Mathias Vételé

Désactivation de l’ouverture de session interactive sur un compte Active Directory

Table des matières

Contexte

Au sein de notre entreprise, nous utilisons des comptes de service, qui ne sont utilisé que dans un but : lancer / exécuter un service précis.

Cependant, ces comptes sont souvent oubliés, et laissés de côtés, ainsi, ils deviennent les cibles idéales pour des attaques. De plus, ces comptes possèdent souvent deux critères très recherchés par les attaquants : Des **privilèges souvent élevés**, et un **mot de passe fixe**, rarement ou **jamais renouvelé**.

Désactiver l’ouverture de session interactive sur ces comptes précisément intervient donc dans un contexte plus global de sécurisation de l’infrastructure informatique. Elle permet notamment de :

- **Bloquer les mouvements latéraux :** Empêche un attaquant d'utiliser ce compte pour se connecter en Bureau à distance (RDP) et naviguer facilement sur votre réseau pour attaquer d'autres cibles.
- **Protéger les identifiants (Critique) :** L'ouverture *automatique* stocke souvent le mot de passe en clair (ou mal protégé) dans le registre Windows, l'offrant sur un plateau aux attaquants.
- **Garantir la traçabilité (Imputabilité) :** Si une session interactive est ouverte, il devient impossible de savoir si une action a été faite par le logiciel légitime ou par un humain (administrateur ou pirate).
- **Respecter le "Moindre Privilège" :** Un service tourne en arrière-plan. Il n'a techniquement **jamais** besoin d'une interface graphique ou d'une souris pour fonctionner. Ce droit est inutile et dangereux.

Récupération des comptes concernés

Dans notre contexte, les comptes sur lesquels nous souhaitons désactiver l'ouverture de session interactive, sont donc nos comptes de services. Nous allons commencer par récupérer la liste entière de ces comptes présents dans notre domaine via Powershell.
Pour ceci, je vais utiliser ce script :

```powershell

Import-Module ActiveDirectory
$SearchFilter = "svc_*"

try {
    $SvcUsers = Get-ADUser -Filter "sAMAccountName -like '$($SearchFilter)'" -Properties DisplayName, Enabled |
        Select-Object -Property DisplayName, sAMAccountName, Enabled

    if ($SvcUsers) {
        $SvcUsers | Format-Table -AutoSize
        Write-Host "`nNombre total d'utilisateurs trouvés : $($SvcUsers.Count)"
    } else {
        Write-Host "Aucun utilisateur Active Directory local trouvé avec le préfixe '$($SearchFilter)'."
    }

} catch {
    Write-Error "Erreur lors de la connexion ou de la requête à Active Directory : $($_.Exception.Message)"
}
```

Le résultat de ce script est une liste organisée avec les informations suivantes :

DisplayName	sAMAccountName	Enabled
AD Service	svc_ad	True

Ainsi, j'ai donc pu récupérer tous mes comptes de service (ici 99 comptes), avec l'informations sur leur statut (Actif ou non).

Gestion de la criticité des comptes

Tous ces comptes sont donc censés être utilisés pour faire tourner des services spécifiques.
Je vais maintenant trier ces comptes selon leur criticité au niveau de l'entreprise.
Après un premier tri, je peux donc retirer une dizaine de comptes qui ne sont plus utilisés, ou dépréciés.

Ensuite, je mets en place 4 vagues, en fonction de la criticité du compte pour les activités de l'entreprise :

25	1ere vague	*(*Test + comptes désactivés + *Qualif)*
24	2e vague	Prod + peu critique
24	3e vague	Prod critique
18	4e vague	Très critique

Ces vagues définissent l'ordre d'action pour les futures semaines.

Le but étant faire la modification sur les comptes de la 1ere vague, puis voir si cela pose un problème dans la semaine, et ainsi de suite pour les suivantes.

Mise en place technique

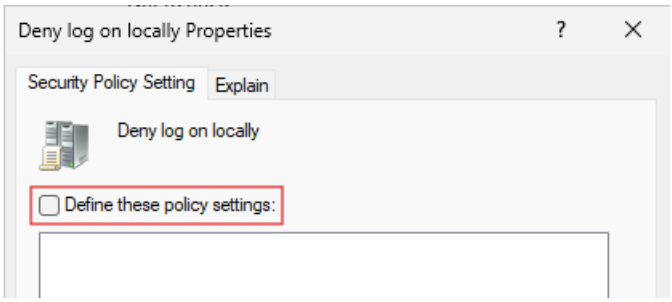
Pour la désactivation de l'ouverture de session interactive, une GPO doit être créée.
Les paramètres à définir se trouvent au chemin suivant :

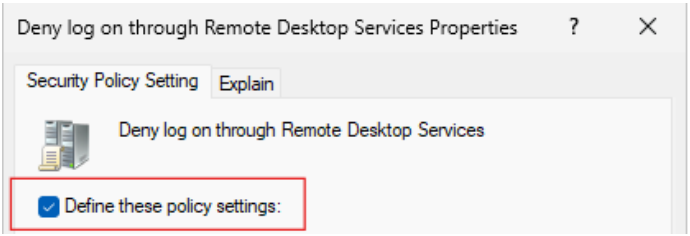
Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateurs >

« Refuser l'ouverture de session locale »

« Refuser l'ouverture de session à travers un bureau à distance »

Nous allons devoir définir cette politique, en cochant cette case :



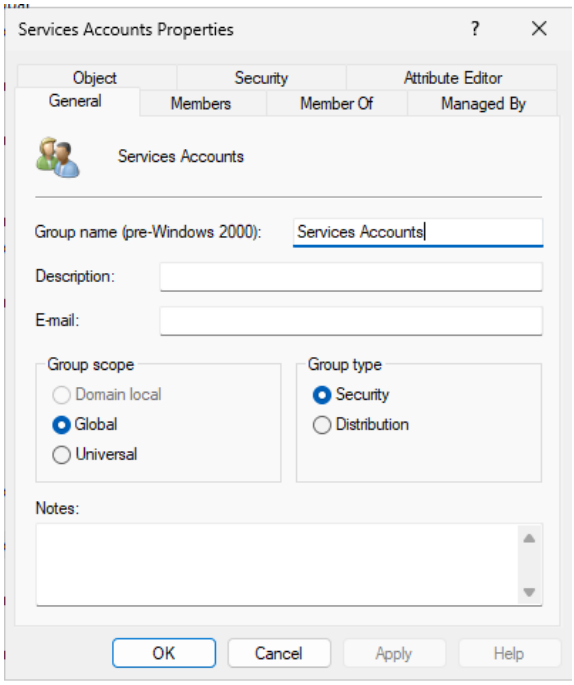


à noter que cette politique prend le dessus sur l'autre politique « **Autoriser la connexion locale », ainsi, si un utilisateur est présent dans les deux politiques, il sera bloqué, et la connexion lui sera refusée.*

Assignation aux Utilisateurs / Groupes

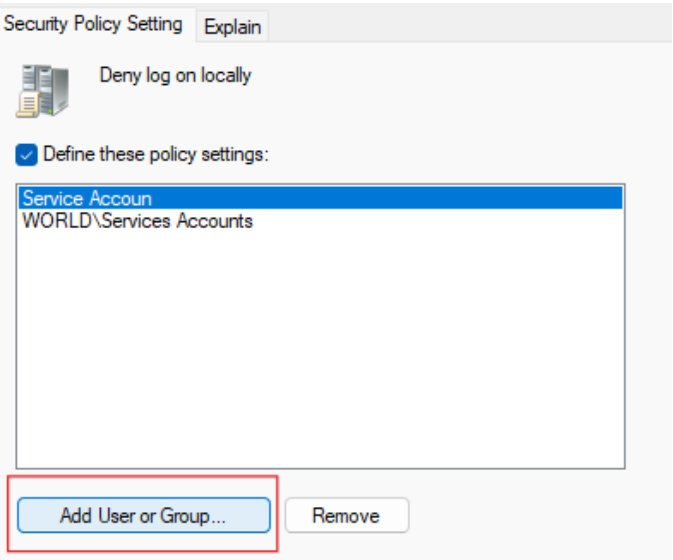
Une fois que la politique est définie, il nous faut maintenant l'assigner à nos utilisateurs ou groupes concernés.

Je vais donc créer un groupe, et le peuplé avec tous les comptes inclus dans la première vague.



Je vais ensuite l'alimenter au fur et à mesure avec les comptes des vagues suivantes.

Depuis la GPO, accéder directement au menu d'assignation



Puis y ajouter le groupe en question.

Test de validation

Il faut maintenant tester que la GPO soit bien effective sur les comptes en question.

J'utilise donc un compte présent dans mon groupe ***« Services Accounts »*** pour tenter de me connecter à un serveur via un bureau à distance.

Lors de l'ouverture de la session, je tombe sur ce message d'erreur, qui me valide bien le fonctionnement de notre GPO.