Université IBM i 2017

17 et 18 mai – IBM Client Center de Bois-Colombes

S14 - Sécuriser les accès distants à DB2

Mercredi 17 mai – 16h00-17h30

Dominique GAYTE
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

php.spool lorena monitor i distant.backup

Sécurité de la base de données

- Historiquement
  - Les accès à la base de données étaient sécurisés par les applications
  - On ne pouvait accéder aux données qu'à travers les applications 5250 (écrans twinax)
  - Les options de menus donnaient l'accès aux actions autorisées
  - Les objets de la base de données étaient peu (pas !) sécurisés
- Aujourd'hui
  - L'IBM i est un système ouvert
  - On accède aux données de nombreuses manières
    - Par le réseau
    - Sans passer par les applications historiques

La Sécurité aujourd'hui

- Il faut revoir l'organisation de la Sécurité sur le réseau
- Ne plus faire confiance seulement au seul pare-feu externe
- Chaque niveau, chaque élément doit être sécurisé
  - Les « objets », notamment la base de données
  - Les applications
  - Les serveurs
  - Les communications
  - Les composants du réseau
- Arrivée du GDPR (RGPD)
  - La protection des données personnelles devient une obligation !

Les objectifs

- Renforcer la Sécurité d'accès aux objets
- Chiffrer les communications (et les données ?)
- Limiter l'exposition des données sur le réseau
- …

Renforcer la Sécurité des objets

Avant tout

- Il faut sécuriser les objets de la base de données
- Eviter les profils utilisateur disposant de *ALLOBJ
- Utiliser les listes d'autorisation et les profils de groupe pour simplifier la mise en œuvre
- Travailler au niveau de la bibliothèque
  - *EXCLUDE ne permet pas de voir le contenu
- Eviter les droits publics pour les objets de la BD
  - Par défaut *CHANGE
  - Devrait être *EXCLUDE
- Voir mes séminaires des années précédentes

Droits publics

- Paramètre AUT des commandes de création

```
 Créer un fichier physique (CRTPF)

 Indiquez vos choix, puis appuyez sur ENTREE.

 Groupe de noeuds . . . . . .   *NONE          Nom, *NONE
   Bibliothèque . . . . . .                    Nom, *LIBL,
*CURLIB
 Clé de partitionnement . . . . .              Nom
              + si autres valeurs
 Droits . . . . . . . . . . . . .   *LIBCRTAUT     Nom,
*LIBCRTAUT, *ALL...
```

F4

```
Créer une bibliothèque (CRTLIB)

                          Autres paramètres

Droits . . . . . . . . . . . . . . . AUT           *LIBCRTAUT
Droits pour objets créés . . . . . CRTAUT         *SYSVAL
Audit pour objets créés  . . . . . CRTOBJAUD      *SYSVAL
```

Valeur Système **QCRTAUT** *CHANGE

Ne pas donner de droits permanents aux utilisateurs !

- Liste d'autorisation avec
  - *PUBLIC *EXCLUDE
  - GRPLECT *USE groupe pour la lecture directe
  - GRPMODIF *CHANGE groupe pour la modification directe
- Protéger la bibliothèque et les objets avec cette liste
- Le propriétaire des objets est le propriétaire des programmes
  - Il n'a aucun droit spécial (*JOBCTL ou *SPLCTL parfois)
- Utiliser la délégation de droits et l'héritage
  - USRPRF (*OWNER) pour les programme point d'entrée
  - USEADPAUT(*YES) pour les autres (valeur par défaut)
- Attention aux programmes qui contiennent du SQL à recréer
  - CRTSQLRPGI …. DYNUSRPRF(*OWNER)
  - CRTPGM … USRPRF(*OWNER) (avec des modules)

Authority Collection

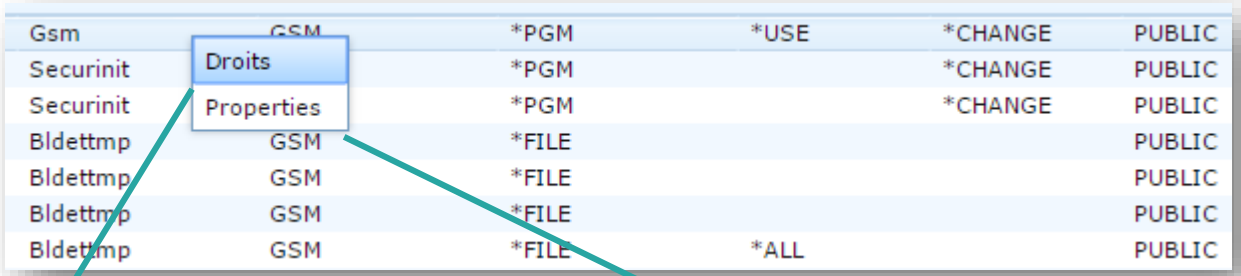
- Fonction qui permet à l'administrateur de la Sécurité de mieux comprendre les mécanismes d'attributions des droits réellement mis en œuvre dans le cadre d'une application
- Utile pour n'octroyer que les droits nécessaires aux utilisateurs
- Intégré à l'IBM i (V7R3) (et au microcode)
- Capture d'informations 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

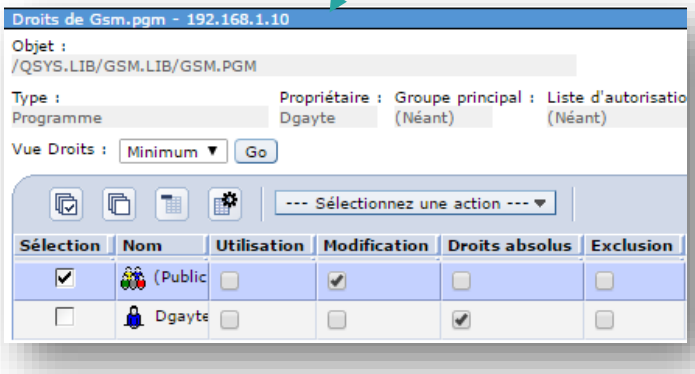
Ce qui est analysé

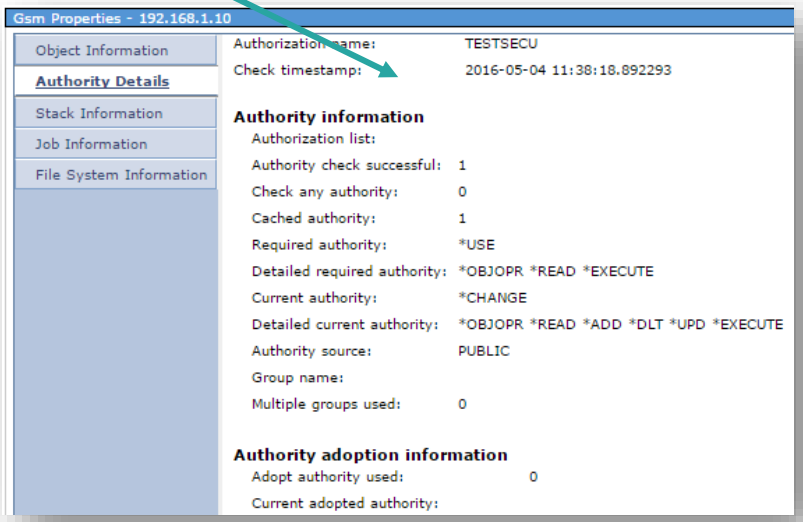
- Droits utilisés
  - Profil utilisateur
  - Groupes
  - Droits publics
  - Adoption de droits
- Sur tous types d'objets (et IFS)
- Une entrée est stockée dans la base données pour vérification des droits
- Attention à la charge du système
  - Mise en œuvre pour un profil
  - Tests
  - Arrêt
  - Analyse

Affichage d'une collection

- Visualisation des droits utilisés pour accéder à l'objet

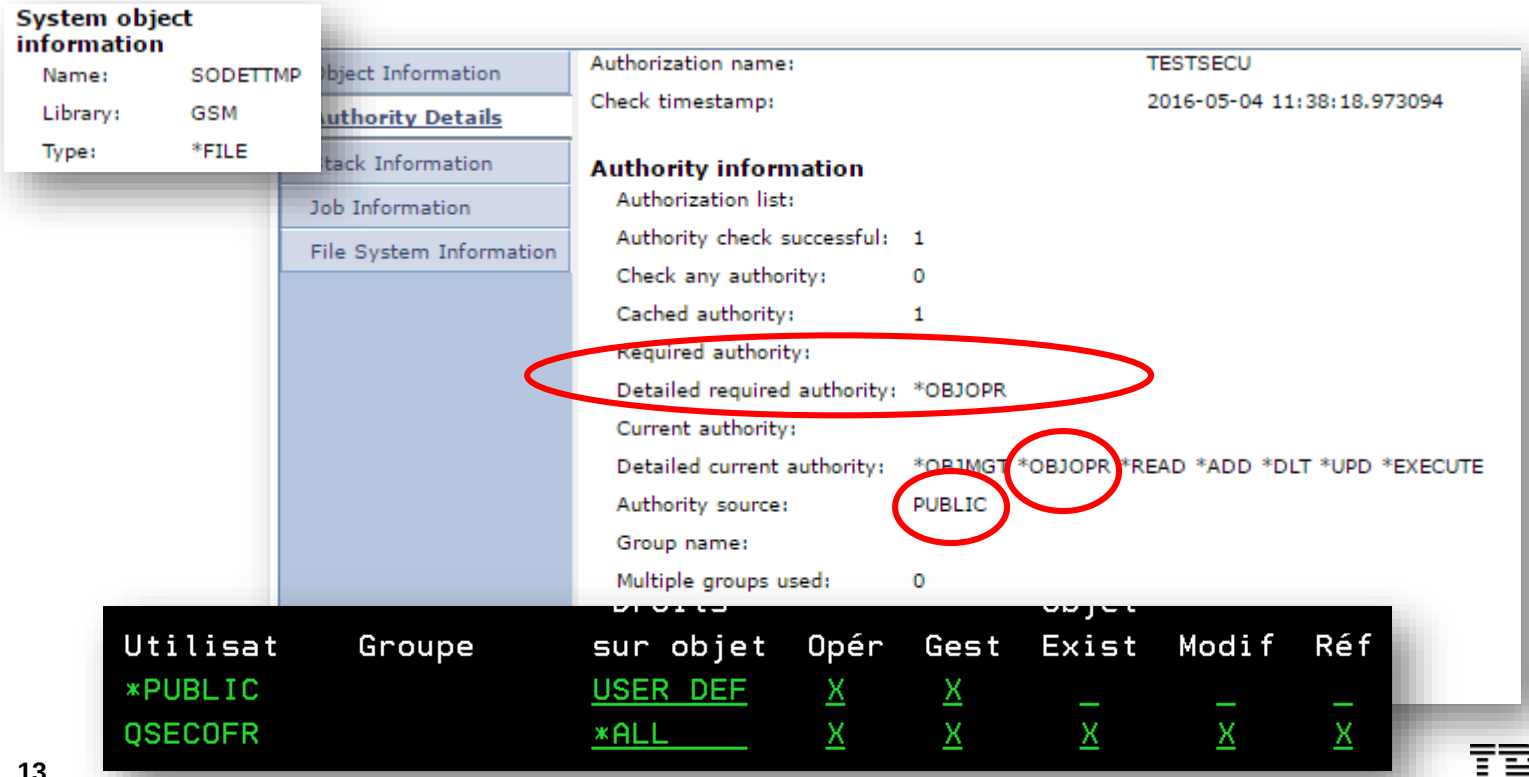






Propriétés

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



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
```

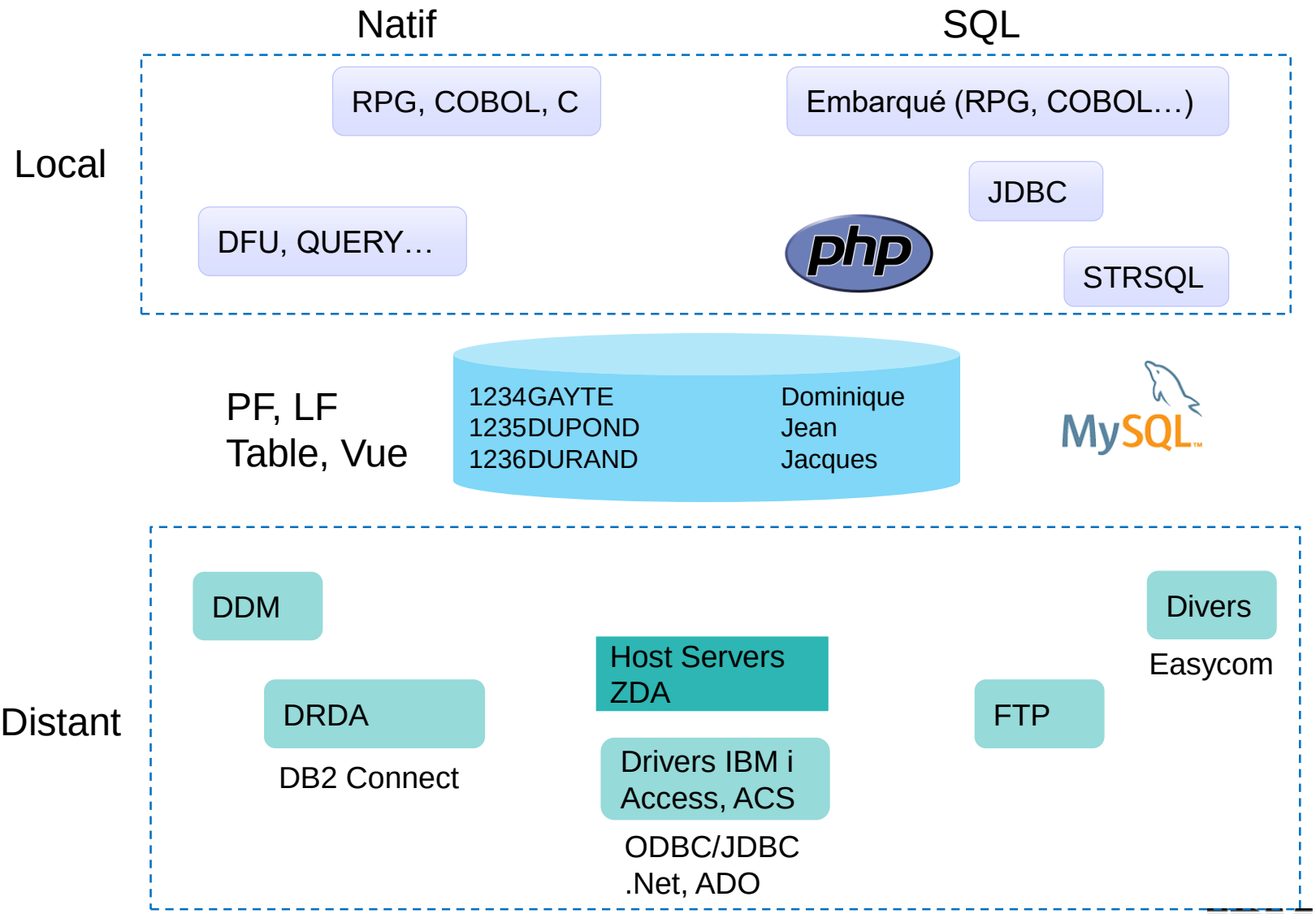
AUTHORIZATION_N...	CHECK_TIMESTAMP	SYSTEM_OBJECT_N...	SYSTEM_OBJECT_SCH...	SYSTEM_OBJECT_T...	ASP_NAME	ASP_NUM...	OBJECT_NAME
TESTSECU	2016-05-04 14:43:04.672636	GSM	GSM	*PGM	*SYSBAS	0	GSM
TESTSECU	2016-05-04 14:43:04.672623	GSM	GSM	*PGM	*SYSBAS	0	GSM
TESTSECU	2016-05-04 14:41:57.761403	GSM	GSM	*PGM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

Les interfaces d'accès à DB2 for i



DDM & DRDA

- Accès à des données sur un système distant
  - Au niveau enregistrement (DDM)
    - CRTDDMF pour pointer sur le fichier distant comme s'il était en local
  - SQL (DRDA)
    - WRKRDBDIRE pour définir la BD distante
    - CONNECT TO pour se connecter à la BD distante
    - Ensuite SQL comme si on était en local
- STRTCPSVR SERVER(*DDM)
  - Ports 446, 447 et 448

```
*                    *              drda        000:53:38   Listen   446
*                    *              ddm         003:45:20   Listen   447
*                    *              ddm-ssl     003:45:20   Listen   448
```

  - Travaux QRWTLSTN & QRWTSRVR de QSYSWRK

DDM & DRDA et la Sécurité

- Commande CHGDDMTCPA
  - AUTOSTART : ne pas démarrer automatiquement si inutile
  - PWDRQD : le mot de passe peut ne pas être demandé ! Connexion automatique sans mot de passe si le profil existe déjà sur le système cible. Ne pas utiliser les valeurs suivantes :
    - *USRID ou *NO : par défaut (plus en V7R3), pas de demande de PWD
    - *VLDONLY : il n'est pas obligatoire mais est vérifié s'il est fourni

```
                Modifier attributs TCP/IP DDM (CHGDDMTCPA)

Indiquez vos choix, puis appuyez sur ENTREE.

Serveur à démarrage auto . . . . AUTOSTART      *YES
Méthode authent la plus basse  . PWDRQD         *USRID
Algor. chiffrement le plus bas   ENCALG         *DES
```

    - Le mot de passe circule en clair : utiliser la valeur *USRIDPWD et forcer ENCALG(*AES)
- Attention ! Il est possible d'exécuter une commande sur le système distant
  - SBMRMTCMD
- On peut utiliser un point d'exit pour valider la connexion
  - Paramètre DDMACC de CHGNETA

Host Servers

- Utilisés par les applications clientes (IBM i Access, ACS, System i Navigator, ODBC, JDBC…)
- Server Mapper, port 449, PZSOSMAPD
- Signon Server, port 8476 & 9476, QZSOSIGN & QZSOSGND
- Central Server, port 8470 & 9470, QZSCSRVS & QZSCSRVSD
- Database server, port 8471 & 9471, QZDA*
- Remote Commande Server, port 8475 & 9475, QZRCSRVS & QZRCSRVSD
- …
- STRHOSTSVR SERVER(*DATABASE) ou *ALL

Mot de passe & Host Servers

- Ces fonctions sont intégrées au SSO avec EIM
  - Pas d'échange de mot de passe
  - C'est un ticket Kerberos crypté qui transite indiquant que l'authentification a été réalisée au niveau du serveur Kerberos (Active Directory, par exemple)
- Le mot de passe des Host Servers ne circule pas en clair
- Mais les données, elles, circulent en clair
  - Chiffrement…

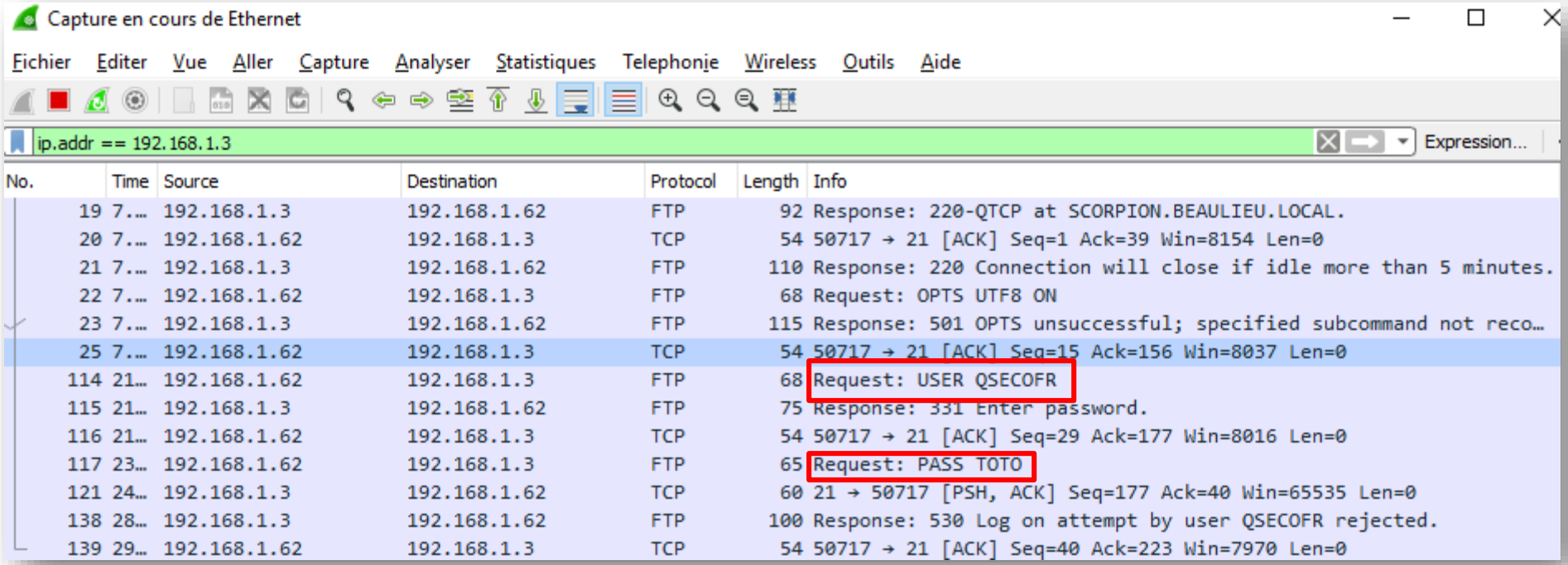
Chiffrement

Connexion et données

Chiffrement de la connexion

- Connexions classiques aux IBM i sont non sécurisées
  - Emulation écran, FTP
  - ID et mot de passe circulent en clair
- Un simple test !
  - FTP vers un IBM i
  - Traces avec WireShark (par exemple)
  - ID et PWD en clair (et les données aussi !)
  - En TELNET (PC5250) à peine plus complexe
    - EBCDIC
- Voir présentation de 2013
  - S28 - La mise en œuvre de SSL afin de sécuriser les connexions avec un IBM i

WireShark : FTP



Power Systems

WireShark : Telnet

Capture en cours de Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 192.168.1.3 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
188	30…	192.168.1.3	239.255.255.253	SRVLOC	91	Service Request, V2 XID - 223
453	87…	192.168.1.62	192.168.1.3	TN5250	68	TN5250 Data to Mainframe[Malformed Packet]
454	87…	192.168.1.3	192.168.1.62	TCP	60	23 → 50414 [PSH, ACK] Seq=2248 Ack=257 Win=65535 Len=0
455	87…	192.168.1.3	192.168.1.62	TN5250	66	TN5250 Data from Mainframe
456	87…	192.168.1.62	192.168.1.3	TN5250	66	TN5250 Data to Mainframe
457	87…	192.168.1.3	192.168.1.62	TCP	60	23 → 50414 [PSH, ACK] Seq=2260 Ack=269 Win=65535 Len=0
458	87…	192.168.1.3	192.168.1.62	TN5250	68	TN5250 Data from Mainframe
459	87…	192.168.1.62	192.168.1.3	TN5250	3395	TN5250 Data to Mainframe[Malformed Packet]
460	87…	192.168.1.3	192.168.1.62	TCP	60	23 → 50414 [PSH, ACK] Seq=2274 Ack=3610 Win=65535 Len=0
461	87…	192.168.1.3	192.168.1.62	TN5250	558	TN5250 Data from Mainframe
462	87…	192.168.1.62	192.168.1.3	TCP	54	50414 → 23 [ACK] Seq=3610 Ack=2778 Win=525056 Len=0
570	10…	192.168.1.62	192.168.1.3	TN5250	86	TN5250 Data to Mainframe
571	10…	192.168.1.3	192.168.1.62	TCP	60	23 → 50414 [PSH, ACK] Seq=2778 Ack=3642 Win=65535 Len=0

```
> Frame 570: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: AsustekC_d5:ee:85 (60:a4:4c:d5:ee:85), Dst: Ibm_5d:02:f9 (40:f2:e9:5d:02:f9)
> Internet Protocol Version 4, Src: 192.168.1.62, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 50414, Dst Port: 23, Seq: 3610, Ack: 2778, Len: 32
v Telnet
  > TN5250 Protocol
  v End of Record
      Command: End of Record (239)
```

```
0000  40 f2 e9 5d 02 f9 60 a4  4c d5 ee 85 08 00 45 00    2Z).9-u <N.e....
0010  00 48 46 4a 40 00 80 06  00 00 c0 a8 01 3e c0 a8   .... ... ..{y..{y
0020  01 03 c4 ee 00 17 46 9e  e1 b5 d0 c0 b2 c2 50 18   ..D..... ..}{.B&.
0030  08 03 83 cc 00 00 00 1e  12 a0 00 00 04 00 80 03   ..c..... ........
0040  07 39 f1 11 06 35 d8 e2  c5 c3 d6 c6 d9 11 07 35   .91..5QS ECOFR..5
0050  e3 d6 e3 d6 ff ef                                 TOTO..
```

```
..c..... ........
.91..5QS ECOFR..5
TOTO..
```

SSL : *Secure Socket Layer*

- C'est un protocole de sécurisation des échanges sur Internet
  - A utiliser à partir de V3.0
- TLS (*Transport Layer Security*) est la nouvelle version
  - TLS 1.0 équivalent de SSL 3.1
- Création d'un « tunnel » dans lequel les informations circulent cryptées
- Possibilité de s'assurer de l'identité du serveur et du client
- S'appuie sur des certificats émis par des autorités de certification (CA)

SSL et IBM i

- L'IBM i dispose en standard de tout ce qui faut pour SSL
- DCM (Digital Certificate Manager) pour la gestion en graphique des certificats (SS1 option 34)
- Les serveurs IBM i le supporte
  - Telnet, FTP
  - HTTP
  - IBM i Access for Windows
  - LDAP, DRDA…
- Les clients standard IBM i le supporte
  - IBM i Access for Windows
  - ACS

Chiffrement des données

- Au niveau de l'ASP
- Au niveau de la zone de la base de données
  - Field procedure
- Est-ce utile pour sécuriser les accès distants ?

Car c'est transparent ! C'est le moteur de base de données qui déchiffre.
Les données nous apparaissent toujours en clair, sauf si on court-circuite DB2 for i !

Limiter les données exposées

Fichiers logiques et Sécurité

- Les fichiers logiques (vues) peuvent être utilisés pour limiter les données exposées
- Interdire tous les droits sur les données d'un fichier physique (table)
  - Droits d'opération nécessaires
- Créer un logique (vue) sur ce fichier
  - Sélection d'enregistrements
  - Choix de colonnes
  - Adapter les droits sur les données
- L'utilisateur qui a accès au logique (vue) ne voit que la partie des données utile à son travail
- Mais c'est plutôt une ancienne méthode…

LF, Vues et Sécurité

12349	3450
12351	2500
12352	2500

SELECT NUMSAL, SALAIRE
FROM EMPLOYE
WHERE SALAIRE > 2400

SELECT NUMSAL, CONGES
FROM EMPLOYE

12345	15
12346	22
12347	2
12348	22
12349	33
12350	22
12351	12
12352	11

12345	DUPONT	Jean	2000	15
12346	DUPONT	Aline	2100	22
12347	DURAND	Patrick	1500	2
12348	GAYTE	Dominique	1200	22
12349	DESMOULINS	Didier	3450	33
12350	DESHAIES	Justin	2300	22
12351	DESFOREST	Alain	2500	12
12352	DESMARAIS	Sylvie	2500	11

PUBLIC *EXCLUDE
PROFILX OPERATION

Row & Column Access Control (RCAC)

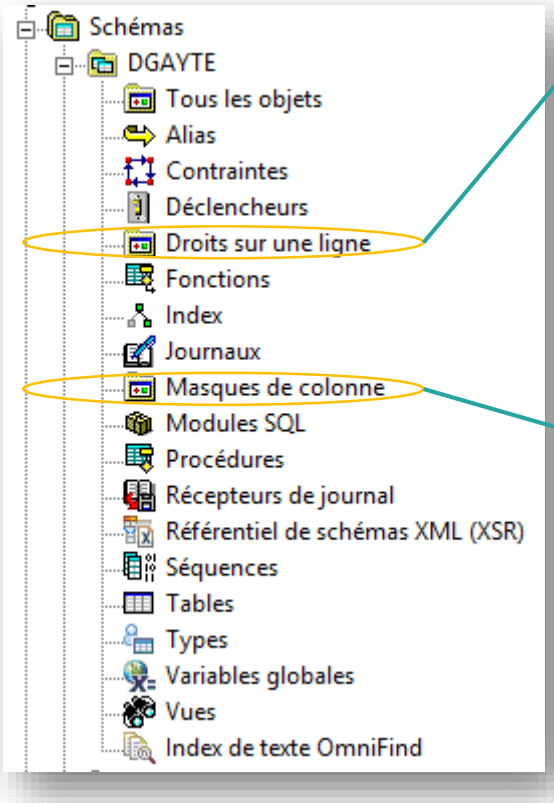
- Option 47 de SS1
  - IBM Advanced Data Security for i
  - Non facturable
  - A partir de la V7R2
- RCAC permet de limiter l'accès à certaines données de type ligne et/ou colonne, aux seules personnes (ou groupes de personnes) qui sont habilitées à connaître le contenu de ces données
- RCAC utilise deux approches
  - Des permissions sur les lignes
    - Ne montre que les lignes autorisées
  - Des masques sur les colonnes
    - Peut obfusquer en tout ou partie une valeur de colonne

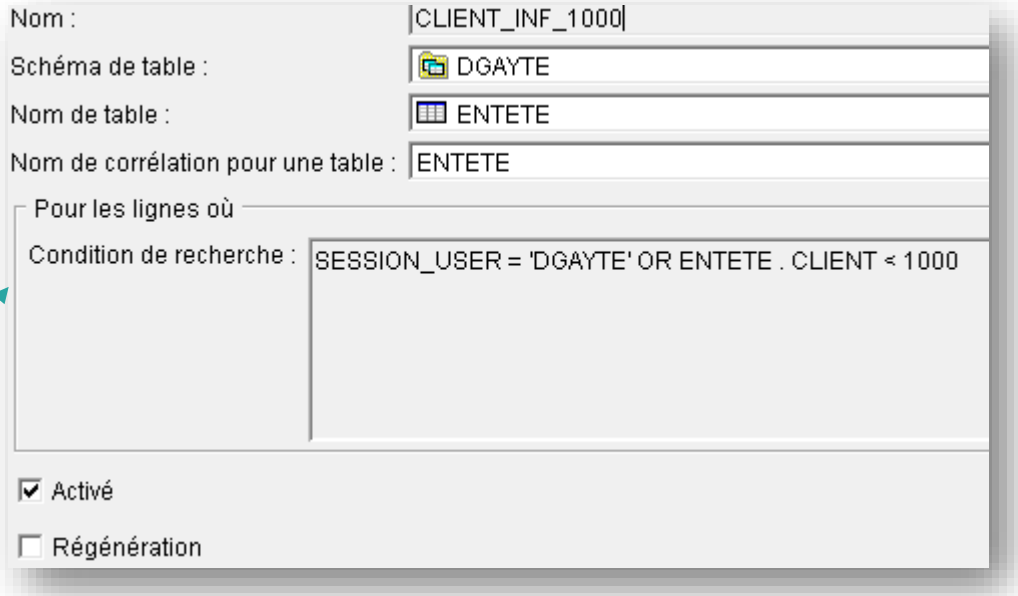
Row & Column Access Control (2)

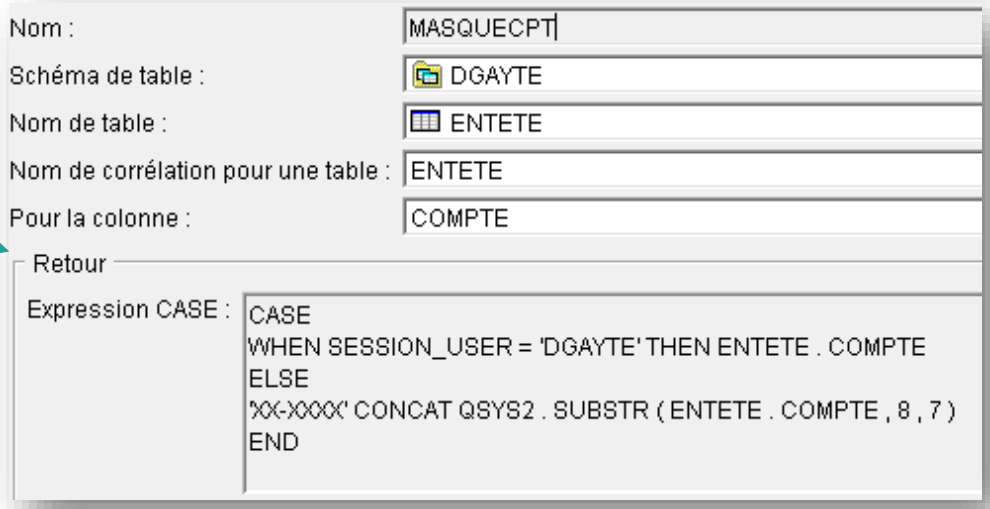
- Même les utilisateurs qui ont des droits *ALLOBJ ne peuvent passer outre les autorisations qui ont été définies au travers de RCAC
- Transparent pour les applications utilisant la base de données
- Fonctionne aussi en mise à jour
  - Interdiction d'écrire une donnée qui n'est pas autorisée par RCAC

System i Navigator

- Nouvelles options
- SP à appliquer (SI56695)

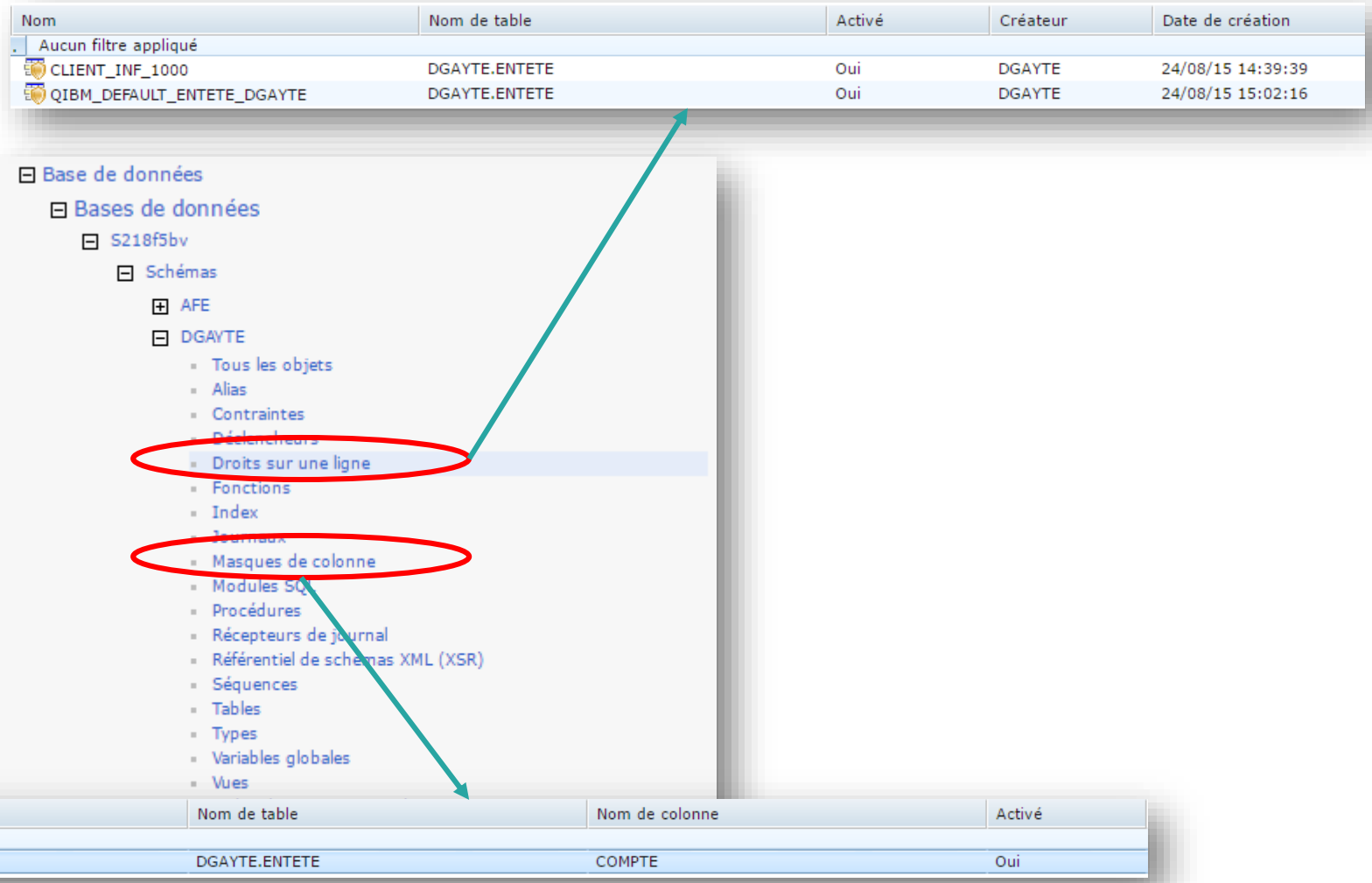






Navigator for i

- Disponible dans l'interface



Points d'exit

- Le programme associé à un point d'exit est exécuté à chaque évènement concernant ce point d'exit
- Il existe de nombreux points d'exit, pour ce qui nous concerne :
  - Pour les connexions ODBC/JDBC
  - Pour FTP
- Très intéressant pour
  - Limiter les accès
  - Limiter les actions
  - Tracer ce qui est fait
- Définis avec la commande WRKREGINF

Point d'exit ODBC/JDBC

- QIBM_QZDA_INIT
  - A l'initialisation de la connexion
- QIBM_QZDA_SQL1 et QIBM_QZDA_SQL2
  - Lors de l'exécution d'une requête SQL
  - Permettent de récupérer la requête demandée
- Deux paramètres
  - CHAR(1) qui permet d'accepter ou de refuser l'opération
  - CHAR(x) qui contient des informations sur le contexte
    - Profil utilisateur
    - Requête (pour QIBM_QZDA_SQLx)
- Arrêter et relancer le serveur *DATABASE (attention à la production !)
  - ENDHOSTSVR SERVER(*DATABASE) ENDACTCNN(*DATABASE)
  - STRHOSTSVR SERVER(*DATABASE)

Exemple de filtrage sur le profil utilisateur

```
      * Dominique GAYTE - NoToS - Pour Université IBM i 2017
      * Programme d'exit pour  QIBM_QZDA_INIT format ZDAI0100
      * Vérification du profil utilisateur qui se connecte en ODBC/JDBC
      *
      /Copy QSYSINC/QRPGLESRC,EZDAEP

     DAccepte          S              1

     C     *Entry        PList
     C                   Parm                    Accepte
     C                   Parm                    EZDQIF

      /FREE
       *INLR = *On;
       //
       // On n'accepte que les connexions de DGAYTE ou de profils Qxxx
       //
       If EZDUP='DGAYTE'
             Or %Subst(EZDUP:1:1)='Q';
         Accepte =*On;
       Else;
         Accepte =*Off;
       EndIf;
       Return;
      /END-FREE
```

```
     DEZDQIF           DS
     D*                                        Qzda Init Format
     D EZDUP                    1     10
     D*                                   User profile name
     D EZDSID                  11     20
     D*                                   Server identifier
     D EZDFN                   21     28
     D*                                   User exit format name
     D EZDFID                  29     32I 0
     D*                                   Requested function id
     D EZDIT                   33     95
     D*                                   Interface type         @B1A
     D EZDIN                   96    222
     D*                                   Interface name         @B1A
     D EZDIL                  223    285
     D*                                   Interface level        @B1A
```

DGAYTE/QZDA_INIT

Test

- WRKREGINF

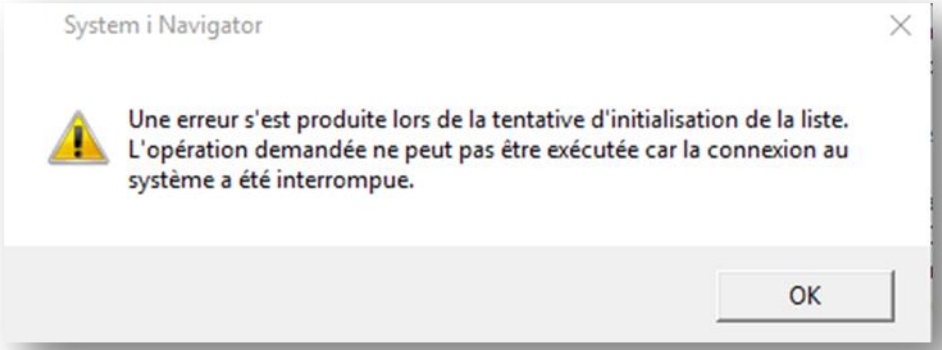
```
Exit point:   QIBM_QZDA_INIT          Format:   ZDAI0100

Type options, press Enter.
  1=Add   4=Remove   5=Display   10=Replace

             Exit
            Program     Exit
Opt          Number     Program        Library

__                      __________     __________
__                1     QZDA_INIT      DGAYTE
__
```

- Avec System i Navigator, Base de données
- Si connexion avec un profil différent de DGAYTE et Qxxx



Points d'exit FTP

- 2 points d'exit dans notre contexte
- QIBM_QTMF_SVR_LOGON
  - Appelé à la connexion
  - Permet de définir l'environnement FTP
    - Accepter ou rejeter la connexion
    - Dossier initial initial (permet de limier l'impact si la commande CD est interdite)
    - Mode *LIBL ou *PATH
    - SSL (FTPS)
  - QIBM_QTMF_SERVER_REQ
    - Autorise ou interdit des opérations (CD, Delete, get, put…)

FTP : Exemple de filtrage lors de la connexion

```
      *Pour            - Exit FTP - restriction des connexions   *
      *Associer au point d'exit QIBM_QTMF_SVR_LOGON FMT: TPCL0200*
      *
!!!Extrait !!!

Select;
 When %Subst(UserID:1:UserIDLen) = 'PIRATE1';     //Interdit
      AllowLogin = Rejet;
 When %Subst(UserID:1:UserIDLen) = 'FTPIFS';      // Accès initial à l'IFS
      AllowLogin = Accepte;
      AppInfoDS.NameFmt = 1;
      …
      AppInfoDS.FileListFmt = 1;
      HomeDir = '/edi/Import';
      HomeDirLen = %Len(%Trim(HomeDir));

 WHEN %Subst(UserID:1:UserIDLen) = 'FTPBIB';      //Accès initial à une bibliothèque
      AllowLogin = Accepte;
      AppInfoDS.NameFmt = 0;
      …
      CurLib = 'BIBEXPORT';
 Other;                                           //connexion sur l'IFS dans /home/PROFIL
      AllowLogin = Accepte;
      AppInfoDS.NameFmt = 1;
      …
      //on constitue le chemin  /home/PROFIL
      HomeDir = '/home/' + %Subst(UserID:1:UserIDLen);
      HomeDirLen = %Len(%Trim(HomeDir));
EndSl;

%Subst(AppInfo:1:AppInfoLen) = AppInfoDS;
```

```
dRejet          c                   Const(0)
dAccepte        c                   Const(1)
```

DGAYTE/FTPLOGON

FTP : Exemple de filtrage des actions

```
      * Dominique GAYTE - NoToS - Pour Université IBM i 2017
      *Pour            - Exit FTP - restriction des connexions    *
      *Associer au point d'exit QIBM_QTMF_SERVER_REQ'*
      *
!!!Extrait !!!

IF OperationID = StartFTP;              //Démarrage de FTP , OK
       AllowOperation = Accepte;
       *InLR = *On;
       Return;
Elseif UserProfile = 'FTPIFS' ;
  SELECT;
   WHEN OperationID = CreateDir ;       //Création de répertoire
      AllowOperation = Rejet;
   WHEN OperationID = DeleteDir ;       //Suppression de répertoire
      AllowOperation = Rejet;
   WHEN OperationID = ChangeDir ;       //Changement de répertoire

      //Si on est dans /Home on accepte, sinon on refuse
      if   %xlate(Lower: Upper:%subst(OperationInfo:1:5)) = '/HOME' ;
         AllowOperation = Accepte;
      else ;
         AllowOperation = Rejet;
      ENDIF;
   WHEN OperationID = DeleteFile;       //Suppression de fichier
      AllowOperation = Rejet;
   WHEN OperationID = PutFile   ;       //Envoi de fichier
      AllowOperation = Accepte;
   WHEN OperationID = GetFile   ;       //Réception de fichier
      AllowOperation = Accepte;
  ENDSL;
 Else ;                 //Pour tous les autres profils tout est refusé
  AllowOperation = Rejet;
 Endif;
```

Et aussi

- Pare-feu intégré de l'IBM i
  - CFGTCP option 4 : Work with TCP/IP port restrictions
  - Permet de filtrer les ports en entrée. Autorisation par profil (groupe)
- IDS : Système de Détection d'intrusion
  - En graphique
  - Depuis la V6R1
  - Pour la surveillance, alerte par mail ou MSGQ

Conclusions

- DB2 est le cœur de votre système
- Mettre en place une Sécurité des objets efficace pour les bibliothèques et des fichiers
- Protéger les accès distants
  - Au niveau des applications (FTP, CA, ODBC/JDBC…)
  - Par des points d'Exit
- Tracer !