

KHAN Nauman - nk@blue-channel.com
FACQ GUIRAUD Guilian – guilian@gayte.it

https://i.gayte.it

IBM i

Webinar SSO & IBM i

SSO industrialization between IBM i and Active Directory



KHAN Nauman

- Ex-IBMer (20 years' experience) & founder of Blue-Channel (Blue for Big Blue !) in 2008
- Operational marketing for IBM Business Partners (BPs) and Start-Ups, "only" with IBM

FACQ GUIRAUD Guilian

- Systems and Networks Engineer
- SSO and security implementer for I.GAYTE.IT



About Us

I.GAYTE.IT research & develop innovative IBM i security and modernization software solutions

A few words from Mr Dominique GAYTE, I.GAYTE.IT's CEO & IBM Champion.
With over 35 years' experience in securing IBM i servers and implementing SSOs on hundreds of IBM i partitions all over the world, we wanted to converge our experience with extensive customer feedback to design unique & high added value software solutions for IBM i clients to protect their IBM i investments within an ever-increasing hostile IT environment.





- Recognized for its innovation and research

AD-iCT

STR-iCT

FRANCE 2030

bpifrance



Single Sign On

Definition

- SSO : « *Single Sign-On* »
- Single signature system
- A solution that allows users on a company’s network to access all the authorized resources, on a **single authentication** basis that happened on initial access to the network
- We will place ourselves in a **Microsoft Active Directory** network context

The problem

- Logins / Passwords are essential protections for our IT infrastructure
  - Biometrics are increasingly used
- Users have x logins for x software
  - Windows
  - Messaging
  - Different IBM i's
  - Web Servers
  - …
- A work overload for administrators
  - Management of multiple solutions and authentication platforms
    1 user = n accounts, n userID's, n passwords
  - 30% of a company's Help Desk calls are linked to problems regarding user access to software when they try to authenticate to them
  - Hence a simplification of user authentication processes that can lead to security vulnerabilities
- … for users
  - Daily entry of usernames and passwords to access company data and software
  - Management of multiple usernames / passwords and linked security rules
  - Watch out for security rules transgressions !
- Auditors want stricter user account management policies
  - Notably a password policy reinforcement

SSO between IBM i and Active Directory

- Two distinct layers
- **Kerberos** for authentication
  - The link with AD itself
- **EIM** for the association between the AD account and the IBM i user profile
- Very effective and efficient solution
- More than 20 years of hindsight
  - Hundreds of installations

But…

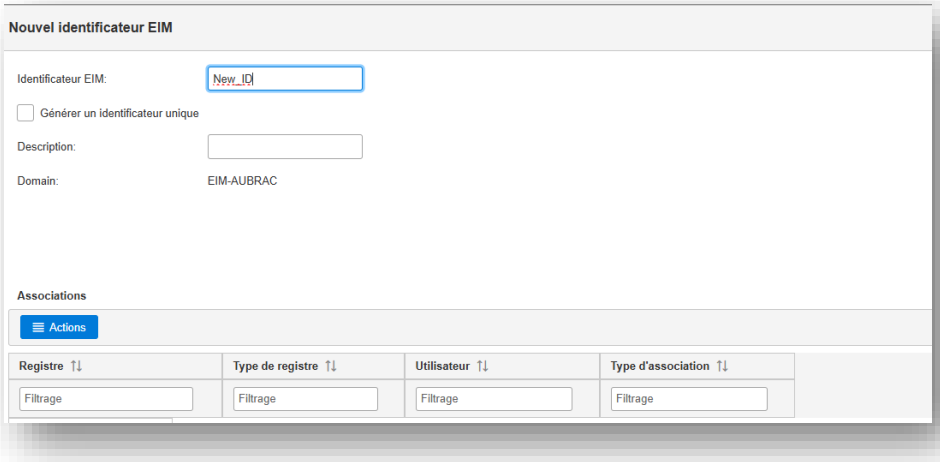
- Entering associations is tedious
  - More than a dozen clicks per association (per user / per partition) via Navigator for i
  - No possibility of integration into the company’s enrolment processes
- No tool to manage accounts
- No updates for backups using replication software
- Need to do an option 21 to backup SSO associations
  - Complex restoration
- No audit functions
- No user account data extraction to fill in new partitions…

The Kerberos layer

- Often the most difficult layer to implement
- Pretty technical to configure
  - AD
    - Kerberos
  - IBM i
  - DNS
  - Network
- Requires an Active Directory Administrator account
- And an IBM i Security Officer
  - Navigator for i must be operational

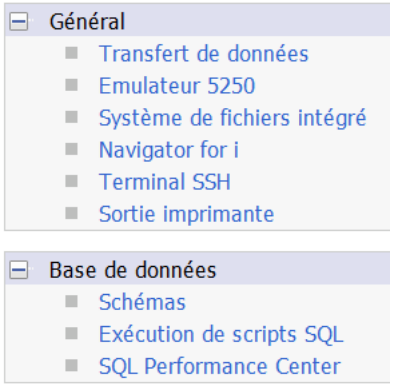
The EIM layer

- Uses the IBM i's LDAP directory
  - It has to be operational !
- Need to define an association between
  - An Active Directory account
  - An IBM i user profile for the partition
- Around 15 mouse clics per user with Navigator for i !



The SSO

- Very effective, very fast
- Works without issues since more than 20 years
- For
  - ACS (Telnet, SQL scripts, prints, IFS…)
  - FTP
  - NetServer (no more deactivated NetServer accounts !)
  - HTTP (Apache on IBM i)
  - …
- Very flexible for affected profiles
  - We can decide who will or won’t be affected



AD-iCT is



- A complete tool that fills in all identified gaps
  - Mass mappings import (csv or Physical File)
  - Account creation / deletion interface
    - Green screen
    - Commands
    - Sored procedures
    - REST API
  - Associations management
    - Non existent profiles
    - Duplicates
    - Power accounts (*ALLOBJ)
  - Backup updates
  - Data extraction in a file
    - Backups (Otherwise you almost need to do an option 21)
    - Feeding new partitions
  - Centralized management

Interfaces

- Green screen
- Graphical
  - Windows app
- REST API
  - To create associations / profiles with PowerShell for example

Green screen (5250)

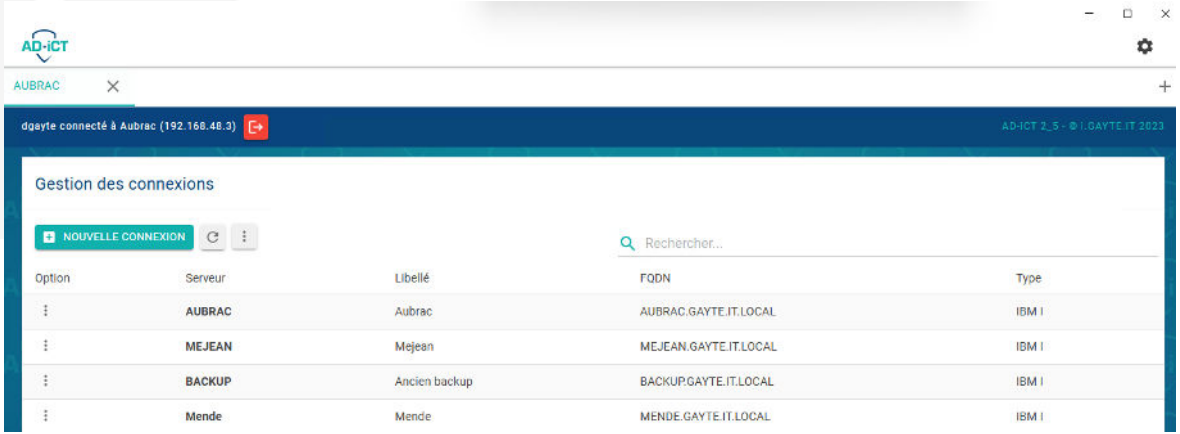
- For IBM i administrators
- Visualizing the EIMs of other partitions
  - Importing remote associations
  - With target change to use the locally defined target
  - Export / import automation
- Mass import form a csv of Physical File
- Mass deletion
  - Non existent targets (profiles)
  - Everything
- Visualizations
  - Non existent targets or duplicates
  - Duplicate sources
  - *ALLOBJ

Green screen (5250)

- Fast association creation
- Programs (*PGM) that you can integrate in you user creation CLs

Graphical interface

- Windows application
- Same functionalities than the green screen



Tasks automation

- The goal is to reduce SSO management tasks to its essentials
- Depending on your organization, with AD-iCT you can use:
  - Programs (*PGM) to integrate in you user creation CLs
  - A fast association creation interface
  - REST APIs
- Backup updates
- Data extractions for simple backups

The APIs

- Web service which allow, among other things
  - Creating user profiles and their EIM associations
  - Deleting user profiles and their EIM associations
- Ideal for managing change from Active Directory, with 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
```

The AD-iCT maintenance, it’s

- Product maintenance
  - Scalable
  - Fixes
- Support if you have a problem with the SSO that we implemented

Merci /
Thank you

KHAN Nauman
nk@blue-channel.com

FACQ GUIRAUD Guilian
guilian@gayte.it

https://i.gayte.it

