

Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

S35 - Mise en œuvre de SSO sur IBM i : retours d'expérience

19 novembre 11:15 - 12:15

Julien LAURIER
Gaia Mini Systèmes
julien.laurier@gaia.fr

IBM

common
FRANCE

Présentation

Julien LAURIER

Chez Gaia depuis 2020
Technicien IBM i



GAIA / VOLUBIS

Formation (débutant, perfectionnement)
Expertise IBM i
Centre de Services



Agenda

1. Single Sign-On
 - Sécurité - SSO - Kerberos - LDAP - EIM
2. SSO sur l'IBM i
 - Schéma de fonctionnement
 - Configuration ACS et RDi
3. Prérequis et Mise en œuvre
 - Navigator for i - Réseau au top
 - Etapes clés
4. Bien préparer et Eviter les risques
 - PRA
 - Migration / Anciennes installations
5. Résoudre les problèmes éventuels
 - kinit
 - CCSID
 - LDAPCollector (QMGTools)
6. Liens utiles

Power Week

18 -19 - 20 novembre 2025



Single Sign-On

IBM
common
FRANCE

IBM

Constat

- Les sociétés sont toujours plus sensibles à la **sécurité informatique**
- Une des problématiques est l'**authentification**, et de fait la **gestion des mots de passe**
- L'une des solutions est de **ne plus avoir à saisir, ni transmettre un simple mot de passe**, en mettant en place une solution de **Single Sign-On (SSO)**, qui permet de ne se signer qu'une seule fois

Single Sign-On

- L'utilisateur s'**authentifie une fois**, ensuite il est reconnu sans nouvelle authentification sur un certain nombre de **systèmes et services déclarés**
- Il existe plusieurs solutions qui se basent souvent sur l'**Active Directory**, l'annuaire de référence des utilisateurs de l'entreprise, ainsi que **Kerberos**

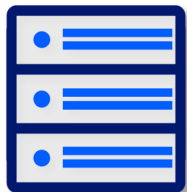


Implémentation



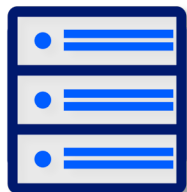
Un serveur Kerberos

Fournisseur de tickets



Un serveur LDAP

Dialogue entre domaines

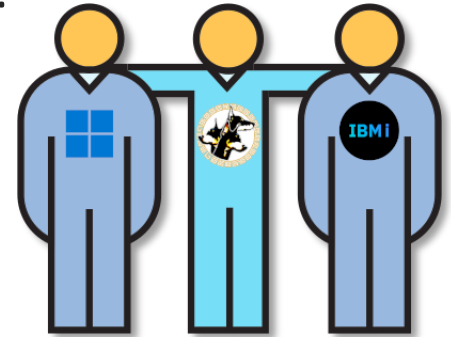


Un serveur EIM

Associations d'utilisateurs

Kerberos

- **Kerberos** V4 : 1985 → Kerberos V5 : 1993 → krb5-1.22.1 : 20/08/2025
- Protocole d'**authentification** sécurisé basé sur la confiance :
 - Le **client** fait confiance à **Kerberos**
 - Le **serveur** fait confiance à **Kerberos**
- Conçu au **MIT** et financé par la **DARPA**
- Rôle : Contrôle et distribution des **tickets**
- Parfaitement intégré aux domaines Windows :
(Et sur la plupart des autres)



KDC - Key Distribution Center

=

AD - Active Directory

=

DC - Domain Controller



LDAP

- Lightweight **D**irectory **A**ccess **P**rotocol
- Simplification de la norme X500
- **Annuaire** avec arborescence (Système de fichiers / ObjectClass)
Modèle AD Microsoft : gaia.lan → DC=gaia,DC=lan

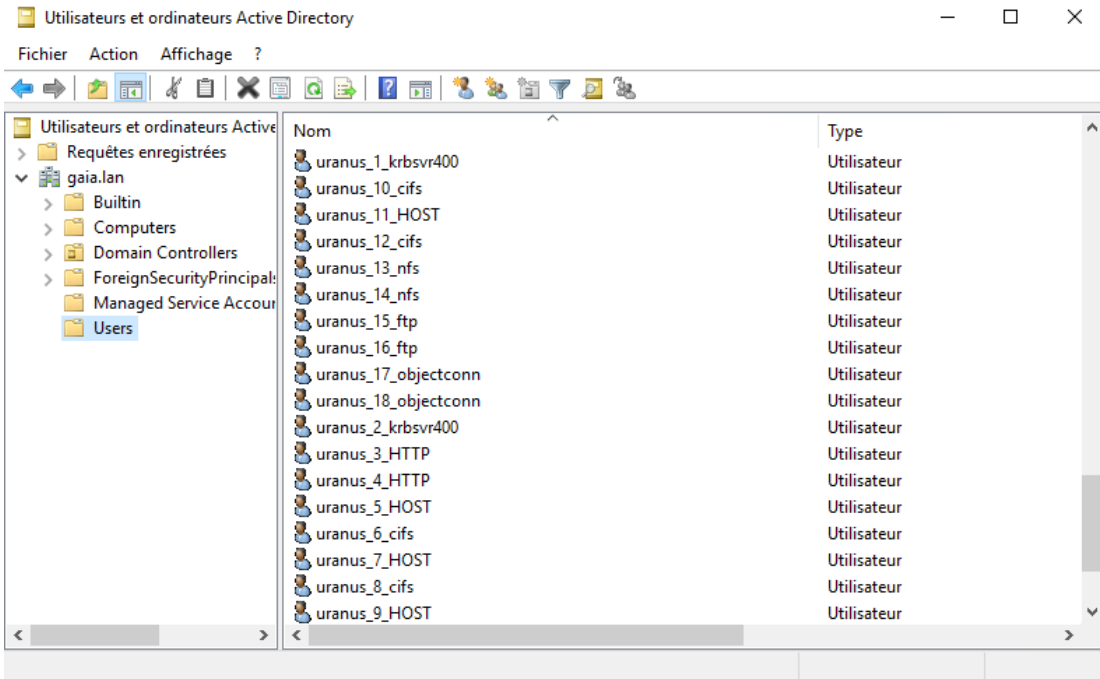
DN	CN	OU	DC
Distinguished Name	Common Name	Organizational Unit	Domain Controller
Relative DN	cn=ibmi_7_HOST,cn=users,dc=GAIA,dc=NET		

- Protocole de communication (Bind DN)
- Echanges cryptés par Kerberos

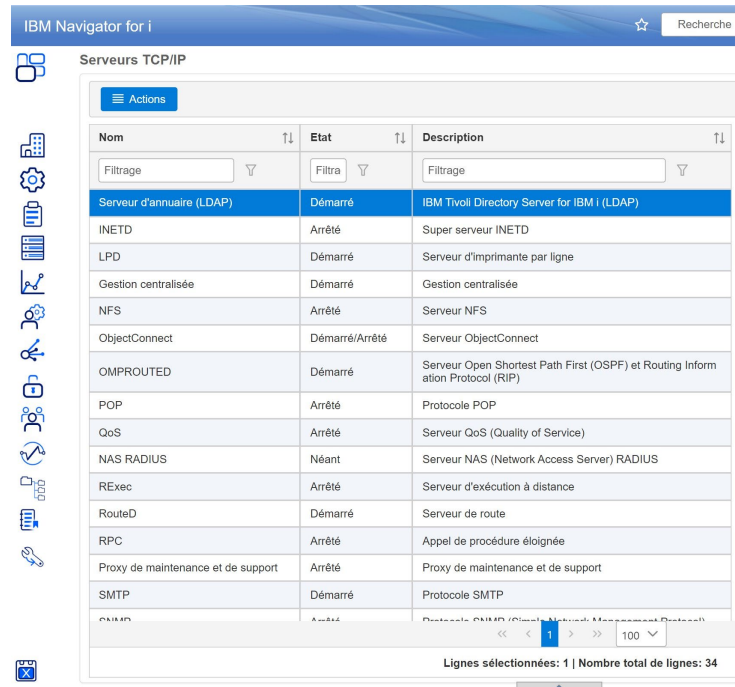
LDAP	LDAPS
389	636

LDAP

Windows

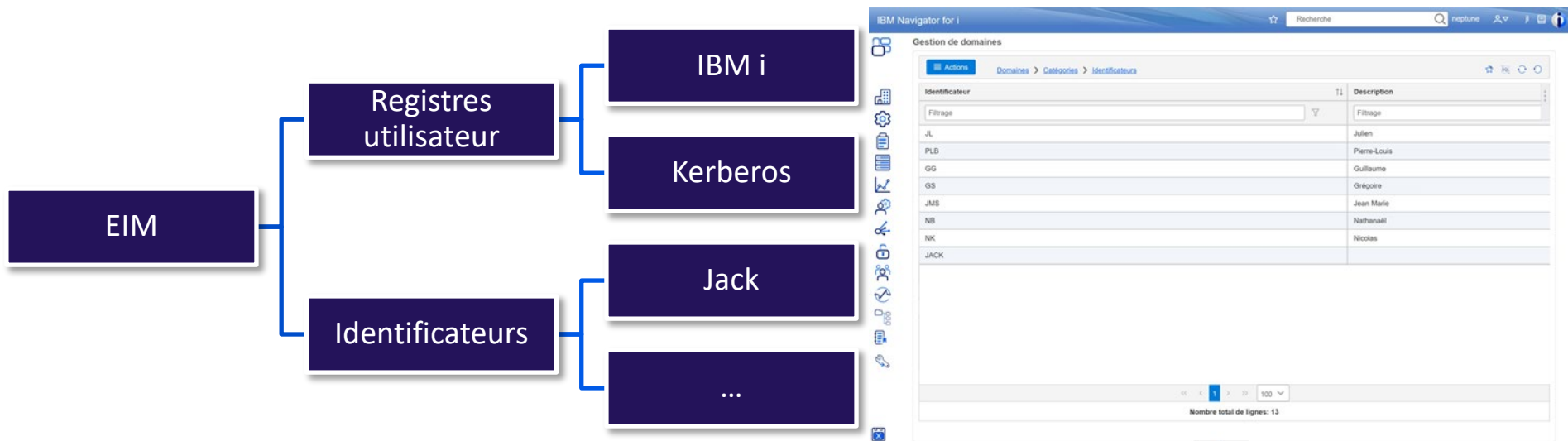


IBM i



EIM

- Enterprise Identity Mapping
- Association des utilisateurs (Profil Windows / Profil IBM i)



Authentification ~~Autorisations~~

- **Kerberos** est utilisé pour **valider l'accès à un service** pour un utilisateur donné
- Ses **droits** d'accès et d'actions dans ce service **ne sont pas gérés** directement via le protocole **Kerberos**
- Les **droits utilisés** une fois connecté restent **ceux du profil côté serveur**, associé via **EIM**

Power Week

18 -19 - 20 novembre 2025

IBM i

IBM
common
FRANCE

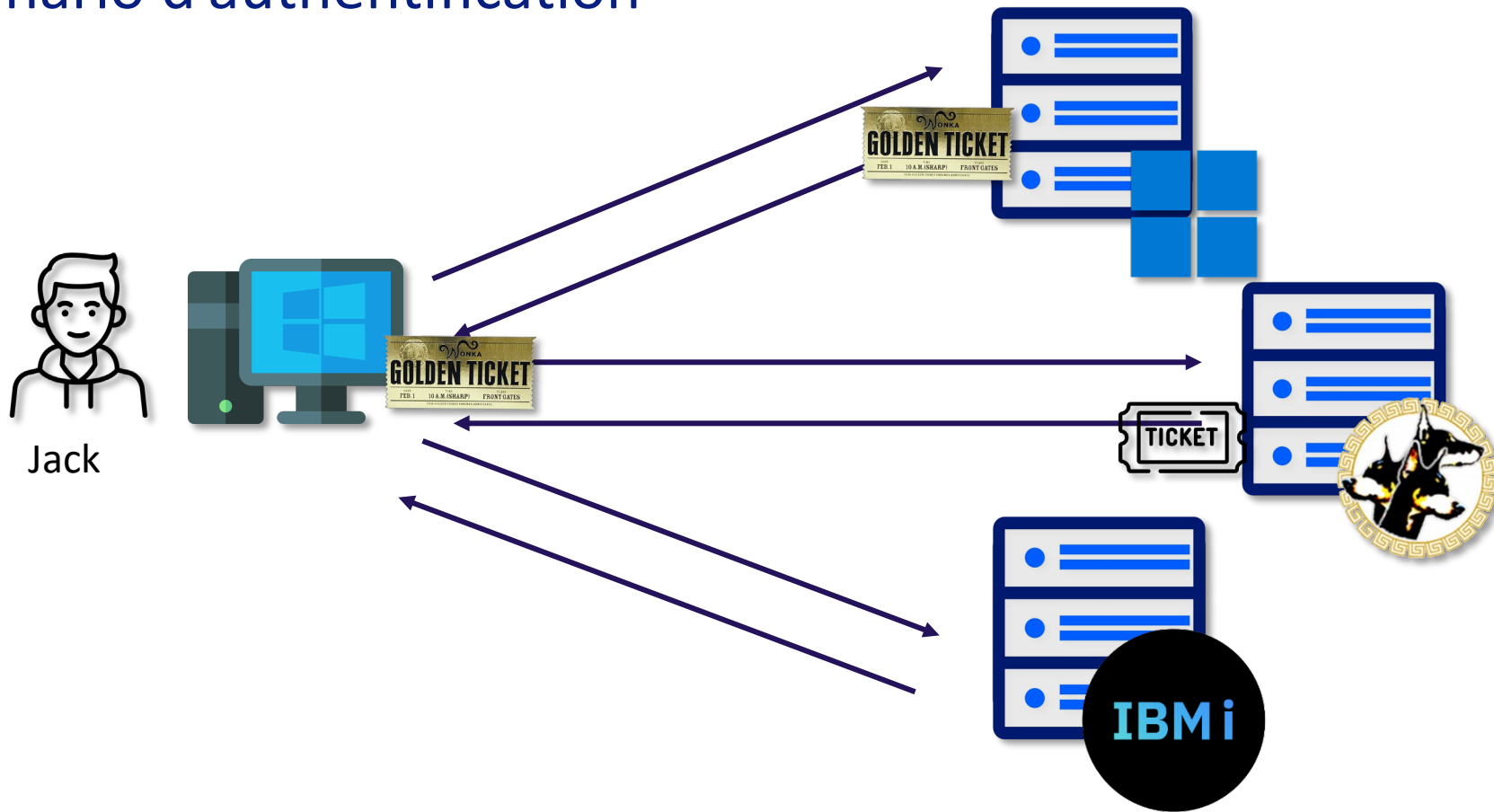
IBM

SSO sur l'IBM i

Éléments de langage

- **Key Distribution Center - KDC** : Serveur Kerberos d'authentification et de distribution des tickets
- **Ticket Granting Ticket - TGT** : Ticket maître permettant de demander des ST
- **Service Ticket - ST** : Ticket dédié à un service kerberisé
- **Service Principal Name - SPN** : Identifiant au sens Kerberos du service pour lequel on souhaite s'authentifier
- **Mappage EIM** : Association des utilisateurs AD / IBM i

Scénario d'authentification



Scénario textuel

- L'utilisateur s'**authentifie** sur le **domaine** via login/mot de passe
- Le serveur **Kerberos** émet un **challenge en cryptographie** symétrique
- Si le **client** réussit → **Kerberos** fournit un **Ticket Granting Ticket (TGT)**
Ce dernier est renouvelé chaque jour à l'ouverture de la session
- Demande d'un **Service Ticket (ST)** au **Key Distribution Center (KDC)** en transmettant le **TGT** et le **Service Principal Name (SPN)** souhaité
Chaque service a un SPN dédié (IBM i, ObjectConnect, NetServer...)
- Si le **TGT** valide & **SPN** trouvé dans le **LDAP** de **Kerberos** → le **KDC** fournit un **ST**
Le ST est au format PAC (Privilege Account Certificate), il peut contenir des informations de groupes d'autorisations
- Le **client** présente son **ST** au serveur disposant du **service** demandé
- Le **serveur** valide ou non le **service** puis l'**utilisateur** via **EIM**

Power Week

18 -19 - 20 novembre 2025



IBM
common
FRANCE

IBM

Prérequis et Mise en œuvre

Prérequis - Outils

Navigator for i	IBM i Access Client Solution (ACS)	Gestion AD
Dernière version (min. 09-2021)	À jour (version actuelle : 1.1.9.9)	
Mise en place du LDAP	Accès IBM i	Ajout des services Kerberos
Mise en place et gestion EIM	Récupération du .bat de création des services	



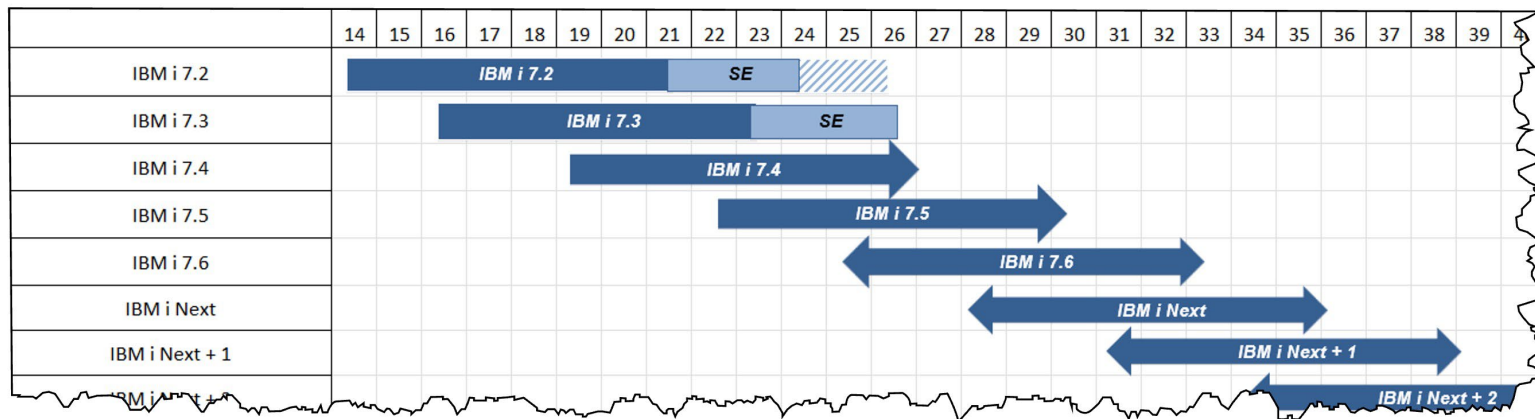
Prérequis - Logiciels nécessaires

Logiciel	Option	Description
57xxSS1	12	Host Servers
57xxSS1	30	Qshell
57xxSS1	33	Portable App Solutions Environment
57xxNAE	*BASE	IBM Network Authentication Enablement for i

```
SELECT product_id,  
       product_option,  
       release_level,  
       installed  
FROM   qsys2.software_product_info  
WHERE  (product_id LIKE '57__SS1'  
        AND product_option IN ('12', '30', '33'))  
        OR product_id LIKE '57__NAE';
```











Prérequis - Version d'OS

<https://www.ibm.com/support/pages/release-life-cycle>



Version	Sortie	Fin du support standard
V7R3	15/04/2016	30/09/2023
V7R4	21/06/2019	09/30/2026
V7R5	10/05/2022	
V7R6	18/04/2025	

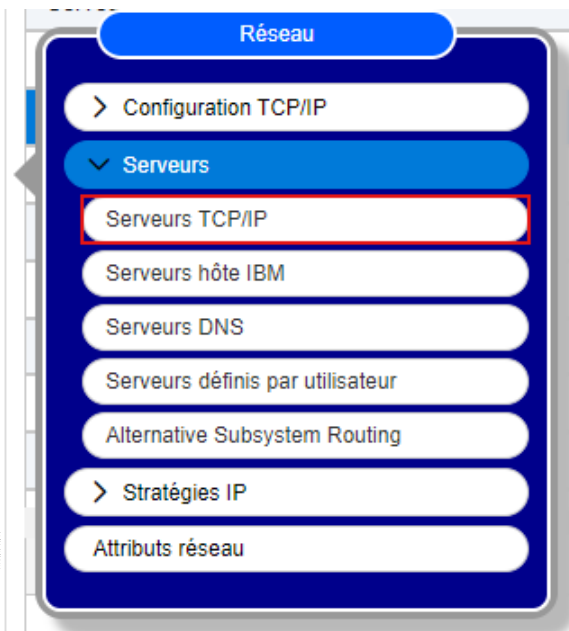
Etapes de mise en œuvre

1. Réinitialisation de la configuration du LDAP  ACS
2. Configuration du LDAP  Navigator for i
3. Configuration de Kerberos  Navigator for i
4. Création des utilisateurs des services Kerberos sur l'AD  PowerShell sur l'AD
5. Validation de la configuration via kinit  ACS
6. Configuration du domaine EIM  Navigator for i
7. Inscription des utilisateurs  Navigator for i
8. (Facultatif) Activation du SSO pour NetServer  Navigator for i
9. Configuration des clients (ACS, RDi...)  ACS  RDi

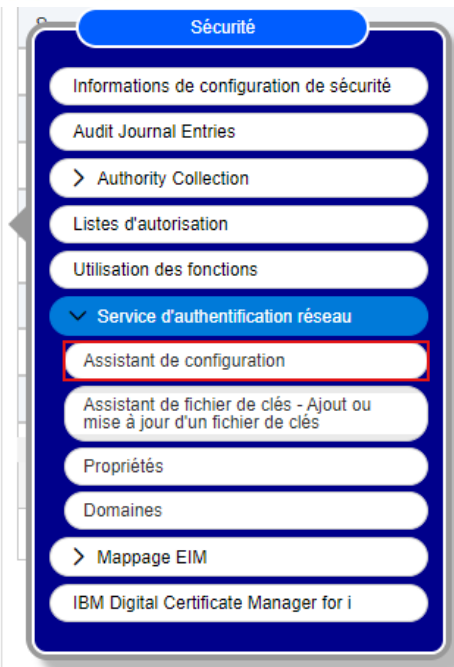
Tout (ou presque) sur Navigator for i



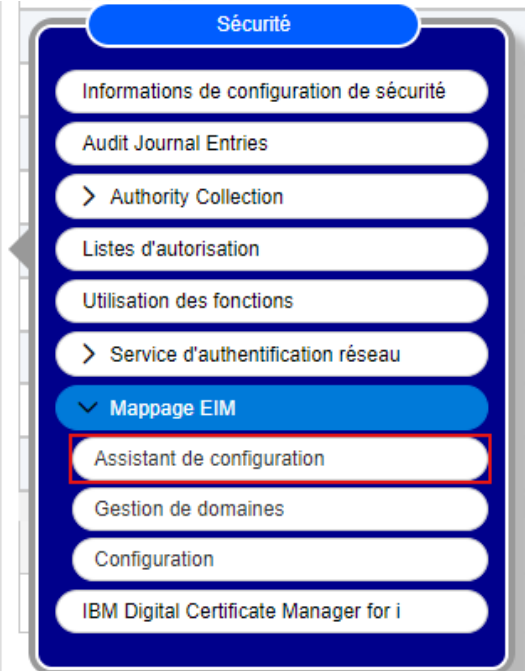
LDAP



Kerberos



EIM



L'aide sera toujours apportée sur l'IBM i à ceux qui la méritent !

IBM Navigator for i

Recherche

Configuration de service d'authentification réseau

✓ ✓ ✓ **●** ● ●

Select Keytab Entries

Kerberos enabled services require a keytab file to authenticate client identities. A keytab file is used to securely store an encrypted version of the service principal's long term key.
For which of the following services would you like to add or update the keytab entry?

- ☒ IBM i Kerberos Authentication
- ☐ LDAP
- ☒ HTTP Server powered by Apache
- ☒ IBM i NetServer
- ☒ IBM i Network File System (NFS) Server
- ☒ IBM i Network FTP Server
- ☒ IBM i ObjectConnect Server

[Details](#)

Do you want to set the same password for the selected keytab entries?
The password will be saved in the keytab file. The password needs to be same with the password of the principal on the KDC.
Keytab:/QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab

☒ Oui

*Mot de passe:

*Mot de passe pour confirmation:

☐ Non

[< Back](#) [Next >](#)

[X Annulation](#)

Inscription des associations utilisateurs

Sécurité

Informations de configuration de sécurité

> Journal d'audit

> Collecte des droits

Listes d'autorisation

Utilisation des fonctions

> Détection des intrusions

> Gestion des clés des services de chiffrement

> Service d'authentification réseau

▼ Mappage EIM

Assistant de configuration

Gestion de domaines

Configuration

IBM Digital Certificate Manager for i

Connexion au contrôleur de domaine EIM

Contrôleur de domaine : IBM1.DOMAIN.LAN

*Type d'utilisateur: Nom distinctif

*Nom distinctif: cn=Administrator

Mot de passe

Indication d'un mot de passe:

Nouvel identificateur EIM

Identificateur Eim: PN

☐ Générer un identificateur unique

Description:

Domaine: EIM

Associations

Actions

Registre ↑↓	Type de registre ↑↓	Utilisateur ↑↓
Filtrage	Filtrage	Filtrage
IBM1.DOMAIN.LAN	IBM i	PN
DOMAIN.LAN		PNOM

OK Annulation

Activation de NetServer

IBM Navigator for i

1

Serveurs TCP/IP

Actions

Nom T1	Etat T1	Description T1
Filtrage	Filtrage	Filtrage
EDRSQ	Arrêté	Extended Dynamic Remote SQL
FTP	Démarré	Protocole de transfert de fichier
Serveurs HTTP	Démarré	Serveurs HTTP
Serveurs d'applications intégrées	Démarré	Serveur d'application Web et de services
Support IBM i pour la fonction Voisinage	Démarré	Support IBM i pour la fonction Voisinage
IBM i NetServer	Arrêté	IBM i NetServer for IBM i (LD)
Serveur d'annuaire (LDAP)	Démarré	IBM i NetServer for IBM i (LD)
INETD	Arrêté	Super serveur INETD
LPD	Démarré	Serveur d'imprimante par ligne
Gestion centralisée	Démarré	Gestion centralisée
NFS	Arrêté	Serveur NFS
OMPROUTED	Arrêté	Serveur Open Shortest Path First (OSPF)
POP	Arrêté	Protocole POP

Lignes sélectionnées: 1 | Nombre total de lignes: 33

IBM Navigator for i

2

Serveurs TCP/IP

Actions

Nom T1	Etat T1	Description T1
Filtrage	Filtrage	Filtrage
EDRSQ	Arrêté	Extended Dynamic Remote SQL
FTP	Démarré	Protocole de transfert de fichier
Serveurs HTTP	Démarré	Serveurs HTTP
Serveurs d'applications intégrées	Démarré	Serveur d'application Web et de services
Support IBM i pour la fonction Voisinage	Démarré	Support IBM i pour la fonction Voisinage
IBM i NetServer	Arrêté	IBM i NetServer for IBM i (LD)
Serveur d'annuaire (LDAP)	Démarré	IBM i NetServer for IBM i (LD)
INETD	Arrêté	Super serveur INETD
LPD	Démarré	Serveur d'imprimante par ligne
Gestion centralisée	Démarré	Gestion centralisée
NFS	Arrêté	Serveur NFS
OMPROUTED	Arrêté	Serveur Open Shortest Path First (OSPF)
POP	Arrêté	Protocole POP

Lignes sélectionnées: 1 | Nombre total de lignes: 33

3

Propriétés d'IBM i NetServer

Général

Avancé

Sécurité

Configuration de WINS

ID utilisateur invité:

Méthode d'authentification:

Autoriser l'authentification via la méthode de hachage de mot de passe du gestionnaire de réseau local:

Signature obligatoire des demandes par les clients:

Réduction au prochain démarrage

ID utilisateur invité:

Méthode d'authentification:

☒ Autoriser l'authentification via la méthode de hachage de mot de passe du gestionnaire de réseau local

Signature obligatoire des demandes par les clients:

Restauration des valeurs en cours

Sauvegarde

Fermeture

Mise en place sur ACS

■ Gestionnaire de sessions (global)

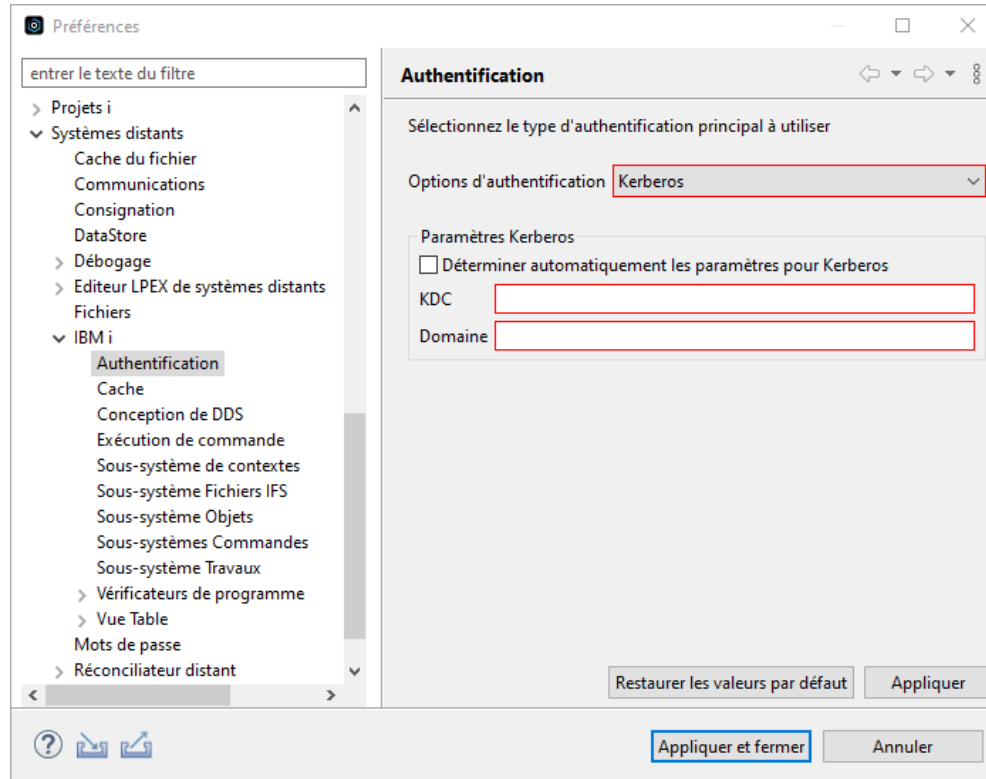
The screenshot shows the 'Editer le système sélectionné' window with the 'Connexion' tab selected. The 'Invite de mot de passe' section has three radio buttons: 'Utilisation de données d'identification partagées', 'Utilisation du nom d'utilisateur par défaut pour une invite ponctuelle par système' (with a text field for 'Nom d'utilisateur par défaut'), and 'Utilisation de l'authentification Kerberos, pas d'invite' (which is selected and highlighted with a red box). The 'Performances' section has a dropdown for 'Fréquence de vérification de l'adress...' set to 'A chaque fois' and a text field for 'Adresse IP :'. The 'Ports' section has a dropdown set to '22' and the label 'Connexions SSH'. At the bottom are 'OK', 'Application', and 'Annulation' buttons.

■ Connexion du hod (la session)

The screenshot shows the 'Editer le système sélectionné' window with the 'Avancé' tab selected. The left sidebar shows a tree view with 'Connexion' expanded and 'Avancé' selected (highlighted with a red box). The 'Avancé' section has two text fields: 'Délai de connexion (secondes)' and 'Délai d'inactivité (minutes)', both set to '0'. Below these are two radio buttons for 'Signal de présence' (set to 'Non') and 'Activation d'ENPTUI' (set to 'Oui'). The 'Informations de connexion IBM i' section has a dropdown for 'Invite de mot de passe' set to 'Utilisation de l'authentification Kerberos, pas d'invite' (highlighted with a red box), a text field for 'ID utilisateur :', and two radio buttons for 'Ignorer l'ouverture de session' (set to 'Oui'). At the bottom are 'OK', 'Annuler', 'Clavier...', and 'Aide' buttons.

Mise en place sur RDi

Fenêtre → Préférences → Systèmes distants → IBM i → Authentification



Power Week

18 -19 - 20 novembre 2025



Bien préparer
-
Eviter les risques

IBM
common
FRANCE

IBM

Éléments à connaître sur votre environnement

- Accès à l'IBM i et à l'AD
- Le mot de passe du LDAP IBM i
- Nom de domaine et adresse IP de l'IBM i (à vérifier sur l'IBM i et sur le réseau)
- Le nom de domaine du KDC (AD)
- Les règles de mot de passe sur le domaine (pour les services)
- La liste des associations profil Windows ↔ profil IBM i
- La valeur système QRMTSIGN doit être égale à *VERIFY

Plan de Reprise d'Activité

- Impératif de tester son PRA, régulièrement et jusqu'au bout !
- En fonction du type de PRA, la mise en œuvre sera différente
 - Si la machine de backup change de nom au niveau du réseau pour le PRA la configuration côté IBM i doit être terminée en PRA
 - Quoi qu'il arrive, tester la configuration du SSO dans les conditions les plus proches possibles d'une application du PRA
- Ne pas oublier de répliquer les associations utilisateur, elles sont propres à l'IBM i et ne sont ni stocké dans un simple fichier, ni dans un autre type d'objet (accès uniquement via API)
- Attention ! Si le réseau est impacté, si l'IBM i ne voit plus l'AD le SSO ne fonctionne plus !
- Prévoir une solution de repli en cas de dysfonctionnement, en cas de crise le SSO ne sera pas nécessairement la priorité, l'accès à la machine et le fonctionnement de la production prime souvent
- Si le SSO n'est plus fonctionnel, les utilisateurs devront saisir leur mot de passe, qu'ils n'auront pas saisi depuis longtemps...

Power Week

18 -19 - 20 novembre 2025



IBM
common
FRANCE

IBM

Résoudre les problèmes éventuels

Problèmes souvent rencontrés

- CCSID utilisé lors d'une première configuration, différent du CCSID utilisé pour modifier ou refaire cette configuration
- Problèmes de synchronisation d'horloge entre les serveurs et clients
- Incohérence entre le nom sous lequel la machine se connaît et le nom sous lequel le domaine la connaît
 - Pour connaître le nom de l'IBM i d'après le DNS pour le client

```
PS > ping -a 192.168.xxx.xxx
```

- Sur l'IBM i :

```
SELECT host_name FROM sysibmadm.env_sys_info;
```


Nettoyage des anciennes configurations

- Les objets et fichiers stream SSO sont partout !
- Même sans tentative de configuration antérieurs des résidus de configuration peuvent persister
- Pour commencer sur de bonnes bases, nettoyez le terrain !

Nettoyage des anciennes configurations

- Un petit avant goût

```
===> CLRLIB LIB(QUSRDIRDB)
===> DTLIB LIB(QUSRDIRDB)
===> DTLIB LIB(QUSRDIRCF)
===> DTLIB LIB(QUSRDIRCL)

===> RMVDIR DIR('/qibm/userdata/os400/dirsrv') SUBTREE(*ALL)

===> DLTUSRSPC USRSPC(QUSRSYS/QGLDCFG)
===> DLTVLDL VLDL(QUSRSYS/QGLDVLDL)

===> DLTUSRQ USRQ(QDIRSRV2/QGLDPUBQ)

===> RMVLNK OBJLNK('/qibm/userdata/os400/networkauthentication/krb5.conf')
===> RMVLNK OBJLNK('/qibm/userdata/os400/networkauthentication/keytab/krb5.keytab')
```

Erreurs Kerberos

```
kinit -k krbsvr400/ibmi.domain.lan@DOMAIN.LAN
```

- Attention le nom de domaine doit être en majuscule !
- Ne pas confondre krbsvr400 et krbsrv400 (fréquent)
- S'il n'y a pas de problème la commande n'affiche rien
Sinon on obtient un code
- Messages fréquents avec aide
 - <https://www.ibm.com/support/pages/enterprise-identity-mapping-eimnetwork-authentication-services-nas-error-codes-and-solutions>
- Liste exhaustive
 - <https://www.ibm.com/docs/en/zos/2.5.0?topic=r-messages>

Erreurs Kerberos - Exemples

Symptom Code	Error Description	Solution
0x80090304	Error in System Access for Windows Detail trace kerb::InitializeSecurityContext() failed rc=0x80090304 kerb::mapSSPItoRC: sec_e_internal_error -> cwb_intenal_error	Change Encryption to AES
0x96c73a06	EUVF06014E Unable to obtain initial credentials Status 0x96c73a06 - Client principal is not found in security registry.	<p>The SPN (Service Principle Name) is not or multiple available in the Windows Active Directory.</p> <p>Solution 1: We can run the command "<i>ldifde -m -f output.txt</i>" from Windows Active Directory to create a list of all the users and we can check for duplicate service principal entries.</p> <p>Solution 2: Reset the password for the Active Directory Service principal account so that it matches what is in the IBM i keytab list</p> <p>Solution 3: Check information for symptom/error code 96c73a0e</p>
0x96c73a0e	EUVF06014E Unable to obtain initial credentials. Status 0x96c73a0e - Encryption type is not supported.	<p>Often seen on Windows 2008 domains and Windows 7 systems. This domain do not support DES encryption by default.</p> <p>Solution 1: Since end of 2011 the encryption AES is available for R540 and above. The following document describes this issue: https://www.ibm.com/support/pages/node/684323</p> <p>Solution 2: Another way is to enable DES on Windows 2008 Active Directory which is described in Microsoft KB 977321.</p>



LDAP Collector

- En dernier recours, ouverture d'un incident chez IBM, se munir de QGMTools
- LDAP Collector pour la partie LDAP
 - <https://www.ibm.com/support/pages/complete-ldap-directory-server-cleanup-and-reconfigure>

```
QMGTOOLS/LDAPCOL BINDDN('cn=Administrator') LDAP_PW(*****)
```

- HTTPAdmin Collector pour une log plus globale sur Navigator for i

```
QMGTOOLS/HTTPADMCOL FTPRSP(N)
```

Power Week

18 -19 - 20 novembre 2025



IBM
common
FRANCE

IBM

Liens utiles

Liens utiles

- Kerberos
 - <https://web.mit.edu/kerberos>
 - <https://github.com/heimdal/heimdal/>
- Support IBM (attention aux liens qui disparaissent par magie 🏠)
- Nettoyage du LDAP
 - <https://www.ibm.com/support/pages/complete-ldap-directory-server-cleanup-and-reconfigure>
 - <https://www.ibm.com/support/pages/cleanup-eim-and-nas-enterprise-identity-mapping-and-network-authentication-service>
- Kerberos
 - <https://www.ibm.com/support/pages/enterprise-identity-mapping-eimnetwork-authentication-services-nas-error-codes-and-solutions>
 - <https://www.ibm.com/docs/en/zos/2.5.0?topic=r-messages>
- LDAPCollector (QMGTools)
 - <https://www.ibm.com/support/pages/qmgtools-eimssoldap-collector>
- CVE IBM i
 - <https://www.ibm.com/support/pages/bulletin/search?q=ibm%20i>

MERC

The word "MERC" is displayed in a large, bold, white sans-serif font against a plain white background. Each letter of the word is filled with a different portrait of a diverse professional. The 'M' features a woman with long dark hair wearing a green top. The first 'E' shows a smiling man in a green patterned shirt. The 'R' depicts a woman with her hands clasped in front of her, wearing a light blue shirt. The 'C' shows a man in a blue suit and yellow tie. The final 'C' features a man with glasses wearing a blue shirt. The portraits are cropped to fit the shapes of the letters, and the letters have a subtle drop shadow.