AIM-AD

Table des matières

Objectifs

Ce projet propose un ensemble de scripts Powershell permettant de réaliser des rapports sur les comptes Microsoft Active Directory, afin d'aider les administrateurs système à la gestion des entrées sorties d'utilisateurs.

Les 3 principaux scripts sont :

- `InactiveAccountsManager.ps1` :
- `PasswordExpirationNotifier.ps1` :
- `DisabledAccountsSummary.ps1` :

Comment mettre en oeuvre les scripts

Pré-requis

Les scripts doivent être installés sur un serveur Windows membre du domaines et disposer des composants suivants :

- **PowerShell** : Version 5.1 ou supérieure.
- **Module Active Directory** : Requis pour interagir avec les comptes.
- **Accès SMTP** : Nécessaire pour l'envoi des notifications par e-mail.

Installation du projet

Télécharger l'archive du projet au format ZIP et déposer celle-ci sur le serveur Windows.

Extraire le contenu de l'archive dans le dossier `C:\Scripts\aim-ad-main`.

Configuration du logo

Placer le logo de l'entreprise dans le dossier `C:\Scripts\aim-ad-main\logo.png`

Configuration des variables

Ouvrir le fichier `C:\Scripts\aim-ad-main\config.ps1` avec un éditeur de texte et modifier les variables suivantes selon vos besoins :

- `$emailSupport` : Adresse e-mail du support technique.
- `$phoneSupport` : Numéro de téléphone du support (sans points comme séparateurs).
- `$urlSupport` : URL du portail de support.
- `$PortalSupport` : URL du portail de réinitialisation de mot de passe.
- `$SmtpPort` : Port SMTP (par défaut : 587).
- `$SmtpSSL` : Activer/désactiver SSL pour SMTP (par défaut : $true).

Créer les identifiants de connexion SMTP (facultatif)

Si votre serveur SMTP requière une authentification avec un **utilisateur** et un **mot de passe**, utiliser le script suivant pour générer le fichier de connexion.

Executer le script :

```
cd "C:\Scripts\aim-ad-main\"
.\Generate-SmtpCredential.ps1
```

Laisser le chemin par défaut pour créer le fichier `smtp_credential.xml`.

Renseigner l'utilisateur et le mot de passe.

Créer et configurer le compte de service

Si vous avez déjà configuré un compte de service, vous pouvez passer directement à l'étape Planifier l'exécution des scripts.

Le compte de service sera un **compte gMSA (Group Managed Service Account)**.

Les comptes gMSA sont conçus pour être utilisés par des services et des tâches planifiées, et ils offrent une gestion automatique des mots de passe, ce qui réduit les risques liés à la gestion manuelle des mots de passe.

La procédure pour créer un compte gMSA nommé **`SVC-IAM-USERS`**, le configurer pour être utilisé sur le contrôleur de domaine **`SRV-DC03`**.

Le nom du serveur destiné à l'execution des scripts IAM-Users devra être modifié en fonction de votre infrastructure.

> [!IMPORTANT]
> Cette procédure ne prend pas en compte la création de la clé KDC racine. Nous prennons le parti que

> cette configuration a déjà été réalisée.
> Si vous utiliser un compte de service classique, n'oubliez pas d'ajouter le commentaire `//ACCOUNT_PROTECTED//` dans le descriptif pour protégrer le compte d'une désactivation.

Prérequis

1. **Niveau fonctionnel de domaine** :
   - Le domaine doit être au moins au niveau fonctionnel **Windows Server 2012** pour prendre en charge les comptes gMSA.
2. **Module Active Directory PowerShell** :
   - Assurez-vous que le module Active Directory est installé sur le serveur où vous exécutez les commandes PowerShell.
3. **Droits d'administration** :
   - Vous devez disposer des droits d'administrateur de domaine pour créer et configurer un compte gMSA.

Procédure pour créer et configurer un compte gMSA

1. Créer le compte gMSA

1. **Ouvrir PowerShell en tant qu'administrateur** :
   - Sur un contrôleur de domaine ou un serveur avec le module Active Directory installé, ouvrez PowerShell en tant qu'administrateur.
2. **Créer le compte gMSA** :
   - Exécutez la commande suivante pour créer le compte gMSA :

```
New-ADServiceAccount -Name "SVC-IAM-USERS" `
                -Description "gMSA tâches planifiées IAM Users" `
                -DNSHostName " SVC-IAM-USERS.yourdomain.com" `
                -ManagedPasswordIntervalInDays 30 `
                -PrincipalsAllowedToRetrieveManagedPassword "SRV-DC03$"
`
                -Enabled $True
```

   - `SVC-IAM-USERS` : Nom du compte gMSA.
   - `yourdomain.com` : Remplacez par le nom de votre domaine.
   - `SRV-DC03$` : Nom de l'ordinateur (avec le symbole `$`) autorisé à récupérer le mot de passe du compte gMSA. Remplacez par le nom de votre serveur.
3. **Vérifier la création du compte gMSA** :

- Pour vérifier que le compte gMSA a été créé, exécutez :

```
Get-ADServiceAccount -Identity SVC-IAM-USERS
```

---

2. Configurer le compte gMSA sur le serveur SRV-DC03

1. **Installer le compte gMSA sur le serveur** :
   - Sur le serveur `SRV-DC03`, exécutez la commande suivante pour installer le compte gMSA :

```
Install-ADServiceAccount -Identity SVC-IAM-USERS
```

2. **Vérifier l'installation du compte gMSA** :
   - Pour vérifier que le compte gMSA est correctement installé, exécutez :

```
Test-ADServiceAccount -Identity SVC-IAM-USERS
```

     - Si la commande retourne `True`, le compte gMSA est correctement configuré.

3. **Autoriser le compte gMSA à se connecter en tant que tâche**

Afin que le compte gMSA soit en mesure d'exécuter le script via la tâche planifiée, il faut l'autoriser à ouvrir une session en tant que tâche. Sinon, le script ne pourra pas s'exécuter en principe (mais j'ai déjà rencontré des cas où cela fonctionne sans ce paramètre). Pour cela, il faut créer une GPO et l'appliquer sur le(s) serveur(s) qui vont utiliser le gMSA, ou modifier la stratégie locale (gpedit.msc).

Si l'on fait une GPO, ce qui sera le cas en production, il faudra modifier ce paramètre :

`Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Attribution des droits utilisateurs > Ouvrir une session en tant que tâche`

---

3. Configurer les permissions pour le compte gMSA

1. **Créer un groupe de sécurité** :
   - Créez un groupe de sécurité nommé `GRP_IAM_Users` dans Active Directory.

2. **Ajouter le compte gMSA au groupe** :
   - Ajoutez le compte gMSA au groupe `GRP_IAM_Users` :

```
Add-ADGroupMember -Identity GRP_IAM_Users -Members SVC-IAM-USERS$
```

3. **Déléguer les permissions** :
    - Déléguer les permissions nécessaires pour désactiver les utilisateurs inactifs au groupe `GRP_IAM_Users` :
        - Ouvrez **Utilisateurs et ordinateurs Active Directory**.
        - Cliquez avec le bouton droit sur l'OU ou le domaine où les utilisateurs inactifs doivent être désactivés, puis sélectionnez **Déléguer le contrôle**.
        - Suivez l'assistant pour déléguer les permissions au groupe `GRP_IAM_Users`.
        - Sélectionnez **Créer une tâche personnalisée pour déléguer**.
        - Choisissez **Uniquement les objets utilisateur suivants dans ce dossier**.
        - Cochez **Propriété générale**, **Propriété d'écriture** et **Propriété de lecture**.
        - Sous **Permissions**, cochez uniquement **Désactiver un compte utilisateur**.

Planifier l'exécution des scripts

Le script `CreateScheduledTask.ps1` permet de créer les taches planifiées pour l'exécution des scripts IAM-AD.

Executer le script `CreateScheduledTask.ps1` dans une fenêtre powershell :

```
cd "C:\Scripts\aim-ad-main\"
.\CreateScheduledTask.ps1
```

Choisisser un numéro de 1 à 3 pour planifier les scripts :

1. `DisabledAccountsSummary.ps1`
2. `InactiveAccountsManager.ps1`
3. `PasswordExpirationNotifier.ps1`

Suivre les indications à l'écran.

Les taches planfiées suivantes sont créées, pour une execution quotidienne à 01h00.

- **DisabledAccountsSummaryTask**
- **InactiveAccountsManagerTask**
- **PasswordExpirationNotifierTask**

> [!IMPORTANT]
> Si vous utilisez un compte gMSA n'ajouter le caracère `$` à la fin du nom. Le script gére le nommage de l'utilisateur en fonction du type. (Exemple : `SVC-IAM-USERS`)

ATTENTION aux actions du script `InactiveAccountsManager.ps1`

Le script `InactiveAccountsManager.ps1` désactive les utilisateurs inactifs depuis plus de 45 jours. Les comptes dont la description contient `//ACCOUNT_PROTECTED//` sont exclus.

Mode simulation :
Pour vérifier les utilisateurs qui seraient désactivés sans appliquer les modifications (Exemple de commande) :

```
cd "C:\Scripts\aim-ad-main\"
.\InactiveAccountsManager.ps1 -AdminEmails "philippe.candido@emerging-it.fr" -
SmtpServer "smtp.eu.org" -EmailFrom "AD-DisabledAccounts-report@mg.cpf-it.fr" -
debugMode -DryRun
```