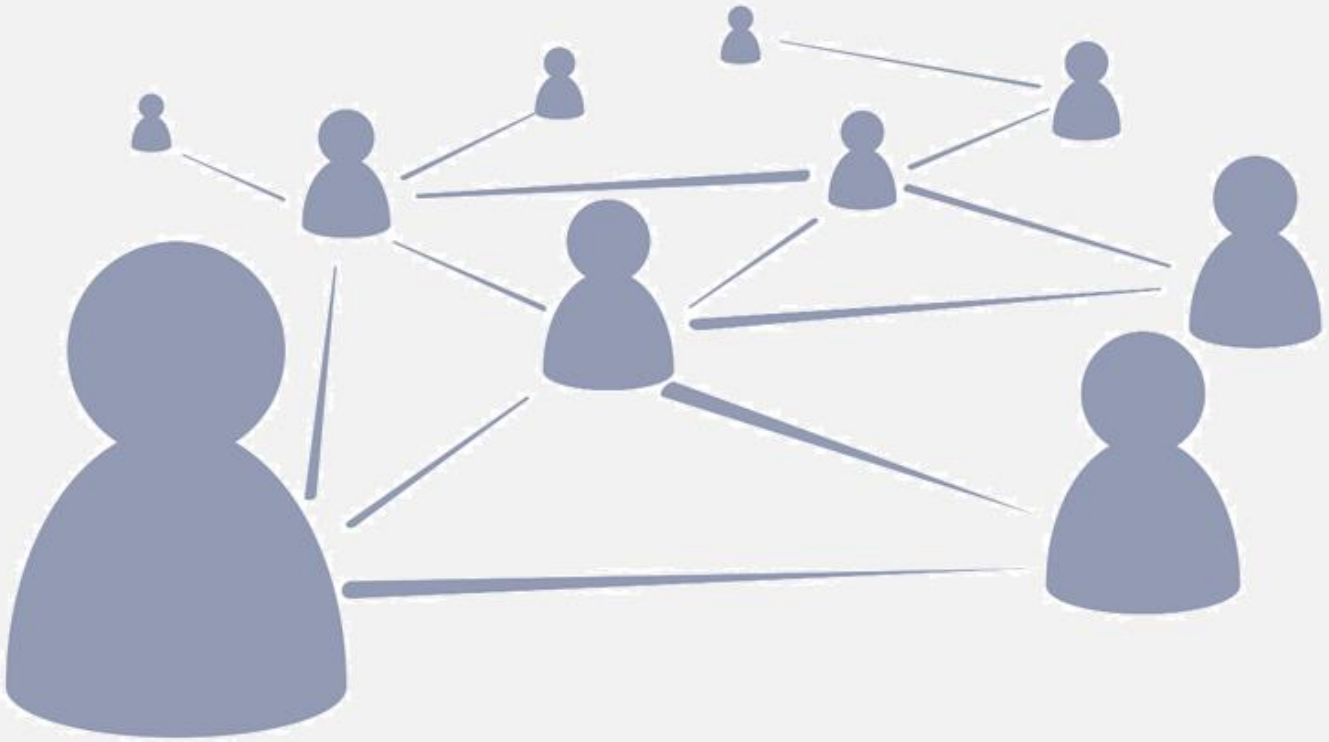
Sécurité IFS & ransomware

Dominique GAYTE
dominique@gayte.it– https://i.gayte.it
06 30 17 02 55

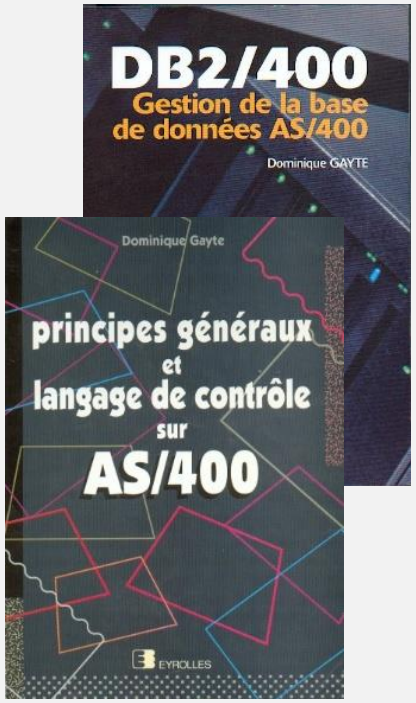
common FRANCE

MEMBER OF common EUROPE



Dominique GAYTE

- Intervenant « AS/400 » depuis 1990
- Sécurité
  - Audit
  - SSO, SSL
  - Sécurisation de la base de données et applications
  - Édition de logiciels sur la Sécurité IBM i



Dominique GAYTE
Consultant IBM i
i.gayte.it
dominique@gayte.it

Les ransomwares

Actuellement, une des préoccupations majeures en termes de Sécurité

Actualités

L'INFORMATICIEN

CYBERSÉCURITÉ

L'un des plus grands hôpitaux d'Île-de-France paralysé par un ransomware

Les attaquants, dont on ignore encore l'identité, réclament une rançon de dix millions d'euros, sans quoi ils menacent de poursuivre le blocage des services hospitaliers et de divulguer les données dérobées dans le SI du CHSF. Semblent avoir

CYBERSÉCURITÉ

Holiday Inn : une cyberattaque

CYBERSÉCURITÉ

L'hôpital de Cahors visé par une cyberattaque

by VICTOR MIGET le 20 SEPTEMBRE 2022

CYBERSÉCURITÉ

Uber victime d'un piratage

by GUILLAUME PÉRISSAT le 1

moins un compte AWS ou encore son logiciel de suivi des dépenses. Selon le New York Times, qui serait en contact avec le hacker, ce dernier a trompé un employé d'Uber par SMS, se faisant passer pour un responsable de l'informatique de l'entreprise afin d'obtenir son mot de passe.

Actualités (2)

L'INFORMATICIEN

28 SEPTEMBRE 2022

Caen victime d'une cyberattaque

Le 26 septembre, la capitale du Calvados a essuyé une attaque. Si plusieurs services ont été mis à l'arrêt, la réactivité des services informatiques de l'agglomération a, semble-t-il, permis d'éviter le pire.

29 SEPTEMBRE 2022

Budget 2023 : une enveloppe pour la cybersécurité

Le gouvernement a dévoilé, lundi 26 septembre, son projet de loi de finances (PLF) pour 2023. Une part sera attribuée à la lutte contre la cybercriminalité.

6000 milliards de dollars, c'est le coût mondial de la cybercriminalité en 2021. Face à ce coût exorbitant, l'État cherche à muscler les défenses françaises. Le budget 2023 dévoilé par le ministre de l'Économie Bruno Lemaire, lundi 26 septembre, renferme un important volet cybersécurité.

29 SEPTEMBRE 2022

Le pôle universitaire Léonard-de-Vinci visé par une cyberattaque

Les pirates sont entrés en contact avec le pôle universitaire et menacent de divulguer les informations. Une enquête a été ouverte et confiée au parquet de Paris.

Actualités (3)

L'INFORMATICIEN

> Cybersécurité

Un groupe de hackers recrute pour déployer SolidBit

Un groupe d'acteurs malveillants recrute de nouveaux membres sur des forums du dark web afin de diffuser le ransomware SolidBit.

RANÇONGICIEL (ransomware)

Technique d’attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l’envoi à la victime d’un logiciel malveillant qui chiffre l’ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement

Ransomware et IBM i ?

- Exécution du logiciel malveillant dans l'IBM i
  - Ce n'est pas une préoccupation
- Cryptage des données de l'IBM i
  - Tout à fait possible
  - Via les partages de fichiers (NetServer …)
- Extraction de données
  - Fuites de données
  - Attention au RGPD (CNIL) et à la double (triple) peine si fuite de DCP (Données à Caractère Personnel)

Il faut donc

- Sécuriser l'IFS
- Configurer les serveurs
  - FTP
  - NetServer
    - Gérer les partages
- Sauvegarder, sauvegarder, sauvegarder….
  - Rotation des « bandes » adaptée

Sécuriser l’IFS

L’IFS : principes

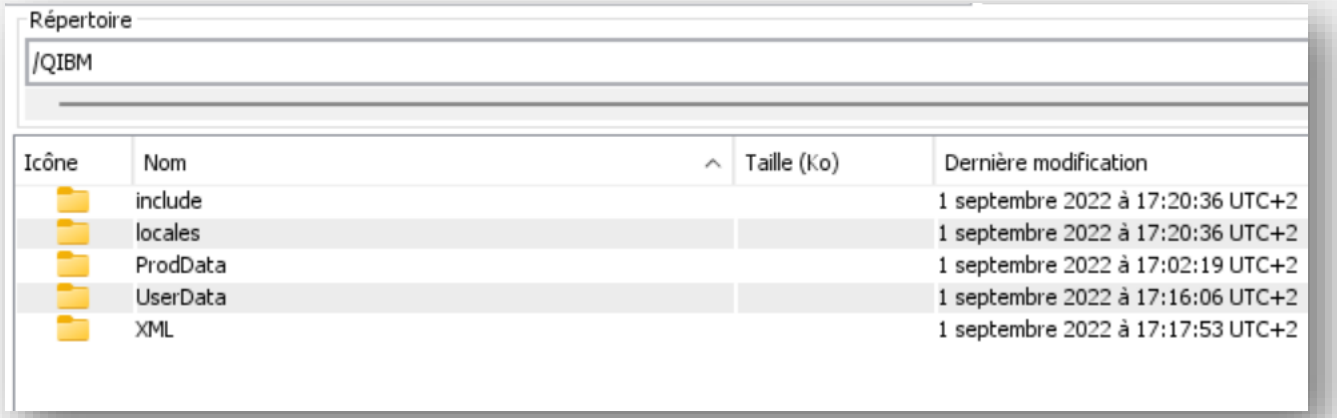
- IFS : Integrated File System
- Structure de fichiers arborescente de l’IBM i
- Englobe tout ce qui est sur les disques, notamment
  - QSYS.LIB : l’OS (IBM i), la base de données…
  - QDLS : vieux système de fichier (office Vision, PCS)
  - QOpenSys : le monde Unix (Attention, les majuscules et les 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
  - Les données de nombreux logiciels indispensables
    - Configuration dans /QIBM/UserData
    - Exécutables
  - 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 RGPD

Accès à l'IFS par…

- L'IBM i
  - WRKLNK…
- NetServer (partage de fichiers Windows)
- Par FTP
- ACS (Système de fichiers intégré)
  - Assez récent mais évite de partager des dossier via NetServer
- Navigator for i
- Applications diverses (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
  - Liste d'autorisation
  - Pas d'adoption de droits !
- Mais notation différente
  - Droits sur les **données** à la mode Unix (paramètre DTAAUT)
    - *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 sur l'objet
  - Droits sur **l'objet** (paramètre OBJAUT)
    - *OBJEXIST, *OBJMGT, *OBJREF, *OBJALTER, *NONE

Les droits de l'IFS : 5250

- Commande WRKAUT, CHGAUT

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

- Attention à la séparation données/objet

Opt	Utilisat	Droits sur données	Droits sur objet Exist	Gest	Modif	Réf
_	*PUBLIC	*NONE	X	X	X	X
_	DGAYTE	*RWX	X	X	X	X

- Modification du propriétaire CHGOWN
- Modification du groupe principal CHGPGP

Les droits de l'IFS : Navigator for i

- Dans un navigateur

Système de fichiers intégré - Scorpion.notos.beaulieu

Actions

Ouverture
Nouveau dossier...
Suppression...
Rebaptiser...
Téléchargement en aval...
Téléchargement en amont...
Déplacement...
Copie...
Informations sur les attributs du dossier
Partage
Droits
Propriétés

Nom
Aucun filtre app
.txt
1
bin
Catalogues
core
CurrConv
debug1_AJS.t
debug3_AJS.t
debug_AJS.tx
derby.log
dev
Domi
DS112

Droits de Zendsvr6 - Localhost

Objet :
//www/zendsvr6

Type : Répertoire
Propriétaire : Qtmhhttp
Groupe principal : (Néant)
Liste d'autorisation : (Néant)

--- Sélectionnez une action ---

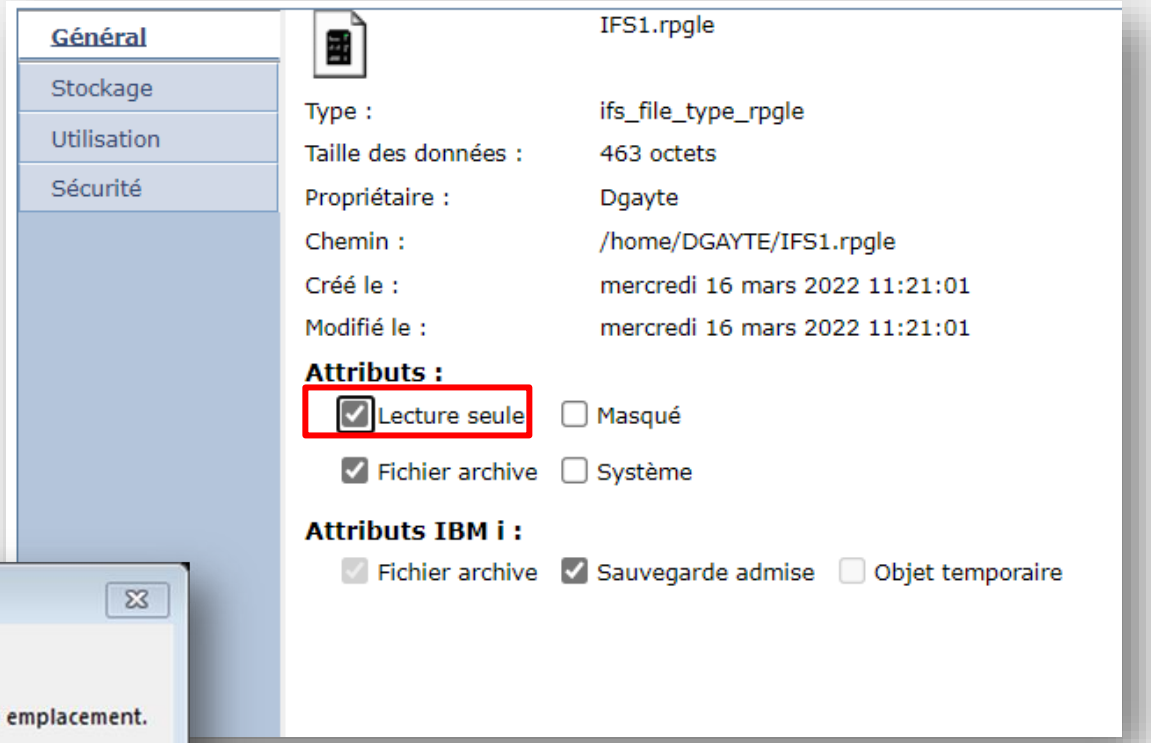
Sélection	Nom	Lecture	Ecriture	Exécution	Gestion	Existence	Modification	Référence	Exclusion	A partir de la liste d'autorisation
☑	(Public	☑	☐	☑	☐	☐	☐	☐	☐	☐
☐	Qtmhh	☑	☑	☑	☑	☑	☑	☑	☐	☐

Ajout... Retrait

Propriétaire Groupe principal Liste d'autorisation

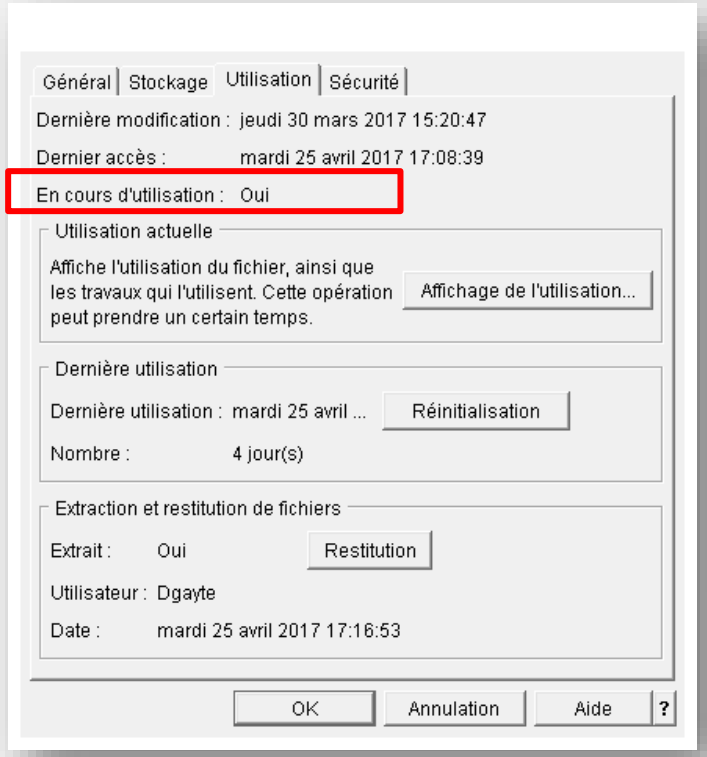
Attribut de lecture seule

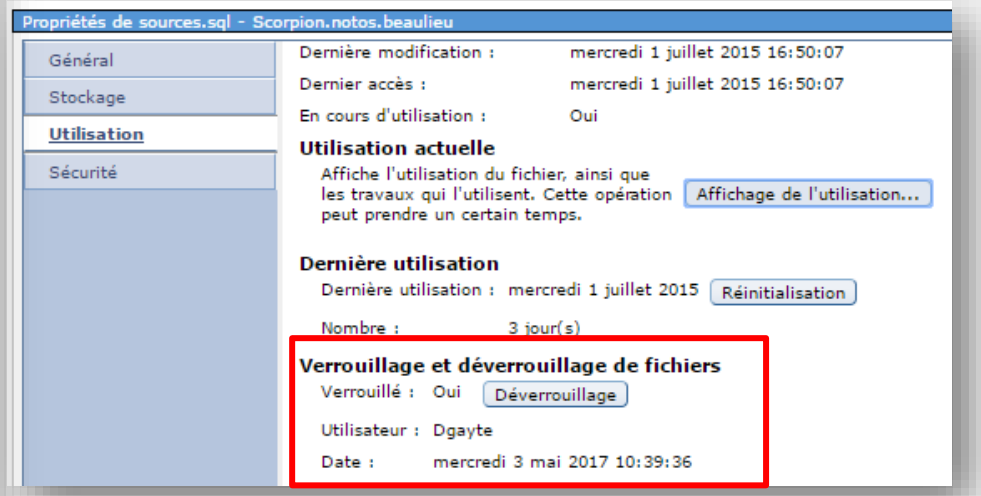
- Empêche une modification des données (même *ALLOBJ)
  - Mais le fichier peut être renommé !
- 5250 : CHGATR OBJ('/tmp/facturdec.csv') ATR(*READONLY) VALUE(*YES)
- Difficile à gérer pour la totalité des fichiers !



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 pour pouvoir les traverser
- 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 système
  - 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

```
                                Poste de journal

Objet  . . . . . . . :                    Bibliothèque . . . . :
Membre . . . . . . . :
Données incomplètes  :   Non              Donn poste réduites  :   *NONE
Séquence . . . . . . :   132902
Code . . . . . . . . :   T  - Poste trace d'audit
Type . . . . . . . . :   DO - Suppression d'objet

             Données spécifiques du poste
Colonne      *...+....1....+....2....+....3....+....4....+....5
 00701      '                                    ªóKY  CqQASP01'
 00751      '    00001    FRFRA  Y                 /usr/local/'
 00801      'zendsvr6/var/db/zsd.db-journal'
```

Traçabilité (2)

- Journalisation

```
                                Poste de journal

Objet  . . . . . . . . :   /home/DGAYTE/krb5ccname
Données incomplètes    :   Non              Donn poste réduites  :   *NONE
Séquence . . . . . . . :   6428
Code . . . . . . . . . :   B  - Système de fichiers intégré
Type . . . . . . . . . :   WA - Ecriture, image-après

             Données spécifiques du poste
Colonne      *...+....1....+....2....+....3....+....4....+....5
 00001      '        ªóJJ  4Ü       ë                        KR'
 00051      'B5CCNAME=FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTI'
 00101      'CATION/creds/krbcred_8eb542f0  '
```

Traçabilité (3)

- Point d’exit sur les accès à l’IFS
- QIBM_QPWFS_FILE_SERV
- Permet de savoir qui accède à quel dossier/fichier de l’IFS via Net Server
- Permet aussi d’interdire certaines actions
  - Ouverture en modification
  - Accès à un sous dossier…
- C’est très bavard !

Configurer FTP

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
```

- Sinon on peut utiliser la commande QUOTE SITE NA x
  - 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 bibliothèque (*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…)

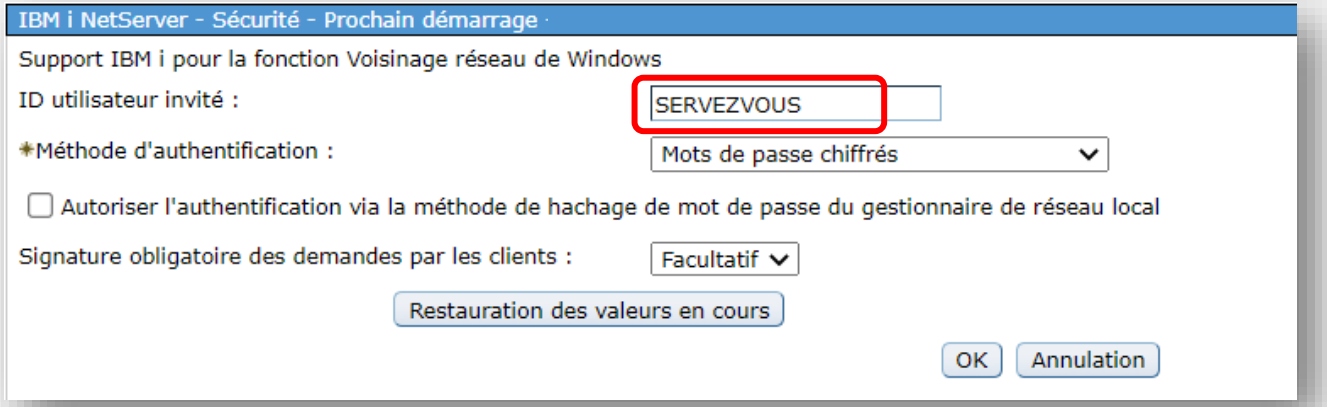
Configurer NetServer

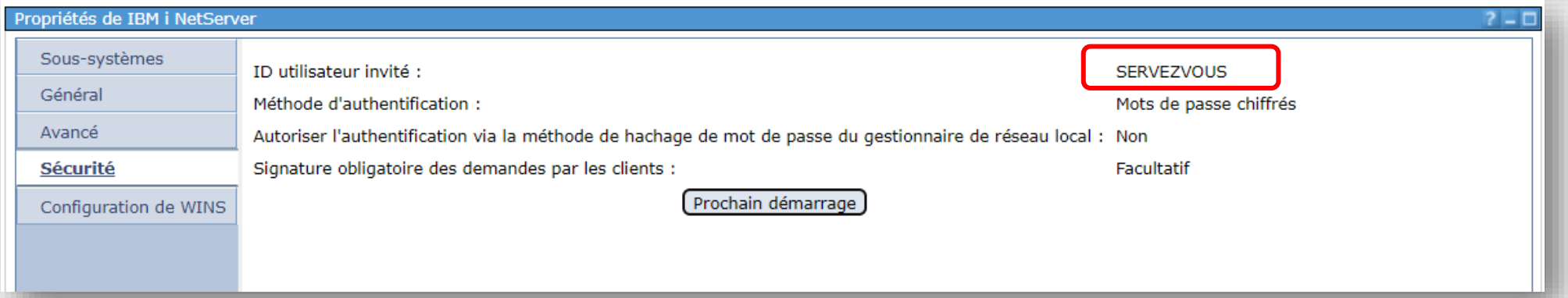
Netserver : le partage de fichiers

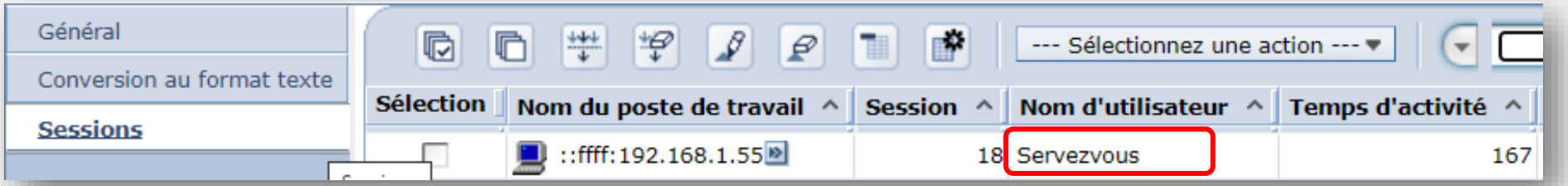
- Transforme l’IBM i en serveur de fichiers Windows
- Des dossiers de l’IFS sont partagés et accessibles sur le réseau
  - En lecture ou lecture/écriture
  - Les droits d’accès sont vérifiés à partir du profil de connexion

Compte Invité de NetServer

- A ne pas autoriser le compte invité car connexion sans authentification







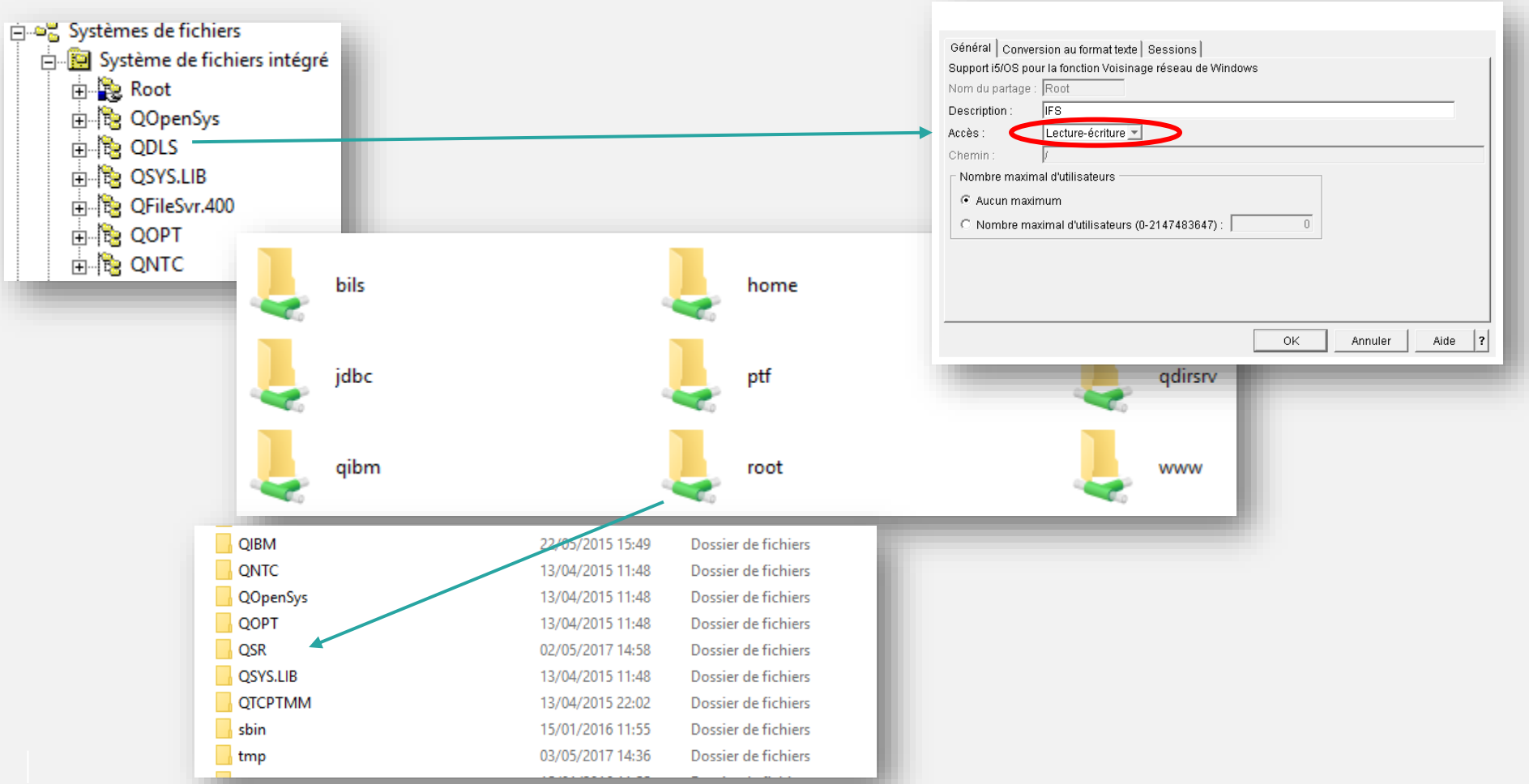
Nouveauté NetServer V7R5

- Sécurisation de l'accès à l'IFS via NetServer par des listes d'autorisations
- La liste est associée à un partage ou à tous les partages (tout NetServer)
- C'est une couche de protection supplémentaire
- Si les droits via l'AUTL
  - < *USE, accès refusé
  - = *USE (ou < *CHANGE) accès en lecture
  - >= *CHANGE accès total (en fonction des caractéristiques du partage)
- Configuré avec
  - Navigator for i
  - Menu **NETS** (QUSRTOOLS)
  - API (QZLSADFS, QZLSADPS, QZLSCHFS, or QZLSCHPS) via un nouveau paramètre optionnel

Gérer les partages de NetServer

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
  - Si public * EXCLUDE
  - 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
```

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

Indiquez les modifications sur les dro

                Droits    Gest
Utilisat.     sur objet   list
*PUBLIC       *EXCLUDE     _
QSYS          *ALL         X
```

Partage de root (3)

- **Interdit !**
- Supprimer le partage de root
- Mais attention aux montages des utilisateurs et services divers
  - 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

Il faut

- Gérer les partages au niveau le plus bas possible
  - **/Compta/Rapports/Data** plutôt que **/Compta**
- Ne pas partager les dossiers système (**/QIBM**, **/QDirSrv**…)
- Supprimer les partages inutiles
  - Traçabilité via point d'exit
- Partager en lecture si possible
  - Ne partager en écriture que des dossiers non vitaux
    - Revoir les process et l'organisation des partages de l'IFS si besoin
  - Mais attention, un partage en lecture permet de récupérer des documents (fuite de DCP)
- Éviter de monter des unités réseau en permanence

Et toujours…

- Sauvegarder, sauvegarder, sauvegarder….
  - Rotation des « bandes » adaptée
- Isolation des sauvegardes (*air gap backup*)
  - Bandes
  - Clones en lecture seule
  - VTL

Merci !