heliaq

LA SÉCURITÉ IBM I, QUI S'EN OCCUPE ?
ET VOTRE AS/400, ON S'EN OCCUPE QUAND ?

IBM i / AS400 : La confiance n'exclut pas la sécurité.

Sommaire

1

Présentation d'Heliaq

Qui sommes nous ?

2

La sécurité IBM i, qui s'en occupe ?

Et votre AS400, on s'en occupe quand ?

3

Les outils de sécurité

4

Notre savoir faire

Nos services

5

Questions / Réponses

1

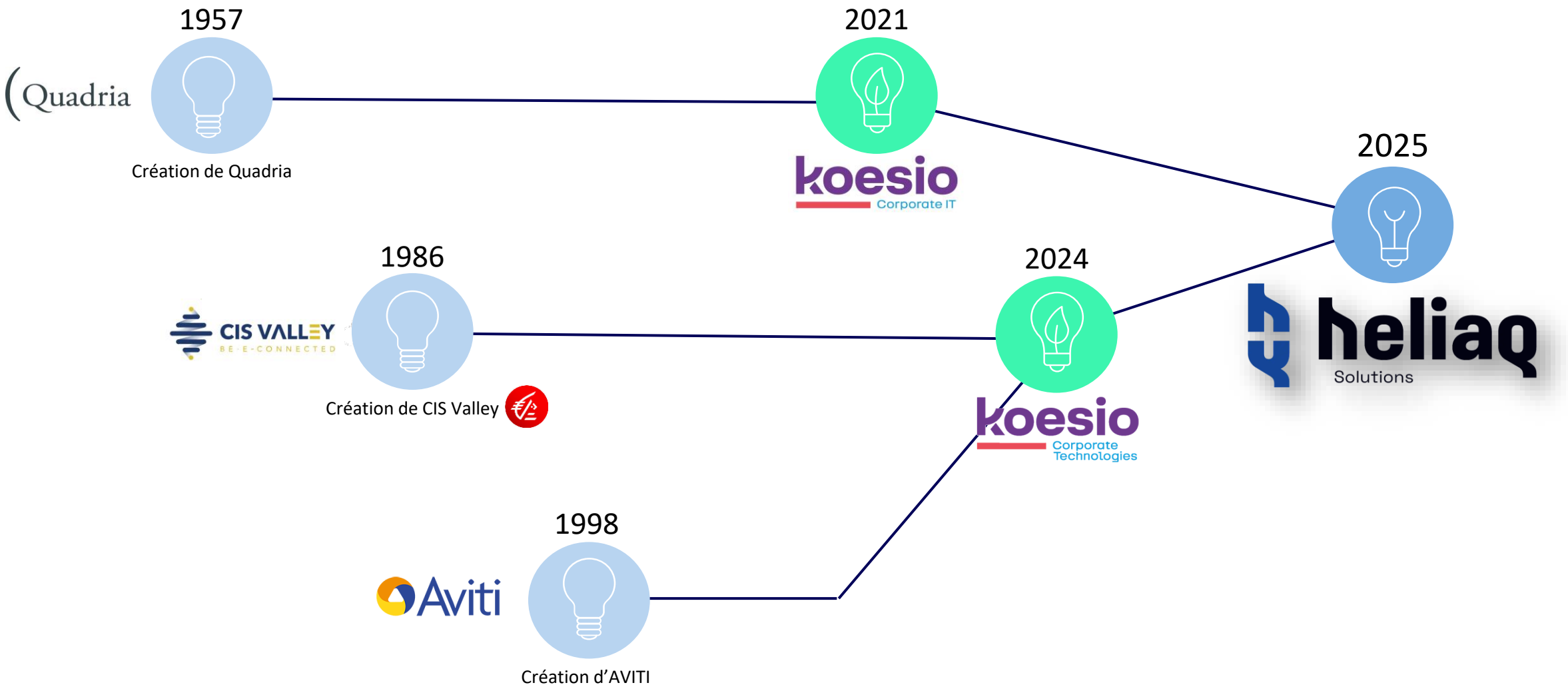
Qui sommes nous ?

heliaq
Solutions

heliaq

Un peu d'histoire

Plus de 60 ans d'activité, plus de 20 ans pour les activités Cloud et Services Managés



Solidité Financière
Pérennité

- Une ESN 100% française
- 360 M€ de CA
- + 6 000 clients
- 25 agences
- 760 salariés
- 7 datacenters opérés
- 94% de clients satisfaits

Au-delà de la technologie

heliaq

heliaq.fr

Pourquoi opter pour heliaq

Une approche 360°, des entités spécialisées

heliaq

- Digital Workplace
- Infrastructures IT
- Software

heliaq Solutions

- Cloud
- Service Managés
- Cybersécurité

Organisation Territoriale Heliaq Solutions

10 Agences :

Bordeaux,

Lyon,

Montpellier,

Nantes,

Orléans,

Paris,

Reims,

Rennes,

Toulouse,

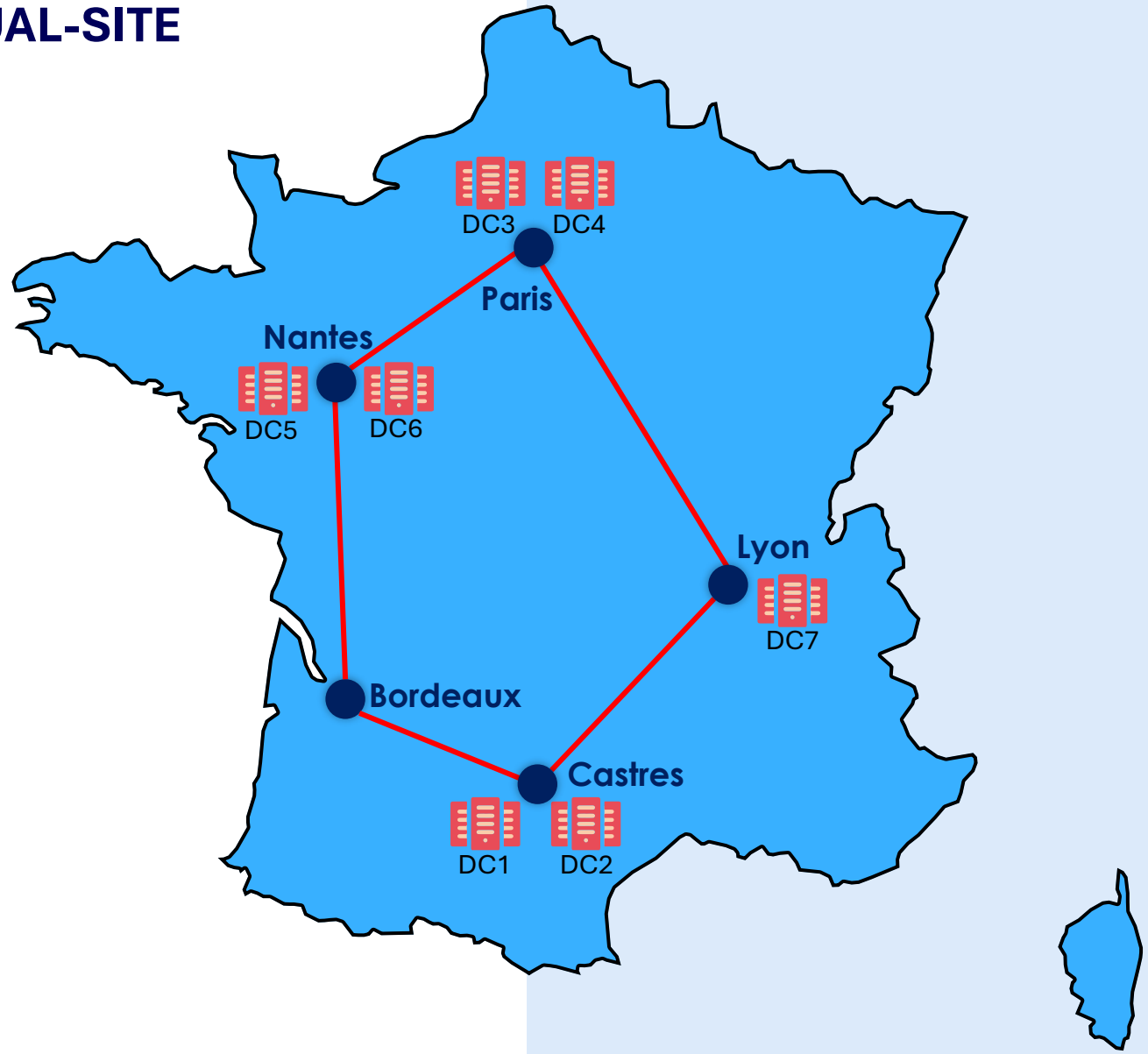
Tours.

280

Ingénieurs & Techniciens

Astreinte 24/7

Nos Datacenters DUAL-SITE



Datacenters Opérateur (Tier IV +)

Surveillance 24/7
2 Centres de service
(Bordeaux et Nantes)

DC dédié IBM Power (BPCE)

Certifications & Labels

- ISO 27001
- HDS
- ISO 14001
- ICPE
- OHSAS 18001
- ISO 22301
- ISO 50001
- EU Code of Conduct
- PCI-DSS

Confiance numérique

Souveraineté

- ✓ Hébergement souverain
- ✓ Société de droit français
- ✓ Actionnariat français
- ✓ Solutions françaises privilégiées
- ✓ Datacenters en France métropolitaine
- ✓ Centres de Services basés en France
- ✓ Données stockées en France
- ✓ Conformité RGPD

Qualité de service

- ✓ Certification ISO 27001 sur l'ensemble de nos activités
- ✓ Certification Hébergement de Données de Santé (HDS) des datacenters et des services managés (6 niveaux)
- ✓ Offres et services managés s'appuyant sur les bonnes pratiques ITIL
- ✓ Accompagnement sur mesure

RGPD Conformité

ISO 27001 certified by CERTI TRUST

HDS Hébergeur Données de Santé certified by CERTI TRUST

ITIL

2

Le paradoxe de la sécurité IBM i

La sécurité IBM i, qui s’en occupe ?

Et votre AS/400 on s’en occupe quand ?

heliaq

for Business

Le danger n’est pas dans l’action, mais dans l’inaction

55 %

Le nombre d’entreprises françaises ayant subi une cyberattaque en 2024

3,8 m€

Le coût moyen d’une violation de données pour une entreprise en France

(perte de productivité, réparation des systèmes, impacts réputationnels)

34 %

Des cyberattaques touchent des TPE/PME/ETI

68 %

Des cyberattaques avec une motivation lucrative

En 2024, plus d’1 entreprise sur 2 a été attaquée.

Le risque n’est plus théorique : il est quotidien.

Mettre en place des actions concrètes, c’est assurer sa résilience.

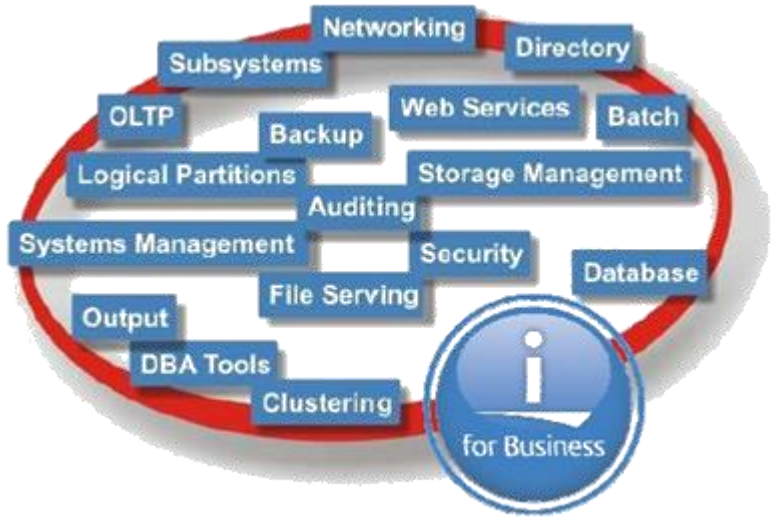
Le paradoxe de l'IBM i

Sécurité intégrée

IBM i Héberge les applications **critiques** de l'entreprise

ERP, Finance, Ressources humaines, GPAO, GMAO

i comme **intégré**



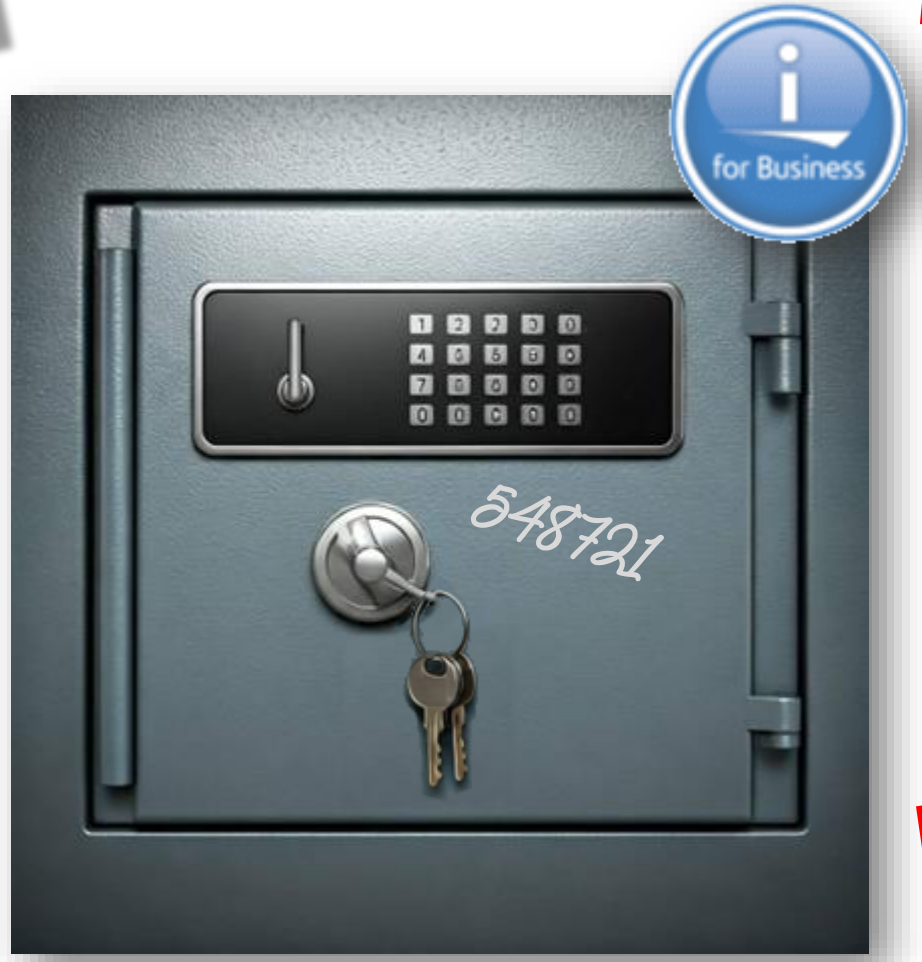
En natif dans le système

- Niveau de sécurité (QSECURITY)
- Validation de l'intégrité des objets
- Gestion de la politique de mot de passe
- SSO Active Directory (EIM)
- Authentification multi facteur
- Gestion des droits
- Chiffrement des flux (5250, FTP, ...)
- Traçabilité (journal d'audit)
- Chiffrement des données sur bande (BRMS)
- Gestionnaire de certificats numériques (DCM)

Le paradoxe de l'IBM i

Et pourtant...

- Mot de passe inchangé depuis plusieurs années
- Profils avec mot de passe par défaut
- Pas de politique de mot de passe
- Partage réseau à la racine de l'IFS
- Partage réseau avec profil « invité »
- Objets avec droits excessifs (*PUBLIC)
- Niveau de sécurité insuffisant (QSECURITY)



- Chiffrement des flux non implémenté (5250, FTP, ...)
- Mots de passe en clair sur le réseau (WireShark)
- Droits *ALLOBJ pour trop d'utilisateurs
- Pas d'utilisation des listes d'autorisations
- Bandes de sauvegarde stockée à demeure dans la librairie
- Pas de sauvegarde système régulière (SAV21)
- Pas d'externalisation des sauvegardes

Faut-il attendre l'apocalypse ?

Le jour où les cybercriminels découvriront l'IBM i

C'est pour quand ?
Etes vous prêt ?

Nostradamus a prédit :
Les cybercriminels vont découvrir l'IBM i en 20 ??

01 Janvier 20 ??

3

Les outils de sécurité

Sécuriser, Détecter, Protéger

heliaq

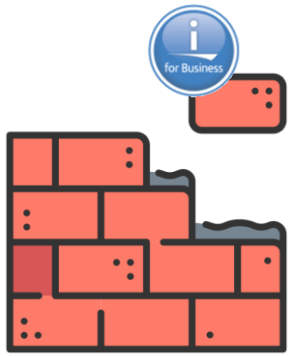
for Business

Portfolio des outils à disposition pour sécuriser son environnement

Introduction

Sécuriser son environnement IBM i, ça commence par sécuriser son Système d'Information de manière globale.

Les solutions techniques sont mutualisables avec les autres environnements



IBM i reste la brique du SI qui héberge souvent les applications critiques de l'entreprise, il ne faut pas la mettre de côté.

Sécuriser le matériel et ses interfaces d'administration

Serveurs IBM Power et le stockage associé

Power Systems

PowerVM

- **Les mots de passe par défaut ont-ils été modifiés ?**
  - ASMI (admin, ...) pour l'accès au processeur de service (FSP et eBMC)
  - Connexion HMC (Passw0rd) pour l'accès d'une HMC au serveur
  - Console HMC (hscroot / abc123) pour l'accès à la console HMC
  - Baies de disques (admin / passw0rd!) pour l'accès aux contrôleurs des baies de disques
  - Librairies de bandes (admin / passw0rd!) pour l'accès à l'interface des librairies de bandes
  - QSECOFR des outils de maintenance DST (QSECOFR/QSECOFR, 11111111/11111111, ...) pour l'accès au microcode des LPAR IBM i
- **Les niveaux de firmware sont-ils à jour ?**
- **Les correctifs de sécurités (PTFs) sont ils appliqués**

Historical CVE Vulnerabilities

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NATIONAL VULNERABILITY DATABASE

Search the database at this link.

C'est vrai aussi pour
les autres environnements
du Système d'Information

Sécuriser les accès aux interfaces d'administration du stockage

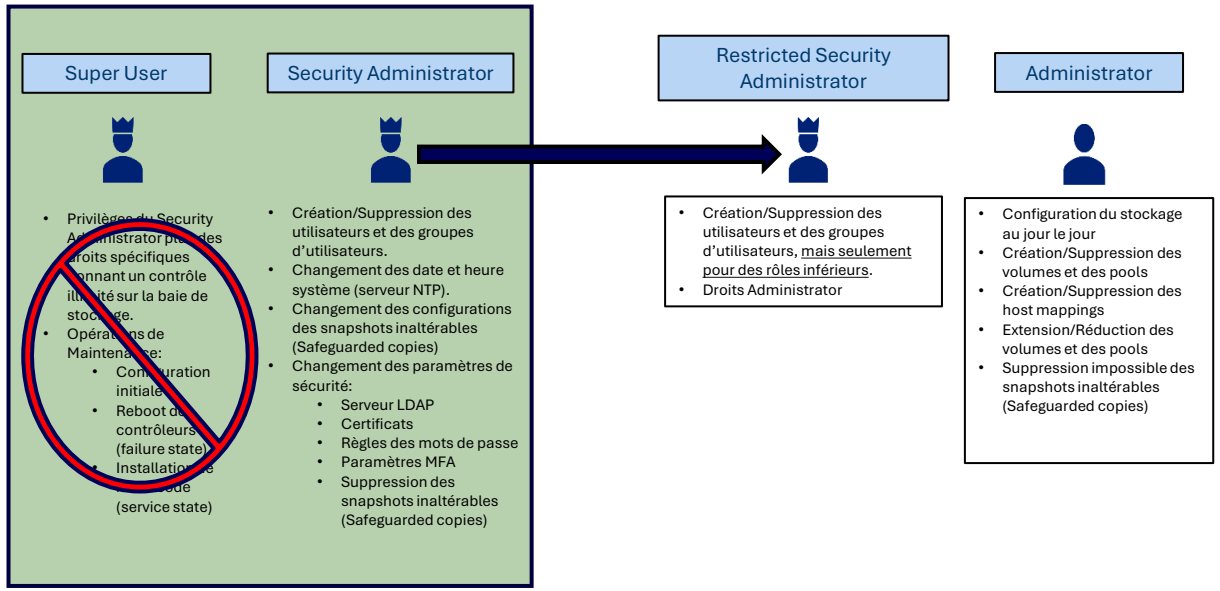
Baies de disques IBM Flashsystem

- Sécuriser les connexions sur les baies de stockage et les serveurs de sauvegarde grâce à des dispositifs de MFA (**Multi-Factor Authentification**) disponibles en standard (Depuis Virtualize 8.5.x).

- Limiter les droits Super User et Security Administrator avec la fonction **TPI (Two-Person Integrity)**

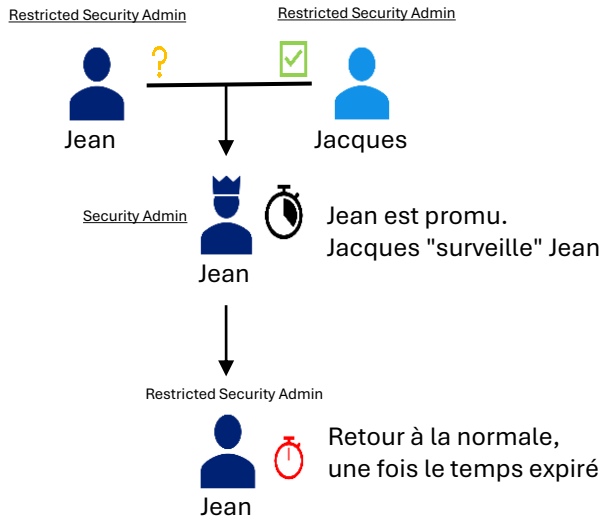
Lorsque le TPI est activé:

- Le compte Super User est verrouillé et ne peut plus être utilisé.
- Les utilisateurs de type Security Administrator ont leurs droits réduits et deviennent **Restricted Security Administrator**



Un utilisateur Restricted Security Administrator peut retrouver les privilèges du rôle **Security Administrator**

- Après accord donné par un autre utilisateur **Restricted Security Administrator**
- Pour une période donnée (entre 10mns et 24 heures).



Durcissement du système d'exploitation

Activer les sécurités du système d'exploitation IBM i

- Valeurs systèmes :
  - QSECURITY : 30 ou 40 minimum
  - QLMTSECOFR : conserver la valeur livrée, 1
- Politique de mot de passe :
  - QPWDCHGBLK Block password change
  - QPWDEXPITV Password expiration interval
  - QPWDEXPWRN Password expiration warning
  - QPWDLMTAJC Limit adjacent digits in password
  - QPWDLMTCHR Limit characters in password
  - QPWDLMTREP Limit repeating characters in password
  - QPWDLVL Password level
  - QPWDMAXLEN Maximum password length
  - QPWDMINLEN Minimum password length
  - QPWDPOSDIF Limit password character positions
  - QPWDRQDDGT Require digit in password
  - QPWDRQDDIF Duplicate password control
  - QPWDRULES Password rules
  - QPWDVLDPGM Password validation program

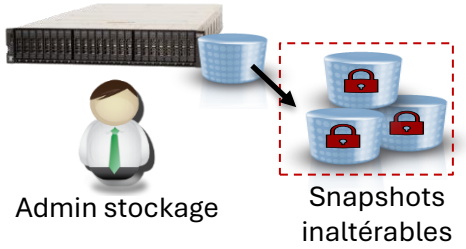
- Gestion des droits :
  - Compte *ALLOBJ
  - Droit *PUBLIC
  - Création de liste d'autorisation
  - Partages et droits IFS

- Chiffrage des flux 5250, FTP, ODBC, Kerberos,
- Activation SSO / EIM

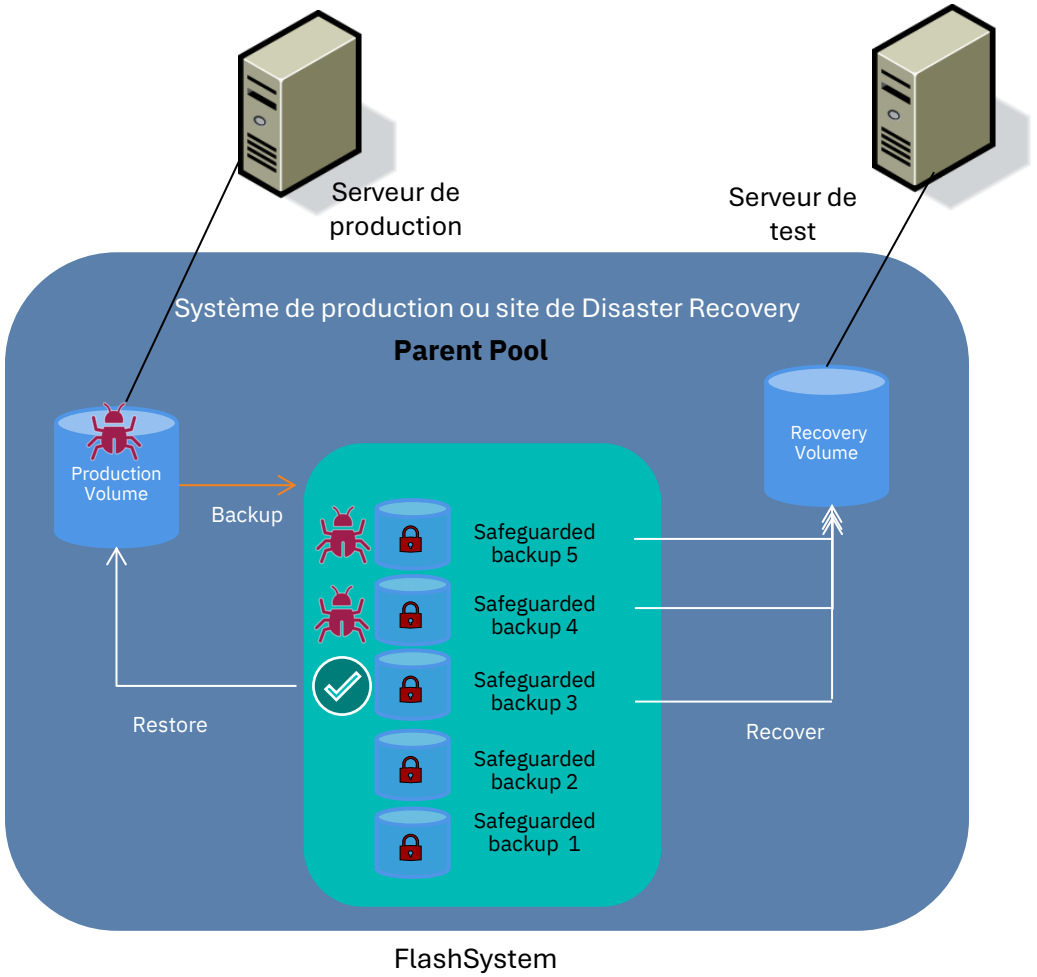
C'est aussi nécessaire pour les autres environnements du Système d'Information

Sauvegarder et protéger les données

Snapshots inaltérables sur baie de disques

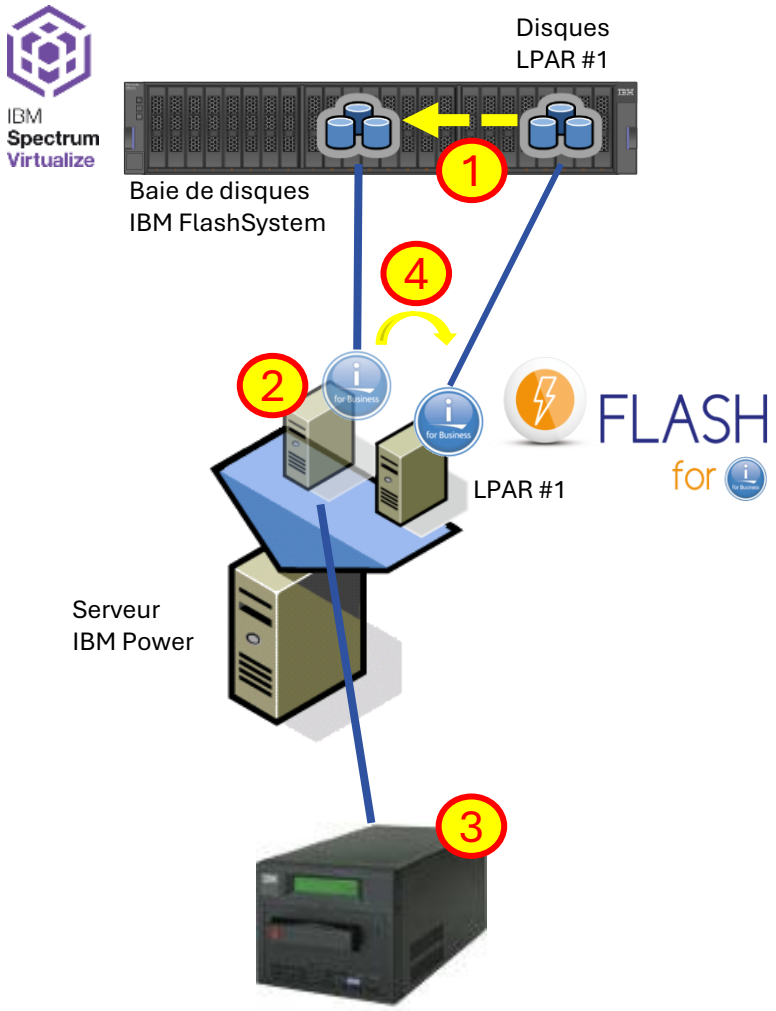


- Depuis Juillet 2021, IBM Virtualize intègre la fonction « Safeguarded FlashCopy », des copies inaltérables des données de production.
- Les copies SGC sont prises à intervalle régulier.
- Elles ne peuvent être altérées ou supprimées par un administrateur de stockage.
- **Ce sont des snapshots inaltérables.**



Sauvegarder et protéger les données

Snapshots automatisés / Sauvegarde sans interruption de service



Principe :
Créer un clone temporaire d'une partition via un snapshot du stockage
Exécuter la sauvegarde sur le clone en « temps masqué »

Flash4i exécute automatiquement :

0. Appel de la fonction QUIESCE
1. Déclenchement du flashcopy « nocopy »
   (Seules les données modifiées prennent de la place)
2. Création d'une partition clone
3. Sauvegarde du clone en « temps masqué »
4. Envoi des logs de sauvegarde sur LPAR #1
5. Suppression ou arrêt du clone

Remarques :

- Le clone est créé instantanément via IBM Snapshot
- Le clone est indépendant de la LPAR de production
- Aucun impact sur la production
- Avec ou sans BRMS (pas besoin de revoir le logiciel de sauvegarde
- Sauvegarde sur LTO ou VTL (ce qui est configuré sur la production)

Sauvegarder et externaliser les données

Offre bandes IBM LTO, du simple lecteur à la librairie

Lecteur simple
IBM TS22x0

Lecteur simple ou double
montage en rack via MME

Autoloader IBM TS2900
1 lecteur – 9 bandes

Figure 1. Base Module 3555-L3A

Figure 2. Expansion Module3555-E3A

Librairie IBM TS4300
1 à 3 lecteurs – 30 bandes

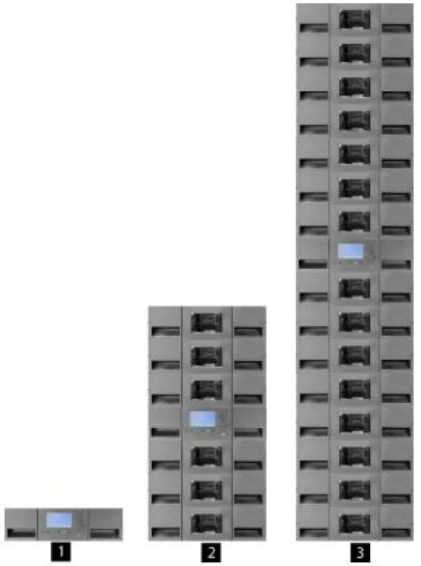


Figure 3. Configuration comparison

Librairie IBM TS4300
48 lecteurs – 640 bandes

- Immuabilité des sauvegardes, c'est-à-dire sortir la bande de la librairie
- Chiffrement des données sur bande :
  - Directement à partir d'IBM i (5770-SS1 option 35 : CCA Cryptographic Service Provider)
  - Depuis BRMS
  - Depuis le lecteur de bande (hors lecteur simple)
- Librairies de sauvegarde virtuelles (VTL)
  Dell DataDomain, IBM FalconStor

  - Externalisation automatique et électronique des sauvegardes via réplication (2 VTL, 2 sites)
  - Immuabilité des sauvegardes via fonction logicielle
  - Chiffrement des données via fonction logicielle

Utilisable pour tout environnement

Détecter les comportements anormaux

Focus sur la détection de Ransomware

FlashCore: Coopération étroite entre IBM et Micron. Développements conjoints

Micron + IBM

FLASHCORE MODULE 4

RANSOMWARE THREAT DETECTION

- Parmi les différentes méthodes de détection de la présence de malware (Cryptolocker, Ransomware), IBM propose en standard la détection sur changement de comportement des données (**via la console Storage Insights Pro**) :
  1. Détection d'une évolution anormale (à la baisse) du taux de compression des données
  2. Détection de cyber attaque par le dispositif RTD (Ransomware Threat Detection)

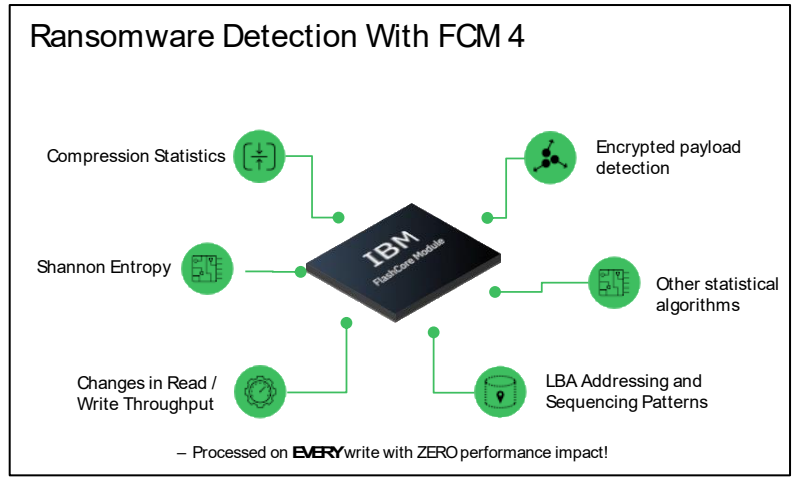
- Les baies de disques IBM (depuis Virtualize 8.6.0) intègrent **RTD SW** (Ransomware Threat Detection Software) : Les contrôleurs analysent une écriture sur cent. Les alertes remontent via la console Storage Insights Pro, puis peuvent être transmises à un SIEM/SOAR.

Stockage mutualisable pour tous les environnements

Disque FCM4

Compression / Chiffrement / Ransomware Detection

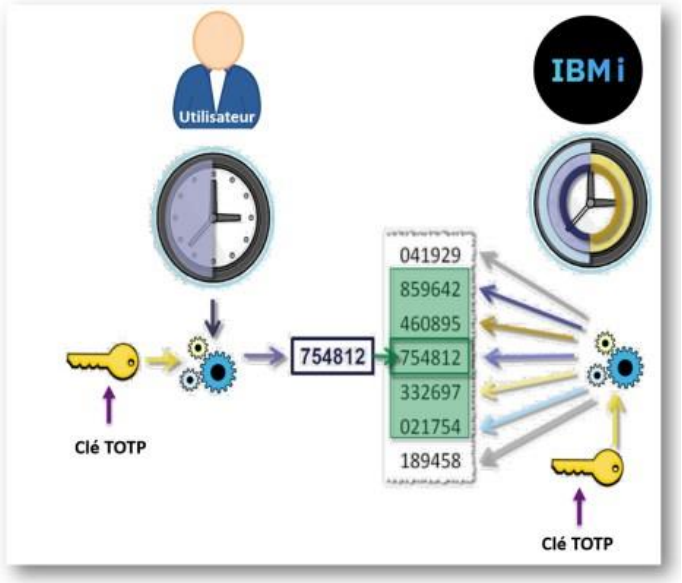
- Les modules FCM4 ont été annoncé par IBM en avril 2024 et intègrent le **RTD HW** (Ransomware Threat Detection Hardware). Toutes les écritures sont analysées directement par chaque module FCM4 (nécessite Virtualize 8.6.3 ou +). La détection est réalisée au niveau de chaque volume et les alertes remontent via la console Storage Insights Pro, puis peuvent être transmises à un SIEM/SOAR.

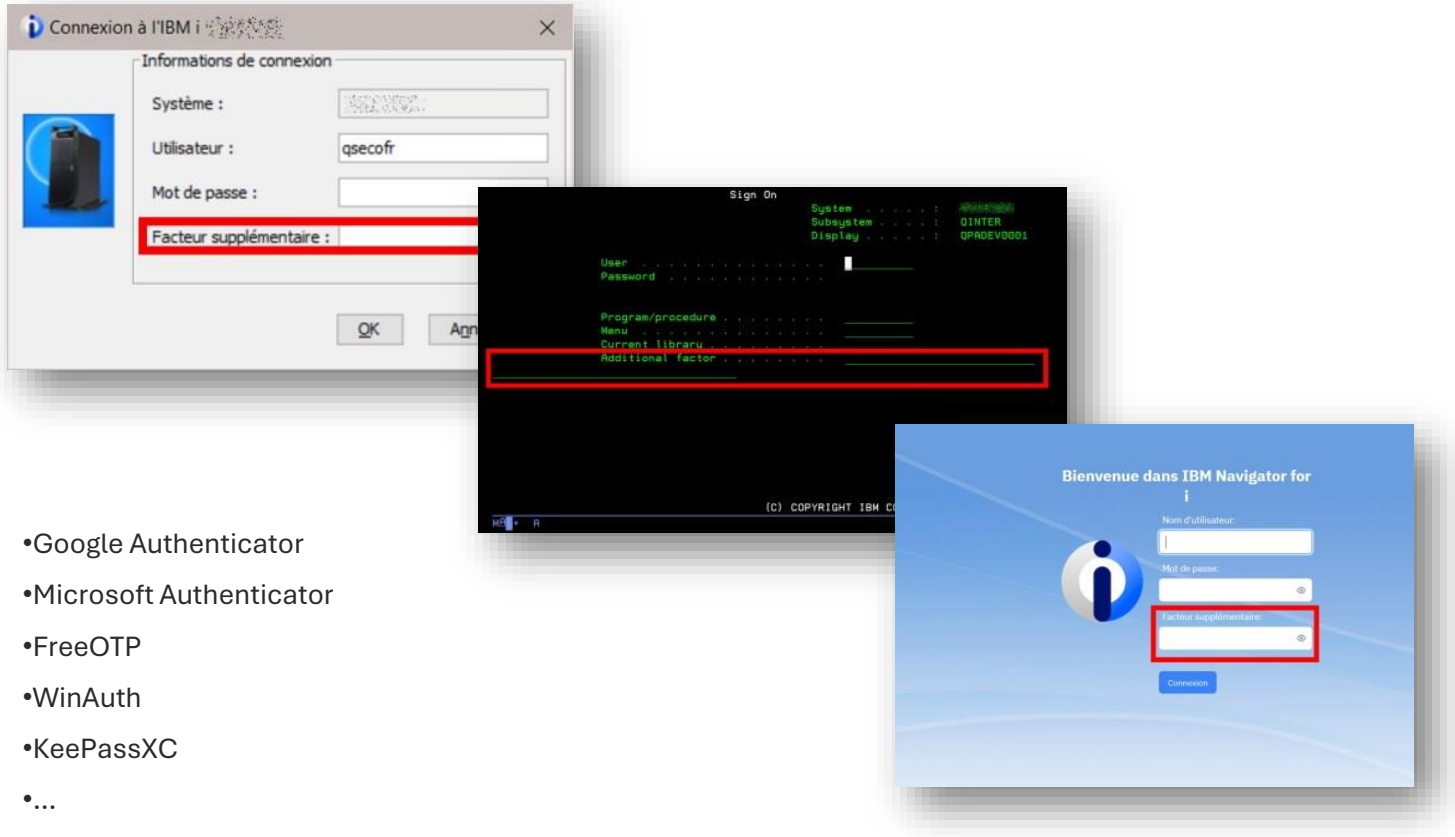


IBM i V7R6, premier OS intégrant le MFA

Une version orientée sécurité

- MFA (Multi-Factor Authentication) intégré de base dans le système d'exploitation et basé sur des mots de passe à validité limitée dans le temps (Protocole TOTP : Time-based One-Time Password)





- Google Authenticator
- Microsoft Authenticator
- FreeOTP
- WinAuth
- KeePassXC
- ...

Ce qu’il faut retenir

Le constat

- Le paradoxe : l'IBM i héberge les applications critiques, sa sécurité est souvent laissée de coté
- La sécurisation de l’IBM i doit être intégrée dans la sécurisation globale du SI (Mutualiser)

Le plan d’action

1. Sécuriser les consoles d’administration (ASMI, HMC, baie de disques, …)
2. Durcir les systèmes d’exploitation (utiliser les nombreuses possibilités de l’IBM i intégrée en standard)
3. Activer une politique de mot de passe globale (SYSVAL QPWD*) et/ou SSO
4. Mettre l’accent sur la sécurité des données (Sauvegarder, externaliser, chiffrer, répliquer vers le cloud, …)
5. Mettre en place des moyens de détection rapides (Détection des comportement anormaux sur les données, …)

Les avantages de l’IBM i

- Profiter de la V7R6 avec toutes les améliorations sur la sécurité (MFA, …)

4

Notre savoir faire

Nos services

heliaq

for Business

Notre équipe pour vous accompagner

Une équipe certifiée IBM

IBM Gold Partner

+ de 20 collaborateurs spécialisés IBM Power sur l'ensemble des agences

10 partenaires

IBM GOLD France

Notre savoir faire pour vous accompagner

INFRASTRUCTURES

- Configuration IBM Power 10
- Upgrade Matériels
- Partitionnement
- Stockage

CLOUD, SERVICES MANAGES

- Maintien en Condition Opérationnelle MCO / MACO
- PCA / PRA
- LPAR de Test / Dèv / Prod
- LPAR de Consultation

SERVICES

- Audit Consulting
- Installation On Premise
- Montée de version / PTF
- Développement TMA

CYBERSÉCURITÉ

+ de 25 collaborateurs spécialisés Cybersécurité

5 Services pour sécuriser vos infrastructures avec le cloud et les services managés

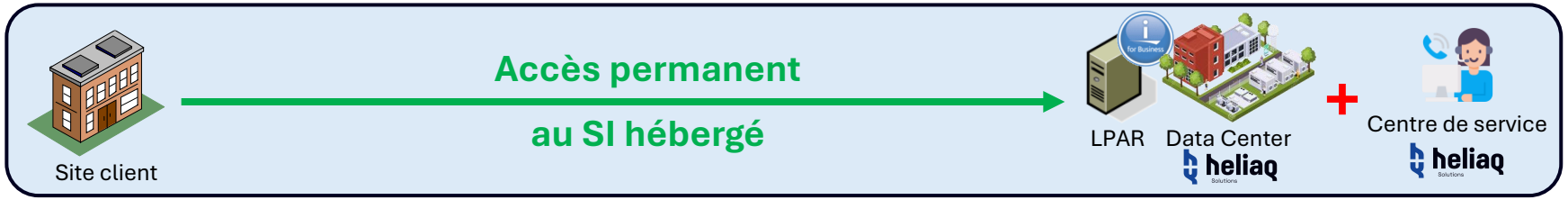
1/ Service Power **SM**
Services **M**anagés On-Premise

2/ Service Power **BK**
Back**k**up as a Service
(BaaS)

3/ Module Power **DR**
Disaster **R**ecovery as a Service
(DRaaS)

4/ Module Power **PRA**
PRA as a Service
(PRAaaS)

5/ Module Power **Cloud**
Move to **Cloud**
(M2C)



Cycle d'une TMA opérationnelle RPG / GAP (CTO400)

Start PDM / RDI / VSCODE

1ère Phase (Acquisition du périmètre)

Quelques jours / mois

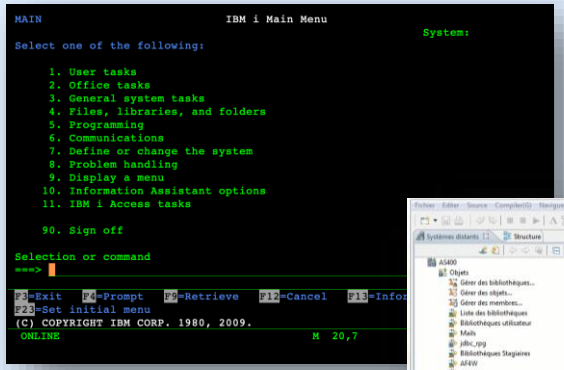
2ème Phase (Développement en //)

Refresh 1 à 2 fois / mois

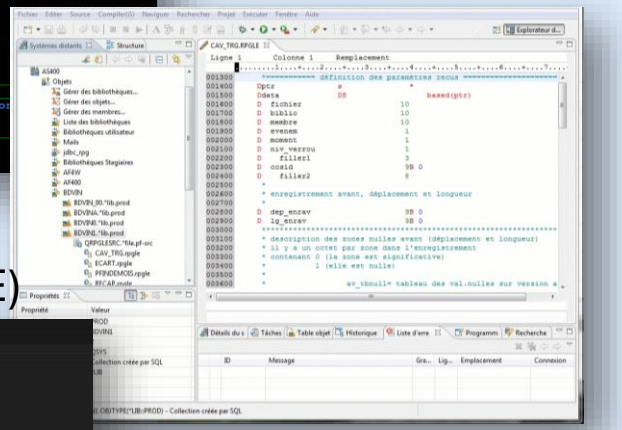
3ème Phase (Point trimestriel)

Développements commentés
Supports orientés techniques
Notices utilisateurs et process

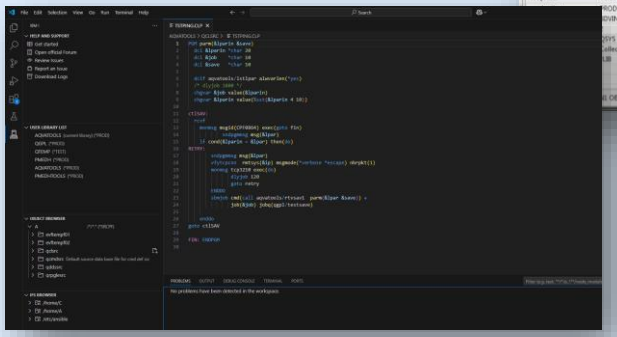
RPG/GAP (avec PDM)



RPG/GAP (sous RDI)



RPG/GAP (sous VSCODE)



Ou développement One Shot

CDC Obligatoire
Recettage
Delivery

Notre offre Heliaq for IBM i

Une offre complète à 360°

1. Cloud :

- ✓ Privé
- ✓ Souverain
- ✓ Public chez IBM
- ✓ Hybride

2. Projets On-Premise :

- ✓ Services managés, MCO
- ✓ Refresh Technologique
- ✓ MAJ PTF's
- ✓ Accompagnement sur mesure

3. Services managés :

- ✓ Montée de version
- ✓ Installation de correctifs
- ✓ Partition IBM i Mono ou Dual DC
- ✓ Audit de performances
- ✓ Assistance technique / TMA

- ✓ Haute disponibilité applicative ou matérielle
- ✓ Sauvegarde mutualisée
- ✓ PRAaaS, BaaS
- ✓ MCO des partitions IBM i
- ✓ MCO applicatif : IKOS (Erp immobilier)

MERCI !

heliaq