Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

S75 - Changement de version 7.4/7.5 vers 7.6
Comment ne pas se tromper ?

20 novembre 13:45 - 14:45

Laurent MERMET
IBM France
laurent.mermet@ibm.com

Ludovic MENARD
IBM France
ludovic_menard@fr.ibm.com

LM²

IBM

common FRANCE

Agenda

- ✓ Introduction
- ✓ Préparation et recommandations
- ✓ Fonctions supprimées en 7.6
- ✓ Post-migration
- ✓ Niveau de Sécurité 40 impératif
- ✓ Nouveautés 7.6 – sécurité
- ✓ Nouveautés 7.6 – autres évolutions
- ✓ Questions/Réponses

Power Week

18 -19 - 20 novembre 2025

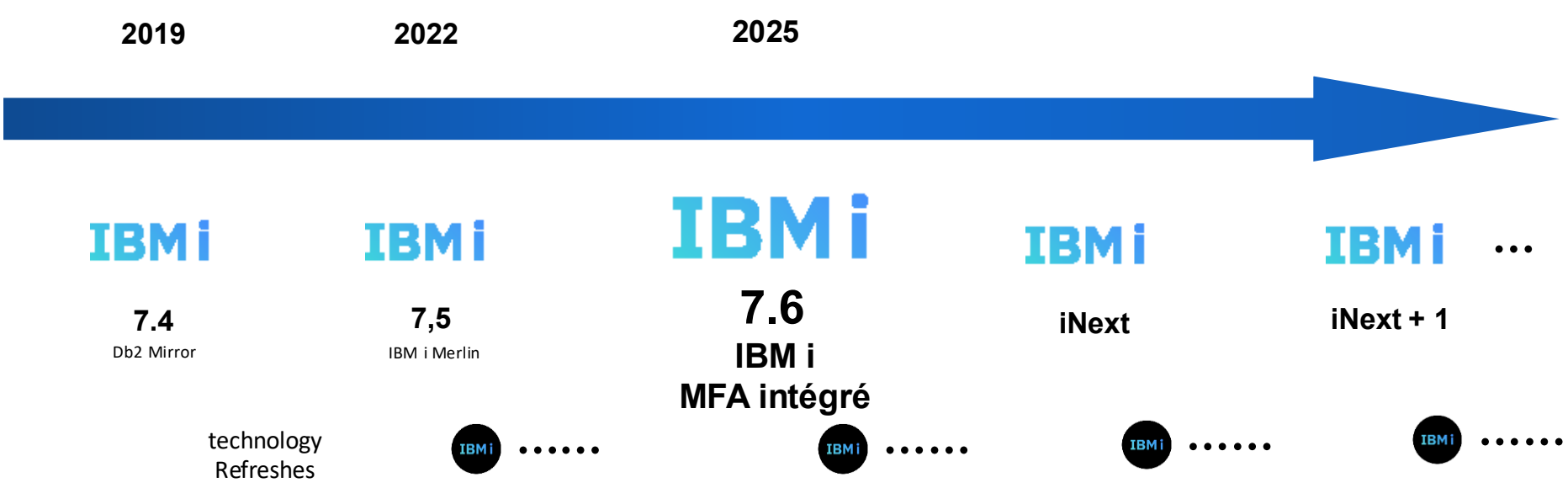
IBM common FRANCE

IBM

Introduction

Feuille de route IBM i

Annonce : 8 avril



** Toutes les déclarations concernant l'orientation et l'intention futures d'IBM sont susceptibles d'être modifiées ou retirées sans préavis et ne représentent que des buts et des objectifs.

** Les flèches indiquent un « état en cours » et n'impliquent aucune date spécifique.

IBM i 7.6 Restez en sécurité. Restez innovant.

Sécurité

- ✓ L'authentification multifacteur intégrée (MFA) améliore la sécurité contre les ransomwares
- ✓ Simplifiez le respect de la conformité réglementaire grâce à une authentification avancée et une nouvelle protection des profils utilisateur
- ✓ Réduire encore les coûts et améliorer le coût total de possession (TCO)

Administration du système

- ✓ Navigator for i a été entièrement mis à jour pour prendre en charge l'authentification multifacteur
- ✓ Les informations et les avertissements d'expiration de licence sont désormais inclus dans le tableau de bord multisystème principal
- ✓ Ajoutez et supprimez dynamiquement des ports membres dans une agrégation de liens Ethernet sans nécessiter de panne de communication

Base de données

- ✓ Le code pour l'extension IBM i Db2 for i a amélioré la validation de la syntaxe SQL et l'intégration avec les plates-formes GenAI
- ✓ Les avancées SQL permettent l'open source, l'automatisation des systèmes et la surveillance de la sécurité
- ✓ Prise en charge de FINAL TABLE et OLD TABLE pour fournir aux programmeurs SQL de nouvelles fonctionnalités

Développement d'applications

- ✓ Compilation basée sur Git et débogage amélioré qui permet des méthodologies et des techniques de développement modernes
- ✓ Langages supplémentaires pris en charge dans Code for IBM i pour étendre la portée mondiale des développeurs
- ✓ Offre aux développeurs des choix d'algorithmes plus sécurisés pour protéger les informations d'identification et les données des applications

Power Week

18 -19 - 20 novembre 2025

IBM

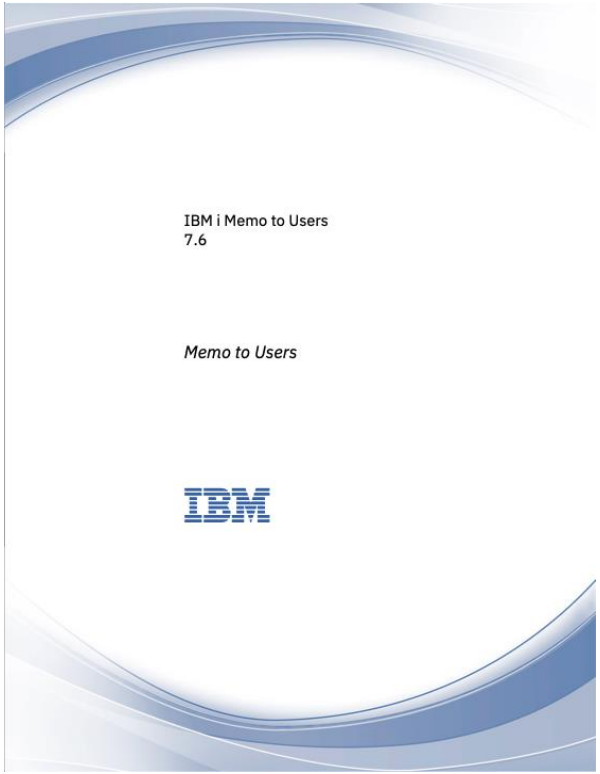
common FRANCE

IBM

Préparation et recommandations

Préparation et recommandations

- **A lire en premier**
  - ✓ Memo to Users 7.5
    - ✓ https://www.ibm.com/docs/en/ssw_ibm_i_75/rzaq9/rzaq9.pdf
  - ✓ Memo to Users 7.6
    - ➢ https://www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf



Installing IBM i 7.6 over IBM i 7.4

If you are installing IBM i 7.6 over IBM i 7.4, you should also read the *IBM i Memo to Users* for IBM i 7.5. It contains incompatibility-related information about the new functions and enhancements incorporated in IBM i 7.5 and IBM i 7.6.

You can also view the IBM i 7.5 *IBM i Memo to Users* in IBM Docs under the IBM i 7.5 release :

https://www.ibm.com/docs/en/i/7.5?topic=documentation-memo-users

Préparation et recommandations

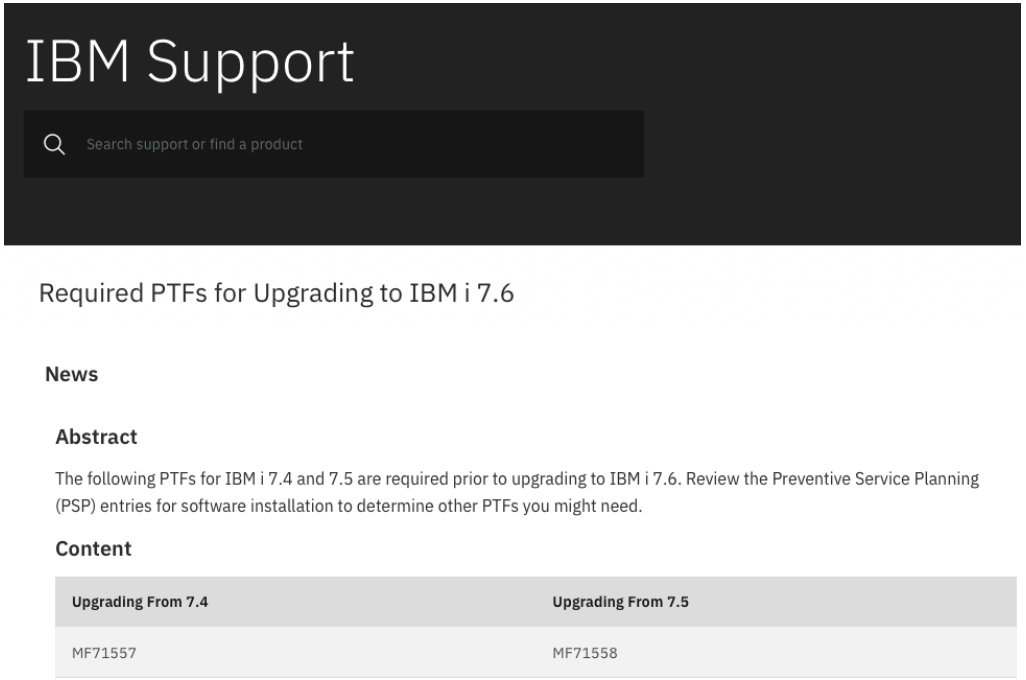
- **Vérifiez la compatibilité matérielle et logicielle**
  - ✓ Power10 minimum ou ultérieur pour l'IBM i 7.6
  - ✓ HMC version 10 ou supérieur
  - ✓ VIOS à mettre à jour pour la compatibilité Power10 et IBM i 7.6
  - ✓ Les disques de type D910 ne sont plus supportés.
  - ✓ Le PPP, IKEv1 et certains WAN ne sont plus supportés

	Enhancement Landing Pages
IBM i 7.6	TR1 - Base Enhancements
IBM i 7.5	TR7 - TR6 - TR5 - TR4 - TR3 - TR2 - TR1 - Base Enhancements
IBM i 7.4	TR12 - TR11 - TR10 - TR9 - TR8 - TR7 - TR6 - TR5 - TR4 - TR3 - TR2 - TR1 - Base Enhancements
IBM i 7.3	TR13 - TR12 - TR11 - TR10 - TR9 - TR8 - TR7 - TR6 - TR5 - TR4 -TR3 - TR2 -TR1 - Base Enhancements
IBM i 7.2	TR9 - TR8 - TR7 - TR6 - TR5 - TR4 - TR3 - TR2 - TR1 - Base Enhancements

IBM i Technology Updates
https://www.ibm.com/support/pages/node/1119129/

Préparation et recommandations

- **Identifiez et appliquez les PTFs requises**
  - ✓ https://www.ibm.com/support/pages/node/7176506
    - ✓ PTFs pour préparer l'installation et/ou les médias virtuels pour la mise à jour
  - ✓ MF71557 : 7.4
  - ✓ MF71558 : 7.5



Préparation et recommandations

- ✓ Lister tous les profils *ALLOBJ, *SECADM, *IOSYSCFG, *AUDIT, *SERVICE
- ✓ Lister les profils inactifs ou non utilisés depuis 90 jours
- ✓ Vérifier la complexité des mots de passe (ANZDFTPWD, ANZUSRPRF)
- ✓ Identifier les objets publics mal sécurisés
- ✓ Vérifier les autorisations spéciales (DSPAUTUSR)
- ✓ Lister les exit programs actifs (WRKREGINF, WRKREGEXIT)
- ✓ Vérifier l'usage de connexions non chiffrées (FTP, Telnet, etc.)
- ✓ Capturer les valeurs de sécurité actuelles : DSPSECA
- ✓ Sauvegarder QAUDJRN (si activé)
- ✓ Vérifier QPWDLVL, QPWDRULES, QPWDMAXLEN, QMAXSIGN, QLMTSECOFR

Préparation et recommandations

- **Renforcer les droits d'accès et les autorités**
  - ✓ De nombreuses commandes et API nécessitent désormais des droits supplémentaires, notamment *IOSYSCFG ou QIBM_IOSYSCFG_VIEW, pour accéder à des valeurs système, des attributs réseau ou certaines vues SQL sensibles (ex : QSYS2.SECURITY_INFO)

- **Profils utilisateur système**
  - ✓ IBM i 7.6 introduit de nouveaux profils utilisateur système (par exemple, QPGMR_NC) et modifie la manière dont l'autorité est gérée pour certains profils existants (QPGMR, QSECOFR, QSYSOPR, QUSER). Vérifiez les dépendances et accordez les autorités nécessaires aux nouveaux profils. Certains profils obsolètes seront supprimés.
- **Java**
  - ✓ Assurez-vous d'utiliser des versions de Java supportées (par exemple, Java 8 ou Java 17). Si vous avez des applications qui dépendent de versions plus anciennes de Java (comme Java 11, qui n'est plus supporté par 7.6), vous devrez les mettre à jour ou revoir vos applications.

Préparation et recommandations

- **Supprimer les protocoles et API obsolètes**
  - ✓ Désactivez et retirez tout usage de PPP, IKEv1, et des API associées, qui ne sont plus pris en charge et présentent des risques de sécurité

- **Produits non supportés**
  - ✓ Certains produits ou fonctions ne sont plus supportés sur IBM i 7.6. Identifiez-les et planifiez leur remplacement ou leur abandon (ex : DB2 Web Query, certaines versions de GoAnywhere, CICS Transaction Server for i - pour lequel il n'y a pas de remplacement direct, l'option est de migrer vers des options natives IBM i).

- **Restreindre l'accès aux informations sensibles**
  - ✓ L'accès à certaines vues et fonctions SQL (QSYS2.SECURITY_INFO, QSYS2.ASP_INFO, etc.) est désormais limité par des droits spécifiques

Préparation et recommandations

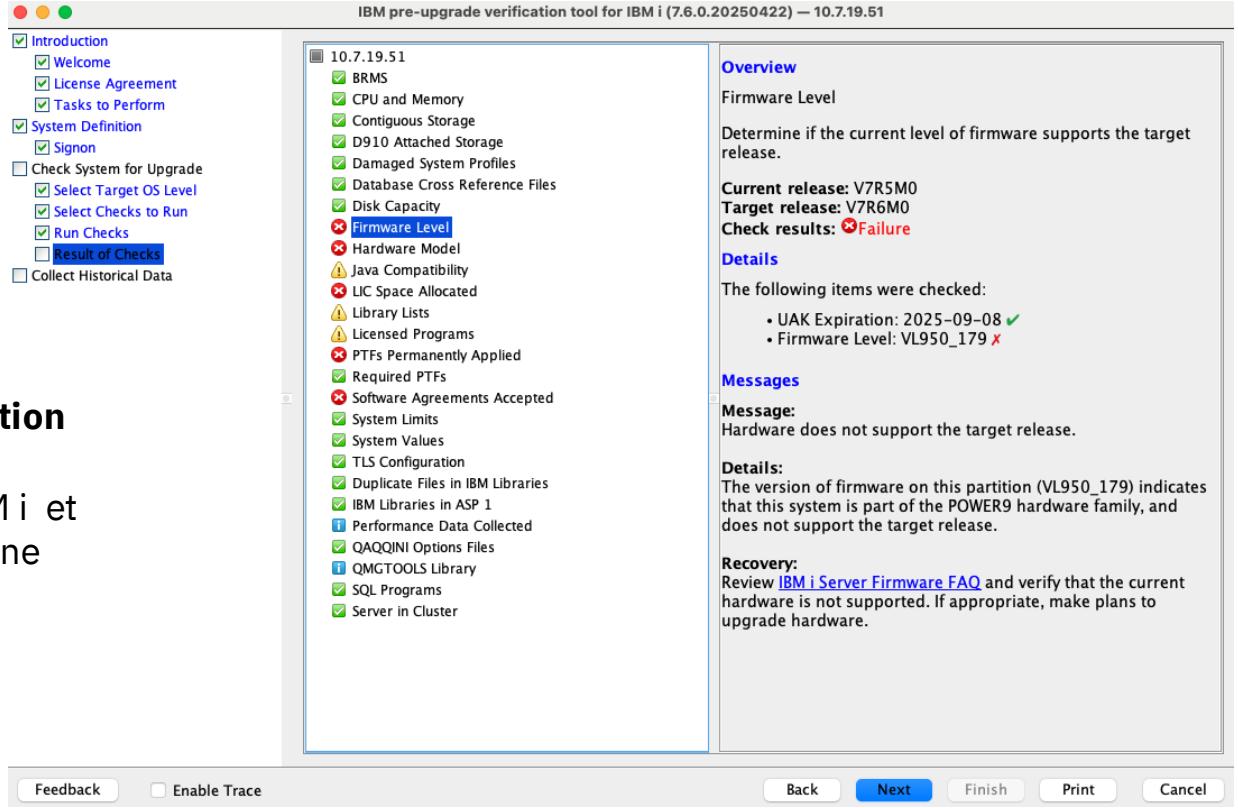
- Vérifiez l'espace disque et la taille des partitions pour répondre aux besoins de 7.6.
  - ✓ Minimum de 35 GB pour 520-byte sectors (DS8000, virtual disk with VIOS as server)
  - ✓ Minimum de 40 GB pour 512-byte sectors (SVC, Storwize, virtual disks with VIOS VSCSI)
  - ✓ Minimum de 70 GB pour Native-attached SAS/SCSI (Both 520-byte or 4K sectors)

- Sauvegardez intégralement votre système (sauvegarde complète et test de restauration)
  - ✓ SAVE 21
  - ✓ Utilisation de BRMS
  - ✓ Flashcopy
  - ✓ …

- Si vous utilisez BRMS, la licence 5770-BR1 n'est plus supportée, vous devrez passer à 5770-BR2 qui est une option par abonnement.

Préparation et recommandations

PRUV

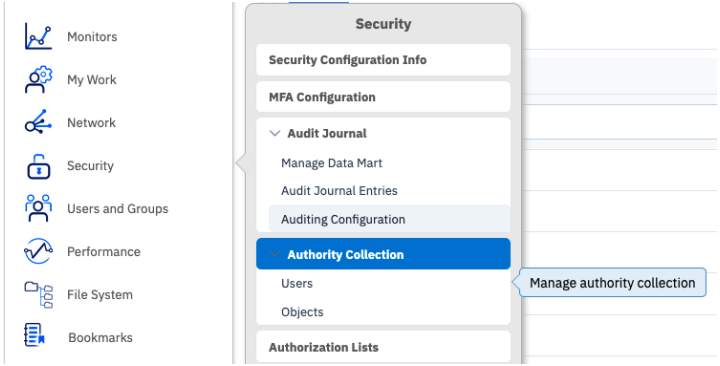


Outil IBM **PRe-Upgrade Verification**

Cet outil examine la partition IBM i et détermine si la mise à jour vers une autre version est possible.

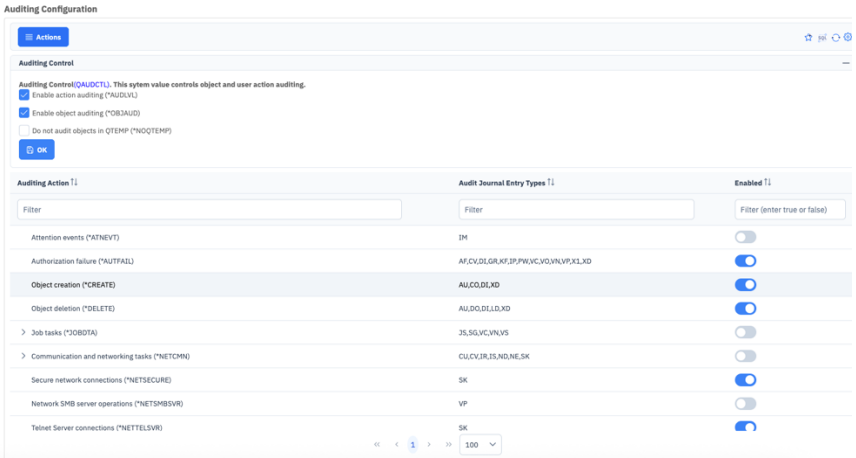
https://www.ibm.com/support/pages/ibm-pre-upgrade-verification-tool-ibm-i

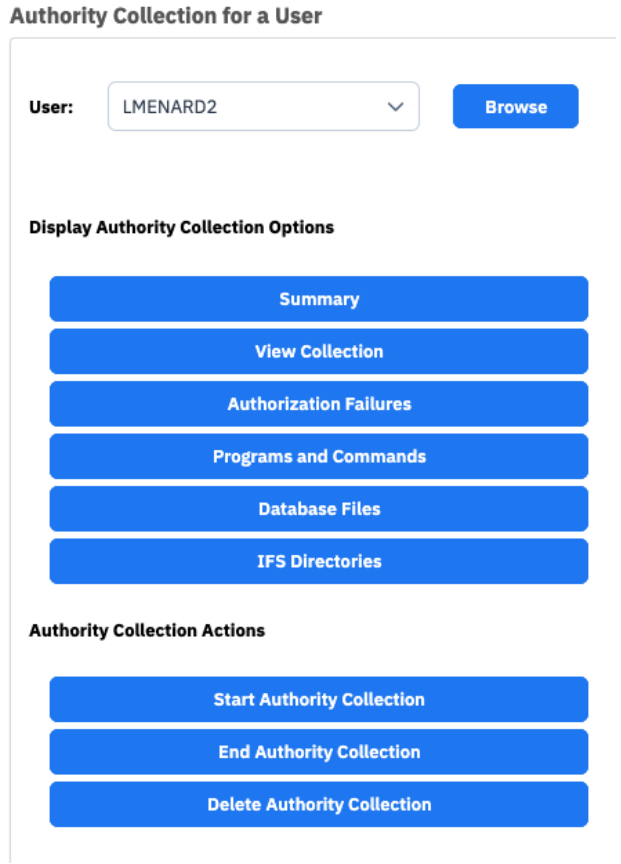
Préparations et recommandations



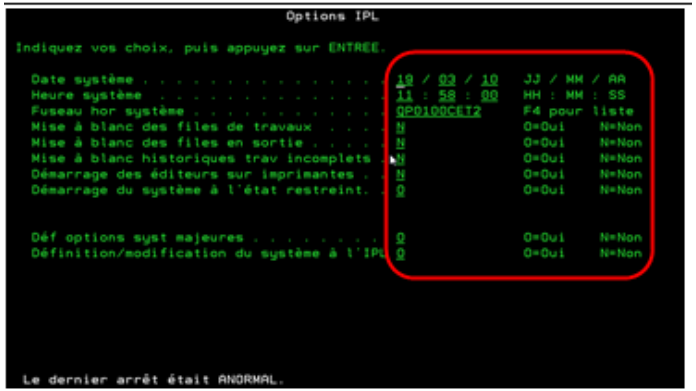
Audit de sécurité

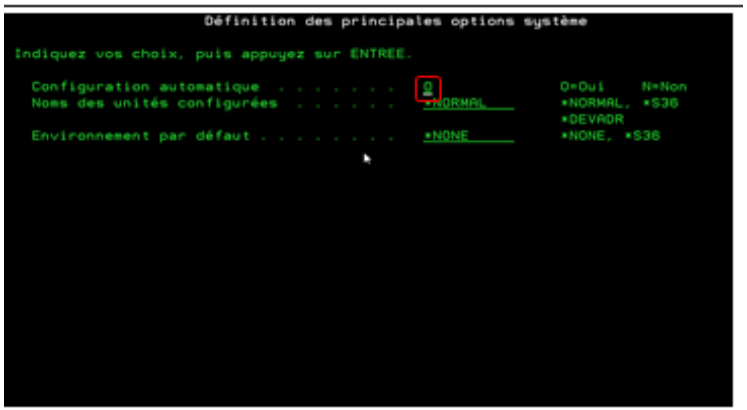
- Profils
- Objects

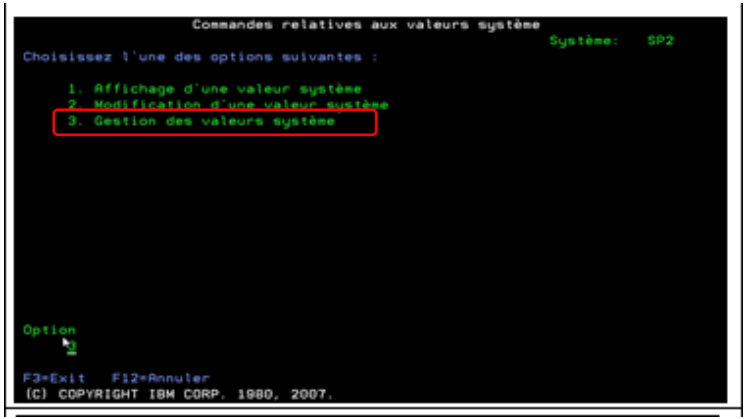




Les options au 1er IPL







Et les valeurs systèmes

- ✓ QALWOBJRST to *ALL
- ✓ QFRCCVNRST to 0
- ✓ QIPLTYPE to 2
- ✓ QINACTITV to *NONE
- ✓ QJOBMSGQFL to *PRTWRAP
- ✓ QJOBMSGQMX to 64
- ✓ QLMTDEVSSN to 0
- ✓ QLMTSECOFR to 0
- ✓ QMAXSIGN to *NOMAX
- ✓ QPFRADJ to 2
- ✓ QPWDEXPITV to *NOMAX
- ✓ QSCANFSCTL add *NOPOSTRST
- ✓ QVFYOBJRST to 1

QSECURITY à la valeur du système à restaurer
QPWDLVL à la valeur du système à restaurer

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

IBM

Fonctions IBM i supprimées en 7.6

Produits supprimés

Fonctions IBM i	Option de produit	Produit de remplacement
Bootstrap Protocol (BOOTP) server	Option de base 5770-SS1	Une fonction de remplacement est le serveur DHCP Kea développé par l'Internet Systems Consortium (ISC). D'autres produits sont disponibles.
Native Dynamic Host Configuration Protocol (DHCP) server	Option de base 5770-SS1	Une fonction de remplacement est le serveur DHCP Kea développé par l'Internet Systems Consortium (ISC). D'autres produits sont disponibles.
Remote Authentication Dial In User Service (RADIUS)	Option de base 5770-SS1	Aucun
Domain Name System (DNS) Server	IBM i (5770-SS1) option 31	Il existe de nombreux serveurs DNS externes disponibles sur le marché qui peuvent être exploités.
Route Daemon (RouteD)	Option de base 5770-SS1	OMPROUTED d'IBM i est une alternative à RouteD. OMPROUTED prend en charge les protocoles de routage RIP, RIP nouvelle génération (RIPng) pour IPv6, ainsi que OSPF (Open Shortest Path First).
Virtual Private Network (VPN) Internet Key Exchange version 1 (IKEv1) protocol	Option de base 5770-SS1	La solution de remplacement plus moderne et plus sécurisée d'IBM i est le protocole VPN IKEv2.
IP Payload Compression protocol (IPComp)	Option de base 5770-SS1	IPComp est pris en charge avec IKEv1, mais pas avec IKEv2. Comme IKEv1 est en cours de retrait, IPComp est également supprimé.
Quality of Service (QoS) Server	Option de base 5770-SS1	Aucun

Produits supprimés

Fonctions IBM i	Option de produit	Produit de remplacement
FAX (IBM Facsimile Support for i)	5798-FAX	CloudFax de International Presence FastFax de Fresche Solutions BlueSeries Fax de System & Method A/S Ce ne sont toutefois pas les seuls produits de remplacement disponibles. D'autres entreprises peuvent également proposer des solutions offrant une fonction de fax.
FRCA (Fast Response Cache Accelerator) for HTTP Server	Option de base 5770-SS1	Le serveur HTTP IBM pour i (basé sur Apache) dispose de plusieurs options de mise en cache intégrées.
Performance Graphics	Option Performance Tools for i (5770-PT1)	Navigator for i
Performance Advisor	Option de Performance Tools for i (5770-PT1)	Aucun
Graphical Data Display Manager (GDDM)	IBM i (5770-SS1) option 14	Aucun
OptiConnect	IBM i (5770-SS1) option 23	L'utilisation principale d'OptiConnect est de permettre à ObjectConnect (une autre option installable du produit 5770-SS1) de fonctionner via OptiConnect virtuel. Une alternative consiste à exécuter ObjectConnect sur IP avec TLS (Transport Layer Security).
Binary Synchronous Communications (Bisync) protocol	Option de base 5770-SS1	Aucun
Point to Point Protocol (PPP) and Layer 2 Tunneling Protocol (L2TP)	Option de base 5770-SS1	Aucun

Produits supprimés

Fonctions IBM i	Option de produit	Produit de remplacement
Retait progessif de certains outils dans IBM Rational Development Studio for i RLU, SDA, FCMU, APF, CGU, DFU	Rational Development Studio for i (5770-WDS) option 21	Il existe plusieurs options de remplacement, notamment Rational Developer for i, Code for i, et d'autres.
Business Graphics Utility	5761-DS2	Il existe plusieurs options de remplacement, notamment Rational Developer for i, Code for i, ainsi que d'autres.
IBM Technology for Java 11 64bit	5770-JV1 option 19	Utilisez des versions de Java prises en charge, telles que Java 8 ou Java 17.
Management Central	Fait parti du système d'exploitation	Le seul accès à Management Central se fait via Access for Windows, qui n'est plus pris en charge depuis avril 2019.
IBM Universal Manageability Enablement	5770-UME	Aucun
CICS Transaction Server for i	5770-DFH	I n'existe pas de remplacement direct pour IBM CICS Transaction Server pour i. La meilleure option consiste à migrer vers des solutions natives d'IBM i, telles que les commandes CL, les API RESTou d'autres applications personnalisées.
XML Toolkit for i	5733-XT2	5733-XT2 et toutes ses options sont hors service depuis septembre 2023. Parmi les produits de remplacement pour XML Toolkit for i, on trouve le support XML de IBM Db2 for i, noxDB et eXpat. D'autres entreprises peuvent également proposer des solutions offrant une fonctionnalité équivalente à XML Toolkit for i.
Licence sans expiration pour IBM Backup, Recovery and Media Services for i	5770-BR1	Utiliser5770-BR2.

Post-migration

Recommandations post-migration

- ✓ Régler QPWDLVL et configurer QPWDRULES
- ✓ Activer et configurer l'audit système QAUDCTL / QAUDLVL
- ✓ Configurer un MFA si pertinent
- ✓ Restreindre les profils *ALLOBJ
- ✓ Forcer TLS 1.2+ pour les connexions réseau
- ✓ Désactiver les services non utilisés
- ✓ Sécuriser les objets critiques (BDD, programmes)

Suivi et surveillance continue

- ✓ Mettre en place une revue mensuelle des journaux QAUDJRN
- ✓ Planifier un audit sécurité annuel avec un outil spécialisé
- ✓ Intégrer IBM i dans un SIEM
- ✓ Automatiser des alertes critiques

Power Week

18 -19 - 20 novembre 2025

Niveau de Sécurité 40 impératif

Niveau de Sécurité 30

- **Sécurité d'ouverture de session et de ressources**
  - ✓ **Philosophie :** Ce niveau se concentre sur l'authentification des utilisateurs et le contrôle d'accès aux objets du système (programmes, fichiers, bibliothèques, etc.). L'idée est que chaque utilisateur doit avoir un profil et un mot de passe valides, et doit avoir des autorisations spécifiques pour accéder aux ressources.
  - ✓ **Fonctionnalités clés :**
    - **Authentification par mot de passe :** Les utilisateurs doivent s'authentifier avec un ID utilisateur et un mot de passe valides.
    - **Sécurité des objets :** Le système applique les autorisations définies sur les objets. Par exemple, si un utilisateur n'a pas l'autorité *READ sur un fichier, il ne pourra pas le consulter.
    - **Autorités spéciales :** Seuls les profils créés avec la classe de sécurité *SECOFR (administrateurs de sécurité) se voient attribuer automatiquement l'autorité spéciale *ALLOBJ (accès à tous les objets). Pour les autres utilisateurs, les autorisations doivent être accordées explicitement.

Niveau de Sécurité 30

- **Limites et risques**
  - ✓ **Vulnérabilités d'intégrité :** C'est la lacune majeure du niveau 30. Il ne fournit pas de protection d'intégrité du système d'exploitation. Un programmeur ou un opérateur ayant des connaissances avancées, et potentiellement de "mauvaises intentions", peut contourner la sécurité des ressources et élever ses privilèges, voire obtenir l'autorité *ALLOBJ.
  - ✓ **Appels directs à des interfaces non documentées :** Le système n'empêche pas les tentatives d'appels directs à des programmes système qui ne sont pas des interfaces documentées et sécurisées. Cela ouvre la porte à des manipulations internes non autorisées.
  - ✓ **Vulnérabilité des descriptions de travail (Job Descriptions) :** Un utilisateur pourrait potentiellement soumettre un travail en utilisant une description de travail qui spécifie un profil utilisateur différent (avec des privilèges plus élevés) s'il a suffisamment d'autorité sur cette description de travail.
  - ✓ **Accès direct aux blocs de contrôle internes :** Des programmes en état utilisateur peuvent accéder directement aux blocs de contrôle internes du système ou au contenu des objets via leur adresse. C'est une brèche majeure en termes de sécurité et d'intégrité.

Sécurité 40

- **Sécurité d'ouverture de session, de ressources et protection d'intégrité du système d'exploitation**
  - ✓ **Philosophie :** Le niveau 40 s'appuie sur le niveau 30 en ajoutant une couche cruciale de **protection d'intégrité du système d'exploitation**. Il vise à empêcher les tentatives de contournement des mécanismes de sécurité, même par des utilisateurs très avertis. C'est le **niveau minimum recommandé** par IBM pour un environnement sécurisé.

Sécurité 40

- **Fonctionnalités clés (en plus de celles du niveau 30) :**
  - ✓ **Protection d'intégrité du système :** C'est la caractéristique principale. Le système détecte et empêche les tentatives de manipulation des composants internes du système ou de contournement des contrôles de sécurité. Les violations d'intégrité entraînent l'échec de l'opération et la génération de messages dans le journal d'audit.
  - ✓ **Prévention de l'utilisation d'interfaces non supportées :** Le système empêche les programmes d'appeler directement des programmes système qui ne sont pas des interfaces publiques et documentées. Cela limite considérablement les "points d'entrée" potentiels pour des attaques.
  - ✓ **Protection des descriptions de travail :** Le système applique des contrôles plus stricts pour empêcher qu'un utilisateur n'exécute un travail sous un profil autre que le sien, même s'il a accès à la description de travail.
  - ✓ **Protection de l'espace associé aux programmes :** L'espace associé à un objet programme (pour les programmes OPM (Original Program Model) ne peut pas être modifié directement par des programmes en état utilisateur. Pour les programmes ILE (Integrated Language Environment), cette protection est active à tous les niveaux de sécurité.
  - ✓ **Protection de l'espace d'adresse d'un travail :** Au niveau 40 (et encore plus au niveau 50), un programme en état utilisateur ne peut pas obtenir l'adresse d'un autre travail sur le système, empêchant ainsi la manipulation directe d'objets associés à d'autres travaux.
  - ✓ **Validation des paramètres :** Lorsque des paramètres sont passés entre des programmes en état utilisateur et des programmes en état système (les interfaces du système d'exploitation), ces paramètres sont rigoureusement vérifiés pour éviter que des valeurs inattendues ne compromettent l'intégrité du système.
  - ✓ **Protection matérielle améliorée du stockage :** Permet de définir des blocs d'informations système en mémoire comme lecture-écriture, lecture seule ou sans accès, renforçant l'isolement des processus.

Passage du Niveau de Sécurité de 30 à 40

- **Sécurité accrue :** Votre système devient beaucoup plus résistant aux tentatives de contournement de la sécurité et aux manipulations internes.
- **Stabilité renforcée :** En bloquant les opérations non intentionnelles ou malveillantes sur l'intégrité du système, vous réduisez les risques d'instabilité ou de plantage.
- **Conformité :** Le niveau 40 est souvent un prérequis pour de nombreuses normes de conformité (PCI DSS, HIPAA, SOX, etc.) en raison de sa protection d'intégrité.
- **Impact potentiel sur les applications non conformes :** Si vous avez des applications (surtout anciennes) qui tentent d'accéder au système d'une manière non documentée ou qui contournent les autorisations (ce qui est rare mais possible), elles pourraient commencer à échouer au niveau 40. Il est crucial de tester toutes les applications après la transition.
- **Moins de vulnérabilités connues :** Historiquement, des vulnérabilités ont été découvertes au niveau 30 qui sont automatiquement corrigées par la protection d'intégrité du niveau 40.
- En conclusion, migrer vers le niveau de sécurité 40 est une étape fondamentale et fortement recommandée pour la robustesse et la sécurité de votre environnement IBM i. C'est une protection essentielle contre les menaces internes et externes les plus sophistiquées.

Comparaison détaillée

Caractéristique	QSECURITY=30 (Sécurité d'accès aux ressources)	QSECURITY=40 (Protection d'intégrité du système d'exploitation)
Philosophie	Contrôle qui accède à quoi.	Protège le système lui-même contre les tentatives de contournement des contrôles d'accès et les manipulations internes.
Protection Intégrité OS	Faible. Un utilisateur avancé peut potentiellement contourner les autorisations.	Forte et Active. Le système détecte et bloque les tentatives de manipulation des composants internes.
Accès Interfaces Non Documentées.	Possible. Ouvre la porte aux vulnérabilités et exploits.	Bloqué. Ferme une voie majeure pour les attaques.
Contrôle Paramètres	Moins rigoureux.	Rigoureux. Valide strictement les données échangées avec le système.
Protection Mémoire	Plus faible pour les anciens programmes (OPM).	Améliorée. Protège l'espace associé aux programmes contre les altérations.
Vulnérabilité potentielle	Moyen à Élevé. Facile à exploiter pour un attaquant averti.	Faible à Moyen. Nécessite des attaques beaucoup plus sophistiquées.
Recommandation IBM	Non recommandé pour la production.	Fortement recommandé et niveau par défaut pour les nouvelles installations et la production. Essentiel pour la conformité et la stabilité.

Power Week

18 -19 - 20 novembre 2025

Nouveautés 7.6 – sécurité

MFA

- **Authentification Multi-Facteur (MFA) intégrée :**
  - ✓ C'est la nouveauté majeure. IBM i 7.6 intègre nativement la MFA directement dans le système d'exploitation.
  - ✓ Elle prend en charge les mots de passe à usage unique basés sur le temps (TOTP), compatibles avec des applications comme Google Authenticator.
  - ✓ La MFA est applicable à tous les points d'authentification, y compris les sessions "écran vert" (5250) et FTP.
  - ✓ Elle fonctionne même sans connexion Internet entre le périphérique d'authentification et IBM i, ce qui renforce la sécurité des profils critiques comme QSECOFR, même en cas de déconnexion réseau.
  - ✓ Des implémentations indépendantes de la MFA sont disponibles pour les outils de service du système (SST) et les outils de service dédiés (DST).
  - ✓ Il est possible de configurer des intervalles d'authentification MFA, par exemple, une seule authentification par jour de travail.
  - ✓ Navigator for i prend également en charge la MFA.

Profils utilisateurs

- **Améliorations de la gestion des mots de passe et des profils utilisateur :**
  - ✓ La valeur par défaut du niveau de mot de passe système (QPWDLVL) est désormais **3** pour les nouvelles installations, et la valeur par défaut des règles de mot de passe (QPWDRULES) est ***ALLCRTCHG *LMTPRFNAME *MINLEN15 *REQANY3**, encourageant des mots de passe plus robustes.
  - ✓ De nouveaux profils utilisateur système sont introduits (par exemple, QPGMR_NC, QSECOFR_NC, QSYSOPR_NC), qui sont "Non-Changeable" (non modifiables) et bénéficient des mêmes droits que leurs homologues, mais sans mot de passe par défaut et sans support MFA. Cela permet de renforcer la sécurité de ces profils système en évitant les modifications accidentelles ou malveillantes.
  - ✓ Des modifications d'autorité sont apportées à diverses commandes, vues SQL, API, services et fonctions, nécessitant des autorités spéciales accrues (*IOSYSCFG, *SECADM, et *SECOFR) et excluant l'autorité publique (*PUBLIC) pour plusieurs éléments.

Crypto et certificats

- **Cryptographie avancée :**
  - ✓ De nouvelles API cryptographiques sont prises en charge, y compris l'algorithme PBKDF-2 (Password Based Key Derivation Function 2) pour le hachage des mots de passe et ECC/SHA3.
  - ✓ **Chiffrement du pool de stockage auxiliaire (ASP) :** IBM i 7.6 permet de chiffrer l'ASP système (ASP 1), ce qui protège les données utilisateur. Cela nécessite l'option 45 du programme sous licence du système d'exploitation (Encrypted ASP Enablement) et peut être activé sans temps d'arrêt via les outils de service.
  - ✓ Les tentatives de connexion DRDA/DDM (Distributed Relational Database Architecture / Distributed Data Management) tentent d'abord d'utiliser l'algorithme de chiffrement AES, puis DES si AES n'est pas supporté.
- **Gestion des certificats et connexions sécurisées :**
  - ✓ Des améliorations sont apportées au gestionnaire de certificats numériques (DCM) pour faciliter la gestion des certificats TLS (Transport Layer Security).
  - ✓ Un nouveau serveur de connexion hôte (HCS) est introduit pour authentifier et transférer les nouvelles connexions vers d'autres serveurs hôtes, exigeant l'utilisation de TLS et de certificats numériques.
  - ✓ La commande CFGHOSTSVR permet de configurer si les connexions non sécurisées sont autorisées pour chaque serveur hôte, avec des options pour désactiver toutes les connexions non sécurisées (*SECURE), les activer toutes (*ALL), ou les autoriser uniquement sur les interfaces de bouclage (*SECLOOP).
  - ✓ Les clients de débogueur IBM peuvent désormais sécuriser leurs connexions.

Audit et autorisations

- **Fonctionnalités d'audit améliorées :**
  - ✓ De nouvelles valeurs d'audit et entrées de journal d'audit ont été ajoutées pour une meilleure traçabilité des actions utilisateur et des événements système, notamment pour la collection d'autorités de l'IFS (Integrated File System).
  - ✓ De nouveaux services SQL sont disponibles pour les fonctions d'audit et de sécurité.

- **Granularité des autorisations :**
  - ✓ Le nouvel ID de fonction QIBM_IOSYSCFG_VIEW permet aux administrateurs d'accorder un rôle en lecture seule pour la consultation des informations de configuration du système d'entrée/sortie, sans avoir à accorder l'autorité spéciale *IOSYSCFG, qui est souvent trop permissive.

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

IBM

Nouveautés 7.6 – autres évolutions

Autres évolutions

- **Chiffrement de l'ASP système**
  - ✓ Protection accrue des données stockées.
  - ✓ IBM i 7.6 permet de chiffrer l'ASP système (ASP 1), ce qui protège les données utilisateur. Cela nécessite l'option 45 du programme sous licence du système d'exploitation (Encrypted ASP Enablement) et peut être activé sans temps d'arrêt via les outils de service.

- **Modifications sur les IDs d'outils de maintenance**
  - ✓ Connexion obligatoire en mode DST avec un ID valide lors d'opérations sensibles.
  - ✓ Les anciens IDs génériques (11111111, 22222222) sont supprimés depuis 7.5.

- **Blocage de l'IPL si le mot de passe QSECOFR est celui par défaut**
  - ✓ Renforce la sécurité lors des démarrages système.

Power Week

18 -19 - 20 novembre 2025

Questions/Réponses


MERCI
LM2