Sommaire

1 Avant-Propos 4

2 Introduction 4

3 Script PowerShell 4

4 Automatiser le processus Erreur : source de la référence non trouvée

1. Avant-Propos

Préciser ici la finalité et le domaine d’application du document ; peut être mis en préface ou au début d’un titre *Introduction*

Automatisation de la suppression des sessions d’utilisateurs et de leurs données au démarrage d’une session.

# Introduction

Des ordinateurs d’emprunts sont mis à disposition des agents.

Ces derniers disposent des accès administrateurs sur la machine.

Cela créée alors une faille de sécurité offrant à la session active l’accès aux données des agents précédemment connectés à cet ordinateur. (Notamment les dossiers WorkFolders)

Afin de préserver la sécurité des données, une solution permettant la suppression automatique des sessions et données des utilisateurs doit être mise en place.

# Script PowerShell

1. Créer un script .ps1 (Fichier PowerShell)

Pour ce faire vous pouvez créer un fichier texte puis modifier l’extension de ce fichier en .ps1

Si vous ne parvenez pas à modifier le type de fichier(l’extension), activez l’affichage des extensions de fichier, tel que :

  

1. Saisissez le code suivant :

$logFilePath = "C:\Windows\System32\GroupPolicy\User\Scripts\Logon\SuppressionUtilisateurLogs.log"

$ErrorActionPreference = "Stop"

Start-Transcript -Path $logFilePath -Append

try {

$currentUserProfile = $env:USERPROFILE

$deletedUserNames = @()

Get-CimInstance -ClassName Win32\_UserProfile | Where-Object { $\_.LocalPath -like '\*\Users\\*' -and $\_.LocalPath -ne $currentUserProfile } | ForEach-Object {

$deletedUserNames += $\_.LocalPath

Remove-CimInstance -InputObject $\_ -ErrorAction Stop

}

Write-Output "Utilisateurs supprimés : $($deletedUserNames -join ', ')"

}

catch {

Write-Error "Erreur : $\_"

}

finally {

Stop-Transcript

}

1. Enregistrez le script

Explications du script :

* ***«  Get-CimInstance -ClassName Win32\_UserProfile »***

Sélectionne les profils de la machine

* ***« Where-Object { $\_.LocalPath -like '\*\Users\\*' »***

Filtre les utilisateurs réels

* ***« and $\_.LocalPath -ne $currentUserProfile »***

Désélectionne l’utilisateur de la session active

* ***« ForEach-Object { $deletedUserNames += $\_.LocalPath Remove-CimInstance »***

Supprime les sessions utilisateur sélectionnés

1. Automatiser le processus
2. Ouvrez le gestionnaire des tâches (CTRL + SHIFT + ECHAP)



1. Sélectionnez « Exécuter une nouvelle tâche »
2. Ouvrez gpedit.msc en prenant soin d’activer les privilèges d’administration
3. Configuration utilisateur > Paramètres Windows > Scripts (ouverture/fermeture)

> Ouverture de session > Scripts PowerShell > Ajouter

1. Lorsque vous cliquez sur « Parcourir… » vous êtes redirigés vers

C:\Windows\System32\GroupPolicy\User\Scripts\Logon

Ici , collez votre Fichier PowerShell contenant le script et sélectionnez le

 Il devrait apparaître de cette manière

Appliquer > OK

1. Redémarrer l’ordinateur > Lancement de session

Pour vérifier si cette manipulation a fonctionné,

Vous pouvez vérifier la présence d’utilisateurs dans le dossier C:\Users

Vous pouvez vérifier la présence du fichier de logs dans le dossier

C:\Windows\System32\GroupPolicy\User\Scripts\Logon

**ATTENTION** : Cette solution supprime toutes les données utilisateurs présentes sur la machine en cours d’utilisation. Les données perdues ne peuvent être récupérées.

**La manipulation n’aboutit pas ?**

Vérifiez si l’utilisateur qui démarre sa session est administrateur de la machine.

Prenez soin, à l’étape 4.2 de sélectionner « Créez cette tâche avec des privilèges d’administration »

Vérifiez l’intégrité du code, le contenu du fichier PowerShell