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

NoToS

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

php.Spool

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

LoReNa

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

Sommaire

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

Profils utilisateur – Mot de passe - QPWDRULES

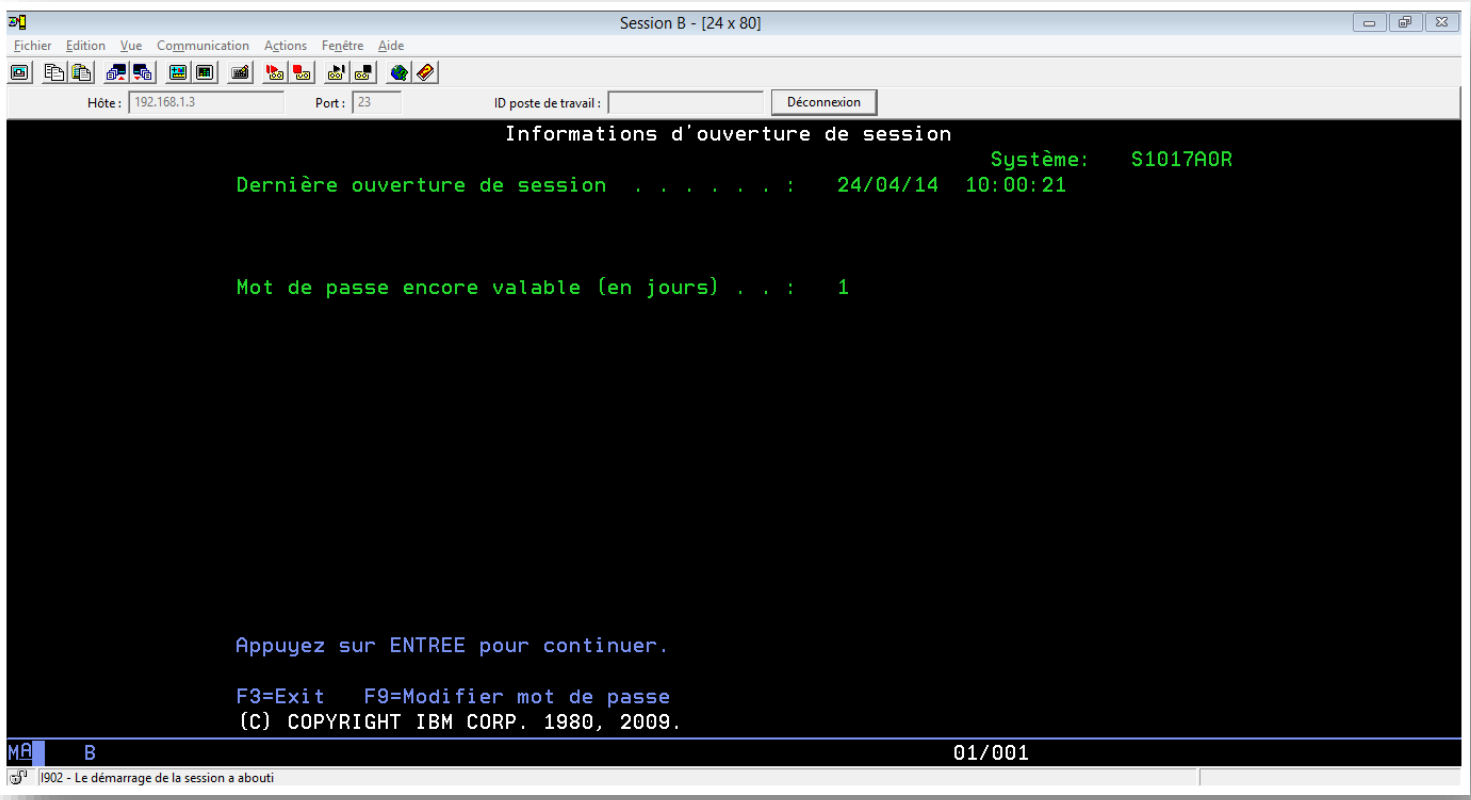
- Nouvelle valeur système (ou dans les profils) de la V6R1
- QPWDRULES permet de mieux correspondre aux règles générales du système d'information
  - *PWDSYSVAL : valeur par défaut (comme avant, utilise les autres valeurs système : QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF 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
  - *DGTMIN**n** : 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

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

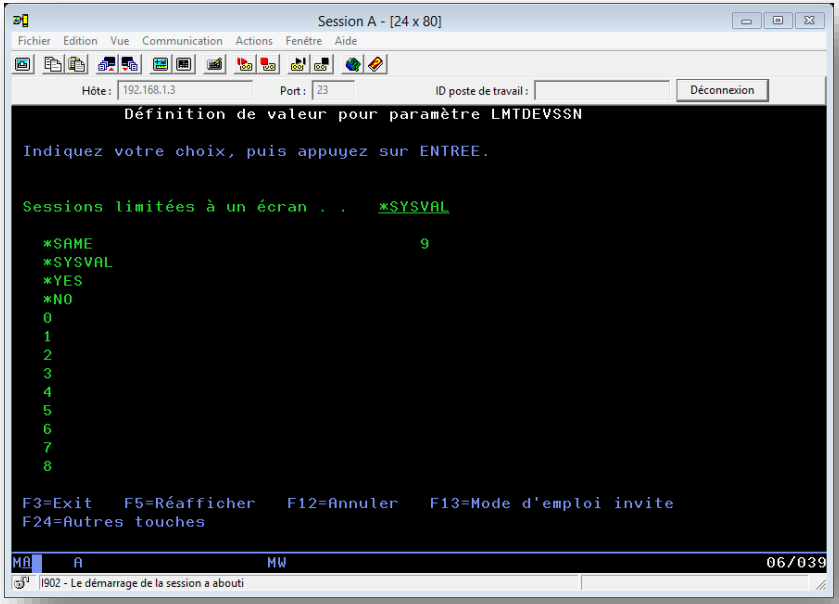


QPWDCHGBLK

- 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



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

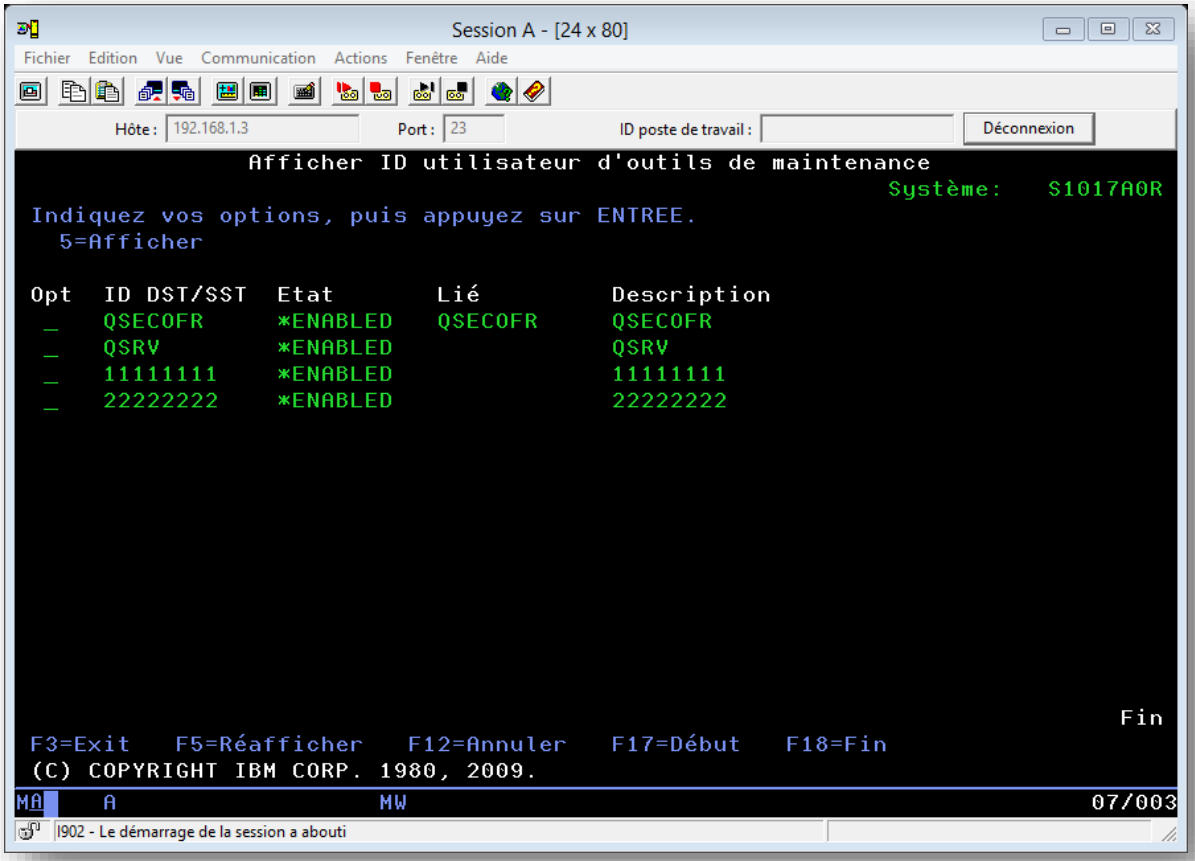
- Deux nouveaux paramètres en V7R1
- USREXPDATE : Mise hors fonction (*DISABLED) d'un profil utilisateur à une date donnée
  - *NONE : pas d'expiration
  - Date : date d'expiration (au format du JOB)
  - * USREXPITV : date calculée à partir du paramètre USREXPITV
- USREXPITV : durée avant expiration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

Commande DMPUSRPRF

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

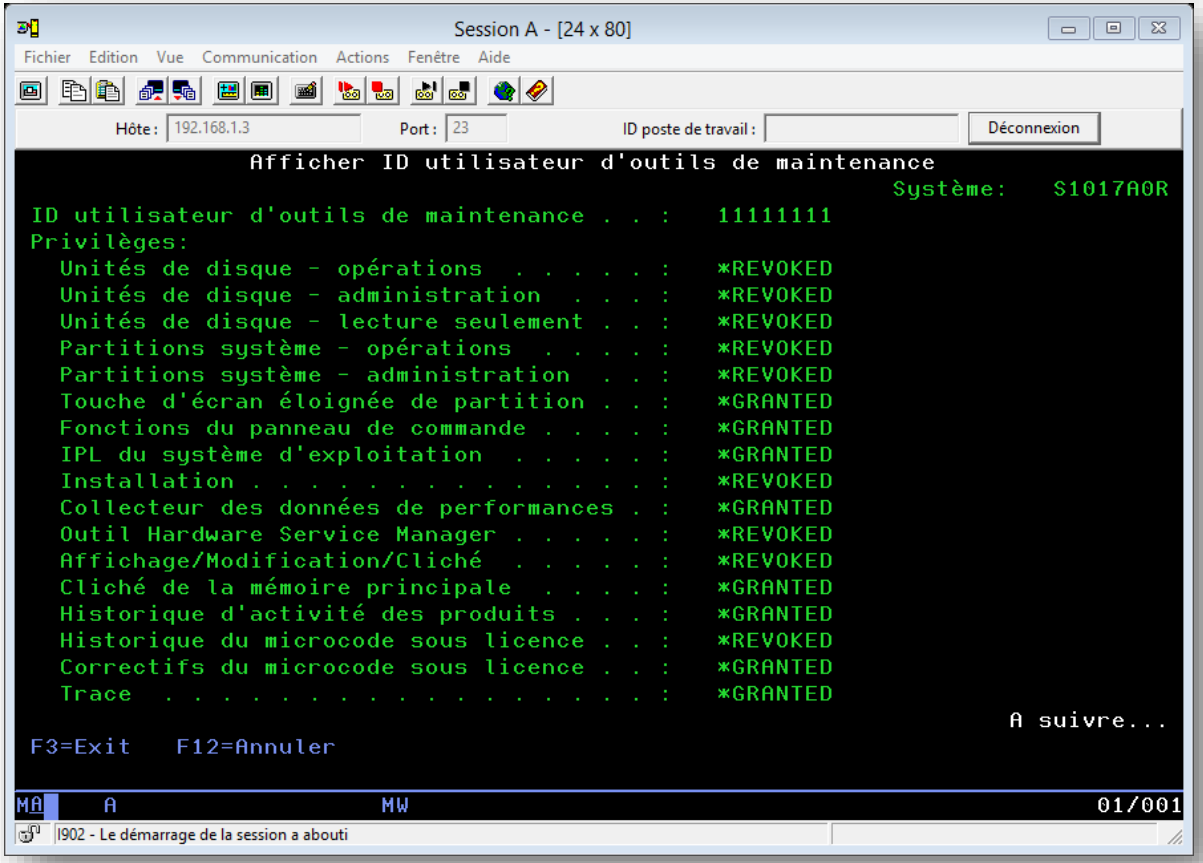
Commande DSPSSTUSR

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



Commande DSPSSTUSR (2)

- Option 5 : visualisation des privilèges



Rappel sur les PTFs

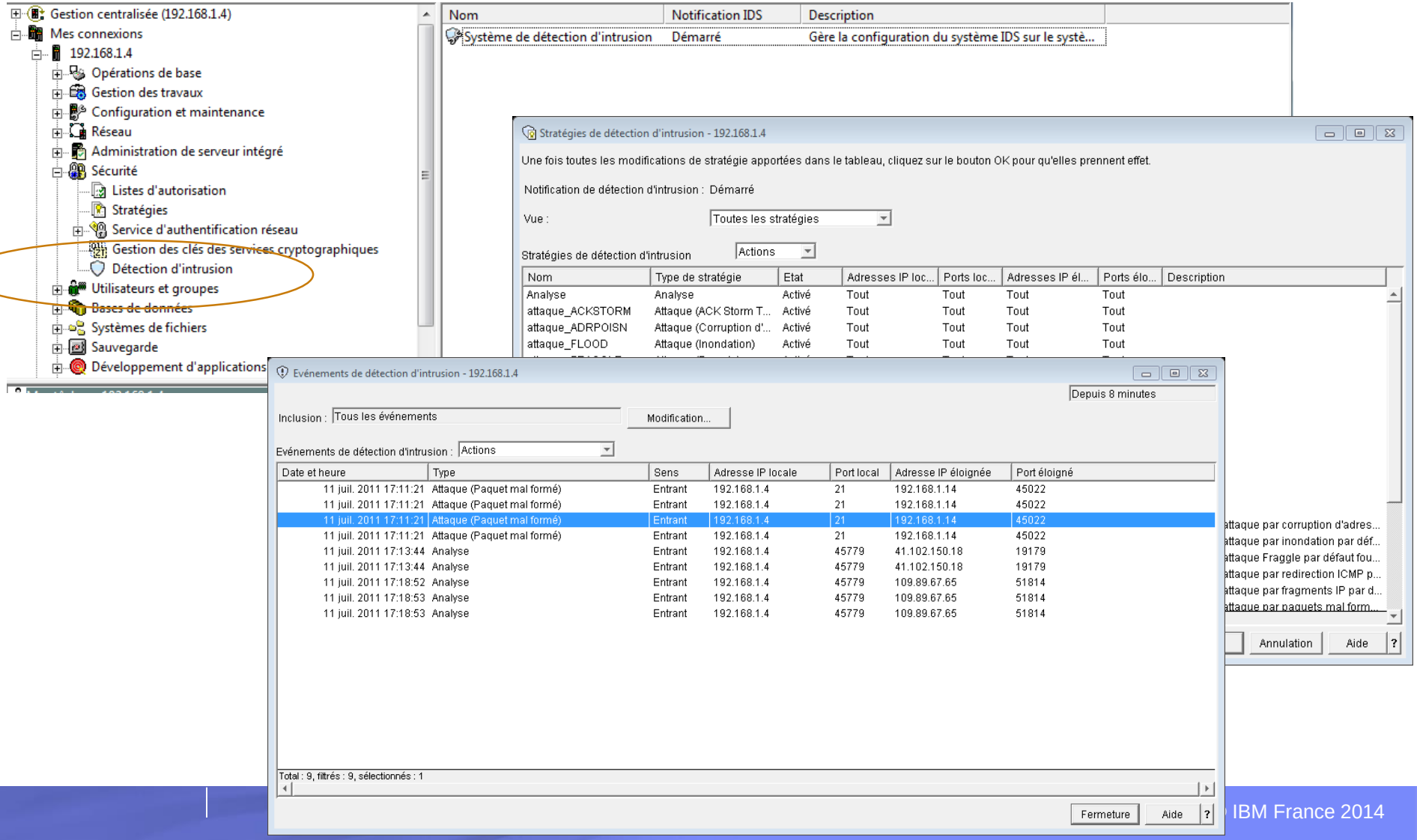
- PTFs individuelles
- Cumulatives
  - A une date donnée
- Groupes PTF
  - Tout ce qui concerne un thème
  - Base de données, Sécurité, Java, Hiper, TCP/IP
- Technology Refresh (V7R1)
  - Evolutions entre deux versions majeures
  - La TR 7 de la V7R1 a apporté le RPG IV full free, par exemple

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

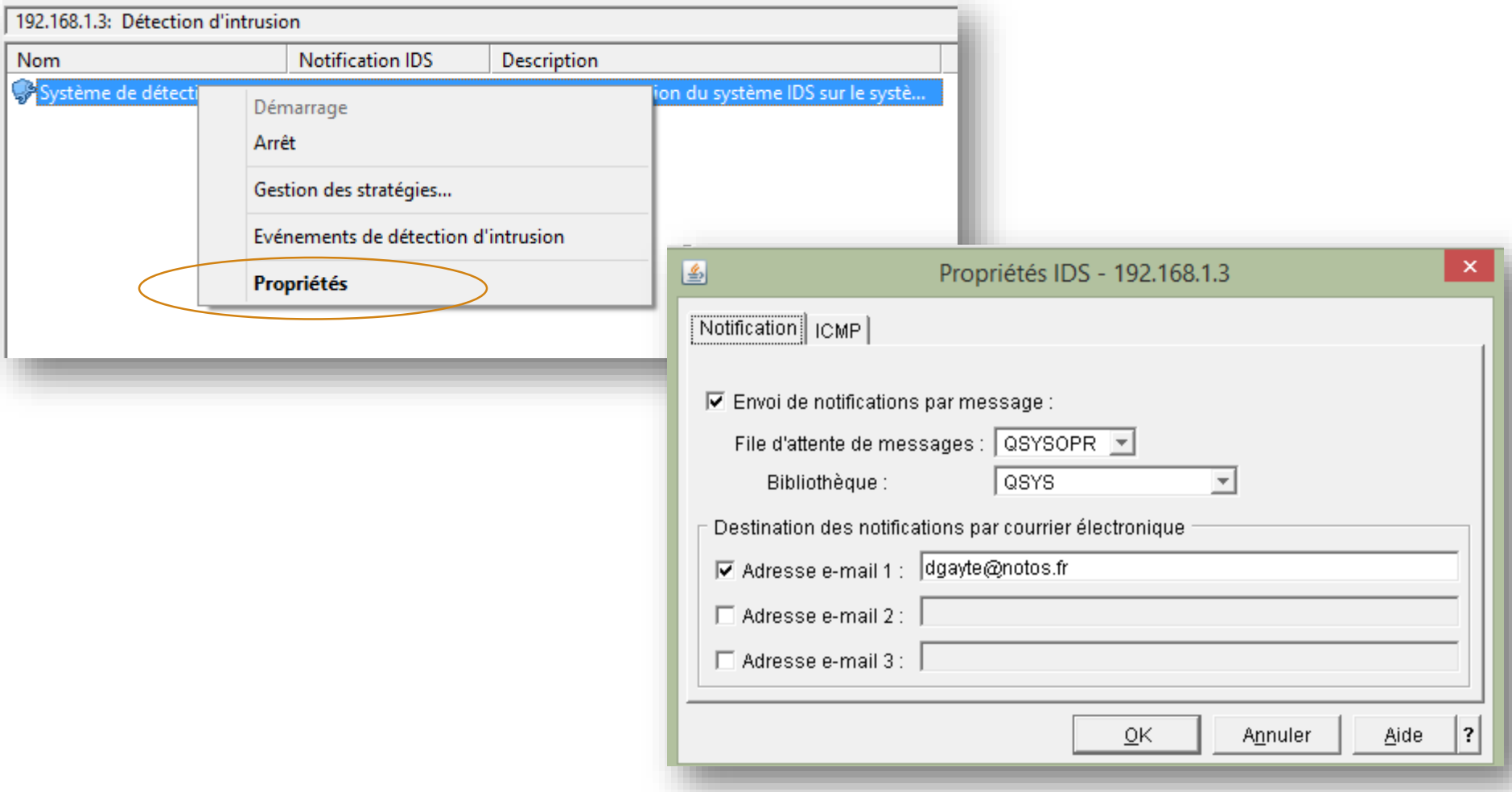
IBM i Security Intrusion detection *7.1*
http://publib.boulder.ibm.com/infocenter/iseries/v7r1m0/topic/rzaub/rzaub.pdf

Mise en œuvre



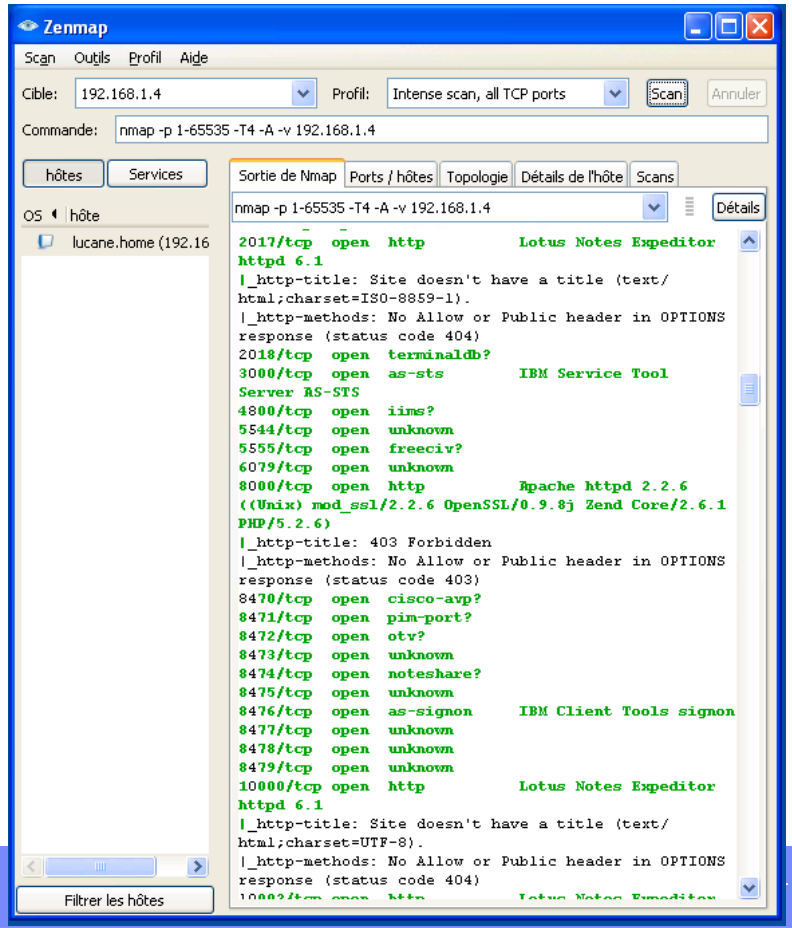
Propriétés

- A partir de System i Navigator



Pour tester

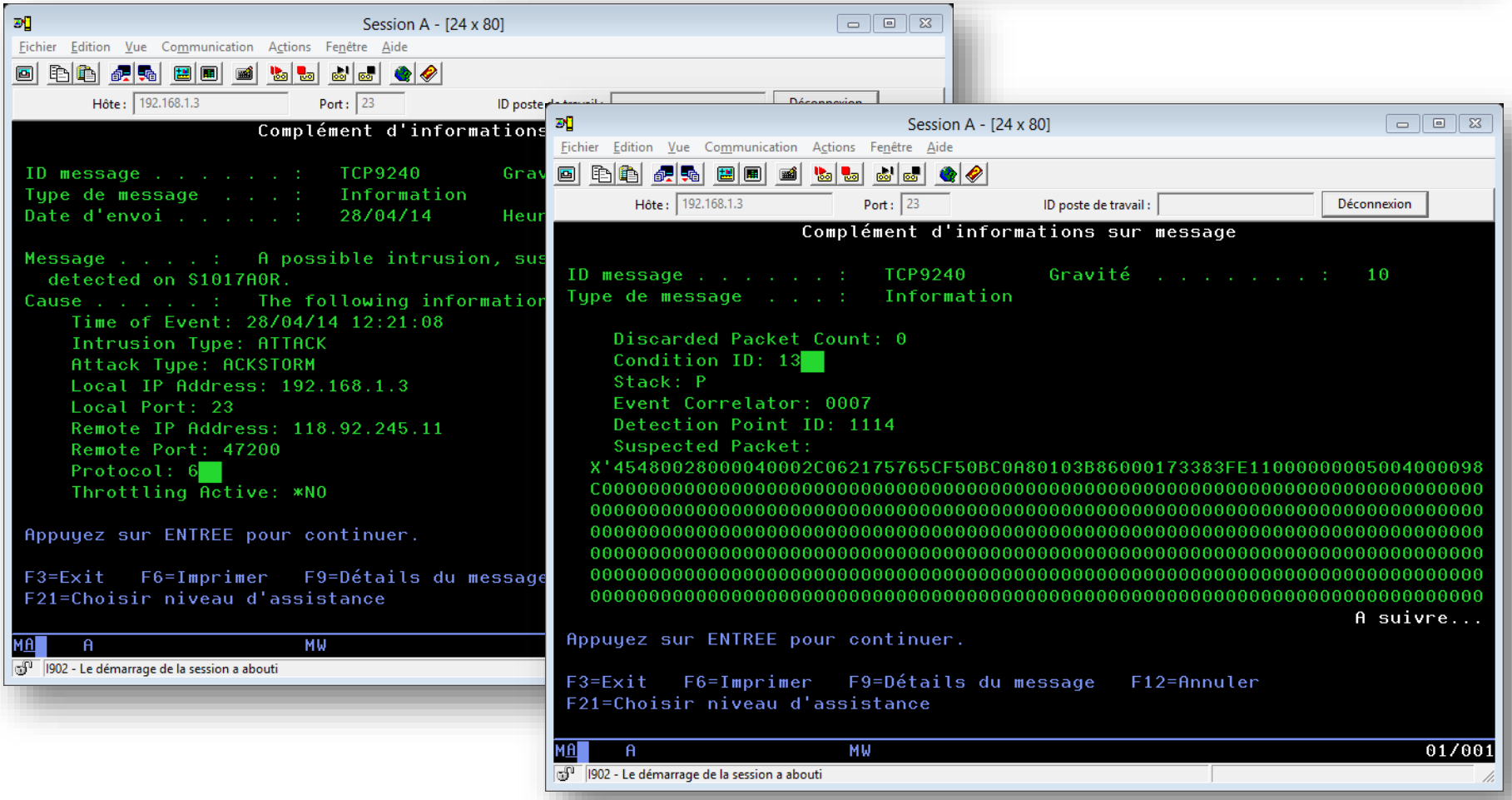
- Scanner
  - Nmap
  - SuperScan (McAfee)
  - Et bien d'autres



Alertes

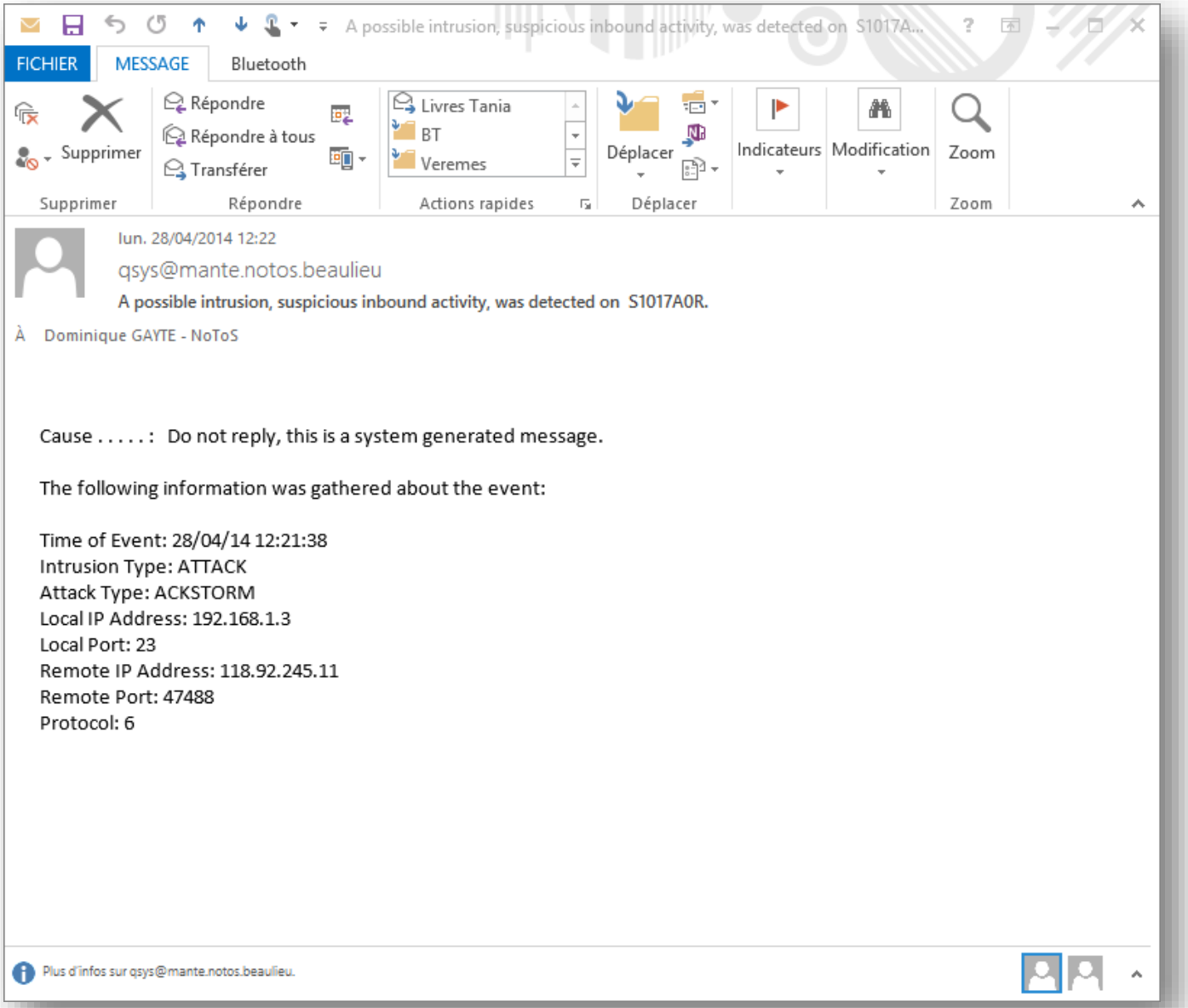
- Dans QSYSOPR

```
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



DB2 : *Field Procedure*

- Programme d'exit appelé à chaque action sur la colonne (insert/update/read)
- Quelle que soit l'origine (SQL, RPG, ODBC…) !
- Sorte de trigger sur une colonne
- Ajouté avec un ALTER TABLE (ou CREATE)
- Un *field procedure* par colonne
- Utilisé notamment pour crypter les données d'une colonne !
  - Totalement
  - Ou partiellement
- Apparu en V7R1

Programme appelé

- Le programme appelé est un *PGM ILE
  - Pas d'OPM, pas de *SRVPGM, pas de Java
  - Pas de SQL autorisé, pas de ACTGRP(*NEW)
- Reçoit 9 paramètres
- Assez complexe

Codification

- Exemple : cryptage des 4 premiers caractères du n° carte
  - Syntaxe dans l'éditeur de script de System i Navigator

```
CREATE TABLE dgayte.fieldproc(
z1 INT,
z2 CHAR(16));
```

```
ALTER TABLE dgayte.fieldproc
ALTER COLUMN Z2   SET FIELDPROC dgayte.field_proc;
```

```
INSERT INTO dgayte.fieldproc VALUES(1, '123456789012345');
INSERT INTO dgayte.fieldproc VALUES(1, '3210654987123122');

SELECT * FROM dgayte.fieldproc;
```

Selon l'utilisateur

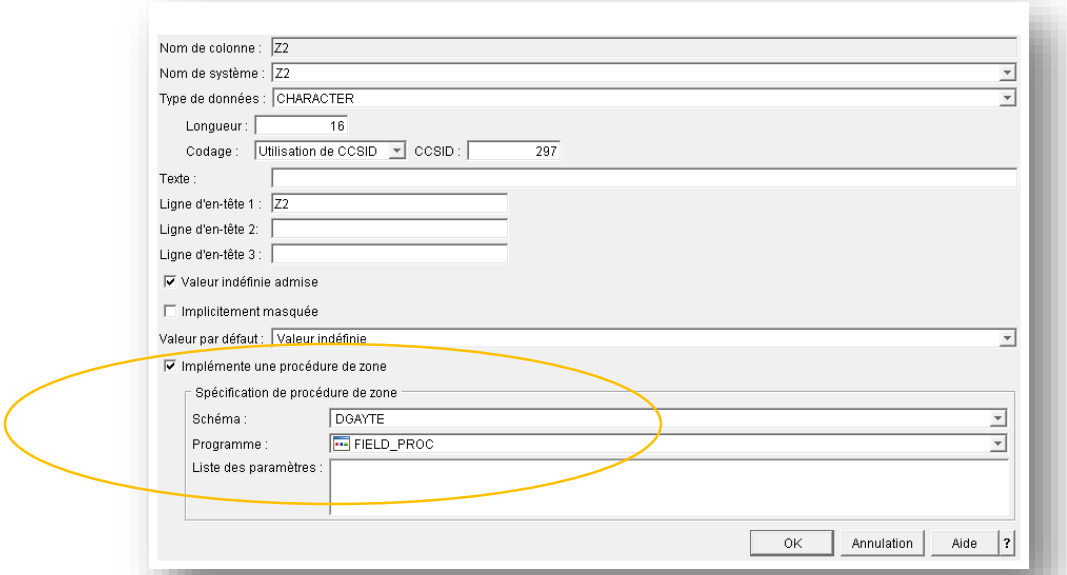
Z1	Z2
1	****56789012345
2	****654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

Z1	Z2
1	123456789012345
2	3210654987123122

Visualisation

- System i Navigator

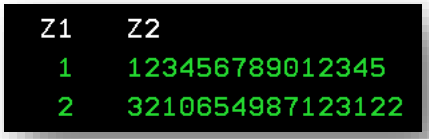
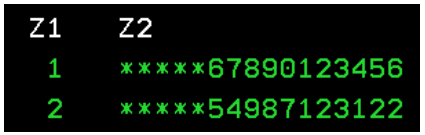
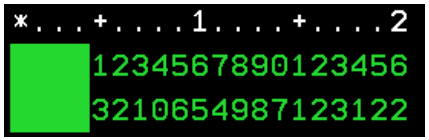
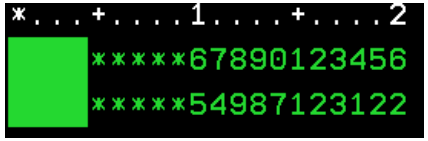


- DSPFFD

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

Utilisation

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

	QSECOFR		Autre
Navigator	Z1 | Z2 1 | 123456789012345 2 | 3210654987123122		Z1 | Z2 1 | *****56789012345 2 | *****654987123122
STRSQL			
DSPPFM			
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%'
```

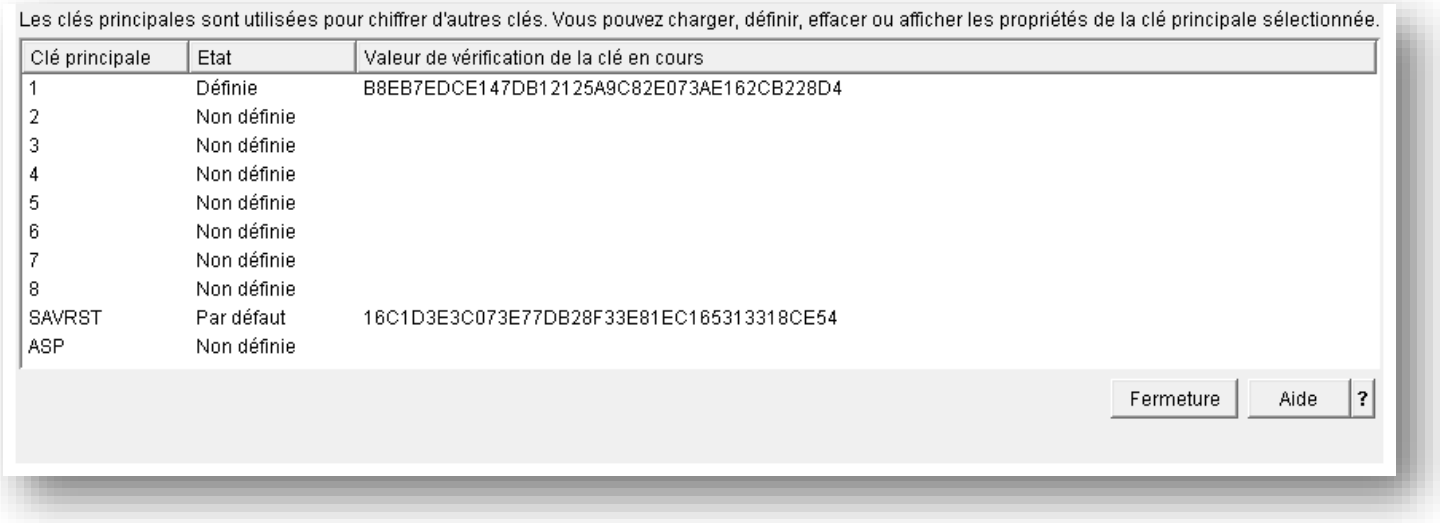
- Dans notre exemple, problème si le profil ne voit pas les premiers caractères (***)
- Les profils non autorisés ne voient que des '*' pas '123'

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)



- 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 pourvoir 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 un copie (la sauvegarde d'origine reste en clair)

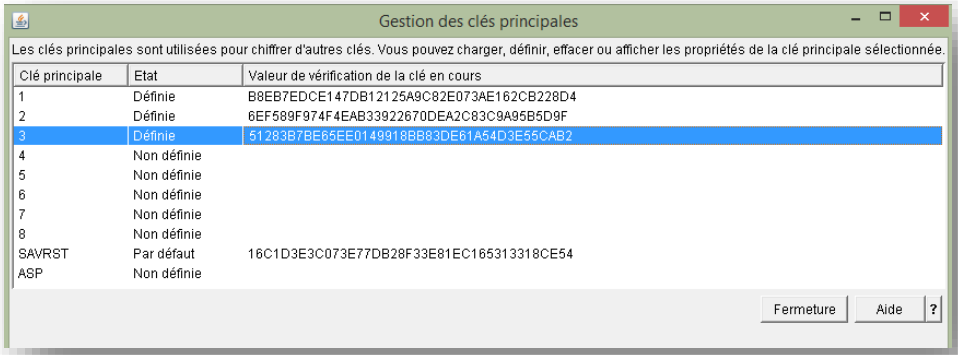
Cryptage et BRMS

- 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

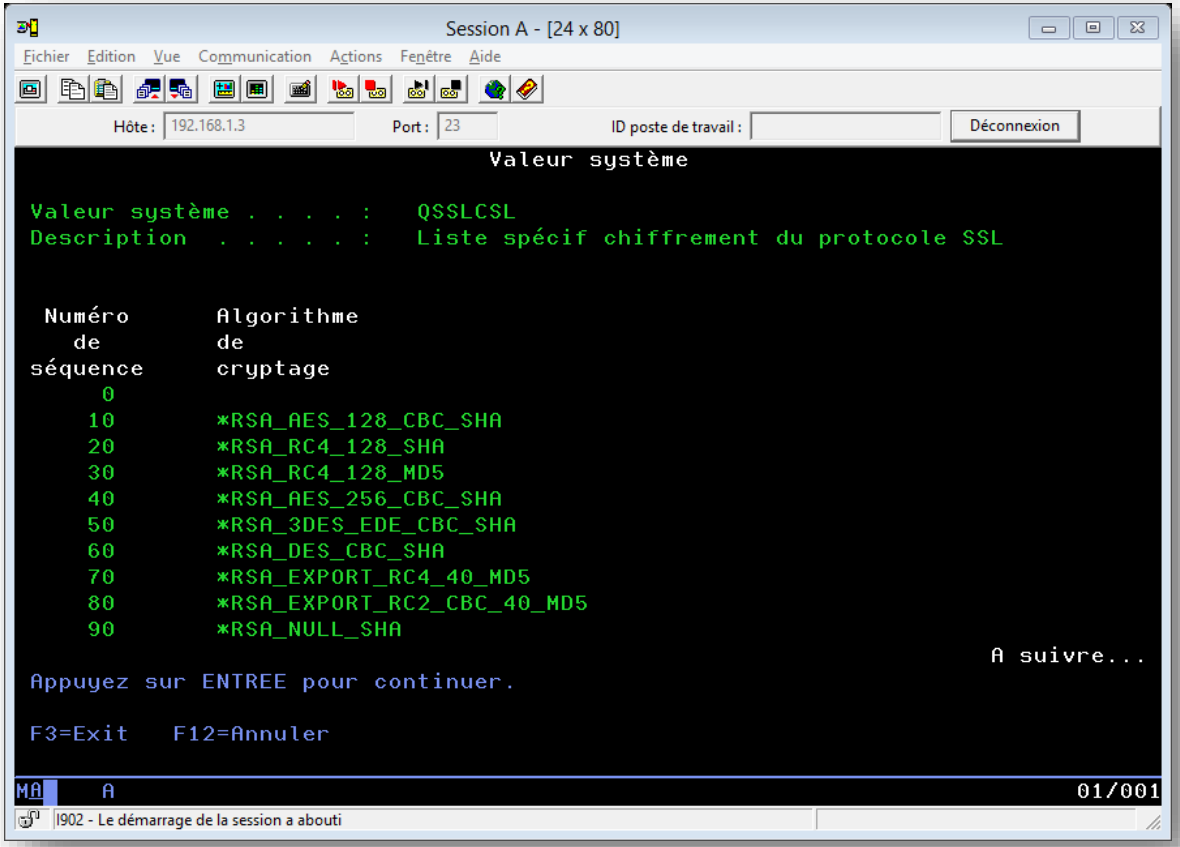
Platforms Impacted (780):
IBM Power 795 (9117-FHB)
IBM Power 780 (9179-MHB)
IBM Power 770 (9117-MMB)

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)

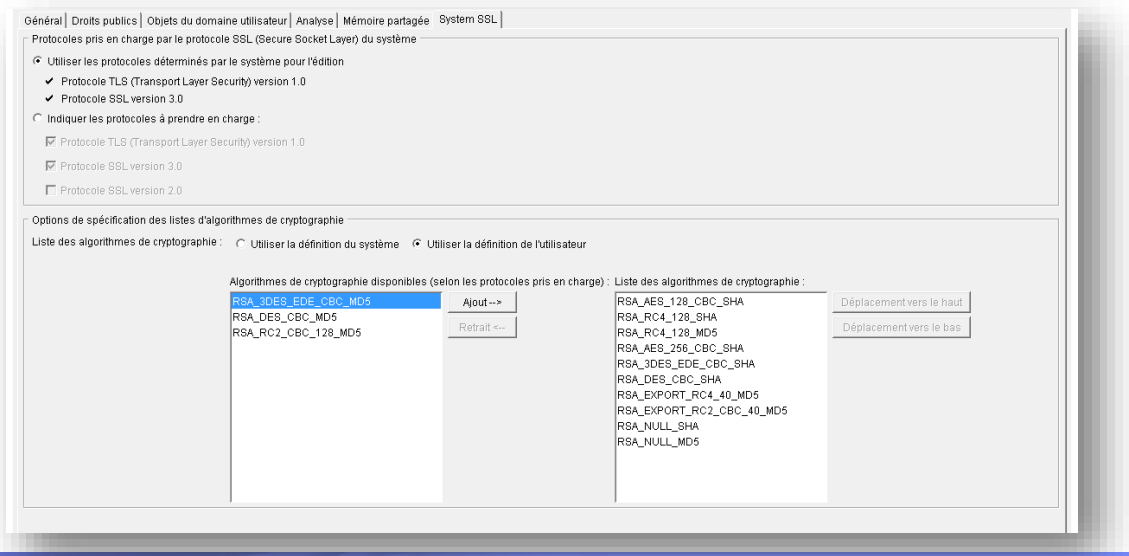
SSL : valeurs système QSSLCSL

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



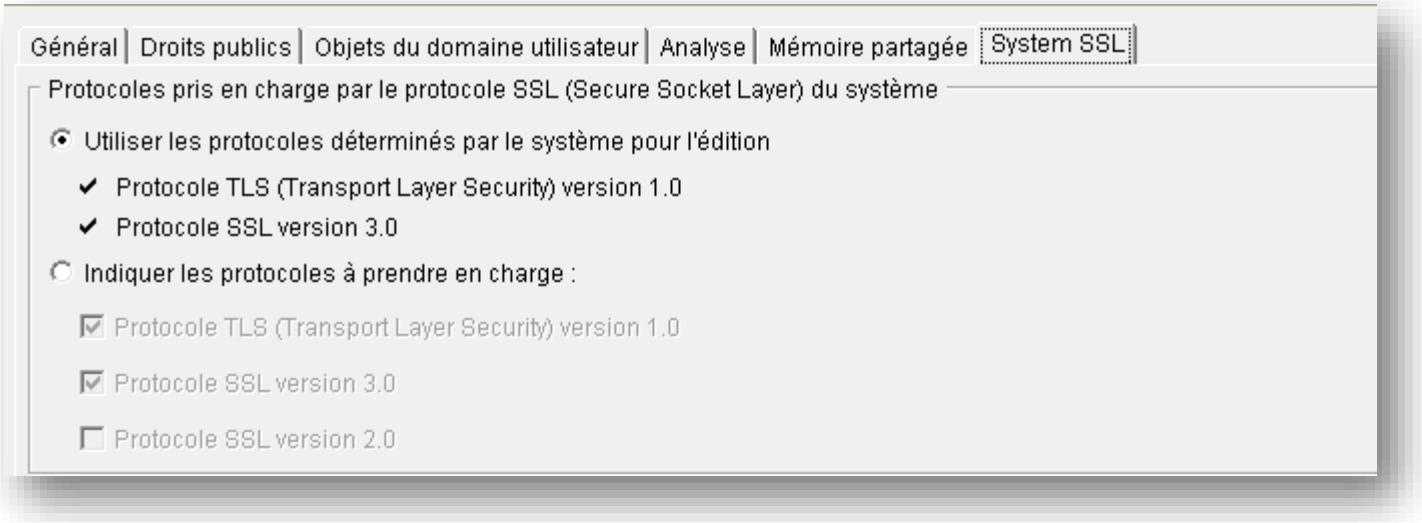
SSL : valeurs système QSSLCSLCTL

- **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

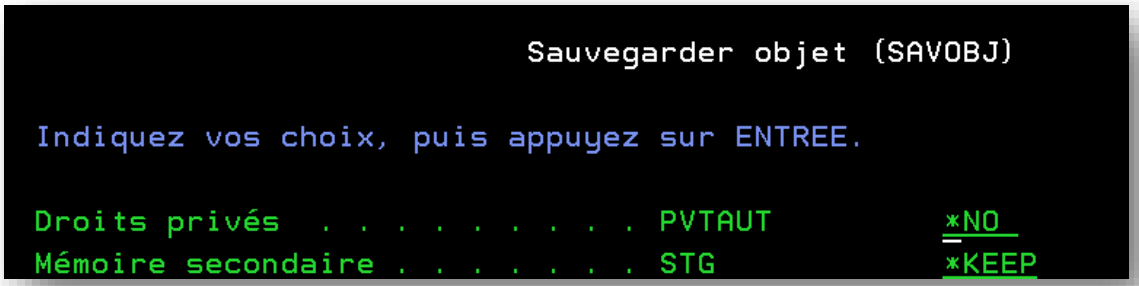
```
Principal: nfs/mante.notos.beaulieu@NOTOS.BEAULIEU
  Key version: 1
  Key type: 128-bit AES
  Entry timestamp: 2014/04/29-15:12:10

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



S8 - Sécurité IBM i : nouveautés 6.1 et 7.1

Merci de votre attention

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