cilasoft

Dotez-vous de la meilleure sécurité pour vos données IBM i,

elles le valent bien !

Présentation animée par Guy Marmorat - le 14/05/2014 - IBM Paris

Quels seront les thèmes de cette session ?

1. Présentation de Cilasoft
2. Les Réglementations
3. L’audit et la Sécurité sur IBM i
   a. L’audit
   b. Le contrôle d’accès
   c. La confidentialité

Copyright 2014 © Cilasoft

1. **Présentation de Cilasoft**
2. **Les Réglementations**
3. **L'audit et la Sécurité sur IBM i**
   a. **L'audit**
   b. **Le contrôle d'accès**
   c. **La confidentialité**

Copyright 2014 © Cilasoft

Qui sommes-nous ?

25 ans d'expérience sur IBM i (AS/400, iSeries)

Cilasoft est éditeur de logiciels d'audit, de compliance et de sécurité spécialisés sur IBM i

Cilasoft est certifié :

- IBM Advanced Business Partner
- Ready For PureSystems
- Ready For Security Intelligence

Ses solutions sont reconnues comme leaders sur la plateforme IBM i et sont référencées dans le IBM Global Solutions Directory

Et

IBM i Solution Editions

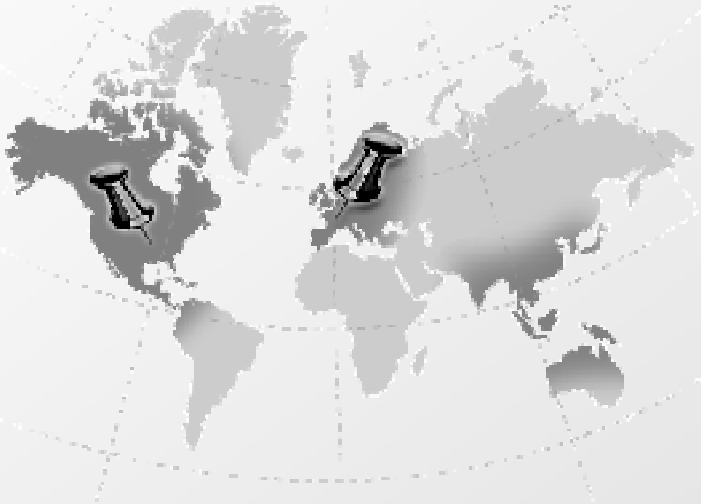
Copyright 2014 © Cilasoft

Qui sommes-nous ?

Editeur à l'International

La Suite Compliance Cilasoft :

1. **QJRN/400**
2. **CONTROLER**
3. **DATABASE VIEW MONITOR (DVM)**
4. **ELEVATED AUTHORITY MANAGER (EAM)**
5. **CENTRAL**
6. **POST FILE**



Siège Social à Annecy, France

Filiale à Atlanta, USA

Réseaux de Partenaires à travers le monde

Clients : + de 300 dans 65 pays

Copyright 2014 © Cilasoft

Cilasoft Compliance Suite

QJRN/400

AUDIT & COMPLIANCE

⇨ Rapports et Alertes sur les évènements Bases de données et Système

DVM

AUDIT DES ACCES EN LECTURE

⇨ Audit des accès en lecture sur vos données sensibles au niveau enregistrement

⇨ QUI a vu QUEL enregistrement, COMMENT et QUAND ?

CONTROLER

CONTRÔLE D'ACCES GLOBAL

⇨ ODBC, JDBC, OLE DB
⇨ FTP, DDM, DRDA
⇨ NetServer
⇨ File open
⇨ SQL engine

EAM

ELEVATED AUTHORITY MANAGER

⇨ Attribuez des Droits sous Contrôle
⇨ Diminuez les Profils puissants
⇨ Réduisez le nombre d'erreurs humaines

CENTRAL

⇨ Plateforme d'échanges de données depuis un site central

POST FILE

⇨ Rapports et Alertes Stand-Alone ou intégré

Copyright 2014 © Cilasoft

Meilleure technologie dans le monde d'IBM i avec un investissement constant dans la R&D

- Aucune modification dans les applications existantes
- Gestion de **l'impact sur le disque et CPU** à travers différents procédés d'optimisation
- Compatible avec les environnements **IASP**
- Langues disponibles : **Français**, **Anglais, Espagnol**
- Interfaces **graphiques et 5250**

Copyright 2014 © Cilasoft

Critères de choix d'un produit de sécurité.

- Tester et comparer
- Attention aux interfaces graphiques séduisantes qui cachent un moteur poussif
- Les qualités que vous devez exiger :
  - Cout en CPU maitrisé afin d'absorber les augmentations de charge ponctuelles ou définitives
  - Configuration très flexible, capable de traiter des cas nouveaux
  - Résultats pertinents, tant en contenu qu'en présentation
  - Sécurité interne et monitoring irréprochable
  - Haut niveau d'automatisation
  - Et même si cela va de soi : doit tout couvrir
- Tenté par le module intégré dans l'ERP? segregation of duties

Copyright 2014 © Cilasoft

1. Présentation de Cilasoft
2. **Les Réglementations**
3. L'audit et la Sécurité sur IBM i
   a. L'audit
   b. Le contrôle d'accès
   c. La confidentialité

Copyright 2014 © Cilasoft

PCI-DSS

Exigences PCI-DSS
Mettre en place et gérer un réseau sécurisé : Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte.
Mettre en œuvre des mesures de contrôle d'accès efficaces : Limiter l'accès aux données des porteurs de carte aux cas de nécessité professionnelle absolue.
Surveiller et tester régulièrement les réseaux : Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte.

PCI-DSS (Payment Card Industry – Data Security Standard)

☞ Norme internationale créée en 2004, obligatoire pour toutes les entités responsables d'opérations par cartes bancaires.

☞Garantir la sécurité des données sensibles des porteurs de cartes bancaires et la confidentialité des données de paiement.

Copyright 2014 © Cilasoft

SOX

- Loi adoptée en 2002 aux USA, suite aux scandales Enron et Worldcom.
- Bonne gouvernance des systèmes d'information (référence à COBIT) : améliorer la transparence et l'exactitude des informations financières, éviter les fraudes et rétablir la confiance des investisseurs.
- Sociétés cotées aux USA, mais aussi leurs filiales
- Responsabilité pénale de la Direction, indépendance des auditeurs, contrôle interne efficace sur le reporting financier (section 404 de la loi)
- JSOX, C198, LSF, Circular 052, …

Copyright 2014 © Cilasoft

SOX

Exigences SOX
Contrôler l'accès aux données critiques ou sensibles.
Identifier et surveiller les vulnérabilités et incidents de sécurité.
Détecter et résoudre les problèmes d'accès non autorisés à l'information, aux applications et à l'infrastructure.
Mettre en place un système de traçabilité/log performant Evaluer l'efficacité des contrôles internes par la mise en place d'audit.

Copyright 2014 © Cilasoft

Bâle II

Exigences Bâle II
Risques relatifs à la sécurité des biens et des personnes (sabotage, vol, fraude, etc.)
Les risques informatiques liés au développement et à la maintenance des programmes, aux traitements et à l'utilisation des services de télécommunications (incidents d'exploitation dans les systèmes de production, accès non autorisés, erreurs de traitement, pertes ou altérations accidentelle de données transmises, etc.)
Les risques de gestion interne (malveillance interne, risques en matière de sous-traitance, etc.

- Démarche mondiale de réglementation du monde bancaire depuis 2004
- Transparence dans la gestion des risques opérationnels, meilleure adéquation entre fonds propres et risques encourus
- Obligation de publier sur l'évaluation et la gestion des risques (quantification des risques, leur pilotage et reporting).

Copyright 2014 © Cilasoft

Autres réglementations

- **HIPPA** (Health Insurance Portability and Accountability Act)
  sécurité et confidentialité des données médicales
- **21CFR Part11** (Food & Drug Administration)
  destiné aux fabricants de médicaments et matériel médical
- **LSF** Loi de Sécurité Financière, applicable en France
- Référentiel **COBIT (**Control Objectives for Information and related Technology)
  édité par l'ISACA et l'IT Governance Institute.

Organismes de contrôle

France : ACP (Autorité de Contrôle Prudentielle)
Luxembourg : CSSF (Commission de Surveillance du Secteur Financier)
Suisse : CFB (Commission Fédérale des Banques) et FINMA (Autorité Fédérale de Surveillance des Marchés Financiers)
Canada : AMF (L'Autorité des Marchés Financiers)
…

Copyright 2014 © Cilasoft

1. Présentation de Cilasoft
2. Les Réglementations
3. **L’audit et la Sécurité sur IBM i**
   a. **L’audit**
   b. Le contrôle d’accès
   c. La confidentialité

Copyright 2014 © Cilasoft

Choix de la piste d'audit :

Caractéristiques requises :

- fiable (en terme d'alimentation et de gestion)
- infalsifiable
- non sélective
- la plus proche du système

Les mécanismes d'alimentation :

- l'application
- les programmes trigger
- les messages système
- l'historique système
- la journalisation

Les types de piste :

- fichier
- journal

INDEPENDANCE AVEC LES APPLICATIONS AUSSI !!
Une application peut-elle s'auto auditer ?

Copyright 2014 © Cilasoft

La journalisation

Utilisée pour :

- haute disponibilité
- réplication de données
- contrôle de validation
- réparation de base de données
- audit

Journaux système et base de données de même structure :

- entête (horodatage, user, programme, job, ip, opération, …)
- poste variable selon l'évènement (record si opération sur fichier)

Journal d'audit système QSYS/QAUDJRN piloté par :

- la valeur système QAUDLVL / 2
- la valeur système QAUDCTL
- les valeurs d'audit sur les objets (CHGOBJAUD &CHGUSRAUD)

Journaux de données :

- démarrage non sélectif
- niveau fichier, membre, record

Copyright 2014 © Cilasoft

Journalisation et Haute Disponibilité Logiciel

- La valeur d'audit *CHANGE fut pendant très longtemps la seule méthode permettant d'identifier des changements au niveau objet afin de les répliquer

- Cela peut générer un nombre considérable d'entrées ZC dans le journal système et de ce fait engendrer une pollution inutile

Les postes D-xx dans les journaux de données remplaceront avantageusement les entrées ZC du journal système (une ouverture en modification ne générera pas de poste dans ce cas).
Configurez votre logiciel HA afin d'en bénéficier…

Copyright 2014 © Cilasoft

Journalisation et Haute Disponibilité Logiciel

Les postes D-xx dans les journaux de données remplaceront avantageusement les entrées ZC du journal système (une ouverture en modification ne générera pas de poste dans ce cas). Configurez votre logiciel HA afin d'en bénéficier

Journal Code	Entry Type	Description
D	CT	Create database file
D	DC	Remove referential integrity constraint
D	DF	File was deleted
D	DH	File saved
D	DJ	Change journaled object attribute
D	DT	Delete file
D	DZ	File restored
D	EF	Journaling for a physical file ended (ENDJRNPF)
D	GT	Grant authority
D	TD	Remove trigger

cilasoft

Audit

Journaux

MINENTDTA in CRTJRN, CHGJRN
➔ *NONE, *FILE, *FLDBDY

FIXLENDTA in CRTJRN, CHGJRN
➔ *JOB, *USER, *PGM, *PGMLIB, *RMTADR

```
                 Work with Journa

Journal  . .         . :   GLT               Libr

Attached rece        . :   GLT0339           Library  . . .        :   IJRNDTA

Text . . . .       . . :   GLT DEMO ENVIRONMENT                         F_GLT

ASP  . . . . .     . . :   1                 Journaled obj   :
Message queue      . . :   QSYSOPR             Current  .      . . :        51
  Library  . .     . . :     *LIBL             Maximum  .    . . . :    250000
Manage receiver    . . :   *SYSTEM           Recovery coun . . . :   *SYSDFT
Delete receiver    . . :   *NO               Receiver size options:   *RMVINTENT
Journal cache      . . :   *NO                                        *MAXOPT2
Manage delay . .   . . :   10                Fixed length data  . :   *JOB
Delete delay . .   . . :   10                                         *USR
Journal type . .   . . :   *LOCAL                                     *PGM
Journal state   .  . . :   *ACTIVE                                    *PGMLIB
Minimize entry data  :     *NONE                                      *RMTADR
```

Copyright 2014 © Cilasoft

IMAGES in STRJRNPF
➔ *AFTER, *BOTH

Journaux

OMTJRNE in STRJRNPF
➔ *NONE, *OPNCLO

```
                    Start Journal Physical File (ST    PF)

Type cho   s, press Enter.

Physical  ile to be journaled  .                    Name, generic*, *ALL
  Library  . . . . . . . . . . .     *LI           Name, *LIBL, *CURLIB
             + for more values
                                      LIBL
Journal  . . . . . . . . . . . .                    Name
  Library  . . . . . . . . . . .     *LIBL         Name, *LIBL, *CURLIB
Record images  . . . . . . . . .    *AFTER         *AFTER, *BOTH
Journal entries to be omitted  .    *NONE          *NONE, *OPNCLO
Logging level  . . . . . . . . .    *ERRORS        *ERRORS, *ALL
```

Copyright 2014 © Cilasoft

Journaux

```
                        Display Journal Entry Details

Journal  . . . . . :   GLT              Library  . . . . . :   IJRNDTA

Sequence . . . . . :   44
Code . . . . . . . :   R  - Operation on specific record
Type . . . . . . . :   UP - Update, after-image

Ignore APY/RMV . . :   No
Ref constraint . . :   No
Trigger  . . . . . :   No
Program  . . . . . :   QDZTD00001
  Library  . . . . :     QTEMP
  ASP device . . . :     *SYSBAS
System sequence  . :   0
Thread identifier  :   *OMITTED
Receiver . . . . . :   GLT0339
  Library  . . . . :     IJRNDTA
  ASP device . . . :     *SYSBAS
Journal identifier :   X'3B50000628140E8C0104'
```

Comment interpréter le programme
UPDDTA ➔ QDZTD00001
STRSQL, UPDATE ➔ QCMD
ou autre menu

Copyright 2014 © Cilasoft

cilasoft

Audit

Modification dynamique depuis V5R3

```
                    Change Journaled Object (CHGJRNOBJ)

Type choices,     s Enter.

Objects:
  Object . . .   . . . . . .          Name, generic*, *ALL
    Library  .   . . . . . .   *LIBL   Name, *LIBL, *CURLIB
  Object type    . . . . . .          *FILE, *DTAARA, *DTAQ, *LIB
                 for more values

Include or omit  . . . . . .   *INCLUDE  *INCLUDE, *OMIT
                + for more values

Attribute  . . . . . .                  *IMAGES, *OMTJRNE...
Images . . . . . . . . . . *SAME        *SAME, *AFTER, *BOTH
Omit journal entry . . . . . *SAME      *SAME, *NONE, *OPNCLOSYN
```

Copyright 2014 © Cilasoft

Solution ?

☞ QJRN/400

Copyright 2014 © Cilasoft

cilasoft

QJRN/400

System & Database Auditing

Rapports d'Audit pertinents
Satisfaire les Auditeurs

Utilise le journal d'IBM i pour tracer les évènements Système et Bases de Données

DISCRET
ET ROBUSTE

- ⇨ Produit des rapports et alertes pertinents et compréhensibles
- ⇨ Large choix de rapports : **planifiables, en temps réel**
- ⇨ **Modèles d'Audit standards et personnalisables**
- ⇨ Désynchronisation possible entre les phases d'extraction et de reporting
- ⇨ **Compatible** avec toutes les solutions de **haute disponibilité**
- ⇨ Partenaire IBM pour QRadar, interfacé avec les principales solutions SIEM ; formats LEEF, CEF, RFC3164, RFC5424

Copyright 2014 © Cilasoft

Le module **Audit Bases de données** permet de produire des rapports d'audit sur les changements dans les données

(*Au niveau Fichier, Enregistrement, Zone*)

⇨Les modifications effectuées dans la base de données via des programmes en dehors des applications (SQL, DFU, etc…)
⇨Les évènements intervenus en dehors des heures ouvrables,
⇨Les modifications de zones sensibles telles que les limites de crédit, tarifs, remises, données client/ fournisseur/personnel, paie, RIB, CB…

Le module **Audit Système** permet de produire des rapports d'audit sur les évènements système

(*Au niveau Objet, Evènement*)

⇨Modifications des valeurs système, profils, droits sur les objets, listes d'autorisation, …
⇨Tentatives d'accès (authentification ou accès à un objet)
⇨Activité des profils sensibles (ex: *ALLOBJ, etc.)
⇨Mouvements d'objet en production
⇨Actions sur les fichiers spool, adoption de droits, les exit points, etc
⇨Lecture/utilisation d'objets sensibles (fichier, pgm, menu, commande, etc)

Copyright 2014 © Cilasoft

Audit

Contactez-nous pour revoir la démo
e-mail:
sales@cilasoft.com

Mini démo effectuée le 14 mai 2014 :

- Auditer les changements de champs sensibles dans des fichiers critiques avec QJRN/400
- Auditer toute modification de données réalisée en dehors de l'application avec QJRN/400

Copyright 2014 © Cilasoft

1. Présentation de Cilasoft
2. Les Réglementations
3. L’audit et la Sécurité sur IBM i
    a. L’audit
    b. Le contrôle d’accès
    c. La confidentialité

Copyright 2014 © Cilasoft

Pourquoi renforcer la sécurité standard ?

(ne pas la remplacer !)

Modèle traditionnel :

- Un utilisateur avec des droits *USE peut télécharger le fichier client
- Un utilisateur avec des droits *CHANGE peut écraser le fichier client

Modèle adoption :

- Pas de contrôle des profils *ALLOBJ

Un utilisateur avec possibilités restreintes peut lancer des commandes en mode remote

Pas de visibilité pour les accès non-5250, pas de log en standard

Besoin d'une sécurité « contextuelle »

Idéal : modèle traditionnel + contrôle d'accès

Copyright 2014 © Cilasoft

cilasoft

Le Contrôle d'Accès

Accès par la commande WRKREGINF

Le programme d'exit décide (accepte ou rejette) avant la sécurité standard (peut donc bloquer QSECOFR)

Les points d'exit classiques

IBM exit point	Format	Description
QIBM_QHQ_DTAQ	DTAQ0100	Original Data Queue Server
QIBM_QNPS_ENTRY	ENTR0100	Network Print Server - entry
QIBM_QNPS_SPLF	SPLF0100	Network Print Server - spool file
QIBM_QPWFS_FILE_SERV	PWFS0100	File Server
QIBM_QRQ_SQL	RSQL0100	Original Remote SQL Server
QIBM_QTG_DEVINIT	INIT0100	Telnet Device Initialization
QIBM_QTG_DEVTERM	TERM0100	Telnet Device Termination
QIBM_QTMF_CLIENT_REQ	VLRQ0100	FTP Client Request Validation
QIBM_QTMF_SERVER_REQ	VLRQ0100	FTP Server Request Validation
QIBM_QTMF_SVR_LOGON	TCPL0100	FTP Server Logon
QIBM_QTMF_SVR_LOGON	TCPL0300	FTP Server Logon
QIBM_QTMX_SERVER_REQ	VLRQ0100	REXEC Server Request Validation
QIBM_QTMX_SVR_LOGON	TCPL0100	REXEC Server Logon
QIBM_QTMX_SVR_LOGON	TCPL0300	REXEC Server Logon
QIBM_QTOD_SERVER_REQ	VLRQ0100	TFTP Server Request Validation
QIBM_QZDA_INIT	ZDAI0100	Database Server - entry
QIBM_QZDA_NDB1	ZDAD0100	Database Server - data base access
QIBM_QZDA_ROI1	ZDAR0100	Database Server - object information
QIBM_QZDA_ROI1	ZDAR0200	Database Server - object information
QIBM_QZDA_SQL1	ZDAQ0100	Database Server - SQL access
QIBM_QZDA_SQL2	ZDAQ0200	Database Server - SQL access
QIBM_QZHQ_DATA_QUEUE	ZHQ00100	Data Queue Server
QIBM_QZRC_RMT	CZRC0100	Remote Command/Program Call
QIBM_QZSO_SIGNONSRV	ZSOY0100	TCP Signon Server

Le Contrôle d'Accès

Accès par la commande CHGNETA

Les points d'exit « ancêtres »

```
                          Display Network Attributes

DDM request access . . . . . . . . . . . . . . . . :   *OBJAUT

Client request access  . . . . . . . . . . . . . . :   *OBJAUT
```

Copyright 2014 © Cilasoft

cilasoft

Le Contrôle d'Accès

- Les points d'exit classiques ne sont pas dynamiques, sauf TELNET
- Ils acceptent en général un seul programme par point
- Ils sont reliés aux serveurs hôte ou serveurs TCP/IP (et donc leurs Prestart jobs correspondants)

PreStart Job	IBM Exit Point		
QNPSERVS	QIBM_QNPS_ENTRY		
QPWFSERV*	QIBM_QPWFS_FILE_SERV		
QRWTSRVR	*DDM		
QSQSRVR	QIBM_QRQ_SQL	QIBM_QSQ_CLI_CONNECT	
QTFTP*	QIBM_QTMF_SERVER_REQ	QIBM_QTMF_SVR_LOGON	
QTRXC*	QIBM_QTMX_SERVER_REQ	QIBM_QTMX_SVR_LOGON	
QTTFT*	QIBM_QTOD_SERVER_REQ		
QTVDEVICE	QIBM_QTG_DEVINIT	QIBM_QTG_DEVTERM	
QZDASOINIT	QIBM_QZDA_INIT	QIBM_QZDA_NDB1	QIBM_QZDA_SQL1/2
QZHQSSRV	QIBM_QHQ_DTAQ	QIBM_QZHQ_DATA_QUEUE	
QZRCSRVS	QIBM_QZRC_RMT		
QZSOSIGN	QIBM_QZSO_SIGNONSRV		

Copyright 2014 © Cilasoft

Le Contrôle d'Accès

Exit

- **DRDA : Inclus dans DDM – ne descend pas au niveau instruction SQL**
- **Socket : pas disponible avant 7.1, difficile à coder**
- Depuis la V6R1, il est désormais possible de connaitre les informations du client au moment de l'authentification (System i Navigator, Download Client Access, Excel, Java, etc…)
- Ne pas confondre TELNET et le démarrage d'un job interactif

Copyright 2014 © Cilasoft

cilasoft

Data-Centric: SQL & QRY

Protocol	Access protection methods				
	SQL Database Server	Qry Governor	Database Monitor	Original Client Access	Proprietary Point
odbc	x	x	x		
jdbc	x	x	x		
oledb, .net, Client Access, iNav	x	x	x		
PCS400				x	
Showcase					x
STRSQL		x	x		
RUNSQLSTM		x	x		
DRDA		x	x		
Query/400 (RUNQRY, WRKQRY, ...)			x		
OpnQryf			x		
SEQUEL			x		
QSH			x		
SQL RPG / SQL CBL programs		X	X		

Copyright 2014 © Cilasoft

cilasoft

Data-Centric: SQL & QRY

Protocol	Access protection methods				
	SQL Database Server	Qry Governor	Database Monitor	Original Client Access	Proprietary Point
odbc	x	x	x		
jdbc	x	x	x		
oledb, .net, Client Access, iNav	x	x	x		
PCS400				x	
Showcase					x
STRSQL		x	x		
RUNSQLSTM		x	x		
DRDA		x	x		
Query/400 (RUNQRY, WRKQRY, ...)			x		
OpnQryf			x		
SEQUEL			x		
QSH			x		
SQL RPG / SQL CBL programs		X	X		

Copyright 2014 © Cilasoft

cilasoft

Data-Centric: SQL & QRY

Protocol	Access protection methods				
	SQL Database Server	Qry Governor	Database Monitor	Original Client Access	Proprietary Point
odbc	x	x	x		
jdbc	x	x	x		
oledb, .net, Client Access, iNav	x	x	x		
PCS400				x	
Showcase					x
STRSQL		x	x		
RUNSQLSTM		x	x		
DRDA		x	x		
Query/400 (RUNQRY, WRKQRY, ...)			x		
OpnQryf			x		
SEQUEL			x		
QSH			x		
SQL RPG / SQL CBL programs		X	X		

Copyright 2014 © Cilasoft

cilasoft

L'execution de commandes et le paramètre « Limit capabilities »

5250	*dspsysval qdate*
FTP Server	Quote Rcmd *dspsysval qdate*
REXEC	RUNRMTCMD CMD('*dspsysval qdate*') RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( )
Client Access	Rmtcmd //system *dspsysval qdate*
ODBC / DRDA	CALL QSYS.QCMDEXC ('*dspsysval qdate*', 0000000015.00000)
iSeries Navigator	cl:*dspsysval qdate*
DDM	SBMRMTCMD CMD('*dspsysval qdate*') DDMFILE(library/DDMfile)

Copyright 2014 © Cilasoft

Solution ?

☞ CONTROLER

Copyright 2014 © Cilasoft

cilasoft

CONTROLER
Global Access Control

Protégez vos Données Sensibles !
Sécurisez vos accès sur IBM i !

Utilise les exit points d'IBM i pour bloquer/alerter, loguer l'activité interne comme externe

- **Couvre tous les points d'accès sur IBM i**
- Approche **Data-Centric**
- **Complète la Sécurité standard de l'OS**, que ce soit en mode traditionnel ou en adoption de droits
- Modèle de configuration fourni en standard
- Fonctionnalités avancées pour les environnements complexes

PUISSANT
ET PEU
IMPACTANT

Copyright 2014 © Cilasoft

CONTROLER

CONTROLER est le module de Contrôle d'Accès GLOBAL qui complète la sécurité standard de l'OS et fournit une approche "data-centric"

- Couvre tous les protocoles d'accès classiques, tels que **FTP, ODBC, DDM, DRDA, Netserver, TELNET,..**
- Gère n'importe quelle commande utilisateur et système
- Identifie / bloque les ouvertures de fichiers critiques hors du contexte applicatif
- Traite le moteur SQL (CQE & SQE) de 2 façons différentes, dont le moteur SQE en mode bloquant
- Traite n'importe quel travail qui démarre, s'arrête, passe en JOBQ
- Identifie/pénalise les requêtes SQL consommatrices de CPU
- Impact très faible sur les performances, spécialement pour une utilisation intensive de ODBC/JDBC
- Vocabulaire exhaustif utilisable dans les règles
- Large choix d'actions et d'alertes

CONTROLER se compose de 2 modules qui peuvent fonctionner séparément :

Module **Contrôle des Protocoles d'Accès** & Module **Contrôle des Commandes**

Copyright 2014 © Cilasoft

Le Contrôle d'Accès

Contactez-nous pour revoir la démo
e-mail:
sales@cilasoft.com

Mini démo :

- Auditer/bloquer les transactions SQL sur des critères multiples avec CONTROLER
- Adopter une approche « data-centric » pour protéger de manière imparable vos fichiers critiques avec CONTROLER

Copyright 2014 © Cilasoft

1. Présentation de Cilasoft
2. Les Réglementations
3. L’audit et la Sécurité sur IBM i
    a. L’audit
    b. Le contrôle d’accès
    c. La confidentialité

Copyright 2014 © Cilasoft

La confidentialité

Au niveau Objet (Qui a ouvert ce fichier ?)
Au niveau Enregistrement (Qui a lu cet enregistrement ?)

Objet :

Postes ZC & ZR dans QAUDJRN (valeur d'audit *ALL sur fichier)
Postes OP dans journal de données (OMTJRNE(*NONE))
Point d'exit QIBM_QDB_OPEN

Enregistrement :

Application (par exemple, envoi de postes utilisateurs pour certaines lectures) ➔ incomplet
Field procedures (à partir de 7.1) ➔ donne seulement la valeur du champ, pas de l'enregistrement
Read triggers ➔ seule solution jusqu'à présent, fort impact potentiel sur les performances

Contournement : tokenisation, encryption

Copyright 2014 © Cilasoft

La confidentialité

Solution ?

☞ DVM

Copyright 2014 © Cilasoft

cilasoft

DATABASE VIEW MONITOR

Audit Read Access

Renforcez la confidentialité de vos données critiques !

Utilise un procédé lié aux fichiers pour détecter, loguer, alerter les accès en lecture de vos données sensibles au niveau enregistrement de fichier

- ⇨ Identifie les **enregistrements lus** dans les fichiers critiques
- ⇨ Récupération optimisée des variables du contexte
- ⇨ **Rapports et alertes** sous conditions
- ⇨ **Impact sur la performance minimisée**
- ⇨ **Mode blocage** possible, incluant le mode simulation

Copyright 2014 © Cilasoft

DVM audite les accès en lecture et plus précisément, sait quand un utilisateur lit des données sensibles

QUI a vu QUEL enregistrement, COMMENT et QUAND ?

Audit des lectures (*Au niveau Enregistrement*)

- Définit des conditions précises permettant d'identifier les lectures à risque
- Récupération optimisée des variables du contexte
- Mode blocage possible, incluant le mode simulation
- Mode simulation afin que vous puissiez tester les règles avant de les déployer : assurez-vous que le fichier bloquant ne perturbe pas les activités quotidiennes des utilisateurs
- Déclenchement d'actions et d'alertes sous de multiples formes

Copyright 2014 © Cilasoft

La confidentialité

Contactez-nous pour revoir la démo
e-mail:
sales@cilasoft.com

Mini démo :

- Auditer/bloquer les lectures d'enregistrements pour les données ultra-confidentielles avec DVM

Copyright 2014 © Cilasoft

Références d'Ouvrages & Auteurs

Carol Woodbury:
www.skyviewpartners.com
IBM i & i5/OS Security & Compliance : A Pratical Guide
IBM i Security Administration and Compliance

Dan Riehl:
www.securemyi.com
Articles System i news magazine
Formation en ligne
Newsletter

Larry Youngren : iProDeveloper & search400
Articles dédiés à la journalisation

Pat Botz :
www.botzandassociates.com
Articles sur le Single Sign-On

Copyright 2014 © Cilasoft

cilasoft

Cilasoft vous remercie de votre attention !

Nous restons à votre écoute pour échanger et répondre à toutes vos questions

NORTH AMERICA OFFICE

Cilasoft USA Inc.
3495 Piedmont Rd
Building 11, Suite 710
Atlanta, GA 30305
USA

Phone: 1 404 495 5912

E-mail: **contact.usa@cilasoft.com**

SIEGE SOCIAL

Cilasoft France
ZI Les Iles, 190 route des Sarves
74370 Metz-Tessy (Annecy)
France

Phone: +33 4 50 69 45 98
Fax: +33 4 50 69 45 99

E-mail: **sales@cilasoft.com**