

# Université **IBM i**

## 19 et 20 novembre 2024

### IBM Innovation Studio Paris

#### **S25 - Mise en œuvre de SSO sur IBM i : retours d'expérience**

19 novembre 16:00 - 17:00

**Julien Laurier**

Gaia Mini Systèmes

*julien.laurier@gaia.fr*



uui2024

#ibmi

#uui2024



common  
FRANCE

# Université IBM i

19 et 20 novembre 2024

**IBM i**  
continuous innovation  
continuous integration

IBM



## Centre de services IBM i

- Mutualisé
- A distance



## Modernisation

- Accompagnement
- Prototypage



## Expertise technique

- Prestations de service (audit, consulting...)
- Transfert de connaissances (workshops)



## FORMATIONS

SUR SITE  
A DISTANCE

INTER  
SUR MESURE



## COURS EN LIGNE

FORMATS COURS

REPLAYS EN LIGNE



## BASE DE CONNAISSANCE

IBM i

EN LIGNE



### GRMT5250

Consultez l'écran 5250 d'un autre utilisateur  
en temps réel directement sur l'IBM i

**PRINCIPE**  
GRMT5250 vous permet d'accéder rapidement à l'écran 5250 d'un autre utilisateur, directement depuis votre session IBM i.  
Il ne nécessite pas de passer par des outils intermédiaires tel que Teams.

**ABONNEMENT ANNUEL 2000€ HT / PARTITION**

#### REPRENEZ LE CONTRÔLE

Inspiré de notre propre expérience dans la maintenance sur IBM i, nous l'avons conçu pour les professionnels de l'IBM i. Cette solution est idéale pour intervenir rapidement sur les sessions utilisateurs bloquées ou pour diagnostiquer et corriger des bugs en temps réel.  
En plus de cette fonctionnalité clé, notre outil offre une gamme d'options supplémentaires qui simplifient la gestion des sessions utilisateurs sur l'IBM i, améliorant ainsi l'efficacité et la réactivité de votre équipe technique. Optez pour une solution intuitive et intégrée, qui vous permet de superviser au mieux les travaux de votre IBM i depuis votre poste de travail.

#### PRINCIPALES CARACTÉRISTIQUES

- Piloter simplement les travaux 5250
- Consulter les activités utilisateurs en temps réel
- Tous vos travaux interactifs et batch regroupés au même endroit via la console de GRMT5250
- Intervenir rapidement
- Gérer les messages en interrogation sur les sessions utilisateurs
- Gérer les sessions inactives

#### CONTACT

Demandez votre démo !

- ☎ 04 72 53 00 12
- ✉ [contact@gaia.fr](mailto:contact@gaia.fr)
- 🌐 <https://www.gaia.fr>



# Agenda

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

Université IBM i

19 et 20 novembre 2024



IBM

# Single Sign-On

# Constat

- Les sociétés sont de plus en 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**



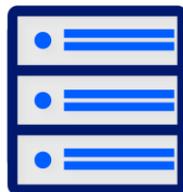
# Implémentation



Un serveur Kerberos  
Fournisseur de tickets



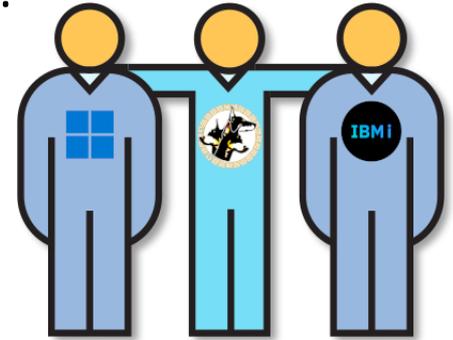
Un serveur LDAP  
Dialogue entre domaines



Un serveur EIM  
Associations d'utilisateurs

# Kreberos

- **Kerberos** V4 : 1985 → Kerberos V5 : 1993 → krb5-1.21.3 : 26/06/2024
- 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

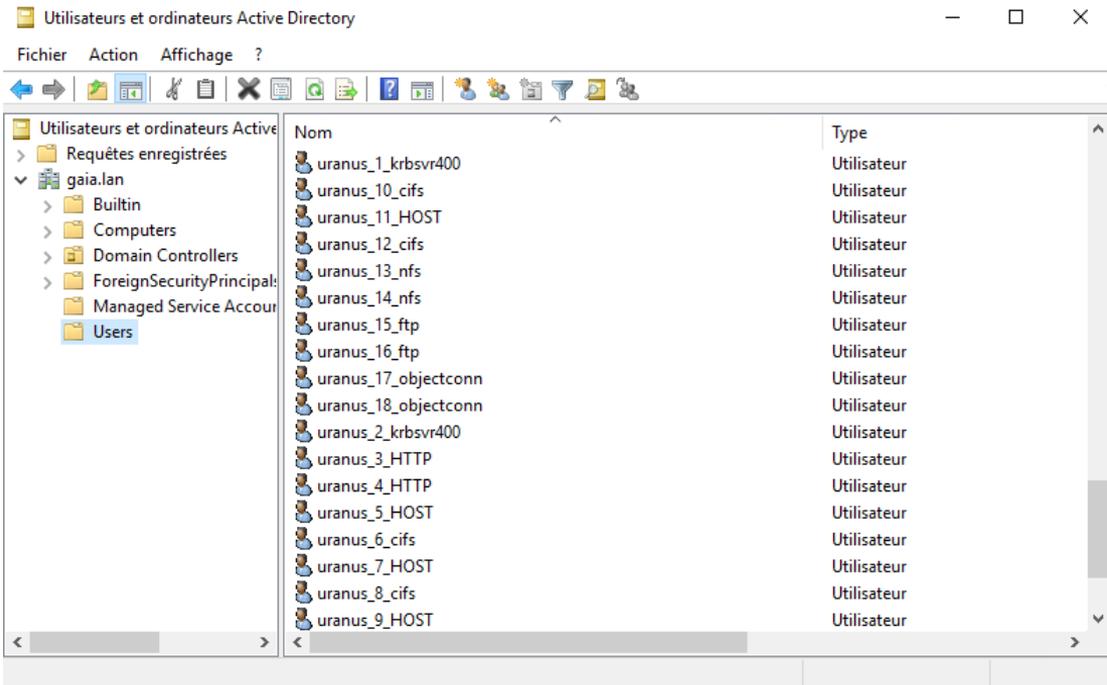
DN	CN	OU	DC
Distinguished Name	Common Name	Organizational Unit	Domain Controller
Relative DN	cn=ibmi_7_HOST,cn=users,dc=GAIA,dc=NET		

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

LDAP	LDAPS
389	636

# LDAP

## Windows



Utilisateurs et ordinateurs Active Directory

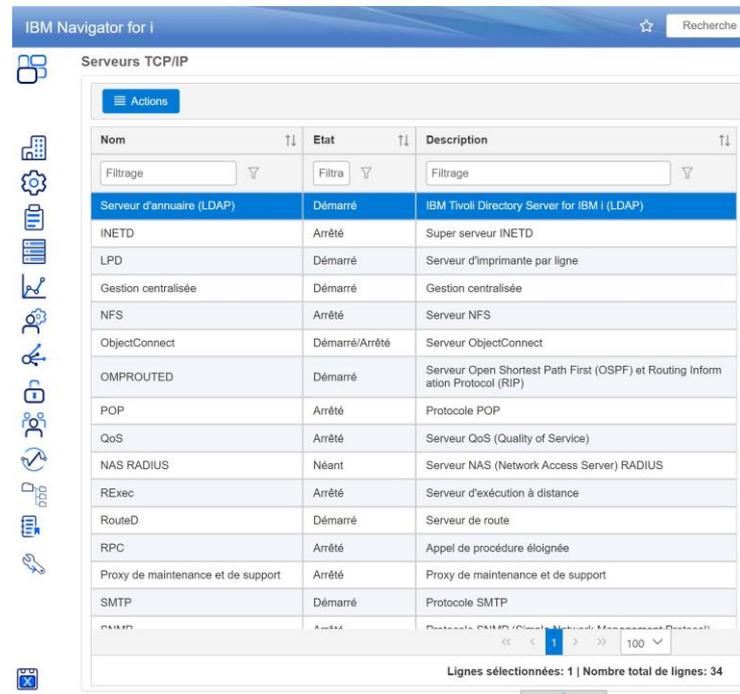
Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- gaia.lan
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

Nom	Type
uranus_1_krbsvr400	Utilisateur
uranus_10_cifs	Utilisateur
uranus_11_HOST	Utilisateur
uranus_12_cifs	Utilisateur
uranus_13_nfs	Utilisateur
uranus_14_nfs	Utilisateur
uranus_15_ftp	Utilisateur
uranus_16_ftp	Utilisateur
uranus_17_objectconn	Utilisateur
uranus_18_objectconn	Utilisateur
uranus_2_krbsvr400	Utilisateur
uranus_3_HTTP	Utilisateur
uranus_4_HTTP	Utilisateur
uranus_5_HOST	Utilisateur
uranus_6_cifs	Utilisateur
uranus_7_HOST	Utilisateur
uranus_8_cifs	Utilisateur
uranus_9_HOST	Utilisateur

## IBM i



IBM Navigator for i

Recherche

Services TCP/IP

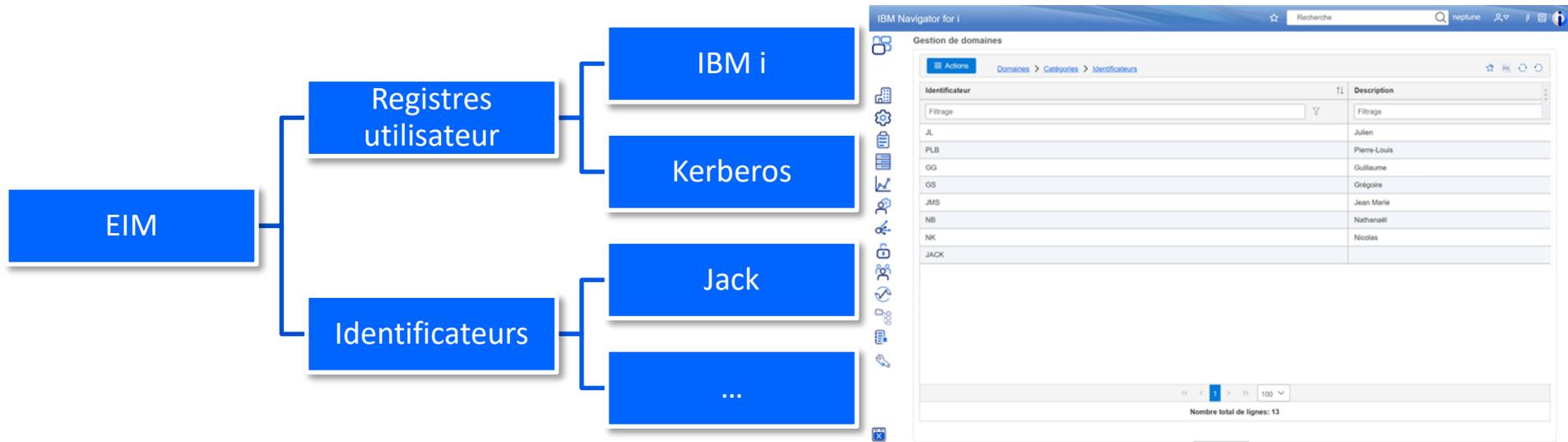
ACTIONS

Nom	Type	Etat	Description
Serveur d'annuaire (LDAP)		Démarré	IBM Tivoli Directory Server for IBM i (LDAP)
INETD		Arrêté	Super serveur INETD
LPD		Démarré	Serveur d'imprimante par ligne
Gestion centralisée		Démarré	Gestion centralisée
NFS		Arrêté	Serveur NFS
ObjectConnect		Démarré/Arrêté	Serveur ObjectConnect
OMPROUTED		Démarré	Serveur Open Shortest Path First (OSPF) et Routing Information Protocol (RIP)
POP		Arrêté	Protocole POP
QoS		Arrêté	Serveur QoS (Quality of Service)
NAS RADIUS		Néant	Serveur NAS (Network Access Server) RADIUS
RExec		Arrêté	Serveur d'exécution à distance
RouteD		Démarré	Serveur de route
RPC		Arrêté	Appel de procédure éloignée
Proxy de maintenance et de support		Arrêté	Proxy de maintenance et de support
SMTP		Démarré	Protocole SMTP
SNMP		Arrêté	Détails SNMP (Simple Network Management Protocol)

Lignes sélectionnées: 1 | Nombre total de lignes: 34

# EIM

- Enterprise Identity Mapping
- Association des utilisateurs (Profil Windows / Profil 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
- **Mapping EIM** : Association des utilisateurs AD / 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

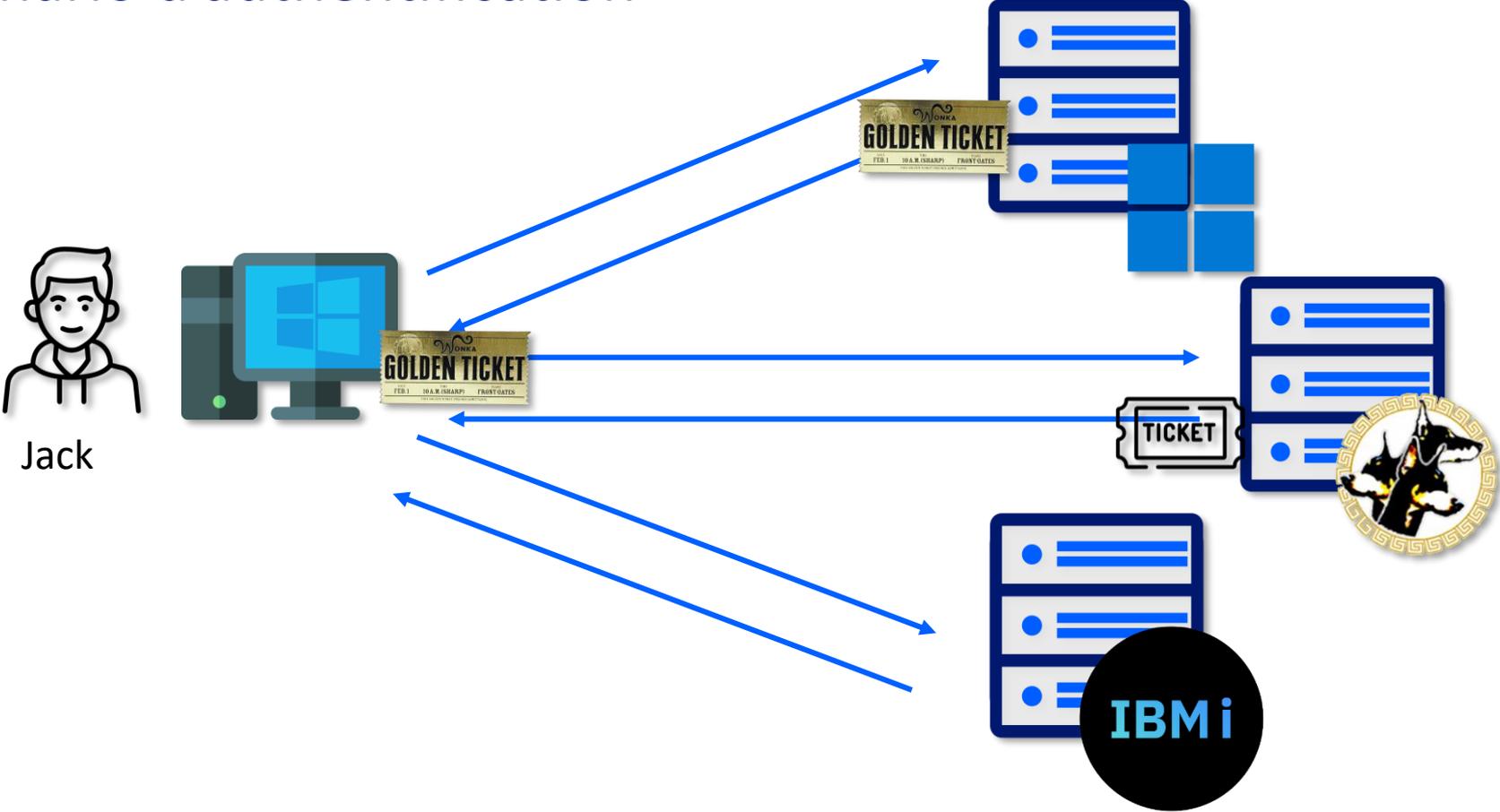
Université IBM i

19 et 20 novembre 2024



# SSO sur l'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**



# 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 : 1.1.9.6)	
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	

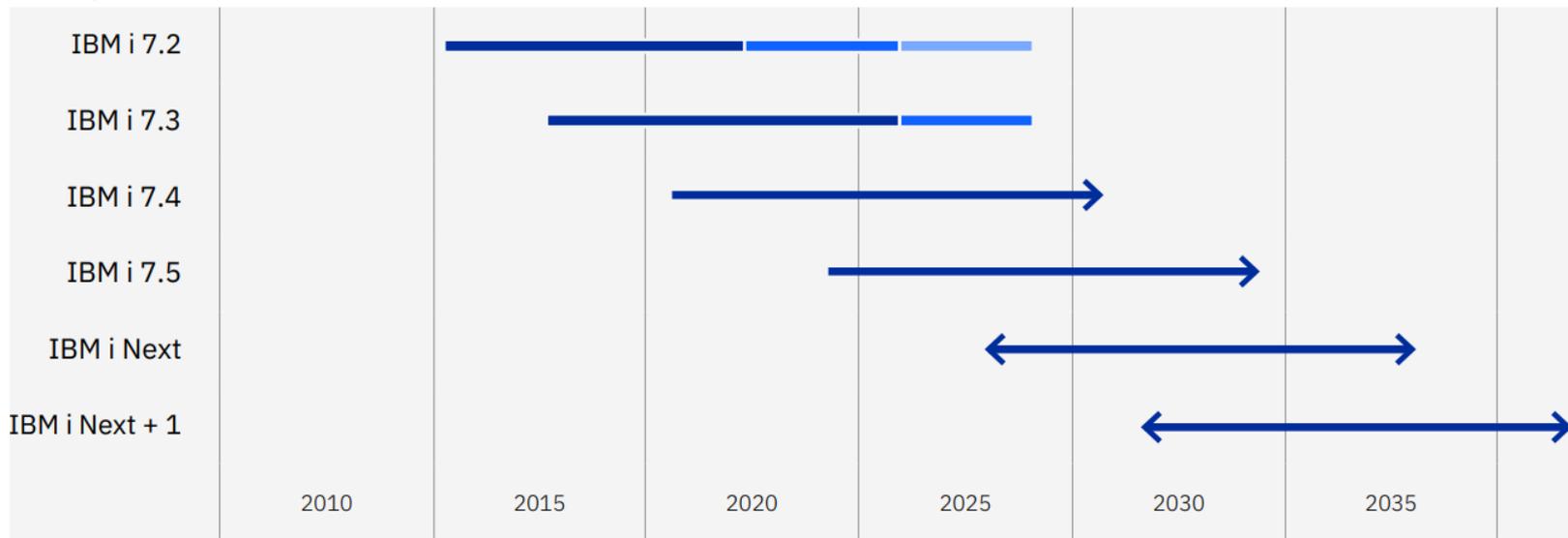
# Prérequis - Logiciels nécessaires

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	Fin du support étendu
V7R3	15/04/2016	30/09/2023	30/09/2026
V7R4	21/06/2019		
V7R5	10/05/2022		

# Etapas 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

Réseau

- > Configuration TCP/IP
- ▼ Serveurs
  - Serveurs TCP/IP
  - Serveurs hôte IBM
  - Serveurs DNS
  - Serveurs définis par utilisateur
  - Alternative Subsystem Routing
- > Stratégies IP
- Attributs réseau



Kerberos

Sécurité

- Informations de configuration de sécurité
- Audit Journal Entries
- > Authority Collection
- Listes d'autorisation
- Utilisation des fonctions
- ▼ Service d'authentification réseau
  - Assistant de configuration
  - Assistant de fichier de clés - Ajout ou mise à jour d'un fichier de clés
  - Propriétés
  - Domaines
- > Mappage EIM
- IBM Digital Certificate Manager for i



EIM

Sécurité

- Informations de configuration de sécurité
- Audit Journal Entries
- > Authority Collection
- Listes d'autorisation
- Utilisation des fonctions
- > Service d'authentification réseau
- ▼ Mappage EIM
  - Assistant de configuration
  - Gestion de domaines
  - Configuration
- IBM Digital Certificate Manager for i

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

The screenshot shows the 'Configuration de service d'authentification réseau' (Network Authentication Service Configuration) window in IBM Navigator for i. The window title is 'IBM Navigator for i' and it includes a search bar with the text 'Recherche'. The main content area is titled 'Configuration de service d'authentification réseau' and features a progress indicator at the top with seven steps, the fourth of which is highlighted in green. Below the progress indicator, the section 'Select Keytab Entries' contains a list of services with checkboxes: 'IBM i Kerberos Authentication' (checked), 'LDAP' (unchecked), 'HTTP Server powered by Apache' (checked), 'IBM i NetServer' (checked), 'IBM i Network File System (NFS) Server' (checked), 'IBM i Network FTP Server' (checked), and 'IBM i ObjectConnect Server' (checked). A 'Details' button is located below the list. The text below the list asks: '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'. There are two radio buttons: 'Oui' (selected) and 'Non'. Below the radio buttons are two password input fields: '\*Mot de passe:' and '\*Mot de passe pour confirmation:'. At the bottom of the window, there are 'Back' and 'Next' buttons, and an 'Annulation' (Cancel) button in the bottom right corner.

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 : IBMI.DOMAIN.LAN

\*Type d'utilisateur:

\*Nom distinctif:

**Mot de passe**

Indication d'un mot de passe:

### Nouvel identificateur EIM

Identificateur Eim:

Générer un identificateur unique

Description:

Domaine: EIM

**Associations**

Registre ↑↓	Type de registre ↑↓	Utilisateur ↑↓
<input type="text" value="Filtrage"/>	<input type="text" value="Filtrage"/>	<input type="text" value="Filtrage"/>
IBMI.DOMAIN.LAN	IBM i	PN
DOMAIN.LAN		PNOM

# Activation de NetServer - 1

IBM Navigator for i

Recherche

qsecofr

### Serveurs TCP/IP

Actions

Nom ↑↓	Etat ↑↓	Description ↑↓
EDRSQL	Arrêté	Extended Dynamic Remote SQL
FTP	Démarré	Protocole de transfert de fichier
Serveurs HTTP	Démarré	Serveurs HTTP
Serveurs d'applications intégrés	Démarré	Serveur d'application Web et de services
Réseau	Démarré	Support IBM i pour la fonction Voisinage
> Configuration TCP/IP	Arrêté	IBM Tivoli Directory Server for IBM i (LDAP)
▼ Serveurs	Arrêté	Super serveur INETD
Serveurs TCP/IP	Démarré	Serveur d'imprimante par ligne
Serveurs hôte IBM	Démarré	Gestion centralisée
Serveurs DNS	Arrêté	Serveur NFS
Serveurs définis par utilisateur	Arrêté	Serveur Open Shortest Path First (OSPF)
Alternative Subsystem Routing	Arrêté	Protocole POP
> Stratégies IP		
Attributs réseau		

Lignes sélectionnées: 1 | Nombre total de lignes: 33

# Activation de NetServer - 2

IBM Navigator for i

Recherche

qsecofr

Serveurs TCP/IP

Actions

Nom ↑↓	Etat ↑↓	Description ↑↓
Filtrage	Filtrage	Filtrage
EDRSQL	Arrêté	Extended Dynamic Remote SQL
FTP	Démarré	Protocole de transfert de fichier
Serveurs HTTP	Démarré	Serveurs HTTP
Serveurs d'applications intégrés	Démarré	Serveur d'application Web et de services
<b>IBM i NetServer</b>	<b>Démarré</b>	<b>Support IBM i pour la fonction Voisinage</b>
Serveur d'annuaire (LDAP)	Démarré	IBM Tivoli Directory Server 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

# Activation de NetServer - 3

Propriétés d'IBM i NetServer

Général

Avancé

**Sécurité**

Configuration de WINS

ID utilisateur invité:

Mots de passe/Authentication réseau

Méthode d'authentification:

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

Signature obligatoire des demandes par les clients: Facultatif

Réduction au prochain démarrage

ID utilisateur invité:

Méthode d'authentification: Mots de passe/Authentication réseau

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

Signature obligatoire des demandes par les clients: Facultatif

Restauration des valeurs en cours

Sauvegarde

X Fermeture

# Mise en place sur ACS

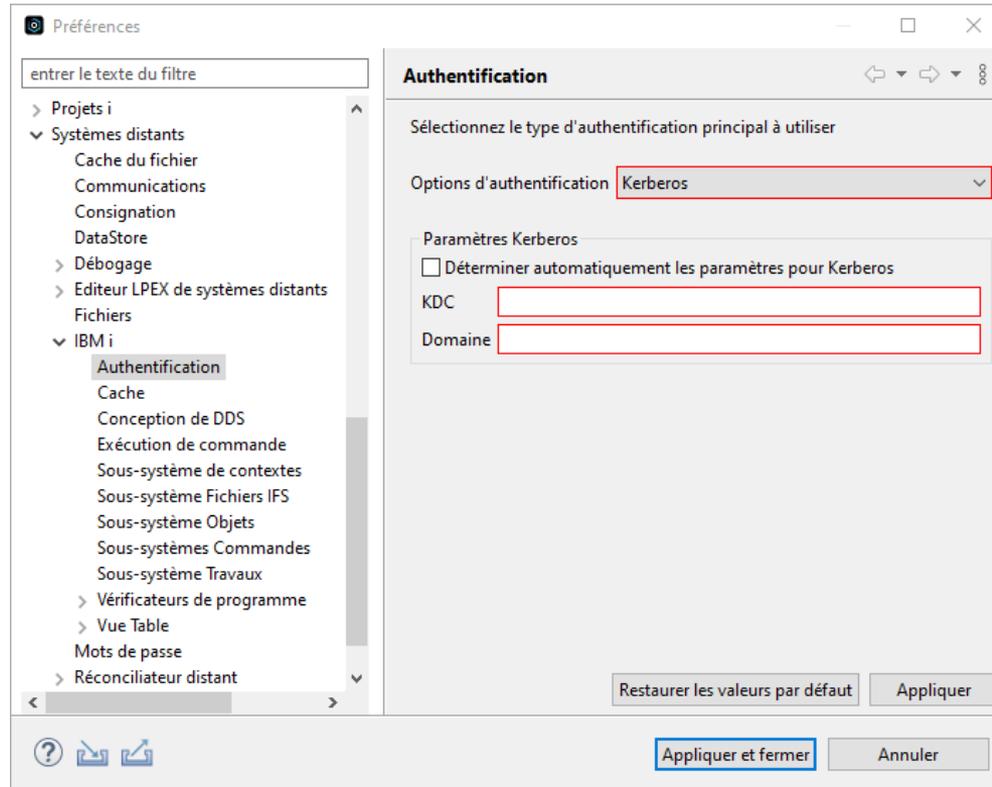
- Gestionnaire de sessions (global)

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

- Connexion du hod (session)

The screenshot shows the 'NEPTUNE' configuration window with the 'Connexion' tab selected. The left sidebar lists 'Connexion', 'Avancé', 'Imprimante associée', 'TLS/SSL', 'SLP', 'Ecran', 'Police', 'Impression d'écran', 'Préférences', 'Options de démarrage', and 'Langue'. The 'Avancé' section contains several settings: 'Délai de connexion (secondes)' and 'Délai d'inactivité (minutes)' both set to '0'; 'Signal de présence' with 'Oui' selected; 'Activation d'ENPTUI' with 'Oui' selected; 'Informations de connexion IBM i' section with 'Invite de mot de passe' set to 'Utilisation de l'authentification Kerberos, pas d'invite', 'ID utilisateur' set to 'jl', and 'Ignorer l'ouverture de session' with 'Oui' selected. At the bottom are 'OK', 'Annuler', 'Clavier...', and 'Aide' buttons.

# Mise en place sur RDi





# Bien préparer - Eviter les risques

# 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 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 disfonctionnement, 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 leurs mots de passe, qu'ils n'auront pas saisi depuis longtemps...



# Résoudre les problèmes éventuels

# Problèmes souvent rencontrés

- CCSID utilisé lors d'une première configuration, différent du CCSID utilisé pour modifier ou refaire cette configuration
- Incohérence entre le nom sous lequel la machine se connait et le nom sous lequel le domaine la connait  
Pour valider :
  - ping -a 192.168.x.x pour connaître le nom de la machine d'après le DNS
  - Sur l'IBM i :

```
==> CHGTCPDMN
```

```
Host name ..... 'ibmi'
```

# Nettoyage des anciennes installations

- Les objets et fichiers (ifs) liés au SSO sont partout !
- Même sans tentative de configuration antérieurs des résidus de configuration peuvent être présente
- Pour commencer sur de bonnes bases, nettoyez le terrain !

# Nettoyage des anciennes installations

- Un petit avant goût des opérations de nettoyage

```
CLRLIB LIB(QUSRDIRDB)
```

```
DLTLIB LIB(QUSRDIRDB)
```

```
DLTLIB LIB(QUSRDIRCF)
```

```
DLTLIB LIB(QUSRDIRCL)
```

```
QSH CMD('rm -rf /qibm/userdata/os400/dirsrv')
```

```
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.company.com@COMPANY.COM
```

- 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><b>Solution 1:</b> 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><b>Solution 2:</b> Reset the password for the Active Directory Service principal account so that it matches what is in the IBM i keytab list</p> <p><b>Solution 3:</b> 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><b>Solution 1:</b> Since end of 2011 the encryption AES is available for R540 and above. The following document describes this issue: <a href="https://www.ibm.com/support/pages/node/684323">https://www.ibm.com/support/pages/node/684323</a></p> <p><b>Solution 2:</b> Another way is to enable DES on Windows 2008 Active Directory which is described in Microsoft <a href="#">KB 977321</a>.</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)
```

Université IBM i

19 et 20 novembre 2024



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>

MERCS

