered in a light gray color. The nodes are small circles, and the lines are thin and connect the nodes in a dense, interconnected pattern.

# Rappels SQL sur IBM i

- Le langage d'exploitation des bases de données relationnelles
  - Manipulation des données
  - Définition des données
  - Sécurisation des données
  - Contrôle des transactions
- Un standard, connu notamment
  - Par les jeunes
  - Par les administrateurs (de base de données) non IBM i

# SQL sur IBM i



- A la demande
  - STRSQL
  - System i Navigator
  - ACS (recommandé)
  - Autres (client ODBC/JDBC : Excel...)
- Dans les programmes (Embedded SQL)
  - RPG, COBOL...
  - CL (RUNSQL, RUNSQLSTM)
- Procédures stockées
  - Exécution en environnement hétérogène
  - Sur une connexion base de données (ODBC/JDBC...)

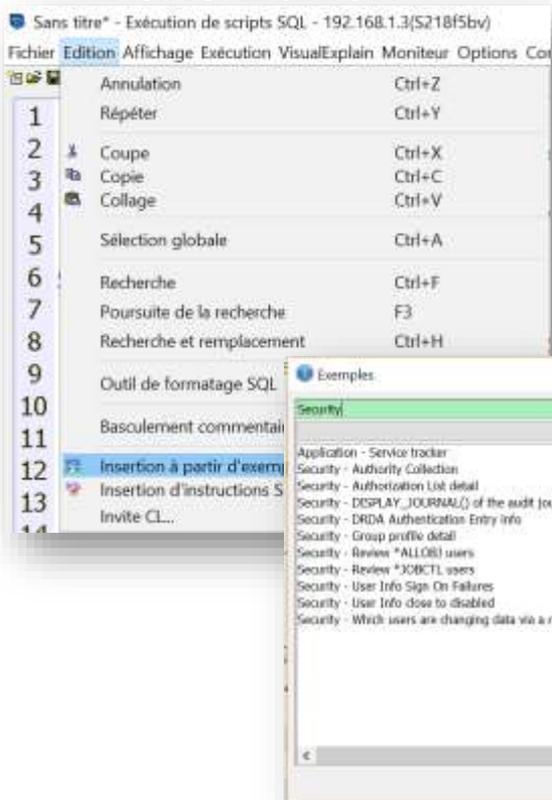
# ACS et l'exécution de scripts SQL

- A partir de la version 1.1.7.0
- Avec coloration syntaxique
- Copier/coller des résultats
- Envoi dans une table IBM i
- Enregistrement des requêtes
- Visual Explain

```
-- category: IBM i Services  
-- description: Application - Service tracker  
--  
-- Review all the Security related IBM i Services  
--  
SELECT *  
FROM QSYS2.SERVICES_INFO  
WHERE SERVICE_CATEGORY = 'SECURITY';
```

# ACS : utilisation d'exemples SQL

## ■ Dans Edition



Sans titre\* - Exécution de scripts SQL - 192.168.1.3(S218f5bv)

Fichier Edition Affichage Exécution VisualExplain Moniteur Options Co...

Annulation Ctrl+Z

1 Répéter Ctrl+Y

2 Coupe Ctrl+X

3 Copie Ctrl+C

4 Collage Ctrl+V

5 Sélection globale Ctrl+A

6 Recherche Ctrl+F

7 Poursuite de la recherche F3

8 Recherche et remplacement Ctrl+H

9 Outil de formatage SQL

10 Basculement commentai...

11 Insertion à partir d'exem...

12 Insertion d'instructions S...

13 Invite CL...

14

Exemples

- Security
- Application - Service tracker
- Security - Authority Collection
- Security - Authorization List detail
- Security - DISPLAY\_JOURNAL() of the audit journal
- Security - DRDA Authentication Entry info
- Security - Group profile detail
- Security - Review \*ALL081 users
- Security - Review \*JOBCTL users
- Security - User Info Sign On Failures
- Security - User Info close to disabled
- Security - Which users are changing data via a remote conn...

```
2 -- category: IBM / Services
3 -- description: Application - Service tracker
4 --
5 -- Review all the Security related IBM / Services
6 --
7 SELECT *
8 FROM QSYS2.SERVICES_INFO
9 WHERE SERVICE_CATEGORY = 'SECURITY';
10
```

SERVICE_CATEGORY	SERVICE_SCHEMA_NAME	SERVICE_NAME	SQL_OBJECT_TYPE	OBJECT_TYPE	SYSTEM_OBJECT
SECURITY	QSYS2	USER_INFO	VIEW	*FILE	USER_INFO
SECURITY	QSYS2	FUNCTION_INFO	VIEW	*FILE	FCN_INFO
SECURITY	QSYS2	FUNCTION_USAGE	VIEW	*FILE	FCN_USAGE
SECURITY	QSYS2	GROUP_PROFILE_ENTRIES	VIEW	*FILE	GROUPLIST
SECURITY	QSYS2	SQL_CHECK_AUTHORITY	SCALAR FUNCTION	*SRVPGM	SQL_C00001
SECURITY	QSYS2	SET_COLUMN_ATTRIBUTE	PROCEDURE	-	-
SECURITY	QSYS2	DRDA_AUTHENTICATION_ENTRY_INFO	VIEW	*FILE	DRDA_AUTHE
SECURITY	QSYS2	OBJECT_PRIVILEGES	VIEW	*FILE	OBJ_PRIV
SECURITY	QSYS2	AUTHORIZATION_LIST_INFO	VIEW	*FILE	AUTHL_INFO
SECURITY	QSYS2	AUTHORIZATION_LIST_USER_INFO	VIEW	*FILE	AUTL_USERS

# Sécuriser en utilisant SQL

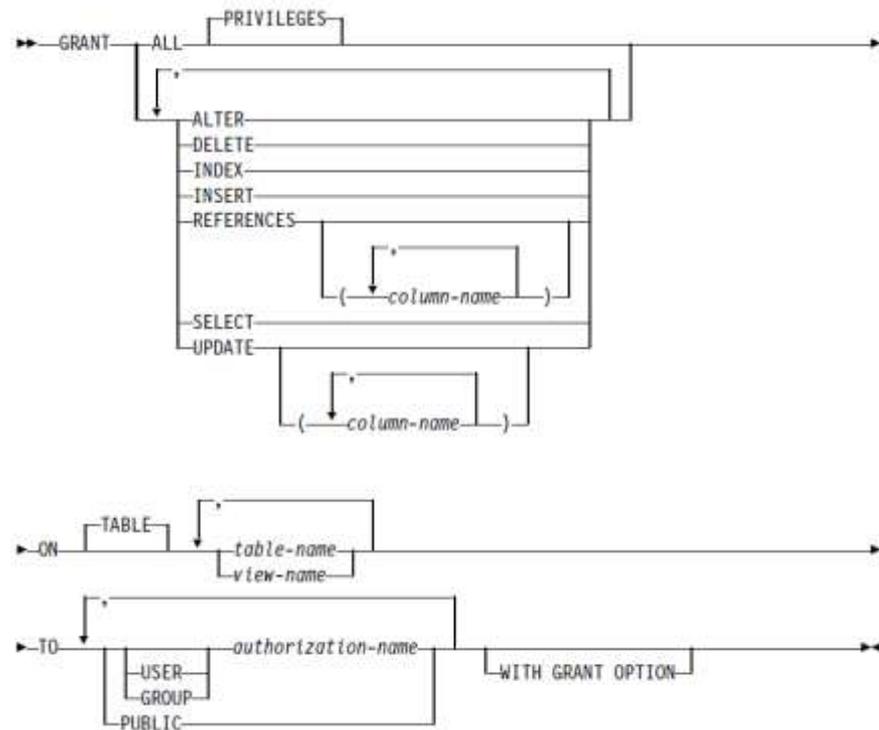


# Sécuriser avec SQL

- Les déclarations
  - GRANT & REVOKE
- RCAC
  - Limitation de l'accès aux données (lignes et colonnes)
- Field procédure
  - Programme d'exit appelé à chaque action sur la colonne

# GRANT & REVOKE

- Ordres SQL natifs pour gérer les droits sur les objets de DB2 for i et sur les données
- En remplacement des commandes CL
  - GRTOBJAUT & RVKOBJAUT



# Fonction VERIFY\_GROUP\_FOR\_USER

- Nouvelle fonction qui permet de savoir si le profil utilisateur appartient à un groupe
- Renvoi un entier : 1 si vrai, 0 sinon

```
VALUES VERIFY_GROUP_FOR_USER(SESSION_USER,'COMPTA');
```

00001

0

# RCAC (Row and Column Access Control)



- Option 47 de SS1
  - IBM Advanced Data Security for i
  - Non facturable
  - Apparue en V7R2
- RCAC permet de limiter l'accès à certaines données de type ligne et/ou colonne, aux seules personnes (ou groupes de personnes) qui sont habilitées à connaître le contenu de ces données
  - Même si on est \*ALLOBJ
  - Administrateur défini avec la commande WRKFCNUSG
    - Fonction QIBM\_DB\_SECADM
- RCAC utilise deux approches
  - Des permissions sur les lignes
  - Des masques sur les colonnes

# Permission sur ligne

- Une permission sur ligne est un objet DB2
- Créé avec SQL
- Doit être activée par un ALTER TABLE
- Elle ne laisse voir qu'une partie des lignes à certains utilisateurs

```
CREATE PERMISSION Client_Inf_1000
ON dgayte.entete
FOR ROWS WHERE
    SESSION_USER = 'DGAYTE'
OR client < 1000
ENFORCED FOR ALL ACCESS ENABLE ;

ALTER TABLE dgayte.entete ACTIVATE ROW ACCESS CONTROL;
```

# Exemple RCAC Ligne

```
CREATE PERMISSION dgayte.Client_Inf_1000
ON dgayte.entete
FOR ROWS WHERE
    SESSION_USER = 'DGAYTE'
OR client < 1000
ENFORCED FOR ALL ACCESS ENABLE
Instruction CREATE PERMISSION terminée pour CLIENT_INF_1000 de DGAYTE
ALTER TABLE dgayte.entete ACTIVATE ROW ACCESS CONTROL
L'exécution de l'instruction ALTER est terminée pour la table ENTETE
```

```
SELECT * FROM dgayte.entete ORDER BY CLIENT desc
```

DGAYTE

CLIENT	TOTAL
29.483	2.264,2536
29.482	2.264,2536
29.481	3.729,3640
29.480	2.698,4432
29.479	2.264,2536
29.478	2.649,8453
29.477	2.682,9953
29.476	3.756,9890

QSECOFR

CLIENT	TOTAL
701	7.775,7170
701	275,7448
701	22,1760
701	2.730,7313
701	892,8369
701	3.043,2769
700	40.868,0960
700	28.918,4417

# Masque sur colonne

- Un masque sur colonne est un objet DB2
- Créé avec SQL
- Doit être activé par un ALTER TABLE
- Il laisse voir tout ou partie d'une colonne
  - Masquage possible de caractères

```
CREATE [OR REPLACE] MASK cc_mask ON client
FOR COLUMN credit_card RETURN
CASE
    WHEN SESSION_USER = 'QSECOFR' THEN credit_card
    WHEN VERIFY_GROUP_FOR_USER(SESSION_USER,'ADMIN_CPT') = 1 THEN credit_card
    ELSE 'XXXXXXXXXXXX' CONCAT SUBSTR(credit_card,13, 4)
END
ENABLE;

ALTER TABLE client ACTIVATE COLUMN ACCESS CONTROL;
```

# Exemple colonne

```
CREATE OR REPLACE MASK dgayte.masquecpt ON dgayte.entete
FOR COLUMN compte RETURN
CASE
  WHEN SESSION_USER = 'DGAYTE' THEN compte
ELSE
  'XX-XXXX' CONCAT SUBSTR(compte, 8, 7)
END
ENABLE ;
ALTER TABLE dgayte.entete ACTIVATE COLUMN ACCESS CONTROL;
```

```
SELECT CLIENT, TOTAL, COMPTE FROM dgayte.entete ORDER BY CLIENT desc
```

DGAYTE

CLIENT	TOTAL	COMPTE
29.483	2.264,2536	10-4030-029483
29.482	2.264,2536	10-4030-029482
29.481	3.729,3640	10-4030-029481
29.480	2.698,4432	10-4030-029480
29.479	2.264,2536	10-4030-029479
29.478	2.649,8453	10-4030-029478

QSECOFR

CLIENT	TOTAL	COMPTE
701	7.775,7170	XX-XXXX0-00070
701	275,7448	XX-XXXX0-00070
701	22,1760	XX-XXXX0-00070
701	2.730,7313	XX-XXXX0-00070
701	892,8369	XX-XXXX0-00070
701	3.043,2769	XX-XXXX0-00070

# Field Procedure

- Programme d'exit appelé à chaque action sur la colonne (insert/update/read)
- Quelle que soit l'origine (SQL, RPG, ODBC...) !
- Sorte de trigger sur une colonne
- Ajouté avec un ALTER TABLE (ou CREATE)
- Un field procedure par colonne
- Utilisé notamment pour crypter les données d'une colonne !
  - Totalement au niveau physique
  - Ou partiellement (au niveau de l'utilisateur)
- Apparue en V7R1

# Programme appelé

- Le programme appelé est un \*PGM ILE
  - Pas d'OPM, pas de \*SRVPGM, pas de Java
  - Pas de SQL autorisé, pas de ACTGRP(\*NEW)
- Reçoit 9 paramètres
- Assez complexe

# Codification

- Exemple : « cryptage » des 4 premiers caractères du n° carte

```
CREATE TABLE dgayte.fieldproc(  
  z1 INT,  
  z2 CHAR(16));
```

```
ALTER TABLE dgayte.fieldproc  
ALTER COLUMN Z2 SET FIELDPROC dgayte.field_proc;
```

```
INSERT INTO dgayte.fieldproc VALUES(1, '123456789012345');  
INSERT INTO dgayte.fieldproc VALUES(1, '3210654987123122');  
  
SELECT * FROM dgayte.fieldproc;
```

Selon l'utilisateur

Z1	Z2
1	****56789012345
2	****654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

A background of a complex network graph with numerous nodes and connecting lines, rendered in a light gray color. The nodes are small circles, and the lines are thin, creating a dense web of connections across the entire page.

# **IBM i Services**

# IBM i Services



- Ensemble « d'objets » SQL offrant
  - L'accès à des fonctions système
  - L'équivalent de commandes CL
  - Fonctions scalaires
  - UDTF (tables)
  - Vues
- Une partie concerne la Sécurité
- Très dépendants des versions de l'IBM i, TR et PTFs...
- Utiles pour
  - Récupérer des listes dans des programmes
  - Des administrateurs non IBM i

# IBM i Services : Sécurité



- <http://ibm.biz/DB2foriServices>

IBM i Service	Type of Service	IBM i 7.3	IBM i 7.2	IBM i 7.1
<b>Security Services</b>				
QSYS2.AUTHORITY_COLLECTION	<b>View</b>	Base	-	-
QSYS2.AUTHORIZATION_LIST_INFO	<b>View</b>	SF99703 Level 4	SF99702 Level 16	-
QSYS2.AUTHORIZATION_LIST_USER_INFO	<b>View</b>	SF99703 Level 4	SF99702 Level 16	-
QSYS2.DRDA_AUTHENTICATION_ENTRY_INFO	<b>View</b>	Base	SF99702 Level 5	SF99701 Level 34
QSYS2.FUNCTION_INFO	<b>View</b>	Base	Base	SF99701 Level 26
QSYS2.FUNCTION_USAGE	<b>View</b>	Base	Base	SF99701 Level 26
QSYS2.GROUP_PROFILE_ENTRIES	<b>View</b>	Base	Base	SF99701 Level 23
QSYS2.OBJECT_PRIVILEGES	<b>View</b>	SF99703 Level 4	SF99702 Level 16	-
QSYS2.SQL_CHECK_AUTHORITY()	<b>UDF</b>	Base	Base	SF99701 Level 21
QSYS2.USER_INFO	<b>View</b>	Enhanced in Base Enhanced: SF99703 Level 4	Base Enhanced: SF99702 Level 16	Introduced: SF99701 Level 26 Enhanced: SF99701 Level 29 Enhanced: SF99701 Level 42
SYSPROC.SET_COLUMN_ATTRIBUTE()	<b>Procedure</b>	Base	Base	Base

# Vue AUTHORIZATION\_LIST\_USER\_INFO

- Extraire les droits d'une liste d'autorisations (commande DSPAUTL)

```
SELECT *  
FROM QSYS2.AUTHORIZATION_LIST_USER_INFO  
WHERE AUTHORIZATION_NAME = 'DGAYTE';
```

```
SELECT *  
FROM QSYS2.AUTHORIZATION_LIST_USER_INFO  
WHERE AUTHORIZATION_NAME = '*PUBLIC';
```

AUTHORIZATION_LIST	AUTHORIZATION_NAME	OBJECT_AUTHORITY	OWNER
DGLENAT	*PUBLIC	*EXCLUDE	DGLENAT
DSTBKP	*PUBLIC	*EXCLUDE	SMERINO
MALISTE	*PUBLIC	*CHANGE	BHERNANDEZ
PMCSI	*PUBLIC	*EXCLUDE	PMCSI
QINAVMNTR	*PUBLIC	*USE	QLWISVR
QIWSADM	*PUBLIC	*USE	QSECOFR
QLWISVR	*PUBLIC	*EXCLUDE	QSYS

# Vue AUTHORIZATION\_LIST\_INFO

- Objets protégés par une liste d'autorisations (commande DSPAUTLOBJ)

```
SELECT *  
FROM QSYS2.AUTHORIZATION_LIST_INFO  
WHERE AUTHORIZATION_LIST = 'PMCSI';
```

AUTHORIZATION_LIST	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_TYPE	OBJECT_ATTRIBUTE
PMCSI	PMCSI	PMCSIJEX9	*PGM	CLP
PMCSI	PMCSI	PMCSIJMR	*PGM	CLP
PMCSI	PMCSI	PMCSIJMG1	*PGM	RPGLE
PMCSI	PMCSI	PMCSIJMG2	*PGM	CLP
PMCSI	PMCSI	PMCSIJNM	*PGM	CLP
PMCSI	PMCSI	PMCSIJRN	*PGM	RPGLE
PMCSI	PMCSI	PMCSIJRS	*PGM	RPGLE
PMCSI	PMCSI	PMCSIM01	*PGM	CLP
PMCSI	PMCSI	PMCSIM02	*PGM	CLP
PMCSI	PMCSI	PMCSIM03	*PGM	CLP
PMCSI	PMCSI	PMCSIM09	*PGM	CLP
PMCSI	PMCSI	PMCSIOPEN	*PGM	CLP

# Vue OBJECT\_PRIVILEGES

- Droits sur un objet (commande DSPOBJAUT)

```
SELECT * FROM QSYS2.OBJECT_PRIVILEGES  
WHERE OBJECT_NAME = 'DGAYTE' AND  
SYSTEM_OBJECT_SCHEMA = 'QSYS' AND  
OBJECT_TYPE = '*LIB';
```

OBJECT_SCHEMA	OBJECT_NAME	SYSTEM_OBJECT_NAME	OBJECT_TYPE	AUTHORIZATION_NAME	OBJECT_AUTHORITY
QSYS	DGAYTE	DGAYTE	*LIB	*PUBLIC	*USE
QSYS	DGAYTE	DGAYTE	*LIB	QSECOFR	*ALL
QSYS	DGAYTE	DGAYTE	*LIB	ADMINWQ	*EXCLUDE
QSYS	DGAYTE	DGAYTE	*LIB	AMTV1	*EXCLUDE

# UDTF OBJECT\_STATISTICS

- Statistiques sur des objets

```
SELECT *  
FROM TABLE(QSYS2.OBJECT_STATISTICS('DGAYTE', 'FILE')) F  
ORDER BY OBJSIZE DESC;
```

OBJNAME	OBJTYPE	OBJOWNER	OBJDEFINER	OBJCREATED	OBJSIZE	OBJATTRIBUTE	OBJTEXT
WWW241213	*FILE	QSECOFR	QSECOFR	2013-12-24 16:07:46.000000	1539334144	SAVF	-
PSPL041013	*FILE	DGAYTE	DGAYTE	2013-10-04 17:19:39.000000	947937280	SAVF	-
QAEZD00010	*FILE	DGAYTE	DGAYTE	2013-03-18 16:45:27.000000	324161536	PF	-
PINC041013	*FILE	DGAYTE	DGAYTE	2013-10-04 18:38:48.000000	320102400	SAVF	-
IFS_INIT	*FILE	DGAYTE	DGAYTE	2018-01-10 09:15:37.000000	139509760	PF	-
TPSQL540	*FILE	DGAYTE	DGAYTE	2010-09-03 18:19:26.000000	74473472	SAVF	TP SQL Version 540

# Vue GROUP\_PROFILE\_ENTRIES

- Liste des profils de groupe et des profils associés

```
SELECT *  
FROM qsys2.group_profile_entries;
```

GROUP_PROFILE_NAME	USER_PROFILE_NAME	USER_TEXT
COMPTA	NOUVEAU	-
NOGROUP	NOBODY	ZendCore PASE User NoBody
NOGROUP	QTMHHTTP	Profil utilisateur de serveur HTTP
QPGMR	JPFLORIN	-
QPGMR	PBOSSE	-
QWQADMIN	AMELIA	-

--Liste des groupes

```
SELECT GROUP_PROFILE_NAME, count(*) AS NB  
FROM qsys2.group_profile_entries  
GROUP BY GROUP_PROFILE_NAME;
```

GROUP_PROFILE_NAME	NB
COMPTA	1
NOGROUP	2
QPGMR	2
QWQADMIN	4
WQADMIN	1

# Vue USER\_INFO

- Détail des profils utilisateurs (DSPUSRPRF ou API QSYRUSRI)

```
SELECT * FROM qsys2.user_info ;
```

- Très utile pour les revues de profil (liste des profils \*ALLOBJ)

```
SELECT AUTHORIZATION_NAME, SPECIAL_AUTHORITIES,  
USER_CLASS_NAME FROM qsys2.user_info  
WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%' ;
```

AUTHORIZATION_NAME	SPECIAL_AUTHORITIES	USER_CLASS_NAME
SMERINO	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS ...	*SECOFR
SMOLLE	*ALLOBJ	*SECOFR
SSHDUSR	*ALLOBJ	*USER
SUPPORT_I	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS ...	*SECOFR
TRIERA	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS ...	*SECOFR
VEREMES	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS ...	*SECOFR
WQADMIN	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS ...	*SECOFR

# Vue USER\_INFO (2)

- Liste des profils disposant directement ou indirectement de \*ALLOB J

```
SELECT AUTHORIZATION_NAME, STATUS, NO_PASSWORD_INDICATOR,  
PREVIOUS_SIGNON  
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;
```

# Vue USER\_INFO (3)

- Liste des profils non utilisés depuis x jours
- Exemple pour 90 jours

```
SELECT AUTHORIZATION_NAME, STATUS, LAST_USED_TIMESTAMP
FROM QSYS2.USER_INFO
WHERE LAST_USED_TIMESTAMP < CURRENT_TIMESTAMP -90 DAYS
AND STATUS <> '*DISABLED'
AND AUTHORIZATION_NAME NOT LIKE 'Q%'
ORDER BY 3 DESC;
```

AUTHORIZATION_NAME	STATUS	LAST_USED_TIMESTAMP
AMTV1	*ENABLED	2018-01-18 00:00:00.000000
SME	*ENABLED	2018-01-17 00:00:00.000000
FMICHIEL	*ENABLED	2018-01-15 00:00:00.000000
DGLENAT	*ENABLED	2017-11-24 00:00:00.000000
GLENATDEV	*ENABLED	2017-11-22 00:00:00.000000
YROEHRIG2	*ENABLED	2017-11-08 00:00:00.000000
BHERNANDEZ	*ENABLED	2017-09-28 00:00:00.000000
PMSOFTICF	*ENABLED	2017-09-18 00:00:00.000000
SMOLLE	*ENABLED	2017-08-17 00:00:00.000000

# Vue USER\_INFO (4)

- Nombre de tentatives de connexions infructueuses

```
SELECT *  
FROM QSYS2.USER_INFO  
WHERE SIGN_ON_ATTEMPTS_NOT_VALID > 0  
ORDER by SIGN_ON_ATTEMPTS_NOT_VALID DESC;
```

AUTHORIZATION_NAME	PREVIOUS_SIGNON	SIGN_ON_ATTEMPTS_NOT_VALID	STATUS	PASSWORD_CHANGE_DATE	NO_PASSWORD_INDICATOR	PA
MYSQL	-		162*DISABLED	2012-05-10 15:12:23.000000	NO	
AMTV2	2017-03-31 17:31:01.000000		7*DISABLED	2017-07-07 15:43:11.000000	NO	
GJARRIGE	2016-03-03 10:36:05.000000		4*DISABLED	2015-03-04 11:03:30.000000	NO	
SFTPUSER	2017-05-11 19:19:39.000000		2*ENABLED	2017-05-11 15:21:10.000000	NO	
SME	2018-01-17 16:09:17.000000		2*ENABLED	2017-04-14 16:29:05.000000	NO	
DSTBKP	-		1*DISABLED	2017-05-10 10:57:03.000000	NO	
WQADMIN	-		1*ENABLED	2013-06-20 10:44:07.000000	NO	

# Vue USER\_STORAGE

- Quantité de mémoire secondaire occupée par un utilisateur (Ko)
- Pour 1 profil

```
SELECT *
FROM QSYS2.USER_STORAGE WHERE
USER_NAME = 'DGAYTE'
```

AUTHORIZATION_NAME	ASPGRP	MAXIMUM_STORAGE_ALLOWED	STORAGE_USED
DGAYTE	*SYSBAS	-	197994752

- Pour tous les profils

```
SELECT user_name, aspgrp,
varchar_format(stgused,'999,999,999,999,999,999,999,
999')
AS "Espace Ko"
FROM qsys2.user_storage ORDER BY 3 DESC
```

USER_NAME	ASPGRP	Espace Ko
DGAYTE	*SYSBAS	197,994,752
QTMHHTTP	*SYSBAS	118,376,516
QSECOFR	*SYSBAS	85,685,312
QBRMS	*SYSBAS	61,805,184
QSYS	*SYSBAS	30,221,776
GDUMAS	*SYSBAS	12,250,044
PHPNOTOS	*SYSBAS	8,995,764

# UDTF DISPLAY\_JOURNAL

- Analyse un journal (DSPJRN)
- Très utile pour le journal d'audit
- Attention à la syntaxe des paramètres
  - Soit positionnels (doivent être dans l'ordre, sans en omettre)
  - Soit en utilisant le nom du paramètre et l'opérateur =>

```
SELECT *  
FROM TABLE(qsys2.display_journal('QSYS', 'QAUDJRN',  
STARTING_RECEIVER_NAME=> '*CURCHAIN',  
journal_entry_types=> 'PW',  
starting_timestamp=> CURRENT_TIMESTAMP -2400 HOURS  
) AS x;
```



AD	Auditing changes
AF	Authority failure
AX	Row and column access control
CA	Authority changes
CD	Command string audit
CO	Create object
CP	User profile changed, created, or restored
DO	Delete object
DS	DST security password reset
GR	Generic record
GS	Socket description was given to another job
LD	Link, unlink, or look up directory entry
OM	Object move or rename
OR	Object restore
OW	Object ownership changed
PA	Program changed to adopt authority
PG	Change of an object's primary group
PW	Invalid password
RA	Authority change during restore
RJ	Restoring job description with user profile specified
RO	Change of object owner during restore
RP	Restoring adopted authority program

# UDTF DISPLAY\_JOURNAL (2)

- Liste des défauts de mots de passe durant les 10 derniers jours

```
SELECT *  
FROM TABLE(qsys2.display_journal('QSYS', 'QAUDJRN',  
STARTING_RECEIVER_NAME=> '*CURCHAIN',  
journal_entry_types=> 'PW',  
starting_timestamp=> CURRENT_TIMESTAMP -240 HOURS  
) AS x;
```

ENTRY_TIMESTAMP	SEQUENCE_NUMBER	JOURNAL_CODE	JOURNAL_ENTRY_TYPE	COUNT_OR_RRN	ENTRY_DATA
2018-05-14 09:57:41.692608	291040T		PW		0E4C1C4D4C9D540404040405CD5404040404040404040...
2018-05-14 11:22:10.683648	380592T		PW		0D7C4C7C1E8E3C540404040D8D7C1C4C5E5F0F0F0F54040...

# UDTF DISPLAY\_JOURNAL (3)

- Suppression d'objets n'étant par des STMF

```
SELECT *  
FROM TABLE(qsys2.display_journal('QSYS', 'QAUDJRN',  
STARTING_RECEIVER_NAME=> '*CURCHAIN',  
journal_entry_types=> 'DO'  
) AS x  
WHERE OBJECT_TYPE <> '*STMF');
```

OBJECT	OBJECT_TYPE	OBJECT_TYPE_INDICATOR	FILE_TYPE_INDICATOR	JOURNAL_IDENTIFIER	CURRENT_USER	JOB_NAME
QPADEV0002QSYS	*DEVD	-	-	-	SMERINO	MENAGE
GSIRCV0346\$\$EDHJRN	*JRNRVC	-	-	-	SMERINO	MENAGE
GS1RCV0347\$\$EDHJRN	*JRNRVC	-	-	-	SMERINO	MENAGE
PMEDHR0360\$\$EDHJRN	*JRNRVC	-	-	-	SMERINO	MENAGE
PM1RCV0356\$\$EDHJRN	*JRNRVC	-	-	-	SMERINO	MENAGE
SMERCV0358\$\$EDHJRN	*JRNRVC	-	-	-	SMERINO	MENAGE
JRNRCV0082AMELIA	*JRNRVC	-	-	-	SMERINO	MENAGE
QSQJRN0816AMTV	*JRNRVC	-	-	-	SMERINO	MENAGE

# Vue SYSTOOLS.GROUP\_PTF\_CURRENCY

- Liste des groupes PTF's et comparaison avec ce qui est disponible

```
SELECT *  
FROM SYSTOOLS.GROUP_PTF_CURRENCY  
ORDER BY ptf_group_level_available - ptf_group_level_installed DESC;
```

PTF_GROUP_CURRENCY	PTF_GROUP_ID	PTF_GROUP_TITLE	PTF_GROUP_LEVEL_INSTALLED	PTF_GROUP_LEVEL_AVAILABLE	PTF_GROUP_LAST_UPDATED_BY_IBM
UPDATE AVAILABLE	SF99720	Current Cumulative PTF Media Documentation	17068	1803203/15/2018	
UPDATE AVAILABLE	SF99718	SF99718 720 Group Security	25	6305/01/2018	
UPDATE AVAILABLE	SF99719	SF99719 720 Group Hiper	89	12005/01/2018	
UPDATE AVAILABLE	SF99775	SF99775 720 Hardware and Related PTFs	2	3103/20/2018	
UPDATE AVAILABLE	SF99715	SF99715 720 Backup Recovery Solutions	18	4104/20/2018	
UPDATE AVAILABLE	SF99776	SF99776 720 High Availability for IBM i	1	904/05/2018	
UPDATE AVAILABLE	SF99713	SF99713 720 IBM HTTP Server for i	20	2704/27/2018	
UPDATE AVAILABLE	SF99702	SF99702 720 DB2 for IBM i	16	2102/07/2018	
UPDATE AVAILABLE	SF99717	SF99717 720 Technology Refresh	3	803/15/2018	
UPDATE AVAILABLE	SF99716	SF99716 720 Java	12	1604/11/2018	
UPDATE AVAILABLE	SF99747	SF99747 720 DB2 Web Query for i V2.1.0	14	1708/24/2017	
UPDATE AVAILABLE	SF99766	720 Print PTFs	2	301/07/2015	
UPDATE AVAILABLE	SF99767	SF99767 720 720 TCP/IP PTF	2	306/25/2016	

- Détail avec SYSTOOLS.GROUP\_PTF\_DETAILS

# UDTF QSYS2.HISTORY\_LOG\_INFO



- Equivalent de DSPLOG
- Liste des message de QHST depuis 1 jour

```
SELECT *  
FROM TABLE(QSYS2.HISTORY_LOG_INFO(CURRENT TIMESTAMP - 1 DAY)) A;
```

ID	MESSAGE_TYPE	MESSAGE_SUBTYPE	SEVERITY	MESSAGE_TIMESTAMP	FROM_USER	FROM_JOB	FROM_PRO
	INQUIRY	-	99	2018-05-14 06:51:03.882651	QSYS	058107/QSYS/QCMNARB02	QMHRMVM
	REPLY	MESSAGE DEFAULT USED	99	2018-05-14 06:51:03.882656	QSYS	000000/QSYS/SCPF	QMHRMVM
	INQUIRY	-	99	2018-05-14 06:51:03.908864	QSYS	058733/PHPNOTOS/LSTSBSSTS	QMHRMVM
	REPLY	MESSAGE DEFAULT USED	99	2018-05-14 06:51:03.908866	QSYS	000000/QSYS/SCPF	QMHRMVM
	INFORMATIONAL	-	0	2018-05-14 06:51:08.268959	QSYS	000000/QSYS/SCPF	QMHLOGER
	INFORMATIONAL	-	0	2018-05-14 06:51:09.352442	QSYS	000000/QSYS/SCPF	QWCISCFR

# Merci de votre attention !

Dominique GAYTE - NoToS  
*dgayte@notos.fr – www.notos.fr*

