iBelieve 2020

Présent et Futur de l'IBM i

Evènement
On-line
5 Nov

# SESSION

# Retour d'expérience après 20 années dédiées à la Sécurité sur IBM i

Un évènement organisé par :

itheis & IBM

Avec : FRESCHE GAIA Gamma soft GROUPE HISI REMAIN Resiliane XCASE

# Agenda

- Bien comprendre le paramètre LMTCPB des profils : Un classique revisité
- Renforcement de l'Authentification
- Modifications manuelles dans vos données (les identifier, les bloquer, les justifier)
- Meilleures pratiques pour les utilisateurs à privilèges
- Retours clients sur des renforcements dans la sécurité ou la résolution de cas de fraudes
- Questions/Réponses
- L'Offre de Service Resiliane


# Bien comprendre le paramètre LMTCPB des profils :

# Un classique revisité

```
                    Change User Profile (CHGUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . . . > IBELIEVE      Name
User password  . . . . . . . . . .   *SAME

Set password to expired  . . . .     *NO           *SAME, *NO, *YES
Status . . . . . . . . . . . . . .   *ENABLED      *SAME, *ENABLED, *DISABLED
User class . . . . . . . . . . . .   *USER         *SAME, *USER, *SYSOPR...
Assistance level . . . . . . . . .   *SYSVAL       *SAME, *SYSVAL, *BASIC...
Current library  . . . . . . . . .   *CRTDFT       Name, *SAME, *CRTDFT
Initial program to call  . . . . .   *NONE         Name, *SAME, *NONE
  Library  . . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Initial menu . . . . . . . . . . . > IBELIEVE      Name, *SAME, *SIGNOFF
  Library  . . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Limit capabilities . . . . . . . .   *NO           *SAME, *NO, *PARTIAL, *YES
Text 'description' . . . . . . . . > 'iBELIEVE user profile'
```

```
                    Display User Profile - Basic
.....................................................................
:                   Limit Capabilities - Help                       :
:                                                                   :
|                   Additional Message Information                  |

Message ID . . . . . :   CPD0175
Date sent  . . . . . :   10/12/20      Time sent  . . . . . :   18:12:44

Message . . . . :   Command UPDDTA in library *LIBL not allowed.

Cause . . . . . :   The command was typed on a command line or run in a REXX
  procedure by a user with limited capabilities, but the command is not
  allowed for limited users.
Recovery  . . . :   Do one of the following:
    -- Type a menu option or a command that is not restricted.
    -- Have the security officer change the command to allow it from the
  command line or in a REXX procedure (ALWLMTUSR parameter on the Change
  Command (CHGCMD) command).
    -- Have the security officer change your user profile to remove limited
  capability (LMTCPB parameter on the Change User Profile (CHGUSRPRF)
  command).
```

```
Selection or command
===> upddta erpfile/glfclien

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel

Command UPDDTA in library *LIBL not allowed
```

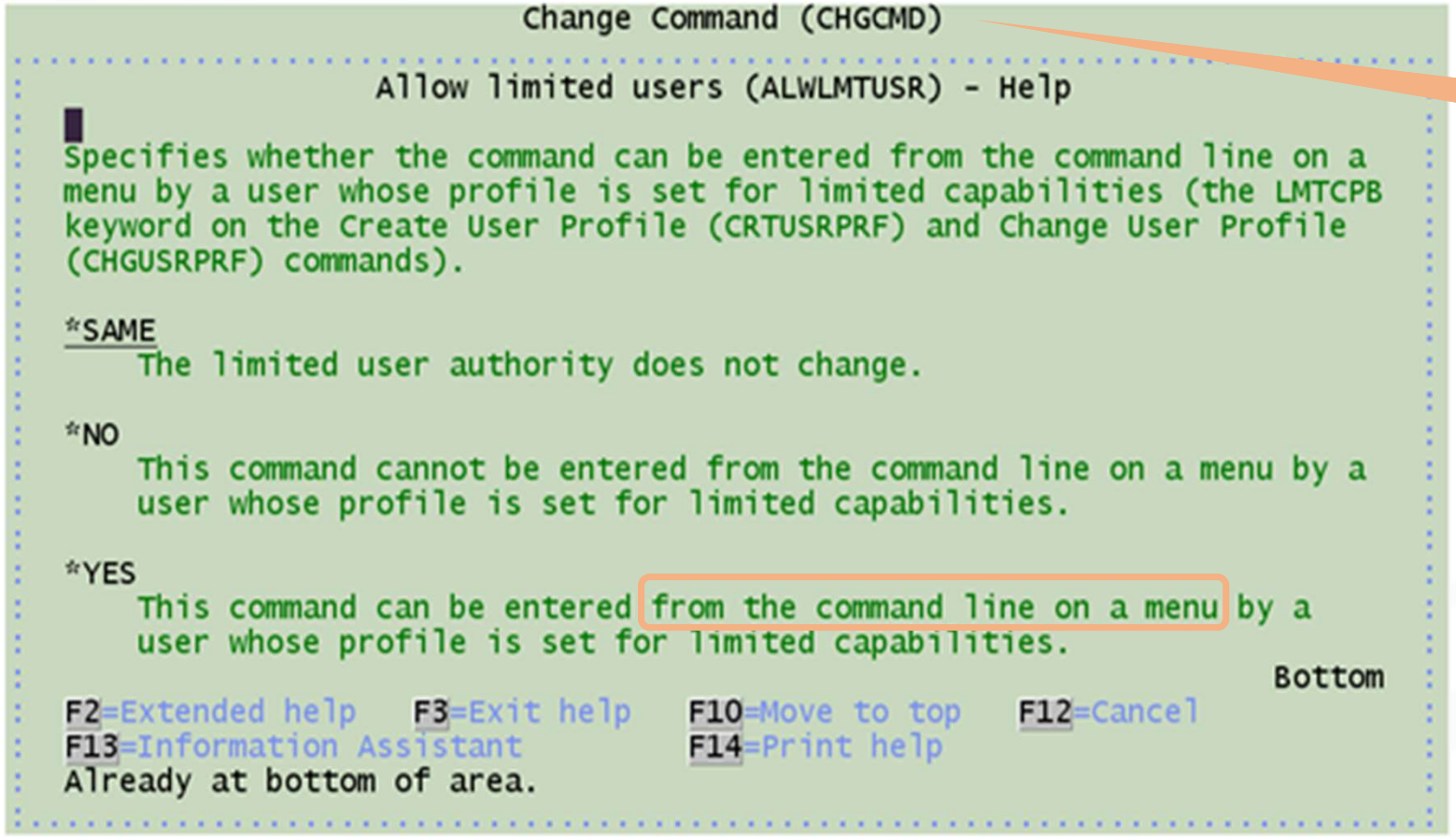
**CHGCMD CMD(QSYS/UPDDTA)**
**ALWLMTUSR(*YES)**

```
Selection or command
===> upddta erpfile/glfclien

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel

Command UPDDTA in library *LIBL not allowed
```

**CHGUSRPRF USRPRF(IBELIEVE)**
**LMTCPB(*NO)**




**CHGCMD CMD(QSYS/UPDDTA)**
**ALWLMTUSR(*YES)**

## Comment connaître les commandes accessibles ?

**DSPCMD donne l'information de façon unitaire**

```
                        Display Command Information

Command  . . . . . :   UPDDTA          Library  . . . . . :   QSYS

Program to process command . . . . . :   QDZCMDP
  Library  . . . . . . . . . . . . . :     QSYS
  State used to call program . . . . . :   *SYSTEM
Source file  . . . . . . . . . . . . . :   S000006991
  Library  . . . . . . . . . . . . . . :   QTEMP
Source file member . . . . . . . . . . :   UPDDTA
Validity checking program  . . . . . . :   *NONE
Mode(s) in which valid . . . . . . . . :   *PROD
                                           *DEBUG
                                           *SERVICE
Where allowed to run . . . . . . . . . :   *IREXX      *IPGM       *EXEC
                                           *INTERACT
Allow limited user . . . . . . . . . . :   *YES
Maximum positional parameters  . . . . :   2
```

## Comment connaître les commandes accessibles ?

Réaliser un utilitaire qui liste les commandes (DSPOBJD en OUTFILE, fonction table OBJECT_STATISTICS) et récupère le paramètre ALWLMTUSR (api QCDRCMDI).

**Allow limited user.** Whether or not a user with limited authorities is allowed to run this command. The possible values are 0 (*NO) or 1 (*YES).

Commandes livrées par IBM avec *YES :

| | |
|---|---|
| QIWS | STRPCO |
| QSYS | CALL |
| QSYS | DSPJOB |
| QSYS | DSPJOBLOG |
| QSYS | DSPMSG |
| QSYS | SIGNOFF |
| QSYS | SNDMSG |
| QSYS | WRKMSG |

*Droit *ALL sur la commande requis pour pouvoir changer ce paramètre par CHGCMD.*

## Comment auditer les changements des commandes faits par CHGCMD?

- Aucun poste d'audit système dédié à ces actions
- Il faut donc activer l'audit sur ces objets

  Exemple : CHGOBJAUD OBJ(QSYS/CHGCMD) OBJTYPE(*CMD) OBJAUD(*ALL)
- Des postes CD seront déposés dans le journal QAUDJRN à chaque exécution
- Analyser ces postes CD avec la commande DSPJRN ou le service SQL DISPLAY_JOURNAL
- Auditer aussi l'utilisation de la commande CHGCMDDFT (valeurs par défaut)

**Exemple** :

```
with cd_entries as (select entry_timestamp, myjrn.current_user, job_name, job_user, program_library, program_name, remote_address,
cast(cast(SUBSTR(entry_data ,2, 10) as char(10) for bit data) as char(10) ccsid 1141) as cmd_name,
cast(cast(SUBSTR(entry_data ,12, 10) as char(10) for bit data) as char(10) ccsid 1141) as cmd_lib,
case cast(cast(SUBSTR(entry_data ,30, 1) as char(10) for bit data) as char(1) ccsid 1141)
when 'Y' then 'CLP'  when 'N' then 'Cmd Line'  when 'R' then 'REXX'  when 'E' then 'API'  when 'B' then 'Batch'
end as cmd_context,
cast(cast(SUBSTR(entry_data ,31, 500) as char(500) for bit data) as char(500) ccsid 1141) as cmd_string
from table( qsys2.Display_Journal ('QSYS','QAUDJRN', Journal_Codes => 'T', STARTING_RECEIVER_NAME => '*CURCHAIN' )) as myjrn
where journal_entry_type = 'CD')
select * from cd_entries where cmd_name in ('CHGCMD', 'CHGCMDDFT');
```

## Comment être plus « fin » sur le contrôle des commandes ?

***De plus,***
***quid des***
***commandes batch ?***

## Liste des protocoles permettant de lancer des commandes

**User profile : LMTCPB(*NO) & Commande CL : ALWLMTUSR(*NO)**

| Protocoles | Syntaxes des commandes |
|---|---|
| **5250** | ***dspsysval qdate*** |
| **FTP Server** | Quote Rcmd ***dspsysval qdate*** |
| **REXEC** | RUNRMTCMD CMD(***'dspsysval qdate'***) RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( ) |
| **FTP Client** | Syscmd ***dspsysval qdate*** |
| **IBM i Access for Windows** | Rmtcmd //system ***dspsysval qdate*** |
| **ODBC / DRDA** | Call qsys2.qcmdexc (‘***dspsysval qdate***') |
| **ACS – Run SQL Script** | cl:***dspsysval qdate*** |
| **DDM** | SBMRMTCMD CMD(***'dspsysval qdate'***) DDMFILE(library/DDMfile) |
| **PuTTY** | db2 "call qsys2.qcmdexc (***'dspsysval qdate'***)” |

## Liste des protocoles permettant de lancer des commandes

**User profile : LMTCPB(*NO) & Commande CL : ALWLMTUSR(*NO)**

| Protocoles | Syntaxes des commandes |
|---|---|
| 5250 | *dspsysval qdate* |
| FTP Server | Quote Rcmd ***dspsysval qdate*** |
| REXEC | RUNRMTCMD CMD(***'dspsysval qdate'***) RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( ) |
| FTP Client | Syscmd ***dspsysval qdate*** |
| IBM i Access for Windows | Rmtcmd //system ***dspsysval qdate*** |
| ODBC / DRDA | Call qsys2.qcmdexc (‘***dspsysval qdate***') |
| ACS – Run SQL Script | cl:***dspsysval qdate*** |
| DDM | SBMRMTCMD CMD(***'dspsysval qdate'***) DDMFILE(library/DDMfile) |
| PuTTY | db2 "call qsys2.qcmdexc (***'dspsysval qdate'***)” |

Les Protocoles ne respectant pas LMTCPB

## Comment contrôler les commandes lancées via ces protocoles non 5250?

**Function Usage (WRKFCNUSG)**

Le service SQL FUNCTION_INFO donne la liste des fonctions utilisables pour les commandes à distance

| FUNCTION_ID | DEFAULT_USAGE | ALLOBJ_INDICATOR | FUNCTION_NAME_MESSAGE_TEXT | FUNCTION_DESCRIPTION_MESSAGE_TEXT |
|---|---|---|---|---|
| QIBM_QTMF_CLIENT_REQ_9 | ALLOWED | NOT USED | CL Commands ... | Use of client subcommand SYSCMD to execute CL commands. |
| QIBM_QTMF_SERVER_REQ_9 | ALLOWED | NOT USED | CL Commands ... | Use of server subcommand RCMD to execute CL commands. |
| QIBM_XE1_OPNAV_RUNCMD | ALLOWED | NOT USED | - | - |

*Pas exhaustif !*

*Aucune granularité*

## Comment contrôler les commandes lancées via ces protocoles non 5250?

**Points d'exit (WRKREGINF)**

- 2 points d'exit disponibles sur les commandes : QIBM_QCA_CHG_COMMAND & QIBM_QCA_RTV_COMMAND
- Une entrée par commande
- Programme d'exit activé lors de l'utilisation de la commande quelle que soit le mode d'exécution.

**Mais comment protéger les commandes de façon globale et uniquement en mode non 5250 ?**

- En utilisant les points d'exit liés aux protocoles
- Le programme d'exit pourrait ainsi contenir une règle générique qui récupère l'attribut LMTCPB de l'utilisateur connecté, repère l'action de lancer une remote commande, et décide de bloquer si l'attribut n'est pas conforme.

*Exhaustif !*

*Granularité forte*

*Mais effort de développement*

## Liste exhaustive des protocoles permettant de lancer des commandes

**User profile : LMTCPB(*NO) & Commande CL : ALWLMTUSR(*NO)**

| Protocoles | Syntaxes des commandes | Exit Points |
|---|---|---|
| **5250** | ***dspsysval qdate*** | QIBM_QCA_RTV_COMMAND |
| **FTP Server** | Quote Rcmd ***dspsysval qdate*** | QIBM_QTMF_SERVER_REQ |
| **REXEC** | RUNRMTCMD CMD(***'dspsysval qdate'***) RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( ) | QIBM_QTMX_SERVER_REQ |
| **FTP Client** | Syscmd ***dspsysval qdate*** | QIBM_QTMF_CLIENT_REQ |
| **IBM i Access for Windows** | Rmtcmd //system ***dspsysval qdate*** | QIBM_QZDA_SQL2 |
| **ODBC / DRDA** | Call qsys2.qcmdexc (‘***dspsysval qdate***') | QIBM_QZDA_SQL2 ⚠ |
| **ACS – Run SQL Script** | cl:***dspsysval qdate*** | QIBM_QZDA_SQL2 |
| **DDM** | SBMRMTCMD CMD(***'dspsysval qdate'***) DDMFILE(library/DDMfile) | CHGNETA DDMACC( ) |
| **PuTTY** | db2 "call qsys2.qcmdexc (***'dspsysval qdate'***)” | Database Monitor ⚠ |

Les Protocoles ne respectant pas LMTCPB

# Renforcement de l'Authentification

## Valeurs système impliquées dans la gestion des mots de passe

**Complexité des mots de passe**
- complexité dans leur gestion
- coût de leur gestion
- impact sur la productivité des utilisateurs

Plus le mot de passe est complexe, plus il devient un facteur de risque car on ne peut plus s'en souvenir….

Valeurs 0 et 2 à proscrire si aucun client en Windows 95/98, ME, Server 2000

QPWD*

| | | |
|---|---|---|
| QMAXSGNACN | *SEC | Action to take for failed signon attempts |
| QMAXSIGN | *SEC | Maximum sign-on attempts allowed |
| QPWDCHGBLK | *SEC | Block password change |
| QPWDEXPITV | *SEC | Password expiration interval |
| QPWDEXPWRN | *SEC | Password expiration warning |
| QPWDLMTAJC | *SEC | Limit adjacent digits in password |
| QPWDLMTCHR | *SEC | Limit characters in password |
| QPWDLMTREP | *SEC | Limit repeating characters in password |
| QPWDLVL | *SEC | Password level |
| QPWDMAXLEN | *SEC | Maximum password length |
| QPWDMINLEN | *SEC | Minimum password length |
| QPWDPOSDIF | *SEC | Limit password character positions |
| QPWDRQDDGT | *SEC | Require digit in password |
| QPWDRQDDIF | *SEC | Duplicate password control |
| QPWDRULES | *SEC | Password rules |
| QPWDVLDPGM | *SEC | Password validation program |
| QSECURITY | *SEC | System security level |

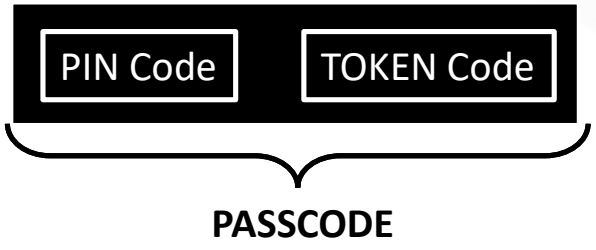
## L'Authentification Multi-Facteurs (MFA) exige au moins 2 des 3 facteurs suivants :

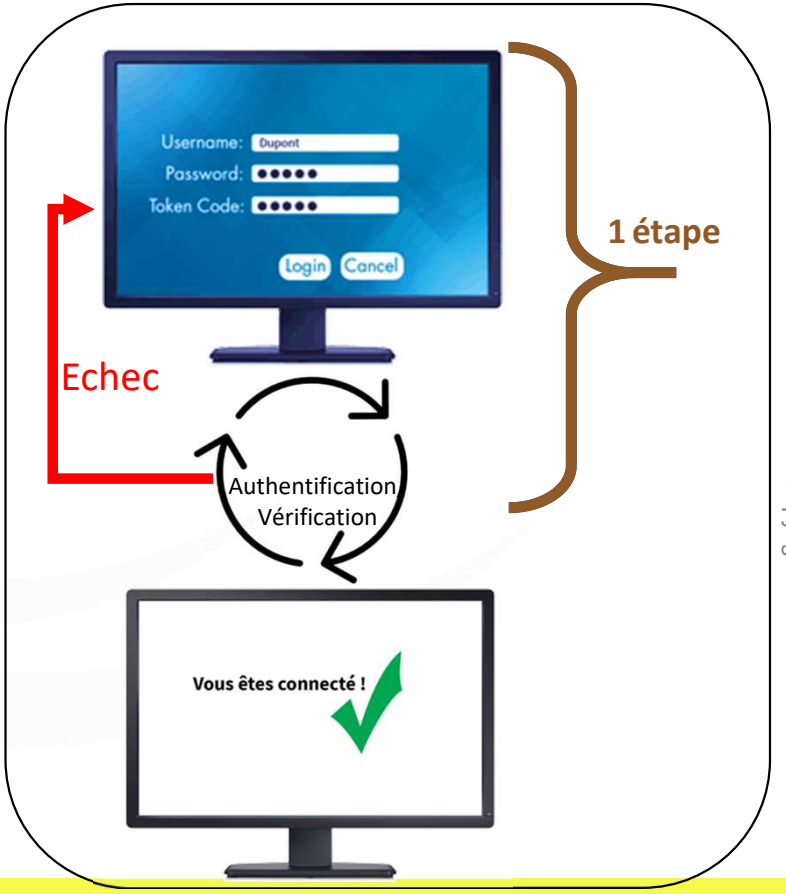
- ✓ **Ce que l'on sait (connaissance)** : UserID/ Mot de passe / PIN / Réponse
- ✓ **Ce que l'on a (possession)** : Téléphone portable / Clé physique
- ✓ **Ce que l'on est (inhérence)** : Empreinte digitale / Iris / Voix

**Authentification en 1 étape**

- ➢ Facteurs d'authentification demandés en même temps
- ➢ Validation de tous les facteurs avant acceptation de l'accès
- ➢ En cas d'échec, l'utilisateur ne connait pas le facteur invalide

**Si !! Si !!, C'EST POSSIBLE sur IBM i !**



## Comment l'implémenter ?

Changer le programme initial des utilisateurs nécessitant ce type de challenge en y intégrant une communication sécurisée avec votre serveur d'authentification (connexion, établissement du dialogue, récupération de la décision du serveur, échec ou succès du processus)

**Les bénéfices :**

- Finalement plus simple et moins couteux que des mots de passe complexes si c'est bien intégré au système d'authentification existant
- Même un processus à 2 étapes est un renforcement, y compris via un simple email
- Répond aux règlementations actuelles … et futures (PCI-DSS 3.2, 23 NYCRR, HIPAA, …)

## Challenges …

- Ségrégation des Users ID entre les machines clientes et le serveur d'authentification
- Interroger une liste de serveurs d'authentification en cas de non disponibilité de l'un d'eux
- Code doit être robuste et discret car en plein milieu d'un processus sensible

**Nec Plus Ultra !**

- Connexion avec un système de ticket
- Déclencher des challenges par rapport à des contextes spécifiques
- Couvrir les connexions autres que 5250
- Principe des « 4 Yeux »

```
System value . . . . . :   QSECURITY
Description  . . . . . :   System security level


System security level  . . . :   40     10=Physical security only (no longer
                                          supported)
                                        20=Password security only
                                        30=Password and object security
                                        40=Password, object, and operating
                                          system integrity
                                        50=Password, object, and enhanced
                                          operating system integrity
```

# Modifications manuelles dans vos données
# - les identifier, les bloquer, les justifier -

**A titre d'exemples, des modifications directes peuvent être faites via des :**

- commandes système : UPDDTA, CHGDTA, CPYF, RUNQRY OUTTYPE(*OUTFILE), …
- commandes ou programmes non système : DBU, TAA Tools, des commandes dupliquées (UPDDTA2), …
- commandes ouvertes sur SQL : STRSQL, RUNSQL, RUNSQLSTM, QSH db2, …
- protocoles « SQL friendly » : System i Navigator (option « edit contents »), ACS Run SQL Script, DRDA, CLI, node.js, …
- utilitaires SQL avec drivers ODBC : DBeaver, WinSQL, …
- protocoles avec des options de masse : ACS Navigator for i (options clear, import), Data transfer to IBM i, FTP (client ou server vers IBM i), ObjectConnect (SAVRSTOBJ MBROPT(*ALL) ALWOBJDIF(*ALL)), …

## Comment les identifier ?

**Journal QAUDJRN :**

- Si l'attribut « auditing value » du fichier est *CHANGE ou *ALL, un poste ZC est généré à chaque ouverture du fichier pour update
- Donc, une entrée ZC ne veut pas nécessairement dire qu'il y a eu une modification !

**Database journal :**

- Chaque update, insert, delete, génère un poste dans le journal au niveau « journal code = R »
- Les éléments discriminants forts, permettant de repérer si la modification est en dehors de l'application, sont les derniers niveaux dans le call stack, soit les colonnes PROGRAM_NAME & PROGAM_LIBRARY (zones JOPGM & JOPGML)
- Cas faciles : les CPP de DFU et DBU sont connus et documentés : QZDTD00001 et DBU00821
- Cas plus difficile : STRSQL depuis une ligne de commande ouverte dans le menu de votre ERP : ERPPGM/MENU.
  STRSQL depuis MAIN: QSYS/QCMD.
- Autres éléments discriminants utiles pour des applications non 5250: adresse IP, user, job

**Comment faire ?**

- DISPLAY_JOURNAL avec filtre sur les colonnes PROGRAM_NAME & PROGAM_LIBRARY.
- 2 options: Rester large au niveau bibliothèque ou plus précis au niveau bibliothèque et programme (mais plus difficile à maintenir).

## Comment les bloquer ?

- Par les droits sur les commandes (insuffisant)
- Par les droits sur les fichiers (mieux, mais insuffisant)
- Via RCAC (pas recommandé de le faire sur toute la base, juste les fichiers critiques)
- Par l'adoption de droits dans l'application (bonne méthode, mais insuffisant aussi)

**Ces méthodes ne fonctionnent pas pour les profils *ALLOBJ (en dehors de RCAC)**

- Par les points d'exit traditionnels (mais les protocoles n'ont pas tous des points d'exit associés
  par exemple : DRDA, STRSQL, open-source, QSH, …)
- Par le point d'exit Open Database File. (La meilleure solution, mais…. délicat à écrire/maintenir - charge CPU, récursivité, …)

## Comment les justifier ?

- Interdire l'utilisation en « libre-service » de commandes telles que STRSQL, UPDDTA
- Obliger les utilisateurs à passer par un système d'enregistrement avec numéro de ticket avec:
  - description de la raison
  - enregistrement de la piste d'audit.

# Meilleures pratiques
# pour les utilisateurs à privilèges

**Droits excessifs en Production**

- Risque d'erreur
- Risque de malveillance
- Non conforme avec les règlementations
- Mauvaises pratiques

**Utilisateurs ayant besoin de droits élevés :**

- Compte de service
- QSECOFR

**Utilisateurs ayant <u>parfois</u> besoin de droits élevés :**

- Développeur
- Administrateur système
- Administrateur base de données
- Support applicatif
- Consultant externe

PCI Security Standards Council

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **10.2.2** Toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur | **10.2.2** Vérifier que toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur sont consignées. | Les comptes possédant des privilèges accrus, comme les comptes « administrateur » ou « racine », sont potentiellement plus dangereux pour la sécurité ou la fonctionnalité opérationnelle d'un système s'ils venaient à être compromis. Sans un journal des activités exécutées, une organisation est incapable de retracer tout problème provoqué par une erreur administrative ou d'une utilisation illicite d'un privilège à l'action et à l'individu spécifiques. |

**Payment Card Industry (PCI) Normes en matière de sécurité des données**

**Solutions**

- Donner des droits temporaires, de façon contrôlée, avec piste d'audit
- Assez facile à implémenter
- Pas de « casse » en Production.

**Comment donner des droits supplémentaires ?**

Agir au niveau du profil :

- Donner des droits spéciaux directement
- Changer le profil de groupe – ajouter un nouveau profil de groupe
- Ajouter le profil ou son groupe dans une liste d'autorisation

Agir au niveau du travail :

- Passer par un programme adoptant les droits d'un profil cible (propagation des droits dans la pile au-dessus)
- Passer par un programme swapant vers un profil cible (héritage des droits du profil cible)

**Comment loguer l'activité du profil pendant l'élévation de droits ?**

- Loguer les commandes dans le journal QAUDJRN - CHGUSRAUD USRPRF(IBELIEVE) AUDLVL(*CMD)
- Extraire les postes de QAUDJRN
- Extraire les postes du journal base de données
- Extraire la joblog
- Récupérer les écrans – STRCPYSCN
- Récupérer les instructions SQL – STRDBMON

**Nec plus ultra :**

- Ne pas donner la ligne de commande, mais une liste de commandes déjà préparées
- Etendre l'élévation en dehors du 5250
- Réduire les droits des comptes de service par des élévations ciblées dans les scripts et CLP
- N'autoriser certaines commandes sensibles qu'au travers d'une élévation contrôlée
- Coupler la demande d'élévation avec un système de ticket
- Attention aux « sorties » possibles durant l'élévation temporaire (SBMJOB, group jobs, ATTN, etc..)

PCI Security Standards Council

| Conditions PCI DSS | Procédures de test | Directive |
|---|---|---|
| **10.2.2** Toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur | **10.2.2** Vérifier que toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur sont consignées. | Les comptes possédant des privilèges accrus, comme les comptes « administrateur » ou « racine », sont potentiellement plus dangereux pour la sécurité ou la fonctionnalité opérationnelle d'un système s'ils venaient à être compromis. Sans un journal des activités exécutées, une organisation est incapable de retracer tout problème provoqué par une erreur administrative ou d'une utilisation illicite d'un privilège à l'action et à l'individu spécifiques. |
| **10.2.3** Accès à toutes les vérifications à rebours | **10.2.3** Vérifier que les accès à toutes les vérifications à rebours sont consignés. | Des utilisateurs malveillants tentent souvent de modifier les journaux d'audit afin de dissimuler leurs activités et un enregistrement des accès permet à une organisation d[é] incohérences ou altérations [des] journaux pour un compte ind[ividuel] aux journaux identifiant les [comptes] additions et les suppressions [ou] retracer les étapes suivies par le personnel non autorisé. |
| **10.2.4** Tentatives d'accès logique non valides | **10.2.4** Vérifier que les tentatives d'accès logique non valides sont consignées. | Les individus malveillants font souvent plusieurs tentatives pour accéder aux systèmes ciblés. De multiples tentatives infructueuses de connexion peuvent indiquer qu'un utilisateur non autorisé tente d'utiliser la « force brute » ou de deviner un mot de passe. |
| **10.2.5** L'utilisation et les modifications des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation de privilèges, et toutes les modifications, additions ou suppressions aux comptes avec des privilèges racines ou administratifs | **10.2.5.a** Vérifier que l'utilisation des mécanismes d'identification et d'authentification est consignée.<br>**10.2.5.b** Vérifier que toutes les élévations de privilège sont consignées.<br>**10.2.5.c** Vérifier que tous les changements, additions ou suppressions apportés à un compte avec privilèges racine ou administratives sont consignées. | Sans savoir qui était connecté au moment d'un incident, il est impossible d'identifier les comptes qui ont pu être utilisés. En outre, les utilisateurs malveillants peuvent tenter de manipuler les contrôles d'authentification avec l'intention de les contourner ou d'usurper un compte valide. |

**10.2.5.b** Vérifier que toutes les élévations de privilège sont consignées.

# Retours clients sur des renforcements dans la sécurité ou la résolution de cas de fraudes

Resiliane

# Retours clients sur des renforcements dans la sécurité ou la résolution de cas de fraudes

## Agro-alimentaire

Des camions remplis de marchandise sortent de l'usine alors que le client ne paie pas !

- ⚠ Investigation infructueuse dans le Journal Base de Données
- ⚠ L'explication se trouvait dans le Journal Système !

## Industrie

Un Directeur Financier … au compte courant impossible à reconstituer

- ⚠ Démasqué par son activité nocturne régulière et bizarre……
- ⚠ La séparation des tâches reste un des piliers incontournables

## Banque Privée

**Un Administrateur Système licencié se retourne contre son employeur et gagne son procès**

- ⚠ Ou comment prouver qu'un Utilisateur a bien accédé à des données confidentielles… ?

Changement d'adresse d'un client exilé fiscal

- ⚠ Mise en place d'une piste d'audit robuste pour toutes les modifications faites sur des données sensibles.


## Banque

### Un Administrateur Système bien caché derrière un Profil Générique !

- ⚠ Vérification des phrases SQL par injection d'un secret dans le commentaire

### Principe des « 4 Yeux »

- ⚠ Pour une transaction ou intervention sensible
  - travail figé, déverrouillé par une autre personne en saisissant son passcode, capture des écrans

## Assurance

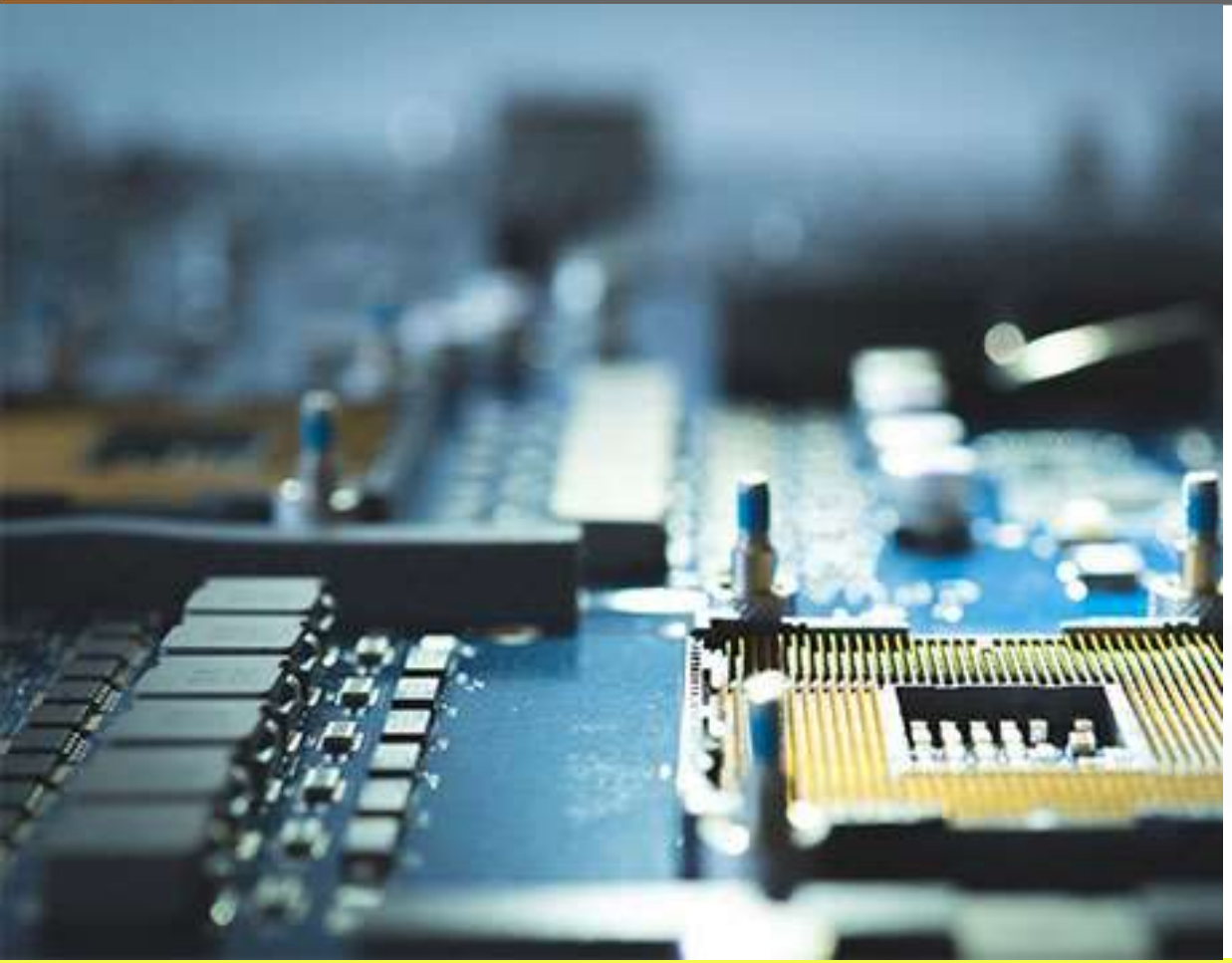
### Justification des SQL directs

- ⚠ Saisie d'un ticket valide dans les commentaires SQL en cas d'update.

## Telecom

### Virus dans l'IFS

- ⚠ Empêcher l'apparition de nouveaux .exe dans l'IFS, que ce soit par création, restauration ou renommage, en dehors des procédures de mise en production très bien contrôlées.



## Organisme dans la monétique

### Méthode « Zero Trust » avec les points d'exit !

- ⚠ L'Utilisateur doit d'abord passer la barrière du « logon » avec des vérifications au niveau IP, device, application cliente. Chaque sollicitation capturée par un point d'exit de type « request » est également vérifiée au niveau statement, bibliothèque/fichier, répertoire IFS, type d'accès

- ⚠ Cela demande une gestion très rigoureuse des permissions et surtout des tests en pré-production irréprochables

## Banque

Exit point et coût CPU

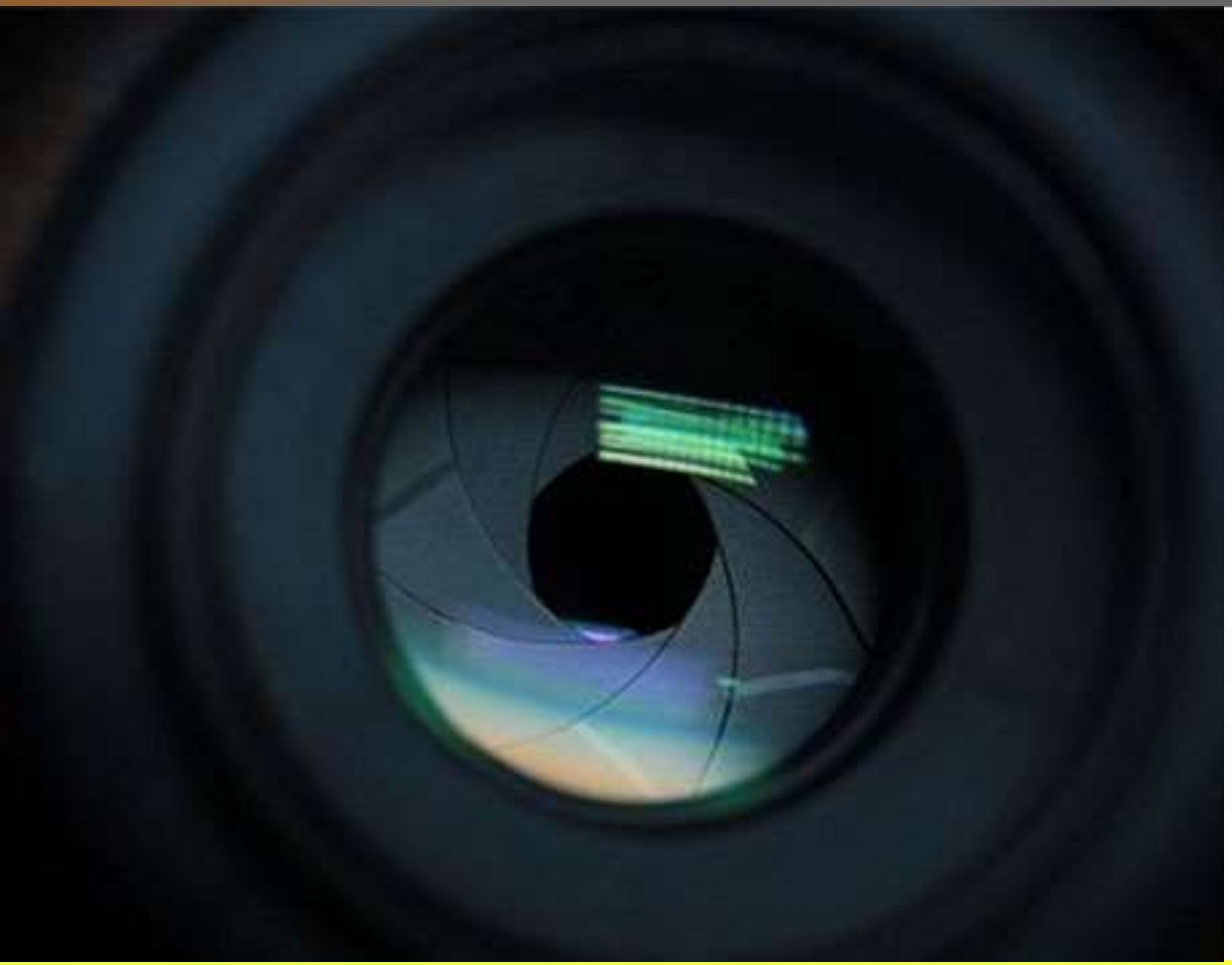
- ⚠ Chaque mois, le programme d'exit était débranché la veille du pic d'activité de l'appli mobile et rebranché une fois le pic passé, car le coût CPU du programme d'exit provoquait des time-out dans l'appli mobile…

## Autre Banque

QSECURITY 20 (Et oui !)

QUSER *ALLOBJ + profil de groupe ! Si si !! ;-)

- ⚠ Ces 2 banques voulaient gérer leur sécurité avec des points d'exit en plus de la restriction ligne de commande



## Entreprise possédant des données hautement confidentielles

Les accès hors application : cauchemar ou politique de l'autruche ??….

- ⚠ La puissance de SQL, le foisonnement du monde Open-Source, PASE rendent ce sujet très délicat.
- ⚠ L'implémentation du point d'exit Open Database File donne d'excellent résultats

Améliorations sympathiques et encore peu utilisées suite à des propositions de Cilasoft à IBM Rochester

- ✓ Point d'exit Open Database File, *AFTER sur le point d'exit sur les commandes, valeurs multiples pour CDCLP dans les postes CD de QAUDJRN, optimisation de la fonction cache de RCAC)

**Ma recommandation du jour :**

- ✓ Prenez grand soin de toutes vos pistes d'audit
  - définition,
  - rétention,
  - protection,
  - possibilité de restauration,
  - intégrité.

# L’Offre de Service Resiliane



Resiliane


Resiliane vous aide à résoudre les problèmes

de sécurité et de conformité

dans l'environnement IBM i

Resiliane

## Exemples de Prestation de Service

- Aider à l'implémentation de rapports d'audit, de règles de contrôle d'accès et de paramètres de configuration
- Être votre Officier de Sécurité à temps partiel
- Vous accompagner à résoudre les problèmes listés dans votre rapport d'audit officiel et/ou vous aider à préparer votre prochain audit
- Effectuer des tests de violation d'accès (Ethical Hacking)
- Investiguer en cas de suspicion d'activités frauduleuses
- etc

*Les missions s'effectuent sur site et/ou à distance (français et/ou anglais)*

Resiliane

Les besoins en matière de sécurité
et conformité sont multiples !

Contactez-nous

pour toute question,

pour tout complément d'information,

ou pour tout simplement échanger sur
l'Audit & la Sécurité sur IBM i

✉ contact@resiliane.com
resiliane.com

# Merci de votre attention
# Portez-vous bien
# Et
# À bientôt !