Université IBM i 2017

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

S44 - Sécuriser l'IFS

Jeudi 18 mai – 15h15-16h45

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

NoToS

- Expertise autour de l'IBM i
  - Sécurité
  - Regard moderne
  - 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

L'IFS : principes

- IFS : Integrated File System
- Structure de fichiers arborescente de l'IBM i
- Englobe tous ce qui est sur les disques
  - QSYS.LIB : le monde objet (système, base de données…)
  - QDLS : vieux système de fichier (office Vision, PCS)
  - QOpenSys : le monde Unix (Attention, les majuscules et les minuscules ont un sens)
  - Root (au sens strict) type PC

L'IFS : est-ce important au niveau Sécurité ?

- Oui ! Et de plus en plus
- L'IFS sert à stocker (de manière plus ou moins temporaire) des données parfois critiques
  - Virements au format XML (SEPA)
  - Exportation/importation de données
    - Format CSV, PDF …
    - Comptabilité
    - Commerciale
    - Paie
    - Listes de clients
    - …
  - Souvent des données à caractère personnel : attention au GDPR (RGPD)

Accès à l'IFS

- Par l'IBM i
  - WRKLNK…
- Par Netserver (partage de fichiers Windows)
- Par System i Navigator et ACS
- Par FTP
- Applications Unix
- …
- Il y a donc autant de modes de protections à prendre en considération !

Les droits de l'IFS

- Droits comparables à ceux des objets de l'IBM i
  - Droits Privés : pour chaque utilisateur (ou Groupe) spécifié
    - Propriétaire
  - Droits publics : tous les autres
  - Groupe Principal
  - Liste d'autorisation
  - Pas d'adoption de droits !
- Mais notation différente
  - Droits sur les données à la mode Unix
    - *R : *OBJOPR and *READ
    - *W : *OBJOPR, *ADD, *UPD, *DLT
    - *X : *OBJOPR and *EXECUTE
    - Combinaisons possibles *R, *W, *X, *RW, *RX, *WX, *RWX
    - *NONE aucun droit aux données
    - *EXCLUDE aucun droit à l'objet
  - Droits sur l'objet
    - *OBJEXIST, *OBJMGT, *OBJREF, *OBJALTER, *NONE

Les droits de l'IFS : 5250

- Commande WRKAUT, CHGAUT

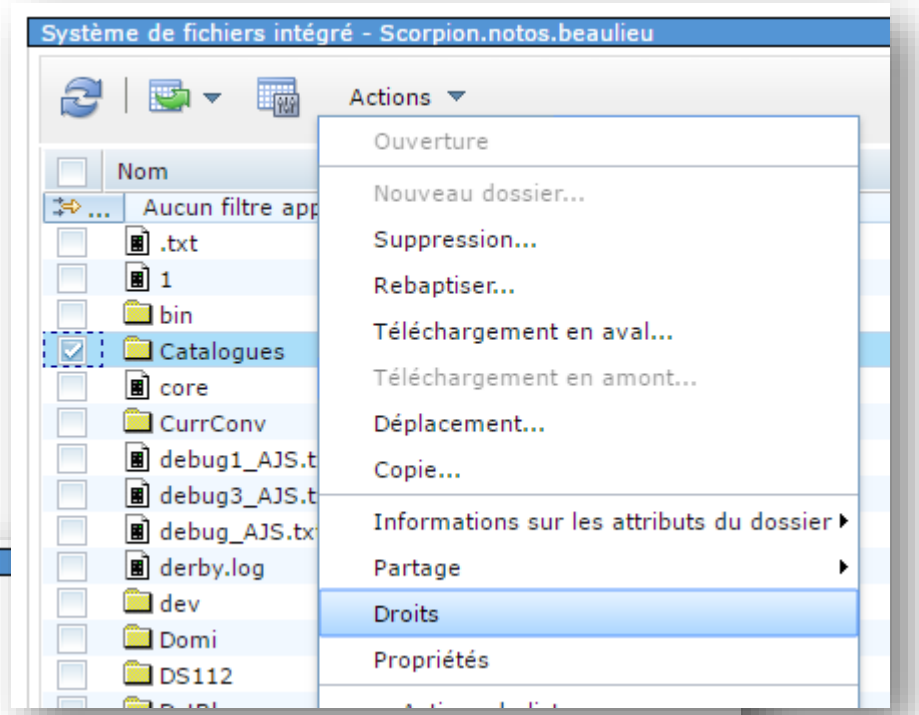
```
                Droits sur  ------Droits sur les données-------
Utilisat         données    Opér   Lect   Ajout   MàJ   Suppr   Exéc
_________       _________
*PUBLIC         *RX          X      X                             X
QTMHHTTP        *RWX         X      X       X      X      X      X
DGAYTE          *R           X      X
```

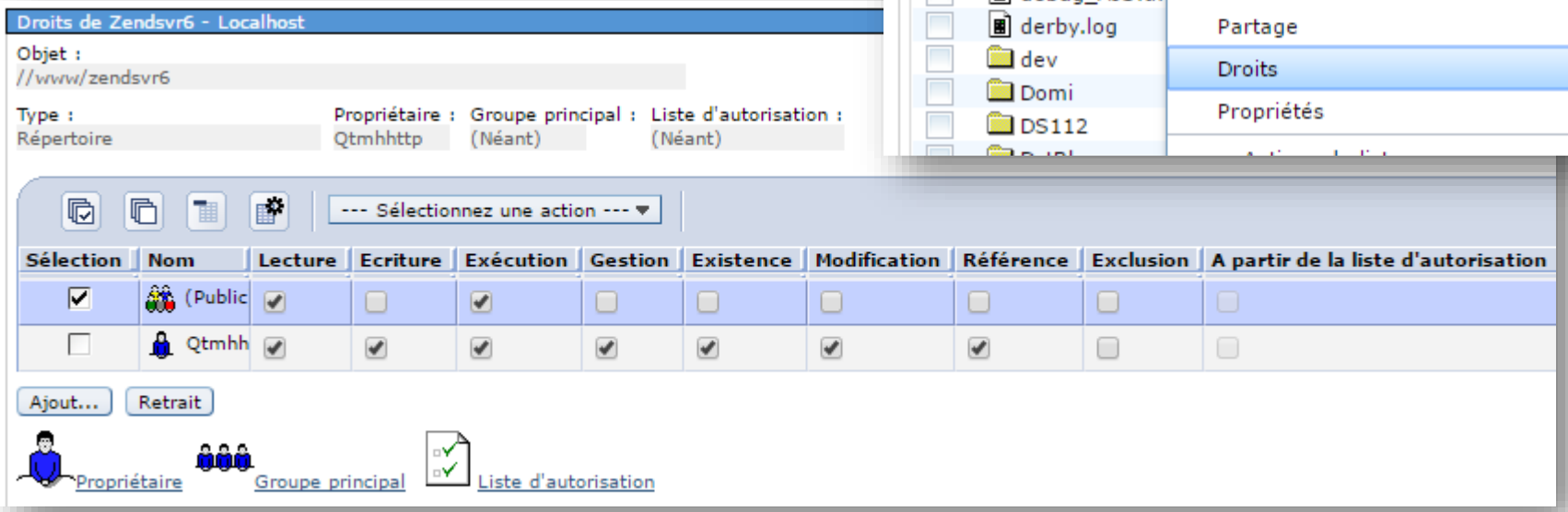
```
                Droits sur  ---Droits sur objet----
Utilisat         données    Exist   Gest   Modif   Réf
_________       _________
*PUBLIC         *RX
QTMHHTTP        *RWX           X      X       X      X
DGAYTE          *R
```

- Modification du propriétaire CHGOWN
- Modification du groupe principal CHGPGP

Les droits de l'IFS : Navigator for i

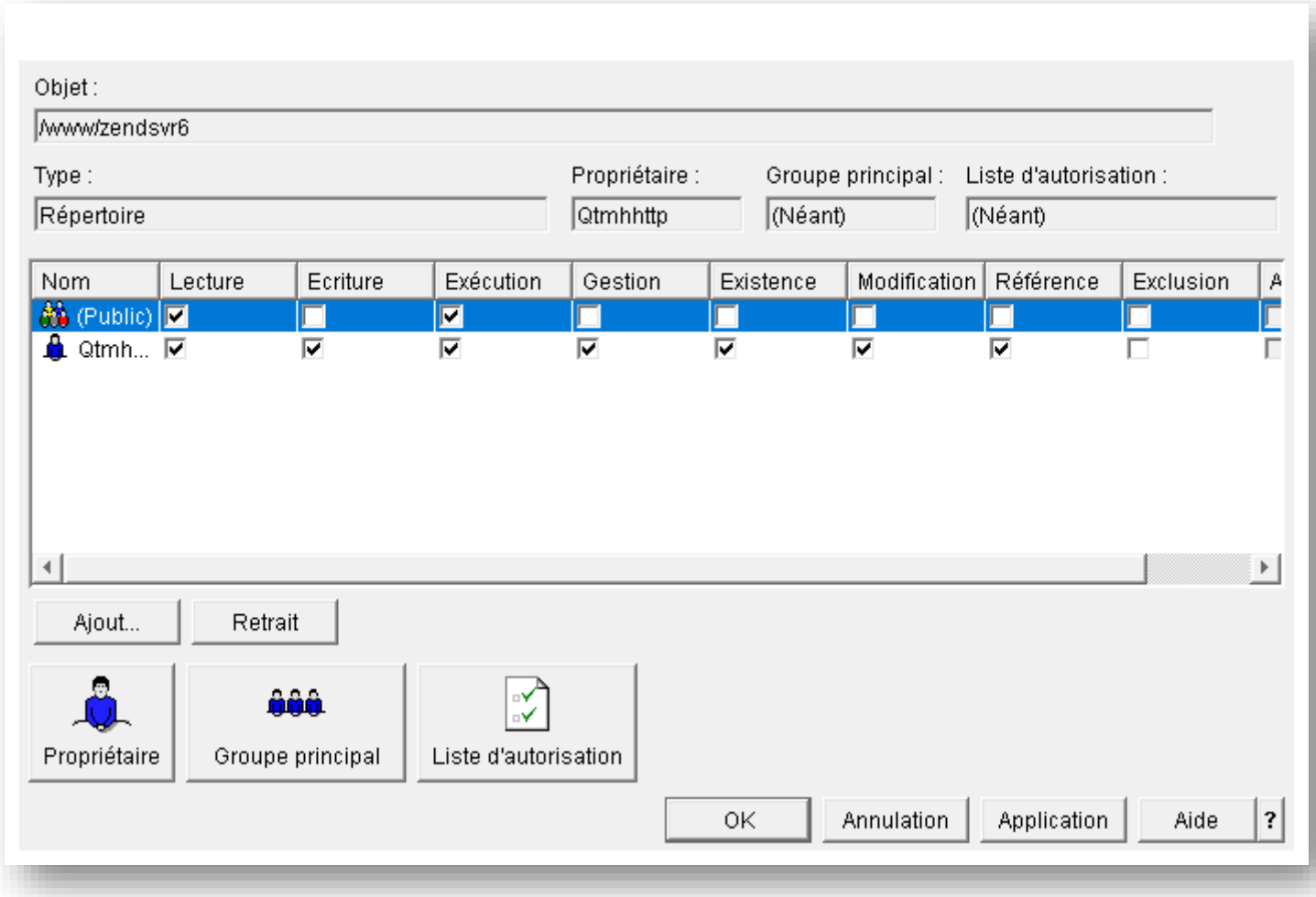
- Dans un navigateur





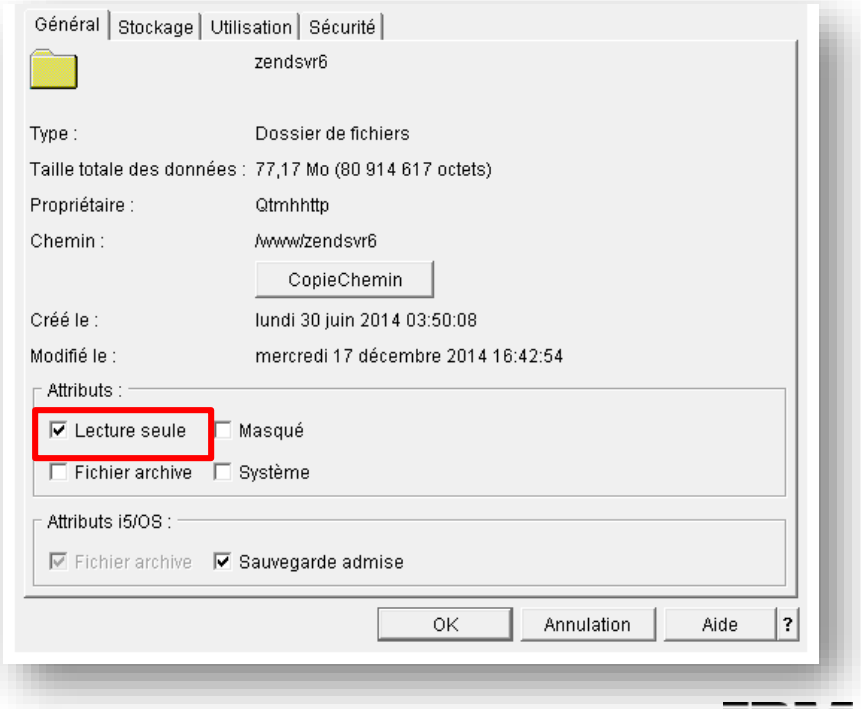
Les droits de l'IFS : System i Navigator

- Client lourd



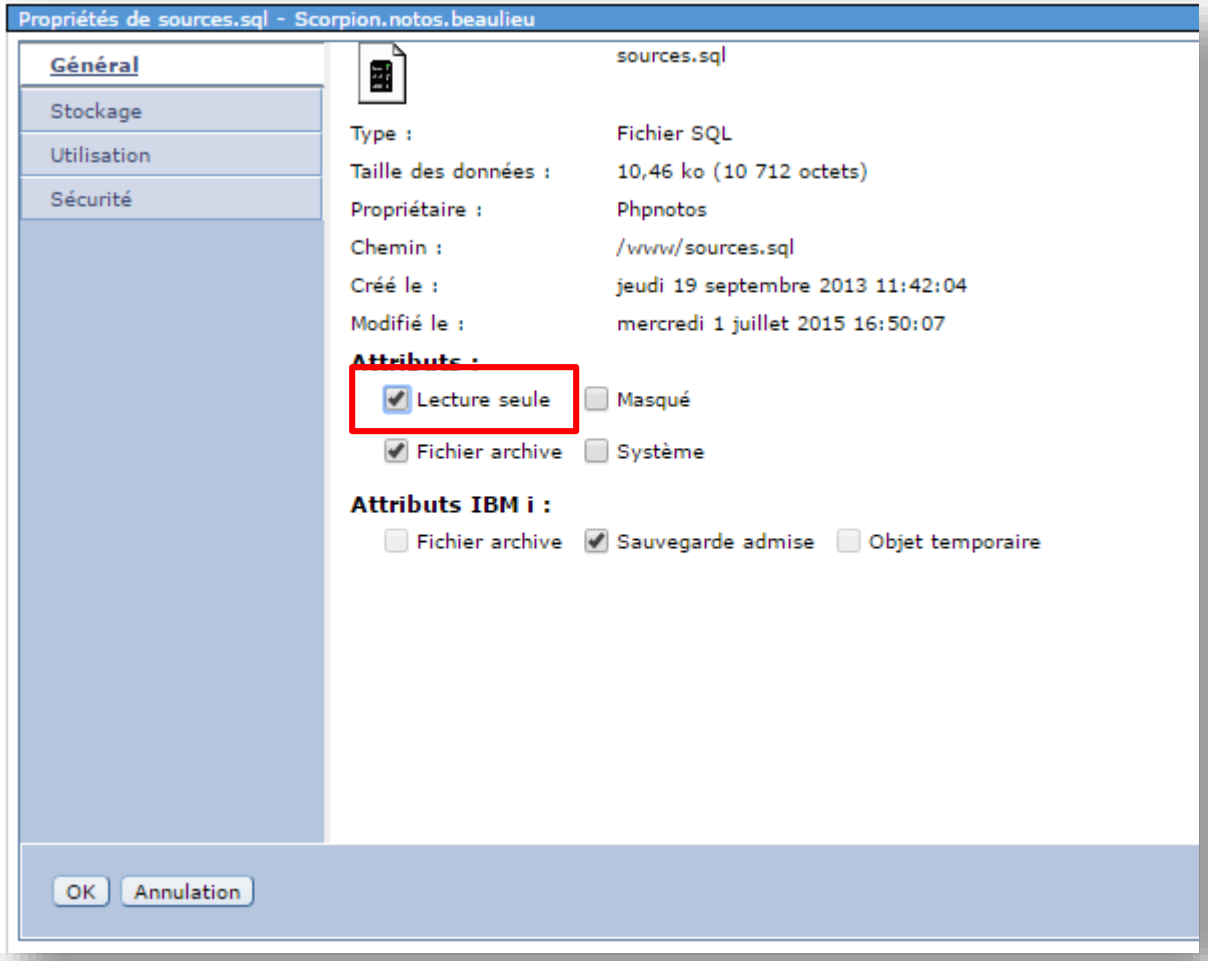
Attribut de lecture seule

- Empêche une modification des données (même *ALLOBJ)
  - Mais le fichier peut être renommé !
- 5250 : CHGATR OBJ('/tmp/facturdec.csv') ATR(*READONLY) VALUE(*YES)
- System i Navigator



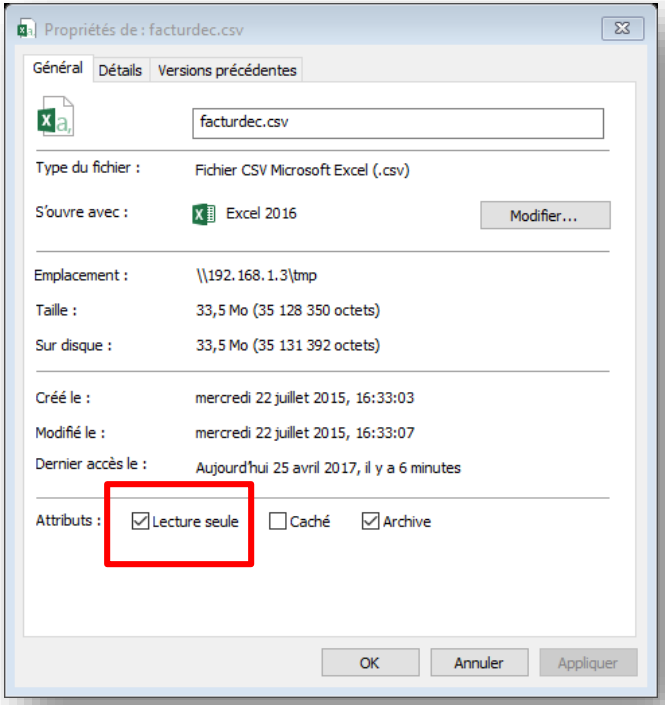
Attribut de lecture seule (2)

- System i Navigator

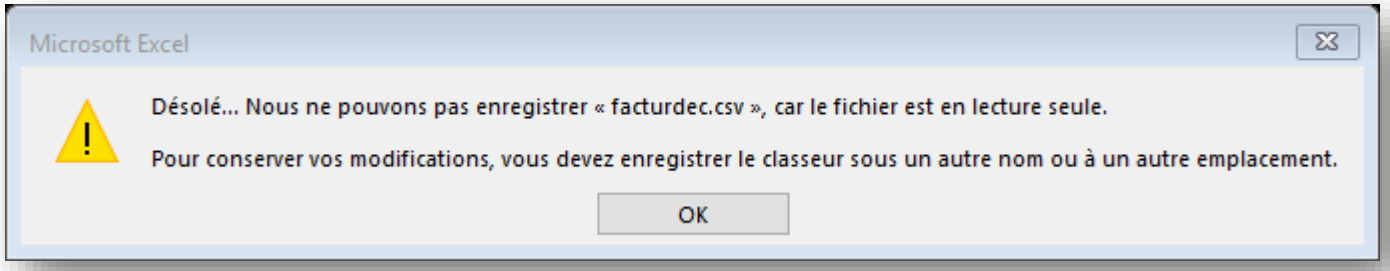


Attribut de lecture seule (3)

- Gestionnaire de fichiers de Windows

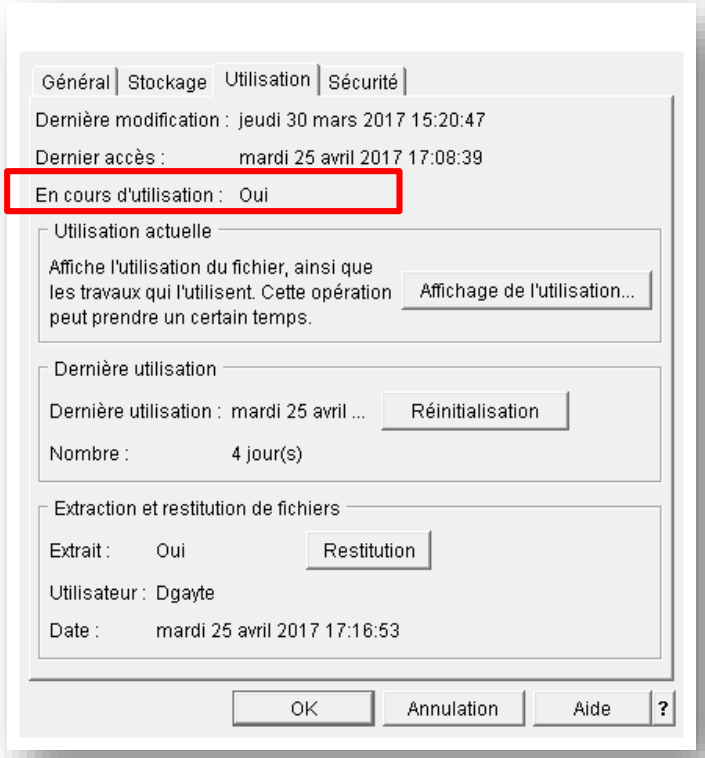


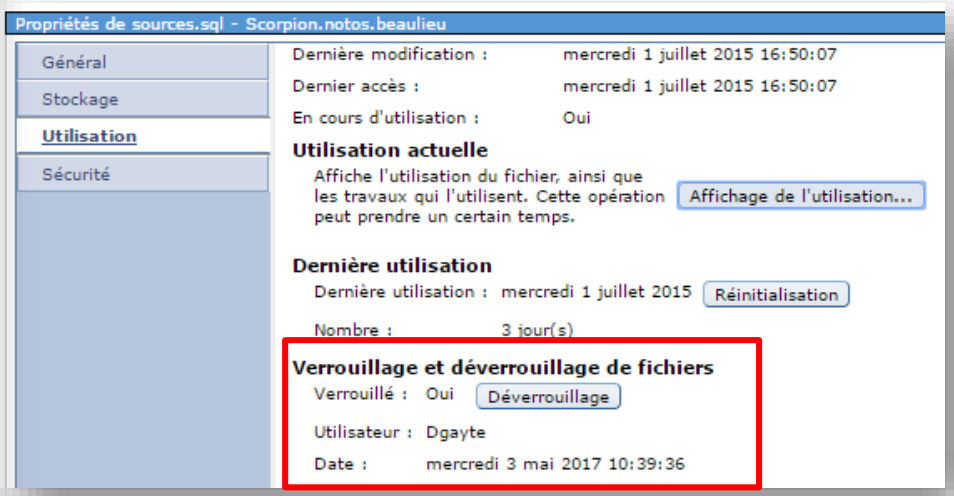
- Résultat



Verrouillage

- Par la commande CHKOUT
  - Possibilité de verrouiller toute l'arborescence
  - CHKOUT OBJ('/xml') SUBTREE(*ALL)
- Libération par un CHKIN





Accéder à un élément de l'IFS

- Avoir les droits *X sur tous les répertoires de la hiérarchie
- Avoir les droits nécessaires sur le fichier/dossier lui-même
  - *R, *W selon l'action demandée

Pour accéder à :

/www/Zendsvr6/htdocs/php.spool/index.php

Il faut disposer des droits :

- *X sur
  - /
  - /www
  - /www /Zendsvr6/
  - /www/Zendsvr6/htdocs
  - /www/Zendsvr6/htdocs/php.spool
- *R (ou *W …)
  - index.php

Droits par défaut lors de la création

- Attention aux droits par défaut lors de la création d'un fichier/répertoire
- En général héritage du niveau supérieur
- Dépend de l'environnement de création (IBM i, Unix, PC)
- Par exemple la liste d'autorisation du dossier parent
  - Est transmise pour la création d'un dossier ou d'un fichier en IBM i ou à partir d'un PC
  - N'est pas transmise en UNIX
  - Idem pour les droits privés qui ne sont pas transmis en UNIX

Petite synthèse sur les droits de l'IFS

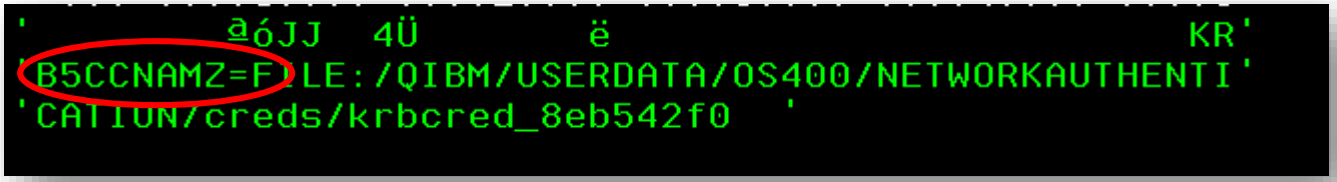
- Protéger les répertoires importants
  - Pas de droits *X sur le répertoire ne permet pas d'accéder aux fichiers ou aux sous répertoires
- Protéger les fichiers importants
  - Ne pas donner de droits publics
    - Donner la valeur *EXCLUDE pour *PUBLIC
  - Minimiser les droits privés
  - Eventuellement attribut en lecture seule
  - Donner des droits par défaut limités lors de leur création
    - CPY, CPYTOIMPF, CPYTOSTMF
- Utiliser les listes d'autorisations et les groupes
  - Pour simplifier le travail de codification

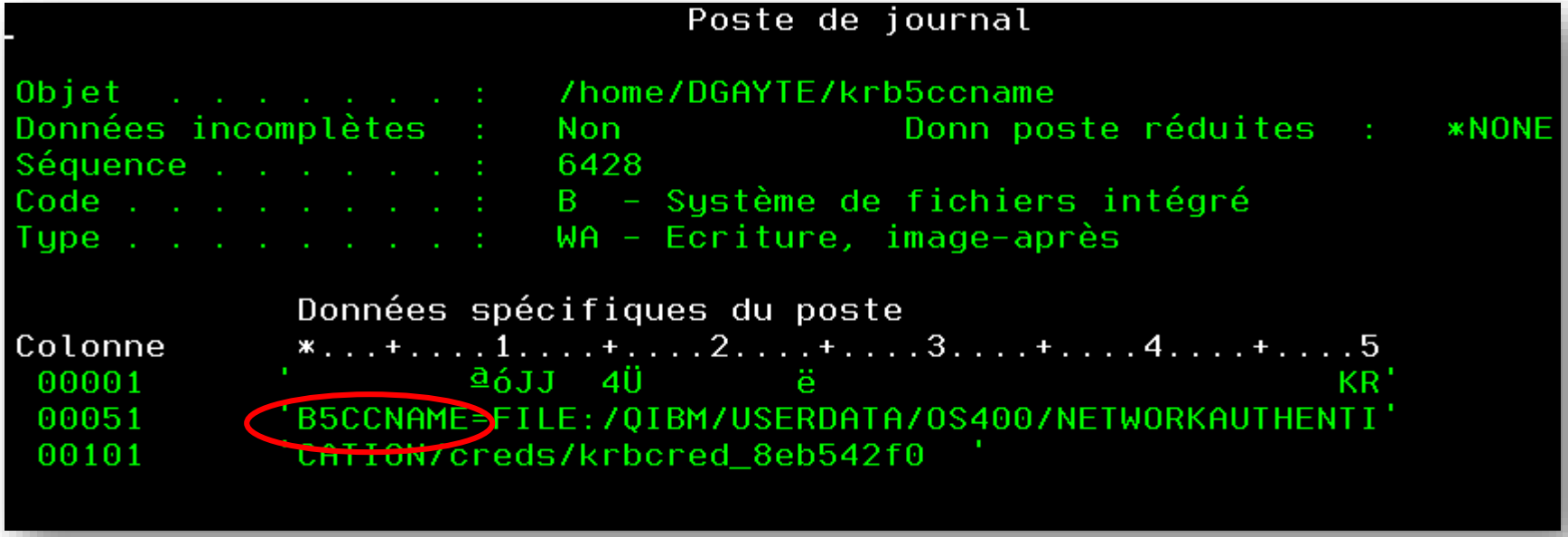
Traçabilité

- Audit
  - QAUDCTL(*OBJAUD)
  - Commande CHGAUD pour les répertoires/fichiers à auditer
    - Pour un répertoire possibilité d'auditer tous les sous-répertoires
  - Lors de la création d'un répertoire (CRTDIR) le paramètre CRTOBJAUD précise comment les fichiers/répertoires seront audités par défaut

Traçabilité (2)

- Journalisation





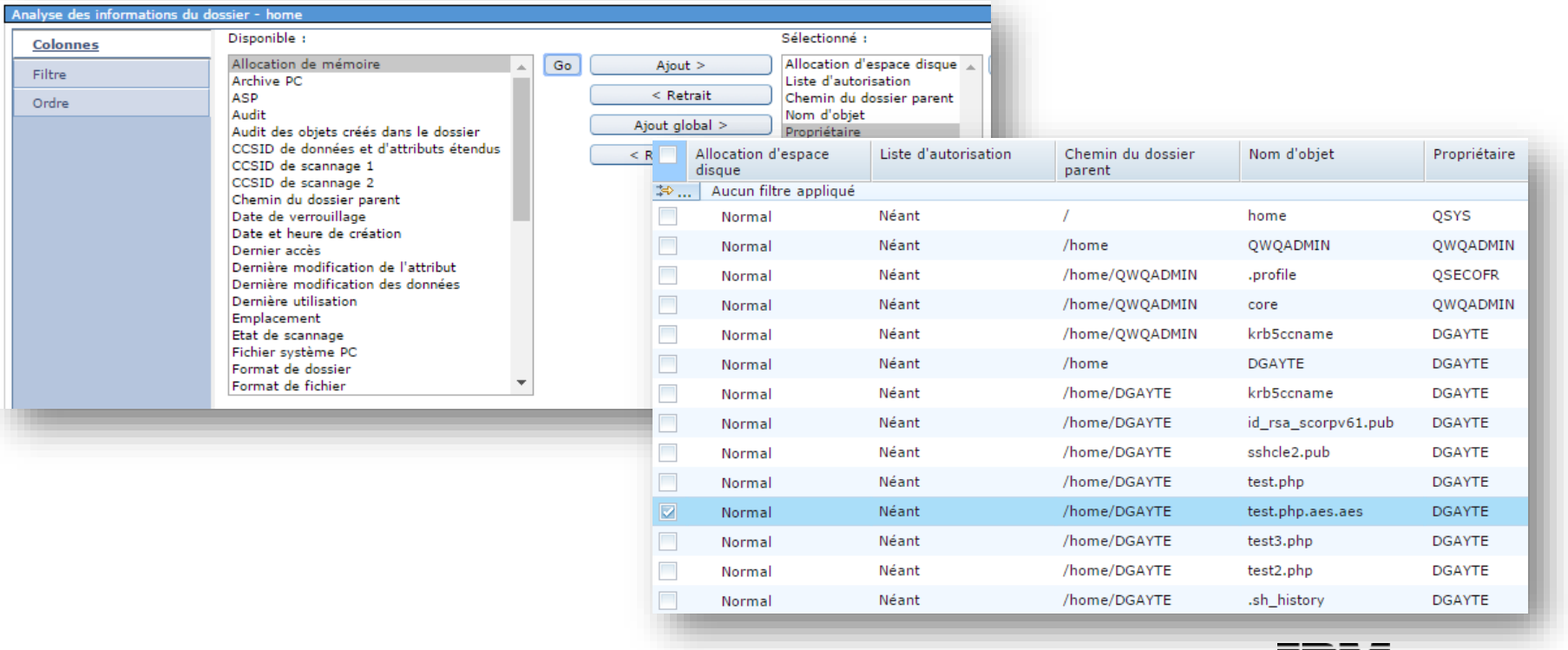
Informations sur l'IFS

- Commande PRTPUBAUT (Imprimer droits publics)

```
                          Fichier spoule
Fichier . . . . :   QPSECPUB                        Page/Ligne  150/4
Contrôle  . . . .   _______                         Colonnes    1 - 78
Recherche . . . .   _______________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...
 Type d'objet . . . . . . . . . :   *DIR
 Répertoire . . . . . . . . . . :   /home/DGAYTE/.eclipse
                                                    Droits
                                       Liste        sur        ----------Objet
 Objet                    Propriét     autor        données    Ges   Exist   M
 RSE                      DGAYTE       *NONE        *NONE       X      X
                               Objets définis avec droits publics (rapport int
5770SS1 V7R2M0  140418
 Type d'objet . . . . . . . . . :   *DIR
 Répertoire . . . . . . . . . . :   /home/DGAYTE
                                                    Droits
                                       Liste        sur        ----------Objet
 Objet                    Propriét     autor        données    Ges   Exist   M
 .ssh                     DGAYTE       *NONE        *NONE       X      X
 .eclipse                 DGAYTE       *NONE        *NONE       X      X
                               Objets définis avec droits publics (rapport int
```

Extraction des informations

- Commande RTVDIRINF ou Navigator for i
- Analyse avec PRTDIRINF ou Navigator for i
  - Ou directement à partir des fichiers générés
    - (QAEZDxxxxO, QAEZDxxxxD de QUSRSYS)

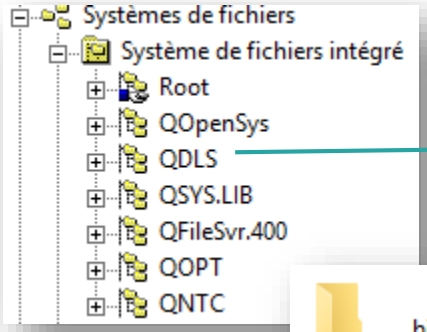


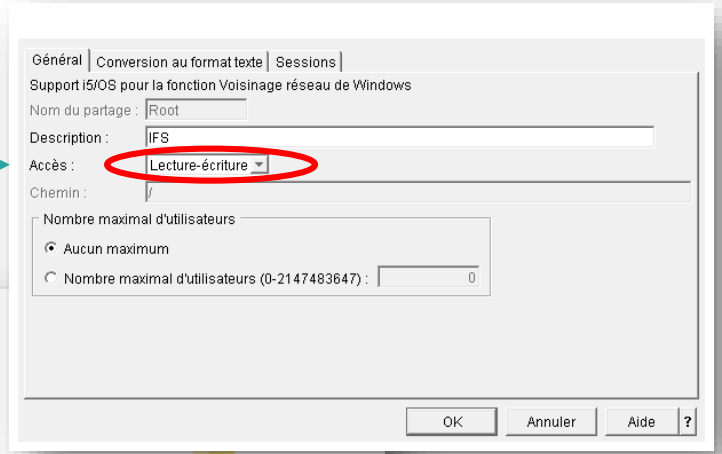
Netserver : le partage de fichiers

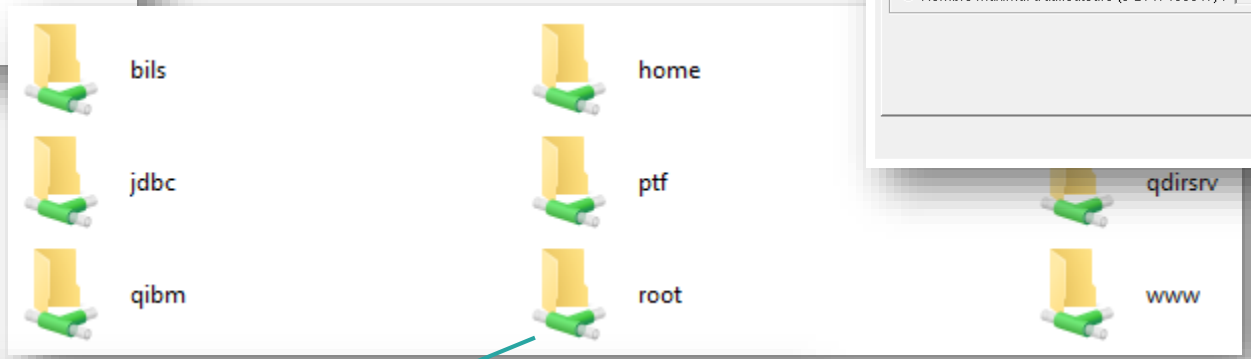
- Transforme l'IBM i en serveur de fichiers Windows
- Des dossiers de l'IFS sont partagés et accessibles sur le réseau
  - En lecture ou lecture/écriture
  - Les droits d'accès sont vérifiés à partir du profil de connexion

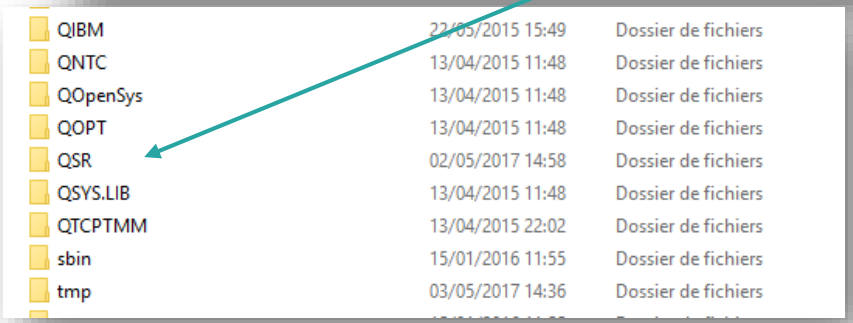
Partage de root

- Root est parfois partagé, parfois même en écriture
- C’est très pratique, mais très dangereux !!!!!!









Partage de root (2)

- Donne accès à QSYS.LIB à partir du partage de fichiers de Windows
- Risques d'erreurs, de malversation, d'incidents
- La liste d'autorisation QPWFSERVER protège QSYS.LIB
  - De NetServer, IBM i Access for Windows, Java Toolbox
  - Mais pas de FTP ou autres
  - Mais pas si le profil est *ALLOBJ

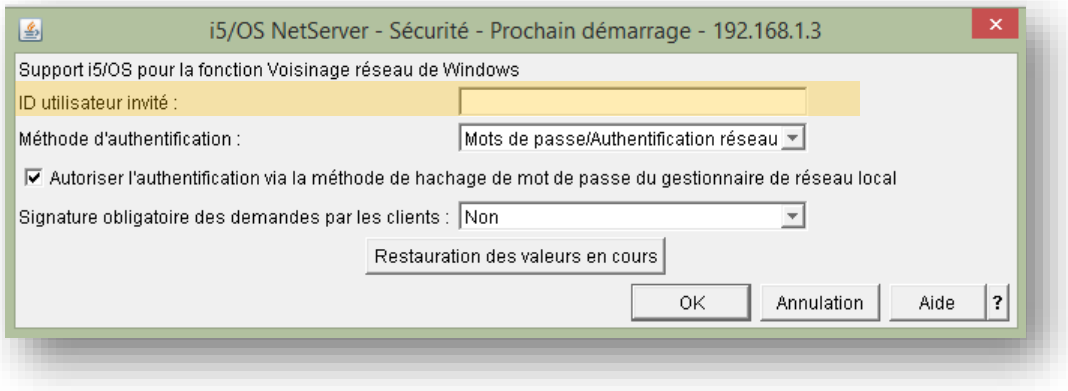
```
Objet  . . . . . :   QPWFSERVER
  Bibliothèque . . :     QSYS

              Droits    Gest
Utilisat    sur objet  list
*PUBLIC     *USE
QSYS        *ALL        X
```

Partage de root (3)

- **A éliminer !**
- Supprimer le partage de root
- Mais attention aux montages des utilisateurs et services divers
  - Avec i5OS NetServer vérifier les points de montage sur Root
  - Identifier les systèmes d'origine
  - Remplacer ce montage par un montage plus adapté (le plus bas possible dans la hiérarchie des dossiers)
    - Modifier les chemins utilisés par les applications distantes

Profil Invité

- Le profil invité permet de se connecter au partage de l'IFS sans avoir de profil utilisateur
- Défini dans les propriétés de NetServer



- Ne pas utiliser le profil invité !

Synthèse Netserver

- Ne pas partager Root
- Limiter les partages à ce qui est essentiel
  - Surtout en écriture
- Toujours partager le niveau le plus bas de l'arborescence
- Adapter les droits des utilisateurs pour les dossiers partagés
- Ne pas utiliser le profil invité
- Possibilité d'utiliser le SSO (EIM) pour un accès transparent

Point d'exit pour IFS

- Créer un programme
- Mettre à jour le point d'exit QIBM_QPWFS_FILE_SERV
  - Commande WRKREGINF
- Le programme sera appelé à chaque action sur l'IFS à partir de NetServer, IBM i Access, Java Toolbox
  - Ouverture, suppression, création, déplacement… d'un fichier
  - Modification d'attribut
  - Copie de fichier (V7R3)
- Arrêter et redémarrer (Attention à la production !!!)
  - Le Server *NETSVR
    - ENDTCPSVR SERVER(*NETSVR)
  - Le SBS QSERVER
    - ENDSBS QSERVER
  - Les Host Server *FILE
    - ENDHOSTSVR SERVER(*FILE)
- Est aussi utilisé pour la traçabilité !

Point d'exit pour IFS : paramètres reçus

- Deux paramètres
  - CHAR(1) en sortie : '0' refusé, '1' accepté
  - CHAR(x) en entrée : informations sur le traitement de l'IFS demandé
- Le premier paramètre permet de valider ou d'arrêter l'opération
- Le second contient toutes les informations nécessaires
  - Deux formats
  - PWFS0100
  - PWFS0200 en V7R3
    - Distinction *STMF, *DIR
    - Informations sur la demande de copie, déplacement et renommage (source et cible)

Second paramètre (format PWFS0100)

Offset		Type	Field	Description
Dec	Hex			
0	0	CHAR(10)	User profile name	The name of the user profile that is calling the server
10	A	CHAR(10)	Server identifier	For the file server, the value is *FILESRV.
20	14	BINARY(4)	Requested function	The function being performed: • **X'0000'** - Change file attributes request • **X'0001'** - Create stream file or directory request • **X'0002'** - Delete file or delete directory request • **X'0003'** - List file attributes request • **X'0004'** - Move request • **X'0005'** - Open stream file request • **X'0006'** - Rename request • **X'0007'** - Allocate conversation request
24	18	CHAR(8)	Format name	The user exit format name being used. For QIBM_QPWFS_FILE_SERV, the format name is PWFS0100.
32	20	CHAR(4)	File access	If the requested function has a value of **X'0005'** (open), this field contains the following structure: • Read access, CHAR(1) **X'F1'** - Yes **X'F0'** - No • Write access, CHAR(1) **X'F1'** - Yes **X'F0'** - No • Read/write access, CHAR(1) **X'F1'** - Yes **X'F0'** - No • Delete allowed, CHAR(1) **X'F1'** - Yes **X'F0'** - No

Offset		Type	Field	Description
Dec	Hex			
36	24	BINARY(4)	File name length	The length of the file name (the next field). The length can be a maximum of 16 MB. If the requested function has a value of **X'0007'** (Allocate conversation request), the file name length is 0.
40	28	CHAR(*)	File name	The name of the file. The length of this field is specified by the file name length (the previous field). The file name is returned in CCSID 1200. If a requested function has a value of one of the following, the file name is provided and the file name length is set: • **X'0000'** - Change file attributes request • **X'0001'** - Create stream file or directory request • **X'0002'** - Delete file or delete directory request • **X'0003'** - List file attributes request • **X'0004'** - Move request • **X'0005'** - Open stream file request • **X'0006'** - Rename request

Notes:

- This format is defined by member EPWFSEP in files H, QRPGSRC, QRPGLESRC, QLBLSRC, and QCBLLESRC in library QSYSINC.
- The APIs available to convert to and from CCSID 1200 are iconv() and CDRCVRT.

Unicode+

FTP

- FTP permet d'accéder à l'IFS
- Il faut être en mode *PATH
  - Configuration initiale du serveur FTP (CHGFTPA)

```
Initial name format  . . . . . .   *PATH          *SAME, *LIB, *PATH
```

  - QUOTE SITE NA 1 en ligne de commande du client FTP

```
ftp> pwd
257 "DGAYTE" is current library.
ftp> quote site na 1
250  Now using naming format "1".
ftp> pwd
257 "/QSYS.LIB/DGAYTE.LIB" is current library.
ftp> cd /www
250 "/www" is current directory.
ftp>
```

  - QUOTE SITE NA 0 pour revenir en mode *LIBL

Sécurité et FTP

- FTP s'appuie sur la Sécurité de l'IFS
  - Bien adapter les droits de l'IFS
- Pour l'imiter les déplacements dans tout l'IFS (y compris QSYS.LIB) mettre en place les points d'exit FTP
- QIBM_QTMF_SVR_LOGON
  - Appelé à la connexion
  - Permet de définir l'environnement FTP
    - Accepter ou rejeter la connexion
    - Dossier initial (permet de limiter l'impact si la commande CD est interdite)
    - Mode *LIBL ou *PATH (*LIBL ne permet pas d'accéder à l'IFS sauf si NAMEFMT est demandé)
    - 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 = Allow;
      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 = Allow;
      AppInfoDS.NameFmt = 0;
      …
      CurLib = 'BIBEXPORT';
 Other;                                           //connexion sur l'IFS dans /home/PROFIL
      AllowLogin = Allow;
      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;
```

DGAYTE/FTPLOGON

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 = 'FTPRRD' ;
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;
```

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

dStartFTP       c                   Const(0)
dCreateDir      c                   Const(1)
dDeleteDir      c                   Const(2)
dChangeDir      c                   Const(3)
dListDir        c                   Const(4)
dDeleteFile     c                   Const(5)
dPutFile        c                   Const(6)
dGetFile        c                   Const(7)
dRenameFile     c                   Const(8)
dCLCmd          c                   Const(9)
```

Et les virus ?

- L'IBM i n'est pas sensible aux virus
- Mais peut être un porteur sain
- Les fichiers de l'IFS peuvent être infectés
- Utilisation d'un anti-virus IBM i ?
  - Peu utilisé…
- Scan à partir d'un anti-virus PC ?
  - Attention au changement de date de dernière utilisation
- Équiper les PC d'anti-virus qui scannent tous les fichiers utilisés

Conclusion

- Il faut absolument protéger l'IFS !
- Utiliser la Sécurité intégrée pour protéger les répertoires et les fichiers
- L'IBM i dispose d'un ensemble de fonctions pour assurer
  - La traçabilité
  - Une protection adaptée à chaque cas particulier