Université IBM i

19 et 20 novembre 2024

IBM Innovation Studio Paris

uii2024
#ibmi
#uii2024

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

IBM

common FRANCE

Université IBM i

19 et 20 novembre 2024

IBM i
continuous innovation
continuous integration

GAIA
VOTRE EXPERT IBM i

Centre de services IBM i
- Mutualisé
- A distance

Modernisation
- Accompagnement
- Prototypage

Expertise technique
- Prestations de service (audit, consulting…)
- Transfert de connaissances (workshops)

VOLUBIS
DEVENEZ UN EXPERT

FORMATIONS
SUR SITE
A DISTANCE
INTER
SUR MESURE

COURS EN LIGNE
FORMATS COURS
REPLAYS EN LIGNE

BASE DE CONNAISSANCE
IBM i
EN LIGNE

IBM

IBM i
continuous innovation
continuous integration

GAIA
VOTRE EXPERT IBM i

C'est aussi des produits

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 i
continuous innovation
continuous integration

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

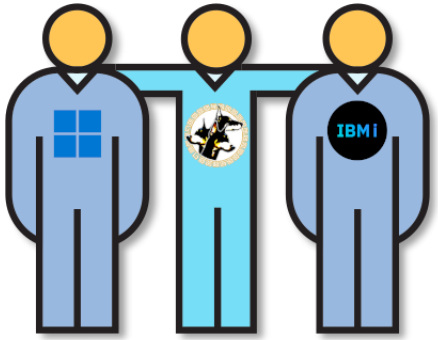
Dialogue entre domaines

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

- **L**ightweight **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

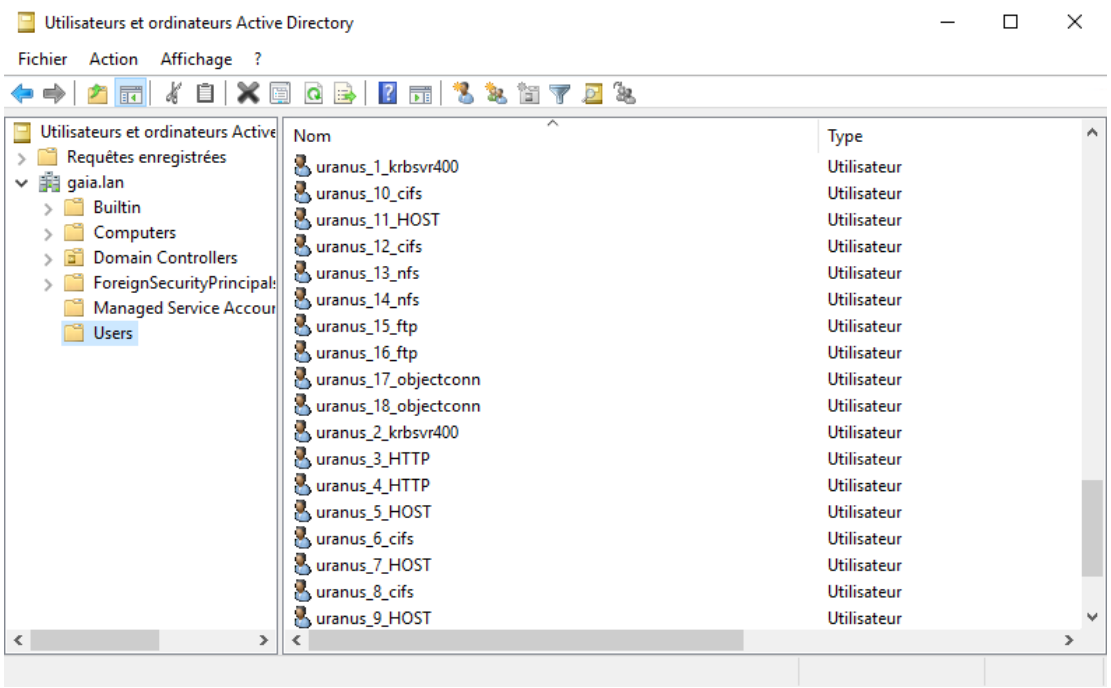
DN	CN	OU	DC
Distinguished Name	Common Name	Organizational Unit	Domain Controller
Relative DN	cn=ibmi_7_HOST,cn=users,dc=GAIA,dc=NET		

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

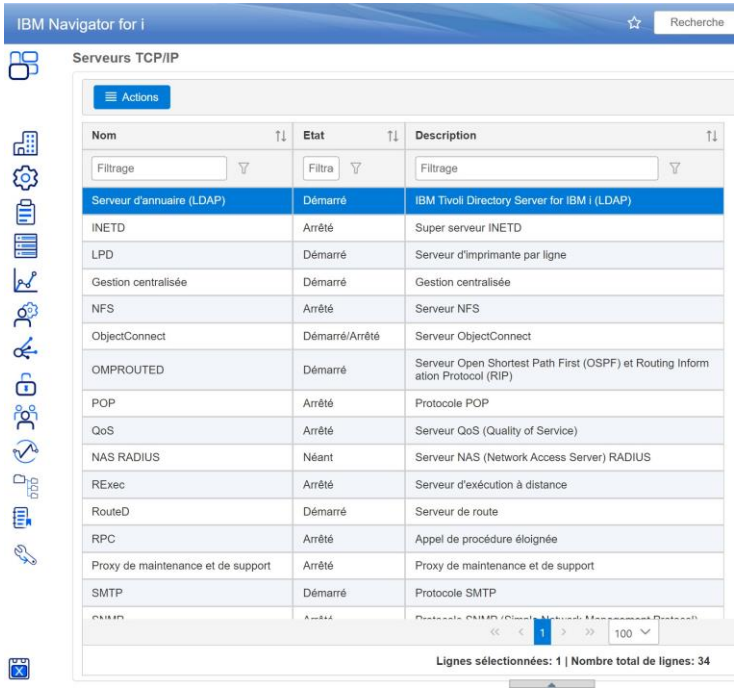
LDAP	LDAPS
389	636

LDAP

Windows

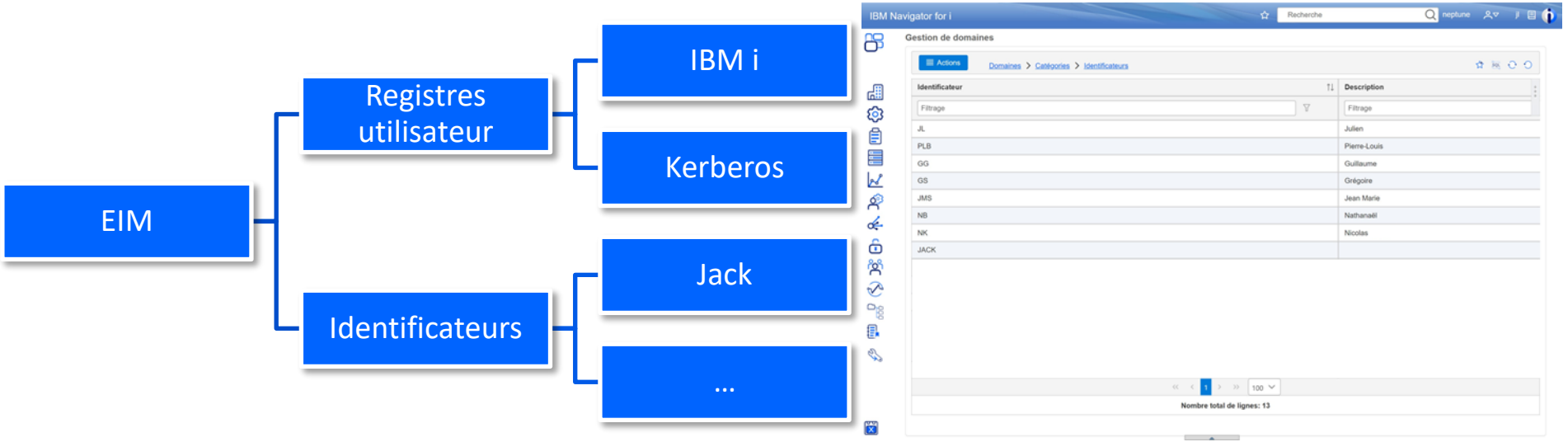


IBM i



EIM

- **E**nterprise **I**dentity **M**apping
- 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

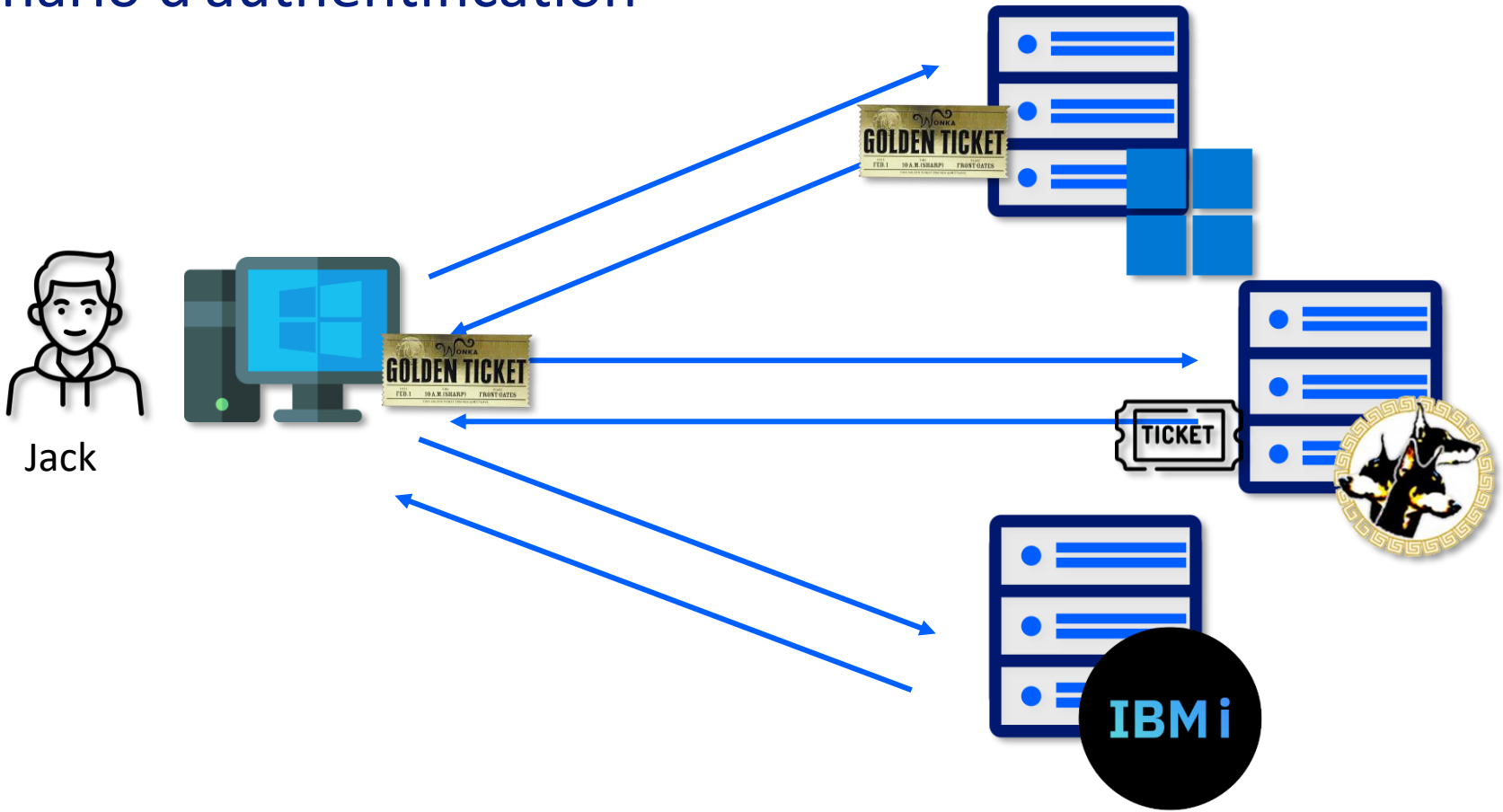
IBM i
continuous innovation
continuous integration

IBM i

IBM

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** réussi ➔ **Kerberos** fourni 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 à un **SPN** dédié (IBM i, ObjectConnect, NetServer…)
- Si le **TGT** valide & **SPN** trouvé dans le **LDAP** de **Kerberos** ➔
  le **KDC** fourni 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**

Université IBM i

19 et 20 novembre 2024

IBM i
continuous innovation
continuous integration

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	

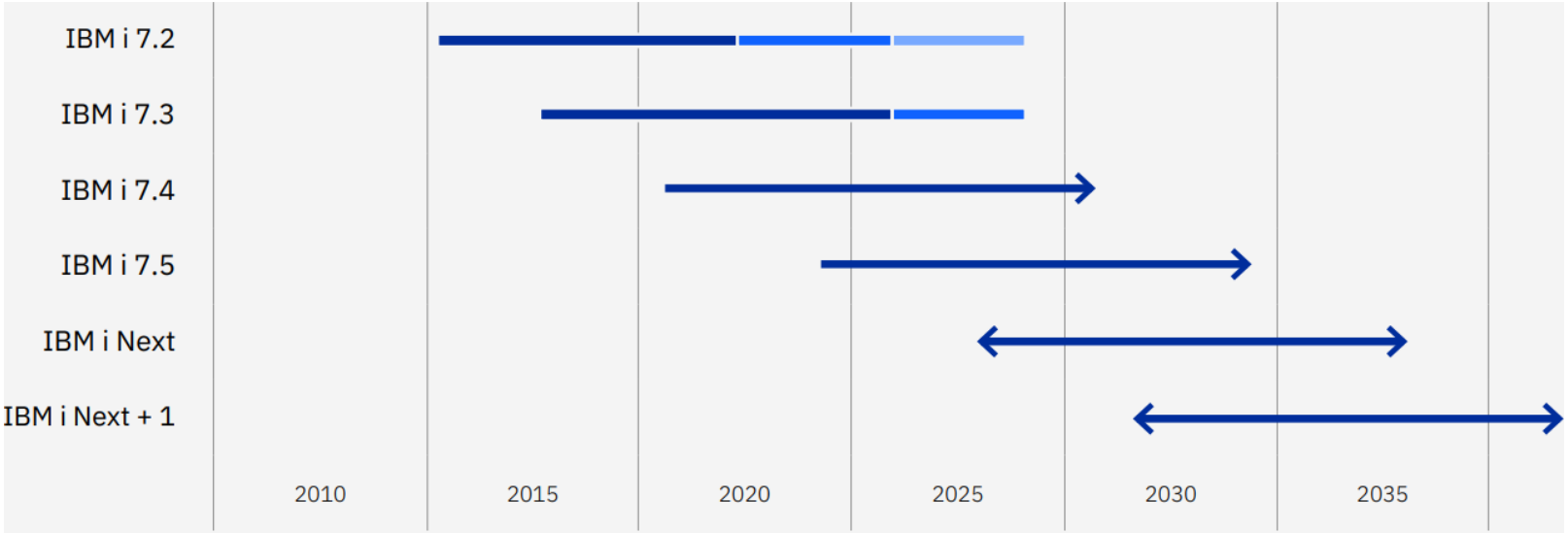
Prérequis - Logiciels nécessaires

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



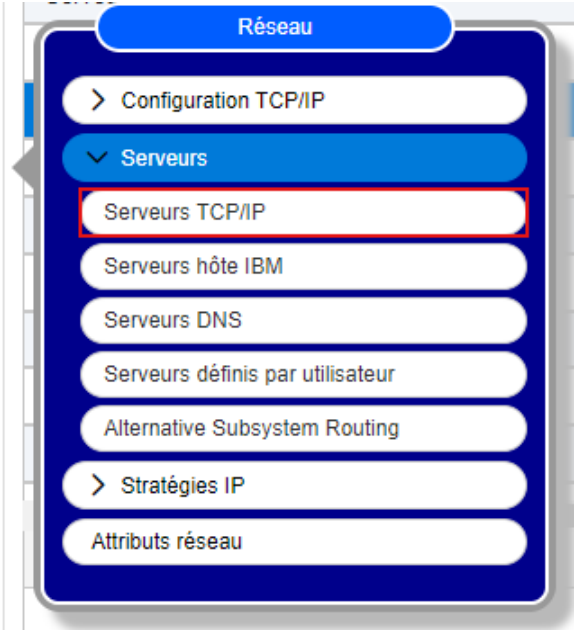
Version	Sortie	Fin du support	Fin du support étendu
V7R3	15/04/2016	30/09/2023	30/09/2026
V7R4	21/06/2019		
V7R5	10/05/2022		

Etapes de mise en œuvre

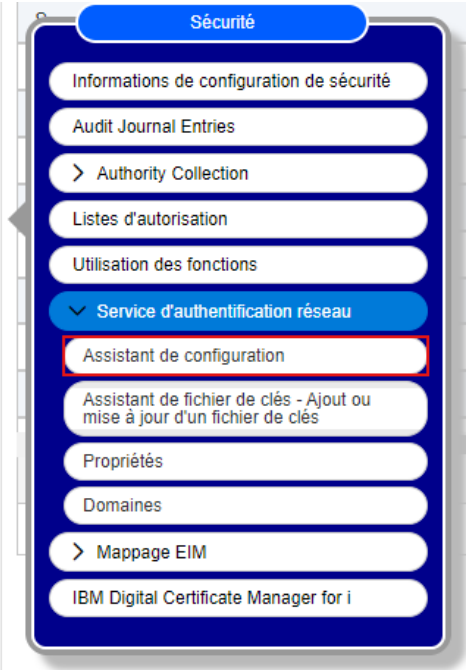
1. Réinitialisation de la configuration du LDAP  ACS
2. Configuration du LDAP  Navigator for i
3. Configuration de Kerberos  Navigator for i
4. Création des utilisateurs des services Kerberos sur l'AD  PowerShell sur l'AD
5. Validation de la configuration via kinit  ACS
6. Configuration du domaine EIM  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

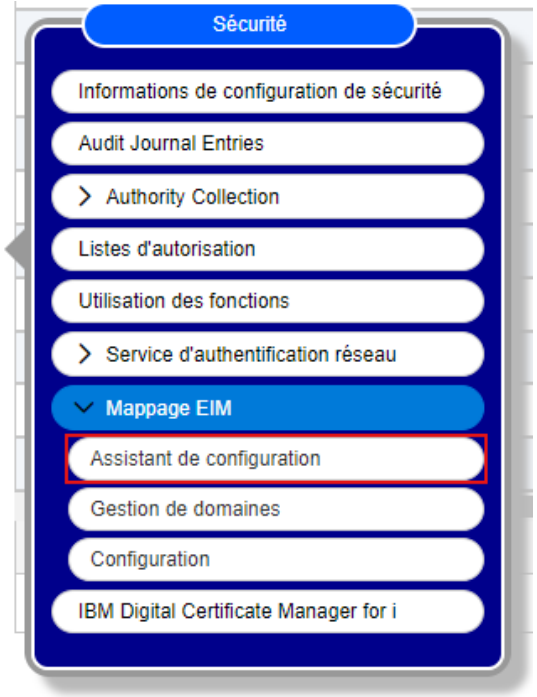
LDAP



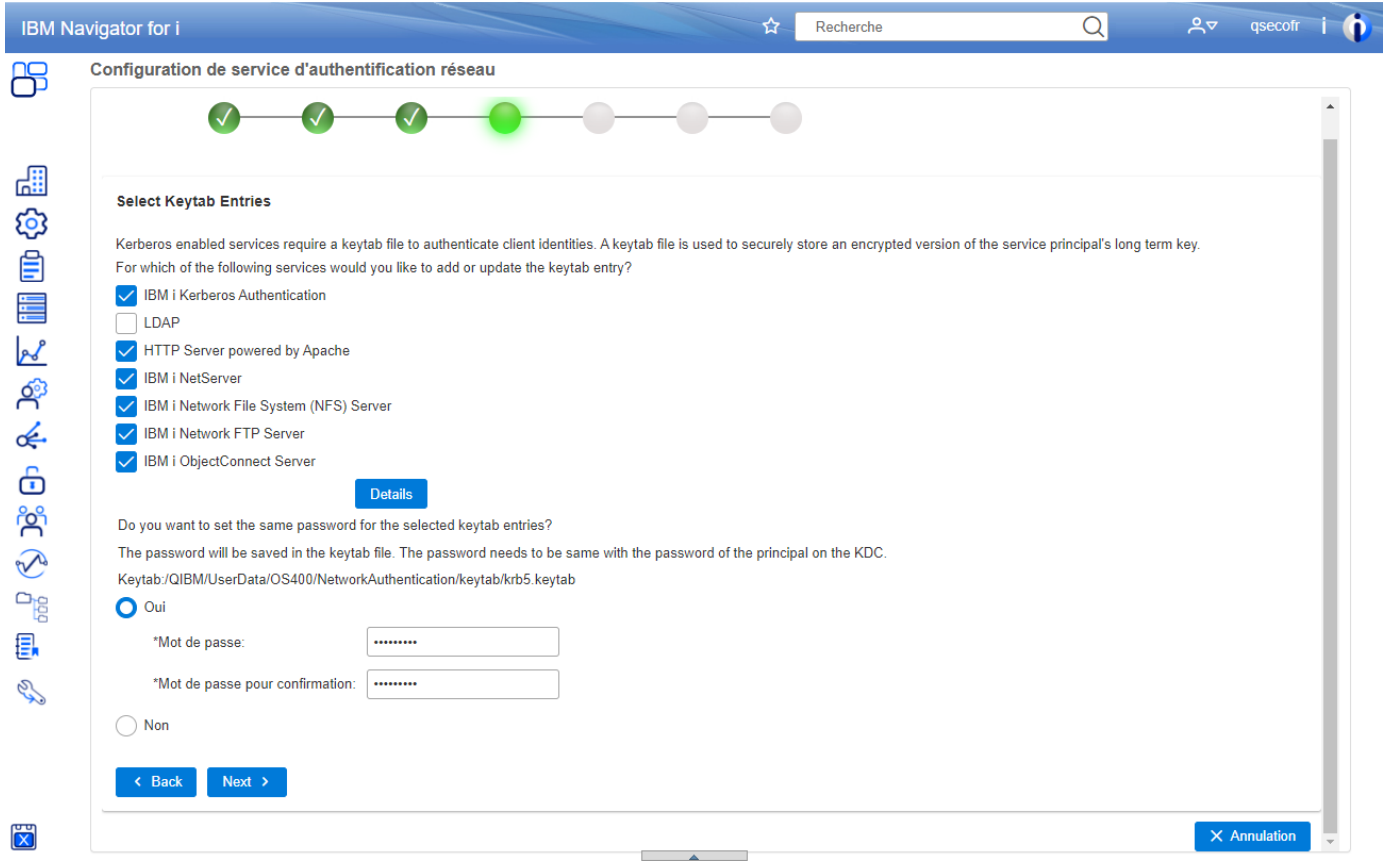
Kerberos



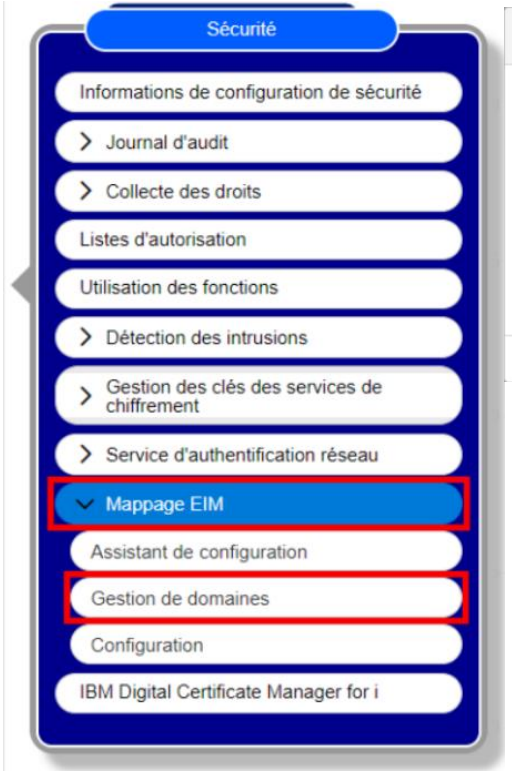
EIM

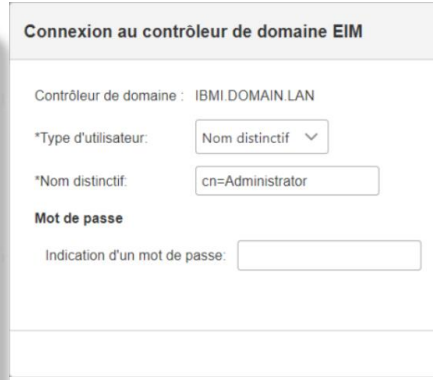


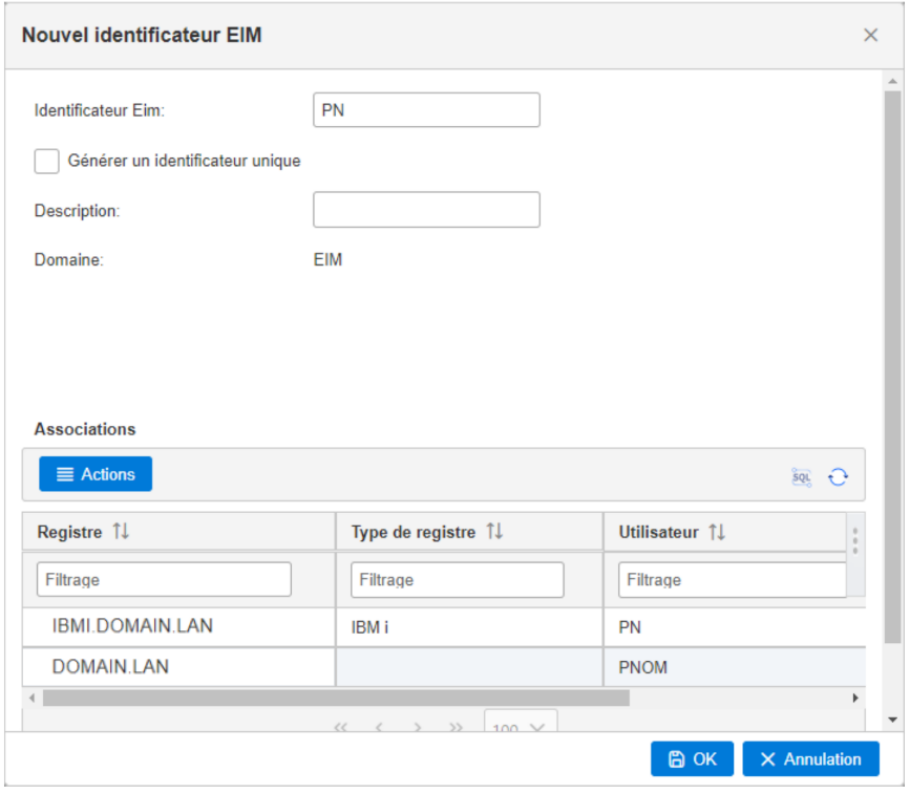
L'aide sera toujours apportée sur l'IBM i à ceux qui la méritent.



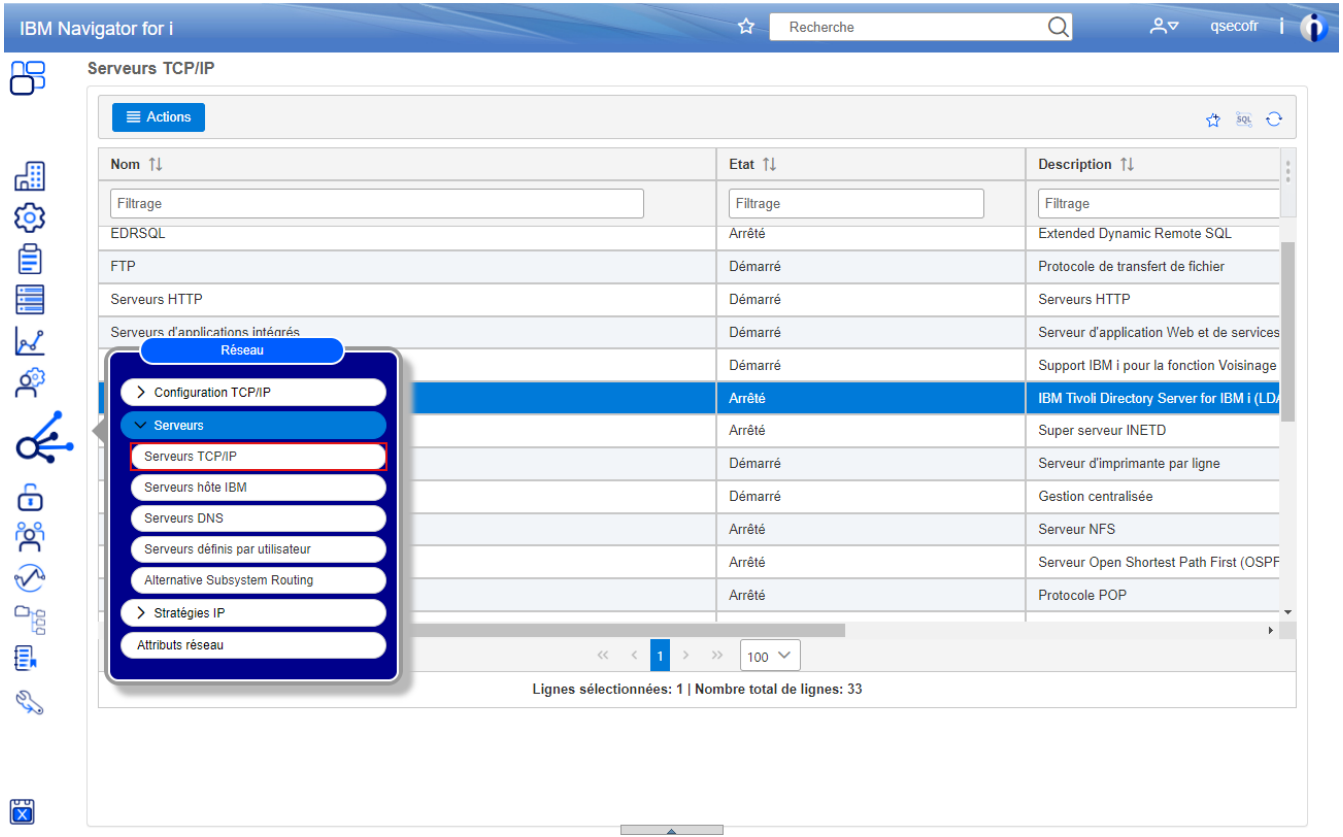
Inscription des associations utilisateurs



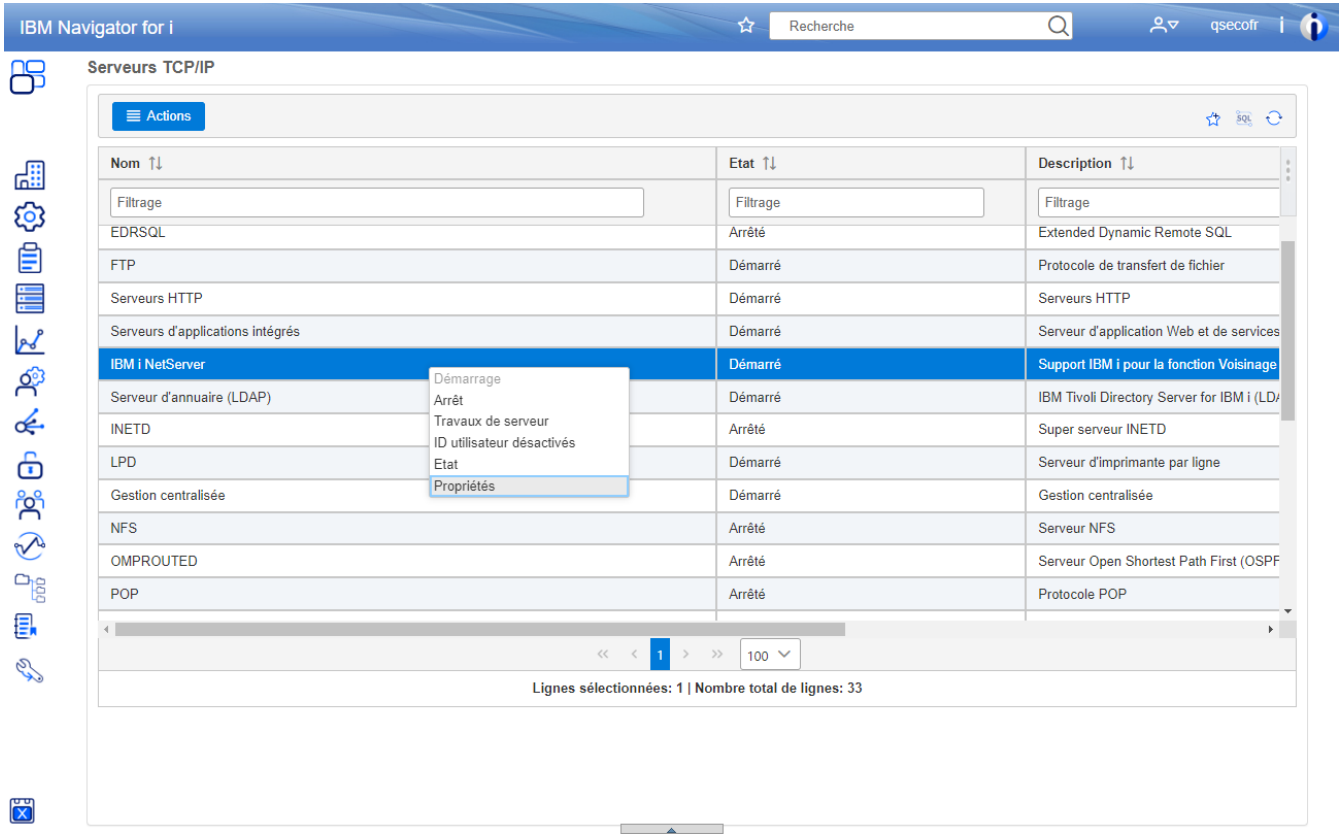




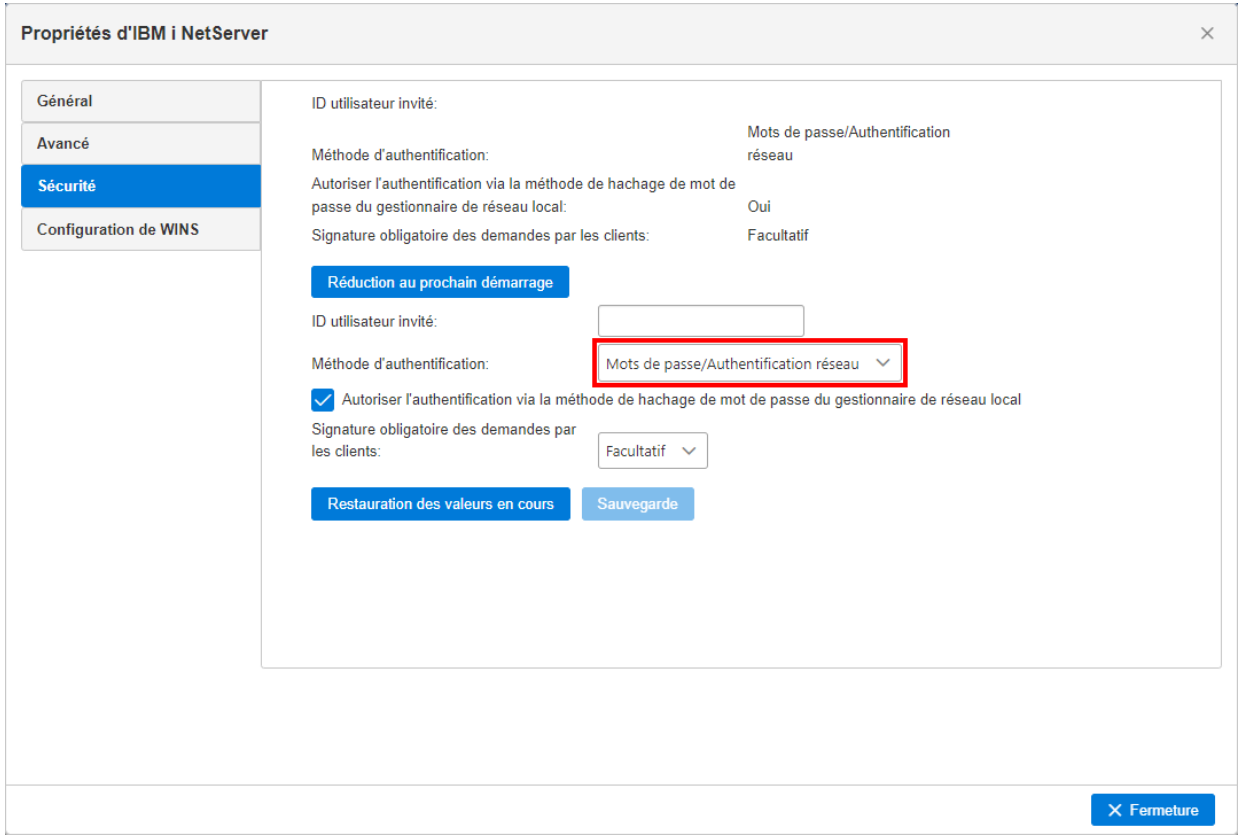
Activation de NetServer - 1



Activation de NetServer - 2

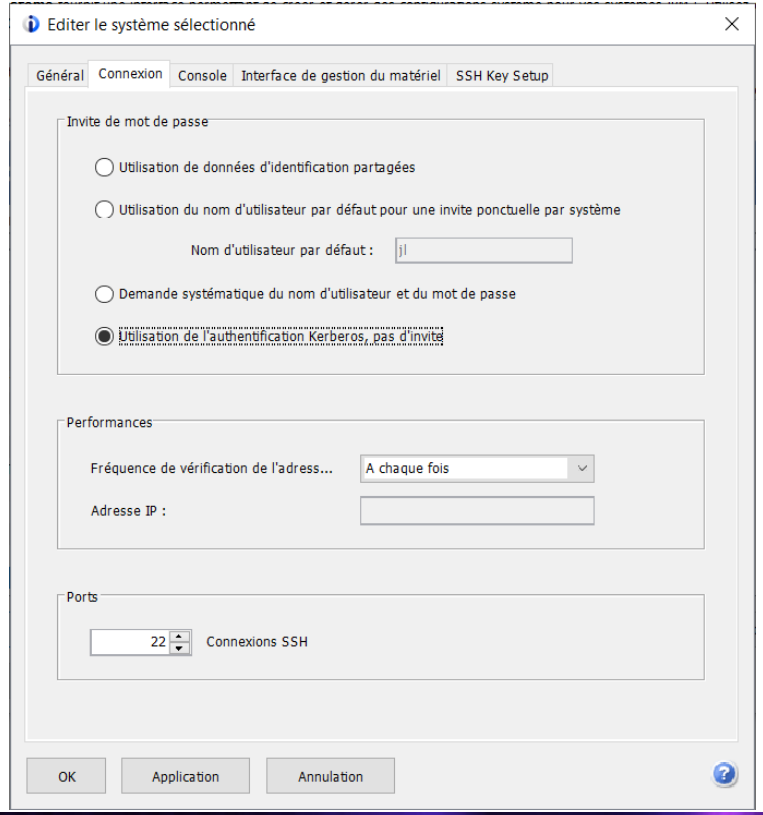


Activation de NetServer - 3

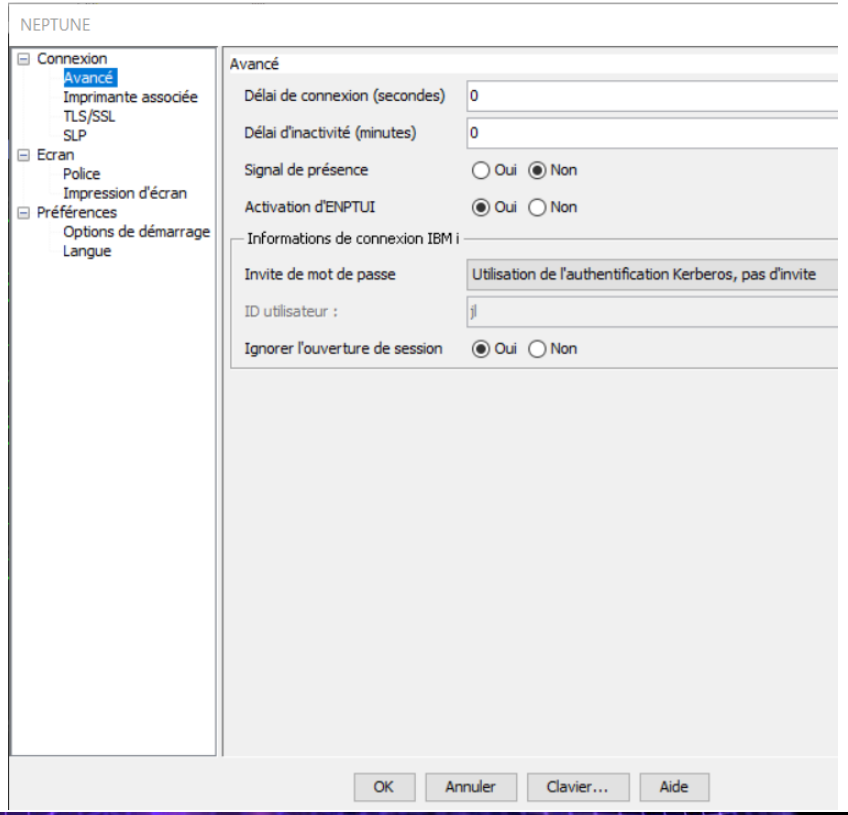


Mise en place sur ACS

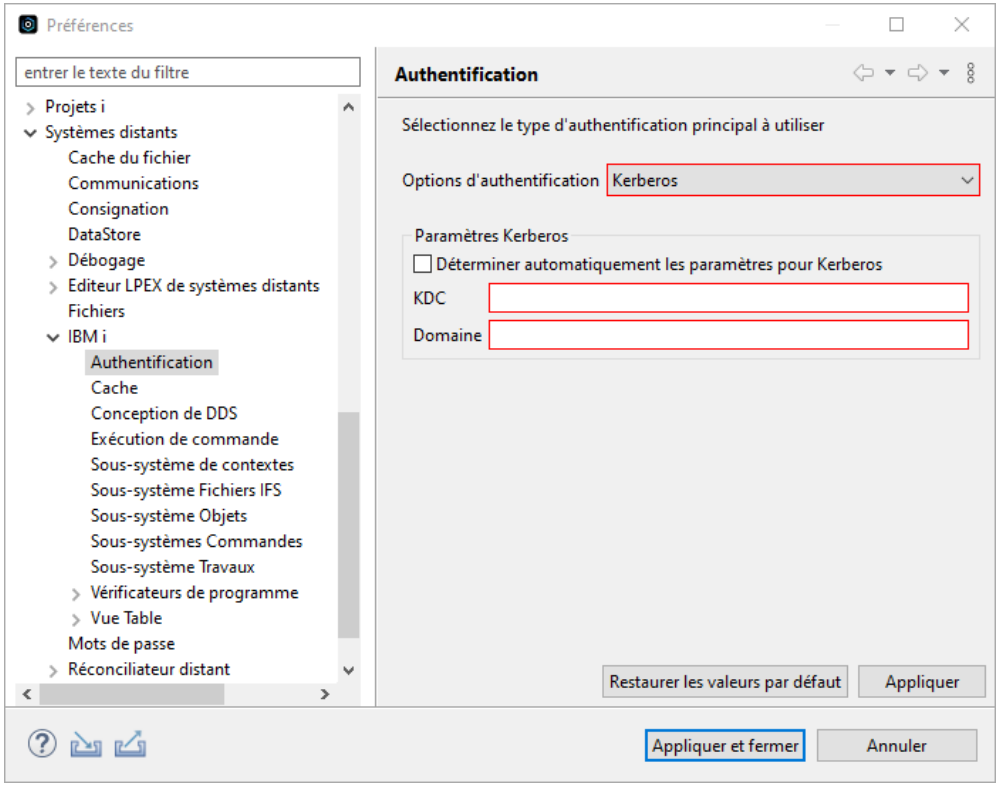
- Gestionnaire de sessions (global)



- Connexion du hod (session)



Mise en place sur RDi



Université IBM i

19 et 20 novembre 2024

IBM i
continuous innovation
continuous integration

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…

Université IBM i

19 et 20 novembre 2024

IBM i
continuous innovation
continuous integration

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

- 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 krb**svr**400 et krb**srv**400 (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 Systemi 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.	The SPN (Service Principle Name) is not or multiple available in the Windows Active Directory. ***Solution 1:*** We can run the command "***ldifde -m -f output.txt***" from Windows Active Directory to create a list of all the users and we can check for duplicate service principal entries. ***Solution 2:*** Reset the password for the Active Directory Service principal account so that it matches what is in the IBM i keytab list ***Solution 3:*** Check information for symptom/error code 96c73a0e
0x96c73a0e	EUVF06014E Unable to obtain initial credentials. Status 0x96c73a0e - Encryption type is not supported.	Often seen on Windows 2008 domains and Windows 7 systems. This domain do not support DES encryption by default. ***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 ***Solution 2:*** Another way is to enable DES on Windows 2008 Active Directory which is described in Microsoft KB 977321.

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)
```

IBM i
continuous innovation
continuous integration

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


MERCI