Power Week

Université IBM i 2019

22 et 23 mai

IBM Client Center Paris

S22 - Comment sécuriser l'IBM i à partir de l'Active Directory ?

Dominique GAYTE
NoToS
dgayte@notos.fr – *06 30 17 02 55*

NoToS

- Expertise autour de l'IBM i

- Sécurité
- PHP sur IBM i
- DB2 Web Query
- Développement de progiciels

lorena

distant.backup

monitor i

power.gdpr

power.sign

power.spool

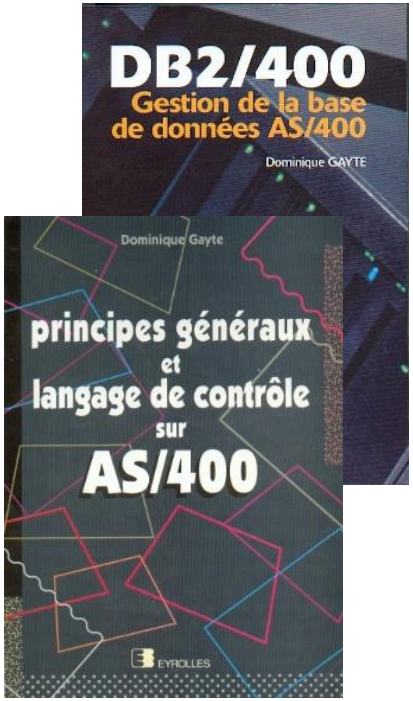
AD-iCT

ON S'ASSOCIE !

iDINFO
L'INGENIERIE DIGITALE

Dominique GAYTE

- Intervenant « AS/400 » depuis 1990
  - Au nom d'IBM
  - Plus de 1 000 journées
- Sécurité
  - Audit
  - GDPR
  - Mise en œuvre : SSO, SSL, sécurisation de la base de données…
- Développements complexes
  - Sécurité
    - Points d'exit
  - API système
  - RPG IV
    - XML
    - Accès bases de données distantes



Plan de la présentation

- Introduction
- Sécurisation des connexions à l'IBM i
  - SSO avec EIM
  - AD-iCT
- Sécurisation des applications et des données de l'IBM i
  - La problématique
  - Solution
  - Organisation proposée
  - AD-iCT

Power Week

Université IBM i

22 et 23 mai 2019

Introduction

IBM

Le contexte

- L'AD (Active Directory de Microsoft) est omniprésent dans les entreprises
- Il sert notamment à centraliser
  - Les authentifications dans le monde Windows
  - La gestion des habilitations
- D'où les questions récurrentes

Comment peut-on s'appuyer sur l'AD pour sécuriser :
- Les connexions à l'IBM i
- Les données et les applications de l'IBM i ?

- L'idée est d'avoir un centre unique de gestion de la Sécurité et des habilitations

L’authentification

- SSO (Single Sign On) avec EIM (*Enterprise Identity Mapping*)
- L’authentification est réalisée au niveau de l’AD seulement
  - Complexité du mot de passe
  - Différentes méthodes possibles
    - Carte à puce
    - Biométrie
    - …
- L’IBM i fait confiance à cette authentification
  - Pas de mot de passe échangé

Les habilitations

- Les habilitations définissent ce que chacun a le droit de faire
- Au niveau de Windows, elles sont gérées avec les groupes de Sécurité de l'AD
- L'idée est de s'appuyer sur ces groupes pour la Sécurité IBM i
- Assure une centralisation de la configuration
  - Plus de Sécurité

Power Week

Université IBM i

22 et 23 mai 2019

Le SSO avec EIM

L'IBM i fait confiance à l'AD !

IBM

Principes

- L'authentification se fait au niveau de l'AD, pas de l'IBM i
  - Les profils utilisateurs peuvent avoir PASSWORD(*NONE)
- Permet une augmentation du niveau de Sécurité des mots de passe
  - Souvent une demande forte des auditeurs
- Simplicité d'accès pour les utilisateurs
  - Un seul mot de passe à retenir, celui de l'AD
- Suppression de l'écran d'ouverture (Telnet ou autres)
- Fini les soucis d'accès à l'IFS et de profils désactivés
- Fiable
- S'appuie sur des produits standards de l'IBM i et de Windows Server

Principes (2)

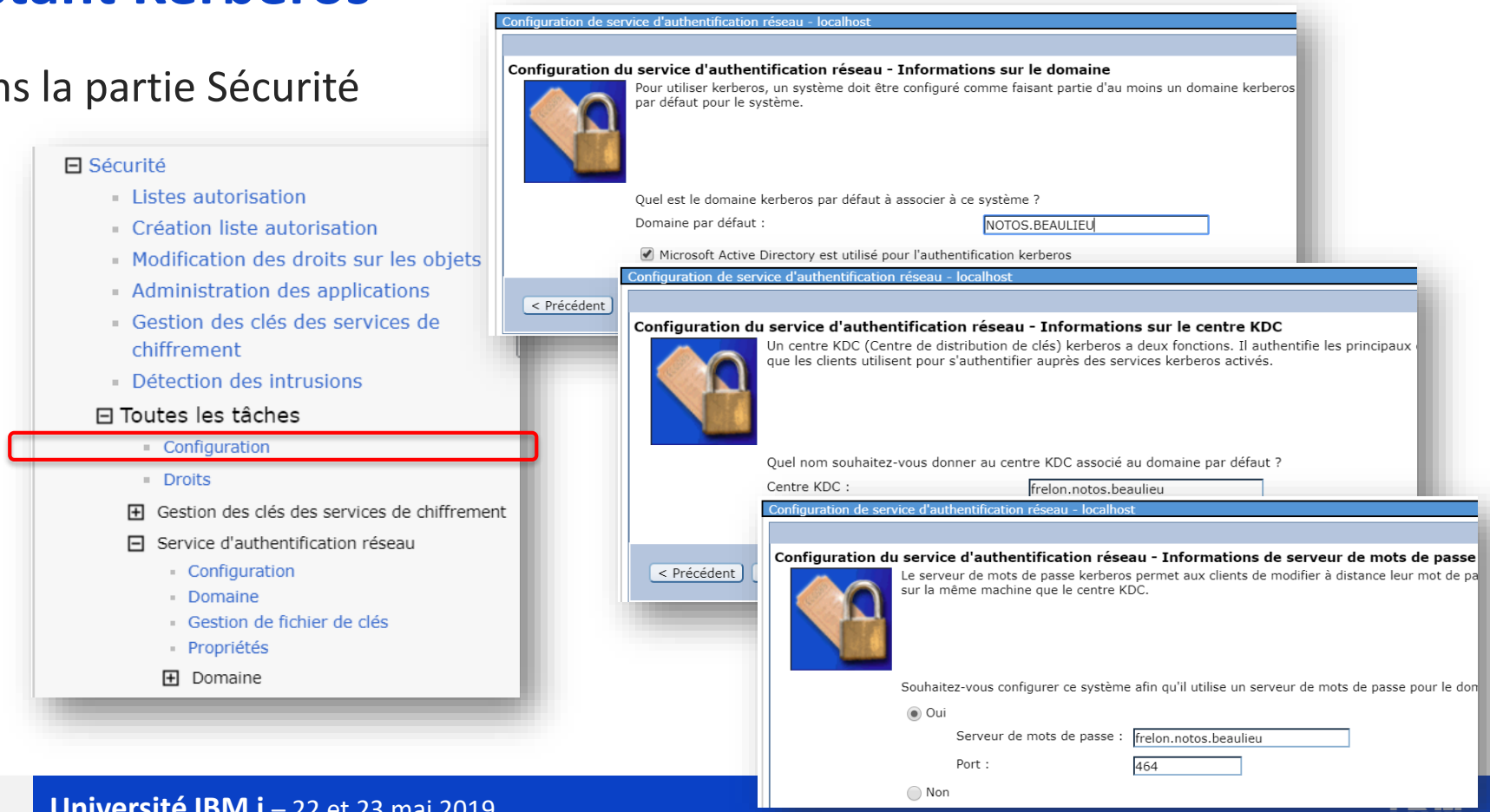
- Le SSO s'appuie sur 2 niveaux
  - Authentification avec Kerberos (*Network Authentication Service*)
  - Autorisation avec EIM (*Enterprise Identity Mapping*)
- L'IBM i fait confiance à l'authentification réalisée par Kerberos (l'AD)
  - Réalisée lors de l'ouverture de la session Windows
  - Pas d'échange de mot de passe ultérieur

Configuration de Kerberos

- Via un assistant graphique
  - System i Navigator (à abandonner…)
  - Navigator for i (à privilégier)
- Génère
  - Des clés coté IBM i
  - Un fichier de commande (.BAT) à appliquer sur un contrôleur de domaine
    - Création d'une douzaine de comptes de service
- La configuration du réseau doit être parfaite
  - Nommage de la partition
  - DNS et reverse
  - Horloges

Assistant Kerberos

- Dans la partie Sécurité

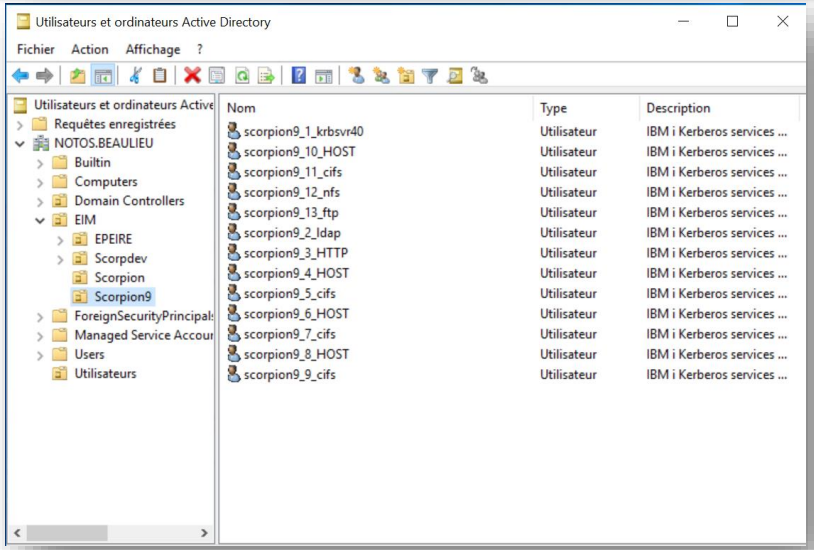


Kerberos coté AD

- Une douzaine de comptes sont créés à partir du fichier de commande généré

```
DSADD user "cn=scorpion9_1_krbsvr40,ou=Scorpion9,ou=EIM,dc=NOTOS,dc=BEAULIEU" -pwd M0nPWDxx  -display scorpion9_1_krbsvr40 -pwdneverexpires yes -desc "IBM i Kerberos services on system scorpion9"
KTPASS -MAPUSER scorpion9_1_krbsvr40 -PRINC krbsvr400/scorpion9.notos.beaulieu@NOTOS.BEAULIEU -PASS M0nPWDxx -mapop set -crypto All -ptype KRB5_NT_PRINCIPAL

DSADD user "cn=scorpion9_2_ldap,ou=Scorpion9,ou=EIM,dc=NOTOS,dc=BEAULIEU" -pwd M0nPWDxx -display scorpion9_2_ldap -pwdneverexpires yes -desc "IBM i Kerberos services on system scorpion9"
KTPASS -MAPUSER scorpion9_2_ldap -PRINC ldap/scorpion9.notos.beaulieu@NOTOS.BEAULIEU -PASS M0nPWDxx -mapop set -crypto All -ptype KRB5_NT_PRINCIPAL
...
```

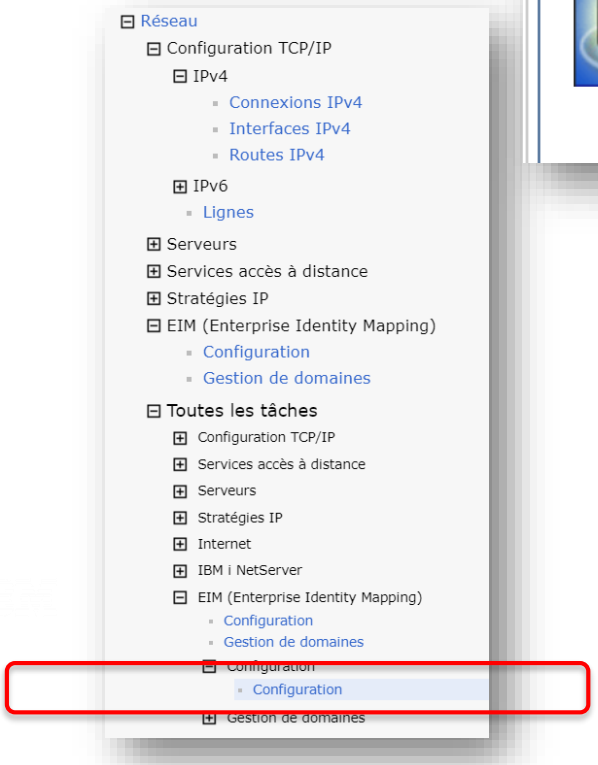


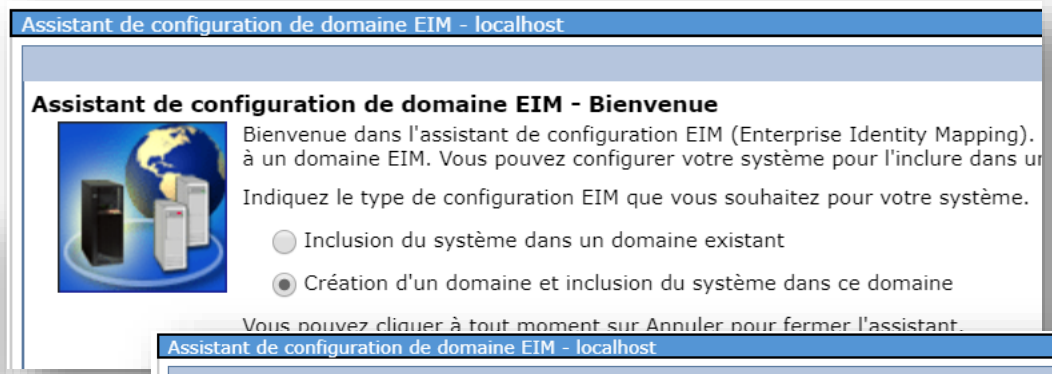
EIM : principes

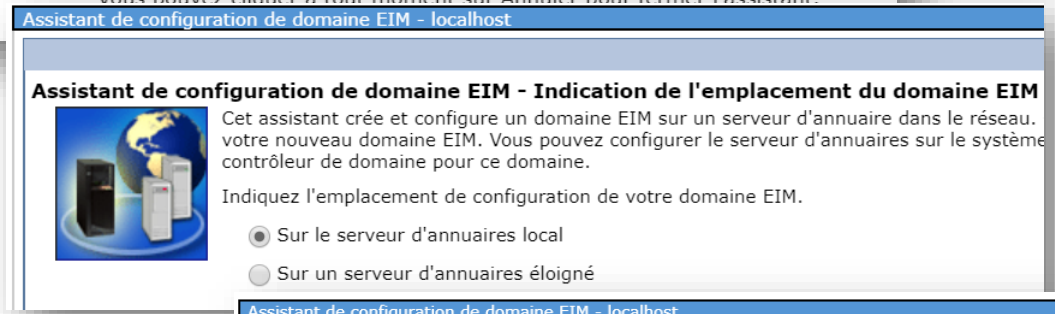
- Association entre
  - Source (compte de l'AD)
  - Cible (profil utilisateur IBM i)
- S'appuie sur l'annuaire LDAP de l'IBM i
  - IBM Tivoli Directory Server for IBM i
- Très souple
  - Pas de loi du tout ou rien
  - Chaque utilisateur peut participer (ou ne pas participer) à EIM
  - On peut avoir des sessions SSO et non SSO sur le même poste

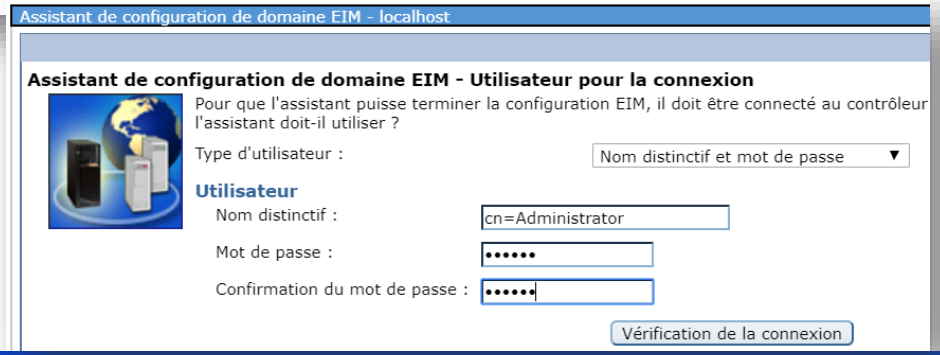
Assistant EIM

- Dans Réseau



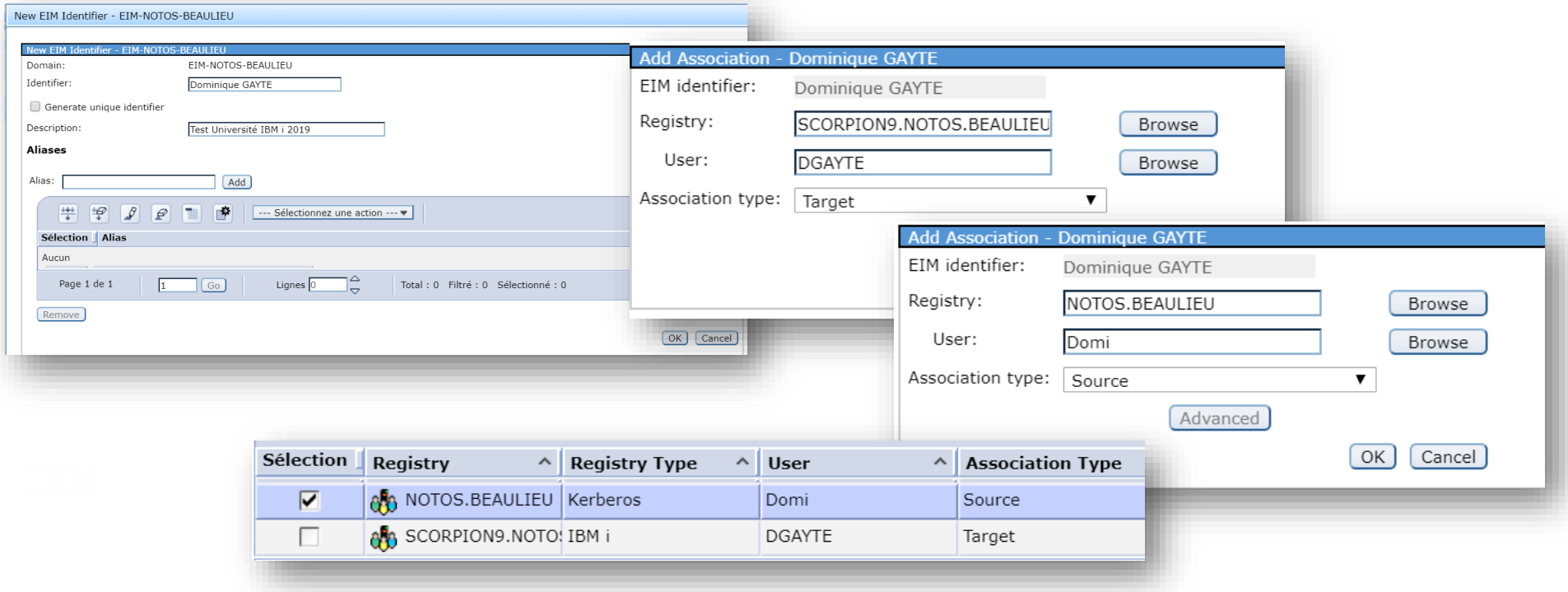






Création des associations

- Se connecter au domaine et ouvrir Identificateurs

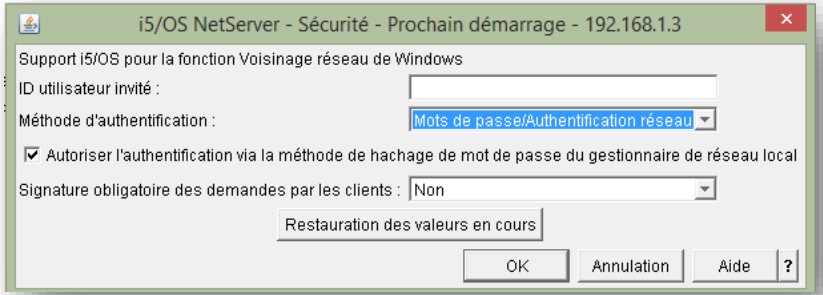


Services supportés

- Tout ce qui est Client Access et ACS
  - Émulation écran
  - ODBC/JDBC
  - Transfert de fichiers
- Partage de fichiers Windows (NetServer)
- HTTP Server (Web)
- FTP, LDAP, QNTC…

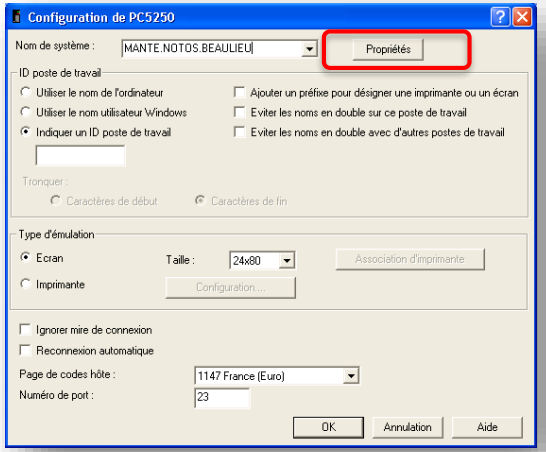
Configuration des serveurs

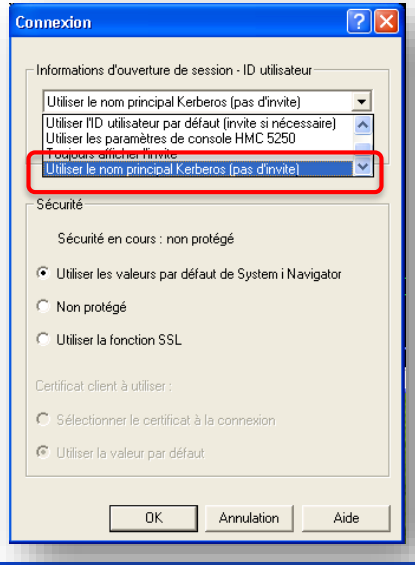
- Telnet
  - Valeur système QRMTSIGN à *VERIFY ou *SAMEPRF
- Configurer le serveur i5 OS NetServer pour qu'il accepte Kerberos
  - Sécurité/prochain démarrage
  - Authentification réseau = Kerberos
  - Mixte avec « Mots de passe/Authentification réseau »
  - Redémarrer le serveur NetServer (attention aux connexions en cours!)



Configuration des clients

- Partage de fichiers Windows : rien à faire
- Client Access (!) ou ACS
  - Modifier les propriétés de la connexion
    - Utiliser le nom principal Kerberos





AD-iCT : AD to i Communication Tools

- Une quinzaine de clics par association
  - Une source
  - Une cible par partition
- Impossible pour plusieurs centaines d'utilisateurs
- AD-iCT solution NoToS
  - Pour tout ce qui est interconnexion entre un IBM i et l'AD
    - Saisie en masse des identifiants
      - A partir d'un fichier ou d'un écran vert
    - Réplication vers un autre système (backup, autres partitions de prod ou de dev…)
      - Les réplications habituelles ne fonctionnent pas
      - Souvent oublié dans les déploiements
    - Et sécurisation (mais c'est le chapitre suivant)

Power Week

Université IBM i

22 et 23 mai 2019

Les autorisations IBM i basées sur l'AD

Comment sécuriser les applications et les données IBM i à partir de l'AD

IBM

La demande

- Question récurrente des Services Informatique

> Comment utiliser l'AD pour sécuriser les données et les applications IBM i ?

- Objectif : gestion unique des habilitations
  - Un seul endroit à gérer, un seul endroit à contrôler : l'AD
- Les habilitations sont réalisées au travers des groupes de Sécurité de l'AD

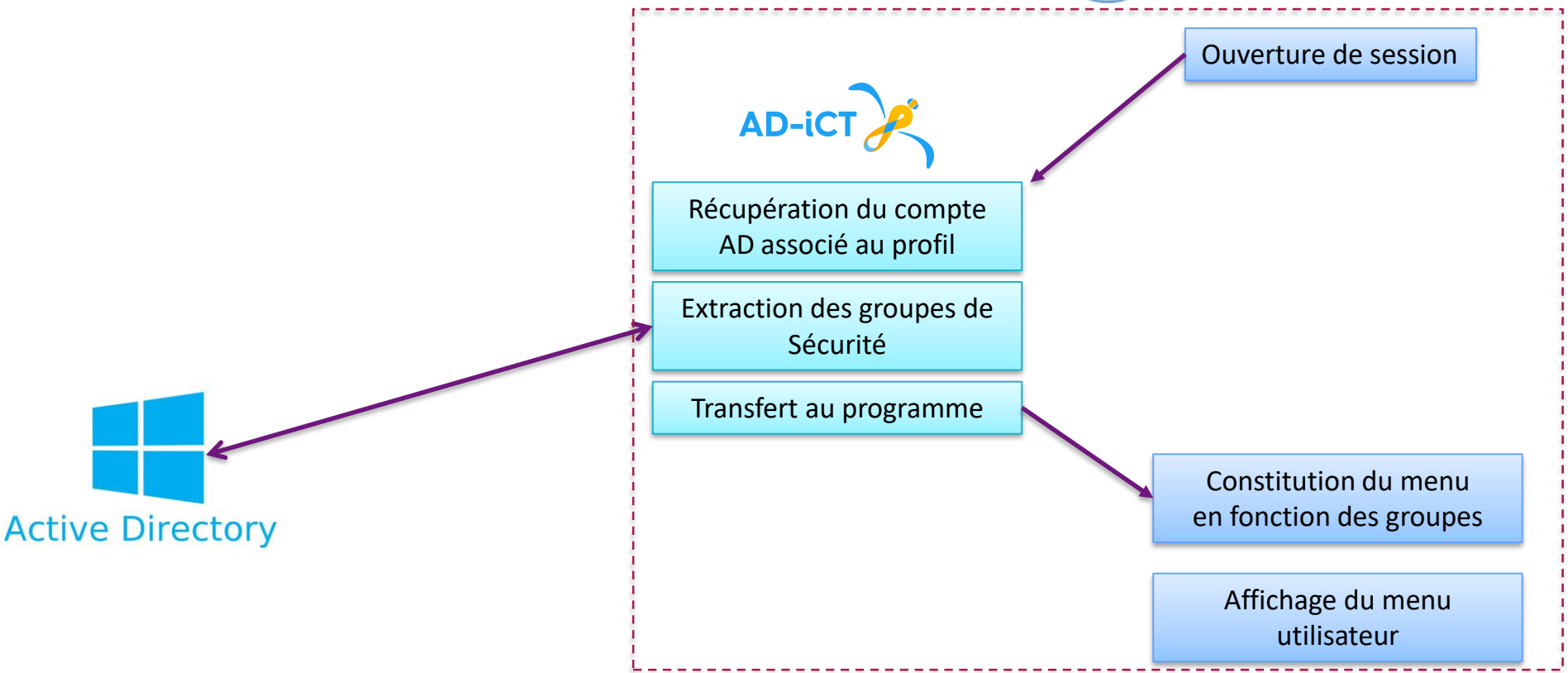
La problématique

- Un programme IBM i doit récupérer dynamiquement les groupes de Sécurité de l'AD auquel appartient un profil
  - Rien de trivial
- La Sécurité en place coté IBM i est faible ou inexistante
- NoToS a développé une application
  - Extraction des groupes Sécurité d'un profil et intégration dans les structures de données IBM i
  - Vérification si un profil appartient à un groupe

La structure applicative proposée

- Création d'un menu dynamique en fonction des groupes de Sécurité de l'AD
- Éventuellement vérification de l'appartenance à un groupe avant d'utiliser une fonction ou une ressource particulière
- Il faut pouvoir faire confiance à l'application
  - Pas de lignes de commandes
  - Droits des utilisateurs adaptés (pas de *ALLOBJ)

Schéma de l'organisation proposée



La base de données

- Droits publics : *EXCLUDE
- Propriétaire : *ALL
- Y a-t-il des accès directs ?
  - ODBC, JDBC, QUERY…
  - Utilisation d'un groupe LECTEUR (*USE)
  - Éventuellement d'un groupe MODIF (*CHANGE, à éviter)
- Utilisation recommandée d'une liste d'autorisation pour une gestion simplifiée

Les applications

- Tous les accès applicatifs se font par la délégation de droits
- Les programmes « points d'entrées » sont avec délégation de droits
  - USRPRF(*OWNER)
  - Propriétaire du programme = propriétaire des données
- Les autres programmes
  - USEADPAUT(*YES) qui est la valeur par défaut
  - Héritage de la délégation de droits du niveau supérieur

AD-iCT

- AD to i Communication Tools
- Ensemble de fonctions qui facilitent l'intégration de l'IBM i dans un AD
- Objectif : renforcement de la Sécurité
- Trois composants
  - Tools for EIM
    - Gestion aisée et automatisée des identifiants EIM
  - Backup for EIM
    - Réplication des identifiants EIM entre différentes partitions IBM i
  - AD Security for i
    - Les applications IBM i traditionnelles s'appuient sur les groupes de Sécurité de l'AD pour la sécurisation des applications et des données

AD-iCT (2)

- Ensemble d'objets
  - Programmes
  - Programmes de services, procédures et fonctions
  - Méthodologie
- A utiliser tel quel par vos équipes
- Ou intégré par nos collaborateurs lors des prestations de consolidation du niveau de Sécurité de vos systèmes

Dominique GAYTE
NoToS
dgayte@notos.fr – *06 30 17 02 55*