Dominique GAYTE
06 30 17 02 55
dominique@gayte.it - https://i.gayte.it

Webinar SSO & IBM i

Déploiement de l'authentification unique (SSO) entre votre environnement IBM i et l'Active Directory (AD)

Dominique GAYTE

I.GAYTE.IT
IBM i Security Software & Services

- Docteur ès sciences
- Intervenant « AS/400 » depuis 1990
- Expert
  - Sécurité
    - Interventions sur la sécurité de plus de 350 partitions IBM i
  - Développements complexes
- Auteur de plusieurs livres sur le sujet
- Formateur
- Conférencier
- Reconnaissance mondiale
- Fondateur de I.GAYTE.IT

Dominique GAYTE - suite

- Distingué par IBM comme IBM Champion
- Décerné aux experts reconnus par IBM

- Reconnu pour son Innovation et sa Recherche

AD-iCT

STR-iCT

FRANCE 2030

bpifrance

Securit.i 2026

- Evènement international Sécurité IBM i
  - https://i.gayte.it/evenement-securit-i-securite-ibm-i/
  - https://www.youtube.com/@igayteit
- Du mardi 09 septembre 2026 09H00
- Au mercredi 10 septembre 2026 17H00
- À Montpellier

- Edition 2027
  - 15 et 16 septembre 2027

La problématique

- Les identifiants/mots de passe sont les protections essentielles de nos systèmes d'information
- Les utilisateurs ont x identifiants pour les applications locales
  - Windows
  - Messagerie
  - Différents IBM i
  - Serveurs Web
  - …
- Une surcharge de travail pour les administrateurs
  - Gestion de plusieurs solutions et plates-formes d'authentification
    1 utilisateur = n comptes, n userID, n mots de passe
  - 30% (de 20 à 40) des appels vers le Help Desk de l'entreprise concernent directement des problèmes d'accès rencontrés par les utilisateurs lors de leur authentification
  - D'où une simplification des processus de connexions utilisateurs pouvant induire des failles de sécurité
- Pour les utilisateurs
  - Saisie au quotidien de plusieurs identifiants et mots de passe pour accéder aux données et applications de l'entreprise
  - Gestion de multiples identifiants / mots de passe et des règles associées
  - Attention aux transgressions des règles de sécurité
- Les auditeurs souhaitent des politiques de gestion des comptes plus strictes
  - Notamment un renforcement de la politique de mots de passe

SSO : « Single Sign-On »

- Système de signature unique
- Solution qui permet aux utilisateurs d'un réseau d'entreprise d'accéder à l'ensemble des ressources autorisées, sur la base d'une authentification unique effectuée lors de l'accès initial au réseau
- Objectifs
  - Simplifier les procédures d’authentification des utilisateurs
  - Renforcer le niveau de sécurité du système d’information
  - Rationaliser la gestion des comptes
- Nous allons nous placer dans le contexte d’un réseau Microsoft, centré sur un Active Directory (AD)

Le SSO entre l'IBM i et l'AD

- Deux couches distinctes
- **Kerberos** pour l'authentification
  - Le lien avec l'AD proprement dit
- **EIM** pour l'association entre les comptes AD et les profils utilisateurs
  - Les associations entre les comptes AD et les profils IBM i
- Solution très efficace et très performante
- Plus de 20 ans de recul
- Près de 400 partitions IBM i installées

Mais…

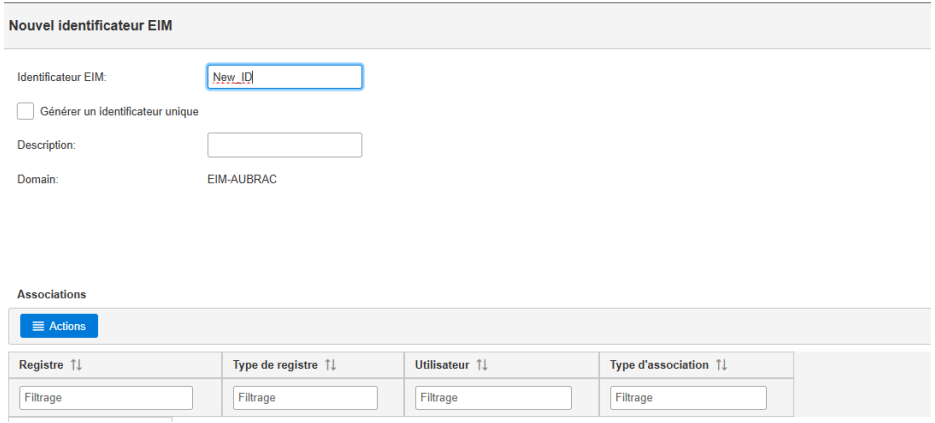
- La saisie des associations est pénible
  - Une quinzaine de clics de souris par association (par utilisateur et par partition) via Navigator for i
  - Pas de possibilité d'intégration dans les processus d'enrôlement de l'entreprise
- Pas d'outils pour manager les comptes
- Pas de mise à jour des backups via les outils de réplication logicielle
- Pas de fonctions d'audit
- Pas d'extraction des comptes pour remplir de nouvelles partition
- Sauvegardes et restaurations complexes
- …

La couche Kerberos

- Souvent la couche la plus complexe à mettre en œuvre
- Assez technique à configurer
  - AD
    - Kerberos
  - IBM i
  - DNS
  - Réseau
- Nécessite un admin du domaine AD
- Et un officier de sécurité IBM i
  - Navigator for i doit être opérationnel

La couche EIM

- Utilise l’annuaire LDAP de l’IBM i
  - Il faut qu’il soit opérationnel !
- Besoin de définir une association entre
  - Un compte AD
  - Un profil utilisateur IBM i pour une partition
- 15 clics de souris par utilisateur avec Navigator for i !



Application supportant le SSO

- Les applications doivent accepter le SSO avec Kerberos
- ACS (et ancien Client Access)
  - 5250
  - SQL ODBC/JDBC
  - Transfert de fichiers
- NetServer (partage de fichier de Windows)
- Apache IBM i (serveur Web)
- FTP, NFS, LDAP
- Et certaines applications…

Les profils utilisateurs concernés

- A choisir, pas de tout ou rien
- Idéal pour les utilisateurs métier
- Pour les administrateurs c'est plus discutable !
- Idéalement, on peut avoir un mot de passe à *NONE pour les profils qui ne font que du SSO
  - Pas de péremption du mot de passe
  - Pas de profils désactivés (IBM i ou NetServer)
- Apporte une réponse aux audits qui réclament une stratégie de mot de passe plus complexe
  - Mais imparfaite pour les profils qui ont un mot de passe <> *NONE

Mais…

- La saisie des associations est pénible
  - Une quinzaine de clics de souris par association (par utilisateur et par partition) via Navigator for i
  - Pas de possibilité d'intégration dans les processus d'enrôlement de l'entreprise
- Pas d'outils pour manager les comptes
- Pas de mise à jour des backups via les outils de réplication logicielle
- Pas de fonctions d'audit
- Pas d'extraction des comptes pour remplir de nouvelles partitions…
- Sauvegardes et restaurations complexes

AD-iCT c’est

- Un outil complet qui comble tous les manques identifiés
  - Importation massive des comptes (csv ou PF)
  - Interface pour création/suppression des comptes (écran vert, commande, PS, WS)
  - Management des associations
    - Profils inexistants
    - Doublons
    - Comptes à pouvoir (*ALLOBJ)
  - Mise à jour du backup
  - Extraction des données dans un fichier
    - Sauvegarde (sinon il faut quasiment une option 21)
    - Alimentation de nouvelles partitions
  - Gestion centralisée

Interfaces

- Écran vert
- Graphique
  - Client lourd Windows
- API REST

Les APIs

- Web Services REST qui permettent
  - De créer les profils utilisateur et les associations EIM
  - De supprimer un profil et ses associations
- Idéal pour piloter le changement à partir de l'AD, en PowerShell

```
# Exemple d'utilisation des APIs d'AD-iCT
# Création d'un profil utilisateur et d'une association
# AD-iCT à partir de version 2.5
#
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("Content-Type", "application/json")
$headers.Add("Authorization", "Basic xxxxxxxxxxxxxxx")

$body = '{"CONNECTION_NAME":"AUBRAC",
"USER_PROFILE":"testcrt",
"AD_ACCOUNT":"tescrtad",
"EIM_IDENTIFIER":"Test CRTPRFEIM",
"EIM_DESCRIPTION":"Ceci est la Description",
"LANGUAGE_CODE":"FRA",
"PROFILE_PARAMETERS":"PASSWORD(*NONE) CURLIB(ADICTDEV2)"
}'

$response = Invoke-RestMethod 'http://192.168.1.100:11022/web/services/CRTPRFEIM' -Method 'POST' -Headers $headers -Body $body
$response | ConvertTo-Json
```

La maintenance AD-iCT c’est

- La maintenance sur le produit
  - Evolutive
  - Corrective
- Et l’assistance en cas de soucis sur le SSO

Merci

Dominique GAYTE
06 30 17 02 55
dominique@gayte.it - https://i.gayte.it

I.GAYTE.IT