Power Systems

Université IBM i

10 et 11 mai 2016 – IBM Client Center de Bois-Colombes

S40 – Les nouveautés sécurité IBM i de la 7.1 à 7.3

Mercredi 11 mai – 13h30-15h00

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

NoToS

- Expertise autour de l'IBM i
  - Sécurité
  - Regard moderne (DB2 Web Query)
- Service
  - Formation, audit, développement…
- PHP sur IBM i avec Zend
- Développement de progiciels
  - Modernisation à valeur ajoutée des IBM i

php.Spool
Valorisation des spools des IBM i (AS/400)
Transformation en PDF, archivage, indexation
http://www.notos.fr/phpSpool.aspx

LoReNa
Gestion de Contenu (ECM)
GED, graphiques, alertes, workflow, GANTT...
http://www.lorena.pro

Sommaire

- Profils utilisateur
- Authority Collection (V7R3)
- Base de données
  - RCAC (V7R2)
  - Field Procedure (V7R1)
- SSL
- SSO

Expiration du profil utilisateur

- Deux nouveaux paramètres en V7R1
- USREXPDATE : Mise hors fonction (*DISABLED) d'un profil utilisateur à une date donnée
  - *NONE : pas d'expiration
  - Date : date d'expiration (au format du JOB)
  - * USREXPITV : date calculée à partir du paramètre USREXPITV
- USREXPITV : durée avant expiration (en jours)
  - Entre 1 et 366

Authority Collection

Authority Collection

- 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

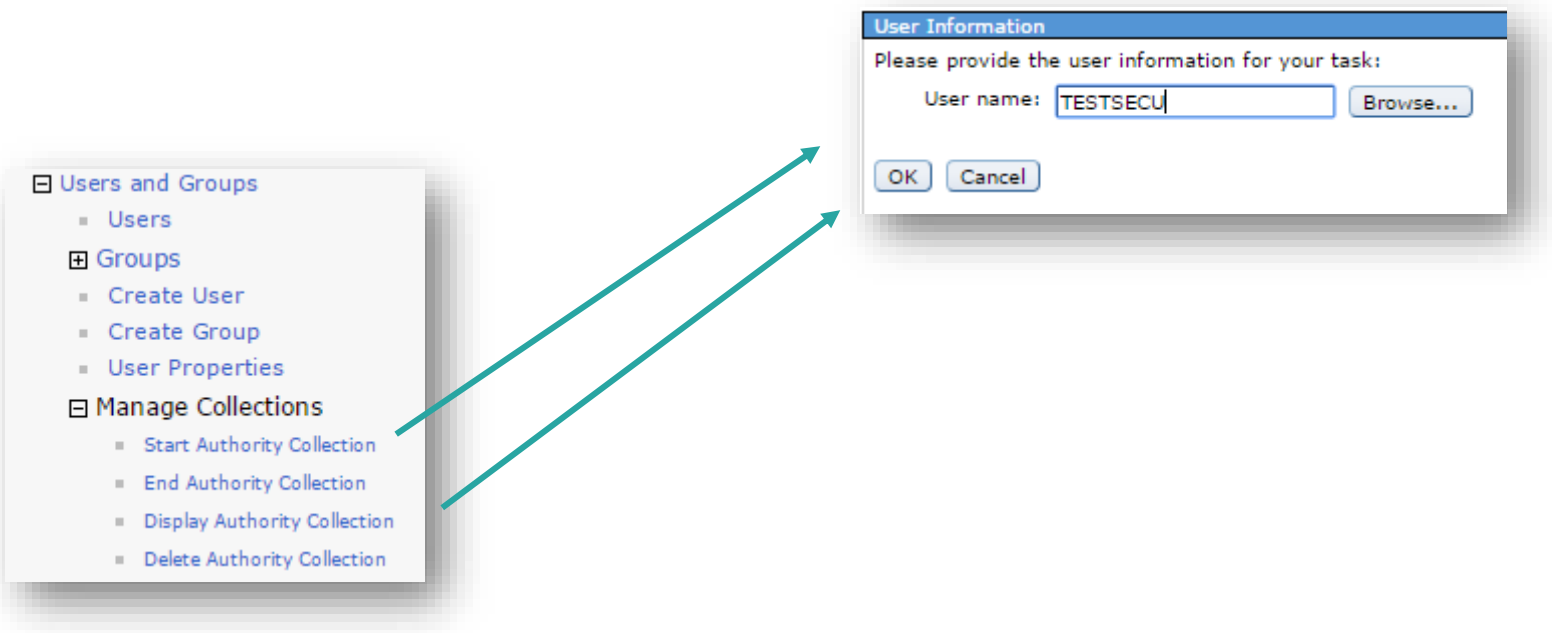
- Droits utilisés
  - Profil utilisateur
  - Groupes
  - Droits publics
  - Adoption de droits
- Sur tous types d'objets (et IFS)
- Une entrée est stockée dans la base données pour vérification des droits
- Attention à la charge du système
  - Mise en œuvre pour un profil
  - Tests
  - Arrêt
  - Analyse

Interfaces

- Commandes de l'IBM i
  - STRAUTCOL
  - ENDAUTCOL
  - DLTAUTCOL
  - DSPUSRPRF
  - DMPUSRPRF
  - RTVUSRPRF
- API
  - QSYRUSRI
- Navigator for i
- SQL (Vues)
  - QSYS2.AUTHORITY_COLLECTION
  - QSYS2.USER_INFO

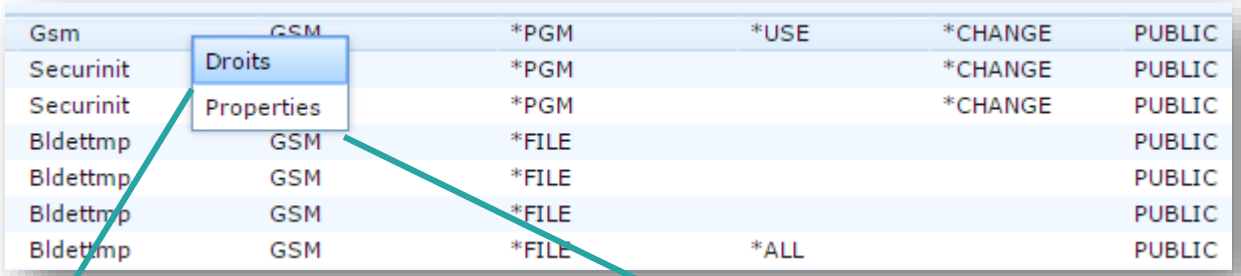
Navigator for i

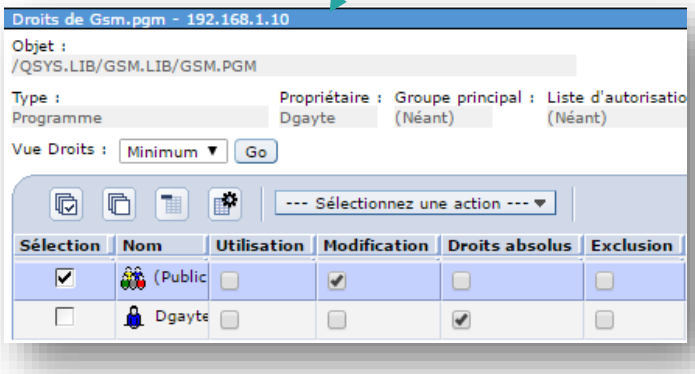
- Dans la gestion des utilisateurs
  - Manage Collections

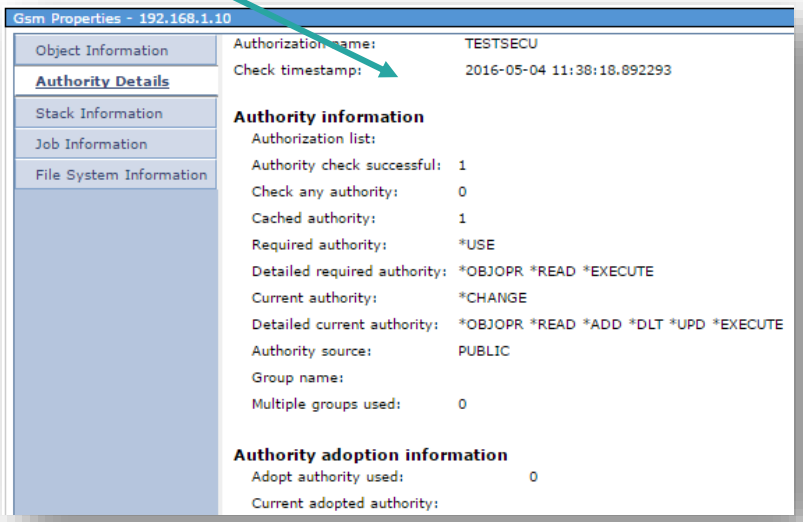


Affichage d'une collection

- Visualisation des droits utilisés pour accéder à l'objet

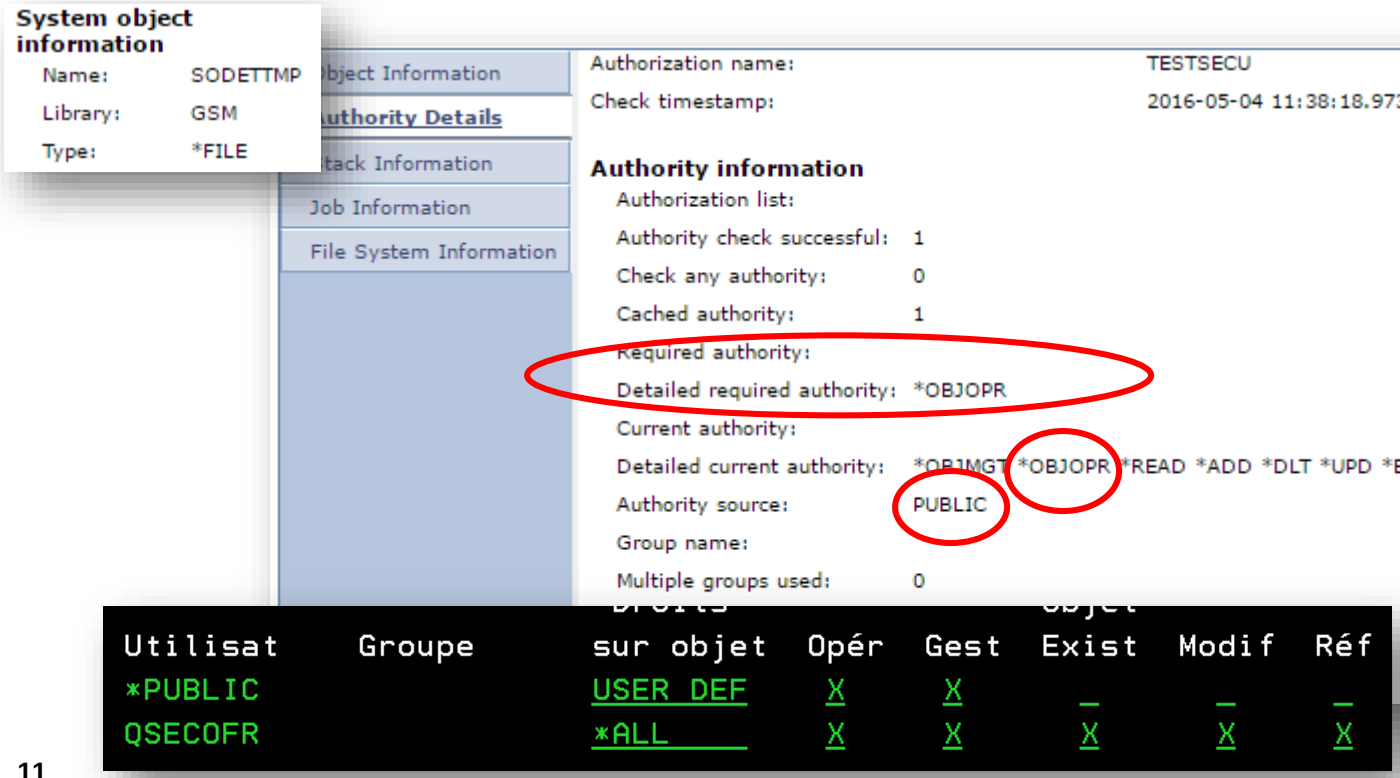






Propriétés

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



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
Famdsp	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	AUTHORIZATION LIST PUBLIC	ADOPTED *ALLOBJ	*ALL	x
Securinit	GSM	*PGM		*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

Utilisation de SQL

- Pour extraire les données à partir des vues
  - QSYS2.AUTHORITY_COLLECTION
  - QSYS2.USER_INFO
- Liste des échecs pour le profil utilisateur TESTSECU

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

AUTHORIZATION_N...	CHECK_TIMESTAMP	SYSTEM_OBJECT_N...	SYSTEM_OBJECT_SCH...	SYSTEM_OBJECT_T...	ASP_NAME	ASP_NUM...	OBJECT_NAME
TESTSECU	2016-05-04 14:43:04.672636	GSM	GSM	*PGM	*SYSBAS	0	GSM
TESTSECU	2016-05-04 14:43:04.672623	GSM	GSM	*PGM	*SYSBAS	0	GSM
TESTSECU	2016-05-04 14:41:57.761403	GSM	GSM	*PGM	-	-	GSM
TESTSECU	2016-05-04 14:41:57.761381	GSM	GSM	*PGM	-	-	GSM

- Liste des utilisateurs ayant une collection

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

AUTHORIZATION_N...	AUTHORITY_COLLECTION_REPOSITORY_EXI...
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

RCAC

RCAC

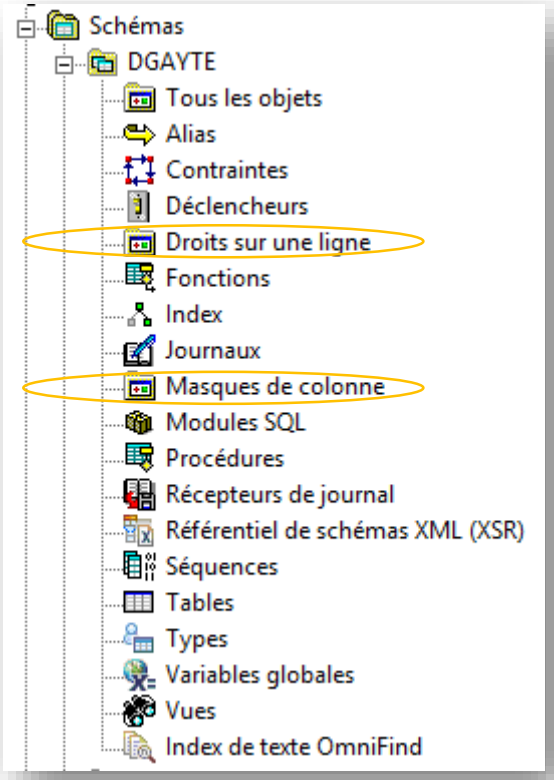
- Row and Column Access Control
- Option 47 de SS1
  - IBM Advanced Data Security for i
  - Non factorable
  - V7R2
- RCAC permet de limiter l'accès à certaines données de type ligne et/ou colonne, aux seules personnes (ou groupes de personnes) qui sont habilitées à connaître le contenu de ces données
- RCAC utilise deux approches
  - Des permissions sur les lignes
  - Des masques sur les colonnes

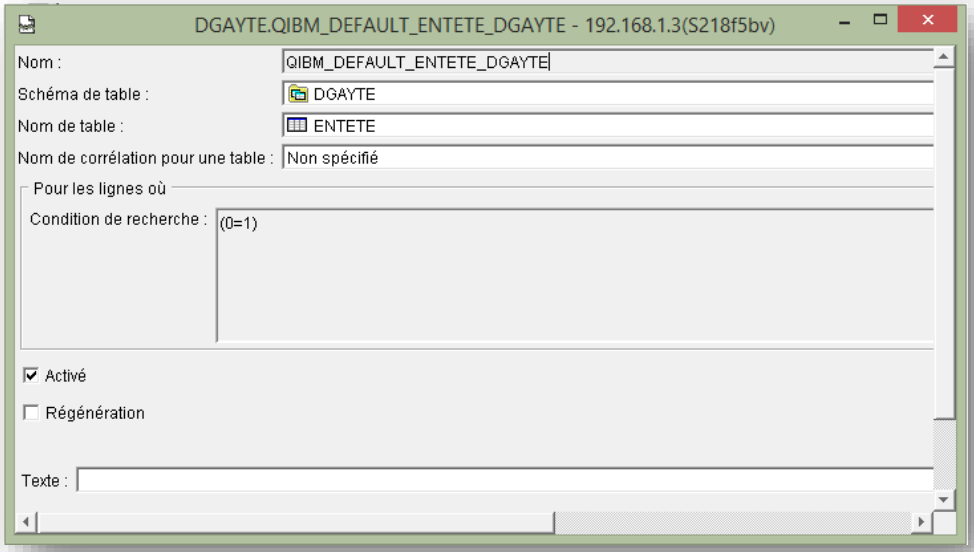
RCAC (2)

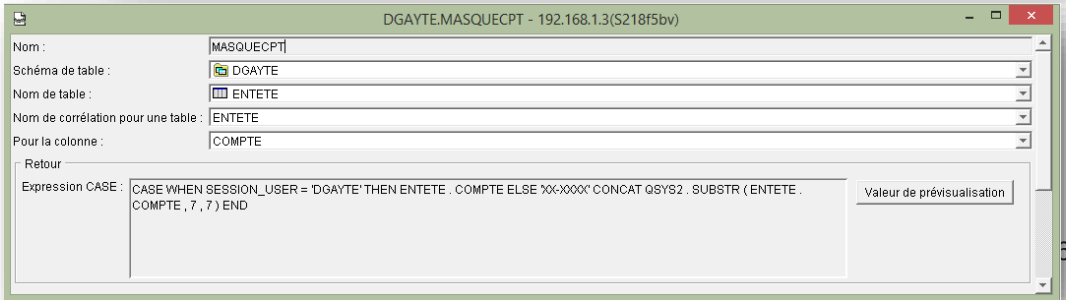
- Même les utilisateurs qui ont des droits *ALLOBJ ne peuvent passer outre les autorisations qui ont été définies au travers de RCAC
- Transparent pour les applications utilisant la base de données
  - Attention avec les mises à jour
- Fonctionne aussi en mise à jour
  - Interdiction d'écrire une donnée qui n'est pas autorisée par RCAC

System i Navigator

- Nouvelles options
- SP à appliquer (SI56695)

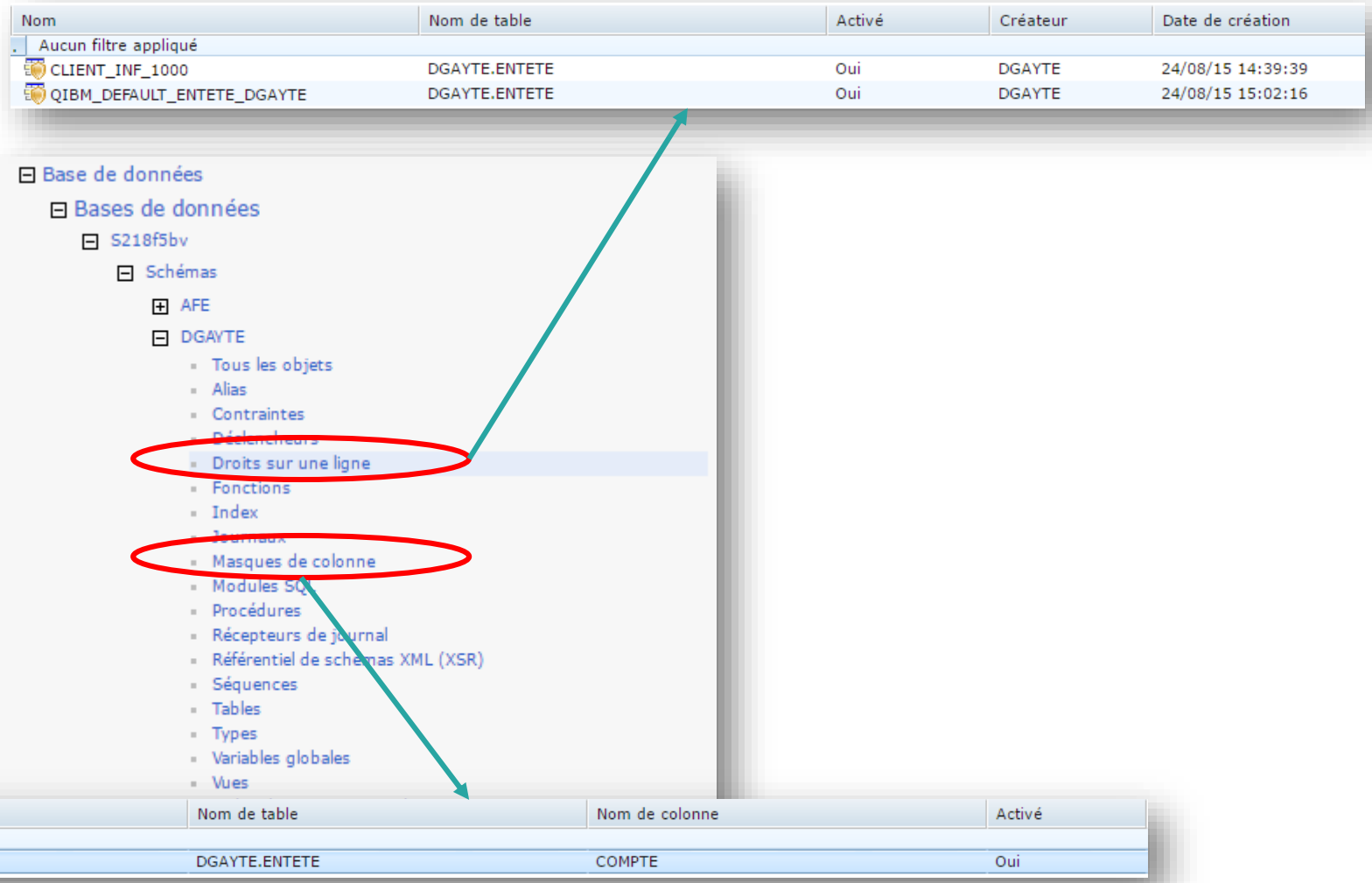






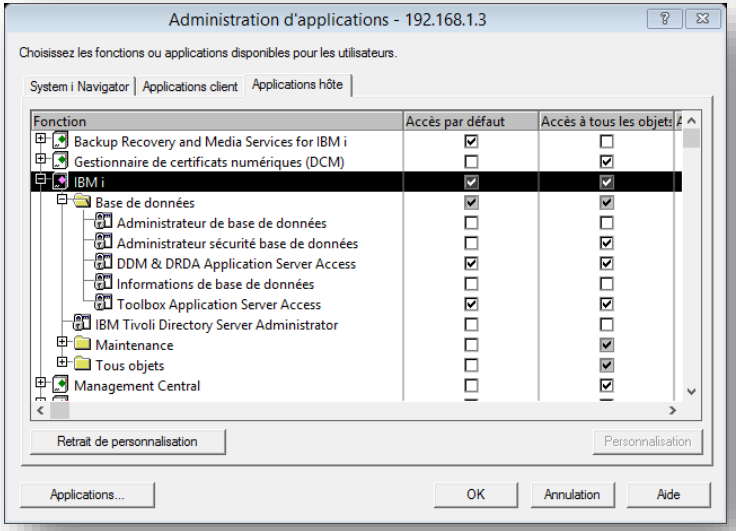
Navigator for i

- Disponible dans l'interface



Sécurité RCAC

- L'utilisateur qui crée la RCAC doit être administrateur de la base de données (même QSECOFR)
  - Sinon SQL0552
- Par la commande WRKFCNUSG
  - Fonction QIBM_DB_SECADM
- Ou par System i Navigator
  - Administration d'applications/Applications hôte



Sécurité RCAC

- Droits attribués à un utilisateur
- A tout le monde
- Aux profils *ALLOBJ

```
                  Modifier utilisation fonction (CHGFCNUSG)

Indiquez vos choix, puis appuyez sur ENTREE.

ID fonction  . . . . . . . . . . > QIBM_DB_SECADM
Utilisateur  . . . . . . . . . . > DGAYTE       Nom
Utilisation  . . . . . . . . . . > *ALLOWED     *ALLOWED, *DENIED, *NONE
Droit par défaut . . . . . . . .   *DENIED      *SAME, *ALLOWED, *DENIED
Droit spécial *ALLOBJ  . . . . .   *NOTUSED     *SAME, *USED, *NOTUSED
```

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 DGAYT
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

Exemple colonne (2)

- Même chose avec DFU
- Avec QSECOFR

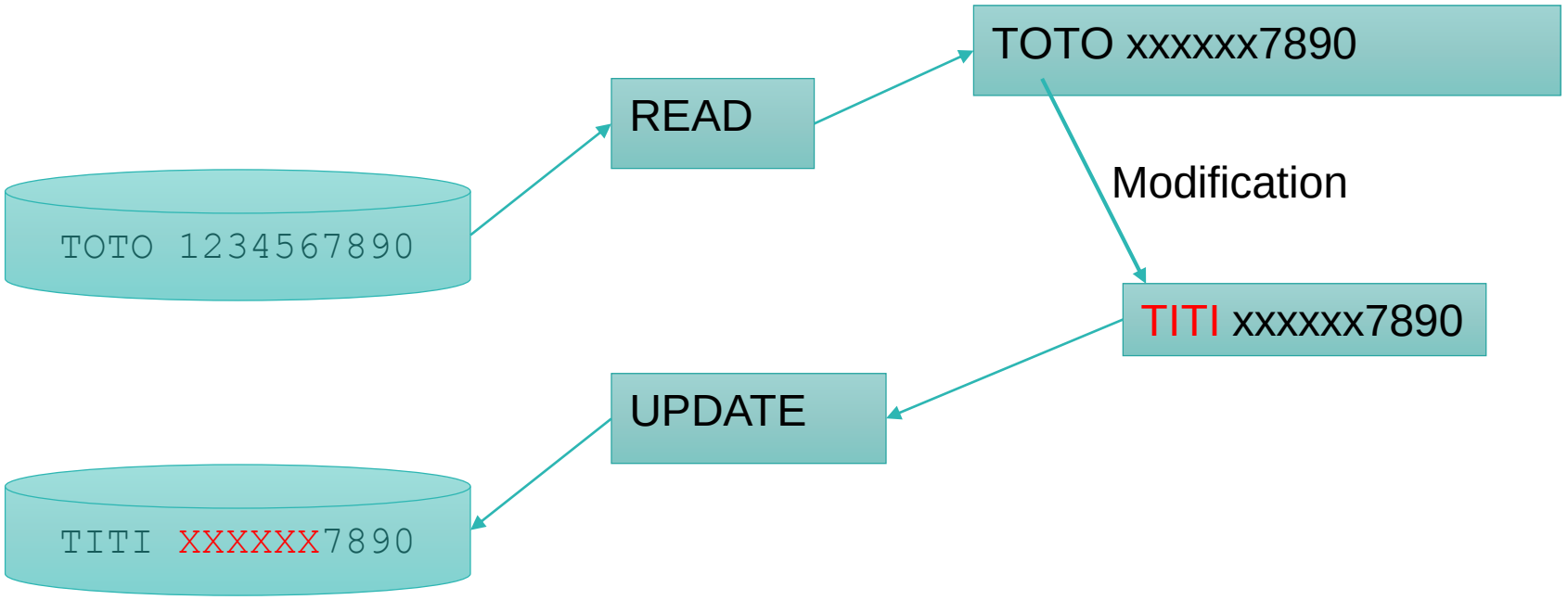
```
GESTION DE DONNEES D'UN FICHIER                Mode . . . . :   MODIFICATION
Format . . . . :   ENTETE2                     Fichier  . . :   ENTETE

*RECNBR:          1
CLIENT:         676
TOTAL:      272315495
NUMCDE:         43659
SUBTOTAL:   246439362
TAXES:       19715149
PORT:         6160984
COMPTE:    XX-XXXX-000676
DATECDE:   2001-07-01
```

Syntaxe (2)

- Désactivation temporaire
  - Ligne
    - ALTER TABLE client DEACTIVATE ROW ACCESS CONTROL;
  - Colonne
    - ALTER TABLE client DEACTIVATE COLUMN ACCESS CONTROL;
- Suppression
  - DROP MASK | PERMISSION
- Modification
  - ALTER MASK | PERMISSION

Mises à jour accidentelles

- En RPG, COBOL… possibilité de mises à jour accidentelles sur des colonnes en partie masquées



Commandes

- Les droits RCAC sont stockés dans la table elle-même
  - Ils sont donc sauvegardés par SAVLIB et SAVOBJ, déplacés par MOVOBJ, dupliqués (par défaut) par CRTDUPOBJ
- Une table (ou fichier physique) avec des droits RCAC ne peut pas être sauvegardée dans une version d'OS précédente
- Une table (ou fichier physique) avec des droits RCAC, restaurée sur un système ne possédant pas l'option 47 ne peut plus être ouverte
- Pour voir la liste des droits RCAC existants, regarder le contenu des tables systèmes SYSCONTROLS et SYSCONTROLSDEP de QSYS2

CRTDUPOBJ

- Nouveau paramètre ACCCTL (Access Control)
  - Valeur *ALL obligatoire si RCAC sur la table
- Les RCAC sont copiées
- Toutes les lignes sont copiées, même celles qui ne sont pas autorisées
- Les colonnes non masquées sont copiées

CPYF

- Ne copie que les données ! Pas RCAC
- Seules les données permises sont copiées
  - Lignes autorisées
  - Colonnes masquées
- Idem pour CPYTOIMPF

Journalisation

- Les données dans les journaux sont des données brutes, non masquées
- Il faut protéger les journaux (et récepteurs) afin d'éviter le contournement de la sécurité apportée par RCAC

Jointures SQL

- RCAC intervient après la jointure
- Donc pas de soucis de résultats
- Mais il faut réfléchir aux différents cas selon que RCAC soit défini sur la table de gauche, de droite ou les deux

Field Procedure

DB2 : *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
  - Ou partiellement
- Apparu 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
  - Syntaxe dans l'éditeur de script de System i Navigator

```
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

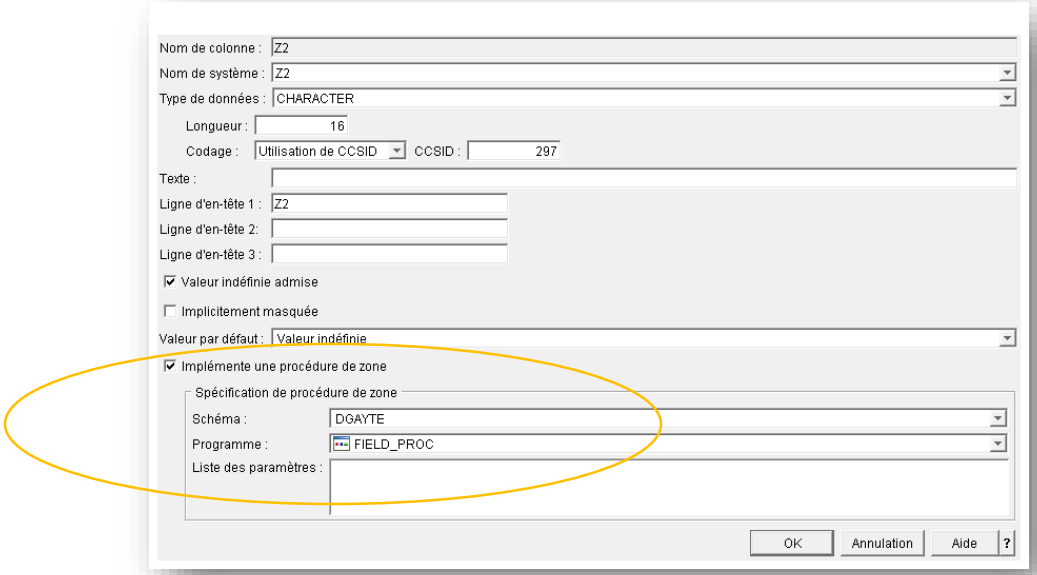
Z1	Z2
1	****56789012345
2	****654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

Visualisation

- System i Navigator



- DSPFFD

```
Informations de niveau zone
             Type          Long  Long    Position          Usage     En-tête
  Zone       données       zone  tampon tampon            zone      colonne
  Z1         BINAIR        9  0       4          1         E-S       Z1
    Accepte la valeur indéfinie
  Z2         ALPHA           16      16         5         E-S       Z2
    Accepte la valeur indéfinie
    ID codé de jeu de caractères    . . . . . :    297
    Nom procédure zone    . . . . . . . . . . :  FIELD_PROC
      Biblio. procédure zone  . . . . . . . . :  DGAYTE
```

Utilisation

- Dans notre exemple, où seul QSECOFR peut voir les données complètes

QSECOFR		Navigator	Autre	
Z1	Z2		Z1	Z2
1	123456789012345		1	*****6789012345
2	3210654987123122		2	*****654987123122

```
Z1    Z2
 1    123456789012345
 2    3210654987123122
```

STRSQL

```
Z1    Z2
 1    *****67890123456
 2    *****54987123122
```

```
*...+....1....+....2
     1234567890123456
     3210654987123122
```

DSPPFM

```
*...+....1....+....2
     *****67890123456
     *****54987123122
```

```
Données spécifiques du poste
*...+....1....+....2....+...
'    123456789012345 '
```

DSPJRN

```
Données spécifiques du poste
*...+....1....+....2....+...
'    *****6789012345 '
```

Mises à jour

- Attention aux mises à jour !
- Selon le profil l'UPDATE SQL ne fonctionne pas s'il y a une condition sur la zone cryptée

```
select dgayte/fieldproc
SET z1 = 10
WHERE z2 like '123%'
```

- Dans notre exemple, problème si le profil ne voit pas les premiers caractères (***)
- Les profils non autorisés ne voient que des '*' pas '123'

SSL

SSL

- SSL est utilisé pour crypter les données qui circulent sur le réseau
- On devrait parler de TLS
- Voir la présentation de S28 de 2013
- Valeurs système qui permettent de spécifier les algorithmes et protocoles supportés
  - QSSLCSL, QSSLCSLCTL, QSSLPCL
  - Les valeurs *OPSYS de QSSLCSLCTL et de QSSLPCL indiquent que se sont les valeurs associées à la version de l'IBM i qui sont prises en compte

SSL (2)

- En V7R2, SSL V3 est désactivé par défaut
- Peut être réactivé avec la valeur système QSSLPCL
- Réorganisation de l'ordre des algorithmes de chiffrement
  - MD5 déclassé, ECDSA/ECDHE en premier (
    - Elliptic Curve Digital Signature Algorithm
    - Elliptic Curve Diffie-Hellman Ephemeral
  - Sysval : QSSLCSL et QSSLCSLCTL

```
10        *ECDHE_ECDSA_AES_128_CBC_SHA256
20        *ECDHE_ECDSA_AES_256_CBC_SHA384
30        *ECDHE_ECDSA_AES_128_GCM_SHA256
40        *ECDHE_ECDSA_AES_256_GCM_SHA384
50        *RSA_AES_128_CBC_SHA256
60        *RSA_AES_128_CBC_SHA
```

SSO

Single Sign On

SSO/EIM

- EIM permet la mise en œuvre d'un Single Sign On dans un environnement Kerberos
- Par exemple avec un Active Directory
- Voir la session S28 de 2014

Nouveautés SSO/EIM

- Utilisation d'AES (*Advanced Encryption Standard*) à la place de DES (*Data Encryption Standard*)
- Cryptage à clés symétriques
- AES est plus solide que DES
  - N'a pas été cassé à ce jour (!)
  - Clé de 128 à 256 bits (56 pour DES)
- DES n'est plus standard sous Windows
- PTF
  - V7R1: SI42919 and SI43918
  - V6R1: SI42957 and SI43919
  - V5R4: SI43034 and SI43920

EIM V7R2

- En V7R2 les applications suivantes peuvent être intégrées à EIM
- FTP client et Serveur
- Telnet client (commande TELNET ou STRTCPTELN)
  - Valeur RMTUSER(*KERBEROS)
  - Utiliser kinit (QSHELL) ou la commande ADDKRBTKT pour renouveler le ticket

EIM V7R2 (2)

- FTP
- Il faut ajouter le principal Kerberos
  - Créer le compte de service dans l'AD pour ftp/hostname@domaine
- Créer les clés coté IBM i
  - keytab add ftp/hostname@domaine
- FTP client
  - FTP RMTSYS(hostname) SECCNN(*KERBEROS)

Power Systems

for Business

Merci pour votre écoute !

Des questions ?

Dominique GAYTE - dgayte@notos.fr
04 30 96 97 33
www.notos.fr

IBM