Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

Immersion dans 2 projets différents de remédiation

18 novembre 14:45 - 15:45

Guy Marmorat
Resiliane
gmarmorat@resiliane.com

IBM

common FRANCE

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

IBM

2 PROJETS DIFFÉRENTS DE REMÉDIATION EN TERMES DE :

- Complexité de l'environnement
- Budget
- Objectifs

Sécurité IBM i - Projet de remédiation

Introduction

Entreprise	PME familiale leader sur le marché français - 4 milliards CA	Etablissement financier français et international (dans le top-20 Europe)
Infra	1 Prod, 1 backup, 1 test/dev	Chaque filiale est équipée d'au moins une partition de SIT (Test/Dev), UAT (Recette), Production, BackUp, parfois infocentre
Ressources IBM i	1 admin à temps partiel, assisté par un partenaire technologique	6 admins dont 4 seniors
Motivation du projet	Confrère ayant subi une attaque aux conséquences lourdes	Le durcissement de la sécurité est un projet prioritaire
Situation de départ	Page blanche - Difficulté d'apprécier le niveau de résistance en cas d'attaque similaire	Chaque filiale est à un niveau différent. De nombreux audits sont menés.
Objectif	Durcir la sécurité de façon urgente mais pérenne, tout en restant compatible avec les ressources et le budget	Sécurité optimale visée, implementée de façon incrémentale
Délai	18 mois	> 5 ans, avec jalons réguliers
Budget	< 100k	?

Sécurité IBM i - Projet de remédiation 1

Déroulement

Audit sécurité finesse 3/5 *(36 items de gravité élevée)*
Test de résistance finesse 3/5 *(91% des scenarios réussis)*

Test de résistance finesse 3/5 *(17% des scenarios réussis)*

Test de résistance finesse 3/5 *(3% des scenarios réussis)*

15 minutes par jour maximum (tâches assurées par le partenaire technologique)

Phase initiale	Phase remédiation 1	Phase fin de remédiation 1	Phase remédiation 2	Phase fin de remédiation 2	Statut	Tâches d'exploitation	Tâches Exploitation Ressources	Projets identifiés

Jour J — 6 mois — 7 mois — 9 mois — 13 mois — 15 mois

- Remédiation des failles de gravité haute et effort faible à moyen
- Contrôle d'accès via les points d'exit (granularité moyenne)

- Tuning en fonction du résultat du test de résistance
- Contrôle des déviations

Fin de projet

Contrôle automatisé des déviations, maintenance des règles de contrôle d'accès, revue de logs

Chiffrement des échanges

Sécurité IBM i - Projet de remédiation 2

Déroulement

Application du plan global de sécurité du groupe au monde IBM i

Audit trail complet, lisible, pertinent

Audit sécurité finesse 4/5
Test de résistance finesse 4/5
(3% des scenarios réussis)

1 admin dédié pour 50/75% de son temps

Phase initiale	Phase remédiation 1	Phase fin de remédiation 1	Phase remédiation 2	Phase fin de remédiation 2	Statut	Tâches d'exploitation	Tâches Exploitation Ressources	Projets identifiés
Jour J	6 mois	7 mois	24 mois	36 mois	> 4 ans			

- Contrôle des comptes à privilèges
- Contrôle d'accès via les points d'exit (granularité élevée)
- Rationalisation des pratiques liées aux échanges de données

- Intégration du monde IBM i au sein du SOC
- Remédiations
- Reporting évènements & déviations
- Déploiement & Consolidation
- CI/CD

Amélioration continue

Contrôle automatisé des déviations, maintenance des règles de contrôle d'accès, revue de logs

- MFA
- Durcissement protection données sensibles

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

IBM

SÉCURITÉ IBM i
PROJET DE REMÉDIATION 1

Phase de remédiation 1

Remédiation des failles de "Gravité Haute" et "Effort Faible à Moyen"
Contrôle d'Accès via les Points d'Exit (Granularité Moyenne)

Remédiation effectuée
(Gravité Elevée & Effort Accepté)

- Renforcement des mots de passe (expiration, complexité)
- QSECURITY passage de 30 à 40
- Possibilités restreintes
- Mots de passe par défaut
- Droits publics sur les profils
- Réduction des partages
- Application des PTFs
- Configuration DDM/DRDA durcie
- Profils de groupe comme marqueur de droits et/ou porteur de droits
- Durcissement config SSH

Remédiation non effectuée
Risque assumé
(Gravité Elevée & Effort jugé trop Important)

- Partie utilisateur de la liste des bibliothèques
- Droits spéciaux des profils
- Droits sur les bibliothèques et objets
- Droits sur les objets de l'IFS
- Adoption de droits, permutation de profils

Implémentation des Points d'Exit

- Utilisation du modèle par défaut, augmenté de JobNotify
- Portée des règles limitée à la bibliothèque et aux répertoires de niveau 1/2/3
- 4 mois en mode simulation / réglage de la config des points d'exit / formation
- Activation du mode bloquant pour les connexions
- Activation partielle du mode bloquant pour les transactions

	Situation testée	Résultat avec droits initiaux	Résultat avec droits usurpés	Remédiation
DB2	Découverte fichiers Db2 potentiellement sensibles	OK	OK	Exit points
	Accès en lecture aux fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
	Téléchargement des fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
	Accès en modification aux fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
SPLF	Découverte fichiers spool potentiellement sensibles	OK	OK	Droits et/ou Exit points
	Accès en lecture aux fichiers spool sensibles	KO	OK	Droits sur OUTQ corrects
IFS	Découverte répertoires partagés	OK	OK	Droits et/ou Exit points
	Navigation dans les répertoires partagés sensibles	OK	OK	Droits et/ou Exit points
	Découverte fichiers stream dans répertoires partagés sensibles	OK	OK	Droits et/ou Exit points
	Accès en lecture aux fichiers stream sensibles	OK	OK	Droits et/ou Exit points
	Téléchargement des fichiers stream sensibles	OK	OK	Droits et/ou Exit points
	Upload de fichiers stream	OK	OK	Droits et/ou Exit points
Profils	Découverte de profils (72)	OK	OK	Exit points
	Découverte de profils en accès public (0)	KO	KO	Droits et/ou Exit points
	Connexion avec des profils avec mot de passe par défaut (12)	OK	OK	Remédiation & contrôle
	Connexion avec des profils puissants avec mot de passe par défaut (10)	**OK+**	OK	Remédiation & contrôle
	Usurpation de droits d'un profil puissant	**OK+**	OK	QSECURITY en 40 - sécurisation jobds
	Ajout *ALLOBJ à mon profil	**OK+**	OK	QSECURITY en 40 - sécurisation jobds
Appli	Programme initial adoptant des droits élevés	OK	OK	Droits
	Découvrir le mécanisme d'enrollement dans l'application	OK	OK	Droits et/ou Exit points
	S'enregistrer soi-même dans l'application	OK	OK	Droits et/ou Exit points
	Intercaler un programme de ligne de commande dans la chaine d'appel du programme initial	OK	OK	Droits et/ou Exit points
	Créer et compiler un programme CL	OK	OK	Droits et/ou Exit points
	Modifier un programme pour qu'il utilise l'adoption de droits	OK	OK	Droits et/ou Exit points
Scripts	Découverte de fichiers Db2 de connexion avec des IP et/ou users et/ou mots de passe	OK	OK	Changer méthodes de connexion
	Découverte de fichiers stream de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Changer méthodes de connexion
	Accès à d'autres serveurs avec les scripts de connexion découverts	KO	KO	
JOBSCDE	Découverte du planning des travaux	OK	OK	Droits et/ou Exit points
	Ajout d'entrée dans le planning	OK	OK	Droits et/ou Exit points
	Action sur entrée existante dans le planning	KO	OK	Droits et/ou Exit points
Divers	Partage root en lecture	KO	OK	Droits et/ou Exit points
	Partage root en lecture/modification	KO	OK	Droits et/ou Exit points
	Changer le paramètre AUTOSTART d'un protocole	KO	OK	Droits et/ou Exit points
	Permettre à des utilisateurs limités de taper certaines commandes	OK	OK	Droits et/ou Exit points

Contexte

Poste de travail non bridé (incluant ACS complet)

Profil sans droit spécial, sans groupe avec possibilités restreintes

OK Test de violation réussi
KO Test de violation échoué
OK+ Test de violation réussi qui permet en plus une élévation de droits et/ou une usurpation de profil

Contexte

Poste de travail non bridé (incluant ACS complet)

Profil sans droit spécial, sans groupe avec possibilités restreintes

	Situation testée	Résultat avec droits initiaux	Résultat avec droits usurpés	Remédiation
DB2	Découverte fichiers Db2 potentiellement sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers db2 sensibles	KO	KO	Exit points
	Téléchargement des fichiers db2 sensibles	KO	KO	Exit points
	Accès en modification aux fichiers db2 sensibles	KO	KO	Exit points
SPLF	Découverte fichiers spool potentiellement sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers spool sensibles	KO	KO	Droits sur OUTQ corrects
IFS	Découverte répertoires partagés	KO	KO	Exit points
	Navigation dans les répertoires partagés sensibles	KO	KO	Exit points
	Découverte fichiers stream dans répertoires partagés sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers stream sensibles	KO	KO	Exit points
	Téléchargement des fichiers stream sensibles	KO	KO	Exit points
	Upload de fichiers stream	KO	KO	Exit points
Profils	Découverte de profils (72)	KO	KO	Exit points
	Découverte de profils en accès public (0)	KO	KO	Droits et Exit points
	Connexion avec des profils avec mot de passe par défaut (12)	KO	KO	Remédiation & contrôle
	Connexion avec des profils puissants avec mot de passe par défaut (10)	KO	KO	Remédiation & contrôle
	Usurpation de droits d'un profil puissant	KO	KO	QSECURITY en 40 - sécurisation jobds
	Ajout *ALLOBJ à mon profil	KO	KO	QSECURITY en 40 - sécurisation jobds
Appli	Programme initial adoptant des droits élevés	KO	KO	Droits
	Découvrir le mécanisme d'enrollement dans l'application	KO	KO	Exit points
	S'enregistrer soi-même dans l'application	KO	KO	Exit points
	Intercaler un programme de ligne de commande dans la chaine d'appel du programme initial	OK	OK	Risque assumé
	Créer et compiler un programme CL	KO	KO	Droits
	Modifier un programme pour qu'il utilise l'adoption de droits	KO	KO	Droits
Scripts	Découverte de fichiers Db2 de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Exit points
	Découverte de fichiers stream de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Exit points
	Accès à d'autres serveurs avec les scripts de connexion découverts	KO	KO	
JOBSCDE	Découverte du planning des travaux	KO	KO	Exit points
	Ajout d'entrée dans le planning	KO	KO	Droits
	Action sur entrée existante dans le planning	KO	KO	Droits
Divers	Partage root en lecture	KO	KO	Droits
	Partage root en lecture/modification	KO	KO	Droits
	Changer le paramètre AUTOSTART d'un protocole	KO	KO	Droits
	Permettre à des utilisateurs limités de taper certaines commandes	KO	KO	Exit points

OK Test de violation réussi
KO Test de violation échoué
OK+ Test de violation réussi qui permet en plus une élévation de droits et/ou une usurpation de profil

Power Week

18 -19 - 20 novembre 2025

IBM

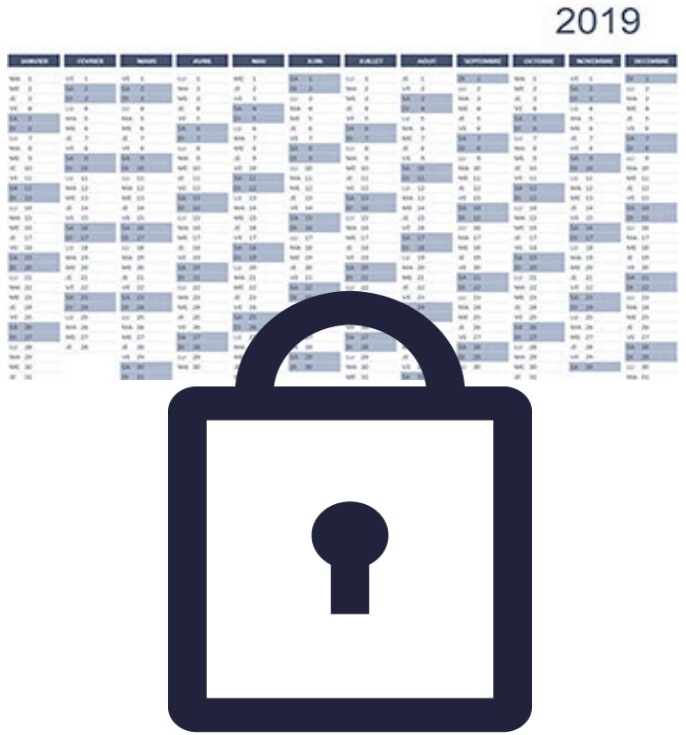
common FRANCE

IBM

SÉCURITÉ IBM i
PROJET DE REMÉDIATION 2

Projet de Sécurité IBM i

- Débuté en 2019
- Planification
- POC & Décision sur l'outillage retenu
- Allocation budget
- Allocation ressources internes & externes
- Définition d’un standard interne de Sécurité IBM i
- Macro-objectifs



Macro-Objectifs

Technologies

Macro-Objectifs

	Exit Points	Elévation Droits	Journal	Service SQL	Autre Soft
Intégration du monde IBM i au sein du SOC	SOFTWARE ✓	SOFTWARE ✓	SOFTWARE ✓		
Remédiations	SOFTWARE		SOFTWARE ✓	✓	
Reporting évènements & déviations	SOFTWARE		SOFTWARE ✓	✓	
Contrôle d'Accès	SOFTWARE ✓				
Contrôle des comptes à privilèges	SOFTWARE ✓	SOFTWARE ✓	✓	✓	
Déploiement & Consolidation				✓	SOFTWARE ✓
CI/CD	SOFTWARE				✓
Rationalisation des pratiques liées aux échanges de données		✓	✓	✓	✓
Renforcement de l'authentification (MFA)	SOFTWARE ✓				SOFTWARE ✓

Utilisation essentielle

SOFTWARE

SOFTWARE

Utilisation secondaire

Projet de Sécurité IBM i

Chaque action doit

à minima contribuer à la mise en conformité avec les directives de Sécurité du Groupe

- ✓ tout en recherchant le meilleur équilibre entre la granularité de la règle, sa lisibilité, sa maintenabilité, sa pertinence **dans le temps**
- ✓ et en créant des indicateurs **mesurant** l'efficacité, la non-régression, les déviations possibles, les éventuels effets de bord des actions entreprises

Prérequis

- Chaque profil est membre d'au moins un groupe, porteur de droits et/ou simplement marqueur

- Planification rigoureuse des PTFs, TR et upgrade de versions (PTFs HYPER appliquées rapidement). Incidents de sécurité traités en priorité

- Toute IP fixe est maintenue dans un référentiel avec des infos complémentaires telles que type d'équipement (device, serveur, …), catégorie (SIT, UAT, production, ...), descriptif, compte de service associé

Chronologie

Janv / Mars : Installation de base & formation
Fév / Juin : Reporting de base
Juin / Déc : Intégration SIEM

Janv 22 / Sept 23 :
Amélioration continue

Oct 20 / Oct 21 : Conception moteur du contrôle d'accès & tuning - temps long en mode apprentissage (intègre aussi l'adoption de la mesure par les utilisateurs)

Juin / Déc : Elévation de droits & Intégration au contrôle d'accès

Oct : Red Team - Script trouvé sur machine Linux mal sécurisée, décodage hash du mot de passe, accès sur une prod IBM i en 5250 avec un compte de service.

Depuis cette date, tous les autres tests d'intrusion ont été contenus et identifiés.

Août 22 / Août 23 :
Passage contrôle d'accès
en mode bloquant

Power Week

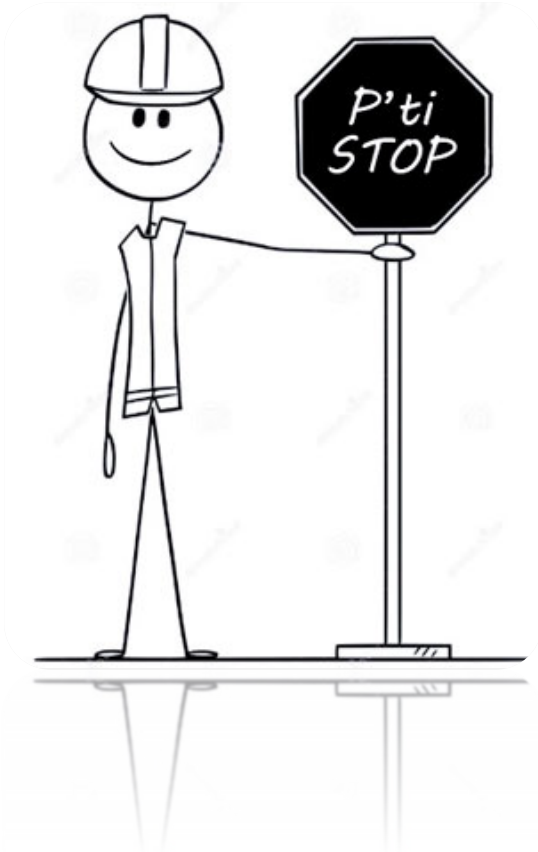
18 -19 - 20 novembre 2025

IBM

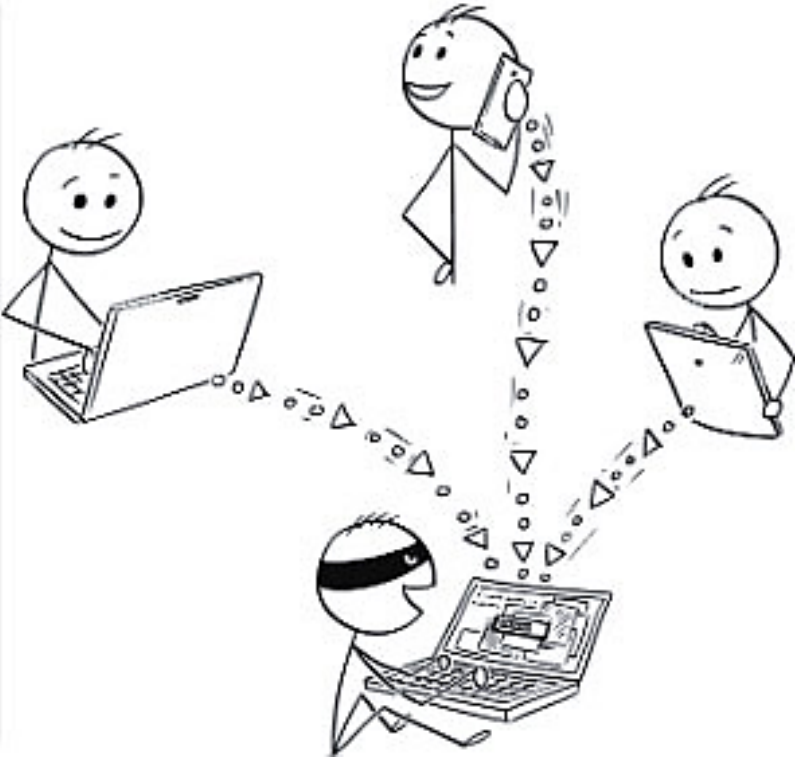
common FRANCE

IBM

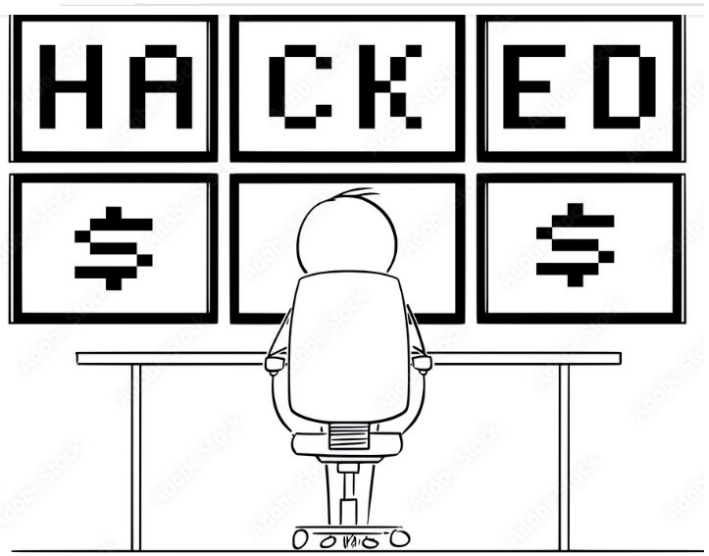
DIGRESSION



Les applications externes



CONFIANCE OU PAS ?



Software Supply Chain Attacks

Une seule attaque est égale à :

De multiples sites infectés et/ou accessibles via des back doors, la propagation étant assurée par des canaux de confiance

Les applications externes

MFT (Managed File Transfer)

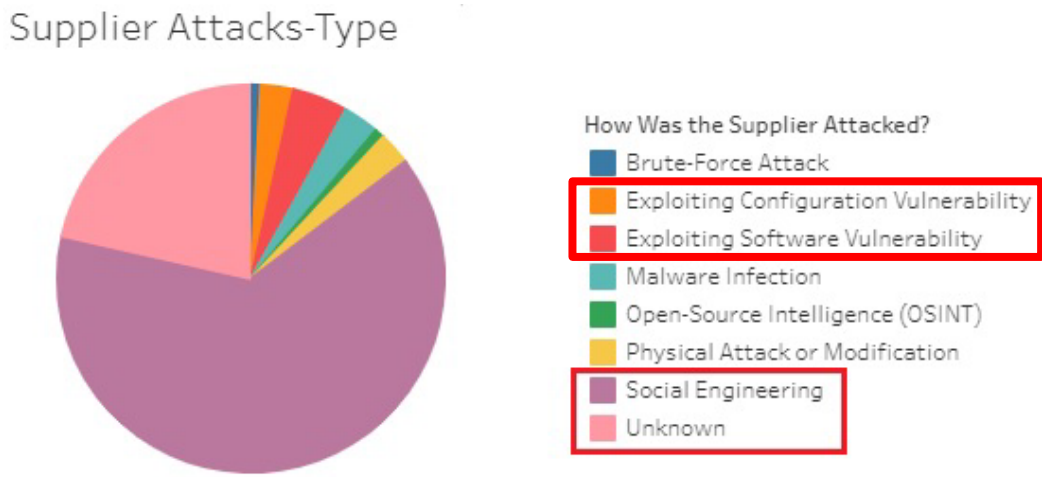
Cleo	9.8	2024-12
Cleo	9.8	2024-10
CrushFTP	not available	2024-12
CrushFTP	10.0	2024-04
CrushFTP	9.8	2023-11
Globalscape	7.5	2023-06
GoAnywhere MFT	not available	2024-12
GoAnywhere MFT	9.8	2024-01
GoAnywhere MFT	7.2	2023-02
IBM Sterling	9.1	2025-01
IBM Sterling	7.5	2024-11
IBM Sterling	9.8	2024-08
IBM Sterling	7.5	2024-08
MoveIT	9.8	2024-06
MoveIT	9.1	2024-06
MoveIT	7.5	2024-05
MoveIT	7.1	2024-01
MoveIT	7.2	2023-11
MoveIT	8.8	2023-09
MoveIT	9.1	2023-07
MoveIT	9.8	2023-06
WS_FTP Server	8.1	2024-08
WS_FTP Server	8.8	2023-11
WS_FTP Server	9.6	2023-09
Titan MFT	9.1	2023-10

SIEM et autres produits de Sécurité

		HIGH (7.x)	CRITICAL (9.x)
SolarWinds	2025		1
	2024	27	7
	2023	22	3
IBM QRadar	2024	3	
	2023	10	
ArcSight	2024	2	1
	2023	1	1
Splunk	2025	2	
	2024	13	
	2023	16	1
Elastic	2024	2	
	2023	15	1
Graylog	2024	1	
	2021	2	2

CONFIANCE OU PAS ?

- Compte de service à privilèges très élevés
- Exfiltration difficilement détectable dans la signature du run
- Application considérée comme critique pour le business



Hacking History and News affecting the IBM i Security perception

Big chock Incredulity	09/08/2015	DEF CON	Live session	“Hack the legacy! IBM i (aka AS/400) revealed”
	02/09/2015	ITJungle	Article	Did IBM i Just Get Hacked at DEF CON?
	16/09/2015	ITJungle	Article	Hacker Defends DEF CON Talk on IBM i Vulns
Scary/ Mutilple layers of defense	16/03/2016	ITJungle	Article	Verizon Outlines Disturbing AS/400 Breach At Water District
Starting to work on it	25/01/2017	ITJungle	Article	What Was Discussed At the Big LUG Meeting
Apps: trusted or not trusted?	27/01/2021	ITJungle	Article	SolarWinds Hack Raises Concern for IBM i Shops
Zero-day - Score = 10	15/12/2021	ITJungle	Article	Critical Log4j Vulnerability Hits Everything, Including the IBM i Server
Software Supply Chain Attack	03/10/2022	ITJungle	Article	Software Supply Chain Attacks Are A Growing Threat
Zero-day on MFT	15/02/2023	ITJungle	Article	Zero-Day Vulnerability in Fortra’s GoAnywhere MFT Being Actively Exploited
IBM i vulns	23/08/2023	ITJungle	Article	A Hacker’s Dozen: 11 New Security Vulns Reported in IBM i
Library List	02/09/2024	TROOPERS24	Live session	"IBM i for Wintel Hackers" by Silent Signal
Privilege escalation	16/09/2024	ITJungle	Article	**Ethical Hackers Discuss Penetration Work On IBM i**

“So one thing to know about this library list issue is that we’ve already discovered like literally hundreds of these,” Varga-Perke said. “So this is not an exception. It seems to be the rule. IBM is cleaning up the place right now, as you can see in their advisories. But yeah, it’s a really rich attack surface. And as you can see, it’s like basic logic bugs. You can find it if you have access to such a system really easily using basically strings.”

Having exit programs in place is a definite plus, Varga-Perke said, particularly as they present “custom defenses that the attackers cannot prepare for.” IBM i shops could also get more information about how hackers are targeting IBM i by implementing honey pots, or canaries, that attract hacker and then track their movements.

Et l'Operating System IBM i

CONFIANCE OU PAS ?

CVE ID	Date	CVSS Base sco	title	PTF 7.3	PTF 7.4	PTF 7.5	PTF 7.6
CVE-2025-50106	11/14/2025	8.1	IBM i is affected by Remote Code Execution, Deserialization of Untrusted Data, and Improper Access Controls vunlerabilities in IBM Java SDK and IBM Java Runtime	SJ06883	SJ06884	SJ06885	SJ06886
CVE-2025-40778	11/6/2025	8.6	IBM i is affected by BIND accepting records with untrusted data, predictable port and query ID, and resource exhaustions in Domain Name System due to multiple vulnerabilities	SJ07573	SJ07572	SJ07452	SJ07574
CVE-2025-36367	10/31/2025	8.8	IBM i is affected by a privilege escalation in IBM i SQL services	SJ07555	SJ07554	SJ07553	SJ07552
CVE-2025-50106	10/7/2025	8.1	IBM i is affected by Remote Code Execution, Deserialization of Untrusted Data, and Improper Access Controls vunlerabilities in IBM Java SDK and IBM Java Runtime	SF99725 - 39	SF99665 - 30	SF99955 - 18	SF99965 - 3
CVE-2025-36097	9/26/2025	7.5	IBM i is affected by denial of service vulnerabilities in IBM WebSphere Application Server Liberty	SJ06599	SJ06597	SJ06596	SJ06595
CVE-2025-36119	8/15/2025	7.1	IBM i is affected by an authenticated user gaining elevated privileges due to a web session hijacking vulnerability in IBM Digital Certificate Manager for i	SJ06550	SJ06552	SJ06557	SJ06558
CVE-2024-6387	8/7/2025	8.1	IBM i is affected by a timing attack, handling signals in an unsafe manner, and uncontrolled memory consumption due to vulnerabilities in OpenSSH				SJ06522
CVE-2024-55898	7/31/2025	9.8	IBM i is affected by multiple vulnerabilities in International Components for Unicode (ICU) option 39				
CVE-2025-33109	7/24/2025	7.5	IBM i is vulnerable to a privilege escalation due to an invalid database authority check	SJ05840	SJ05839	SJ05838	SJ05809
CVE-2024-6119	7/24/2025	7.5	IBM i is affected by errors in OpenSSL as part of IBM Portable Utilities for i due to multiple vulnerabilities	SJ06399	SJ06283	SJ06341	SJ06342
CVE-2025-33108	6/18/2025	8.5	IBM Backup, Recovery and Media Services for i is vulnerable to a user gaining elevated privileges due to an unqualified library call		SJ05906	SJ05907	
CVE-2025-33103	5/17/2025	8.5	IBM i is vulnerable to a privilege escalation vulnerability in IBM TCP/IP Connectivity Utilities for i	SJ05514	SJ05505	SJ05494	
CVE-2025-2947	4/17/2025	7.2	IBM i is vulnerable to a privilege escalation due to incorrect profile swapping in an OS command				
CVE-2024-55898	2/22/2025	8.5	IBM i could allow a user with the capability to compile or restore a program to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege	SJ03652	SJ03651	SJ03650	
CVE-2024-38473	12/8/2024	8.1	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a remote attacker obtaining sensitive information, bypassing security restrictions, and a server-side request forgery due to multiple vulnerabilities	SJ02216	SJ02234	SJ02352	

Nombre de CVE		HIGH (7.x)	CRITICAL (9.x)
IBM i	2020	13	0
	2021	9	5
	2022	22	4
	2023	25	2
	2024	24	4
	>15/11/2025	28	1

*LIBL & SQL Path et la Sécurité

CVE ID	Date	CVSS Base score	title
CVE-2025-33108	6/18/2025	8.5	IBM Backup, Recovery and Media Services for i is vulnerable to a user gaining elevated privileges due to an **unqualified** library call
CVE-2024-55898	2/22/2025	8.5	IBM i could allow a user with the capability to compile or restore a program to gain elevated privileges due to an **unqualified** library call. A malicious actor could cause user-controlled code to run with administrator privilege
CVE-2024-38330	7/3/2024	7	IBM Managed System Services for i and IBM System Management for i are vulnerable to a local user gaining elevated privilege due to **unqualified** library calls
CVE-2024-27264	5/21/2024	7.4	IBM i is vulnerable to a local privilege escalation due to an **unqualified** library call in IBM Performance Tools for i
CVE-2024-25050	4/27/2024	8.4	IBM Rational Development Studio for i is vulnerable to a local privilege escalation due to an **unqualified** library call in compiler infrastructure
CVE-2023-43064	2/10/2024	7	IBM Facsimile Support for i is vulnerable to a local user gaining elevated privileges due to an **unqualified** library call

Adopted authority risks and recommendations

You should use adopted authorities with care to prevent possible security risks.

Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user will not normally have.

Adopted authority provides an important tool for meeting diverse authority requirements, but it should be used with care:

• Make sure that programs that adopt authority and call other programs perform library qualified calls. Do not use the library list (*LIBL) on the call.

Library security and library lists

Attention: A user who is authorized to the commands to work with library lists can potentially run a different version of a program.

ADDLIBLE	*CMD	Add Library List Entry	*USE
CHGLIBL	*CMD	Change Library List	*USE
CHGSYSLIBL	*CMD	Change System Library List	*EXCLUDE
EDTLIBL	*CMD	Edit Library List	*USE
RMVLIBLE	*CMD	Remove Library List Entry	*USE
CHGCURLIB	*CMD	Change Current Library	*USE
SBMJOB	*CMD	Submit Job	*USE
SETASPGRP	*CMD	Set ASP Group	*USE
QLICHGLL	*PGM	Change Library List	*USE
QSYSLIBL	*SYSVAL	System part of the library list	
QUSRLIBL	*SYSVAL	User part of the library list	
	*JOBD		
SET PATH			
…			

Security risks of library lists

This topic gives specific examples of the possible security exposures of library lists and how to avoid them.

Library lists represent a potential security exposure. If a user is able to change the sequence of libraries on the library list, or add additional libraries to the list, the user might be able to perform functions that break your security requirements.

Recommendations for system portion of library list

This topic provides the recommendations for the system portion of the library list.

The system portion of the library list is intended for IBM-supplied libraries. Application libraries that are carefully controlled can also be placed in the system portion of the library list. The system portion of the library list represents the greatest security exposure, because the libraries in this part of the list are searched first.

Source : IBM i 7.5 Security Reference

Techno : Exit Points

- Complète la Sécurité native (contextuelle versus statique)
- Couche sollicitée en premier
- Besoin évident de sécurité contextuelle (object, function usage, exit point)
- 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)

Catégories de Points d'Exit en lien avec la Sécurité :

- ceux attachés à l'authentification (FTP Server, REXEC, ODBC, TCP Logon)
- ceux attachés aux transactions, commandes, fonctions, ... (FTP client, FTP Server, REXEC, ODBC, NetServer, Remote Commands, DDM)
- ceux attachés aux commandes (before, after)
- ceux attachés aux ouvertures de fichiers Db2 (valeur d'audit *CHANGE, *ALL) & IFS stmf (attributs *CRTRUNEXIT & *RUNEXIT)
- ceux attachés aux Sockets (communication de bas niveau - IP & Port)
- ceux attachés au moteur SQL (Query Governor, Query Supervisor)
- ceux plus exotiques (job_notify, virus scanning, profile, password, data queues, …)

Contrôle d’accès : Les fondations

Listes blanches par typologie d'action ou d'objet touché :

- logon,
- Db2,
- IFS,
- remote commande,
- remote programme,
- data queue

Tout compte utilisateur est membre d'au moins un groupe (porteur de droits ou marqueur simple selon les cas)
Granularité des contrôles adaptée pour un pilotage dans la durée et une évolution aisée selon les nouveaux process et besoins de durcissement

Contrôle d’accès : Les fondations

Logon Inbound & Outbound	Compte de service : Profil - IP(s) - Protocole Autre compte : Groupe Profil - IP(s) ou Range – Protocole	NB : NetServer n'a malheureusement pas de point d'exit dédié au logon

DB2	profil/groupe profil - type accès (lecture/modification) - protocole - bibliothèque - fichier (rarement à ce niveau)
IFS	profil/groupe profil - type accès (lecture/modification) - protocole - chemin (rarement au niveau du fichier)
Rmt PGM	profil/groupe profil - protocole - bibliothèque - programme
Rmt CMD	profil/groupe profil - protocole - bibliothèque - commande - paramètres
Fonctions	profil/groupe profil - protocole - fonction
SQL	profil/groupe profil - protocole - partie de la phrase SQL
Commands	profil/groupe profil - travail - IP - Stack (bibliothèque & programme)
Data Queue	profil/groupe profil - type accès (lecture/modification) - bibliothèque - objet *DTAQ

Contrôle d’accès : Les plus+

- Les applications SQL clientes doivent montrer pattes blanches !
- Contrôle renforcé via les registres clients

- Contrôle des commandes lançant du SQL + Contrôle contextuel des phrases SQL
- Commandes sensibles bloquées sauf avec élévation de droit + ticket valide
  - Exemples: CHGSYSVAL, ADDLNK, EDTF, UPDDTA, STRSST, …

- Maintenance d'une piste d'audit des utilisateurs supprimés
- Forcer certains utilisateurs à fermer la session avec l’option LOG(*LIST)

- Construction de la log :
  - transactions rejetées
  - transactions acceptées dans des contextes particuliers :
    - profils puissants
    - recherche de chaîne de caractère potentiellement sensible dans la string
    - autres critères (IP, stack, debug temporaire, etc…)

Contrôle d’accès : Les plus+

- TELNET vs Travail interactif….
- Point d'exit JOB_NOTIFY avec capacité de blocage d'ouverture de session
- Etanchéité des environnements (PROD-PROD, UAT-UAT, SIT-SIT)
- Contrôle renforcé pour les passerelles entre environnements différents

- Contrôle des valeurs de paramètres sensibles sur des commandes telles que : SBMJOB, ADDLNK, EDTF, ADDJOBSCDE, CHGJOBSCDE, …

- Fin du contournement de l'outil de DevOps : Blocage des commandes qualifiées CPYSRCF, RMVM, RNMM, STRRLU, STRSDA, STRSEU
- Blocage des modifications de source pour les bibliothèques et répertoires non référencés en DevOps

- Ajustement dynamique de priorités et de l’activation du multi-processing en fonction de critères tels que le current user, le job, l'IP

Contrôle d’accès : Les plus+

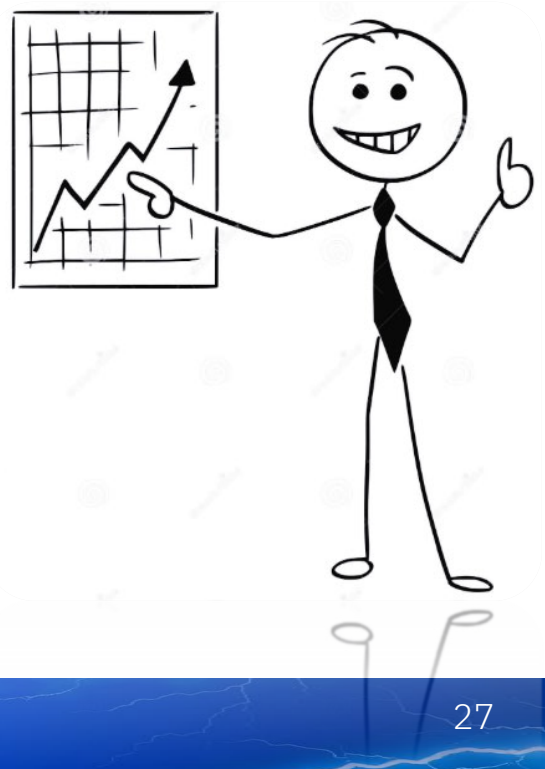
- Console surveillant toutes les partitions de façon globalisée avec auto-refresh

  ou …
- Sonde sur la log

  ➔ Réactivité en mode bloquant impérative

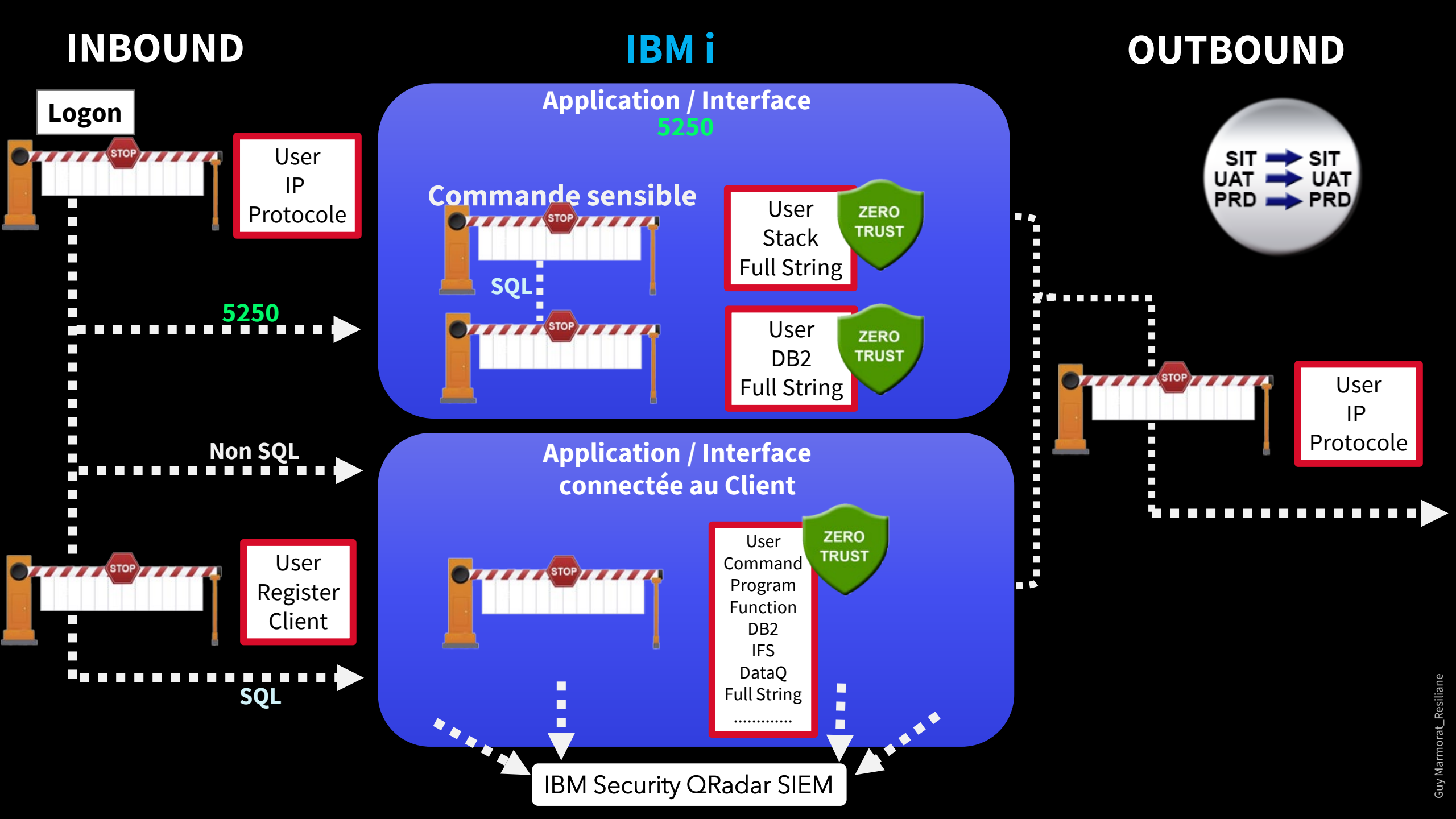
- Modèle de configuration maintenu sur une machine de référence
- Chaque règle est taguée sur une combinaison de 2 valeurs
  - Type partition: SIT, UAT, PROD, Infocentre, backup - Prod, non Prod - toutes
  - Filiale et/ou core banking : pays1, pays2, pays3, …. - soft1, soft2, soft3, ….- tous pays, tous soft
- Facilité de déploiement, confiance, lisibilité

Return On Investment



Elévation de Droits

- Contrôle des utilisateurs à privilèges
- Réduction de leurs droits permanents
- Elévation de droits à la demande et contrôlée par un numéro de ticket (ticket valide, attribué à l'utilisateur et la partition, avec option plage de dates)
- En fin de session élevée : envoi de la piste d'audit dans le ticket (joblog enrichie des SQL, commandes, écrans)
- Ouverture de droits logiques gérés par la couche point d’exit le temps de l’élévation


INBOUND
IBM i
OUTBOUND
Logon
User
IP
Protocole
5250
Non SQL
User
Register
Client
SQL
Application / Interface
5250
Commande sensible
SQL
User
Stack
Full String
ZERO
TRUST
User
DB2
Full String
ZERO
TRUST
Application / Interface
connectée au Client
User
Command
Program
Function
DB2
IFS
DataQ
Full String
.....
ZERO
TRUST
IBM Security QRadar SIEM
SIT
UAT
PRD
SIT
UAT
PRD
User
IP
Protocole
Guy Marmorat_Resiliane

Power Week

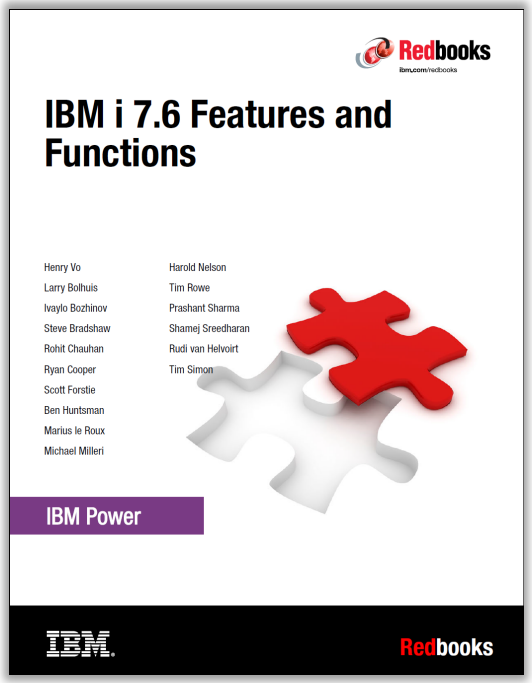
18 -19 - 20 novembre 2025

BONUS VERSION 7.6

OU COMMENT LA VERSION 7.6 AURAIT AIDÉ DANS LA REMÉDIATION ET/OU L'AMÉLIORATION DE LA SÉCURITÉ

BONUS 1 : MFA intégré

- L'authentification multifacteur (MFA) est gratuite et intégrée au système d'exploitation
- Activer MFA permet de l'utiliser. Elle est activée par utilisateur, et non par défaut
- Elle peut être activée dans le système d'exploitation et/ou dans SST (couches et configurations indépendantes)
- Elle prend uniquement en charge le protocole TOTP (Time based One Time Password-RFC 6238)
- Aucune modification d'infrastructure n'est requise (conformément à la RFC 6238)
- Des améliorations sont à prévoir…
- Hypothèse perso : forte exigence client ; IBM a déployé des efforts considérables pour y parvenir (modifications importantes et sensibles – non compatibles avec la version 7.5)
- La compréhension de la « persistance » est essentielle pour une utilisation optimale



From the Redbook:
« *Refer to this IBM i 7.6 doc information as the list of connection protocols that support MFA will likely continue to change over time.* »

BONUS 2 : Nouveau Point d'Exit

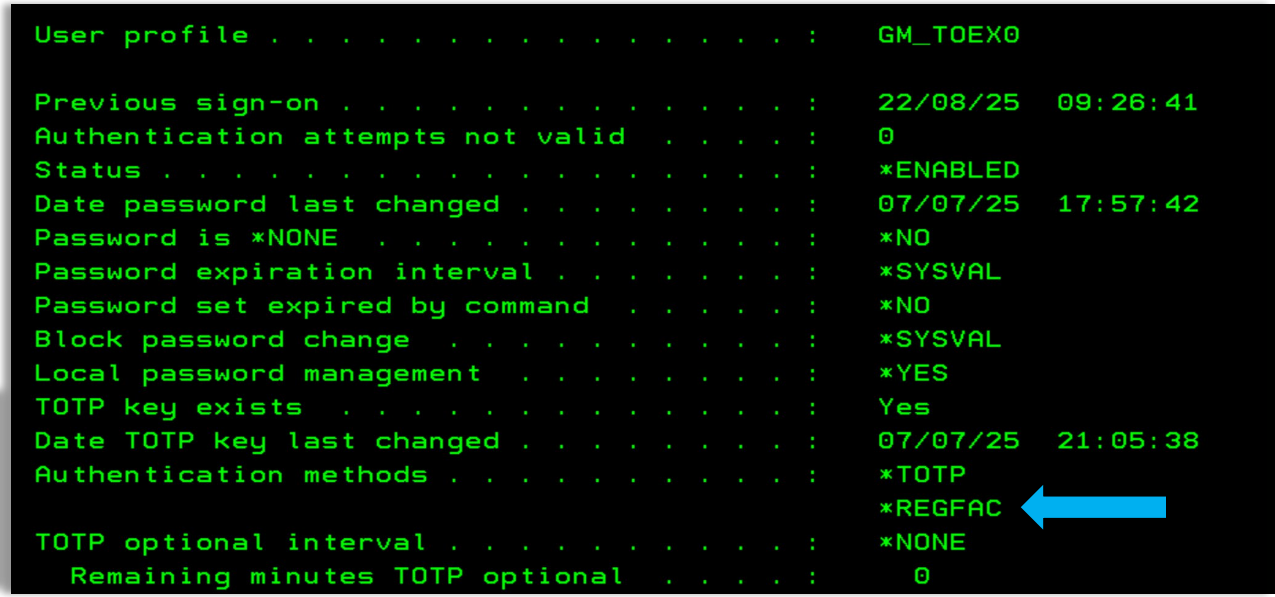
NIST 800-63B-4

SMS, HOTP and TOTP :

pas suffisants pour les normes AAL2 & AAL3

- Point d'exit **universel** appliqué sur l'authentification (QIBM_QSY_AUTH)
- Activé par utilisateur
- Indépendant de l'authentification multifacteur (MFA)
- Peut sécuriser **toute** authentification pour n'importe quel utilisateur (comptes de service) et protocole
- Peut déclencher du MFA supplémentaire
- Lorsque *TOTP + *REGFAC: *TOTP est exécuté en premier, puis ensuite le programme d'exit

Peut être utilisé pour constituer un inventaire complet des catégories d'authentification



BONUS 3 : Contrôle des usurpations

Faits :

- Un profil *ALLOBJ peut se faire passer pour n'importe quel autre profil (y compris QSECOFR) dans une session SQL en utilisant

  "Set session authorization TargetUser"

- Un profil disposant de droits (privés ou publics) >= *USE sur un autre profil peut se faire passer pour lui en utilisant

  "SBMJOB USER(TargetUser)"

Solutions :

- **Ajouter un usage *DENIED pour le profil TargetUser dans la function QIBM_RUN_UNDER_USER_NO_AUTH**
- **Monitorer les entrées QAUDJRN/PW avec violation_type in ('C', 'K', 'O')**
- **Exit points**

IBM Power Ideas Portal:

Rendre modifiable la valeur par défaut "Default authority" pour la passer à *DENIED si on souhaite

BONUS 3 : Contrôle des usurpations

User action auditing : *AUTWARN
GR entry type with F - *USAGEWARN

Impersonation allowed (default)

```
[ 08/28/2025, 10:07:34 AM ]  Run Selected...
set session authorization gm_sales01
Statement ran successfully   (152 ms)


[ 08/28/2025, 10:07:40 AM ]  Run Selected...
SELECT * FROM TABLE(QSYS2.CHANGE_TOTP_KEY('*GEN'))
Statement ran successfully   (266 ms)
```

```
[ 08/28/2025, 10:15:38 AM ]  Run Selected...
CRTPF FILE(QGPL/chgtotp) RCDLEN(100) AUT(*ALL)

CPC7301: File CHGTOTP created in library QGPL.
CPC7305: Member CHGTOTP added to file CHGTOTP in QGPL.
Statement ran successfully   (144 ms)


[ 08/28/2025, 10:15:43 AM ]  Run Selected...
sbmjob cmd(RUNSQL SQL('insert into qgpl.chgtotp (select
                        totp_key_blanks FROM TABLE(QSYS2.CHANGE_TOTP_KEY(''*GEN'')) )
                            ') COMMIT(*NONE) NAMING(*SQL)) job(chgtotp) user(gm_sales01)

CPC1221: Job 817277/GM_SALES01/CHGTOTP submitted to job queue QBATCH in library QGPL.
Statement ran successfully   (146 ms)


[ 08/28/2025, 10:15:47 AM ]  Run Selected...
select interpret(substring(chgtotp, 1, 100) as char(100)) guess from qgpl.chgtotp
Statement ran successfully   (240 ms)
```

Impersonation denied

```
[ 08/28/2025, 10:03:53 AM ]  Run Selected...
CHGFCNUSG FCNID(QIBM_RUN_UNDER_USER_NO_AUTH) USER(SALES) USAGE(*DENIED)

CPC221D: Function QIBM_RUN_UNDER_USER_NO_AUTH usage information changed.
Statement ran successfully   (154 ms)
```

```
[ 08/28/2025, 10:27:58 AM ]  Run Selected...
set session authorization gm_sales01
SQL State: 28000
Vendor Code: -552
Message: [SQL0552] Not authorized to SET SESSION_USER. Cause . . .
```

```
Message ID . . . . . :   CPD1616      Severity . . . . . :   40
Message type . . . . . :   Diagnostic
Date sent  . . . . . :   28/08/25     Time sent  . . . . . :   09:27:06

Message . . . . :   Not authorized to user profile GM_SALES01.
Cause . . . . . :   You are not authorized to user profile GM_SALES01.
Recovery  . . . :   Get authority from  either the security officer or the
  user profile owner, or change the user profile name (USER parameter). Then
  try the command again.
```

BONUS 4 : Découverte & Manipulation de partages

	7.5	7.6
APIs de manipulation de partages	*IOSYSCFG ou ownership requis	*IOSYSCFG ou QIBM_QZLS_NETSVR_SHARE function usage requis
Découverte des partages via QSYS2.SERVER_SHARE_INFO	Info publique	*IOSYSCFG ou QIBM_IOSYSCFG_VIEW function usage requis
Découverte des partages utilisés - Phase audit	Néant	nouveaux entry types C E S U du poste VP

All products / IBM i / 7.5.0 /

A newer version of this product documentation is available. You are viewing an older version.

SERVER_SHARE_INFO view

Last Updated: 2025-10-16

The SERVER_SHARE_INFO view returns information about IBM® i NetServer shares.

This information is similar to what is returned by the List Server Information (QZLSLSTI) and Open List of Server Information (QZLSOLST) APIs.

Authorization: None required.

All products / IBM i / 7.6.0 /

SERVER_SHARE_INFO view

Last Updated: 2025-10-07

The SERVER_SHARE_INFO view returns information about IBM® i NetServer shares.

This information is similar to what is returned by the List Server Information (QZLSLSTI) and Open List of Server Information (QZLSOLST) APIs.

Authorization: The caller must have either *IOSYSCFG special authority or be authorized to the QIBM_IOSYSCFG_VIEW function usage identifier.

Error Message

SQL State: 42502
Vendor Code: -443
Message: [SQL0443] *IOSYSCFG SPECIAL AUTHORITY OR QIBM_IOSYSCFG_VIEW FUNCTION USAGE REQUIRED Cause . . . . . : Either a trigger program, external procedure, or external function detected and returned an error to SQL. If the error occurred in a trigger program, the trigger was on table QDBSSUDF2 in schema QSYS. If the error occurred in an external procedure or function, the external name is QDBSSUDF2 in schema QSYS. The associated text is *IOSYSCFG SPECIAL AUTHORITY OR QIBM_IOSYSCFG_VIEW FUNCTION USAGE REQUIRED. If the error occurred in a trigger program, the associated text is the type of trigger program. If the error occurred in an external function, the associated text is the text of the error message returned from the external function. Recovery . . . : Refer to the joblog for more information regarding the detected error. Correct the error and try the request again.

```
Function ID  . . . . . :   QIBM_IOSYSCFG_VIEW
Function name  . . . . . :   View Input/Output System Configuration

Description  . . . . . :   Allows the ability to view Input/Output system con
figuration information.

Product  . . . . . :   QIBM_BASE_OPERATING_SYSTEM
Group  . . . . . :   *NONE

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

modifiable

BONUS 5 : Audit des partages

Poste VP en version 7.6

The type of entry.

P
Password error

D
NetServer user disabled

A
Authorization list (AUTL) permission failure

C
SMB server or share connection established

E
SMB server or share connection ended

S
SMB Share modified

U
SMB unknown user attempt to connect or guest connection

Poste VP en version 7.5

The type of error that occurred.

P
Password error

D
NetServer user disabled

A
Authorization list (AUTL) permission failure

SYSTOOLS.AUDIT_JOURNAL_VP

ENTRY_TYPE_DETAIL	AUDIT_USER_NAME	SHARE_AUTHORIZATION_LIST	SHARE_NAME	SHARE_TYPE	PERMISSIONS
Server or share connection established	GM	-	RSLAUD	FILE	*R
Server or share connection ended	GM	-	RSLAUD	FILE	-


MERCI