



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



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...

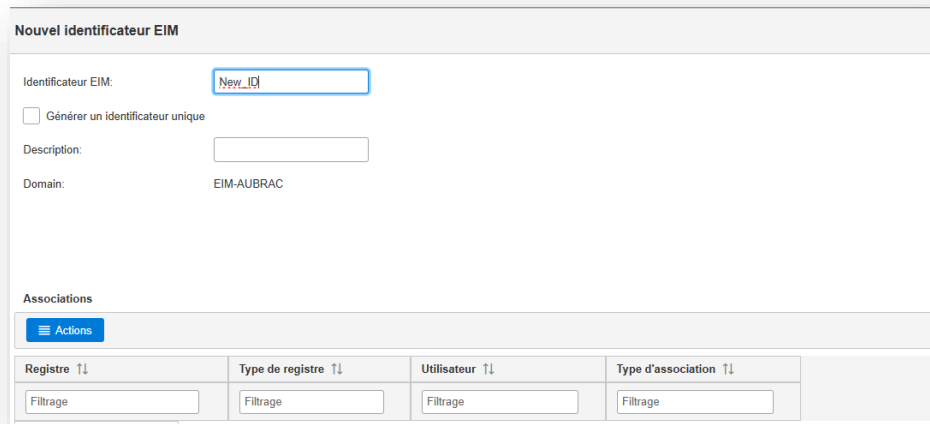
- La saisie des associations est pénible
 - Une quinzaine de clics de souris par association (par utilisateur et par partition) via Navigator for i
 - Pas de possibilité d'intégration dans les processus d'enrôlement de l'entreprise
- Pas d'outils pour manager les comptes
- Pas de mise à jour des backups 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 !



The screenshot shows a web interface for creating a new EIM identifier. The form is titled "Nouvel identificateur EIM" and contains the following fields and options:

- Identificateur EIM:** A text input field containing "New_ID".
- Générer un identificateur unique**
- Description:** An empty text input field.
- Domain:** A text input field containing "EIM-AUBRAC".

Below the form, there is a section titled "Associations" with a blue "Actions" button. At the bottom, there is a table with four columns, each containing a "Filtrage" (filter) input field:

Registre ↕	Type de registre ↕	Utilisateur ↕	Type d'association ↕
Filtrage	Filtrage	Filtrage	Filtrage

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

[-]	Général
■	Transfert de données
■	Emulateur 5250
■	Système de fichiers intégré
■	Navigator for i
■	Terminal SSH
■	Sortie imprimante
[-]	Base de données
■	Schémas
■	Exécution de scripts SQL
■	SQL Performance Center

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 inexistant
 - 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

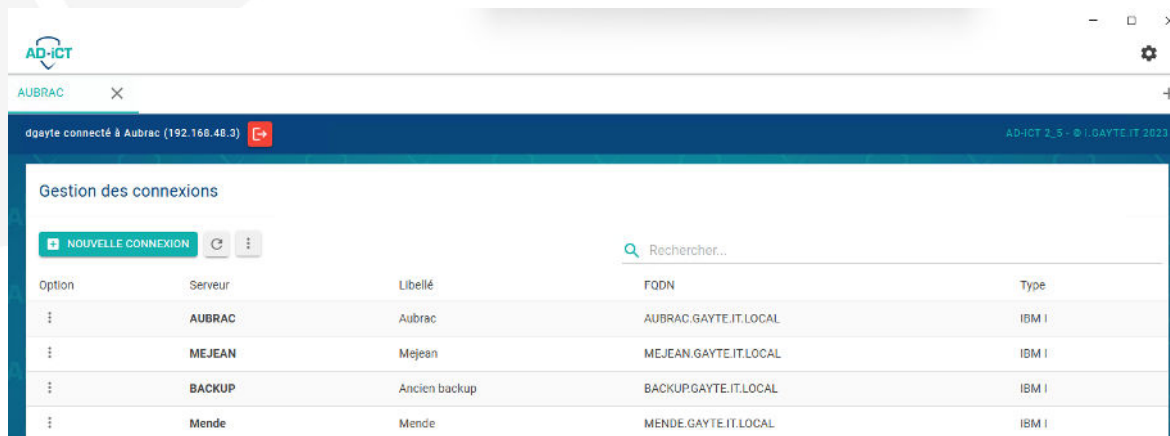
A large, light gray, stylized bird logo is positioned on the left side of the slide, extending from the top to the bottom. The bird is depicted in profile, facing right, with its wings spread. The logo is semi-transparent and serves as a background element for the text.

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



The screenshot displays a web browser window with the AD-ICT logo in the top left corner. The browser tab is labeled 'AUBRAC'. The page content shows a user 'dgayte' connected to 'Aubrac (192.168.48.3)'. The main section is titled 'Gestion des connexions' and includes a 'NOUVELLE CONNEXION' button and a search bar labeled 'Rechercher...'. Below this is a table listing connection options.

Option	Serveur	Libellé	FQDN	Type
⋮	AUBRAC	Aubrac	AUBRAC.GAYTE.IT.LOCAL	IBM I
⋮	MEJEAN	Mejean	MEJEAN.GAYTE.IT.LOCAL	IBM I
⋮	BACKUP	Ancien backup	BACKUP.GAYTE.IT.LOCAL	IBM I
⋮	Mende	Mende	MEUDE.GAYTE.IT.LOCAL	IBM I

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 xxxxxxxxxxxxxxxxx")

$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

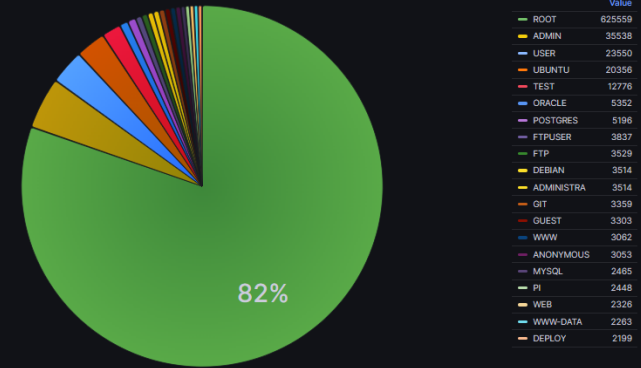


Hostname AUBRAC

Intrusions detected per day



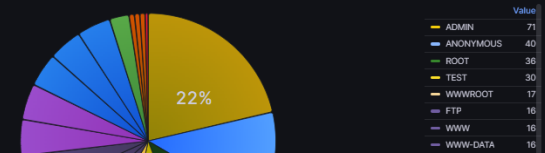
The 20 most used profiles in password violation



Profiles used in FTP connection access attempts

profil	count	percentage
ADMIN	2259	14.5%
ANONYMOUS	1417	9.09%
FTP	1120	7.19%
ROOT	1112	7.14%
WWWROOT	1026	6.59%
WWW	997	6.40%
DATA	957	6.14%
WWW-DATA	955	6.13%
DB	948	6.08%
TEST	931	5.98%

Identific profiles and passwords used in FTP connection access attempts



Merci

Dominique GAYTE

06 30 17 02 55

dominique@gayte.it - <https://i.gayte.it>

