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

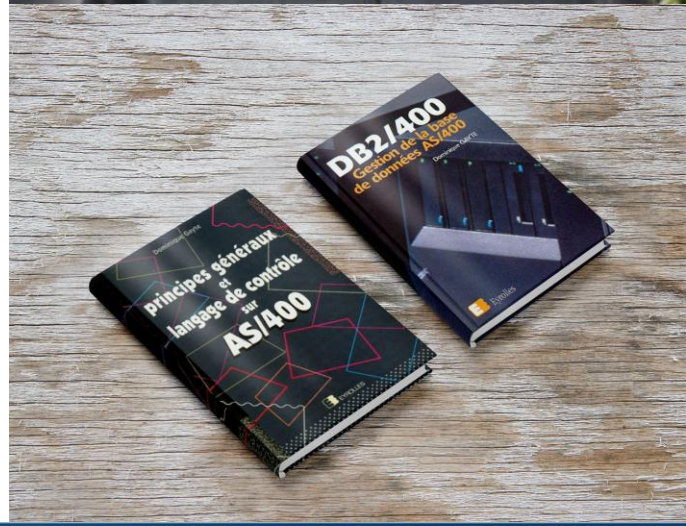
IBM i

AD-iCT

SSO entre un IBM i et un Active Directory

Dominique GAYTE

- Docteur ès sciences
- Intervenant « AS/400 » depuis 1990
- Formateur
- Expert Sécurité IBM i
  - Plus de 350 partitions IBM i auditées
  - Remédiations (sécurisation)
    - Base de données
    - Mots de passe
    - Cryptage de données
  - MFA (V7R6)
- Adore les développements complexes
- Auteur de plusieurs livres sur le sujet



Dominique GAYTE - suite

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

I.GAYTE.IT

- Expertise IBM i
  - Modernisation
  - IA
- Focus sur la Sécurité
- Edition de logiciels

- Reconnu pour son Innovation et sa Recherche

La problématique

- Les identifiants/mots de passe sont les protections essentielles de nos systèmes d'information
  - Biométrie de plus en plus utilisée
- 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

Définition

- 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 IBM i
- Solution très efficace et très performante
- Plus de 20 ans de recul
  - Des centaines d'installations

Mais…

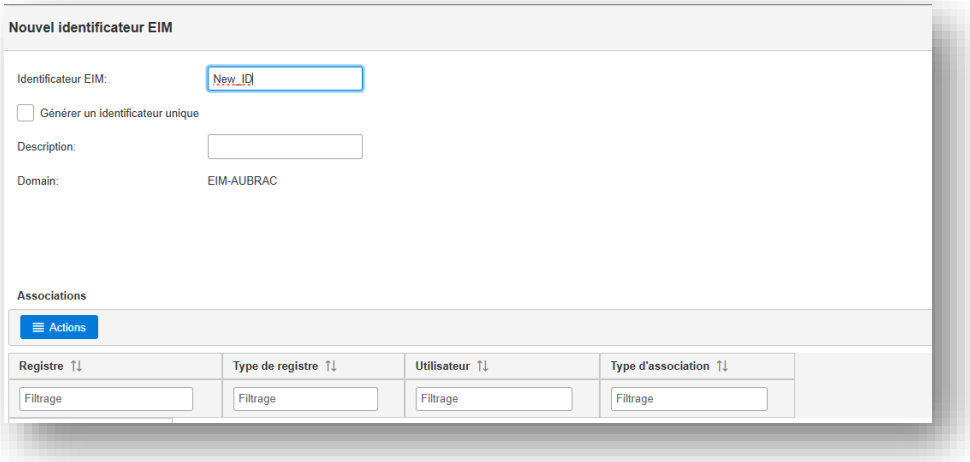
- La saisie des associations est pénible
  - Une quinzaine de clics de souris par association (par utilisateur et par partition) via Navigator for i
  - Pas de possibilité d'intégration dans les processus d'enrôlement de l'entreprise
- Pas d'outils pour manager les comptes
- Pas de mise à jour des backups via les outils de réplication logicielle
- Pas de fonctions d'audit
- Sauvegardes difficiles (Option 21)
- Pas d'extraction des comptes pour remplir de nouvelles partitions…

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

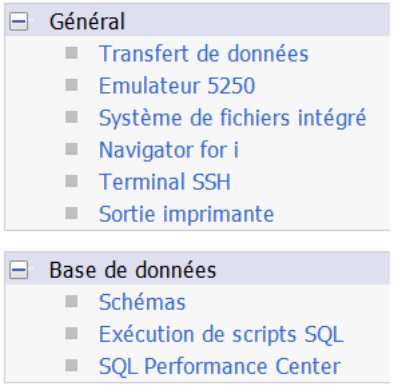
La couche EIM

- 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 !



Le SSO

- Très efficace, très rapide
- Fonctionne sans soucis depuis plus de 20 ans
- Pour
  - ACS (Telnet, scripts SQL, impressions, IFS…)
  - FTP
  - NetServer (plus de comptes NetServer désactivés !)
  - HTTP (Apache sur IBM i)
  - …
- Très souple au niveau des profils concernés



AD-iCT c’est

- Un outil complet qui comble tous les manques identifiés
  - Importation massive des comptes (csv ou PF)
  - Interfaces pour création/suppression des comptes
    - Ecran vert
    - Commande
    - Procédures stockées
    - API REST
  - 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
  - Pour création associations/profils à partir de PowerShell, par exemple

Ecran vert (5250)

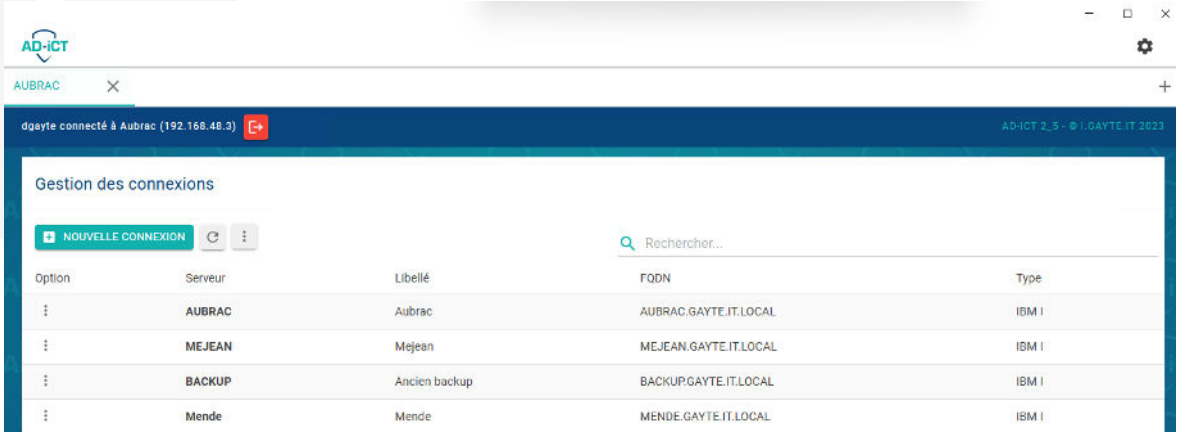
- Pour les administrateurs IBM i
- Visualisation des EIM d’autres partitions
  - Import d’associations distantes
  - Avec changement de cible pour utiliser la cible définie localement
  - Automatisation export/import
- Import en masse à partir de csv ou PF
- Suppression en masse
  - Cibles (profils) inexistantes
  - Tout
- Visualisations
  - Cibles inexistantes ou en doubles
  - Sources en double
  - *ALLOBJ

Ecran vert (5250)

- Création rapide d’association
- Programmes (*PGM) à intégrer dans vos CL de création des profils

Interface graphique

- En mode client lourd Windows
- Mêmes fonctionnalités qu'en 5250



Automatisation des tâches

- L’objectif est de diminuer à l’essentiel les tâches de gestion du SSO
- Selon votre organisation, avec AD-iCT, vous pouvez utiliser :
  - Des programmes (*PGM) à intégrer dans vos CL de création des profils
  - Une interface de création rapide d’association
  - Des API REST
- Mise à jour du backup
- Extraction des données pour sauvegarde simple

Les APIs

- Web Services REST qui permettent notamment
  - 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

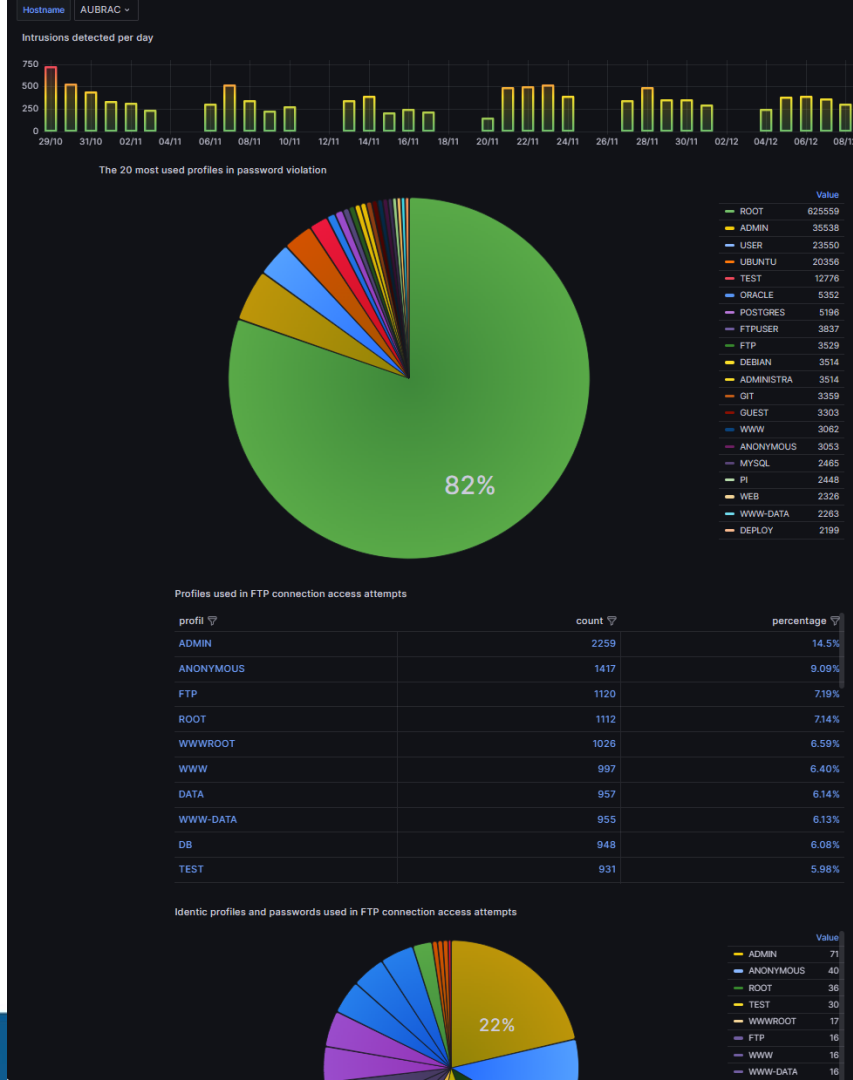
```
# Exemple d'utilisation des APIs d'AD-iCT
# Création d'un profil utilisateur et d'une association
# AD-iCT à partir de version 2.5
#
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("Content-Type", "application/json")
$headers.Add("Authorization", "Basic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

STR-iCT

- Sécurité et traçabilité des IBM i
- Webinar le 28 avril 2026 11H00 en français



Merci

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

I.GAYTE.IT