

TP3

Sécurisation

Travail réalisé par

:

Nermine HAMHOUM

&

Racem MOALLA

Le 23/10/2023.

Table des matières

1- Compétences.....	3
2. Conception du schéma de votre infrastructure.....	4
3. Stratégie de groupe.....	5
4. Sécuriser les comptes.....	9
5. Les scripts d'administration.....	10
6. Audit de sécurité.....	11
7-Un peu d'imagination.....	22
1. La connexion du client à l'AD :.....	22
2. L'installation de LAPS par GPO:.....	23
3. La génération du mot de passe par LAPS :.....	24
8- Conclusion:.....	25
Bibliographie.....	26

Introduction :

Ce TP a pour objectif de nous initier à la sécurisation d'un serveur Active Directory. L'Active Directory est un composant crucial de toute infrastructure informatique, et il est essentiel de le protéger pour garantir la sécurité des données et des ressources.

Au cours de ce TP, nous aborderons des aspects tels que la réalisation d'un audit de sécurité, la gestion des comptes, et l'utilisation des Group Policy Objects (GPOs) liées à Windows Server Update Services (WSUS). Chaque étape nous rapprochera de la compréhension des enjeux de la sécurisation de l'Active Directory.

1- Compétences

Compréhension des étapes pour réaliser un audit de sécurité au sein d'un Active Directory.
Maîtrise de la gestion des attributs des comptes utilisateurs, y compris la gestion des comptes expirés.

Familiarité avec la configuration et la gestion des Group Policy Objects (GPO) liées à Windows Server Update Services (WSUS) pour maintenir la sécurité des mises à jour dans notre environnement Active Directory.

2. Conception du schéma de votre infrastructure

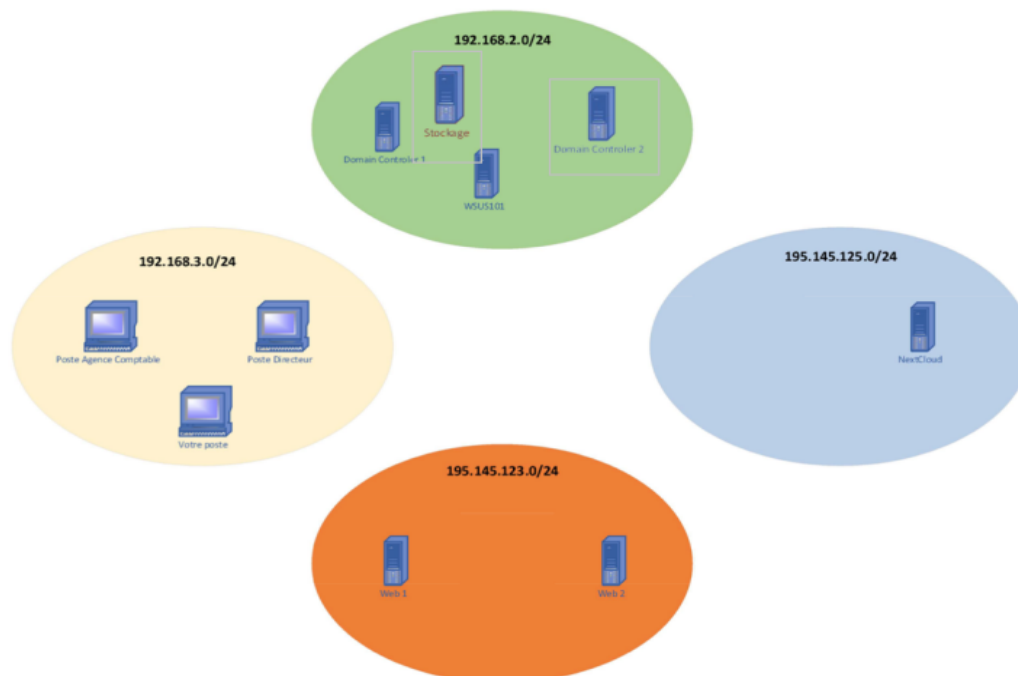


figure 1 : Correction du schéma de notre infrastructure

Nous renforçons la fiabilité et la résilience de notre infrastructure en introduisant un deuxième contrôleur de domaine, DC2, pour garantir une haute disponibilité et une tolérance aux pannes. Ainsi, en cas de défaillance de DC1, DC2 est prêt à prendre le relais, assurant ainsi la continuité de nos opérations.

Pour améliorer la sécurité et la gestion de NextCloud, nous avons choisi de l'isoler, limitant ainsi les interactions avec les serveurs de domaine. Cette isolation contribue à réduire les vulnérabilités potentielles et à renforcer la sécurité globale de NextCloud.

En ce qui concerne les deux serveurs Web, nous avons également pris des mesures pour minimiser les risques de sécurité. Nous avons isolé ces serveurs pour restreindre l'accès et avons mis en place un contrôle plus précis de leur configuration et de leur sécurité.

De plus, nous pouvons mettre en place des pare-feu pour renforcer davantage la sécurité en contrôlant les flux de trafic entrants et sortants vers ces serveurs. Cela garantit une protection supplémentaire contre les menaces potentielles.

3. Stratégie de groupe

Pour mettre en place une GPO visant à activer l'AES, il est nécessaire d'ouvrir l'outil de gestion des stratégies de groupe.

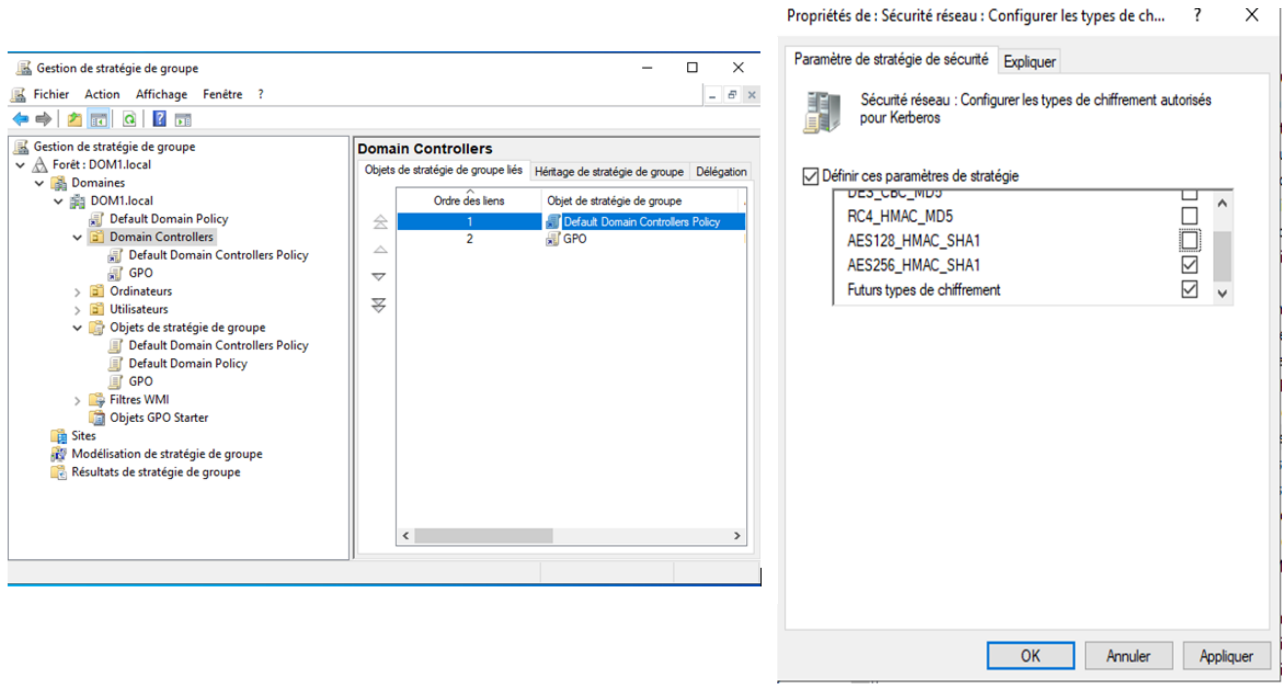


Figure 2 : création du GPO

Dans le cadre de ce travail, nous avons créé un client au sein de notre Active Directory et lui avons attribué l'utilisation de l'Advanced Encryption Standard (AES) pour les tickets Kerberos.

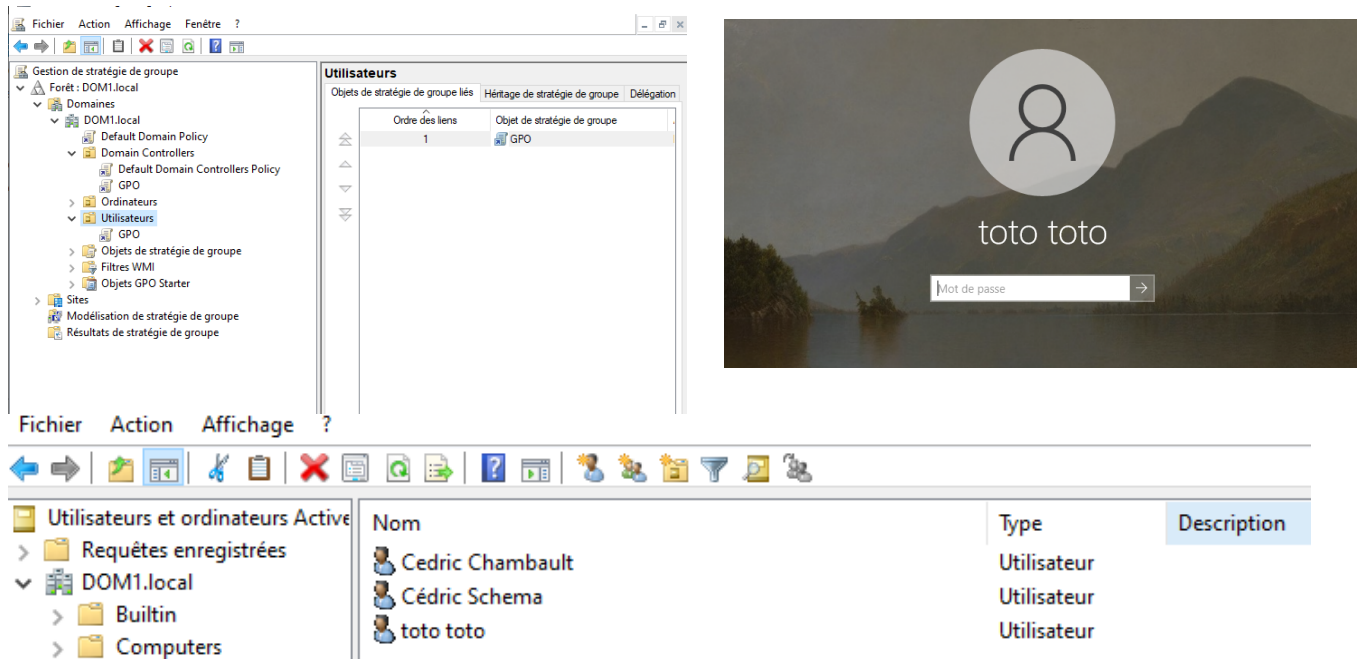


Figure : création du client

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\toto> klist

LogonId est 0x0116f42

Tickets mis en cache : (0)
PS C:\Users\toto> gpupdate
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Users\toto> klist

LogonId est 0x0116f42

Tickets mis en cache : (2)

#0> Client : toto @ DOM1.LOCAL
Serveur : krbtgt/DOM1.LOCAL @ DOM1.LOCAL
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Heure de démarrage : 10/23/2023 18:17:29 (Local)
Heure de fin : 10/24/2023 4:17:29 (Local)
Heure de renouvellement : 10/30/2023 18:17:29 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0x1 -> PRIMARY
KDC appelé : AD1.DOM1.local

#1> Client : toto @ DOM1.LOCAL
Serveur : LDAP/AD1.DOM1.local/DOM1.local @ DOM1.LOCAL
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Heure de démarrage : 10/23/2023 18:17:29 (Local)
Heure de fin : 10/24/2023 4:17:29 (Local)
Heure de renouvellement : 10/30/2023 18:17:29 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0
KDC appelé : AD1.DOM1.local
```

Figure: Vérification de l'application de l'AES sur les tickets Kerberos

Lors de la configuration de notre GPO pour activer l'AES, nous avons vérifié son utilisation dans les Tickets Kerberos. En observant les échanges, nous avons confirmé que l'AES était bien employé, renforçant ainsi la sécurité de nos communications.

```
Heure de renouvellement : 10/19/2023 18:40:53 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0x1 -> PRIMARY
KDC appelé : AD1

#1> Client : Administrateur @ DOM1.LOCAL
Serveur : ldap/AD1.DOM1.local/DOM1.LOCAL @ DOM1.LOCAL
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Heure de démarrage : 10/12/2023 18:43:18 (Local)
Heure de fin : 10/13/2023 4:40:53 (Local)
Heure de renouvellement : 10/19/2023 18:40:53 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0
KDC appelé : AD1

#2> Client : Administrateur @ DOM1.LOCAL
Serveur : host/ad1.dom1.local @ DOM1.LOCAL
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Heure de démarrage : 10/12/2023 18:40:53 (Local)
Heure de fin : 10/13/2023 4:40:53 (Local)
Heure de renouvellement : 10/19/2023 18:40:53 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0
KDC appelé : AD1

PS C:\Users\Administrateur>
```

Figure: Confirmation de l'Utilisation de l'AES pour les Tickets Kerberos

La valeur de l'attribut "msds-supportedencryptiontypes", qui est égale à 16, indique que nous utilisons l'AES 256 bits pour le chiffrement des tickets Kerberos. L'AES 256 bits est un chiffrement avancé et sécurisé, renforçant ainsi la protection de nos communications au sein de l'Active Directory. Cette configuration contribue positivement à la sécurité de notre infrastructure en garantissant que les échanges de données sont effectués avec un niveau de sécurité élevé.

```
PS C:\Users\Administrateur> Get-ADComputer AD1 -properties * | fl
msDS-SupportedEncryptionTypes

PS C:\Users\Administrateur> Get-ADComputer AD1 -properties * | fl msDS-SupportedEncryptionTypes

msDS-SupportedEncryptionTypes : 16
```

Figure: valeur de l'attribut msds-supportedencryptiontypes

15	0xF	DES_CBC_CBC, DES_CBC_MD5, RC4, AES 128
16	0x10	AES 256
17	0x11	DES_CBC_CRC, AES 256
18	0x12	DES_CBC_MD5, AES 256
19	0x13	DES_CBC_CRC, DES_CBC_MD5, AES 256
20	0x14	RC4, AES 256

Figure: Interprétation de la Valeur

(source:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/decrypting-the-selection-of-supported-kerberos-encryption-types/ba-p/1628797>)

4. Sécuriser les comptes

Notre script PowerShell supprime automatiquement les comptes d'utilisateurs expirés de l'Active Directory et envoie une notification par e-mail aux administrateurs pour les informer de cette action. Cela garantit une gestion efficace des comptes inutilisés tout en fournissant une traçabilité essentielle.

```
# Spécifiez les informations du serveur SMTP
$smtpServer = "SMTP.gmail.com"
$smtpPort = 587
$smtpUsername = "Hamhoumoalla"
$smtpPassword = "dhkjddksg*3"
$senderEmail = "Hamhoumoalla@gmail.com"
$recipientEmail = "hamhounermine@gmail.com"

# Récupérez la date actuelle
$currentDate = Get-Date

# Obtenez la liste des comptes d'utilisateur expirés
$expiredUsers = Get-ADUser -Filter {Enabled -eq $true -and AccountExpirationDate -lt $currentDate} -Properties AccountExpirationDate

# Supprimez les comptes d'utilisateur expirés et envoyez un e-mail de notification
foreach ($user in $expiredUsers) {
    $userName = $user.SamAccountName
    $userEmail = $user.UserPrincipalName
    $accountExpirationDate = $user.AccountExpirationDate
    Remove-ADUser -Identity $user -Confirm:$false # Supprimer l'utilisateur

    # Envoyez un e-mail de notification
    $subject = "Compte utilisateur expiré : $userName"
    $body = "Le compte utilisateur $userName ($userEmail) a expiré le $accountExpirationDate et a été supprimé."
    Send-MailMessage -SmtpServer $smtpServer -Port $smtpPort -UseSsl $true -From $senderEmail -To $recipientEmail -Subject $subject
}
```

figure: Script PowerShell de Suppression des Comptes Expirés avec Notification par E-mail

5. Les scripts d'administration

Pour garantir un emplacement approprié pour nos scripts d'administration, nous proposons de les stocker dans le répertoire réseau suivant : "\\réseaux\sysvol\scripts\NotreScripts". Cette décision repose sur plusieurs raisons cruciales. En plaçant nos scripts dans ce répertoire réseau, nous offrons à l'administrateur la flexibilité d'exécution à tout moment, quel que soit l'endroit où il se trouve. Cela simplifie grandement la gestion des scripts, car l'administrateur peut y accéder de manière centralisée.

Pour renforcer la sécurité de leur exécution, nous avons pris des mesures supplémentaires. Des droits d'exécution et de visualisation exclusifs ont été attribués à l'administrateur (Contrôle total, modification...). Ces autorisations exclusives garantissent que seules les personnes autorisées, en l'occurrence l'administrateur, ont la capacité d'exécuter et de visualiser les scripts. Cela renforce la confidentialité et la sécurité des scripts d'administration, ce qui est essentiel pour maintenir l'intégrité du système et la gestion des opérations administratives.

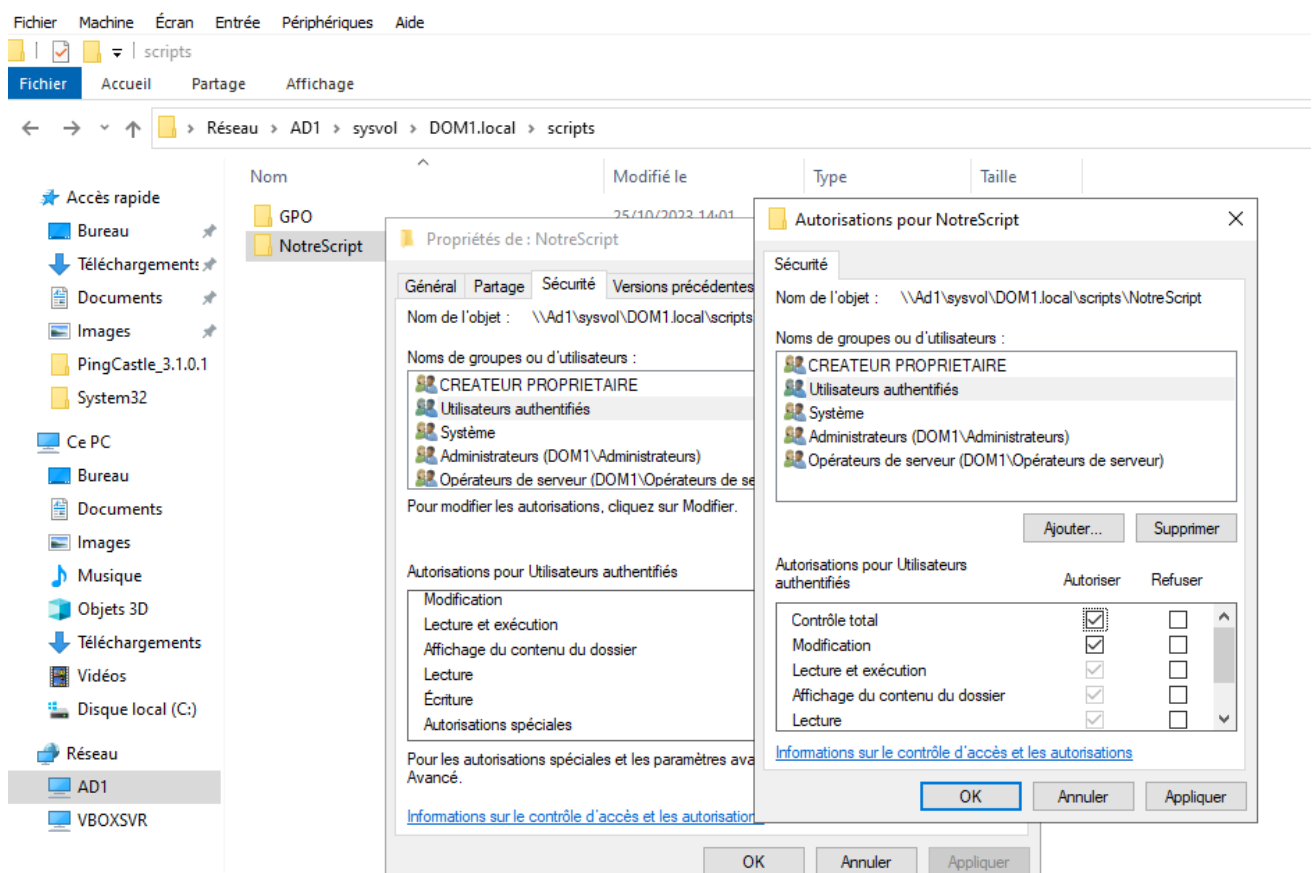


Figure :Script d'administration

6. Audit de sécurité

Nous avons entrepris un audit de sécurité approfondi de notre infrastructure Active Directory en collaboration avec l'outil d'analyse de sécurité PingCastle. Notre objectif était d'identifier et de résoudre les vulnérabilités potentielles dans notre environnement, améliorant ainsi notre posture de sécurité globale. Au début de l'audit, notre Domain Risk Level était de 70 sur 100, avec des scores spécifiques de 31/100 pour les objets obsolètes, 60/100 pour les comptes privilégiés et 70/100 pour les anomalies. Notre niveau de confiance dans les relations de confiance était à son niveau le plus bas, avec un score de 0/100.

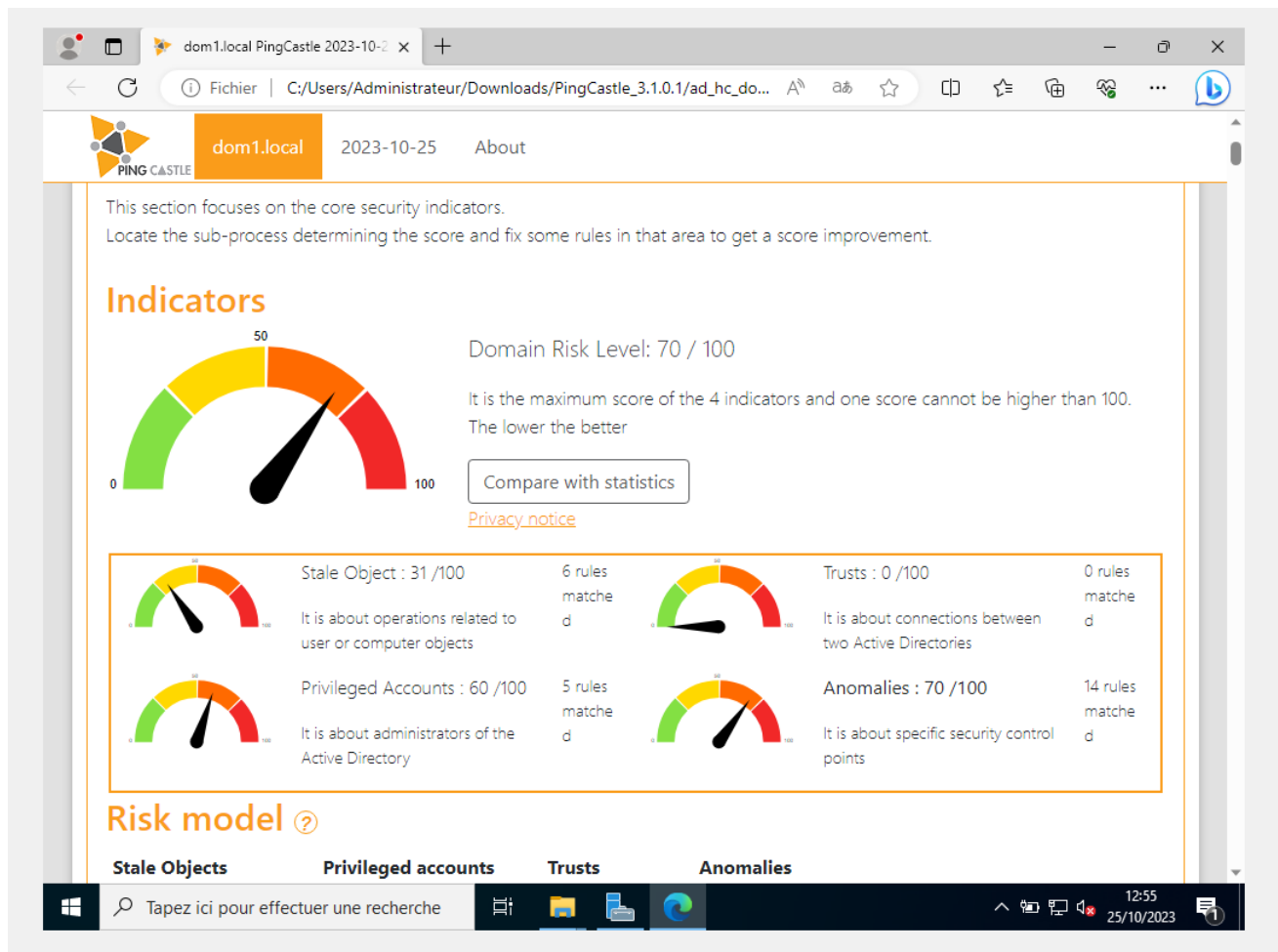


figure:Le score initial de Domain risk

Pour commencer à résoudre les anomalies identifiées, nous allons prendre des mesures immédiates pour sécuriser le service d'impression (Print Spooler) et empêcher son utilisation abusive pour obtenir les identifiants du contrôleur de domaine (DC).

The spooler service is remotely accessible from 1 DC

+ 10 Point(s)

Ensure that the Print Spooler service cannot be abused to get the DC credentials

Rule ID:

A-DC-Spooler

Description:

The purpose is to ensure that credentials cannot be extracted from the DC via its Print Spooler service

Technical explanation:

When there's an account with unconstrained delegation configured (which is fairly common) and the Print Spooler service running on a computer, you can get that computer's credentials sent to the system with unconstrained delegation as a user. With a domain controller, the TGT of the DC can be extracted allowing an attacker to reuse it with a DCSync attack and obtain all user hashes and impersonate them.

Advised solution:

The Print Spooler service should be deactivated on domain controllers. Please note as a consequence that the Printer Pruning functionality (rarely used) will be unavailable.

Figure: Problème du service d'impression

Désactivation du Service d'Impression (Print Spooler) avec PowerShell :

`Stop-Service -Name "Spooler" -Force`

En exécutant cette commande PowerShell sur chaque contrôleur de domaine, nous arrêtons le service d'impression de manière immédiate et forcée. Cette action empêchera toute exploitation potentielle du service d'impression pour accéder aux identifiants du contrôleur de domaine.

Cette étape immédiate et proactive témoigne de notre engagement à sécuriser notre environnement Active Directory et à réduire notre surface d'attaque. Nous continuons à surveiller attentivement notre réseau et à prendre des mesures supplémentaires pour résoudre les autres anomalies identifiées et améliorer notre posture de sécurité globale.

```
PS C:\Users\Administrateur> Get-Service -Name Spooler

Status  Name      DisplayName
-----
Running Spooler   Spouleur d'impression

PS C:\Users\Administrateur> Stop-Service -Name "Spooler" -Force
PS C:\Users\Administrateur>
```

Figure Désactivation du Service d'Impression

Après cette démarche ,nous avons remarqué que l'anomalie a baissé de 10 points.

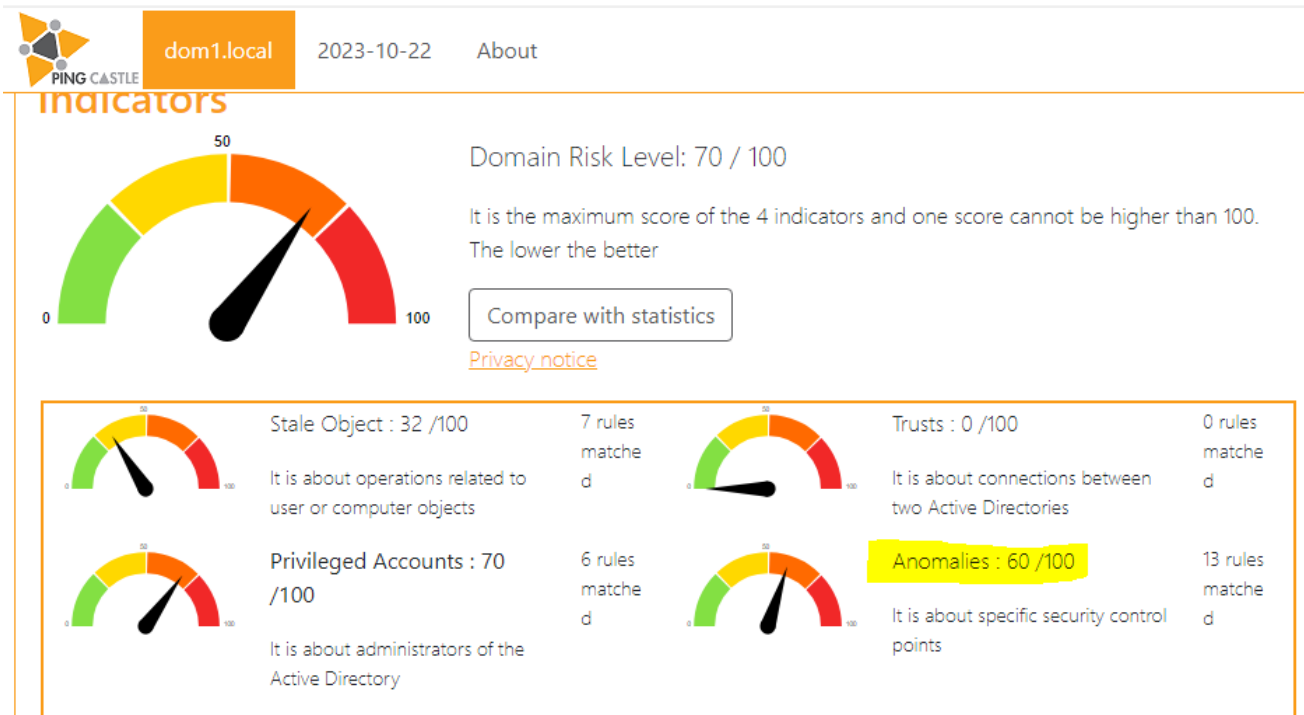


Figure:Premier résultat après la correction de la première anomalie

Remédiation du Problème des Comptes Priviliégiés : Groupe "Schema Admins" non Vide

Le problème signalé par l'outil de sécurité est le suivant : le groupe "Schema Admins" n'est pas vide. Ce groupe, dans l'Active Directory, détient des autorisations très élevées, notamment la capacité de modifier le schéma global de l'annuaire. Par conséquent, il est impératif de garantir que seuls les utilisateurs et comptes de confiance absolument nécessaires soient membres de ce groupe. Pour résoudre ce problème, nous allons suivre une démarche précise :

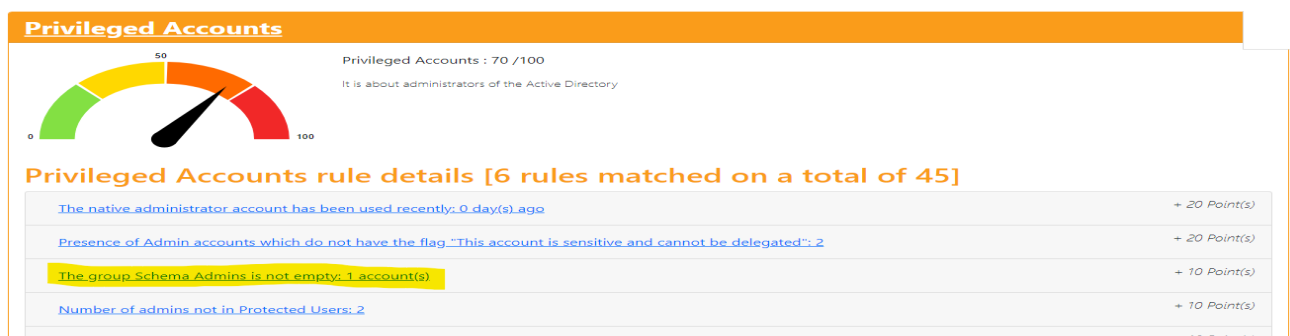


Figure:Problème de groupe d'administrateurs du schéma

Pour remédier au problème du groupe "Schema Admins" non vide, nous allons suivre ces deux étapes :

Étape 1 : Audit et Révision des Membres Actuels :

Nous examinerons attentivement les membres actuels du groupe "Schema Admins". Toute personne qui n'a pas une justification valide pour l'accès au schéma global de l'annuaire sera retirée du groupe.

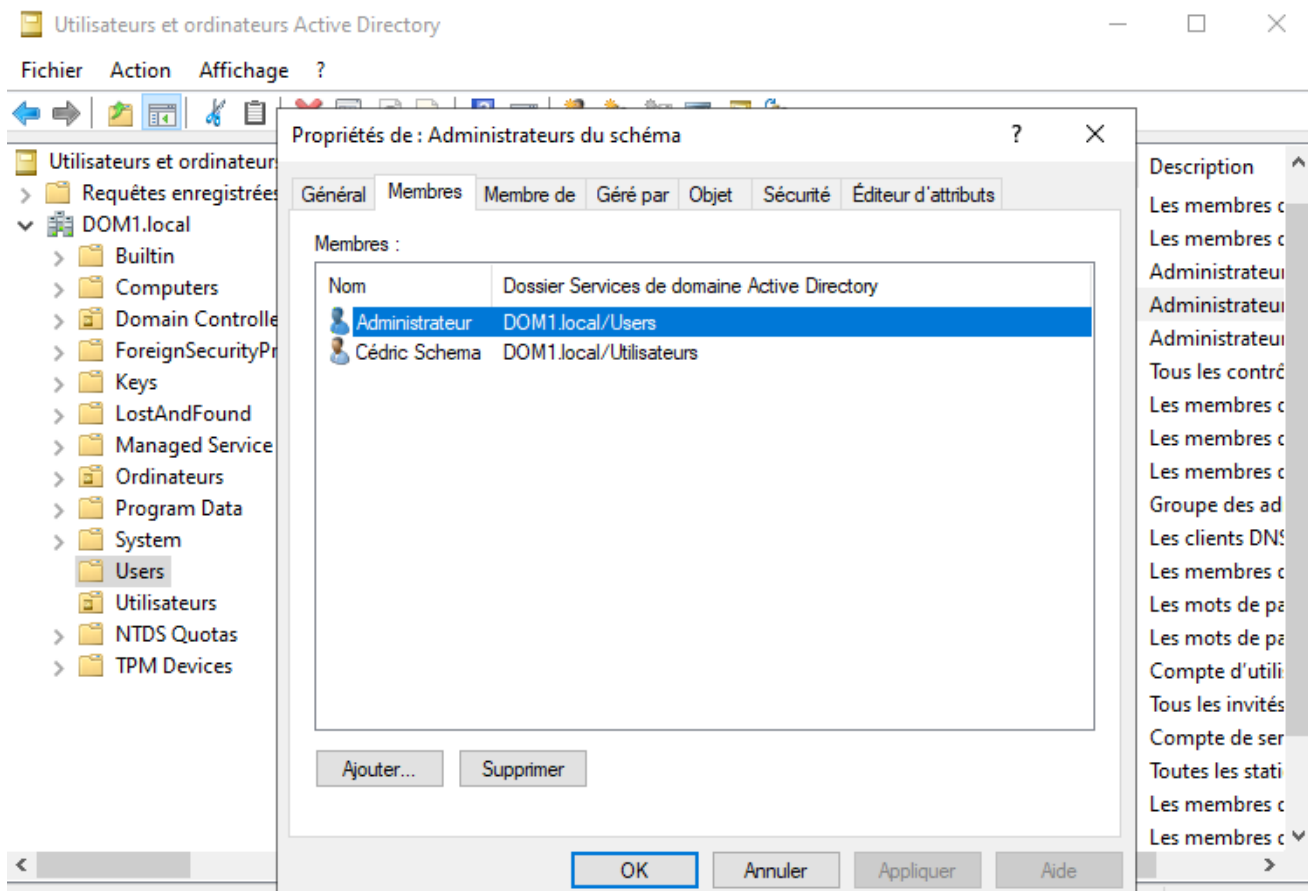


Figure: Propriétés du groupe administrateurs de schéma

Étape 2 : Retrait des Membres Non Nécessaires :

Nous retirerons de manière proactive tous les membres qui ne sont pas justifiés dans le groupe "Schema Admins". Cette action sera réalisée avec précaution pour minimiser les perturbations opérationnelles tout en garantissant que seuls les utilisateurs nécessaires conservent ce niveau de privilège.

Ces étapes garantiront que seuls les utilisateurs ayant une justification valide auront accès au groupe "Schema Admins", réduisant ainsi le risque lié aux comptes privilégiés et améliorant la sécurité globale de notre environnement Active Directory.

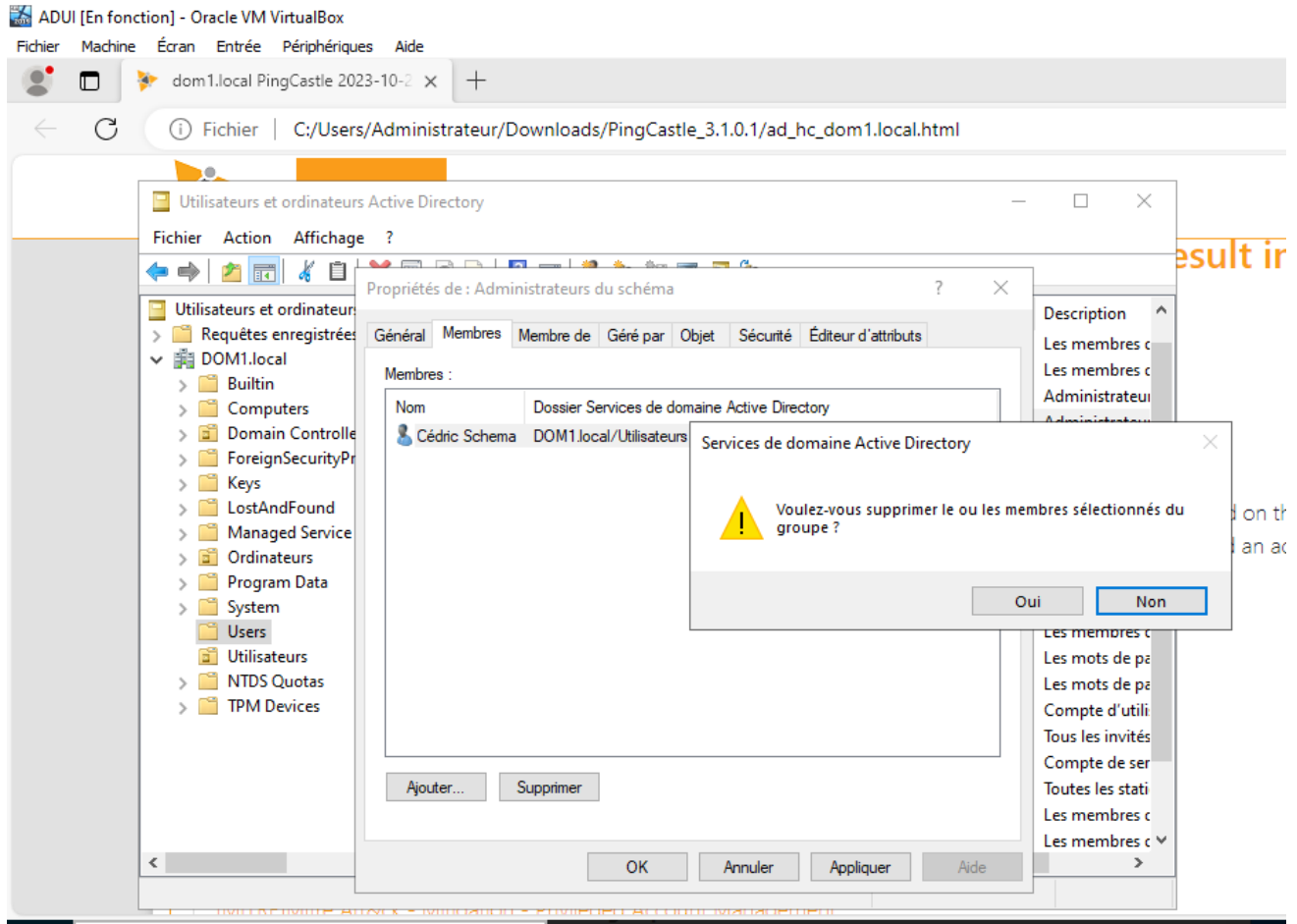


Figure : Suppression des membres du groupe administrateurs du schéma

Nous allons relancé Ping Castle. Le score de privileged accounts a significativement diminué.



dom1.local

2023-10-22

About

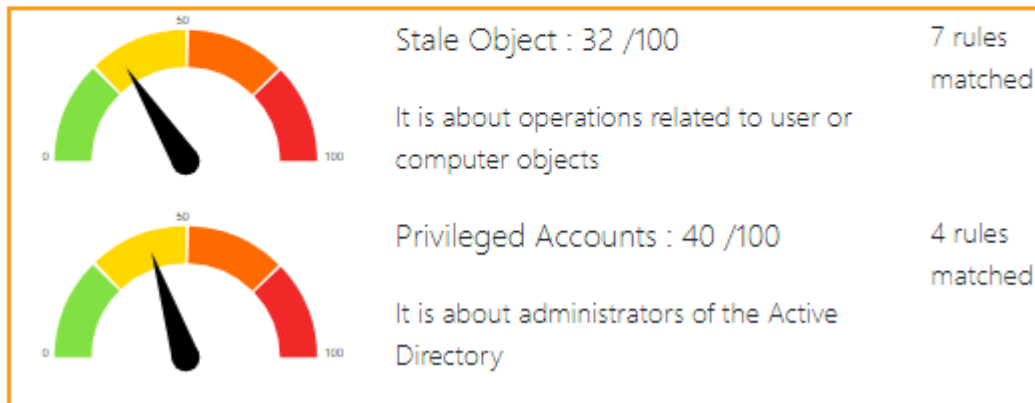


Figure: Baisse de "privileged accounts score"

Problème : Nous avons rencontré un problème lié à la vérification d'objets obsolètes lors du processus d'enregistrement des ordinateurs dans votre domaine Active Directory. Cela signifie que des objets d'ordinateurs inactifs ou obsolètes ne sont pas correctement nettoyés ou désactivés, ce qui peut entraîner une mauvaise gestion des comptes d'ordinateurs.

Check the process of registration of computers to the domain

Rule ID:
S-ADRegistration

Description:
The purpose is to ensure that basic users cannot register extra computers in the domain

Technical explanation:
By default, a basic user can register up to 10 computers within the domain. This default configuration represents a security issue as basic users shouldn't be able to create such accounts and this task should be handled by administrators.

Note: this program checks also the GPO for SeMachineAccountPrivilege assignment. This assignment can be used to restrict the impact of the key ms-DS-MachineAccountQuota.

Advised solution:
To solve the issue, limit the number of extra computers that can be registered by a basic user. It can be reduced by modifying the value of `ms-DS-MachineAccountQuota` to zero (0).

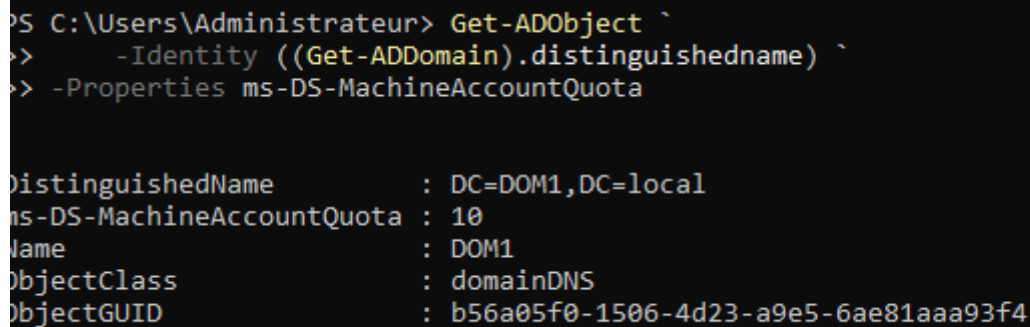
Figure: Probleme lié au nombre d'ordinateurs dans le domaine

Solution : Pour résoudre ce problème, nous allons utiliser Windows PowerShell pour ajuster la configuration de l'attribut responsable de cette vérification. Voici comment procéder :

1. Tout d'abord, nous devons comprendre comment est configurée la vérification des objets obsolètes. Pour cela, nous allons utiliser la cmdlet Get-ADObject pour vérifier la valeur actuelle de l'attribut. Cette étape nous permettra de comprendre la configuration actuelle.

powershell

```
Get-ADObject `
  -Identity ((Get-ADDomain).distinguishedname) `
  -Properties ms-DS-MachineAccountQuota
```



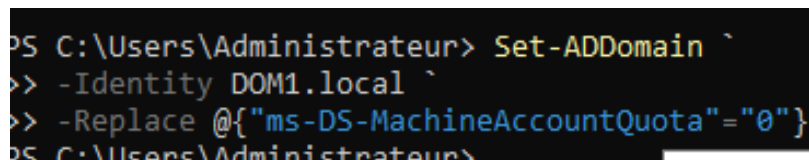
```
PS C:\Users\Administrateur> Get-ADObject `
> -Identity ((Get-ADDomain).distinguishedname) `
> -Properties ms-DS-MachineAccountQuota

DistinguishedName      : DC=DOM1,DC=local
ms-DS-MachineAccountQuota : 10
Name                   : DOM1
ObjectClass             : domainDNS
ObjectGUID              : b56a05f0-1506-4d23-a9e5-6ae81aaa93f4
```

Figure:Les propriétés de machines dans le domaine

2. Une fois que nous avons identifié la configuration actuelle, nous pouvons procéder à la modification de l'attribut pour désactiver la vérification des objets obsolètes. Pour ce faire, nous utiliserons la cmdlet Set-ADDomain. powershell

```
Set-ADDomain `
  -Identity <NomDuDomaine> `
  -Replace @{"ms-DS-MachineAccountQuota"="0"}
```



```
PS C:\Users\Administrateur> Set-ADDomain `
> -Identity DOM1.local `
> -Replace @{"ms-DS-MachineAccountQuota"="0"}
```

Figure:Modification de l'attribut

En effectuant cette modification, nous désactivons la vérification des objets obsolètes, ce qui permettra une meilleure gestion des comptes d'ordinateurs dans votre domaine. Assurez-vous de comprendre les implications de cette modification avant de l'appliquer, car cela peut avoir un impact sur la maintenance de votre infrastructure Active Directory.

Nous avons relancé Ping Castle et nous avons vérifié que stale object a baissé de 10 points:

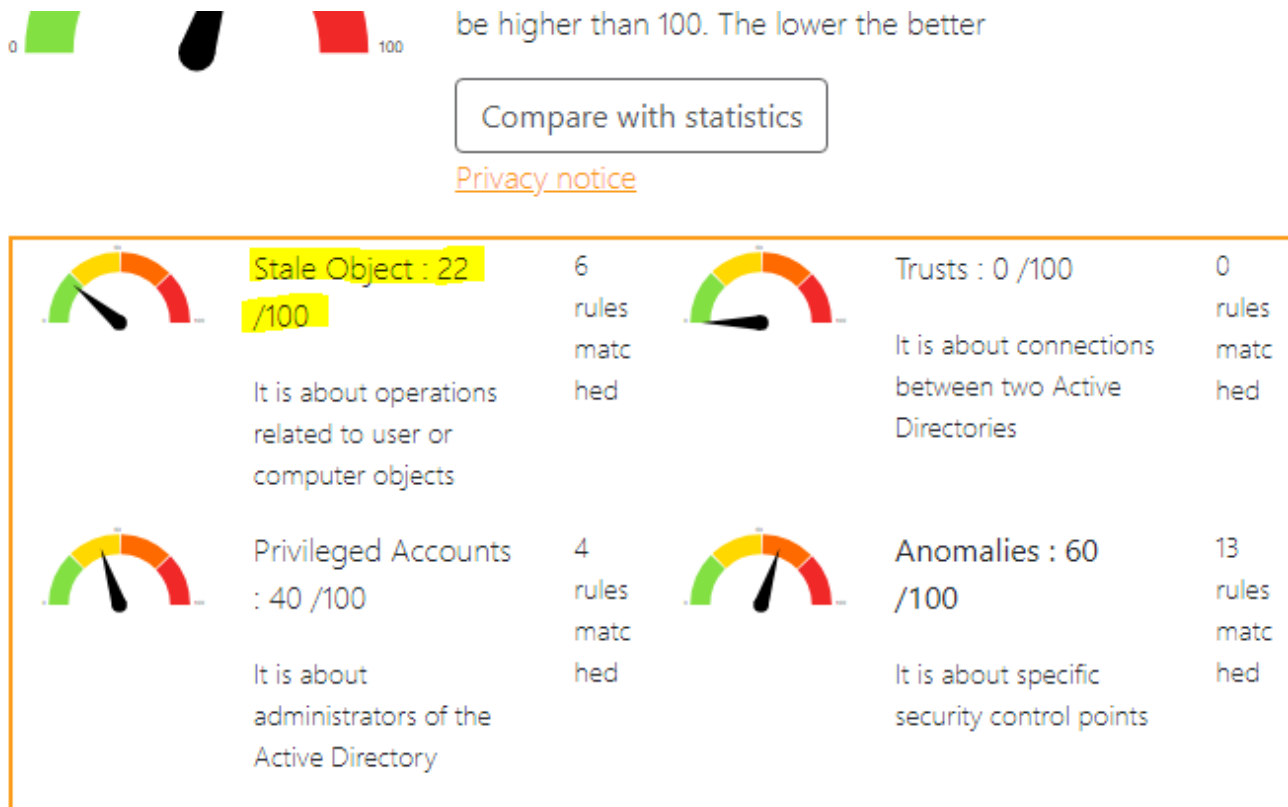


Figure:La baisse de “Stale Object”

De la même façon ,on a procédé pour remédier aux autres problèmes rencontrés:

Recycle bin feature is not enabled



Privileged Accounts : 40 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [4 rules matched on a total of 45]

The native administrator account has been used recently: 10 day(s) ago	+ 20 Point(s)
The Recycle Bin is not enabled	+ 10 Point(s)
Ensure that the Recycle Bin feature is enabled	
Rule ID: P-RecycleBin	
Description:	

Figure: Probleme lié au “recycle bin feature”

Nous avons activé la corbeille Active Directory pour résoudre le problème lié à la fonctionnalité de la corbeille (Recycle Bin Feature).

L'activation de cette fonctionnalité est cruciale car elle ajoute une couche de protection importante pour la gestion des objets Active Directory, permettant de récupérer des données importantes en cas de suppression accidentelle. Elle simplifie considérablement la restauration d'objets sans avoir à restaurer l'ensemble de l'annuaire, ce qui peut économiser du temps et réduire les erreurs potentielles.

```
S C:\Users\Administrateur> Set-ADDomain `
> -Identity DOM1.local `
> -Replace @{"ms-DS-MachineAccountQuota"="0"}
S C:\Users\Administrateur> Enable-ADOptionalFeature -Identity "CN=Recycle Bin Feature,CN=Optional Features,CN=Di
NT,CN=Services,CN=Configuration,DC=DOM1,DC=local" -Scope ForestOrConfigurationSet -Target "DOM1.local"
VERTISSEMENT : L'activation de « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=DOM1,DC=local » e
rréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=DOM
ontinuez.

onfirmer
tes-vous sûr de vouloir effectuer cette action ?
pération « Enable » en cours sur la cible « Recycle Bin Feature ».
O) Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « 0 »)
S C:\Users\Administrateur> _
```

Figure:Activation de la corbeille de l'AD

```
PS C:\Users\Administrateur> Get-ADOptionalFeature -Filter 'Name -eq "Recycle Bin Feature"'

DistinguishedName : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory
Service,CN=Windows NT,CN=Services,CN=Configuration,DC=DOM1,DC=local
EnabledScopes      : {CN=Partitions,CN=Configuration,DC=DOM1,DC=local, CN=NTDS Settings,C
N=AD1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuratio
n,DC=DOM1,DC=local}
FeatureGUID        : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Recycle Bin Feature
ObjectClass         : msDS-OptionalFeature
ObjectGUID         : d567be30-188f-46b9-ad19-b9eefd6d1349
RequiredDomainMode : 
RequiredForestMode : Windows2008R2Forest
```

Figure:Vérification de l'activation de la corbeille de l'AD

Pour le problème du mot de passe, nous avons tenté d'augmenter sa longueur.(Longueur=14)

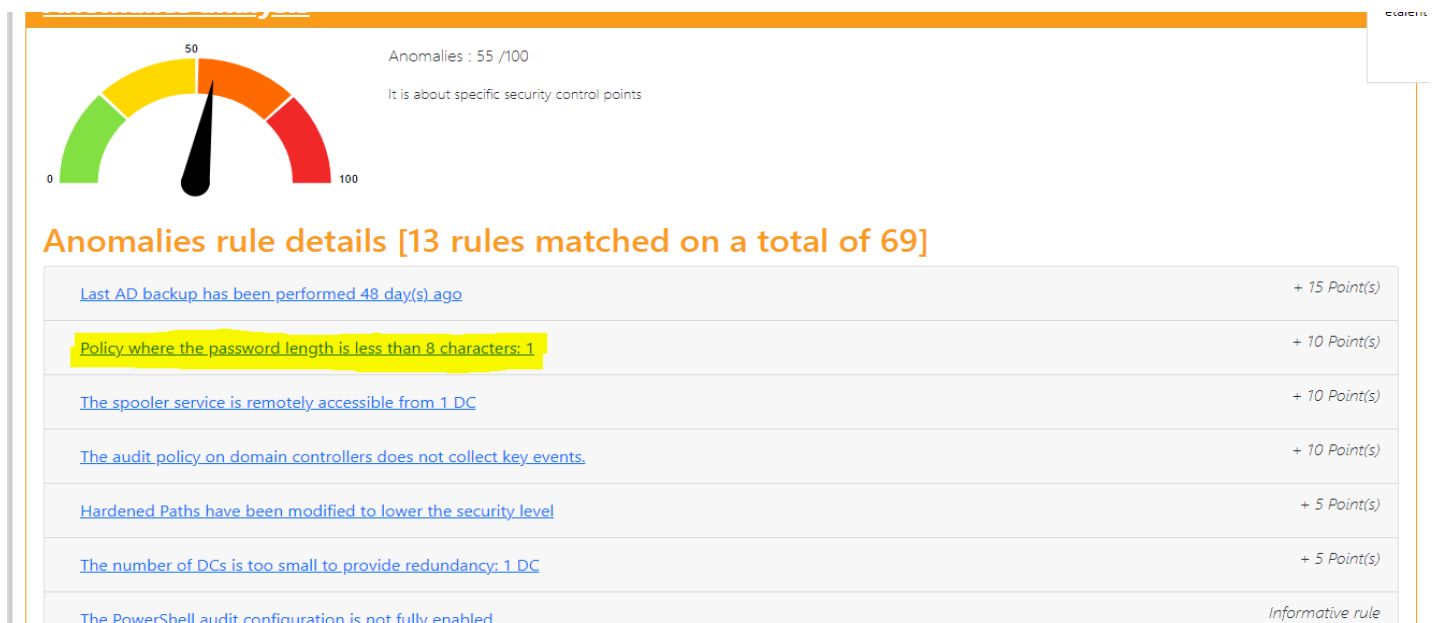


Figure:Probleme de la longueur du mot de passe

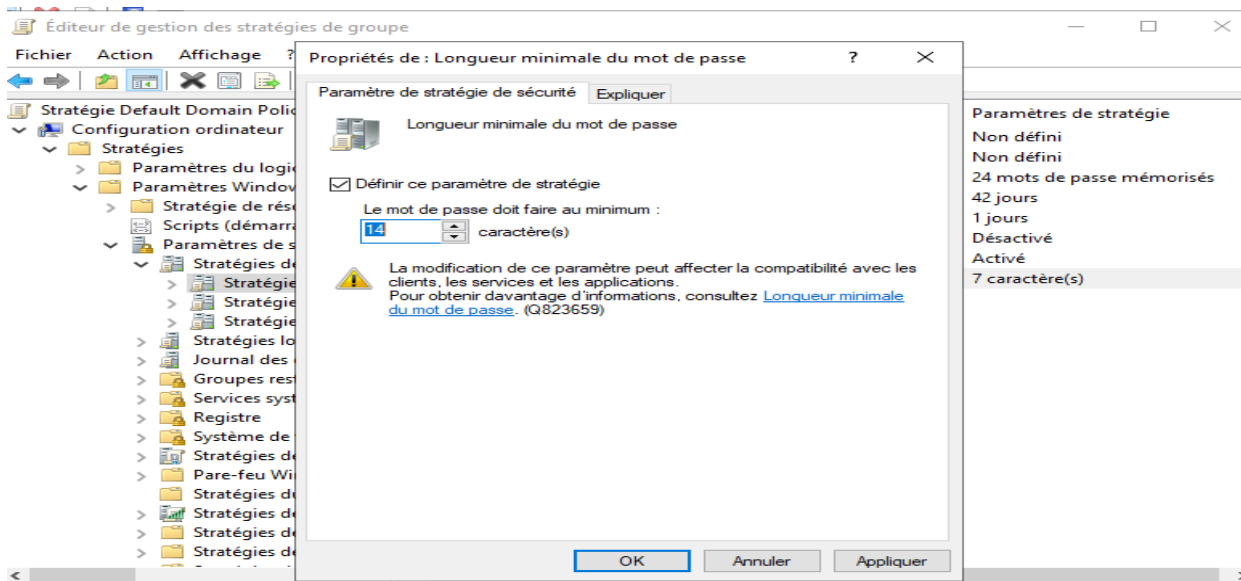


Figure: Modification de la longueur du mot de passe

De même, on a remédié à un autre problème : L'installation de LAPS.

Finalement, nous avons baissé le score de domain risk .

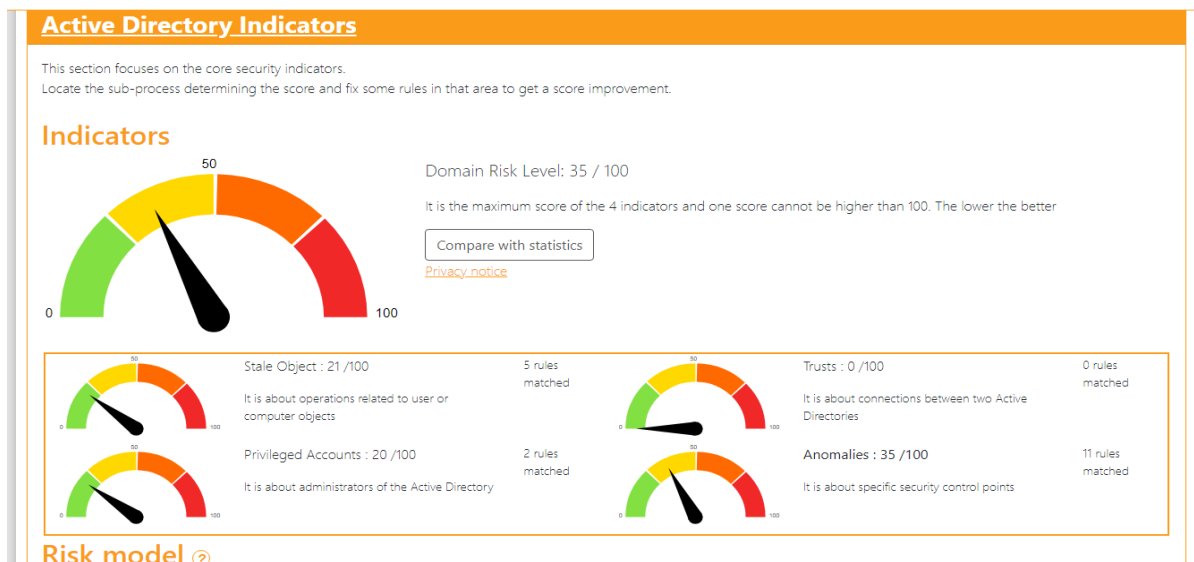


Figure : Le score de risque du domaine a baissé

7-Un peu d'imagination

LAPS (Local Administrator Password Solution) est une solution de gestion des mots de passe pour les comptes Administrateur local sur des ordinateurs Windows. Elle génère et gère de manière sécurisée des mots de passe uniques pour ces comptes, améliorant ainsi la sécurité en évitant que tous les ordinateurs partagent le même mot de passe Administrateur local. LAPS est généralement utilisée dans les environnements d'entreprise pour renforcer la sécurité des postes de travail et des serveurs Windows.

1. La connexion du client à l'AD :

- Tout d'abord, nous avons configuré un ordinateur client pour qu'il rejoigne le domaine Active Directory de notre réseau. Pour cela, nous avons utilisé les informations du domaine, telles que le nom du domaine, le nom d'utilisateur et le mot de passe d'un compte ayant les droits nécessaires.
- Une fois que l'ordinateur client a été correctement joint au domaine, il a pu être géré de manière centralisée par l'Active Directory, ce qui a simplifié l'administration des ordinateurs dans notre réseau.

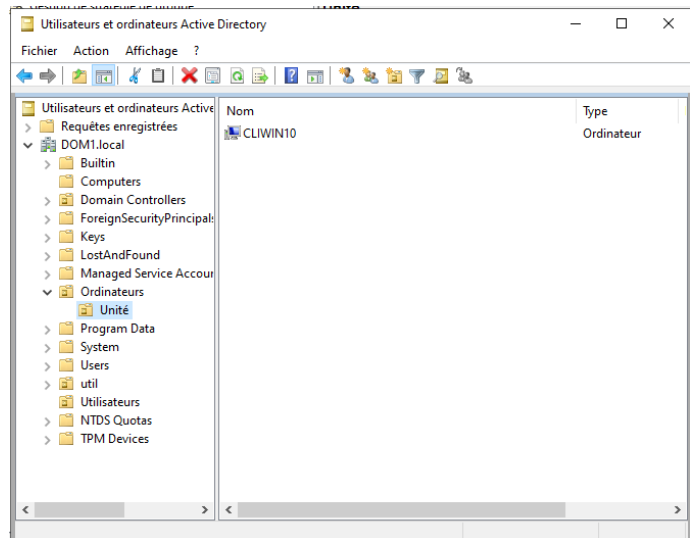
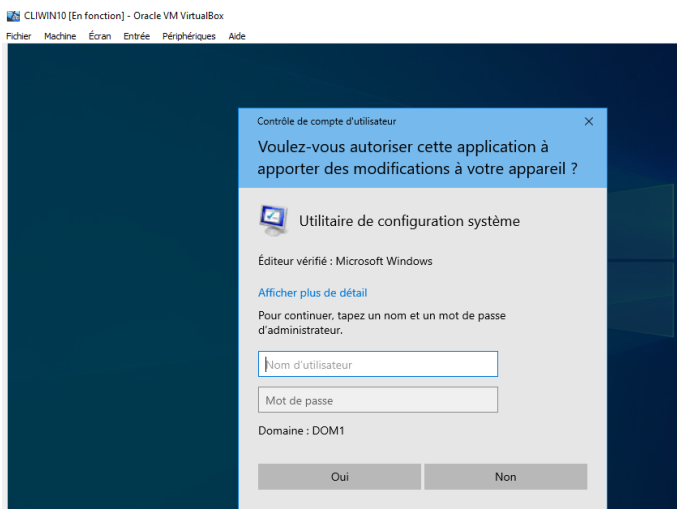


Figure:Connexion du client à l'AD

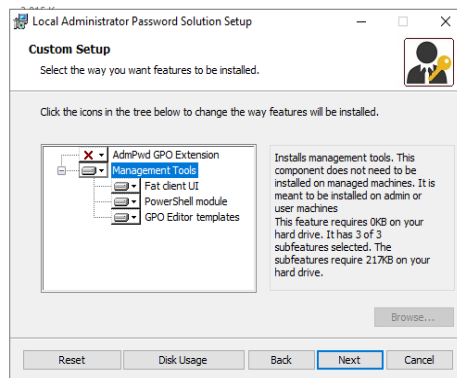


Figure:Installation de LAPS

2. L'installation de LAPS par GPO:

- Après avoir connecté l'ordinateur client à l'Active Directory, nous avons utilisé les stratégies de groupe (GPO) pour déployer l'outil LAPS (Local Administrator Password Solution).
- Nous avons créé une GPO qui contenait les paramètres nécessaires pour installer LAPS sur les ordinateurs cibles. Cela a inclus des fichiers d'installation et des paramètres de configuration.
- Ensuite, nous avons appliqué cette GPO aux ordinateurs ou aux unités d'organisation appropriés dans notre domaine. Lorsque les ordinateurs se sont mis à jour avec cette GPO, LAPS a été installé.

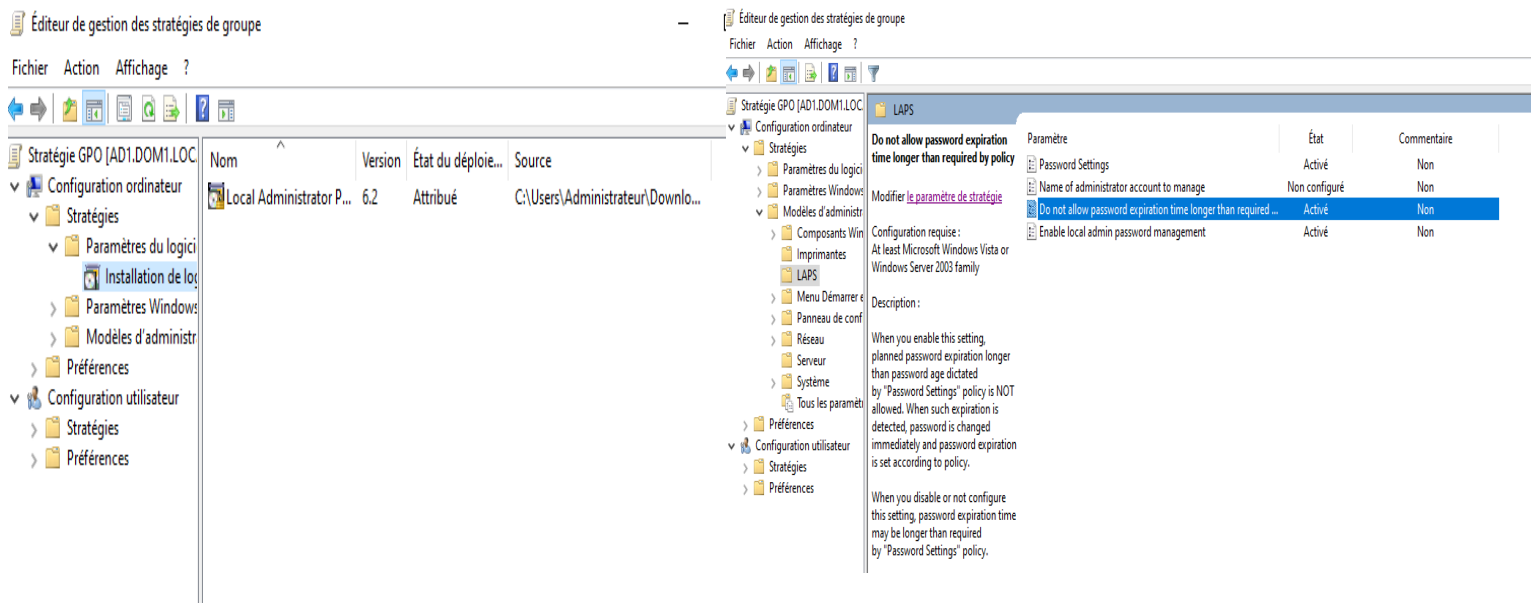


Figure: Installation de LAPS par GPO

3. La génération du mot de passe par LAPS :

- Une fois que LAPS a été installé sur l'ordinateur client, il a automatiquement généré un mot de passe local sécurisé pour le compte administrateur local de cet ordinateur.
- Ce mot de passe a été généré de manière aléatoire et stocké dans l'Active Directory, où il a pu être consulté par les administrateurs autorisés en cas de besoin.

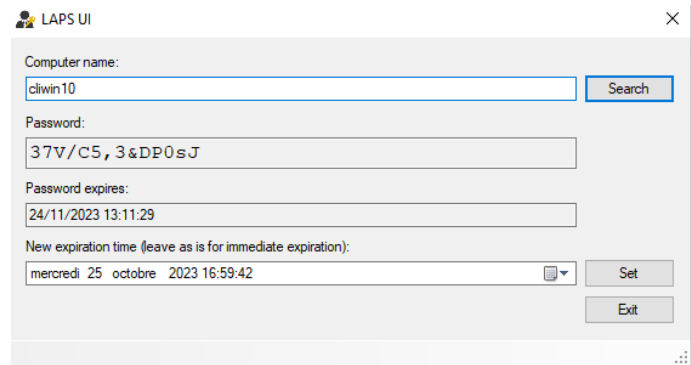
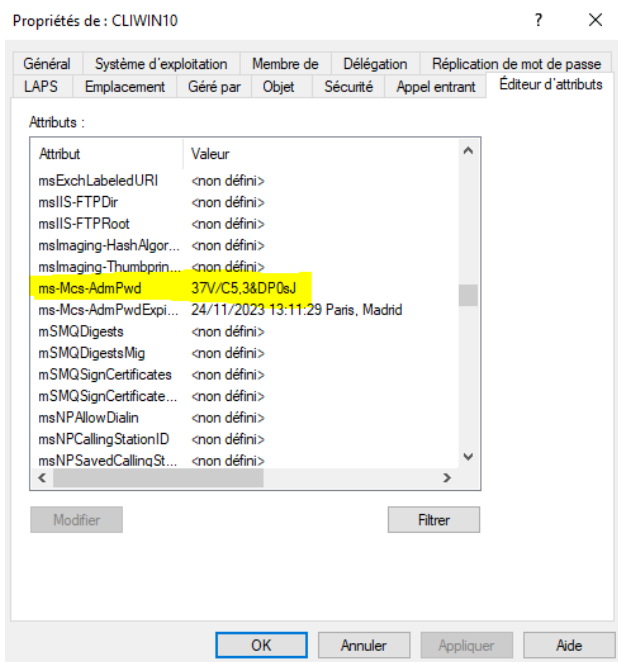


Figure:Récupération du mot de passe

8- Conclusion:

Dans le cadre de ce TP axé sur la sécurisation d'un serveur Active Directory, nous avons pris des mesures significatives pour renforcer la sécurité de notre infrastructure. Nous avons revu et optimisé le schéma de notre infrastructure, activé l'AES pour renforcer la sécurité des tickets Kerberos via une GPO, mis en place un script PowerShell pour la gestion automatisée des comptes expirés, discuté de l'emplacement approprié pour stocker nos scripts d'administration tout en mettant l'accent sur la sécurité, réalisé un audit de sécurité de l'AD et corrigé les problèmes identifiés. Enfin, nous avons installé LAPS pour gérer de manière sécurisée les mots de passe administratifs locaux. L'ensemble de ces mesures vise à protéger notre Active Directory et à renforcer la sécurité de nos données, garantissant ainsi un environnement informatique plus résistant aux menaces potentielles. La sécurisation de l'AD reste un processus continu qui nécessite vigilance et réactivité face aux évolutions constantes des menaces en matière de sécurité.

Bibliographie

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/decrypting-the-selection-of-supported-kerberos-encryption-types/ba-p/1628797>

<https://www.pingcastle.com/>

<https://www.microsoft.com/en-us/download/details.aspx?id=46899>