Tour d'horizon de la Sécurité i5/OS et IBM i

Journées Clubs

Pause Café
Septembre 2012

Sécurité i5/OS et IBM i

La sécurité du système doit remplir 3 objectifs

La Confidentialité

- Protéger contre la divulgation de renseignements à des personnes non autorisées
- Limiter l'accès aux renseignements confidentiels
- Protéger contre les utilisateurs curieux, internes et externes à l'entreprise

L'Intégrité

- Protéger contre les modifications de données non autorisées
- Réduire les manipulations de données aux seuls programmes autorisés
- Assurer que les données soient toujours fiables

La Disponibilité

- Empêcher les modifications accidentelles ou la destruction de données
- Protéger contre les tentatives de modification ou de destruction des ressources système

Sécurité i5/OS et IBM i

Les fonctionnalités mises à disposition par l'OS

- Le niveau de sécurité du système
- Les valeurs système
- La signature des objets
- L'authentification par Single Sign-On
- Les Profils Utilisateurs
- Les Profils de Groupe
- La gestion des droits d'accès aux objets
- Le journal d'Audit de la sécurité
- La journalisation des données et le Commitment Control
- Les points d'Exit
- Les iASp (independent Auxiliary Storage Pool)

Niveaux de sécurité

L'OS de la plateforme offre 4 niveaux de sécurité, indiquée dans la valeur système QSECURITY, du niveau 20 au niveau 50 (le niveau 10 n'est plus utilisable). Ci-dessous les principales différences :

Fonction	niv 20	niv 30	niv 40	niv 50
Sécurité du Menu et du Programme Initial, si LMTCPB(*YES) indiqué dans le profil	oui	oui	oui	oui
Activation des droits d'accès aux objets	**non**	oui	oui	oui
Accès à tous les objets	**oui**	non	non	non
Blocage de l'exécution des programmes utilisant des interfaces non supportées (autres que des commandes système ou des API)	**non**	**non**	oui	oui
Protection évoluée de la mémoire (un bloc est défini R/W, R only, ou NO access)	**non**	**non**	oui	oui
Validation des paramètres passés entre des programmes exécutés à l'état système et ceux à l'état user du domaine utilisateur	**non**	**non**	oui	oui
Règles restrictives d'échange de messages appliquées entre les programmes à l'état utilisateur et les programmes à l'état système	**non**	**non**	**non**	oui
Espace associé à un programme non modifiable directement	**non**	**non**	oui	oui
Protection des blocs de contrôle internes	**non**	**non**	oui	oui

Niveaux de sécurité

Quelques remarques sur les niveaux de sécurité

Si, en faisant **évoluer un niveau** 30 ou 40, vers 40 ou 50, on rencontre des problèmes d'intégrité, il est possible de **redescendre au niveau précédent** sans impact sur la gestion de la sécurité.

Par contre, redescendre au niveau 20, modifie les profils utilisateurs en leur accordant des droits spéciaux supplémentaires, notamment *ALLOBJ.

Un objet appartient au **domaine** *SYSTEM ou au domaine *USER. (vérifiable par DSPOBJD)

Un programme est défini à l'**état** *SYSTEM, *INHERIT ou *USER. (vérifiable par DSPPGM)

Les objets du domaine *SYSTEM ne peuvent être accédés que par des programmes à l'état *SYSTEM, ou à l'état *INHERIT s'ils sont appelés par des programmes à l'état *SYSTEM.

La **protection étendue des blocs mémoires** s'applique aux programmes exécutés à l'état *USER.

Au niveau 40 elle protège des blocs comme le Work Control Block. Au niveau 50 aucun bloc de contrôle interne ne peut être modifié, ceci inclut par exemple l'ODP (Open Data Path)

A partir du niveau 40, l'espace associé à un objet programme ne peut pas être modifié par un programme à l'état *USER.

Au niveau 50 un programme à l'état *USER ne peut pas obtenir les adresses d'un autre job, donc ne peut pas manipuler les objets associés à un autre job.

Niveaux de sécurité

Recherche des informations de violation de la sécurité

On le verra plus loin, mais pour retrouver les informations tracées dans l'Audit Journal, relatives à des violations de type *AUTFAIL (Authority Failure), on recherchera les postes suivants :

- Code = **T** pour Audit Trail Entry (poste de Trace)
- Type = **AF** pour Authority Failure

Dans le détail du poste de journal, il sera indiqué en première position, le type de tentative de violation concernée :

- **C** = Object validation failure
  (en fonction de la valeur système QFRCCVNRST, pendant une restauration d'objet)
- **D** = Unsupported interface (domain) violation
- **J** = Job-description and user-profile authorization failure
  *(job soumis avec une JOBD contenant un profil sur lequel on n'a pas de droit *USE)*
- **R** = Attempt to access protected area of disk (enhanced hardware storage protection)
- **S** = Default sign-on attempt

Valeurs système liées à la sécurité

1 - Sécurisation des valeurs système

Les valeurs système de sécurité, indiquées dans le tableau ci-dessous, peuvent être verrouillées, depuis la V5, avec SST ou DST.
Utiliser STRSST option 7 (Work with System Security) et mettre 2 (Lock) dans « Allow system value security changes »

QALWJOBITP	QAUTORMT	QLMTDEVSSN	QPWDLMTREP	QRETSVRSEC
QALWOBJRST	QAUTOVRT	QLMTSECOFR	QPWDLVL	QRMTSIGN
QALWUSRDMN	QCRTAUT	QMAXSGNACN	QPWDMAXLEN	QRMTSRVATR
QAUDCTL	QCRTOBJAUD	QMAXSIGN	QPWDMINLEN	QSCANFS
QAUDENDACN	QDEVRCYACN	QPWDCHGBLK	QPWDPOSDIF	QSCANFSCTL
QAUDFRCLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QSECURITY
QAUDLVL	QDSCJOBITV	QPWDEXPWRN	QPWDRQDDIF	QSHRMEMCTL
QAUDLVL2	QFRCCVNRST	QPWDLMTAJC	QPWDRULES	QUSEADPAUT
QAUTOCFG	QINACTMSGQ	QPWDLMTCHR	QPWDVLDPGM	QVFYOBJRST

Ceci empêche un utilisateur avec des droits *SECADM ou *ALLOBJ de modifier le contenu de ces valeurs système.

Note : attention à déverrouiller ces valeurs avec DST, en cas de restauration du système, pour l'IPL qui suivra

Valeurs système liées à la sécurité

Les Valeurs Système qui contrôlent directement la sécurité

QALWUSRDMN	Allow user domain objects in the libraries
QCRTAUT	Create default public authority
QDSPSGNINF	Display sign-on information
QFRCCVNRST	Force conversion on restore
QINACTITV	Inactive job time-out interval
QINACTMSGQ	Inactive job message queue
QLMTDEVSSN	Limit device sessions
QLMTSECOFR	Limit security officer
QMAXSIGN	Maximum sign-on attempts
QMAXSGNACN	Action when maximum sign-on attempts exceeded
QRETSVRSEC	Retain Server Security
QRMTSIGN	Remote sign-on requests
QSCANFS	Scan file systems
QSCANFSCTL	Scan file systems control
QSECURITY	Security level
QSHRMEMCTL	Shared memory control
QUSEADPAUT	Use Adopted Authority
QVFYOBJRST	Verify object on restore

Valeurs système liées à la sécurité

2 - Gestion de la restauration des objets sur le système

Trois valeurs système fonctionnent ensemble comme des filtres pour autoriser ou non la restauration. Elles sont examinées dans cet ordre :

QVFYOBJRST valeurs 1 (ne pas vérifier les signatures)
à 5 (restaurer uniquement les objets avec une signature valide)

Si Digital Certificat Manager n'est pas installé, tous les objets sont considérés non signés, et donc restaurés si cette valeur contient 1, 2 ou 3 (la valeur par défaut est 3, restauration des objets non signés, ou avec une signature valide)

QFRCCVNRST valeurs 0 (ne pas convertir)
à 7 (convertir tous les objets)

Le paramètre FRCOBJCVN des commandes RST utilise cette valeur si *SYSVAL est précisé.*
*S'applique aux types d'objets *MODULE, *PGM, *SRVPGM et *SQLPKG.*
*Quand un objet est converti sa signature numérique est supprimée et son état devient *USER.*

QALWOBJRST valeurs *ALL, *NONE (ne pas restaurer si attributs de sécurité)
ou une liste de valeurs parmi *ALWSYSSTT, *ALWPGMADP, *ALWPTF, *ALWSETUID, *ALWSETGID, *ALWVLDERR

*Par sécurité, cette valeur devrait rester à *NONE, et modifiée uniquement en cas de besoin.*
*Elle doit être à *ALL pour recharger le système, une release ou un produit sous licence.*

Valeurs système liées à la sécurité

3 - Gestion de l'Audit de Sécurité du système

L'Audit de sécurité est la seule trace parfaitement infalsifiable des actions effectuées sur le système. Elle est gérée par : un journal, QAUDJRN placé dans QSYS, des récepteurs associés à ce journal, et 3 valeurs système :

QAUDCTL valeurs : *AUDLVL, les actions à tracer sont listées dans les 2 autres valeurs
*OBJAUD, les modifications sur les Objets, ayant une valeur d'Audit autre que *NONE sont tracées dans le journal
*NOQTEMP pas de traces sur les actions effectuées dans QTEMP

Note : ne pas tracer ce qui se passe dans QTEMP peut masquer certaines actions frauduleuses

QAUDLVL et **QAUDLVL2** peuvent se répartir les valeurs suivantes :
*ATNEVT *AUTFAIL *CREATE *DELETE *JOBBAS *JOBCHGUSR *JOBDTA *NETBAS *NETCLU *NETCMN *NETFAIL *NETSCK *OBJMGT *OFCSRV *OPTICAL *PGMADP *PGMFAIL *PRTDTA *SAVRST *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECURITY *SECVFY *SECVLDL *SERVICE *SPLFDTA *SYSMGT
(pour prendre en considération le contenu de QAUDLVL2, indiquer *AUDLVL2 dans QAUDLVL)

Note : certaines valeurs en regroupent d'autres :
**SECURITY regroupe toutes les *SECxx, *JOBDTA regroupe les *JOBxx, ou *NETCMN qui regroupe les *NETxx*

Valeurs système liées à la sécurité

Les actions sur tous les objets, indistinctement, sont définies dans QAUDLVL et QAUDLVL2, comme *CREATE ou *DELETE. Mais la valeur *OBJMGT ne concerne que les actions MOVE ou RENAME appliquées aux objets.

La trace de modifications spécifiques d'un objet, comme le nombre d'incréments d'un fichier, l'ajout ou le retrait d'une contrainte, etc… , est fonction de la valeur d'un attribut de l'objet lui-même (*Object auditing value)* visible avec WRKOBJ).

Cet attribut sera rempli à la création, en tenant compte de la valeur du paramètre CRTOBJAUD de la librairie (ou du répertoire) de l'objet.

Si CRTOBJAUD contient *SYSVAL , la valeur système QCRTOBJAUD est utilisée.

QCRTOBJAUD contient la valeur d'Audit par défaut des objets créés dans une librairie ou un répertoire.

Les valeurs
- *NONE ne tracera pas dans l'Audit journal les modifications sur les objets
- *CHANGE tracera les modifications d'objets
- *ALL tracera en plus tous les accès aux objets
- *USRPRF tracera les modifications sur les objets si elles sont effectuées par un profil audité, avec la commande CHGUSRAUD

Valeurs système liées à la sécurité

4 - Gestion des mots de passe

QPWDCHGBLK (V6R1) Empêche les modifications pendant un certain nombre d'heures (1 à 99)

QPWDEXPITV Durée de validation en jours (1 à 366)

QPWDEXPWRN (V6R1) Délai en jours du warning envoyé avant la péremption (1 à 99)

QPWDLMTAJC (*) Indique si les chiffres adjacents sont autorisés

QPWDLMTCHR (*) Indique les caractères interdits (10 max.), par ex. les voyelles

QPWDLMTREP (*) Indique si un caractère peut être répété, de façon consécutive ou non

QPWDLVL Niveau des mots de passe, de 10 ou 128 caractères

QPWDMAXLEN (*) Longueur maximum autorisée du mot de passe (1 à 128)

QPWDMINLEN (*) Longueur minimum autorisée du mot de passe (1 à 128)

QPWDPOSDIF (*) Indique si un caractère peut être repris, à la même place, du pwd précédent

QPWDRQDDGT (*) Indique si au moins un chiffre est obligatoire

QPWDRQDDIF Limite la reprise des mots de passe précédents (jusqu'à 32 différents)

QPWDRULES (V6R1) Règles de contrôle, soit *PWDSYSVAL (les 7 valeurs avec *(*)* ci-dessus), soit 23 autres valeurs, ex. *LMTPRFNAME qui interdit le nom du profil dans le pwd

QPWDVLDPGM Programme(s) utilisateur effectuant des contrôles supplémentaires
Attention : les mots de passe lui sont transmis non cryptés

La Signature des Objets

L'intégrité peut être renforcée depuis la V5 par la signature numérique des objets.

Les signatures numériques peuvent être prises en compte par la valeur système **QVFYOBJRST**, la commande **CHKOBJITG** (Check Object Integrity) et l'outil Digital Certificate Manager (DCM).
La documentation de DCM se trouve à l'URL:
http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/topic/rzahu/rzahu.pdf

Vous pouvez aussi signer vos propres programmes (tous les programmes sous licence fournis avec le système sont signés).

L'API Add Verifier permet d'ajouter des signatures numériques.
Il est possible d'empêcher ces ajouts, ainsi que la remise à zéro de mots de passe sur les certificats stockés.
SST offre avec l'option de menu « 7. Work with system security », un paramètre pour gérer l'ajout de certificats numériques.

Work with System Security

…
Allow new digital certificates . . . . . 1 1=Yes, 2=No
…

L'authentification par Single Sign-On

Single Sign-on est un processus d'authentification, par lequel un utilisateur peut accéder à plus d'un système en entrant un ID utilisateur unique et un mot de passe.
Dans les réseaux hétérogènes d'aujourd'hui, les administrateurs doivent faire face à la complexité de la gestion d'identification et d'authentification pour les utilisateurs du réseau.

Pour activer un environnement de Single Sign-On, IBM fournit deux technologies qui travaillent ensemble pour permettre aux utilisateurs de se connecter avec leur nom d'utilisateur et le mot de passe Windows et d'être authentifié sur le système i dans le réseau.

Network Authentication Service (NAS) et **Enterprise Identity Mapping** (EIM) sont les deux technologies à configurer pour définir un environnement de Single Sign-On.

Z/OS, AIX , Windows 2000 et Windows XP utilisent le protocole Kerberos pour authentifier les utilisateurs sur le réseau.
Un système sécurisé et centralisé, appelé centre de distribution des clés, authentifie les utilisateurs de Kerberos dans le réseau.

Les Profils Utilisateurs

Petits rappels de base

L'accès au serveur nécessite l'utilisation d'un outil spécifique, le Profil Utilisateur, ayant plusieurs rôles dans le système:

- Il contient des informations de sécurité qui contrôlent la façon dont l'utilisateur s'identifie sur le système, ce qu'il est autorisés à le faire après son identification, et comment ses actions sont auditées.
- Il contient des informations permettant de personnaliser le système pour l'adapter à l'utilisateur.
- Il est un outil de gestion et de récupération pour le système d'exploitation. Le Profil de l'utilisateur contient des informations sur les objets possédés par l'utilisateur et tous les droits privés sur des objets.
- Le nom du Profil Utilisateur identifie les jobs de l'utilisateur et ses spools.

Le niveau minimum de sécurité du système utilisable étant maintenant 20, un Profil Utilisateur doit donc exister pour qu'un utilisateur puisse d'identifier et accéder au système .

Les Profils Utilisateurs

Les droits spéciaux

Les profils utilisateurs peuvent acquérir certains droits, par leur classe ou par attribution individuelle, à la création ou par modification.

Parmi les plus puissants, les droits spéciaux *ALLOBJ et *SPLCTL permettent d'accéder à l'ensemble des objets et des spools du système sans restrictions, le droit *SECADM permet de gérer tous les profils utilisateurs.

Ces profils peuvent être retrouvés et listés facilement avec la commande **PRTUSRPRF**.

Exemple d'utilisation, liste des profils dont les droits spéciaux sont différents de leur classe :

```
                    Print User Profile (PRTUSRPRF)
Type of information . . . . >   *AUTINFO      *ALL, *AUTINFO, *ENVINFO, *PWDINFO, *PWDLVL
Select by . . . . . . . . . . >  *MISMATCH    *SPCAUT, *USRCLS, *MISMATCH
```

Ou bien recherche de certains droits spéciaux, et édition de toutes les informations de sécurité :

```
Type of information . . . . >   *ALL          *ALL, *AUTINFO, *ENVINFO, *PWDINFO, *PWDLVL
Select by . . . . . . . . . . >  *SPCAUT      *SPCAUT, *USRCLS, *MISMATCH
Special authorities . . . . . >  *ALLOBJ      *ALL, *ALLOBJ, *AUDIT, *JOBCTL, *IOSYSCFG,...
                                 *SPLCTL
          + for more values >    *SECADM
```

Les Profils Utilisateurs

Les droits spéciaux

Exemple de liste de type *MISMATCH :

User Profile Information

5770SS1 V7R1M0 100423

Report type . . . . . : *AUTINFO

Select by . . . . . : *MISMATCH

		Special Authorities								
User Profile	Group Profiles	*ALL OBJ	*AUD IT	SYS CFG	*JOB CTL	*SAV SYS	*SEC ADM	*SER VICE	*SPL CTL	User Class
DEMO	*NONE	X							X	*USER
HENRY	*NONE	X					X			*SECOFR
DENIS	*NONE	X	X	X	X		X			*USER
DENIS2	*NONE	X	X	X	X	X			X	*USER
FRANCK	*NONE	X	X		X				X	*USER
JUSTIN	*NONE	X	X	X	X		X			*USER
LOUIS	*NONE	X	X	X	X		X			*USER
MICHEL	*NONE	X								*USER

Les Profils Utilisateurs

Audit des profils avec droits spéciaux

Les actions effectuées avec ces profils peuvent être tracées, dans le journal d'Audit du système.

Pour cela, 2 façons de procéder, combinées ou non :

- Les objets « sensibles » indiquent que les profils seront audités pour leur action sur cet objet, en positionnant la valeur d'Audit de l'objet à *USRPRF.
  Et dans les profils concernés, on précise quelle niveau sera tracé.
- Un ensemble d'actions, effectuées par ce profil, est audité en plus de l'Audit général paramétré

La commande **CHGUSRAUD** est utilisée dans ces cas :

Change User Auditing (CHGUSRAUD)

User profile . . . . . >	SECURITE	Name
+ for more values		
Object auditing value . . . . . >	*CHANGE	*SAME, *NONE, *CHANGE, *ALL
User action auditing . . . . . >	*PGMADP	*SAME, *NONE, *AUTFAIL...
	*PGMFAIL	
	*DELETE	
	*SECURITY	
+ for more values	*SYSMGT	

Les Profils Utilisateurs

Nouveautés V7.1 *concernant le Profil utilisateur*

2 nouveaux paramètres contrôlent la durée individuelle d'utilisation d'un profil.
Ils sont utilisables à la création ou à la modification du profil.

A la fin de la durée indiquée le profil sera mis à l'état *DISABLED.

1°) USREXPDATE User Expiration Date
contient, soit une date d'expiration, soit la valeur *USREXPITV

2°) USREXPITV User expiration Interval
contient un nombre de jours entre 1 et 366

Create User Profile (CRTUSRPRF)

```
.....
User expiration date . . . . . USREXPDATE    *NONE      Date, *NONE, *USREXPITV
User expiration interval . . . . USREXPITV     ____      1-366
.....
```

Si un Profil Utilisateur est restauré et qu'il existe déjà sur le système, ces valeurs sont conservées.

S'il n'existe pas sur le système, ces valeurs sont restaurées, et si la date d'expiration est dépassée le profil est mis à l'état *DISABLED.

Les Profils Utilisateurs

Depuis la V5, il existait déjà 2 options du menu SECTOOLS (outils de gestion de la sécurité) qui géraient globalement l'utilisation de ces fonctions associés aux profils :

SECTOOLS Security Tools System: CILAG71

Work with profiles

1. Analyze default passwords

2. Display active profile list
3. Change active profile list
4. Analyze profile activity

5. Display activation schedule
6. Change activation schedule entry

7. Display expiration schedule ← cde DSPEXPSCD. Affiche la liste des profils concernés
8. Change expiration schedule entry ← cde CHGEXPSCDE. Soumet la désactivation ou la suppression de profils

9. Print profile internals

More...

Les Profils Utilisateurs

Option 7 :

User Profile Expiration Schedule

User Profile	Expiration Date	Action	Owned Object Option	New Owner
TEST	30/11/12	*DISABLE		

Option 8 :

Change Expiration Scd Entry (CHGEXPSCDE)

User profile . . . . . >	TEST	Name	
+ for more values	_____		
Expiration date . . . . . >	'31/12/12'	Date, *NONE	
Action . . . . . >	*DELETE	*DISABLE, *DELETE	
Owned object option:			
Owned object value	*NODLT	*NODLT, *DLT, *CHGOWN	← *si le profil possède des objets*
*User profile name if *CHGOWN*	_____	*Name*	**NODLT bloque la suppression*
Primary group option:			
Primary group value	*NOCHG	*NOCHG, *CHGPGP	
New primary group	_____	Name, *NONE	
New primary group authority .	_____	*OLDPGP, *PRIVATE, *ALL...	

Le job QSECEXP1 sera planifié à 00h01 pour effectuer ces tâches.

Sécurité i5/OS et IBM i - Les Profils de Groupe

Un profil de groupe est un type spécial de profil utilisateur qui fournit les mêmes droits à un groupe d'utilisateurs.
Un profil utilisateur devient profil de Groupe lorsque qu'un profil utilisateur s'y rattache.
Le système le reconnaît alors comme profil de Groupe et lui affecte un GID (Group Identification).
On peut aussi transformer un profil en profil de Groupe en lui affectant manuellement un GID.

C'est un outil de sécurité.
Un profil de Groupe fournit une méthode pour organiser les droits sur le système et les partager entre des utilisateurs.

On peut définir des droits sur les objets, ou des autorisations spéciales, pour des profils de Groupe plutôt que pour chaque profil utilisateur individuel. Un utilisateur peut être rattaché à plusieurs profils de Groupe (jusqu'à 16).
Attention, les droits spéciaux utilisables par un profil individuel sont cumulés, les siens propres plus ceux de chacun des profils de Groupe auquel il est rattaché.

Remarque :
Les objets peuvent avoir un Primary Group Profile (PGP), et cette information est stockée avec l'objet lui-même, pour améliorer les performances de contrôle des droits d'accès.
Les performances seront optimales, si le PGP de l'objet est le 1er profil de Groupe du profil utilisateur accédant à l'objet.

Sécurité i5/OS et IBM i - Les Profils de Groupe

Il est préférable de ne pas affecter de mot de passe aux profils de Groupe, afin de toujours pouvoir rechercher les actions effectuées par les profils individuels, dans l'historique de leurs jobs ou dans l'Audit journal du système.

La commande **DSPAUTUSR** permet de lister les informations sur les profils, en les triant éventuellement par Groupe, ce qui fournit une information intéressante :

Display Authorized Users (DSPAUTUSR)

Sequence . . . . . >	*GRPPRF	*USRPRF, *GRPPRF
Output	*	*, *PRINT

Display Authorized Users

Group Profile	User Profile	Password Last Changed	No Password	Text
GRP1		27/07/11	X	Groupe de test 1
	GMENU	04/09/12		Guy Menu
	HENRY	27/01/12		
GRP2		27/07/11	X	Groupe de test 2
	LUDO	08/11/10		
*NO GROUP				
	DENIS	12/03/12		Demo
	FRANCK	20/08/10	X	

La gestion des droits d'accès aux objets

Description des types de droits sur les Objets

*OBJOPR	Accès à la description, et au contenu en fonction des droits sur les données
*OBJMGT	Gère la sécurité, les move et rename et les fonctions de *OBJALTER et *OBJREF
*OBJEXIST	Suppression, libération de l'espace, save/restore, transfert de propriété
*OBJALTER	Add, clear, initialisation et réorganisation des membres. Modification des attributs
*OBJREF	Référence un fichier parent dans une contrainte d'intégrité référentielle
*AUTLMGT	Ajout et retrait de profils dans les listes d'autorisations

Description des types de droits sur les Données

*READ	Affiche le contenu d'un objet possédant des données
*ADD	Ajoute des entrées dans un objet, comme une MSGQ ou un Fichier
*UPD	Modifie les données d'un objet
*DLT	Retire des entrées dans un objet, comme une MSGQ ou un Fichier
*EXECUTE	Exécute un programme ou un SQL package. Localise un objet en librairie ou de l'IFS

Description des types de droits sur les Champs

*MGT	Gère la sécurité du champ
*ALTER	Modifie les attributs du champ
*REF	Référence le champ comme clé parente dans une contrainte d'intégrité référentielle
*READ	Accède au contenu du champ en lecture
*ADD	Ajoute des données dans le champ
*UPDATE	Modifie le contenu du champ

La gestion des droits d'accès aux objets

Combinaisons de droits fournies par le système

Authority	*ALL	*CHANGE	*USE	*EXCLUDE
Object Authorities				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Data Authorities				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

Tout autre combinaison de droits sera indiqué USER DEF

La gestion des droits d'accès aux objets

Quand un utilisateur veut utiliser un objet, le système vérifie que cet utilisateur possède les droits suffisants.

Le système contrôle d'abord les droits sur la librairie, ou le répertoire, qui contient l'objet.
Si ceux-ci sont suffisants, le système contrôle les droits sur l'objet lui-même.

Les droits d'accès d'un utilisateur à un objet sont vérifiés dans l'ordre suivant:

1. Droits sur l'objet - chemin rapide (droits Public utilisables, si pas d'autres éléments à valider)
2. Droit spécial *ALLOBJ du Profil utilisateur
3. Droits spécifiques du Profil utilisateur sur l'objet
4. Droits du Profil utilisateur sur la liste d'autorisation sécurisant l'objet
5. Droit spécial *ALLOBJ des Profils de Groupe de l'utilisateur
6. Droits spécifiques des Profils de Groupe de l'utilisateur sur l'objet
7. Droits des Profils de Groupe sur la liste d'autorisation sécurisant l'objet
8. Droits Public indiqué sur l'objet ou dans la liste d'autorisation sécurisant l'objet

La gestion des droits d'accès aux objets

Affectation des droits Publics

1°) Toutes les commandes de création d'Objets CRTxxx indique cette information dans le paramètre **AUT**.
Par défaut, AUT contient la valeur ***LIBCRTAUT**, qui fait référence à la Libraire de définition de l'Objet.

↳ 2°) Les commandes CRTLIB et CHGLIB indiquent l'information dans le paramètre **CRTAUT.**
Par défaut, CRTAUT contient la valeur ***SYSVAL**, qui fait référence à la valeur système QCRTAUT.

↳ 3°) La valeur système **QCRTAUT** contient par défaut la valeur ***CHANGE**

La gestion des droits d'accès aux objets

Généralités sur les Listes d'Autorisations

Une Liste d'Autorisations (type d'objet *AUTL) contient une liste d'utilisateurs, et les droits qu'ont les utilisateurs sur les objets que la Liste sécurise.
Chaque utilisateur peut avoir des droits différents sur les objets.
En donnant un droit à un utilisateur sur la Liste d'Autorisations, le système accorde un droit privé à cet utilisateur sur la Liste d'Autorisations.

On peut également utiliser une Liste d'Autorisations pour définir les droits Public sur les objets de la Liste. Si le droit Public d'un objet est défini sur *AUTL, l'objet récupère ses droits Public dans la Liste d'Autorisations.

L'objet Liste d'Autorisations est utilisé comme un outil de gestion par le système. Il contient une liste de tous les objets qui sont sécurisés par la Liste d'Autorisations. Cette information est utilisée pour afficher ou modifier les objets de la Liste d'Autorisations.

On ne peut pas utiliser une Liste d'Autorisations pour sécuriser un profil utilisateur ou une autre Liste d'Autorisations. Une seule Liste d'Autorisations peut être utilisée pour un objet.

Le nom de la Liste d'Autorisations qui sécurise un Objet est stocké avec l'Objet.

La gestion des droits d'accès aux objets

Comparaison entre Liste d'Autorisations et Profil de Groupe

	Authorization list	**Group profile**
Utilisé pour sécuriser plusieurs objets	Oui	Oui
L'utilisateur peut être rattaché à plus d'un élément	Oui	Oui
Un droit privé remplace tout autre droit	Oui	Oui
On doit préciser les droits utilisateur individuellement	Oui	Non
Les droits indiqués sont les mêmes pour tous les objets	Oui	Non
Un objet peut être sécurisé par plus d'un(e)	Non	Oui
Le droit peut être indiqué à la création de l'objet	Oui	Oui (1)
Peut sécuriser tous les types d'objet	Non	Oui
Association supprimée quand l'objet est supprimé	Oui	Oui
Association sauvegardée quand l'objet est sauvegardé	Oui	Oui (2)

1 - Le profil de groupe peut affecter un droit lorsqu'un objet est créé en utilisant le paramètre GRPAUT dans le profil de l'utilisateur qui crée l'objet.
2 - Les droits du PGP sont enregistrés avec l'objet. Les droits privés du groupe sont enregistrées si PVTAUT(*YES) est indiqué avec la commande de sauvegarde.

La gestion des droits d'accès aux objets

Les droits adoptés

Un programme peut adopter, à l'exécution, les droits de l'utilisateur propriétaire de l'objet en plus des droits de l'utilisateur du job.

Les types d'objets *PGM, *SRVPGM, *SQLPKG et programmes Java peuvent adopter des droits.

Note :
Les droits des profils de Groupe du propriétaire de l'objet ne sont pas hérités.

Les commandes de création ou de modification de ces objets peuvent remplacer la valeur *USER par ***OWNER** dans le paramètre **USRPRF** pour activer cette fonctionnalité.

C'est évidemment un trou majeur de sécurité. Il est important de repérer ces objets pour s'assurer du besoin réel.

La commande **PRTADPOBJ** permet de lister ces programmes. Exemple avec QSECOFR :

Print Adopting Objects (PRTADPOBJ)

User profile	USRPRF	QSECOFR	Name, generic*, *ALL
Changed report only	CHGRPTONLY	*NO	*NO, *YES

Le rapport avec CHGRPTONLY à *NO est un rapport complet, avec *YES seuls les nouveaux programmes avec droits adoptés sont listés.

La gestion des droits d'accès aux objets

Exemple de liste initiale avec CHGRPTONLY à *NO

Adopting Objects by User Profile (Full Report)

User profile . . . . . : QSECOFR
Special authorities . . . . . : *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL
*SAVSYS *SECADM *SERVICE *SPLCTL

----------Object----------			----------Library----------			
Name	Type	Public Authority	Name	ASP Device	Public Authority	Private Authorities
QSQIMAIN	*PGM	*USE	QSQL	*SYSBAS	*USE	N
QZSCGETP	*PGM	*USE	QSYS	*SYSBAS	*USE	N

. . .

Liste de contrôle avec CHGRPTONLY à *YES

Adopting Objects by User Profile (Changed Report)

User profile . . . . . : QSECOFR
Special authorities . . . . . : *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL
*SAVSYS *SECADM *SERVICE *SPLCTL

----------Object----------			----------Library----------			
Name	Type	Public Authority	Name	ASP Device	Public Authority	Private Authorities

(There are no objects to list)

La gestion des droits d'accès aux objets

L'accès aux spools

Les spools sont gérés en fonction de plusieurs niveaux de paramètres :

- Les droits spéciaux de l'utilisateur
  - ***JOBCTL**
  - ***SPLCTL**
- Les droits de l'utilisateur sur l'OUTQ
- Les attributs de l'Outq elle-même

OPRCTL	Operator Control	(valeur *YES ou *NO)
DSPDTA	Display Data	(valeur *YES, *NO ou *OWNER)
AUTCHK	Authority Check	(valeur *DTAAUT ou *OWNER)

La combinaison de ces paramètres déterminera les accès suivants :

- Visualisation des spools
- Gestion partielle des spools
- Gestion complète des spools
- Gestion de l'éditeur

Le tableau suivant permet de comprendre l'impact de chacun des paramètres

La gestion des droits d'accès aux objets

paramètres de l'OUTQ			le Profil n'est pas propriétaire de l'OUTQ			Profil propriétaire ou SPCAUT(*SPLCTL)
			Profil défini avec SPCAUT(*NONE)		SPCAUT(*JOBCTL)	
OPRCTL	DSPDTA	AUTCHK	Droits *USE sur l'OUTQ	Droits *CHANGE		
*NO	*YES	*DTAAUT	visu des spools	**visu des spools gestion des spools gestion éditeur**	*identique à SPCAUT(*NONE)*	**visu des spools gestion des spools gestion Editeur**
		*OWNER	visu des spools	visu des spools		
	*NO	*DTAAUT		**visu des spools gestion des spools gestion éditeur**		
		*OWNER				
	*OWNER	*DTAAUT		gestion des spools (*) gestion éditeur		
		*OWNER				
YES	*YES	*DTAAUT	visu des spools	**visu des spools gestion des spools gestion éditeur**	***visu des spools gestion des spools gestion Editeur***	
		*OWNER	visu des spools	visu des spools		
	*NO	*DTAAUT		gestion des spools (*) gestion éditeur		
		*OWNER				
	*OWNER	*DTAAUT		gestion des spools (*) gestion éditeur	gestion des spools (*) gestion éditeur	
		*OWNER				

(*) quelques paramètres de gestion du spool, mais pas changement d'OUTQ

Sauvegardes / Restaurations

Security information saved or restored	Save and restore commands used					
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT	RSTDFROBJ
User profiles	X		X			
Object ownership [1]		X		X		X
Primary group [1]		X		X		X
Public authorities [1]		X		X		X
Private authorities[3]	X	X	X	X	X	X
Authorization lists	X		X			
Authority holders	X		X			
Link with the authorization list and authority holders		X		X		
Object auditing value		X		X		
Function registration information [2]		X		X		
Function usage information	X		X		X	
Validation lists		X		X		
Server Authentication Entries	X		X			
Security information saved or restored	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**

Nouveautés V7.1 concernant la restauration d'Objets

Avec les commande de restauration, dans le paramètre **ALWOBJDIF** (Allow object differences), la possibilité d'utiliser la valeur ***COMPATIBLE** a été ajoutée.

Les valeurs possibles sont donc maintenant :

*AUTL, *FILELVL, *OWNER et *PGP, qui peuvent être combinées.

ou *NONE, *COMPATIBLE ou *ALL, qui sont des valeurs uniques

Comme pour *ALL, la valeur *COMPATIBLE permet d'autoriser toutes les différences utilisables individuellement.
Mais cette valeur autorise uniquement les différences qui sont compatibles avec les fichiers de la base de données.

Cette valeur est préférable à la valeur *ALL qui autorise en plus les différences qui ne sont pas compatibles avec les fichiers de la base de données.

Le Journal d'Audit de la sécurité

Le journal d'Audit du système est un journal possédant 2 spécificités :

- Le nom de cet objet est **QAUDJRN**, dans la librairie QSYS
- Le système écrit des postes, structurés par codes et types, qui sont fonctions des 3 valeurs systèmes déjà évoquées (QAUDCTL, QAUDLVL et QAUDLVL2)

Notes :

- Les récepteurs peuvent être écrits dans n'importe quelle librairie, sous n'importe quel nom.
- Des postes utilisateurs peuvent être ajoutés par programme (avec un code U)

Comme pour tous les journaux, le journal ne peut être créé que si un premier récepteur existe. Les valeurs systèmes associées peuvent ensuite être paramétrées pour commencer à remplir le journal QAUDJRN.

Si l'environnement d'Audit n'est pas déjà créé, on peut utiliser la commande **CHGSECAUD** (V5R4), qui créera les objets et paramètrera les valeurs système :

```
CHGSECAUD       QAUDCTL(*AUDLVL *OBJAUD  *NOQTEMP)              +
                QAUDLVL(*AUTFAIL *SECURITY  *SAVRST *PGMFAIL    +
                *CREATE *DELETE *PGMADP *OBJMGT)                +
                JRNRCV(QGPL/AUDRCV0001)
```

Le Journal d'Audit de la sécurité

Lorsque l'environnement d'Audit est créé, et à tout moment, la commande **DSPSECAUD** permet de visualiser sur un seul écran toutes les informations associées à l'Audit Journal :

Current Security Auditing Values

Security Auditing Journal Values

Security journal QAUDJRN exists . . . . . :	YES
Journal receiver attached to QAUDJRN :	AUDRCV0001
Library . . . . . :	QGPL

Security Auditing System Values

Current QAUDCTL system value . . . . . :	*AUDLVL *OBJAUD *NOQTEMP
Current QAUDLVL system value . . . . . :	*AUTFAIL *SECURITY *SAVRST *PGMFAIL *CREATE *DELETE *PGMADP *OBJMGT
Current QAUDLVL2 system value . . . . . :	*NONE

Le Journal d'Audit de la sécurité

Le journal peut être visualisé par la commande **DSPJRN QAUDJRN**, avec possibilité de paramétrer les date/heure de début et fin de liste, la plage des récepteurs à utiliser, etc..
Des filtres peuvent également être utilisés sur les codes et types de postes à lister.

La liste des codes utilisés dans les postes de QAUDJRN est la suivante :

A - System accounting entry
B - Integrated file system operation
C - Commitment control operation
D - Database file operation
E - Data area operation
F - Database file member operation
I - Internal operation
J - Journal or journal receiver operation
L - License management
M - Network management data
P - Performance tuning entry
Q - Data queue operation
R - Record level operation
S - Distributed mail service for SNA distribution services (SNADS), network alerts, or mail server framework
T - Audit trail entry
U - User generated
Y - Library operation

A chaque code correspond un ensemble de types.
Par exemple, pour le code T, il existe plus de 80 types de postes, comme AF (Authority failure), AP (Program adopt), CO (Object created), DO (Object deleted) ou SV (Change to system value)

Le Journal d'Audit de la sécurité

La commande **DSPAUDJRNE** permet de lister les postes de l'Audit journal liés directement à la sécurité.
On peut lister les postes concernant des actions effectuées par un profil spécifique, ceci permettant de suivre spécifiquement les profils ayant des droits spéciaux.

Display Audit Journal Entries (DSPAUDJRNE)

Journal entry types	AF	AF, CA, CD, CO, CP, CU, CV...	← 30 valeurs possibles
+ for more values			
User profile	*ALL	Name, *ALL	
Journal receiver searched:			
Starting journal receiver . .	*CURRENT	Name, *CURRENT, *CURCHAIN	
Library		Name, *LIBL, *CURLIB	
Ending journal receiver . . .		Name, *CURRENT	
Library		Name, *LIBL, *CURLIB	
Starting date and time:			
Starting date	*FIRST	Date, *FIRST	
Starting time		Time	
Ending date and time:			
Ending date	*LAST	Date, *LAST	
Ending time		Time	
Output	*PRINT	*PRINT, *	

La journalisation des données

En plus du journal d'Audit, des journaux dits « Base de Données », ou « User » sont utilisables depuis plus de 30 ans, pour tracer les modifications d'enregistrements des fichiers Physiques.

La journalisation de certains objets contenant des données, en plus des fichiers Physiques est arrivée progressivement en V5.
A partir de la V5R4, il est maintenant possible de journaliser les objets en librairies de type ***DTAARA**, ***DTAQ**, ou les objets de l'**IFS**.

Les modifications de contenu de ces objets sont donc tracées dans les postes des journaux, avec ceux des objets fichiers, et dans la séquence effectuée par les programmes.

Ceci est particulièrement utile en cas de réplication des données sur un autre serveur.

Pour rappel
Les entrées de journal peuvent inclure :
- l'identification du job, de l'utilisateur et la date/heure
- les images des contenus Avant et Après modifications de l'objet
- les enregistrements quand l'objet a été ouvert, fermé, modifié, sauvegardé, créé, supprimé , etc

En V5R4, les commandes associées sont **STRJRNPF** (pour les fichiers Physique), **STRJRNOBJ** (pour les DTAARA et DTAQ) et **STRJRN** (pour l'IFS). Et les commandes **ENDJRNxxx** correspondantes.

La journalisation des données

Depuis la V6R1 les commandes **STRJRNLIB** et **ENDJRNLIB** permettent de gérer la journalisation de tous les Objets journalisables d'une ou plusieurs librairies en une seule fois.
Attention : les nouveaux objets créés ou ceux qui sont restaurés dans la librairies seront automatiquement journalisés, mais pas ceux déjà présents dans la librairie.

Start Journal Library (STRJRNLIB)

Library	_____	Name, generic*
+ for more values	_____	
Journal	_____	Name
Library	*LIBL	Name, *LIBL, *CURLIB
Inherit rules:		
Object type	*ALL	*ALL, *FILE, *DTAARA, *DTAQ
Operation	*ALLOPR	*ALLOPR, *CREATE, *MOVE...
Rule action	*INCLUDE	*INCLUDE, *OMIT
Images	*OBJDFT	*OBJDFT, *AFTER, *BOTH
Omit journal entry	*OBJDFT	*OBJDFT, *NONE, *OPNCLO
Remote journal filter	*OBJDFT	*OBJDFT, *NO, *YES
Name filter	*ALL	Name, generic*, *ALL
+ for more values		
Logging level	*ERRORS	*ERRORS, *ALL

Les informations de journalisation sont maintenant des attributs de la librairie.

Ceci remplace l'utilisation de la DTAARA QDFTJRN qui indiquait au système comment effectuer cette fonction d'auto-journalisation. *Attention : il faut supprimer la DTAARA si déjà présente.*

La journalisation des données

Diverses opérations concernant les journaux

La commande **STRJRNAP** permet de journaliser les chemins d'accès des membres d'un fichier physique, d'un fichier logique avec clé, ou d'un fichier logique joint.

Les postes de journaux obtenus ne sont pas utilisables par programmes, mais permettent au système d'effectuer une récupération des chemins d'accès, au lieu d'une reconstruction, pendant un IPL après arrêt anormal du système.

Pour rappel :
La commande **EDTRCYAP** permet d'évaluer les temps de récupération des chemins d'accès et indique ceux qui sont protégés ou non.
Alors que la commande **EDTRBDAP** permet de gérer les chemins d'accès non journalisés qui sont à reconstruire.

Les opérations de Commitment Control existent depuis les années 80 sur cette plateforme.
Elles permettent de sécuriser les transactions en refusant celles dont les mises à jour de données sont incomplètes. Ceci permet d'assurer que la Base de données reste intègre

Après journalisation des fichiers, utiliser les commandes **STRCMTCTL** et **ENDCMTCTL** pour activer/désactiver la fonction et **COMMIT** ou **ROLLBACK** pour valider ou refuser l'ensemble des mises à jour de la transaction.

La journalisation des données

Le Remote Journaling

Cette fonctionnalité a été créée en V4 de l'OS, principalement pour répondre aux besoins des produits de réplication.

Principes

- A un journal base de données Local, un journal Remote est associé, sur un autre serveur
- Lorsqu'un récepteur du journal Local est créé, le système créé un récepteur du journal Remote
- Lorsque le système insère un poste dans le journal Local, il envoie ce poste vers le journal Remote
- Il existe 2 modes d'envoi possibles :
  - Synchrone le poste Remote est écrit sur le 2ème serveur, avant le poste du serveur Local
  - Asynchrone les 2 postes sont écrits simultanément, sans coordination entres les actions

Impacts sur la sécurité

- Le journal Remote sert à répliquer les modifications DB Locales, dans une copie maintenue en permanence sur le 2ème serveur (peut sauvegarder les données sans arrêt des accès DB Locaux)
- Le mode Synchrone maintient les données les plus à jour sur le 2ème serveur
- Le mode Asynchrone permet aussi de protéger les données se trouvant en buffer mémoire du serveur Local, les I/Os disque étant périodiques, celles de communication étant immédiates
- A la reprise de la communication, si elle a été interrompue entre les serveurs, le système renvoie automatiquement les postes non transmis vers le journal Remote

La journalisation des données

Le Remote Journaling

Commandes associées

ADDRMTJRN pour créer et associer un journal Remote à un journal Local (dit Source)
A la création, l'état du journal Remote est ***INACTIVE**, les données du journal Source ne lui sont pas envoyées. La commande **CHGRMTJRN** permet de modifier l'état à ***ACTIVE.**

Communication

La communication entre les serveurs utilise le service **DRDA**, et le serveur **DDM** TCP/IP.
Cela nécessite d'ajouter un poste dans les entrées de base de données relationnelle.
(commande **ADDRDBDIRE** ou **WRKRDBDIRE**)

Display Relational Database Entry Detail

Relational database	C23xxxxx	← nom du poste *LOCAL de l'autre serveur
Relational database alias	REMOTE_JOURNALING	
Remote location:		
Remote location	193.xxx.xxx.xxx	← adresse IP de l'autre serveur
Type	*IP	
Port number or service name	*DRDA	
Remote authentication method:		
Preferred method	*USRENCPWD	
Allow lower authentication	*ALWLOWER	
Secure connection	*NONE	
Encryption algorithm	*DES	
Text	Gestion de la communication du Remote Journal	
Relational database type	*REMOTE	← Type de Database

Les iASP (independent Auxiliary Storage Pool)

On parle d'**Independent Disk Pool ou d'Independent Auxiliary Storage Pool**

Cette fonctionnalité permet de gérer des groupes de disques, pouvant être mis Offline ou Online indépendamment des données système, ou d'autres groupes de données.

Un iASP peut rester connecté à un seul serveur, ou être switché sur une autre serveur dans un environnement de clustering.

Cette fonctionnalité a un certain nombre d'impacts de sécurité sur le système :

- Un profil ne peut pas être créé dans un iASP, mais s'il est propriétaire d'objets dans l'iASP son nom y est stocké pour, en cas de switch, se rattacher au profil correspondant d'un autre serveur.
- Une liste d'Autorisations est gérée un peu de la même manière, stockée dans l'ASP système, mais avec une "extension" dans l'iASP, utilisable en cas de switch sur un autre serveur.
- Un iASP ne peut pas déborder (comme le ferait un ASP classique), puisqu'il doit pouvoir être switché
- Un certains nombres d'objets ne peuvent pas être stockés dans les iASP, comme tous les objets de communication, les Documents et les Folders, les JOBQ, les OUTQ, ou le Scheduler.

Vous trouverez dans ce document les informations à connaître:

http://www.redbooks.ibm.com/redbooks/pdfs/sg246802.pdf

L'IFS

Document technique IBM n° 19541539

« Le système d'exploitation n'est pas sensible aux attaques de virus PC.

Les virus attaquent une architecture d'ordinateur spécifique. L'architecture système d'un IBM System i rend hautement improbable qu'un virus puisse être écrit pour l'attaquer.

Les virus PC ne pourront pas infecter (ou s'exécuter sur) le système d'exploitation. Il n'y a pas de programmes IBM anti-virus disponibles pour le système d'exploitation, bien que l'activation d'un scan anti-virus soit fourni avec la V5R3M0.

Bien que le système d'exploitation ne puisse pas être infecté par un virus PC, si l'IFS est utilisé comme serveur de fichiers pour les fichiers PC, les fichiers stockés dans l'IFS peuvent contenir des virus.

Un fichier infecté qui est déplacé ou sauvegardé à partir d'un PC vers l'IFS, puis redistribué à un autre PC peut transmettre un virus au nouveau PC.

De même, si un lecteur réseau est mappé vers l'IFS, un virus s'exécutant sur un PC (et capable d'endommager des fichiers sur un lecteur réseau) peut endommager les fichiers stockés dans l'IFS. »

Scan de l'IFS

Le Scan de l'IFS est géré par des valeurs système et des Point d'Exit.

La valeur système **QSCANFS**, qui indique :
- soit une liste de systèmes de fichiers
- soit *ROOTOPNUD qui signifie que le Scan sera fait dans « root » (/), Qopensys, et les systèmes User-Defined
- soit *NONE pour ne rien scanner

La valeur système **QSCNAFSCTL**, qui indique des contrôles à appliquer au Scan.
Par exemple, *ERRFAIL pour empêcher l'action prévue sur le fichier IFS en cas d'erreur du programme de scan associé, ou *NOPOSTRST pour ne pas scanner après restauration.

Le point d'exit utilisé à l'ouverture d'un fichier :
QIBM_QP0L_SCAN_OPEN - Integrated File System Scan on Open Exit Program

Le point d'exit utilisé à la fermeture d'un fichier :
QIBM_QP0L_SCAN_CLOSE - Integrated File System Scan on Close Exit Program

Sécurité i5/OS et IBM i

Références

	IBM	Security Reference 7.1	SC41-5302-11
Dan Riehl	SecureMyi.com	Security Newsletter for the IBM I	
Carol Woodbury	SkyView Partners	Webinars sécurité	
	Cilasoft	Documentation du produit CONTROLER	
	Vision solutions	Documentation du produit MIMIX	
Christian Massé	Volubis	Documents Pause-Café	