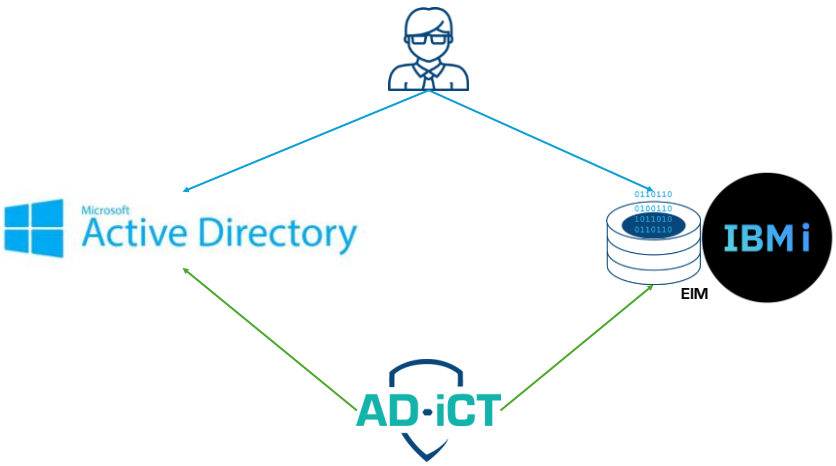
Sécurisation du Single Sign On (SSO)

pour IBM i

AD-iCT : renforcez le SSO entre les IBM i et l'Active Directory

Avec EIM, l'IBM i peut disposer d'un SSO avec l'AD (Active Directory). La solution proposée par IBM est d'excellente facture mais elle est difficilement utilisable en l'état sur une partition en production.

Fort de l'expérience de plusieurs dizaines d'années de sécurisation des IBM i, et de la mise en œuvre d'un SSO sur des centaines de partitions IBM i, I.GAYTE.IT (prononcer à l'anglaise *i get it*) a créé **AD-iCT**, le progiciel qui apporte les fonctionnalités indispensables à l'utilisation et à l'administration d'un SSO en production.



- Lors de la connexion à l'IBM i, aucun mot de passe n'est demandé ni à l'utilisateur, ni à l'AD.

- L'IBM i fait confiance à l'authentification réalisée par l'AD lors de la connexion au domaine (au démarrage du poste de travail, en général)

- Le SSO fait appel à l'association entre le compte AD authentifié et un profil utilisateur IBM i stockée dans l'annuaire EIM

- En cas de session 5250, par exemple, l'écran d'ouverture n'est pas proposé, l'utilisateur se retrouve directement dans son programme initial

- **AD-iCT** permet de maintenir l'annuaire EIM

- **AD-iCT** offre des services supplémentaires afin de simplifier et automatiser les tâches à partir de l'AD

Saisie des associations

Avec EIM, chaque compte AD (la source) doit être associé à un profil utilisateur (la cible) afin que, lors de la connexion SSO une correspondance soit établie pour définir le profil à utiliser.

La saisie de cette association avec les outils standard est longue et fastidieuse (une quinzaine de clics de souris). **AD-iCT** propose plusieurs modes de création automatisée des associations pour répondre aux nombreux besoins des Services Informatiques via des :

- Importations en masse (fichier CSV ou PF)
- Interfaces graphiques ou 5250
- Des *PGM pour l'intégration dans une chaine batch IBM i
- Des API REST pour intégration dans du PowerShell, par exemple

Fonctionnalités

- Importation en masse via CSV ou fichier PF
- API REST pour création des profils et des associations
- Création des associations via *PGM pour intégration en batch
- Visualisation des associations de plusieurs partitions
- Exportation des associations dans PF
- Importation des associations à partir de PF
- Visualisation des cibles manquantes
- Visualisation des sources/cibles en double
- Visualisation des cibles *ALLOBJ
- Synchronisation avec la partition de backup même en cas de réplication logicielle
- Sauvegarde simple des données d'EIM
- Gestion de plusieurs partitions à partir d'une même interface
- Interface graphique et/ou 5250 selon les affinités de chacun

Réplication vers la partition de backup

Les produits de réplication logicielle ne prennent pas en compte les données d'EIM, c'est-à-dire qu'une association définie sur la partition de production n'est pas répliquée sur le système de backup.

AD-iCT permet de synchroniser automatiquement les deux partitions afin de ne pas avoir de dysfonctionnement du SSO lors de la bascule en mode PRA.

La fonction d'export permet d'initialiser une nouvelle partition avec les associations d'une autre ce qui procure des gains de temps significatifs lors de la création de nouveaux environnements.

Environnements complexes

AD-iCT est prévu pour fonctionner dans des environnements complexes contenant :

- Plusieurs domaines sources, c'est à dire plusieurs domaines servant à l'authentification des utilisateurs
- Plusieurs cibles (plusieurs partitions IBM i)

Les associations ayant pour source le domaine AD DOMA.LOCAL et pour cible IBMi1.LOCAL, peuvent être automatiquement copiées vers DOMB.LOCAL et/ou IBMi2.LOCAL ce qui permet des migrations simples de domaines utilisateur et de partitions IBM i, au moins pour ce qui concerne le SSO.

Sauvegardes d'EIM

Les données d'EIM (les associations) sont difficilement sauvegardables (il faut être en mode restreint, par exemple). Sans arrêt de production, AD-iCT exporte ces données dans une table (fichier PF) qui est facilement sauvegardable et restaurable. La fonction d'import reconstitue les associations en quelques secondes.

Et vous, comment intégrez-vous un nouveau collaborateur ?

L'intégration d'un nouveau collaborateur nécessite de lui créer un compte (au moins !) sur chaque système. Au moins un compte sur l'AD et un profil utilisateur (et une association) sur chaque partition IBM i.

Avec AD-iCT vous pouvez créer le profil utilisateur et l'association EIM :

- Soit coté IBM i à l'aide d'un programme (*PGM) à intégrer dans votre chaine de création du profil
- Soit procéder à partir de l'AD via un programme PowerShell qui consomme une API REST exposée par l'IBM i

AD-iCT, le complément indispensable au SSO IBM i

Quel que soit votre contexte et vos compétences (plutôt IBM i, ou plutôt AD) les fonctions d'automatisation d'AD-iCT vous permettent d'utiliser en production le SSO basé sur EIM.

Les fonctions d'AD-iCT sont déjà déployées sur des centaines de partitions IBM i et, avec EIM, elles offrent un SSO puissant, efficace et résiliant.

Nos services

Nous vous assistons dans le déploiement du SSO et dans son maintien en condition opérationnelle.

N'hésitez pas à nous contacter pour toute prestation en rapport avec la Sécurité des IBM i.

AD-iCT est un produit édité par I.GAYTE.IT
IBM i Security Software & Services

Pour plus d'informations

https://i.gayte.it/ad-ict

ad-ict@gayte.it

Vous êtes un partenaire IBM, un MSP hébergeant des IBM i, **nous avons un contrat de partenariat à forte valeur ajoutée pour vous :** i.gayte.it/ipp

I.GAYTE.IT est une marque de GAYTE.IT - Siège - 46, Le Villeret_- 48170 ST JEAN LA FOUILLOUSE - FRANCE
Centre R&D – POLeN - 12 rue Albert Einstein - 48000 MENDE
Agence Montpellier - 32 chemin Notre Dame - 34160 BEAULIEU