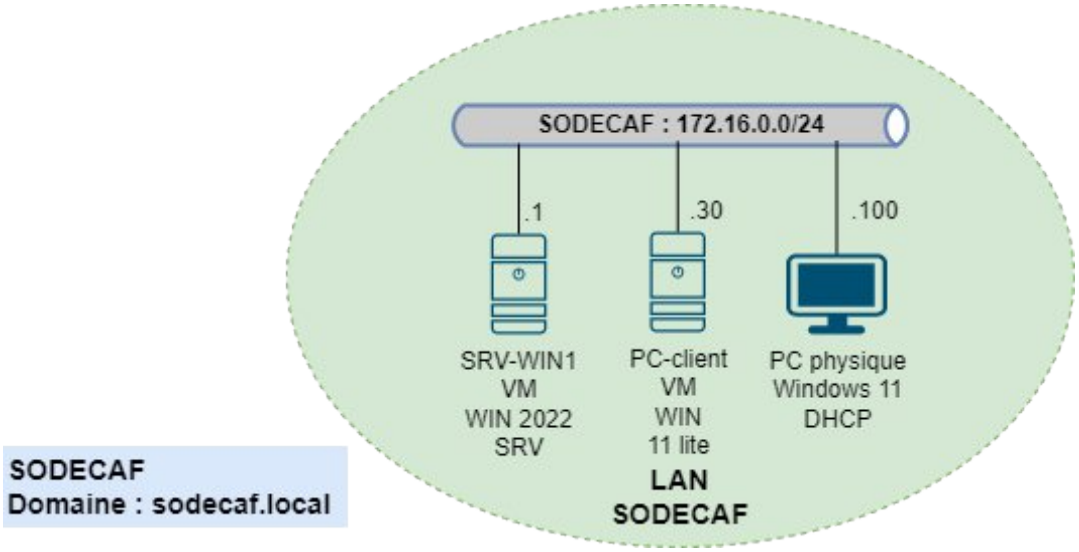
BTS SIO
bloc 2

B2-Act4-TP5 – Powershell et Active Directory (3h)

Introduction

Objectifs

Dans ce TP, Vous allez vous connecter à un annuaire Active Directory avec PowerShell, naviguer dans cet annuaire et y rajouter des informations (Unités d'organisations et utilisateurs).



Prérequis

Pour commencer, il faut que vous utilisiez votre infrastructure de la SODECAF, avec au moins un serveur AD installé, afin de pouvoir accéder à l'annuaire LDAP.
L'accès au LAN de SIO et à Internet se fera par l'intermédiaire de votre routeur pare-feu pfsense.

Travail à effectuer

- Démarrez votre VM serveur SRV-AD1 et votre VM pfsense.
- Sur SRV-AD1, installez le module Poweshell Active Directory avec la commande *Add-WindowsFeature RSAT-AD-PowerShell*.
- Utiliser les commandes de base en annexe 1 pour tester l'ajout et la suppression de nouveaux utilisateurs dans l'AD. Testez la possibilité de se connecter avec ce compte sur la machine cliente Windows 10.
- Utiliser les commandes de l'annexe 2 pour créer des Unités d'organisations, des groupes, et des utilisateurs appartenant à ces groupes. Notez bien les commandes utilisées. Testez.
- Vous devez maintenant écrire le script permettant d'importer les groupes et les utilisateurs du fichier « utilisateurs sodecaf.csv » et de les insérer dans l'AD. Vous pouvez vous aider du TP précédent et du lien https://blog.netwrix.fr/2018/12/19/comment-creer-de-nouveaux-utilisateurs-dactive-directory-avec-powershell/. Vous écrirez une fonction qui génère des mots de passe aléatoires pour chaque utilisateur. Sauvegardez ce script.
- Améliorez votre script en créant un lecteur réseau personnel de travail à chaque utilisateur. Vous devrez mettre à jour PowerShell en version 4 et importer le module NTFSSECURITY (dossier NTFSSECURITY à importer et à déposer dans c:\Users\Administrateur\Documents\WindowsPowerShell\), puis vous aider du lien https://www.it-connect.fr/gerer-les-autorisations-ntfs-en-powershell-avec-ntfssecurity/

Annexe1 : module Powershell AD – les commandes de base

- **Utiliser le module Active Directory**

```
PS C:\> Import-Module ActiveDirectory
```

- **Créer une Unité d'Organisation**

```
                                        "Employés"          "dc=sodecaf,dc=local"
```

- **Créer un compte utilisateur Active Directory**

```
PS C:\> New-ADUser -Name "Paul Bismuth" -GivenName Paul -Surname Bismuth `
 -SamAccountName pbismuth -UserPrincipalName pbismuth@supinfo.com `
 -AccountPassword (Read-Host -AsSecureString "Mettez ici votre mot de passe") `
 -PassThru | Enable-ADAccount
```

Note : L'utilisateur peut se connecter immédiatement après la création de son compte !

- **Créer un groupe Active Directory**

Utilisez la commande ci-dessous pour créer un nouveau groupe global :

```
PS C:\> New-ADGroup -name "Politique" -groupscope Global -Path "ou=Employés,dc=sodecaf,dc=local"
```

- **Ajouter un utilisateur au sein d'un groupe**

La commande ci-dessous ajoute l'utilisateur « pbismuth » au groupe « Politique » :

```
PS C:\> Add-ADGroupMember -Identity "Politique" -Member "pbismuth"
```

- **Activer et désactiver un compte utilisateur**

```
PS C:\> Enable-ADAccount -Identity pbismuth
```

- **Désactivation du compte**

```
PS C:\> Disable-ADAccount -Identity pbismuth
```

- **Désactiver tous les comptes d'un groupe**

Pour désactiver tous les comptes du département nommé « Politique » :

```
PS C:\> Get-ADGroupMember "Politique" | Disable-ADAccount
```

- **Déverrouiller un compte d'utilisateur**

Paul s'est verrouillé après avoir essayé d'utiliser son nouveau mot de passe. Vous pouvez le déverrouiller en utilisant cette simple commande :

```
PS C:\> Unlock-ADAccount pbismuth
```

- **Lister tous les comptes Active Directory**

La commande qui suit vous permettra d'afficher tous les comptes de votre annuaire :

```
PS C:\> Get-ADUser -Filter * | Format-List
```

- **Supprimer un compte utilisateur**

Pour supprimer un compte utilisateur, vous pouvez utiliser la commande qui suit :

```
PS C:\> Remove-ADUser pbismuth
```

N'hésitez pas à aller voir le site de Microsoft pour l'aide complète sur les cmdLets :
https://docs.microsoft.com/en-us/powershell/module/?view=win10-ps

Annexe 2 : les modules cmdLets Active Directory

cmdlet	Description
Add-ADComputerServiceAccount	Ajoute un ou plusieurs comptes de service à un ordinateur Active Directory.
Add-ADDomainControllerPasswordReplicationPolicy	Ajoute des utilisateurs, des ordinateurs et des groupes à la liste des admis ou refusé du read-only domain controller (RODC) Password Replication Policy (PRP).
Add-ADFineGrainedPasswordPolicySubject	Applique une politique de mots de passe précis à un ou plusieurs utilisateurs et groupes.
Add-ADGroupMember	Ajoute un ou plusieurs membres à un groupe Active Directory.
Add-ADPrincipalGroupMembership	Ajoute un membre à un ou plusieurs groupes Active Directory.
Clear-ADAccountExpiration	Efface la date d'expiration d'un compte Active Directory.
Disable-ADAccount	Désactive un compte Active Directory.
Disable-ADOptionalFeature	Désactive une fonctionnalité facultative Active Directory.
Enable-ADAccount	Active un compte Active Directory.
Enable-ADOptionalFeature	Active une fonctionnalité facultative Active Directory.
Get-ADAccountAuthorizationGroup	Obtient les groupes de sécurité Active Directory qui contiennent un compte.
Get-ADAccountResultantPasswordReplicationPolicy	Donne la politique de mot de passe qui en résultent pour la réplication d'un compte Active Directory .
Get-ADComputer	Donne un ou plusieurs ordinateurs Active Directory.
Get-ADComputerServiceAccount	Donne les comptes de service qui sont hébergés par un ordinateur Active Directory.
Get-ADDefaultDomainPasswordPolicy	Donne la politique de mot de passe par défaut pour un domaine Active Directory.
Get-ADDomain	Donne un domaine Active Directory.
Get-ADDomainController	Donne un ou plusieurs contrôleurs de domaine Active Directory, les services fondés sur des critères détectable, les paramètres de recherche, ou en fournissant un identifiant contrôleur de domaine, telles que le nom NetBIOS.
Get-ADDomainControllerPasswordReplicationPolicy	Donne les membres de la liste des admis ou refusé de la Liste du PRP RODC.
Get-ADDomainControllerPasswordReplicationPolicyUsage	Donne la politique de mot de passe ADAccount sur le RODC spécifiée.
Get-ADFineGrainedPasswordPolicy	Donne un ou plusieurs politiques Active Directory bien précis.
Get-ADFineGrainedPasswordPolicySubject	Donne les utilisateurs et les groupes auxquels une politique de mot de passe précise est appliquée.
Get-ADForest	Donne une forêt Active Directory.
Get-ADGroup	Donne un ou plusieurs groupes Active Directory.
Get-ADGroupMember	Donne les membres d'un groupe Active Directory.
Get-ADObject	Donne un ou plusieurs objets Active Directory.
Get-ADOptionalFeature	Donne une ou plusieurs fonctionnalités optionnelles Active Directory.
Get-ADOrganizationalUnit	Donne une ou plusieurs OU d'Active Directory.
Get-ADPrincipalGroupMembership	Donne les groupes Active Directory qui ont un utilisateur, un ordinateur ou un groupe spécifié.
Get-ADRootDSE	Donne la racine d'un arbre d'information du contrôleur de domaine.
Get-ADServiceAccount	Donne un ou plusieurs comptes de service Active Directory.
Get-ADUser	Donne un ou plusieurs utilisateurs Active Directory.
Get-ADUserResultantPasswordPolicy	Donne la politique de mot de passe qui en résulte pour un utilisateur.
Install-ADServiceAccount	Installe un compte de service Active Directory sur un ordinateur.
Move-ADDirectoryServer	Déplace un contrôleur de domaine dans AD DS vers un nouveau site.
Move-ADDirectoryServerOperationMasterRole	Déplace les rôles FSMO vers un contrôleur de domaine Active Directory.
Move-ADObject	Déplace un objet Active Directory ou un conteneur d'objets vers un conteneur ou un domaine différent.
New-ADComputer	Crée un nouvel ordinateur Active Directory.

New-ADFineGrainedPasswordPolicy	Crée une stratégie de mot de passe affinée.
New-ADGroup	Crée un groupe Active Directory.
New-ADObject	Crée un objet Active Directory.
New-ADOrganizationalUnit	Crée une nouvelle unité d'organisation Active Directory.
New-ADServiceAccount	Crée un nouveau compte de service Active Directory.
New-ADUser	Crée un nouvel utilisateur Active Directory.
Remove-ADComputer	Supprime un ordinateur Active Directory.
Remove-ADComputerServiceAccount	Supprime un ou plusieurs comptes de service d'un ordinateur.
Remove-ADDomainControllerPasswordReplicationPolicy	Supprime les utilisateurs, les ordinateurs et les groupes de la liste autorisée ou de la liste refusée du RODC PRP.
Remove-ADFineGrainedPasswordPolicy	Supprime une stratégie de mot de passe affinée.
Remove-ADFineGrainedPasswordPolicySubject	Supprime une stratégie de mot de passe affiné de Active Directory.
Remove-ADGroup	Supprime un groupe Active Directory.
Remove-ADGroupMember	Supprime un ou plusieurs membres d'un groupe Active Directory.
Remove-ADObject	Supprime un objet Active Directory.
Remove-ADOrganizationalUnit	Supprime une unité d'organisation Active Directory.
Remove-ADPrincipalGroupMembership	Supprime un membre d'un ou plusieurs groupes Active Directory.
Remove-ADServiceAccount	Supprime un compte de service Active Directory.
Remove-ADUser	Supprime un utilisateur Active Directory.
Rename-ADObject	Change le nom d'un objet Active Directory.
Reset-ADServiceAccountPassword	Réinitialise le mot de passe du compte de service d'un ordinateur.
Restore-ADObject	Restaure un objet Active Directory.
Search-ADAccount	Donne les comptes utilisateur, ordinateur et service Active Directory.
Set-ADAccountControl	Modifie les valeurs de l'user account control (UAC) pour un compte Active Directory.
Set-ADAccountExpiration	Définit la date d'expiration d'un compte Active Directory.
Set-ADAccountPassword	Modifie le mot de passe d'un compte Active Directory.
Set-ADComputer	Modifie un ordinateur d'Active Directory.
Set-ADDefaultDomainPasswordPolicy	Modifie la stratégie de mot de passe par défaut pour un domaine Active Directory.
Set-ADDomain	Modifie un domaine Active Directory.
Set-ADDomainMode	Définit le niveau fonctionnel du domaine pour un domaine Active Directory.
Set-ADFineGrainedPasswordPolicy	Modifie une politique de mot de passe Active Directory bien précis.
Set-ADForest	Modifie une forêt Active Directory.
Set-ADForestMode	Définit le mode forêt pour une forêt Active Directory.
Set-ADGroup	Modifie un groupe Active Directory.
Set-ADObject	Modifie un objet Active Directory.
Set-ADOrganizationalUnit	Modifie une unité d'organisation Active Directory.
Set-ADServiceAccount	Modifie un compte de service Active Directory.
Set-ADUser	Modifie un utilisateur Active Directory.
Uninstall-ADServiceAccount	Désinstalle un compte de service Active Directory à partir d'un ordinateur.
Unlock-ADAccount	Déverrouille un compte Active Directory.

Pour répertorier toutes les cmdlets disponibles dans le module Active Directory, utilisez la cmdlet « Get-Command *-AD* ».