Université IBM i

19 et 20 novembre 2024

Inventaire des méthodes pour renforcer la Sécurité et l'Auditabilité des données IBM i

Guy Marmorat
Consultant expert Sécurité IBM i
gmarmorat@resiliane.com

IBM

common FRANCE

Université IBM i

19 et 20 novembre 2024

IBM

- Les méthodes d’accès aux données Db2
- Les technologies disponibles pour améliorer l’auditabilité et la protection

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
Mapepire
…

SSH SCP/SFTP
Put
Get …

SSH PASE
cp
mn
rm
chmod …

User Commands (CPP)
DBU …

User Programs
*PGM
*PGMSRV
SQL, RLA

Triggers
ADDPFTRG
CREATE TRIGGER

QUERY/400
RUNQRY
WRKQRY
QQQQRY

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

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

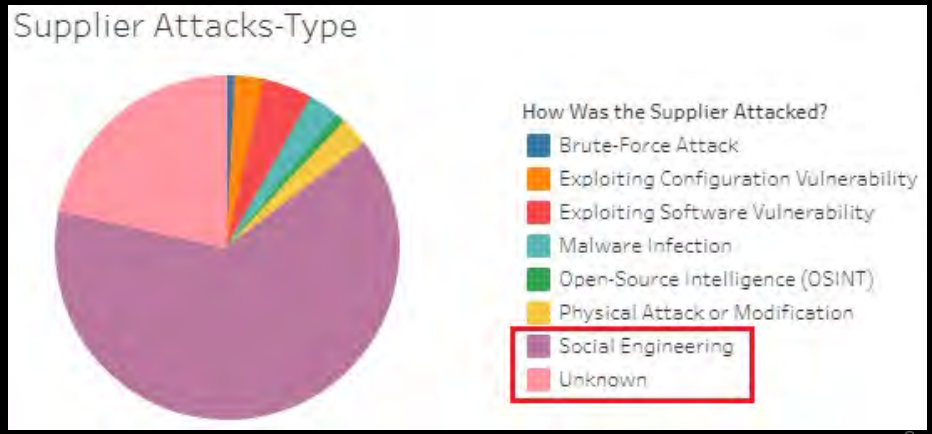
DDM File
Commands (CPYF...)
SQL, RLA

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 …

IBM i

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



https://www.comparitech.com/software-supply-chain-attacks/

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) 

Comment trouver la description des entrées de journal ?

```
Object . . . . . :                    Library  . . . . . :
Member . . . . . :
Incomplete data  . . :   No            Minimized entry data :   *NONE
Sequence . . . . . :   87515767
Code . . . . . :   T  - Audit trail entry
Type . . . . . :   CO - Create object

          Entry specific data
Column    *...+....1....+....2....+....3....+....4....+....5
00001     'NGLFPGM011 XXERPPGM  *PGM    RPGLE                '
00051     '                                                  '
00101     '                                                  '
00151     '                                                  '
00201     '                                                  '
00251     '                                                  '
00301     '                                                  '
```

https://www.ibm.com/docs/en/i/7.5?topic=security-reference
Security Reference Guide, Appendix “Layout of audit journal entries” (only for Journal Code = T)

Model files in QSYS (example : QASYCPJ5 for entry type CP)
(only for Journal Code = T)

Fields you may encounter in many entries for Journal Code T

XXETYP	TYPE OF ENTRY	A	1
XXONAM	Object Name	A	10
XXOLIB	Library name	A	10
XXOTYP	Object type	A	8
XXPNM	Path name	A	5000

---

https://www.ibm.com/docs/en/i/7.5?topic=information-journal-entry-finder
Journal entry information finder

Comment lire les postes de journal ?

Découpage intégré de l'image du poste

```
Object . . . . . :                Library  . . . . . :
Member . . . . . :
Incomplete data  . . :   No        Minimized entry data :   *NONE
Sequence . . . . . :   87515767
Code . . . . . :   T  - Audit trail entry
Type . . . . . :   CO - Create object

          Entry specific data
Column    *...+....1....+....2....+....3....+....4....+....5
00001     'NGLFPGM011 XXERPPGM  *PGM    RPGLE                '
00051     '                                                  '
00101     '                                                  '
00151     '                                                  '
00201     '                                                  '
00251     '                                                  '
00301     '
```

OBJLIB	OBJNAME	OBJTYPE	OBJATTRIBUTE	OBJTEXT
QSYS	CPYAUDJRNE	*CMD		Copy Audit Journal Entries
QSYS	DSPAUDJRNE	*CMD		Display Audit Journal Entries
QSYS	DSPJRN	*CMD		Display Journal
QSYS	RCVJRNE	*CMD		Receive Journal Entry
QSYS	RTVJRNE	*CMD		Retrieve Journal Entry

Program Library	Program Name	Object Type	Symbol Name	Symbol Usage
QSYS	QJOURNAL	*SRVPGM	QjoRetrieveJournalEntries	*PROCEXP

ROUTINE_SCHEMA	ROUTINE_NAME	ROUTINE_TYPE	ROUTINE_BODY	EXTERNAL_NAME	EXTERNAL_LANGUAGE
QSYS2	DISPLAY_JOURNAL	FUNCTION	EXTERNAL	QSYS/QDBSSUDF2(QJOJRNTF)	C
QSYS2	DISPLAY_JOURNAL_ENTRY_INFO	PROCEDURE	EXTERNAL	QSYS/QDBSSUDF2(DSPJEI)	C

ROUTINE_SCHEMA	ROUTINE_NAME	ROUTINE_TYPE	ROUTINE_BODY	EXTERNAL_NAME	EXTERNAL_LANGUAGE
SYSTOOLS	AUDIT_JOURNAL_AD	FUNCTION	SQL	SYSTOOLS/AUDIT_AD(AUDIT_JOURNAL_AD_1)	-
SYSTOOLS	AUDIT_JOURNAL_AF	FUNCTION	SQL	SYSTOOLS/AUDIT_AF(AUDIT_JOURNAL_AF_1)	-
SYSTOOLS	AUDIT_JOURNAL_AP	FUNCTION	SQL	SYSTOOLS/AUDIT_AP(AUDIT_JOURNAL_AP_1)	-
SYSTOOLS	AUDIT_JOURNAL_AU	FUNCTION	SQL	SYSTOOLS/AUDIT_AU(AUDIT_JOURNAL_AU_1)	-
SYSTOOLS	AUDIT_JOURNAL_AX	FUNCTION	SQL	SYSTOOLS/AUDIT_AX(AUDIT_JOURNAL_AX_1)	-
SYSTOOLS	AUDIT_JOURNAL_CA	FUNCTION	SQL	SYSTOOLS/AUDIT_CA(AUDIT_JOURNAL_CA_1)	-
SYSTOOLS	AUDIT_JOURNAL_CD	FUNCTION	SQL	SYSTOOLS/AUDIT_CD(AUDIT_JOURNAL_CD_1)	-
SYSTOOLS	AUDIT_JOURNAL_CO	FUNCTION	SQL	SYSTOOLS/AUDIT_CO(AUDIT_JOURNAL_CO_1)	-

Les postes de journal et leurs fonctions SYSTOOLS

7.5 TR4			7.5 TR3			7.4 TR10			7.4 TR9			7.3 TR12		
JOU	ROUTIN	CREATE	JOU	ROUT	CREATED	JOU	ROUT	CREATED	JOU	ROUT	CREATED	JOU	ROU	CREATED
AD	AUDIT_JOU	2024-10-22	AD	AUDIT_JC	17/11/2023	AD	AUDIT_JC	08/02/2024	AD	AUDIT_JC	31/03/2024	AD		
AF	AUDIT_JOU	2024-10-22	AF	AUDIT_JC	17/11/2023	AF	AUDIT_JC	08/02/2024	AF	AUDIT_JC	31/03/2024	AF	AUDIT_	27/09/2022
AP	AUDIT_JOU	2024-10-22	AP	AUDIT_JC	17/11/2023	AP	AUDIT_JC	08/02/2024	AP	AUDIT_JC	31/03/2024	AP		
AU	AUDIT_JOU	2024-10-22	AU	AUDIT_JC	03/05/2024	AU	AUDIT_JC	04/07/2024	AU	AUDIT_JC	08/09/2024	AU		
AX	AUDIT_JOU	2024-10-22	AX	AUDIT_JC	03/05/2024	AX	AUDIT_JC	04/07/2024	AX	AUDIT_JC	08/09/2024	AX		
CA	AUDIT_JOU	2024-10-22	CA	AUDIT_JC	17/11/2023	CA	AUDIT_JC	08/02/2024	CA	AUDIT_JC	31/03/2024	CA	AUDIT_	27/09/2022
CD	AUDIT_JOU	2024-10-22	CD	AUDIT_JC	17/11/2023	CD	AUDIT_JC	08/02/2024	CD	AUDIT_JC	31/03/2024	CD	AUDIT_	27/09/2022
CO	AUDIT_JOU	2024-10-22	CO	AUDIT_JC	17/11/2023	CO	AUDIT_JC	08/02/2024	CO	AUDIT_JC	31/03/2024	CO	AUDIT_	27/09/2022
CP	AUDIT_JOU	2024-10-22	CP	AUDIT_JC	03/05/2024	CP	AUDIT_JC	04/07/2024	CP	AUDIT_JC	08/09/2024	CP	AUDIT_	27/09/2022
DO	AUDIT_JOU	2024-10-22	DO	AUDIT_JC	17/11/2023	DO	AUDIT_JC	08/02/2024	DO	AUDIT_JC	31/03/2024	DO	AUDIT_	27/09/2022
DS	AUDIT_JOU	2024-10-22	DS	AUDIT_JC	17/11/2023	DS	AUDIT_JC	08/02/2024	DS	AUDIT_JC	31/03/2024	DS		
EV	AUDIT_JOU	2024-10-22	EV	AUDIT_JC	03/05/2024	EV	AUDIT_JC	04/07/2024	EV	AUDIT_JC	08/09/2024	EV	AUDIT_	27/09/2022
GR	AUDIT_JOU	2024-10-22	GR	AUDIT_JC	03/05/2024	GR	AUDIT_JC	04/07/2024	GR	AUDIT_JC	08/09/2024	GR	AUDIT_	27/09/2022
IM	AUDIT_JOU	2024-10-22	IM	AUDIT_JC	17/11/2023	IM	AUDIT_JC	08/02/2024	IM	AUDIT_JC	31/03/2024	IM		
JS	AUDIT_JOU	2024-10-22	JS	AUDIT_JC	03/05/2024	JS	AUDIT_JC	04/07/2024	JS	AUDIT_JC	08/09/2024	JS	AUDIT_	27/09/2022
LD	AUDIT_JOU	2024-10-22	LD	AUDIT_JC	17/11/2023	LD	AUDIT_JC	08/02/2024	LD	AUDIT_JC	31/03/2024	LD		
M0	AUDIT_JOU	2024-10-22	M0	AUDIT_JC	17/11/2023	M0	AUDIT_JC	08/02/2024	M0	AUDIT_JC	31/03/2024			
M6	AUDIT_JOU	2024-10-22	M6	AUDIT_JC	17/11/2023	M6	AUDIT_JC	08/02/2024	M6	AUDIT_JC	31/03/2024			
M7	AUDIT_JOU	2024-10-22	M7	AUDIT_JC	17/11/2023	M7	AUDIT_JC	08/02/2024	M7	AUDIT_JC	31/03/2024			
M8	AUDIT_JOU	2024-10-22	M8	AUDIT_JC	17/11/2023	M8	AUDIT_JC	08/02/2024	M8	AUDIT_JC	31/03/2024			
M9	AUDIT_JOU	2024-10-22	M9	AUDIT_JC	17/11/2023	M9	AUDIT_JC	08/02/2024	M9	AUDIT_JC	31/03/2024			
NA	AUDIT_JOU	2024-10-22	NA			NA	AUDIT_JC	04/07/2024	NA	AUDIT_JC	08/09/2024	NA		
OM	AUDIT_JOU	2024-10-22	OM	AUDIT_JC	03/05/2024	OM	AUDIT_JC	04/07/2024	OM	AUDIT_JC	08/09/2024	OM	AUDIT_	27/09/2022
OR	AUDIT_JOU	2024-10-22	OR	AUDIT_JC	17/11/2023	OR	AUDIT_JC	08/02/2024	OR	AUDIT_JC	31/03/2024	OR		
OW	AUDIT_JOU	2024-10-22	OW	AUDIT_JC	17/11/2023	OW	AUDIT_JC	08/02/2024	OW	AUDIT_JC	31/03/2024	OW	AUDIT_	27/09/2022
PA	AUDIT_JOU	2024-10-22	PA	AUDIT_JC	17/11/2023	PA	AUDIT_JC	08/02/2024	PA	AUDIT_JC	31/03/2024	PA		
PF	AUDIT_JOU	2024-10-22	PF	AUDIT_JC	17/11/2023	PF	AUDIT_JC	08/02/2024	PF	AUDIT_JC	31/03/2024	PF		
PG	AUDIT_JOU	2024-10-22	PG	AUDIT_JC	17/11/2023	PG	AUDIT_JC	08/02/2024	PG	AUDIT_JC	31/03/2024	PG		
PS	AUDIT_JOU	2024-10-22	PS			PS	AUDIT_JC	04/07/2024	PS	AUDIT_JC	08/09/2024	PS		
PU	AUDIT_JOU	2024-10-22	PU	AUDIT_JC	17/11/2023	PU	AUDIT_JC	08/02/2024	PU	AUDIT_JC	31/03/2024	PU		
PW	AUDIT_JOU	2024-10-22	PW	AUDIT_JC	17/11/2023	PW	AUDIT_JC	08/02/2024	PW	AUDIT_JC	31/03/2024	PW	AUDIT_	27/09/2022
RA	AUDIT_JOU	2024-10-22	RA	AUDIT_JC	17/11/2023	RA	AUDIT_JC	08/02/2024	RA	AUDIT_JC	31/03/2024	RA		
RO	AUDIT_JOU	2024-10-22	RO	AUDIT_JC	17/11/2023	RO	AUDIT_JC	08/02/2024	RO	AUDIT_JC	31/03/2024	RO		
RZ	AUDIT_JOU	2024-10-22	RZ	AUDIT_JC	17/11/2023	RZ	AUDIT_JC	08/02/2024	RZ	AUDIT_JC	31/03/2024	RZ		
SK	AUDIT_JOU	2024-10-22	SK	AUDIT_JC	17/11/2023	SK	AUDIT_JC	08/02/2024	SK	AUDIT_JC	31/03/2024	SK		
SM	AUDIT_JOU	2024-10-22	SM	AUDIT_JC	17/11/2023	SM	AUDIT_JC	08/02/2024	SM	AUDIT_JC	31/03/2024	SM		
ST	AUDIT_JOU	2024-10-22	ST	AUDIT_JC	17/11/2023	ST	AUDIT_JC	08/02/2024	ST	AUDIT_JC	31/03/2024	ST	AUDIT_	27/09/2022
SV	AUDIT_JOU	2024-10-22	SV	AUDIT_JC	17/11/2023	SV	AUDIT_JC	08/02/2024	SV	AUDIT_JC	31/03/2024	SV	AUDIT_	27/09/2022
ZC	AUDIT_JOU	2024-10-22	ZC	AUDIT_JC	03/05/2024	ZC	AUDIT_JC	04/07/2024	ZC	AUDIT_JC	08/09/2024	ZC		
ZR	AUDIT_JOU	2024-10-22	ZR	AUDIT_JC	17/11/2023	ZR	AUDIT_JC	08/02/2024	ZR	AUDIT_JC	31/03/2024	ZR		

nouvelles entrées apportées par la version 7.5
C3 - Advanced Analysis Command Configuration (TLSCONFIG)
FT - FTP Client Operations
M0 - Db2 Mirror setup tools
M6 - Db2 Mirror communication services
M7 - Db2 Mirror replication services
M8 - Db2 Mirror product services
M9 - Db2 Mirror replication state

entrées de journal QAUDJRN, dont ceux avec fonction SYSTOOLS		
7.3 TR12	79	14
7.4 TR9	86	40
7.4 TR10	86	40
7.5 TR3	86	38
7.5 T4	86	40
7.5 TR5	86	41

Les postes de journal et leurs fonctions SYSTOOLS

Source SYSTOOLS.AUDIT_JOURNAL_AX

```
BEGIN
DECLARE RESULT_SQL_STATEMENT_TEXT VARGRAPHIC ( 5000 ) CCSID 1200 ;
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
FOR AUDIT_CURSOR CURSOR FOR
SELECT
J . ENTRY_TIMESTAMP ,
J . SEQUENCE_NUMBER ,
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
B . * ,
CHAR ( SUBSTR ( J . ENTRY_DATA , 1 , 1 ) , 1 ) AS A_ENTRY_TYPE ,
CHAR ( SUBSTR ( J . ENTRY_DATA , 2 , 1 ) , 1 ) AS A_OPERATION_TYPE ,
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
FROM TABLE ( QSYS2 . DISPLAY_JOURNAL (
'QSYS' ,
'QAUDJRN' ,
JOURNAL_ENTRY_TYPES => 'AX' ,
STARTING_RECEIVER_LIBRARY => STARTING_RECEIVER_LIBRARY ,
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
) ) AS J
LEFT OUTER JOIN QSQAJMRI AS B
ON CONCAT ( 'AX_ET_' , CHAR ( SUBSTR ( J . ENTRY_DATA , 1 , 1 ) , 1 ) ) = B . MSG_KEY
DO
IF A_SQL_STATEMENT_LENGTH > 0 THEN
BEGIN
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
CASE WHEN A_ENTRY_TYPE = 'T' AND A_OPERATION_TYPE = 'A'
THEN CASE A_COLUMN_ACCESS_CONTROL
WHEN 'A' THEN 'ACTIVATE'
WHEN 'D' THEN 'DEACTIVATE'
WHEN ' ' THEN NULL
ELSE A_COLUMN_ACCESS_CONTROL
END
ELSE NULL
END ,
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
) ;
END FOR ;
RETURN ;
END
```

Audit des ouvertures de fichier - Gestion

```
-- maintain repository of sensitive tables to be audited
-- keep the object audit value ni case of rollback
create or replace table rslaud.tables_to_audit as
(select system_table_schema, system_table_name, object_audit initial_object_audit from qsys2.sysfiles
join table(QSYS2.OBJECT_STATISTICS(system_table_schema, '*FILE')) st
on st.objlib = system_table_schema and st.objname = system_table_name and st.objtype = '*FILE'
where system_table_schema = 'ERPFILE' and native_type = 'PHYSICAL' and system_table_name like 'GLF%'
and right(system_table_name, 1) <> '2' )
with data on replace delete rows ;
insert into rslaud.tables_to_audit values('XXERPDATA', 'GLFCLIEN', ' ') ;
merge into rslaud.tables_to_audit
using table(QSYS2.OBJECT_STATISTICS(system_table_schema, '*FILE')) st
on st.objlib = system_table_schema and st.objname = system_table_name and st.objtype = '*FILE' and initial_object_audit = ' '
WHEN MATCHED THEN UPDATE SET initial_object_audit = object_audit ;

select * from rslaud.tables_to_audit  ;
```

System Table Schema	System Table Name	INITIAL_OBJECT_AUDIT
ERPFILE	GLFCLIEN	*ALL
ERPFILE	GLFCUENTA	*ALL
ERPFILE	GLFTRANS	*NONE
XXERPDATA	GLFCLIEN	*CHANGE

```
-- start auditing *ALL
select 'CHGOBJAUD OBJ(' concat system_table_schema concat '/' concat system_table_name concat ') OBJTYPE(*FILE) OBJAUD(*ALL)' command,
qcmdexc('CHGOBJAUD OBJ(' concat system_table_schema concat '/' concat system_table_name concat ') OBJTYPE(*FILE) OBJAUD(*ALL)') command_result
from rslaud.tables_to_audit
join table(QSYS2.OBJECT_STATISTICS(system_table_schema, '*FILE')) st
on st.objlib = system_table_schema and st.objname = system_table_name and st.objtype = '*FILE'
where initial_OBJECT_AUDIT <> '*ALL' ;
```

COMMAND	COMMAND_RESULT
CHGOBJAUD OBJ(ERPFILE/GLFTRANS) OBJTYPE(*FILE) OBJAUD(*ALL)	1
CHGOBJAUD OBJ(XXERPDATA/GLFCLIEN) OBJTYPE(*FILE) OBJAUD(*ALL)	1

Audit des ouvertures de fichier - Analyse

```
-- using QAUDJRN, check for Db2 file usage (starting with 7.5 TR1 7.4 TR7)
create or replace table gm.audit_zczr as
(SELECT entry_timestamp, jrn.user_name, job_name, program_library, program_name, remote_address,
entry_type_detail, access_type_detail, library_name, object_name
FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_ZC (STARTING_RECEIVER_NAME => '*CURCHAIN',
STARTING_TIMESTAMP => current date - 1 days)) jrn
join rslaud.tables_to_audit on library_name = system_table_schema and object_name = system_table_name and object_type = '*FILE'
) with data on replace delete rows;
insert into gm.audit_zczr
(SELECT entry_timestamp, jrn.user_name, job_name, program_library, program_name, remote_address,
entry_type_detail, access_type_detail, library_name, object_name
FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_ZR (STARTING_RECEIVER_NAME => '*CURCHAIN',
STARTING_TIMESTAMP => current date - 1 days)) jrn
join rslaud.tables_to_audit on library_name = system_table_schema and object_name = system_table_name and object_type = '*FILE');
```

```
-- check accesses outside the application
select * from gm.audit_zczr
where program_library not in ('ERPPGM', 'ERPPTF') and not (job_name = 'QZDASSINIT' and remote_address = '123.456.789.1' and user_name = 'ERPSRVUSER')
order by entry_timestamp;
```

ENTRY_TIMESTAMP	USER_NAME	JOB_NAME	PROGRAM_LIBRARY	PROGRAM_NAME	REMOTE_ADDRESS	ENTRY_TYPE_DETAIL	ACCESS_TYPE_DETAIL	LIBRARY_NAME	OBJECT_NAME
2024-10-23 12:05...	GM ...	QPADEV0009	QTEMP ...	QDZTD00001	10.243.2.3	Change of an object	Open	ERPFILE	GLFCLIEN
2024-10-23 12:05...	GM ...	QPADEV0009	QTEMP ...	QDZTD00001	10.243.2.3	Change of an object	Open	ERPFILE	GLFCLIEN
2024-10-23 12:05...	GM ...	QPADEV0009	QSYS ...	QCMD	10.243.2.3	Read of an object	Open	ERPFILE	GLFCLIEN
2024-10-23 12:05...	GM ...	QPADEV0009	ERPPGM...	GLFPGM001E	10.243.2.3	Change of an object	Open	ERPFILE	GLFCLIEN

Audit des modifications de données de fichier

```
-- using database journal, check for all changes
select entry_timestamp, journal_entry_type type, jrn.current_user, job_name, program_name, remote_address,
cast(cast(SUBSTR(entry_data ,1, 200) as char(200) for bit data) as char(200) ccsid 1141) record_image
from table( qsys2.Display_Journal ('ERPFILE','ERPJRN', Journal_Codes => 'R', STARTING_RECEIVER_NAME => '*CURCHAIN',
STARTING_TIMESTAMP => current date - 1 days)) jrn ;

-- using database journal, check for changes made by DFU
select entry_timestamp, journal_entry_type type, jrn.current_user, job_name, program_name, remote_address,
cast(cast(SUBSTR(entry_data ,1, 200) as char(200) for bit data) as char(200) ccsid 1141) record_image
from table( qsys2.Display_Journal ('ERPFILE','ERPJRN', Journal_Codes => 'R', STARTING_RECEIVER_NAME => '*CURCHAIN',
STARTING_TIMESTAMP => current date - 1 days)) jrn
where program_library not in ('ERPPGM', 'ERPPTF') and not (job_name = 'QZDASSINIT' and remote_address = '123.456.789.1' and user_name = 'ERPSRVUSER') ;
```

ENTRY_TIMESTAMP	TYPE	CURRENT_USER	JOB_NAME	PROGRAM_NAME	REMOTE_ADDRESS	RECORD_IMAGE
2024-10-23 12:10:43..	UB	GM ...	QPADEV0009	QDZTD00001	10.243.2.3	00149150000000000002Mr Jaime GONZALES CCCCCN272-227-2234
2024-10-23 12:10:43..	UP	GM ...	QPADEV0009	QDZTD00001	10.243.2.3	00149150000000000002Mr Jaime GONZALES CCCCCY272-227-2234
2024-10-23 12:10:57...	UB	GM ...	QPADEV0009	GLFPGM001E	10.243.2.3	00149150000000000002Mr Jaime GONZALES CCCCCY272-227-2234
2024-10-23 12:10:57...	UP	GM ...	QPADEV0009	GLFPGM001E	10.243.2.3	00149150000000000002Mr Jaime GONZALES CCCCCY272-227-2234

Auditable

SSH SCP/SFTP
Put
Get ...

SSH PASE
cp
mn
rm
chmod ...

User Commands (CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA

SQL Remote

SELECT	DROP
UPDATE	CREATE
INSERT	ALTER
DELETE	GRANT
MERGE	TRUNCATE

...

Triggers
ADDPFTRG
CREATE TRIGGER

FTP Server
FTP Client
Put
Get
Delete
Rename ...

QUERY/400
RUNQRY
WRKQRY
QQQQRY

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

System Commands

UPDDTA	EDTF	INTER
DSPPFM	DSPF	INTER
SAVxxx	RSTxxx	BATCH
CPYxxx	DMPxxx	BATCH

SNDSMTPEMM ...

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

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

SSH
SCP/SFTP
Put
Get …

SSH
PASE
cp
mn
rm
chmod …

User Commands
(CPP)
DBU …

User Programs
*PGM
*PGMSRV
SQL, RLA

SQL Remote

SELECT	DROP
UPDATE	CREATE
INSERT	ALTER
DELETE	GRANT
MERGE	TRUNCATE

…

Triggers
ADDPFTRG
CREATE TRIGGER

FTP Server
FTP Client
Put
Get
Delete
Rename …

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

File Server
NetServer/QSYS.LIB
Open
Rename
Delete …

System Commands

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

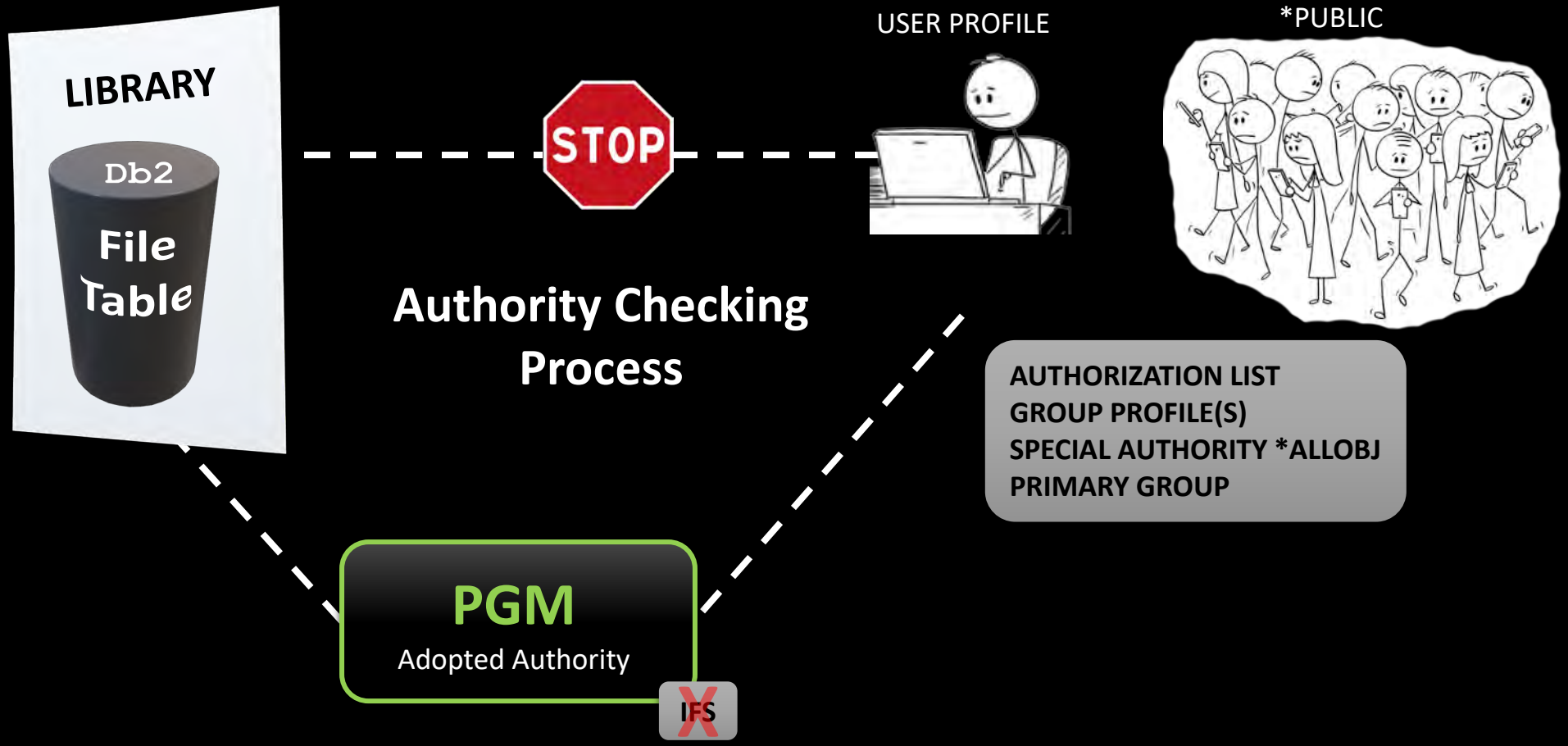
ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

DDM File
Commands (CPYF…)
SQL, RLA

Object Level Security - Fondation de droits statiques

Niveau Objet



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

Triggers
ADDPFTRG
CREATE TRIGGER

QUERY/400
RUNQRY
WRKQRY
QQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

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

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

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

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

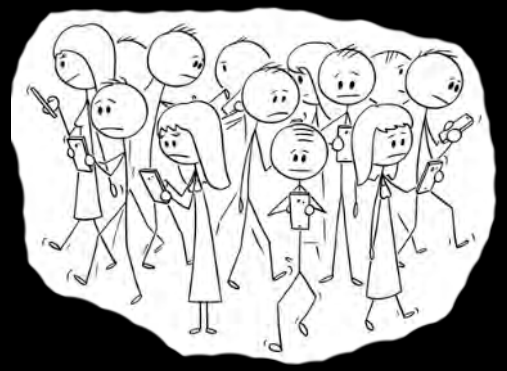
Function Usage – Droits d'accès contextuels basiques

Niveau Protocole

Protocole - Fonction
Navigator for i
FTP
Database Server
DDM - DRDA
…

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

Fonctions d’usage en action

User Name	Usage	User Type	Default Usage	Allobj Indicator	Function ID	Function Name Message Text
EPIADM	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
GM	ALLOWED	GROUP	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
GM_BASICLM	DENIED	USER	ALLOWED	USED	QIBM_DB_ZDA	Toolbox Application Server Access
GRP_EXPLT	ALLOWED	GROUP	DENIED	USED	QIBM_ACCESS_ALLOBJ_JOBLOG	Access job log of *ALLOBJ job
JPLTOOLS	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SQLADM	Database Administrator
JPLTOOLS	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
QDIRSRV	ALLOWED	USER	DENIED	USED	QIBM_QSY_SYSTEM_CERT_STORE	*SYSTEM certificate store
QOBJC	ALLOWED	USER	DENIED	USED	QIBM_QSY_SYSTEM_CERT_STORE	*SYSTEM certificate store
QTCP	ALLOWED	USER	DENIED	USED	QIBM_QSY_SYSTEM_CERT_STORE	*SYSTEM certificate store
QYPSJSVR	ALLOWED	USER	DENIED	USED	QIBM_QSY_SYSTEM_CERT_STORE	*SYSTEM certificate store

```sql
-- list functions default values and usages
select us.user_name, us.usage, user_type, default_usage, allobj_indicator, us.function_id, FUNCTION_NAME_MESSAGE_TEXT
FROM QSYS2.FUNCTION_USAGE us join QSYS2.FUNCTION_INFO fu on us.function_id = fu.function_id
order by us.user_name;

-- add ADMIN group to QIBM_Q1A* (BRMS) if default = DENIED
SELECT fu.function_id, default_usage, allobj_indicator,
'CHGFCNUSG USER(GRP_ADMIN) USAGE(*ALLOWED) FCNID(' concat fu.function_id concat ')' command,
qcmdexc('CHGFCNUSG USER(GRP_ADMIN) USAGE(*ALLOWED) FCNID(' concat fu.function_id concat ')') cmd_result
FROM QSYS2.FUNCTION_INFO fu
where fu.function_id like 'QIBM_Q1A%' and default_usage = 'DENIED'
ORDER BY fu.function_id ;

-- grant GRP_EXPLT to QIBM_ACCESS_ALLOBJ_JOBLOG
SELECT authorization_name,
'CHGFCNUSG USER(' concat authorization_name concat ') USAGE(*ALLOWED) FCNID(QIBM_ACCESS_ALLOBJ_JOBLOG)' command,
qcmdexc('CHGFCNUSG USER(' concat authorization_name concat ') USAGE(*ALLOWED) FCNID(QIBM_ACCESS_ALLOBJ_JOBLOG)') cmd_result
FROM qsys2.user_info up where authorization_name in ('GRP_EXPLT') ;
```

Authorization Name	COMMAND	CMD_RESULT
GRP_EXPLT	CHGFCNUSG USER(GRP_EXPLT) USAGE(*ALLOWED) FCNID(QIBM_ACCESS_ALLOBJ_JOBLOG)	1

Fonctions d'usage en action

```
C:\Users\GUY>ftp 172.168.2.50
Connecté à 172.168.2.50.
220-QTCP at AMIE75.RIT.LOCAL.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
Utilisateur (172.168.2.50:(none)) : gm_basic
331 Enter password.
Mot de passe :

530 Log on attempt by user GM_BASIC rejected.
Échec de l'identification.
ftp>
```

```
-- monitor USAGE FAILURES
select jrn.ENTRY_TIMESTAMP, function_registration_operation, qualified_job_name, user_name, program_name,
user_profile_name, function_name
 from table(SYSTOOLS.AUDIT_JOURNAL_GR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
 where entry_type = 'F' and function_registration_operation = 'USAGE FAILURE' ;
```

ENTRY_TIMESTAMP	FUNCTION_REGISTRATION_OPERATION	QUALIFIED_JOB_NAME	USER_NAME	PROGRAM_NAME	USER_PROFILE_NAME	FUNCTION_NAME
2024-10-23 15:25...	USAGE FAILURE	816199/QTCP/QTFTP00022	QTCP	QTMFSRVR	GM_BASIC	QIBM_QTMF_SERVER_REQ_0
2024-10-23 15:25...	USAGE FAILURE	816199/QTCP/QTFTP00022	QTCP	QTMFSRVR	GM_BASIC	QIBM_QTMF_SERVER_REQ_10
2024-10-23 15:26...	USAGE FAILURE	819823/QUSER/QZRCSRVS	GM_BASIC	QZRCSRVS	GM_BASIC	QIBM_NAV_ALL_FUNCTION
2024-10-23 15:31...	USAGE FAILURE	819615/QUSER/QZDASOINIT	GM_BASICLM	QZDASOINIT	GM_BASICLM	QIBM_DB_ZDA
2024-10-23 15:38...	USAGE FAILURE	819830/QSECOFR/QPADEV000B	QSECOFR	QCMD	QSECOFR	QIBM_DB_SECADM


```
[ 23/10/2024 à 15:31:11 ]  Connexion à la base de données...
 Etat SQL : 08S01
Code fournisseur : -99999
Message : Communication link failure. (Connection was dropped unexpectedly.)
```

```
-- monitor JOBLOG ACCESS FAILURES
SELECT jrn.ENTRY_TIMESTAMP, qualified_job_name, program_name, user_name,
jrn.VIOLATION_TYPE_DETAIL, jrn.USER_PROFILE_NAME, jrn.OBJECT_NAME, jrn.OBJECT_TYPE
FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_AF (STARTING_RECEIVER_NAME => '*CURCHAIN',
STARTING_TIMESTAMP => current date - 1 days)) jrn
where jrn.VIOLATION_TYPE = 'K' and object_name = 'DSPJOBLOG';
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	PROGRAM_NAME	USER_NAME	VIOLATION_TYPE_DETAIL	USER_PROFILE_NAME	OBJECT_NAME	OBJECT_TYPE
2024-10-23 15:23:...	819783/GM_BASIC/QPADEV000B	QCMD ...	GM_BASIC	Special authority violation	GM_BASIC	DSPJOBLOG	*CMD

```
                    Enter SQL Statements

Type SQL statement, press Enter.
  >

     create permission gm.gm_authorized_only on gm.testsec for rows
     where user = 'GM'
     enforced for all access enable
     Not authorized to CREATE PERMISSION.
===>
```

```
Parameters or command
===> dspjoblog 815928/EPI/MONDIAQ
F3=Exit    F5=Refresh        F7=Find
F11=Display elapsed data     F12=Canc
Not authorized to display job log.
```

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

Triggers
ADDPFTRG
CREATE TRIGGER

QUERY/400
RUNQRY
WRKQRY
QQQQRY

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 ...

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

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

IBM i

RCAC/Row - Droits d'accès par Rang

```
-- setup RCAC permissions
create permission erpfile.company_protection on erpfile.glfclien for rows
where (clicomp = '001' and verify_group_for_user(current_user, 'WGRP001') = 1) or
(clicomp = '002' and verify_group_for_user(current_user, 'WGRP002') = 1) or
(clicomp = '003' and verify_group_for_user(current_user, 'WGRP003') = 1) or
(verify_group_for_user(current_user, 'WGRPALL') = 1)
enforced for all access enable ;

alter table erpfile.glfclien activate row access control ;
```

COMPANY ID	Client ID	Client Name	Client Type	Client Status	Taxe Id	Adress 1	Adress 2	Adress 3
001	4915000000000002	Mr Jaime GONZALES	CCCCC	N	272-227-2234	NORTE 15	test 4	EGYPT
001	4915310000000011	Christopher Wang	CCCCC	N	4804554448	Ocean Drive	SOUTH AFRICA	Pretoria
001	5915000000000001	John Ford (Sr.)	CCCCC	Y	913-073-4574	Lambert Walk	Saint Louis	MISOURI
002	4915000000000001	Petros CHRISTOFIDES	EEEEE	Y	275-073-6190	Avenue Petros	LEFKOSIA	CYPRUS
002	4915310000000002	Basel HASSAN	4RSBB	X	888888220000-2	Avenue Jacques Cartie	DUBAI	EMIRATES
003	101245894317825	JOHN Watson	BBBBB	X	VAT-118	Downing Street	PRETORIA	SOUTH AFRICA
003	1234567890000001	Pascal Tarloucellowitch	CCCCC	Y	172-227-2234	NORTE 15	Saint-Etienne	FRANCE
003	1234567890123456	Rastapopoulos	CCCCC	N	233-073-6290	RICHELIEU	Maputo	MOZAMBIQUE
003	5900100010101011	Jean DURAND	GOOD	Y	12345678	Avenue ONTARIO	Perth	AUSTRALIA
003	6078787878787878	Ekaterina RAWITZ	BBBBB	Y	BBBB4	Mining Avenue	KRAKOW	POLAND

- Mécanisme "silencieux" et indépendant des interfaces (clause WHERE implicite)
- Rejeté par défaut (condition 0=1)
- Couvre toute opération au niveau rang (read, update, delete, insert)
- Intervient après object level security
- Permet de présenter un fichier "vide" à un utilisateur *ALLOBJ
- Verrouillage exclusif requis pour *alter table*

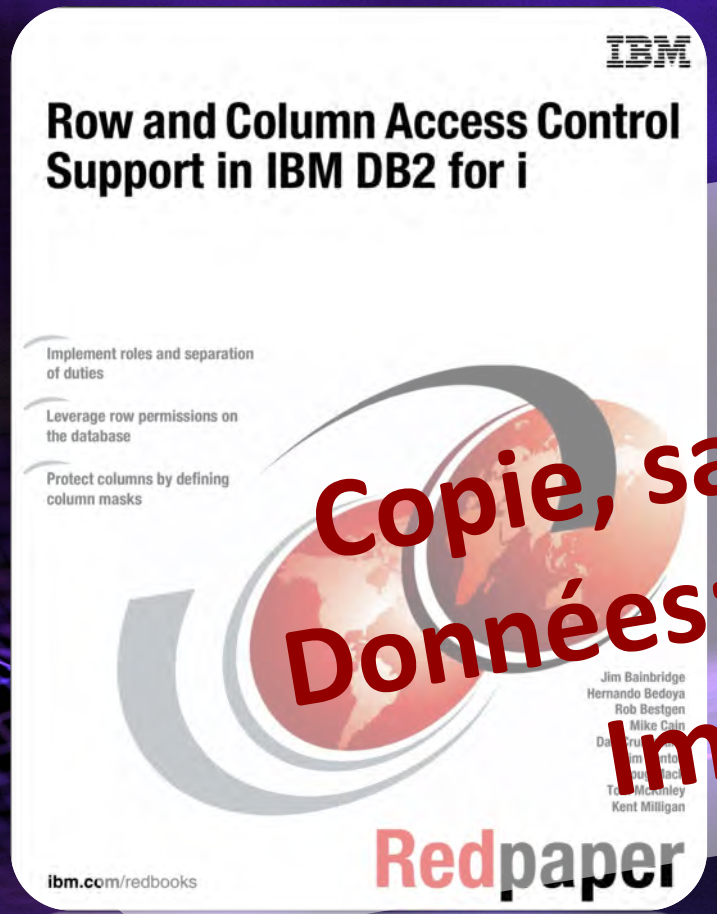
RCAC/Column - Masquage d'une colonne

```
-- setup RCAC masks
create mask erpfile.taxid_masked on erpfile.glfclien for column clitaxid return
case when verify_group_for_user(current_user, 'WGRPALL') = 1 or
clidir2 = 'Saint-Etienne' then clitaxid
else '******************************'
end
enable ;

alter table erpfile.glfclien activate column access control ;
```

COMPANY ID	Client ID	Client Name	Client Type	Client Status	Taxe Id	Adress 1	Adress 2	Adress 3
003	101245894317825	JOHN Watson	BBBBB	X	**********	Downing Street	PRETORIA	SOUTH AFRICA
003	1234567890000001	Pascal Tarloucellowitch	CCCCC	Y	172-227-2234	NORTE 15	Saint-Etienne	FRANCE
003	1234567890123456	Rastapopoulos	CCCCC	N	**********	RICHELIEU	Maputo	MOZAMBIQUE
003	5900100010101011	Jean DURAND	GOOD	Y	**********	Avenue ONTARIO	Perth	AUSTRALIA
003	6078787878787878	Ekaterina RAWITZ	BBBBB	Y	**********	Mining Avenue	KRAKOW	POLAND

- GRATUIT !
- Assez facile à implementer sur des tables bien ciblées
- Mécanisme "silencieux" et indépendant des interfaces (clause WHERE implicite)
- Verrouillage exclusif requis pour *alter table*

RCAC – Ressources



Session iUG 2021

Retour Expérience Eddie Chaffin

Implementation RCAC en environnement M3 multi-sociétés

(En collaboration avec Infor et Kent Milligan IBM Lab Services)

i-UG (UK)

Présentation VOLUBIS 2015

GAIA VOLUBIS

VIGILANCE

Copie, sauvegarde, restauration

Données: Mises à jour, agrégation

Impact performances

RCAC – Sécurité périphérique

Permission, Mask, Alter table

- Inscription dans QIBM_DB_SECADM
- Pas de droit requis sur la table et sa bibliothèque
- Même QSECOFR doit être inscrit !

```
Code fournisseur : -552
Message : [SQL0552] Not authorized to CREATE PERMISSION. Cause . . . . . :   The operation cannot be performed without the required authority. -- CREATE TABLE requires *USE authority to the CRTPF command.
-- CREATE VIEW or CREATE INDEX requires *USE authority to the CRTLF command. -- CREATE ALIAS requires *USE authority to the CRTDDMF command. -- CREATE SCHEMA requires *USE authority to the CRTLIB command.
-- ALTER TABLE requires *USE authority to the ADDPFCST command in order to add constraints, and *USE authority to the RMVPFCST command in order to drop constraints. -- ALTER TRIGGER requires *USE authority
to the CHGPFTRG command. -- CREATE PROCEDURE or CREATE FUNCTION requires *OBJOPR and *ADD authority to the catalog table SYSROUTINES in QSYS2. -- DROP PROCEDURE or DROP FUNCTION requires *OBJOPR and *DLT
authority to the catalog table SYSPARMS in QSYS2. -- CREATE TYPE requires *OBJOPR and *ADD authority to the catalog table SYSTYPES in QSYS2. -- DROP TYPE requires *OBJOPR and *DLT authority to the catalog
table SYSTYPES in QSYS2. -- CREATE TRIGGER requires *USE authority to the ADDPFTRG command. -- DROP TRIGGER requires *USE authority to the RMVPFTRG command. -- CREATE SEQUENCE requires *USE authority to the
CRTDTAARA command. -- DROP SEQUENCE requires *USE authority to the DLTDTAARA command. -- ALTER SEQUENCE requires *USE authority to the RTVDTAARA and CRTDTAARA commands. -- The COMMENT ON statements for
procedures, functions, types, triggers and sequences require *OBJOPR, *READ, and *UPD authority to the catalog table associated with the object. -- SET SESSION AUTHORIZATION requires that the authorization
ID associated with the statement has *ALLOBJ special authority. -- SET CURRENT DEGREE and the QSYS2/RESET_ENVIRONMENTAL_LIMITS procedure require that the authorization ID associated with the statement has
*JOBCTL special authority or be authorized to the QIBM_DB_SQLADM function.  -- CREATE, ALTER, DROP, LABEL ON and COMMENT ON of a MASK or PERMISSION requires that the authorization ID associated with the
statement be authorized to the QIBM_DB_SECADM function.  The same authorization is required to RENAME, DROP or delete an object that is referenced by a mask or permission and to CREATE, DROP, or ALTER a
secure TRIGGER or FUNCTION. Recovery . . . :   Obtain authority from the security officer and try the operation again. Authorization to the QIBM_DB_SQLADM and QIBM_DB_SECADM functions can be handled by
Application Administration in System i Navigator.  The Change Function Usage (CHGFCNUSG) command can also be used to allow or deny use of a function. For example: CHGFCNUSG FCNID(QIBM_DB_SQLADM)
USER(xxxxx) USAGE(*ALLOWED).
```

Administrer QIBM_DB_SECADM

- *SECADM requis - donc *ALLOBJ suffit
  élévation(s) de privilèges possible
- Default authority à *DENIED non modifiable

```
                          Display Function Usage

Function ID  . . . . . :   QIBM_DB_SECURITY_ADMINISTRATOR
Function name  . . . . :   Database Security Administrator Functions
Description  . . . . . :   Database Security Administrator Functions
Product  . . . . . . . :   QIBM_BASE_OPERATING_SYSTEM
Group  . . . . . . . . :   QIBM_DB

Default authority  . . . . . . . . . . . . . :   *DENIED
*ALLOBJ special authority  . . . . . . . . . :   *NOTUSED

User         Type          Usage      User         Type          Usage
EPIADM       User          *ALLOWED
GM           Group         *ALLOWED
GM_ALLOBJ    User          *ALLOWED
GM_BASIC     User          *ALLOWED
JPLTOOLS     User          *ALLOWED
```

QIBM_DB_SECADM permet de :

- Administrer authority collection
- Administrer RCAC
- Administrer droits QSYS.LIB ((droits privés, publics, autl, propriétaire) - excepté droit privé pour lui-même

Lister config RCAC

- Aucun droit requis !!!!!!

```
-- list existing RCAC controls & dependancies
select * from qsys2.syscontrols ;
select * from qsys2.syscontrolsdep ;
```

Vigilance élevée

RCAC – Audit QIBM_DB_SECADM

```sql
-- who is authorized to manipulate RCAC functions?
select us.user_name, us.usage, user_type, default_usage, allobj_indicator, us.function_id, FUNCTION_NAME_MESSAGE_TEXT
FROM QSYS2.FUNCTION_USAGE us join QSYS2.FUNCTION_INFO fu on us.function_id = fu.function_id
where us.function_id = 'QIBM_DB_SECADM'
order by us.user_name;
```

User Name	Usage	User Type	Default Usage	Allobj Indicator	Function ID	Function Name Message Text
EPIADM	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
GM	ALLOWED	GROUP	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
GM_ALLOBJ	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
GM_BASIC	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator
JPLTOOLS	ALLOWED	USER	DENIED	NOT USED	QIBM_DB_SECADM	Database Security Administrator

```sql
-- monitor changes in function QIBM_DB_SECADM
select jrn.ENTRY_TIMESTAMP, qualified_job_name, user_name, program_name, jrn.function_registration_operation, jrn.function_name,
jrn.usage_setting, jrn.user_profile_name, jrn.previous_usage, jrn.function_allobj, jrn.previous_allobj
 from table(SYSTOOLS.AUDIT_JOURNAL_GR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
 where entry_type = 'F' and function_name = 'QIBM_DB_SECADM';
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	PROGRAM_NAME	FUNCTION_REGISTRATION_OPERATION	FUNCTION_NAME	USAGE_SETTING	USER_PROFILE_NAME	PREVIOUS_USAGE
2024-11-04 15...	830499/QUSER/QZDASOINIT	GM_BASIC	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM_BASIC	-
2024-11-04 15...	830499/QUSER/QZDASOINIT	GM_BASIC	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM_BASIC	-
2024-11-04 15...	830499/QUSER/QZDASOINIT	GM_BASIC	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM_BASIC	-
2024-11-04 15...	830499/QUSER/QZDASOINIT	GM_BASIC	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM_BASIC	-
2024-11-04 15...	830499/QUSER/QZDASOINIT	GM_BASIC	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM_BASIC	-
2024-11-04 15...	831301/GM/QPADEV0005	GM	QCMD	CHANGE USAGE	QIBM_DB_SECADM	REMOVED	GM_BASIC	ALLOWED
2024-11-04 15...	831311/QSECOFR/QPADEV0006	QSECOFR	QCMD	USAGE FAILURE	QIBM_DB_SECADM	-	QSECOFR	-
2024-11-04 15...	831314/GM/QINTER	GM	QCMD	CHANGE USAGE	QIBM_DB_SECADM	ALLOWED	GM_ALLOBJ	UNKNOWN
2024-11-04 15...	831301/GM/QPADEV0005	GM	QCMD	CHANGE USAGE	QIBM_DB_SECADM	ALLOWED	GM_BASIC	UNKNOWN
2024-11-04 22...	830500/QUSER/QZDASOINIT	GM	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM	-
2024-11-04 22...	830500/QUSER/QZDASOINIT	GM	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM	-
2024-11-04 22...	830500/QUSER/QZDASOINIT	GM	QZDASOINIT	CHECK USAGE	QIBM_DB_SECADM	-	GM	-

RCAC – Audit fonctions RCAC

```
-- monitor changes in RCAC (QAUDJRN)
select jrn.ENTRY_TIMESTAMP, qualified_job_name, user_name, program_name, jrn.entry_type, jrn.entry_type_detail, jrn.operation_type,
jrn.library_name, jrn.file_name, jrn.mask_name, jrn.column_name, jrn.permission_name, jrn.enabled, jrn.row_access_control,
jrn.column_access_control, jrn.prev_enabled, jrn.prev_row_access_control, jrn.prev_column_access_control, jrn.sql_statement_text
 from table(SYSTOOLS.AUDIT_JOURNAL_AX (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn ;
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	PROGRAM_NAME	ENTRY _TYPE	ENTRY_TYPE_DETAIL	OPERATION _TYPE	LIBRARY _NAME	FILE_NAME	MASK_NAME	COLUMN_NAME	PERMISSION_NAME	ENABLED	ROW_ACCESS _CONTROL	COLUMN_ACCESS _CONTROL
2024-11-04 14...	831301/GM/QPADEV0005	GM	QMNCPYL	T	Table	ALTER	ERPFILT	GLFCLIEN	-	-	-	-	ACTIVATE	ACTIVATE
2024-11-04 14...	831301/GM/QPADEV0005	GM	QMNCPYL	P	Row permission	CREATE	ERPFILT	GLFCLIEN	-	-	QIBM_DEFAULT_GLFCLIE...	YES	-	-
2024-11-04 14...	831301/GM/QPADEV0005	GM	QMNCPYL	T	Table	INTERNAL	ERPFILT	GLFCLIEN	-	-	-	-	-	-
2024-11-04 14...	831301/GM/QPADEV0005	GM	QMNCPYL	T	Table	INTERNAL	ERPFILE	GLFCLIEN	-	-	-	-	-	-
2024-11-04 14...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	P	Row permission	DROP	ERPFILE	GLFCLIEN	-	-	COMPANY_PROTECTION	-	-	-
2024-11-04 14...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	P	Row permission	CREATE	ERPFILE	GLFCLIEN	-	-	COMPANY_PROTECTION	YES	-	-
2024-11-04 14...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	P	Row permission	DROP	ERPFILT	GLFCLIEN	-	-	COMPANY_PROTECTION	-	-	-
2024-11-04 15...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	P	Row permission	CREATE	ERPFILT	GLFCLIEN	-	-	COMPANY_PROTECTION	YES	-	-
2024-11-04 15...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	T	Table	ALTER	ERPFILT	GLFCLIEN	-	-	-	-	ACTIVATE	-
2024-11-04 15...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	M	Column mask	DROP	ERPFILT	GLFCLIEN	TAXID_MASKED	-	-	-	-	-
2024-11-04 15...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	M	Column mask	CREATE	ERPFILT	GLFCLIEN	TAXID_MASKED	CLITAXID	-	YES	-	-
2024-11-04 15...	830499/QUSER/QZDASO...	GM_BASIC	QZDASOINIT	T	Table	ALTER	ERPFILT	GLFCLIEN	-	-	-	-	-	ACTIVATE

```
-- monitor changes in RCAC (Db2 journal)
select jrn.ENTRY_TIMESTAMP, user_name, program_name, journal_entry_type, INTERPRET(SUBSTR(ENTRY_DATA , 1 , 20 ) AS char(20) ) AS entry_data_detail
from table(display_journal ('ERPFILE', 'ERPJRN', STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
 where journal_code = 'D' ;
```

ENTRY_TIMESTAMP	USER_NAME	PROGRAM_NAME	JOURNAL_ENTRY _TYPE	ENTRY_DATA_DETAIL
2024-11-04 14...	GM_BASIC	QZDASOINIT	P2	GLFCLIEN ERPFILE
2024-11-04 14...	GM_BASIC	QZDASOINIT	P1	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	P2	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	P1	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	CG	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	M2	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	M1	GLFCLIEN ERPFILE
2024-11-04 22...	GM	QZDASOINIT	CG	GLFCLIEN ERPFILE

Journal Cod	Entry type	Description
D	CG	Change file
D	M1	Create Mask
D	M2	Drop Mask
D	M3	Alter Mask
D	P1	Create Permission
D	P2	Drop Permission
D	P3	Alter Permission

RCAC – Journaux base de données !!!!!!

```sql
-- who can view Db2 journal entries on a file with RCAC active?
select jrn.ENTRY_TIMESTAMP, user_name, program_name, INTERPRET(SUBSTR(ENTRY_DATA , 1 , 200 ) AS char(200) ) AS entry_data_detail
from table(display_journal ('ERPFILE', 'ERPJRN', STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
where journal_code = 'R' and journal_entry_type = 'UP';
```

ENTRY_TIMESTAMP	USER_NAME	PROGRAM_NAME	ENTRY_DATA_DETAIL
2024-11-04 22:...	WUSRALL	QDZTD00001	0014915000000000002Mr Jaime GONZALES CCCCCY272-227-2234
2024-11-04 22:...	WUSRALL	QDZTD00001	0014915310000000011Christopher Wang CCCCCY4884554448
2024-11-04 22:...	WUSRALL	QDZTD00001	0015915000000000001John Ford (Sr.) CCCCCN913-073-4574
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED
2024-11-04 22:...	WUSRALL	QDZTD00001	NOT AUTHORIZED

Terminé : 10 lignes extraites

Messages | Environnement | select jrn.ENTRY_TIMESTAMP, user_name, program_name, INTERPRET(SUBSTR(ENTRY_DATA , 1 , 200) AS char..

Job: 830500/QUSER/QZDASOINIT JDBC Configuration: Default User: WUSR001

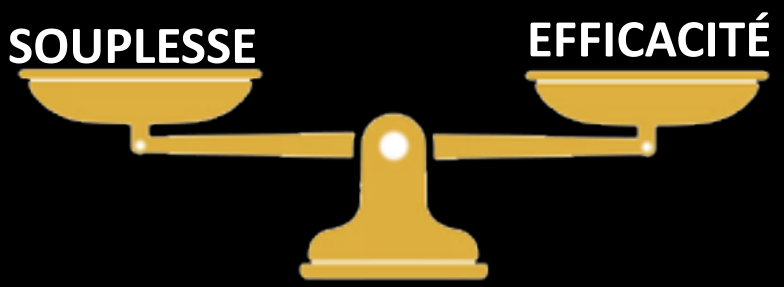
```
DSPJRN JRN(ERPFILE/ERPJRN) RCVRNG(*CURCHAIN) ENTTYP(UP)
```

```
                         Display Journal Entry

Object . . . . . . . :   GLFCLIEN        Library . . . . . . :   ERPFILE
Member . . . . . . . :   GLFCLIEN
Incomplete data  . . :   No              Minimized entry data :   *NONE
Sequence . . . . . . :   80
Code . . . . . . . . :   R  - Operation on specific record
Type . . . . . . . . :   UP - Update, after-image

             Entry specific data
Column       *...+....1....+....2....+....3....+....4....+....5
00001       '003101245894317825 JOHN Watson                    '
00051       '                  BBBBBZVAT-118                   '
00101       '     Downing Street               PRETORIA        '
00151       '          SOUTH AFRICA                       14356'
00201       '6         1234567890          1445784519          '
00251       '     YEUR'
```

Redpaper

Important: RCAC is applied to the table or physical file access. It is not applied to the journal receiver access. Any and all database transactions are represented in the journal regardless of RCAC row permissions and column masks. This makes it essential that IBM i security is used to ensure that only authorized personnel have access to the journaled data.

RCAC – Triggers & Fonctions !!!!!!



TRIGGERS associés à un fichier sous contrôle RCAC

- Option “SECURED” requise (manipulations autorisées pour des utilisateurs inscrits dans QIBM_DB_SECADM)
- Accède aux colonnes masquées

FONCTIONS utilisées dans une permission RCAC

- Option “SECURED” requise (manipulations autorisées pour des utilisateurs inscrits dans QIBM_DB_SECADM)
- Option “NO EXTERNAL ACTION” requise (actions hors Db2 interdites)
- Accède à tous les rangs et toutes les colonnes

VIGILANCE

Doivent faire l’objet de contrôles drastiques (revue de code, mise en production, manipulations, etc…)

```
-- review secured functions & triggers
select * from qsys2.sysroutines where secure = 'Y'
select * from qsys2.systriggers where secure = 'Y'
```

Protégeable
RCAC

SSH
SCP/SFTP
Put
Get ...

SSH
PASE
cp
mn
rm
chmod ...

User Commands
(CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA

SQL Remote

SELECT	DROP
UPDATE	CREATE
INSERT	ALTER
DELETE	GRANT
MERGE	TRUNCATE

...

Triggers
ADDPFTRG
CREATE TRIGGER

FTP Server
FTP Client
Put
Get
Delete
Rename ...

QUERY/400
RUNQRY
WRKQRY
QQQQRY

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

System Commands

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

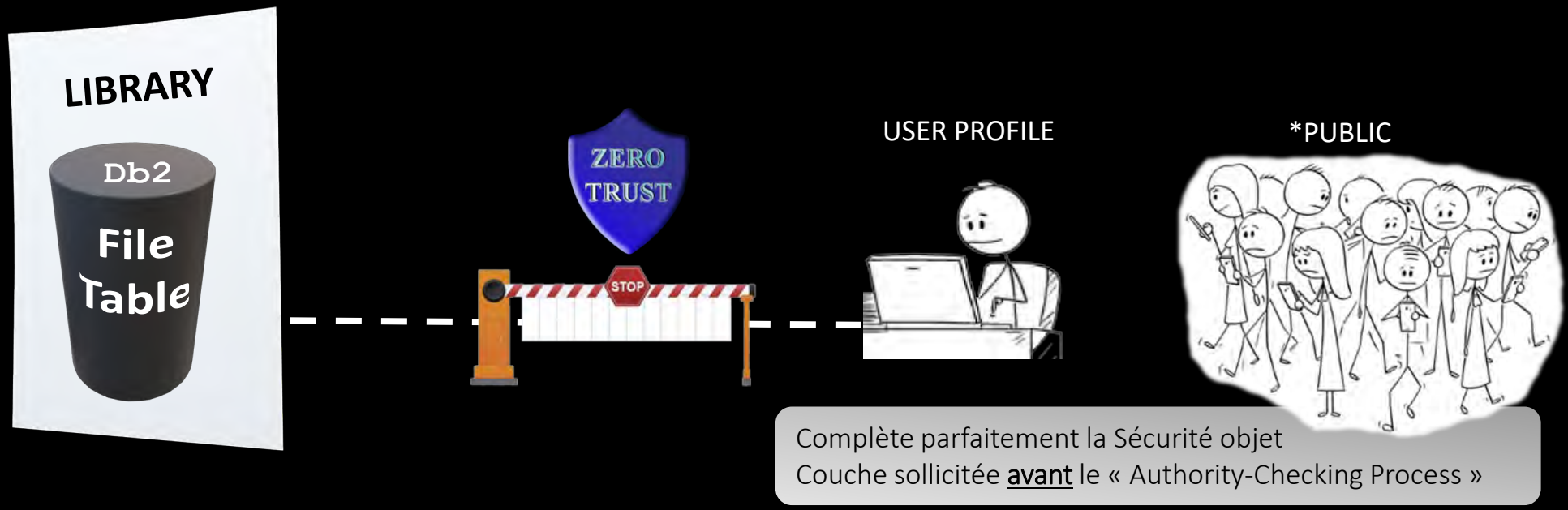
ObjectConnect
SAVRSTxxx

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

SSH SCP/SFTP
Put
Get ...

SSH PASE
cp
mn
rm
chmod ...

User Commands (CPP)
DBU ...

User Programs
*PGM
*PGMSRV
SQL, RLA

SQL Remote

SELECT	DROP
UPDATE	CREATE
INSERT	ALTER
DELETE	GRANT
MERGE	TRUNCATE

...

Triggers
ADDPFTRG
CREATE TRIGGER

QUERY/400
RUNQRY
WRKQRY
QQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

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

System Commands

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

ObjectConnect
SAVRSTxxx

Commands & Pgms
SQL Execution
RUNSQL
RUNSQLSTM
STRSQL
STRQMQRY
QSQPRCED

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

IBM i

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

Triggers
ADDPFTRG
CREATE TRIGGER

QUERY/400
RUNQRY
WRKQRY
QQQQQRY

FTP Server
FTP Client
Put
Get
Delete
Rename ...

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

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

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
…

Eléments de réflexion :

- Nombreuses vulnérabilités découvertes depuis 2022 et qui existent depuis toujours dans notre OS préféré….. (27 CVE avec score > 7 en 2023 et 29 en 2024 !)
- 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)
- Contexte géopolitique tendu …

Contrôle d’accès « contextuel » le plus poussé

Exit points – Premières observations sur Mapepire

Technology preview

Connexion depuis Client js vers Serveur Mapepire sur IBM i

```
                          Historique du travail
                                                        Système . . :   ITEST9
Travail . :   QZDASOINIT    Utilisateur: QUSER        Numéro . . . :   218858

  Travail 218858/QUSER/QZDASOINIT démarré le 31/10/24 à 10:55:07 dans le
    sous-système QUSRWRK de QSYS ; soumis le 31/10/24 à 10:55:07.
  ACGDTA pour 218858/QUSER/QZDASOINIT non journalisé. Code raison . . : 1.
  Imprimante PRT01 non trouvée.
  Erreurs dans la commande CHGJOB pour le travail 218858/QUSER/QZDASOINIT.
  Imprimante PRT01 non trouvée.
  ACGDTA pour 218858/QUSER/QZDASOINIT non journalisé. Code raison . . : 1.
  Le travail a été modifié ; cependant, des erreurs se sont produites.
  User GDUMAS from client 127.0.0.1 connected to server.
  Imprimante PRT01 non trouvée.
  Le travail a été modifié ; cependant, des erreurs se sont produites.
  Les registres spéciaux suivants ont été définis . : CLIENT_ACCTNG: location:
    file:/QOpenSys/pkgs/lib/mapepire/mapepire-server.jar, CLIENT_APPLNAME:
    Node.js client, CLIENT_PROGRAMID: VSCode connector | Version 2.1.2,
   CLIENT_USERID: gdumas, CLIENT_WRKSTNNAME: localhost
```

Connexion depuis Client VSCode Python Jupiter vers Serveur Mapepire sur IBM i

```
                          Historique du travail
                                                        Système . . :   ITEST9
Travail . :   QZDASOINIT    Utilisateur: QUSER        Numéro . . . :   217794

  Travail 217794/QUSER/QZDASOINIT démarré le 28/10/24 à 09:35:25 dans le
    sous-système QUSRWRK de QSYS ; soumis le 28/10/24 à 09:35:25.
  ACGDTA pour 217794/QUSER/QZDASOINIT non journalisé. Code raison . . : 1.
  Imprimante PRT01 non trouvée.
  Erreurs dans la commande CHGJOB pour le travail 217794/QUSER/QZDASOINIT.
  Imprimante PRT01 non trouvée.
  ACGDTA pour 217794/QUSER/QZDASOINIT non journalisé. Code raison . . : 1.
  Le travail a été modifié ; cependant, des erreurs se sont produites.
  User GDUMAS from client 127.0.0.1 connected to server.
  Imprimante PRT01 non trouvée.
  Le travail a été modifié ; cependant, des erreurs se sont produites.
  Les registres spéciaux suivants ont été définis . : CLIENT_ACCTNG: location:
    file:/home/GDUMAS/.vscode/mapepire-server-2.1.4.jar, CLIENT_APPLNAME:
    vscode-db2i 1.6.1-dev, CLIENT_PROGRAMID: VSCode connector | Version
    2.1.4, CLIENT_USERID: gdumas, CLIENT_WRKSTNNAME: 172.30.9.55
```

S29 – MAPEPIRE : le nouveau client pour se connecter à l'IBM i

Session : Demain 10h15

Gautier Dumas – CFD-Innovation

Dans cette session, nous explorerons Mapepire, la nouvelle couche d'accès à la base de données actuellement en Technology Preview.

Mapepire a été conçu pour faciliter le développement d'applications modernes utilisant .NET Core, Node.js, PHP et autres pour l'utilisation de Db2 for i.

En termes simples : les clients Mapepire peuvent être déployés n'importe où ! Et pourraient remplacer les prérequis JDBC ou ODBC.

- Points d'exit QIBM_QZDA_* opérationnels
- IP du poste client = 127.0.0.1 (registre client_wrkstnname ???)
- Pas d'information claire sur l'utilisation de Mapepire

guy marmorat

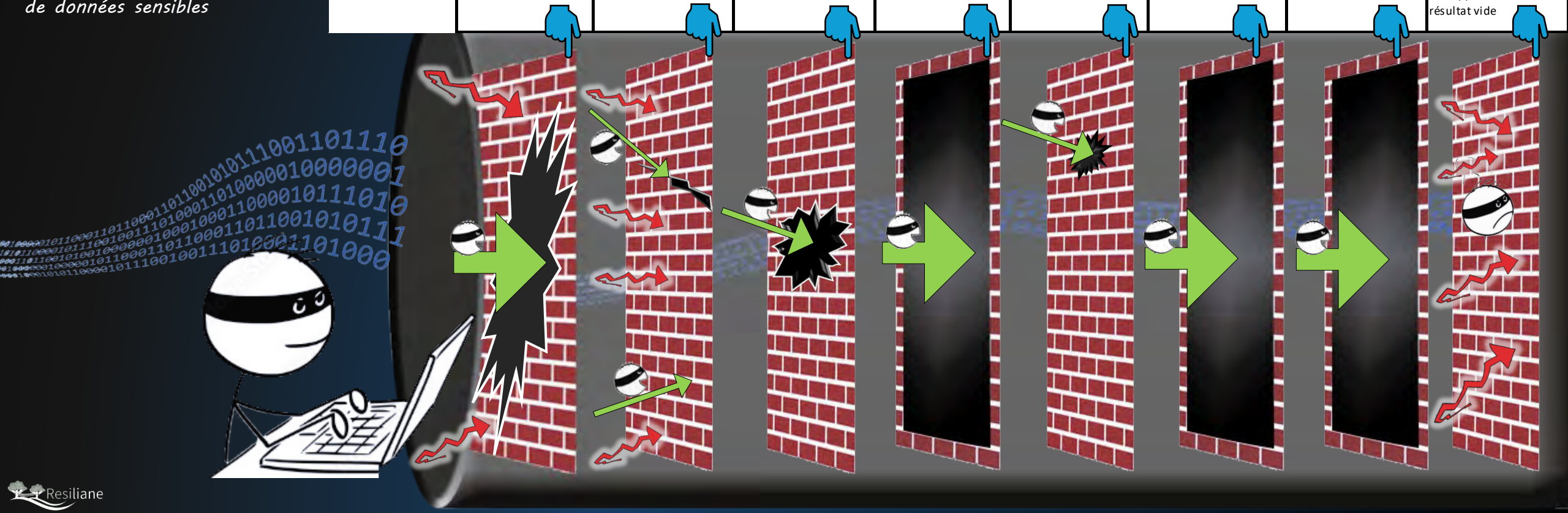
Autres mesures augmentant la protection des données Db2

- 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)

L’efficacité de la sécurité par couches indépendantes

Exemple:
Tentative d’exfiltration de données sensibles

NIVEAU	Poste de travail	Poste de travail	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i
Mesure de protection	droits admin interdits	déploiement software packagé selon role	droits publics *EXCLUDE sur les données; droits *CHANGE via le groupe applicatif	function usage	exit point SQL & FTP (connexion & détail)	exit point SQL (registres client)	exit point sur tables ultra sensibles	RCAC
Statut de la mesure	en place	en place	en place	non activé car redondant avec les points d'exit	en place en mode bloquant	non activé car non supporté par le programme d'exit	non activé car programme d'exit non disponible ou non performant	en place
Méthode(s) de violation	phishing ou utilisateur malhonnête	FTP & DBeaver accessibles	SQL, FTP	SQL, FTP	FTP bloqué, SQL accessible	SQL accessible	SQL accessible	SQL accessible, mais pas de données restituées
Explications	prise de contrôle du poste via un proxy site web et installation d'un exécutable; récupération ID et mot de passe de connexion aux serveurs	ce poste appartenait à un utilisateur ayant un role différent; le poste n'a pas été nettoyé correctement avant redéploiement	le profil utilisé étant membre du groupe applicatif, son accès à la donnée est légitime	function usage non activé	les membres du groupe applicatif sont légitimes à utiliser une application Java manipulant les données IBM i dont la table sensible ciblée	pas de contrôle en place sur le client utilisé.	pas de contrôle supplémentaire sur la table sensible ciblée	permission SQL sur les fichiers sensibles avec analyse des critères d'environnement de travail via une fonction SQL: la lecture d'une table sensible en dehors de l'application donne un résultat vide



Resiliane

Université IBM i

19 et 20 novembre 2024

Merci de votre attention !

Guy Marmorat
Consultant expert Sécurité IBM i
gmarmorat@resiliane.com

Resiliane

IBM

common FRANCE