



IBM Power Systems - IBM i

Modernisation, développement d'applications et DB2 sous IBM i  
*Technologies, outils et nouveautés 2013-2014*

13 et 14 mai 2014 – IBM Client Center Paris, Bois-Colombes

**S8 - Sécurité IBM i : nouveautés 6.1 et 7.1**

*Mardi 13 mai – 16h00-17h30*

Dominique GAYTE – NoToS – [dgayte@notos.fr](mailto:dgayte@notos.fr)



# NoToS

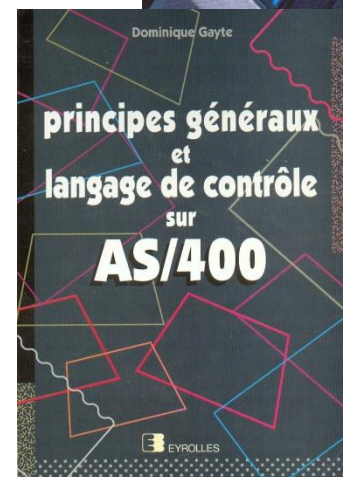
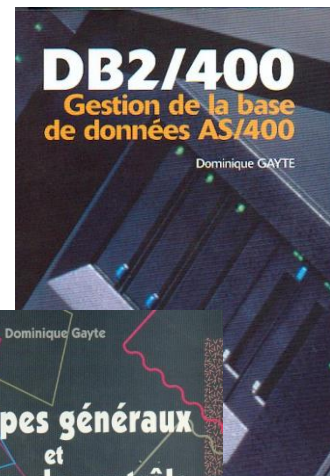
- Expertise autour de l'IBM i
  - Regard moderne
- Service
  - Formation, audit, développement...
- PHP sur IBM i avec Zend
- Développement de progiciels
  - PHP



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



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



# Sommaire

- Profils utilisateur
- PTFs
- IDS
- Cryptage
- DB2 (*field procedure*)
- SSL
- SSO/EIM

## Profils utilisateur – Mot de passe - QPWDRULES

- Nouvelle valeur système (ou dans les profils) de la V6R1
- QPWDRULES permet de mieux correspondre aux règles générales du système d'information
  - \*PWDSYSVAL : valeur par défaut (comme avant, utilise les autres valeurs système : QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF et QPWDRQDDGT)
  - \*DGTLMTLST : le mot de passe ne peut se terminer par un chiffre
  - \*LTRLMTLST : le mot de passe ne peut se terminer par une lettre
  - \*DGTMINn : avec n qui est le nombre de chiffre minimal
  - \*LMTSAMPOS : un caractère ne peut pas être placé au même endroit que dans le précédent mot de passe
  - \*LMTPRFNAME : ne peut contenir le profil utilisateur
- Prend effet au prochain changement de mot de passe

# QPWDRULES (2)

- Dans System i Navigator
- Onglet Validation 1
  - Comme avant
- Onglet Validation 2
  - Nouveautés V6R1 liées à QWDRULES

Général | Validation 1 | Validation 2 | Expiration |

Niveau de mot de passe (en cours) :

Mots de passe courts utilisant un jeu de caractères restreint. (0)

Options de validation de mot de passe

Utiliser les valeurs système de validation de l'onglet Validation 1

Utiliser les règles de validation suivantes. Certaines valeurs système correspondantes indiquées dans l'onglet Validation 1 seront ignorées.

Longueur des mots de passe

Longueur maximale (1 à 10) :

Longueur maximale (1 à 10) :

Restreindre la répétition des caractères :

Répétitions admises

Lettres

Nombre minimal (0 à 9) :

Nombre maximal (0 à 9) :

Restreindre les lettres consécutives

Chiffres

Nombre minimal (0 à 9) :

Nombre maximal (0 à 9) :

Restreindre les chiffres consécutifs

Caractères spéciaux

Nombre minimal (0 à 9) :

Nombre maximal (0 à 9) :

Restreindre les caractères spéciaux consécutifs

Premier caractère

Lettre non admise

Chiffre non admis

Caractère spécial non admis

Dernier caractère

Lettre non admise

Chiffre non admis

Caractère spécial non admis

Ne pas utiliser le même caractère à chaque position du mot de passe précédent

Restreindre l'emploi du profil utilisateur dans le mot de passe

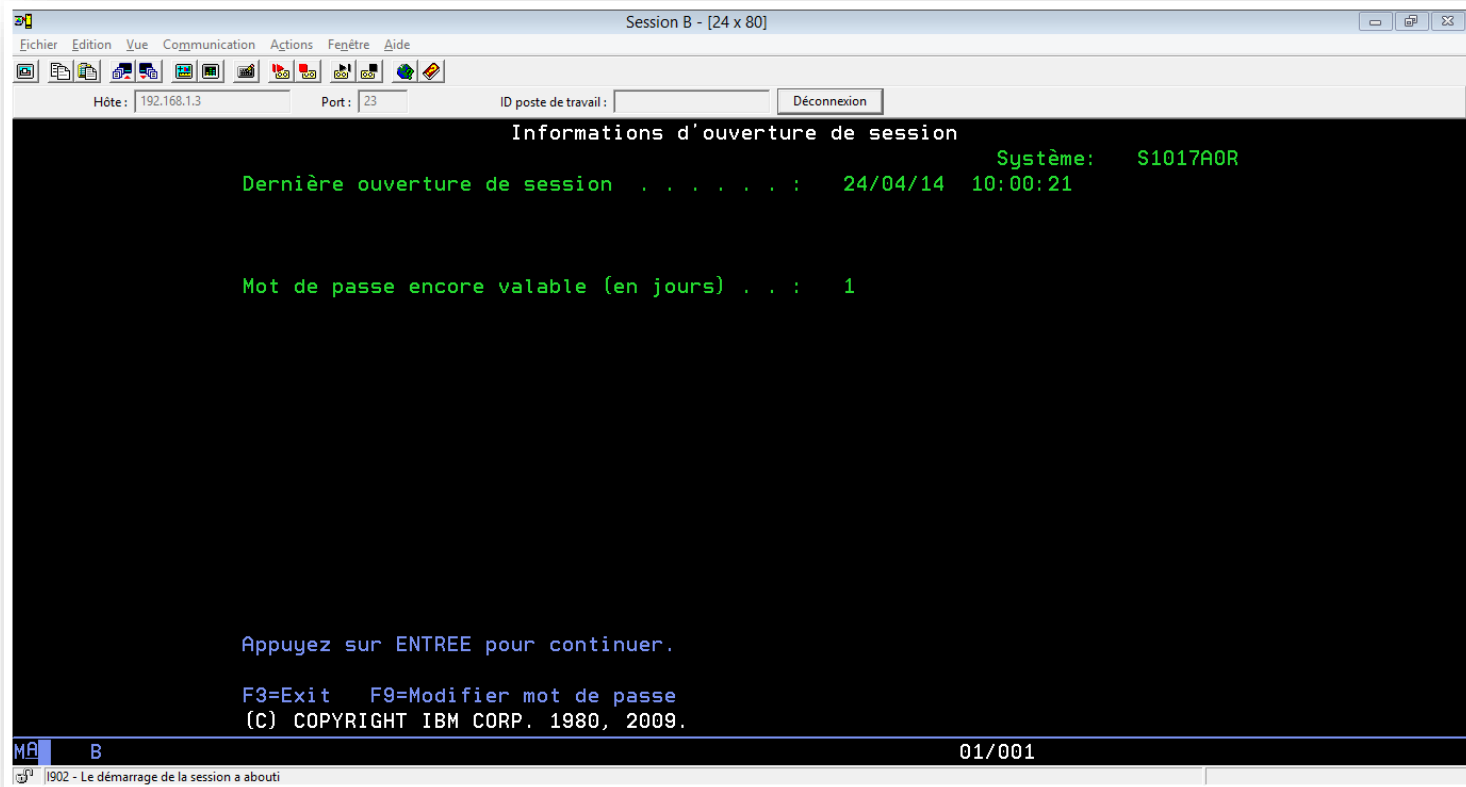
Utiliser un nombre minimal de lettres majuscules et minuscules (0 à 9) :

Utiliser des caractères d'au moins trois des types suivants :

lettres majuscules, lettres minuscules, chiffres et caractères spéciaux

# QPWDEXPWRN

- QPWDEXPWRN définit le délai d'avertissement avant que le mot de passe ne soit expiré (7 jours par défaut)
- Message lors de l'ouverture de session



The screenshot shows a terminal window titled "Session B - [24 x 80]". The window has a menu bar with "Fichier", "Edition", "Vue", "Communication", "Actions", "Fenêtre", and "Aide". Below the menu bar is a toolbar with various icons. The terminal content is as follows:

```
Hôte: 192.168.1.3      Port: 23      ID poste de travail:      Déconnexion
Informations d'ouverture de session
                                Système:  S1017A0R
Dernière ouverture de session . . . . . : 24/04/14 10:00:21

Mot de passe encore valable (en jours) . . : 1

Appuyez sur ENTREE pour continuer.

F3=Exit  F9=Modifier mot de passe
(C) COPYRIGHT IBM CORP. 1980, 2009.
```

At the bottom of the terminal, there is a status bar with "MÂ B" on the left, "01/001" in the center, and a small icon on the right. Below the terminal window, a small status bar reads "1902 - Le démarrage de la session a abouti".

## QPWDCHGBLK

- QPWDCHGBLK empêche les changements de mot de passe répétitifs (heures)
- N'empêche pas
  - Le CHGUSRPRF de l'administrateur
  - La modification si le mot de passe est expiré (PWDEXP(\*YES))
- Pour éviter le contournement de QPWDRQDDIF (empêche la réutilisation des x derniers mots de passe)

# QLMTDEVSSN

- QLMTDEVSSN permet de définir le nombre de sessions écran qu'un utilisateur peut ouvrir
- Avant la V6R1
  - Soit illimité (0)
  - Soit une seule (1)
- A partir de la V6R1
  - 0 : pas de limites
  - 1 à 9 : nombre sessions autorisées

```
Session A - [24 x 80]
Fichier Edition Vue Communication Actions Fenêtre Aide
Hôte: 192.168.1.3 Port: 23 ID poste de travail: Déconnexion
Définition de valeur pour paramètre LMTDEVSSN
Indiquez votre choix, puis appuyez sur ENTREE.
Sessions limitées à un écran . . *SYSVAL
*SAME 9
*SYSVAL
*YES
*NO
0
1
2
3
4
5
6
7
8
F3=Exit F5=Réafficher F12=Annuler F13=Mode d'emploi invite
F24=Autres touches
M A M W 06/039
1902 - Le démarrage de la session a abouti
```



## Amélioration de la commande DSPUSRPRF

- Ajout de nouvelles informations
- Vérifications du mot de passe infructueuses
- Durée de validité du mot de passe
- Date/Heure de création
- Date/Heure de modification
- Date de la dernière utilisation
- Date/Heure de restauration
- Date d'expiration utilisateur

## 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

# Commande DMPUSRPRF

- DMPUSRPRF vous permet de générer un DUMP d'un profil utilisateur
- Dans un fichier spool QPSYDMPU

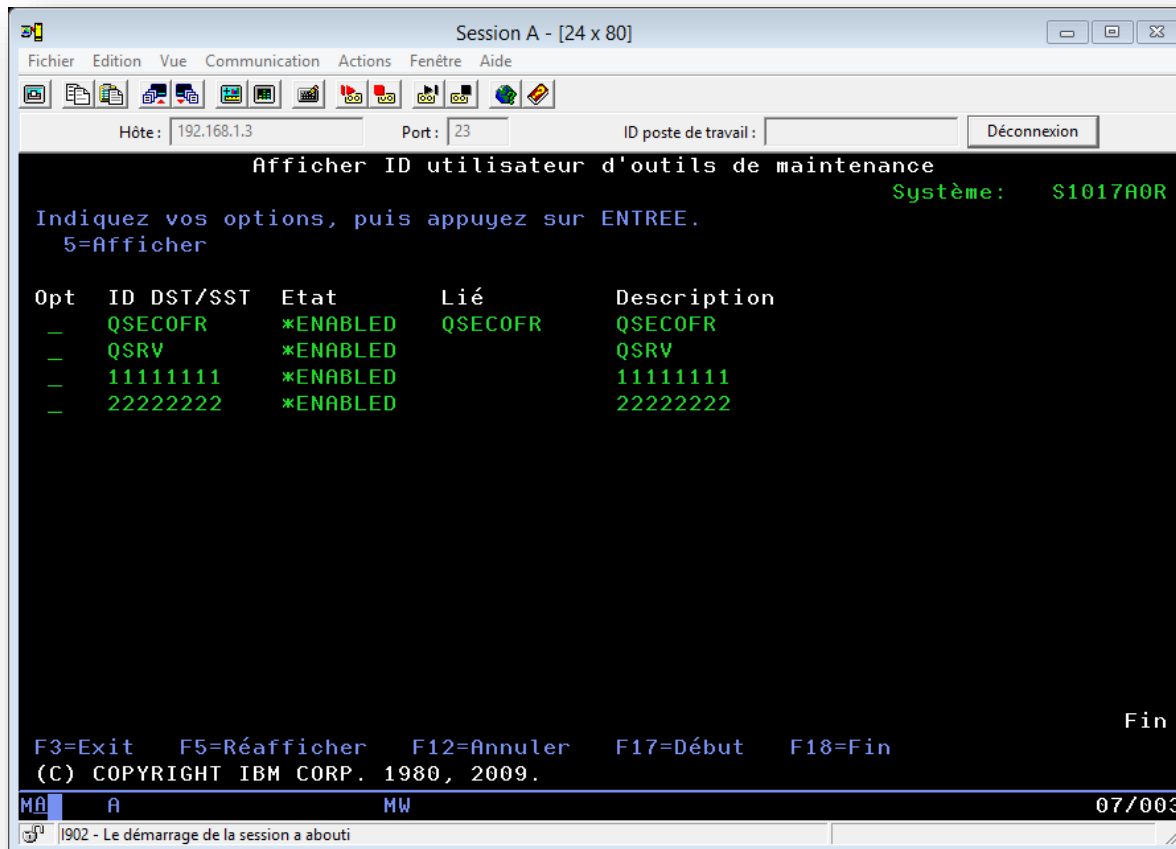
```

Fichier spoule
Fichier . . . . . : QPSYDMPU                               Page/Ligne 11/54
Contrôle . . . . . : B                                   Colonnes 1 - 78
Recherche . . . . . : _____
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
CCSID : *SYSVAL
Séquence de tri : *SYSVAL
Bibliothèque de séquence de tri : *BLANK
Modification bloc mot de passe : *SYSVAL
                                         Profil utilisateur du cliché
5770SS1 V7R1M0 100423
Droits utilisateur obligatoires : Oui
Date d'utilisation de la fonction : *BLANK
Niveau de sauvegarde ASP (hex) : 40
Longueur de sauvegarde ASP : 1706
31 mots de passe précédents (hex) :
                                         7FD8CD355C089E83
                                         4E0DDC0A2BE05D2B
                                         ED62B8B72A0ABCA6
                                         4E0DDC0A2BE05D2B
                                         *BLANK
                                         A suivre...
F3=Exit F12=Annuler F19=Gauche F20=Droite F24=Autres touches

```

# Commande DSPSSTUSR

- DSPSSTUSR affiche la liste des identifiants des *Services Tools (SST/DST)*



The screenshot shows a terminal window titled "Session A - [24 x 80]". The window has a menu bar with "Fichier", "Edition", "Vue", "Communication", "Actions", "Fenêtre", and "Aide". Below the menu bar is a toolbar with various icons. The terminal content is as follows:

```
Session A - [24 x 80]
Hôte: 192.168.1.3   Port: 23   ID poste de travail :   Déconnexion
Afficher ID utilisateur d'outils de maintenance
Indiquez vos options, puis appuyez sur ENTREE.
5=Afficher
                                Système:  S1017A0R

Opt  ID DST/SST  Etat      Lié      Description
-    QSECOFR    *ENABLED  QSECOFR  QSECOFR
-    QSRV       *ENABLED  QSRV     QSRV
-    11111111  *ENABLED  11111111 11111111
-    22222222  *ENABLED  22222222 22222222

F3=Exit  F5=Réafficher  F12=Annuler  F17=Début  F18=Fin
(C) COPYRIGHT IBM CORP. 1980, 2009.
MÂ      A                MW                07/003
| 902 - Le démarrage de la session a abouti
```

# Commande DSPSSTUSR (2)

- Option 5 : visualisation des privilèges

```
Session A - [24 x 80]
Fichier Edition Vue Communication Actions Fenêtre Aide
Hôte: 192.168.1.3 Port: 23 ID poste de travail: Déconnexion

Afficher ID utilisateur d'outils de maintenance
                                Système:  S1017A0R
ID utilisateur d'outils de maintenance . . : 11111111
Privilèges:
Unités de disque - opérations . . . . . : *REVOKED
Unités de disque - administration . . . . : *REVOKED
Unités de disque - lecture seulement . . : *REVOKED
Partitions système - opérations . . . . . : *REVOKED
Partitions système - administration . . . : *REVOKED
Touche d'écran éloignée de partition . . : *GRANTED
Fonctions du panneau de commande . . . . : *GRANTED
IPL du système d'exploitation . . . . . : *GRANTED
Installation . . . . . : *REVOKED
Collecteur des données de performances . . : *GRANTED
Outil Hardware Service Manager . . . . . : *REVOKED
Affichage/Modification/Cliché . . . . . : *REVOKED
Cliché de la mémoire principale . . . . . : *GRANTED
Historique d'activité des produits . . . . : *GRANTED
Historique du microcode sous licence . . . : *REVOKED
Correctifs du microcode sous licence . . . : *GRANTED
Trace . . . . . : *GRANTED

F3=Exit F12=Annuler
                                A suivre...

M A MW 01/001
I902 - Le démarrage de la session a abouti
```

# Rappel sur les PTFs

- PTFs individuelles
- Cumulatives
  - A une date donnée
- Groupes PTF
  - Tout ce qui concerne un thème
  - Base de données, Sécurité, Java, Hiper, TCP/IP
- Technology Refresh (V7R1)
  - Evolutions entre deux versions majeures
  - La TR 7 de la V7R1 a apporté le RPG IV full free, par exemple

# IDS

- Intrusion Detection System
- Détecte si l'AS/400 est soumis à une attaque
- Utilisation de l'audit système
  - QAUDJRN
  - QAUDLVL à *\*ATNEVT*
  - Poste de type IM (Intrusion Monitor)
- Existe depuis la V5R4
- Mais interface graphique à partir de la V6R1

IBM i Security Intrusion detection 7.1

<http://publib.boulder.ibm.com/infocenter/iseriess/v7r1m0/topic/rzaub/rzaub.pdf>

# Mise en œuvre

The screenshot displays the IBM i Security Center interface. On the left is a navigation tree with 'Détection d'intrusion' highlighted. The main window shows the 'Système de détection d'intrusion' status as 'Démarré'. A 'Stratégies de détection d'intrusion' dialog box is open, showing a table of active detection strategies. Below it, the 'Événements de détection d'intrusion' dialog box displays a list of detected events, with one 'Attaque (Paquet mal formé)' event selected.

Nom	Notification IDS	Description
Système de détection d'intrusion	Démarré	Gère la configuration du système IDS sur le systè...

Nom	Type de stratégie	Etat	Adresses IP loc...	Ports loc...	Adresses IP élo...	Ports élo...	Description
Analyse	Analyse	Activé	Tout	Tout	Tout	Tout	
attaque_ACKSTORM	Attaque (ACK Storm T...	Activé	Tout	Tout	Tout	Tout	
attaque_ADRPOISN	Attaque (Corruption d'...	Activé	Tout	Tout	Tout	Tout	
attaque_FLOOD	Attaque (Inondation)	Activé	Tout	Tout	Tout	Tout	

Date et heure	Type	Sens	Adresse IP locale	Port local	Adresse IP éloignée	Port éloigné
11 juil. 2011 17:11:21	Attaque (Paquet mal formé)	Entrant	192.168.1.4	21	192.168.1.14	45022
11 juil. 2011 17:11:21	Attaque (Paquet mal formé)	Entrant	192.168.1.4	21	192.168.1.14	45022
11 juil. 2011 17:11:21	Attaque (Paquet mal formé)	Entrant	192.168.1.4	21	192.168.1.14	45022
11 juil. 2011 17:11:21	Attaque (Paquet mal formé)	Entrant	192.168.1.4	21	192.168.1.14	45022
11 juil. 2011 17:13:44	Analyse	Entrant	192.168.1.4	45779	41.102.150.18	19179
11 juil. 2011 17:13:44	Analyse	Entrant	192.168.1.4	45779	41.102.150.18	19179
11 juil. 2011 17:18:52	Analyse	Entrant	192.168.1.4	45779	109.89.67.65	51814
11 juil. 2011 17:18:53	Analyse	Entrant	192.168.1.4	45779	109.89.67.65	51814
11 juil. 2011 17:18:53	Analyse	Entrant	192.168.1.4	45779	109.89.67.65	51814



# Propriétés

- A partir de System i Navigator

The image shows two screenshots from the System i Navigator interface. The left screenshot displays a table with columns 'Nom', 'Notification IDS', and 'Description'. A context menu is open over the first row, with the 'Propriétés' option circled in orange. The right screenshot shows the 'Propriétés IDS - 192.168.1.3' dialog box. The 'Notification' is set to 'ICMP'. The 'Envoi de notifications par message' checkbox is checked, with 'File d'attente de messages' set to 'QSYSOPR' and 'Bibliothèque' set to 'QSYS'. Under 'Destination des notifications par courrier électronique', the 'Adresse e-mail 1' checkbox is checked and set to 'dgayte@notos.fr'.

Nom	Notification IDS	Description
Système de détecti...		ion du système IDS sur le systè...

Propriétés IDS - 192.168.1.3

Notification: ICMP

Envoi de notifications par message :

File d'attente de messages : QSYSOPR

Bibliothèque : QSYS

Destination des notifications par courrier électronique

Adresse e-mail 1 : dgayte@notos.fr

Adresse e-mail 2 :

Adresse e-mail 3 :

OK Annuler Aide ?

# Pour tester

## ■ Scanner

- Nmap
- SuperScan (McAfee)
- Et bien d'autres



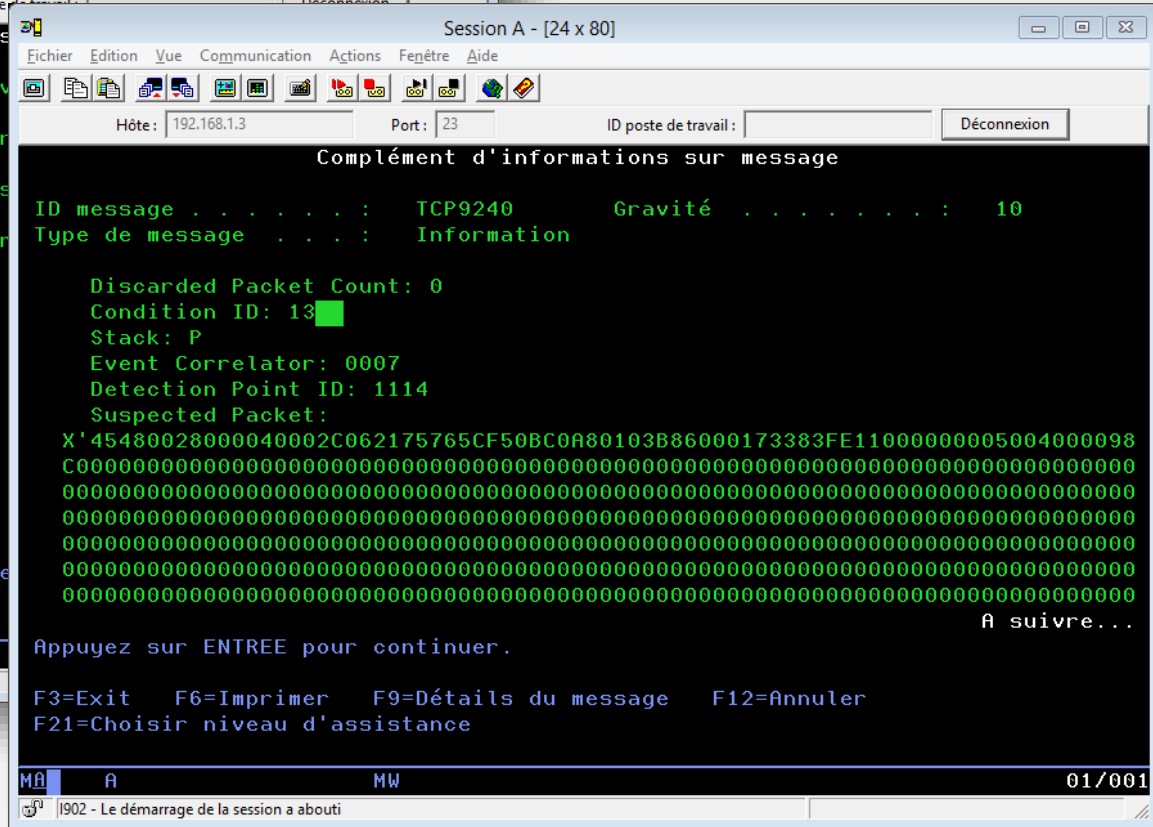
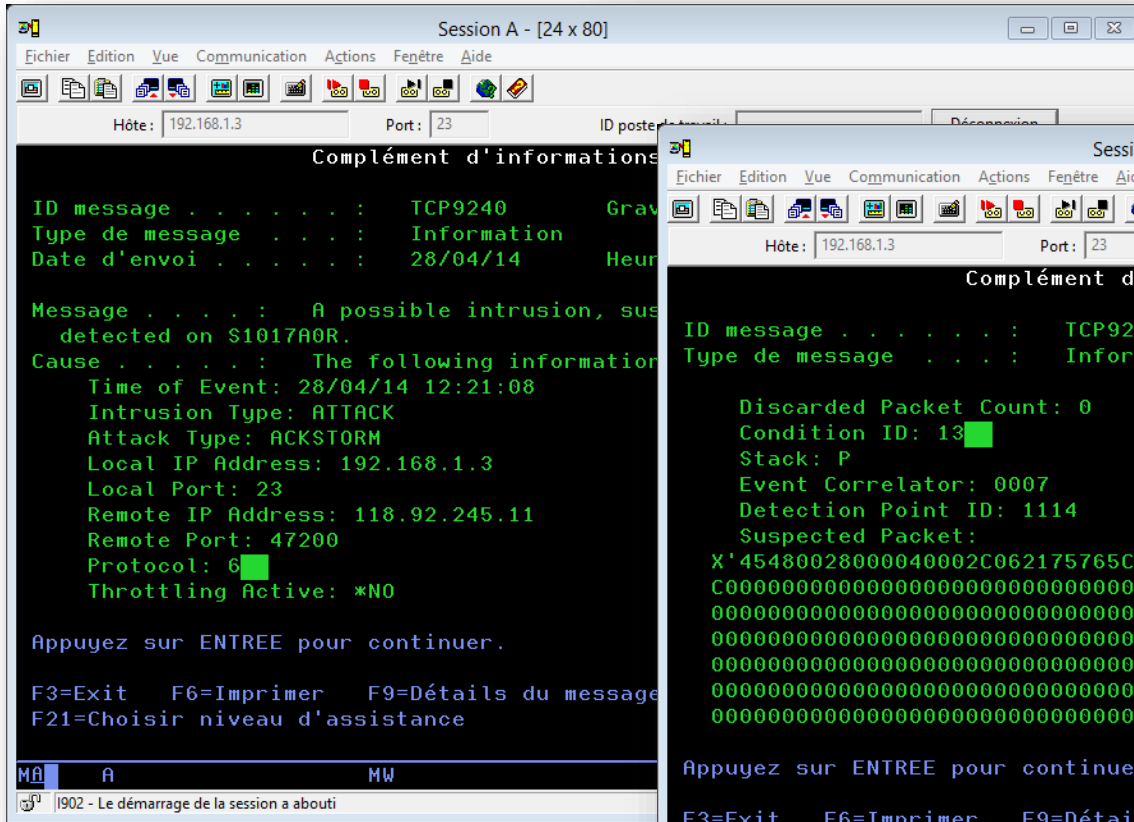
```
zenmap
Scan  Outils  Profil  Aide
Cible: 192.168.1.4  Profil: Intense scan, all TCP ports  [Scan]  [Annuler]
Commande: nmap -p 1-65535 -T4 -A -v 192.168.1.4

hôtes  Services
Sortie de Nmap  Ports / hôtes  Topologie  Détails de l'hôte  Scans
OS  hôte
  lucane.home (192.168.1.4)
  2017/tcp  open  http  Lotus Notes Expeditor
  httpd 6.1
  |_ http-title: Site doesn't have a title (text/html; charset=ISO-8859-1).
  |_ http-methods: No Allow or Public header in OPTIONS response (status code 404)
  2018/tcp  open  terminaldb?
  3000/tcp  open  as-sts  IBM Service Tool
  Server AS-STs
  4800/tcp  open  iims?
  5544/tcp  open  unknown
  5555/tcp  open  freeciv?
  6079/tcp  open  unknown
  8000/tcp  open  http  Apache httpd 2.2.6
  ((Unix) mod_ssl/2.2.6 OpenSSL/0.9.8j Zend Core/2.6.1 PHP/5.2.6)
  |_ http-title: 403 Forbidden
  |_ http-methods: No Allow or Public header in OPTIONS response (status code 403)
  8470/tcp  open  cisco-avp?
  8471/tcp  open  pim-port?
  8472/tcp  open  otv?
  8473/tcp  open  unknown
  8474/tcp  open  noteshare?
  8475/tcp  open  unknown
  8476/tcp  open  as-signon  IBM Client Tools signon
  8477/tcp  open  unknown
  8478/tcp  open  unknown
  8479/tcp  open  unknown
  10000/tcp  open  http  Lotus Notes Expeditor
  httpd 6.1
  |_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
  |_ http-methods: No Allow or Public header in OPTIONS response (status code 404)
  10002/tcp  open  http  Lotus Notes Expeditor
```

# Alertes

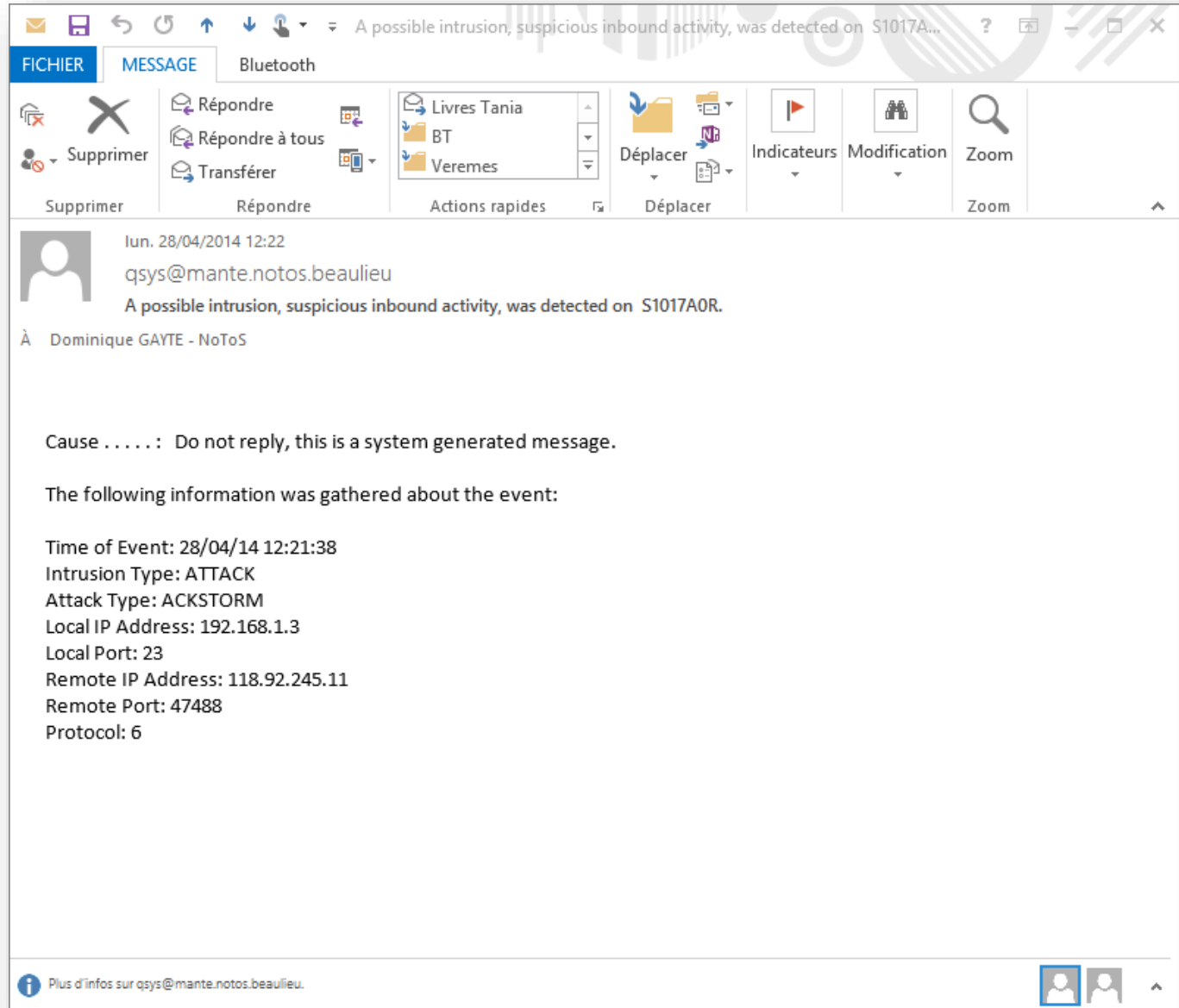
- Dans QSYSOPR

Profil util FMICHIEL désactivé pour l'accès au support IBM pour la fonction Voisinage réseau de Windows.  
 A possible intrusion, suspicious inbound activity, was detected on S1017A0R.



## Alertes (2)

- E-mail



The screenshot shows an email client window with the following content:

**Subject:** A possible intrusion, suspicious inbound activity, was detected on S1017A...

**From:** qsys@mante.notos.beaulieu

**To:** À Dominique GAYTE - NoToS

**Content:**

Cause . . . . . : Do not reply, this is a system generated message.

The following information was gathered about the event:

Time of Event: 28/04/14 12:21:38  
Intrusion Type: ATTACK  
Attack Type: ACKSTORM  
Local IP Address: 192.168.1.3  
Local Port: 23  
Remote IP Address: 118.92.245.11  
Remote Port: 47488  
Protocol: 6

At the bottom, there is a link: [Plus d'infos sur qsys@mante.notos.beaulieu.](#)

## 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
- 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
  - 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

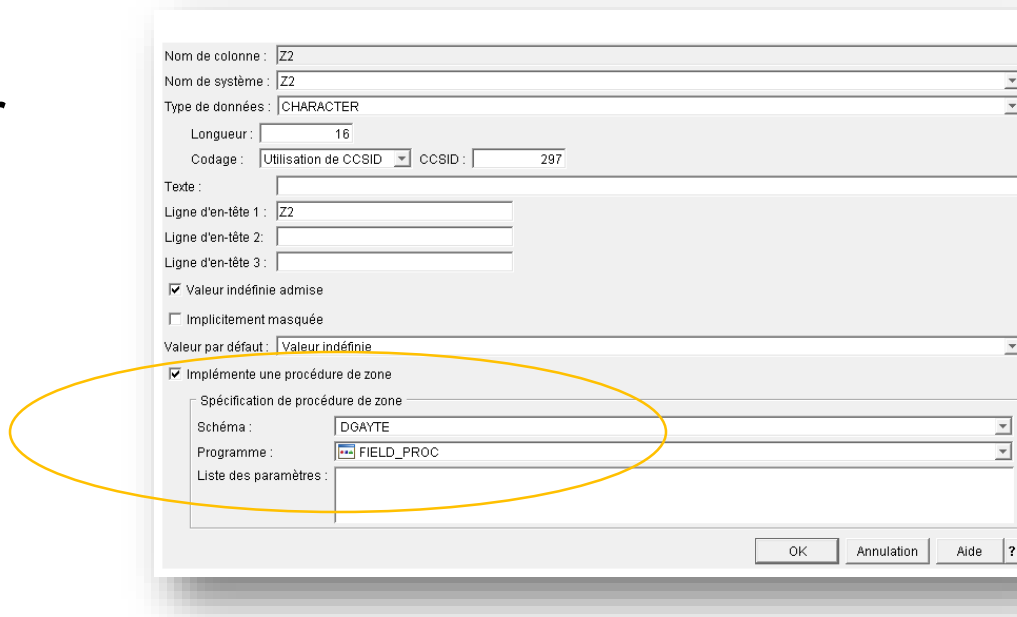
Z1	Z2
1	****56789012345
2	****654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

# Visualisation

- System i Navigator



- DSPFFD

```

Informations de niveau zone
Zone      Type      Long  Long  Position  Usage  En-tête
          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

Z1	Z2
1	123456789012345
2	3210654987123122

## Autre

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

Navigator

Z1	Z2
1	123456789012345
2	3210654987123122

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

STRSQL

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

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

DSPPFM

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

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

DSPJRN

## 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'

# Cryptographie

- Amélioration des interfaces de gestion des clés
- Amélioration Hardware spécifique
- Logiciels sous licences supplémentaires

## Clés principales

- Gestion graphique depuis la V6R1 (Sécurité/ Gestion des clés des services cryptographiques)

Les clés principales sont utilisées pour chiffrer d'autres clés. Vous pouvez charger, définir, effacer ou afficher les propriétés de la clé principale sélectionnée.

Clé principale	Etat	Valeur de vérification de la clé en cours
1	Définie	B8EB7EDCE147DB12125A9C82E073AE162CB228D4
2	Non définie	
3	Non définie	
4	Non définie	
5	Non définie	
6	Non définie	
7	Non définie	
8	Non définie	
SAVRST	Par défaut	16C1D3E3C073E77DB28F33E81EC165313318CE54
ASP	Non définie	

Fermeture Aide ?

- Attention la clé pour les sauvegardes ci-dessus est la valeur par défaut, c'est la même pour tous les IBM i ! Est utilisée lors d'un SAVSYS !

# Définition d'une clé : paraphrase

```

Add Master Key Part (ADDMSTPART)

Indiquez vos choix, puis appuyez sur ENTREE.

Master key . . . . . > 3          1-8, *ASP, *SAVRST
Passphrase . . . . . Ceci est la paraphrase de la clé principale
3
-----
Length of passphrase . . . . . *CALC      1-256, *CALC
    
```

Option ou commande  
 ==> SETMSTKEY MSTKEY(3)

Gestion des clés principales

Les clés principales sont utilisées pour chiffrer d'autres clés. Vous pouvez charger, définir, effacer ou afficher les propriétés de la clé principale sélectionnée.

Clé principale	Etat	Valeur de vérification de la clé en cours
1	Définie	B8EB7EDCE147DB12125A9C82E073AE162CB228D4
2	Définie	6EF589F974F4EAB33922670DEA2C83C9A95B5D9F
3	Définie	51283B7BE65EE0149918BB83DE61A54D3E55CAB2
4	Non définie	
5	Non définie	
6	Non définie	
7	Non définie	
8	Non définie	
SAVRST	Par défaut	16C1D3E3C073E77DB28F33E81EC165313318CE54
ASP	Non définie	

Fermeture Aide ?

**CLRMSTKEY MSTKEY(2) VERSION(\*CURRENT)**

## Fichier de clés

- Gestion graphique depuis la V6R1 (Sécurité/ Gestion des clés des services cryptographiques)
- Sert à crypter les clés qui cryptent
  - Des clés (Key Encrypting Key (KEK))
  - Des données
- Crypté à partir d'une clé principale
- C'est un fichier classique (PF) mais avec des droits d'accès spécifiques
- Q1AKEYFILE de QUSRBRM est utilisé par BRMS

# Cryptographie des supports de sauvegarde

- Unités de sauvegarde LTO 4 et 5 et TS11xx
  - Mise à jour facturable (hardware et microcode)
- Librairies TS3100/3200/3310/3400/3500
- C'est l'unité de sauvegarde qui effectue le cryptage (clés fournies par TKLM)
- Tivoli Lifecycle Key Manager (TKLM)
  - Infrastructure de gestion des clés
  - Indispensable pour la cryptographie des sauvegardes
  - Peut être sur Linux/Windows/AIX/ZOS



## Attention !

- Si vous cryptez les sauvegardes, assurez vous de pouvoir restaurer
- Où sont les clés ?
- TKLM est-il sauvegardé ?
- L'architecture est elle redondante ?
- Faites des tests !



# Cryptographie des SAN

- SAN DS5000 et DS8000
- Cryptage de la totalité des disques
- DS8000 avec TKLM
- DS5000 plus varié

## IBM i Encrypted Backup Enablement 5761SS1 option 44

- Logiciel facturable
- Utilisé pour crypter les sauvegardes sur tous supports
- Possibilité de crypter une copie (la sauvegarde d'origine reste en clair)

# Cryptage et BRMS

- Cryptage avec BRMS
  - Advanced Feature 5761BR1 option 2
  - IBM i Encrypted Backup Enablement – 5761-SS1 option 44
- Pas de SAVSYS, SAVSECDTA, SAVCFG, SAVLIB(\*IBM) ou SAVLIB (Q\*)
- Pas de SAVF ou d'unités optiques
- Performances
  - Plus long car c'est l'IBM i qui travaille
  - Plus de CPU consommé
  - (Beaucoup !) Plus de place utilisée sur le support

```

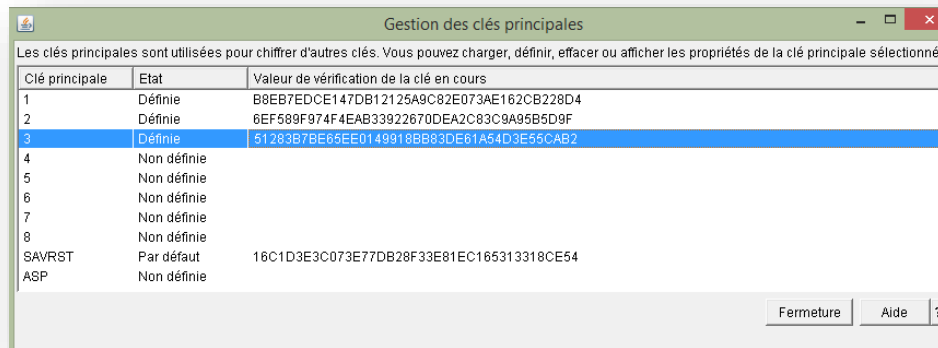
                                Create Media Policy

Type choices, press Enter.

Encrypt Data . . . . . *YES          *NO, *YES
Key store file . . . . . Q1AKEYFILE  Name
Key store library. . . . . QUSRBRM   Name
Key record label . . . . . MONTEST
  
```

## 5770-SS1 Option 45 - Encrypted ASP Enablement

- Cryptage des disques d'un ASP, facturable
- ASP utilisateur ou iASP
- Configurer la clé principale « ASP »



- L'IBM i (microcode) gère les clés de cryptage à partir de la clé principale « ASP »
- Attention à la CPU consommée

# SSL

- SSL est utilisé pour crypter les données qui circulent sur le réseau
- Voir présentation de 2013

# OpenSSL – Vulnérabilité Heartbleed



- Possibilité de récupérer des informations liées à SSL à cause de la défaillance d'une fonctionnalité TLS
- Pas d'authentification nécessaire, peu complexe à utiliser
- Serveurs impactés <https://www-304.ibm.com/support/docview.wss?uid=nas8N1020034>
- Firmware des Power Systems (DSPFMWSTS) à mettre à jour

**Versions (770):**

770.00: 01AL770\_032  
770.10: 01Ax770\_038  
770.20: 01Ax770\_048  
770.21: 01Ax770\_052  
770.22: 01Ax770\_055  
770.31: 01Ax770\_063

**Platforms Impacted (770):**

IBM Power 780 (9179-MHC)  
IBM Power 770 (9117-MMC)  
IBM Power 760 (9109-RMD)  
IBM Power 750 (8408-E8D)  
IBM PowerLinux 7R4 (8248-L4T)  
IBM PowerLinux 7R2 (8246-L2D)  
IBM PowerLinux 7R2 (8246-L2T)  
IBM PowerLinux 7R1 (8246-L1D)  
IBM PowerLinux 7R1 (8246-L1T)  
IBM Power 740 (8205-E6D)  
IBM Power 730 (8231-E2D)  
IBM Power 720 (8202-E4D)  
IBM Power 720 (8202-40A)  
IBM Power 710 (8231-E1D)  
IBM Power 710 (8268-E1D)

**Version (780):**

780.00: 01Ax780\_040  
780.01: 01Ax780\_050

**Platforms Impacted (780):**

IBM Power 795 (9117-FHB)  
IBM Power 780 (9179-MHB)  
IBM Power 770 (9117-MMB)

**Version (773):**

773.00: 01AF773\_033  
773.10: 01AF773\_051

**Platforms Impacted (773):**

IBM Flex System p270 (7954-24X)  
IBM Flex System p260 (7895-23X)  
IBM Flex System p260 (7895-23A)  
IBM Flex System p460 (7895-43X)  
IBM Flex System p260 (7895-22X)  
IBM Flex System p460 (7895-42X)  
IBM Flex System p24L (1457-7FL)

# SSL : valeurs système QSSLCSL

- **Secure Sockets Layer (SSL) cipher specification list (QSSLCSL)**
  - Liste les algorithmes de chiffrement disponibles pour SSL (V6R1)

```
Session A - [24 x 80]
Fichier Edition Vue Communication Actions Fenêtre Aide
Hôte: 192.168.1.3 Port: 23 ID poste de travail : Déconnexion
Valeur système
Valeur système . . . . : QSSLCSL
Description . . . . . : Liste spécif chiffrement du protocole SSL

Numéro de séquence      Algorithme de cryptage
0
10 *RSA_AES_128_CBC_SHA
20 *RSA_RC4_128_SHA
30 *RSA_RC4_128_MD5
40 *RSA_AES_256_CBC_SHA
50 *RSA_3DES_EDE_CBC_SHA
60 *RSA_DES_CBC_SHA
70 *RSA_EXPORT_RC4_40_MD5
80 *RSA_EXPORT_RC2_CBC_40_MD5
90 *RSA_NULL_SHA

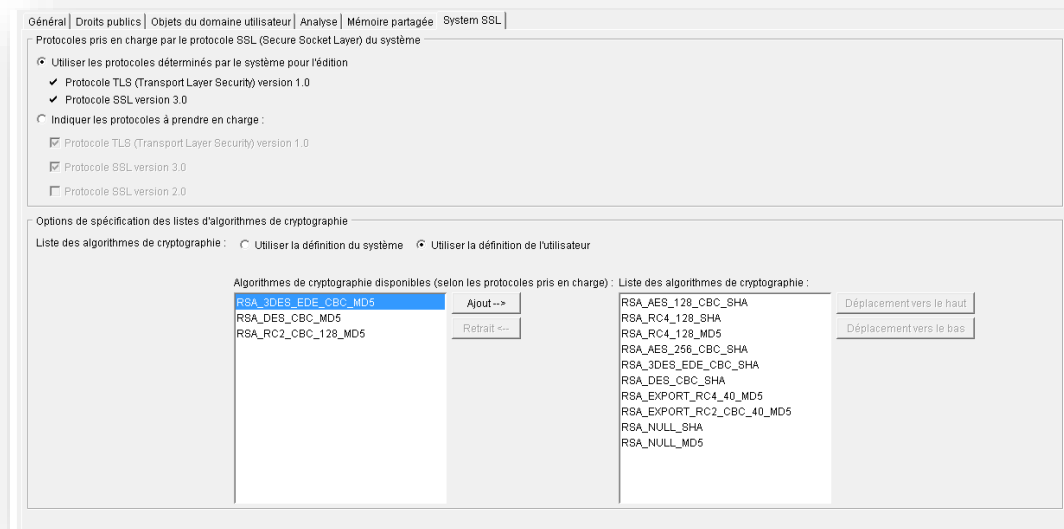
A suivre...

Appuyez sur ENTREE pour continuer.
F3=Exit F12=Annuler
MA A 01/001
1902 - Le démarrage de la session a abouti
```

# SSL : valeurs système QSSLCSLCTL

## ■ Secure Sockets Layer (SSL) cipher control (QSSLCSLCTL)

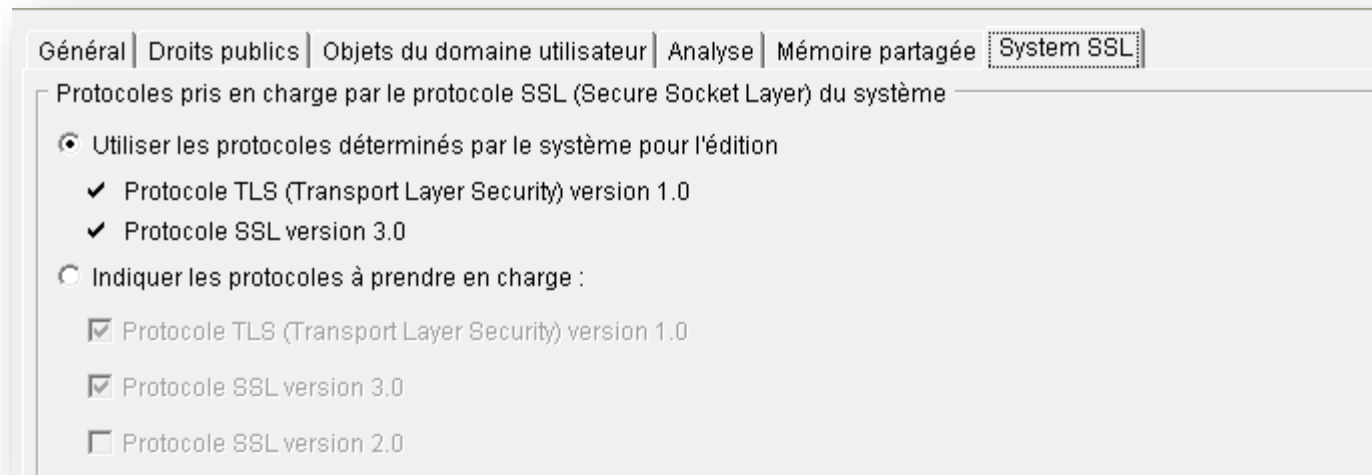
- Contrôle le chiffrement SSL.
- \*OPSYS : Indique que la liste des chiffrements (QSSLCSL ) est constituée automatiquement lors des mises à jour du système
- \*USRDFN : c'est à l'utilisateur de modifier cette liste
  - System i Navigator de préférence !





# SSL : valeurs système QSSLPCL

- **Secure Sockets Layer (SSL) protocols (QSSLPCL)**
  - Indique les protocoles supportés (SSL V3, V2, TLS V1...)



## SSL : Telnet

- Possibilité de démarrer une session TELNET 5250 cliente en SSL (V7R1, mais PTF jusqu'à la V5R4)
- Nécessite la configuration de certificats (DCM)
- Paramètre SSL de la commande TELNET (client)
  - \*YES
  - \*NO
  - \*ENVVAR : fait référence à la variable d'environnement QIBM\_TELNET\_CLIENT\_SSL (Y pour SSL)
- Ou de CHGTELNA (serveur)
  - \*YES : optionnel
  - \*ONLY : SSL obligatoire

## 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

## 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

## Vérification des clés générées

- Pour vérifier, afficher la liste des clés
  - Dans QSH
    - KEYTAB LIST

```
Principal: nfs/mante.notos.beaulieu@NOTOS.BEAULIEU  
Key version: 1  
Key type: 128-bit AES  
Entry timestamp: 2014/04/29-15:12:10
```

```
Principal: nfs/mante.notos.beaulieu@NOTOS.BEAULIEU  
Key version: 1  
Key type: 256-bit AES
```

# Conséquences

- A priori pas de modification pour l'existant
  - Continue d'utiliser DES
  - Mais attention en cas de changement de système
- Pour les nouvelles configuration
  - Ce n'est plus la peine de forcer l'utilisation de DES sur l'AD
    - set +DesOnly à enlever du script de configuration
  - Ce n'est plus la peine de forcer l'utilisation de DES sur les postes Windows

## Sauvegardes/restaurations des droits privés

- En V6R1 possibilité de sauvegarder (restaurer) les droits privés sur un objet
- Avant les droits privés étaient sauvegardés uniquement avec les profils utilisateur. Lors de la restauration
  - RSTUSRPRF
  - RSTOBJ
  - RSTAUT afin de régénérer les droits privés
- Paramètre PVTAUT des commandes SAVxxx et RSTxxx
  - Par défaut \*NO

```
                               Sauvegarder objet (SAVOBJ)

Indiquez vos choix, puis appuyez sur ENTREE.

Droits privés . . . . . PVTAUT      *NO
Mémoire secondaire . . . . . STG      *KEEP
```



IBM Power Systems - IBM i

## S8 - Sécurité IBM i : nouveautés 6.1 et 7.1

Merci de votre attention

Dominique GAYTE- [dgayte@notos.fr](mailto:dgayte@notos.fr)  
04 30 96 97 33  
[www.notos.fr](http://www.notos.fr)

