7 déc. 2023

Événement Online

iBelieve 2023

Présent et Futur de l'IBM i

Un événement organisé par itheis avec la participation d' IBM

ACMi · CFD Innovation · Fresche Solutions · GAIA · IBM · ipls · itheis · M81 IBM i Editor · precisely · Remain Software · resolution XCASE

Inventaire des différentes méthodes permettant le renforcement de la Sécurité et de l'Auditabilité des données IBM i

- Guy MARMORAT -

Inventaire de tous les moyens d'accès aux fichiers / tables Db2

Associated protocols:
ODBC
JDBC
.Net
OLEDB
DRDA
SSH Db2
CLI/QShell Db2
Remote SQL, XDA
VS Code – Db2 for i
…

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
…
+ ☒

SSH
SCP/SFTP
Put
Get …

SSH
PASE
cp
mn
rm
chmod …

User Commands
(CPP)
DBU …

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQRY

IBM i Services
`get_clob_from_file`
`QSYS2.IFS_READ`
`QSYS2.IFS_WRITE`
~~`SYSTOOLS.IFS_RENAME`~~
…

Accessing JOURNAL receiver contents:
QSYS2.DISPLAY_JOURNAL
DSPJRN, RCVJRNE
QjoRetrieveJournalEntries …

FTP Server
FTP Client
Put
Get
Delete
Rename …

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM …
+ ☒

File Server
NetServer/QSYS.LIB
Open
Rename
Delete …

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

Remote Commands:
FTP Server - Quote Rcmd
FTP Client - Syscmd
REXEC - RUNRMTCMD
DDM - SBMRMTCMD
IBM i Access for Windows - RMTCMD
ODBC/DRDA - QCMDEXC via call or select
SSH – System …

Inventaire de tous les moyens d'accès aux fichiers / tables Db2

SSH SCP/SFTP
Put
Get …

SSH PASE
cp
mn
rm
chmod …

User Commands (CPP)
DBU …

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
…

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename …

AUDIT

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx }
CPYxxx DMPxxx } BATCH
SNDSMTPEMM …

File Server
NetServer/QSYS.LIB
Open
Rename
Delete …

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF…)
SQL, RLA

Pourquoi une Piste d'Audit est si importante ?

- Toujours comprendre ce qui s'est passé
- Identifier les tentatives et les violations de sécurité
- Prouver les effets positifs de vos remédiations
- Identifier les effets de bord de vos remédiations
- Identifier les effets négatifs de vos remédiations

Les évènements à auditer et leurs pistes d'audit associées

Evènements à auditer	Journal	Journal code	Entry types	Autres pistes d'audit
Les ouvertures de fichier (en lecture, en modification)	QAUDJRN	T	ZC – ZR (access type = 30 …)	Authority Collection, Exit Point 'Open Database File'
	Database	F	OP	
Les actions au niveau objet (création, suppression, rename, sauvegarde, restauration, droits, propriétaire, ...)	QAUDJRN	T	CO - DO - OM - ZR (access type = 46 47 48) - OR - CA – OW	Command & SQL Exit points, Database Monitor, Plan Cache
	Database	D	CT - DT - FN - DH - DZ - GT – GO	
Les actions sur certains attributs des fichiers (triggers, contraintes, fonctions RCAC, journalisation, ...)	Database	D	TC TD TG - AC DC GC - M1 M2 M3 P1 P2 P3 - DJ EF JF	Command & SQL Exit points, Database Monitor, Plan Cache
	QAUDJRN	T	AX	
Les actions au niveau membre (création, suppression, rename, sauvegarde, restauration, journalisation, clear, reorganize, ...)	Database	F	MC - MD - MN - MF MS - MR - JC EJ JM - CR - RG RM	Command & SQL Exit points, Database Monitor, Plan Cache
Les actions au niveau enregistrement (ajout, modification, suppression)	Database	R	PT PX - UB UP - DL	Triggers (système & SQL), SQL Exit points, Database Monitor, Plan Cache
Les tentatives d'accès aux fichiers	QAUDJRN	T	AF	Authority Collection
Les modifications des valeurs d'audit	QAUDJRN	T	AD	Command Exit point
Les lectures au niveau enregistrement				Read-Triggers (système) 

Auditable

SSH SCP/SFTP
Put
Get …

SSH PASE
cp
mn
rm
chmod …

User Commands (CPP)
DBU …

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
…

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename …

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM …

File Server
NetServer/QSYS.LIB
Open
Rename
Delete …

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

Assure Monitoring and Reporting

Audit Système et Base de données - Rapports et alertes

Enjeux

- Mise en conformité avec les lois et réglementations (RGPD, PCI-DSS, HIPAA, SOX, etc)
- Système de reporting/alerting proactif sur des points clés bien définis
- Investigation, debugging, recherche de litiges et preuves
- Bonnes pratiques (séparation des tâches, dissuasion, éducation, transparence, qualité)

Technologie

- Tout type de journal (système, base de données, propriétaire)
- Données statiques collectées par service SQL ou API
- Reporting lisible, enrichi, automatisé
- Filtre puissant
- Intégration avec les plateformes SIEM via les formats LEEF, CEF, RFC3164, RFC5424, user defined, les protocoles Syslog et LFP (QRadar, Splunk, ArcSight, LogRhythm, Solarwinds, NetWrix, Elastic, …)
- Modèles d'audit disponibles pour certains ERP et personnalisables

Cas d'usage

- Identifier toutes les modifications de données faites en dehors des programmes de l'application
- Collecter des évènements ciblés dans le système (exemple: valeurs système, profils, manipulations d'objets dans QSYS.LIB & IFS, tentatives d'accès, commandes entrées, …)
- Auditer toute opération dans Assure Security via son modèle intégré
- Filtrer, formater, enrichir, envoyer les évènements pertinents en provenance de différentes sources dans une SIEM

Inventaire de tous les moyens d'accès aux fichiers / tables Db2

SSH
SCP/SFTP
Put
Get …

SSH
PASE
cp
mn
rm
chmod …

User Commands
(CPP)
DBU …

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
…

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename …

PROTECTION

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM …

File Server
NetServer/QSYS.LIB
Open
Rename
Delete …

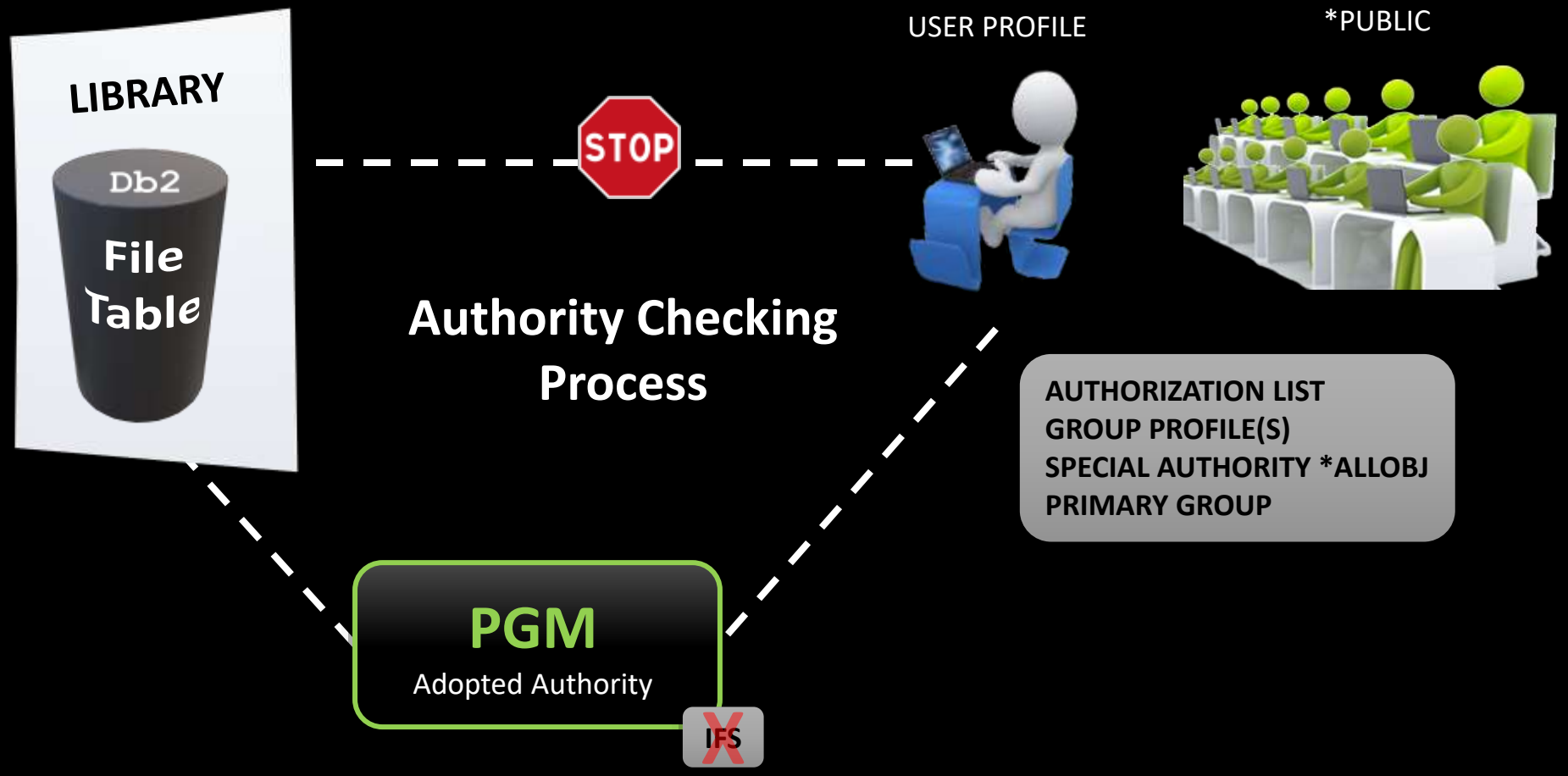
ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

Object Level Security - Fondation de droits statiques

Niveau Objet



Besoin de plus de contexte

Protégeable
Object Level Security

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
...

SSH SCP/SFTP
Put
Get ...

SSH PASE
cp
mn
rm
chmod ...

User Commands (CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM ...

File Server
NetServer/QSYS.LIB
Open
Rename
Delete ...

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

Function Usage – Droits d'accès contextuels basiques

Niveau Protocole

Protocole
Fonction
Navigator for i
FTP
Database Server
…

USER PROFILE

*PUBLIC

FUNCTION_PRODUCT_ID	NUMBER
QIBM_ACS	2
QIBM_BASE_OPERATING_SYSTEM	22
QIBM_NAV	16
QIBM_QINAV_NAVIGATOR_WEB	3
QIBM_QSY_DIGITAL_CERT_MGR	1
QIBM_QTM_TCPIP	18
QIBM_QTMS_TCPIP	1
QIBM_QYCM_CIMOM	11
QIBM_QYPS_MGTCTRL	1
QIBM_XD1_OPNAV	75

Par défaut: *ALLOWED ou *DENIED
Accès précisé pour les profils *ALLOBJ

QIBM_NAV_ALL_FUNCTION	New Nav Access	*DENIED
QIBM_NAV_*	New Nav functions	*ALLOWED
QIBM_DB_ZDA	ODBC	*ALLOWED
QIBM_DB_DDMDRDA	DDM & DRDA	*DENIED
QIBM_QTMF*	FTP	*ALLOWED

Besoin d'encore plus de contexte

Protégeable
Function Usage

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
...

SSH
SCP/SFTP
Put
Get ...

SSH
PASE
cp
mn
rm
chmod ...

User Commands
(CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM ...

File Server
NetServer/QSYS.LIB
Open
Rename
Delete ...

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

RCAC/Row - Droits d'accès par Rang

Niveau Rang

SQL PERMISSION

```
where cliarea = 'EMEA' and
verify_group_for_user (current_user,
'WGRPEMEA') = 1
```

Client ID	Client Name	Client Type	Client St	Taxe Id	Adress 1	Currency	Area
4915000000000001	John Ford	DDDDD	N	213-073-4574	Lambert Walk	EUR	EMEA
4915000000000002	Jaime PENAGOS	DDDDD	Y	172-111-2233	NORTE 5	PES	NOAM
4915310000000011	Chris Wang	AAAAA	Y	8884554448	Ocean Drive	EUR	LACA
4915000000000001	Petros CHRISTOFIDES	DDDDD	N	174-073-6190	Avenue Petros	EUR	ASIP
4915310000000002	Basel Slimani	BBBBB	Y	88888220000-1	Avenue Jacques Cartier	XAF	EMEA
5900100010101011	Jean René DURAND	CCCCC	Y	1234567	Avalon	EUR	ASIP
6078787878787878	Sylvia Krol	BBBBB	Y	BBBB3		ZLT	EMEA
1234567890123456	Rastapopoulos	AAAAA	Y	122-073-6290		EUR	LACA
101245894317825	Andrew Watson	BBBBB	N	VAT-114	Downing Street	USD	NOAM
5489000000000001	Vassou Kichenassamy	DDDDD	N	213-073-4574	Bangalore Street	EUR	XXXX

- Rejeté par défaut (condition 0=1), independant des interfaces, mécanisme "silencieux" (clause WHERE implicite)
- Couvre toute opération au niveau rang (read, update, delete, insert).
- Intervient après object level security.
- Permet de présenter un fichier "vide" à un user *ALLOBJ

Besoin d'encore plus de contexte

RCAC/Column - Masquage d'une colonne

Niveau Colonne

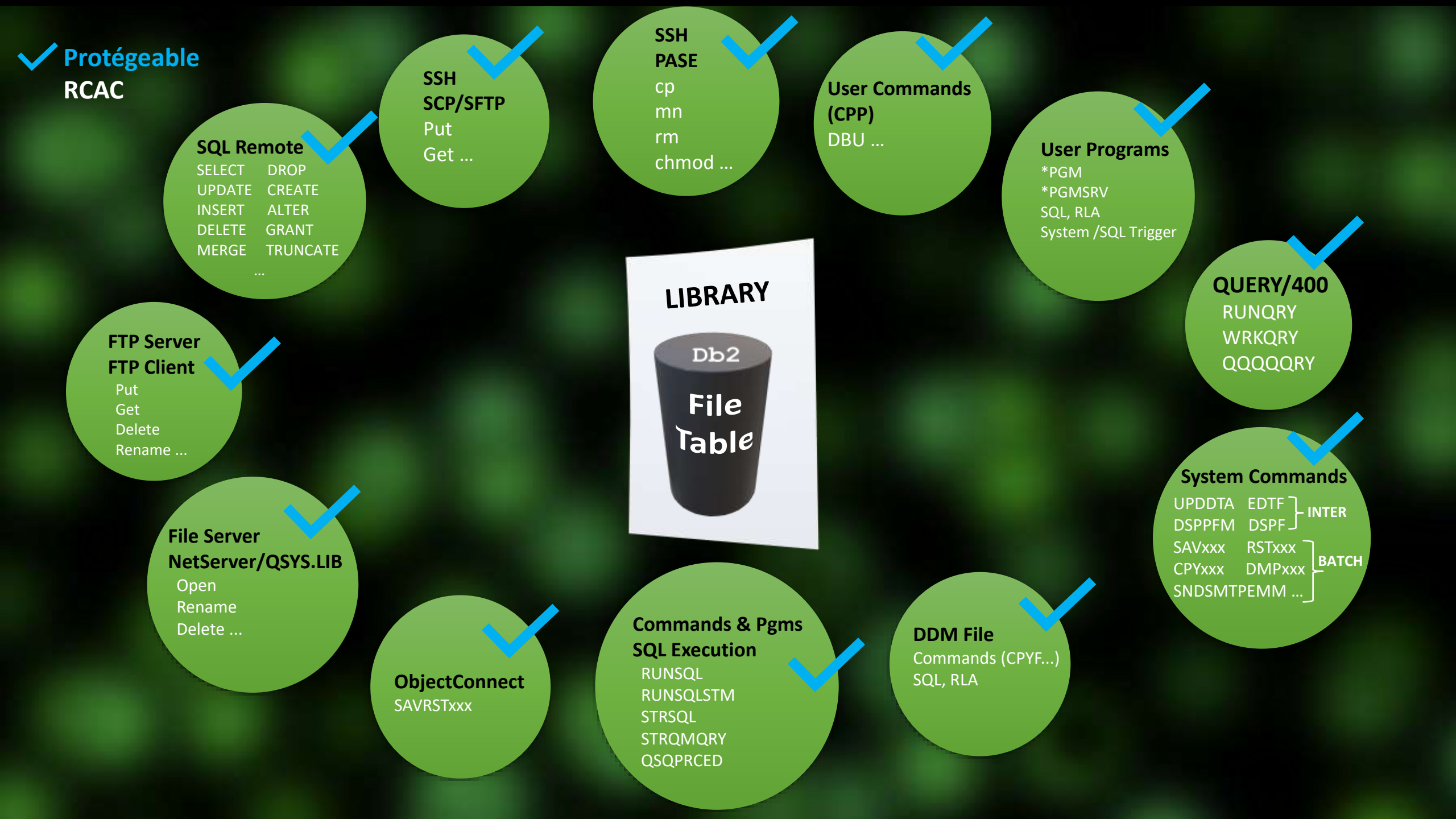
SQL MASK

```
return case when current_user =
'WUSRALL' then clitaxid else
'.....' end
```

Client ID	Client Name	Client Type	Client St	Taxe Id	Adress 1	Currency	Area
4915000000000001	John Ford	DDDDD	N	213-073-4574	Lambert Walk	EUR	EMEA
4915000000000002	Jaime PENAGOS	DDDDD	Y	172-111-2233	NORTE 5	PES	NOAM
4915310000000011	Chris Wang	AAAAA	Y	8884554448	Ocean Drive	EUR	LACA
4915000000000001	Petros CHRISTOFIDES	DDDDD	N	174-073-6190	Avenue Petros	EUR	ASIP
4915310000000002	Basel Slimani	BBBBB	Y	88888220000-1	Avenue Jacques Cartier	XAF	EMEA
5900100010101011	Jean René DURAND	CCCCC	Y	1234567	Avalon	EUR	ASIP
6078787878787878	Sylvia Krol	BBBBB	Y	BBBB3		ZLT	EMEA
1234567890123456	Rastapopoulos	AAAAA	Y	122-073-6290		EUR	LACA
101245894317825	Andrew Watson	BBBBB	N	VAT-114	Downing Street	USD	NOAM
5489000000000001	Vassou Kichenassamy	DDDDD	N	213-073-4574	Bangalore Street	EUR	XXXXX

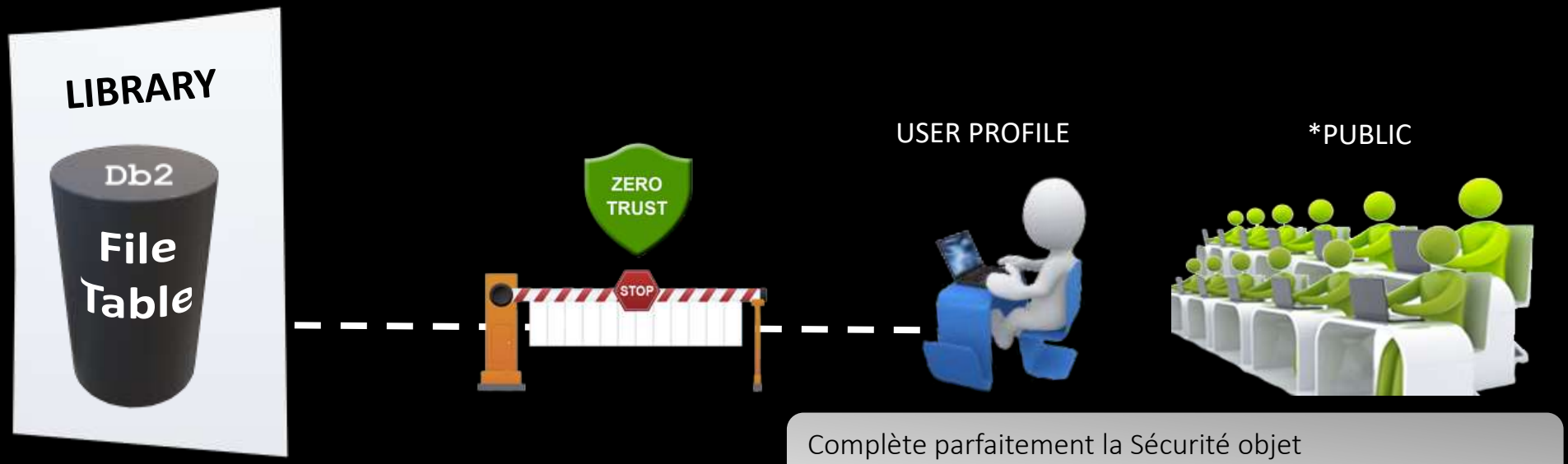
- Indépendant des interfaces
- Couvre toute opération de lecture
- Enregistré dans QIBM_DB_SECADM pour administrer RCAC

Besoin d'encore plus de contexte


Protégeable
RCAC
SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
...
SSH
SCP/SFTP
Put
Get ...
SSH
PASE
cp
mn
rm
chmod ...
User Commands
(CPP)
DBU ...
User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger
QUERY/400
RUNQRY
WRKQRY
QQQQQRY
FTP Server
FTP Client
Put
Get
Delete
Rename ...
LIBRARY
Db2
File
Table
System Commands
UPDDTA EDTF
DSPPFM DSPF
INTER
SAVxxx RSTxxx
CPYxxx DMPxxx
BATCH
SNDSMTPEMM ...
File Server
NetServer/QSYS.LIB
Open
Rename
Delete ...
ObjectConnect
SAVRSTxxx
Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED
DDM File
Commands (CPYF...)
SQL, RLA

Exit points - Droits d'accès contextuels complets

Niveaux
Protocole
Job
TimeStamp
IP
Registre Client
Phrase SQL
…



Complète parfaitement la Sécurité objet
Couche sollicitée avant le « Authority-Checking Process »

Que faire avec un programme d'exit :

- Rejeter certaines connexions et/ou transactions
- Loguer les tentatives rejetées
- Loguer certaines connexions et/ou transactions au caractère sensible (user admin, table critique, IP non recensée, call stack non applicatif, etc…)
- Déclencher des actions (envoi dans une SIEM, alerte, remédiation automatique, challenge MFA, interagir avec un SOAR, etc…)

Contrôle d'accès « contextuel » le plus poussé

Exit points - Droits d’accès contextuels complets

Niveaux
Protocole
Job
TimeStamp
IP
Registre Client
Phrase SQL
…

Catégories de Points d’Exit en lien avec la Sécurité

Ceux qui sont :

- attachés à l’authentification (FTP Server, REXEC, ODBC, TCP Logon)
- attachés aux transactions, commandes, fonctions, … (FTP client, FTP Server, REXEC, ODBC, NetServer, Remote Commands, DDM)
- attachés aux commandes (before, after)
- attachés aux Sockets (communication de bas niveau - IP & Port)
- attachés au moteur SQL (Query Governor, Query Supervisor)
- plus exotiques (job_notify, virus scanning, profile, password, data queues, …)

Contrôle d’accès « contextuel » le plus poussé

Protégeable
Exit Points
Protocoles

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
...

SSH
SCP/SFTP
Put
Get ...

SSH
PASE
cp
mn
rm
chmod ...

User Commands
(CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM ...

File Server
NetServer/QSYS.LIB
Open
Rename
Delete ...

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF...)
SQL, RLA

Exit points - Droits d’accès contextuels complets

Niveaux
Protocole
Job
TimeStamp
IP
Registre Client
Phrase SQL
…

Catégories de Points d’Exit en lien avec la Sécurité

Ceux qui sont :

- attachés à l’authentification (FTP Server, REXEC, ODBC, TCP Logon)
- attachés aux transactions, commandes, fonctions, … (FTP client, FTP Server, REXEC, ODBC, NetServer, Remote Commands, DDM)
- attachés aux commandes (before, after)
- attachés aux Sockets (communication de bas niveau - IP & Port)
- attachés au moteur SQL (Query Governor, Query Supervisor)
- plus exotiques (job_notify, virus scanning, profile, password, data queues, …)

- attachés aux ouvertures de fichiers Db2 (valeur d'audit *CHANGE, *ALL) & IFS stmf (attributs *CRTRUNEXIT & *RUNEXIT)

Contrôle d’accès « contextuel » le plus poussé

Protégeable
Exit Points
Ouvertures fichiers

SQL Remote
SELECT DROP
UPDATE CREATE
INSERT ALTER
DELETE GRANT
MERGE TRUNCATE
...

SSH SCP/SFTP
Put
Get ...

SSH PASE
cp
mn
rm
chmod ...

User Commands (CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA
System /SQL Trigger

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

System Commands
UPDDTA EDTF } INTER
DSPPFM DSPF }
SAVxxx RSTxxx } BATCH
CPYxxx DMPxxx }
SNDSMTPEMM ...

DDM File
Commands (CPYF...)
SQL, RLA

Commands & Pgms SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

ObjectConnect
SAVRSTxxx

File Server NetServer/QSYS.LIB
Open
Rename
Delete ...

FTP Server FTP Client
Put
Get
Delete
Rename ...

Exit points - Droits d’accès contextuels complets

Niveaux
Protocole
Job
TimeStamp
IP
Registre Client
Phrase SQL
…

Eléments de réflexion :

- Plusieurs vulnérabilités importantes découvertes depuis 2022 et qui existent depuis toujours dans notre OS préféré….. (15 CVE avec score > 7 en 2023 !)
- Les éditeurs de logiciels sont attaqués et/ou présentent des failles critiques (SolarWinds, Fortra/GoAnywhere, MOVEit, …). Quid de nos habitudes envers les tiers de confiance ?!!
- Les possibilités SQL et Open-source deviennent plus nombreuses et complexes
- Un utilisateur sans droits avec possibilités restreintes conserve néanmoins des capacités importantes de découverte du système
- Définition d'un accès en lecture ? Un SELECT associé à un download ACS n'est pas équivalent au même SELECT dans une application Java…. (exportation de données pour l’un)
- Enfin, le contexte géopolitique et évènementiel se tend…

Contrôle d’accès « contextuel » le plus poussé

Assure System Access Manager

Utilise les points d'exit pour capturer, bloquer, alerter, loguer les connexions & transactions

Enjeux

- Mise en conformité avec les lois et réglementations (RGPD, PCI-DSS, HIPAA, SOX, etc)
- Prévenir les attaques « classiques » (CryptoLocker et autres malware) et avancées (Advanced Persistent Threat, Software Supply Chain Attacks, diversion attacks)
- Limiter les erreurs humaines
- Prévenir les fuites de données
- Bonnes pratiques (Principle of Least Privilege, isolation, Zero-Trust)
- Intégrité du système et des données (contrôle des modifications directes des données, contrôle des commandes sensibles, etc.)

Technologie

Basé sur les points d'exit

- Protocoles « natifs IBM i » (ODBC, JDBC, FTP, DDM, DRDA, REXEC, NetServer)
- Commandes système et utilisateur
- Protection fichiers Db2 à la source
- Protocoles « non natifs IBM i » (SSH, SFTP, QSH, sockets UDP/TCP, …)

Points clé

- Impact CPU maîtrisé
- Mode simulation/bloquant
- Finesse des règles & vocabulaire
- Listes blanches, noires et combinaisons des deux
- Souplesse de décision de loguer, alerter, déclencher des actions

Cas d'usage

- Besoins simples (log, reporting) répondant aux règlementations
- Contrôle drastique des comptes de service à la connexion (user, IP, registre) et à la transaction (Fortress ou Zero-Trust)
- Environnement multi-iASP (password, SQL, compartimenter les utilisations par iASP, protection *SYSBAS)
- Blocage des accès aux données sensibles en dehors de l'application
- Ne plus permettre d'ajouter le droit spécial *ALLOBJ à la création/modification de profil

Autres mesures augmentant la protection des données Db2

- Encryption des données par les Field procedures
- Anonymisation des données
- Combinaisons de différentes mesures pour durcir les accès aux données sensibles et/ou l’utilisation des interfaces directes (MFA, élévation de droits, système de tickets intégrés aux points d’exit)

Merci de votre attention !

Un événement organisé par itheis avec la participation d' IBM

iBelieve 2023
Présent et Futur de l'IBM i

ACMi CFD INNOVATION FRESCHE SOLUTIONS GAIA IBM ipls itheis M81 IBM i EDITOR precisely REMAIN SOFTWARE resolution XCASE