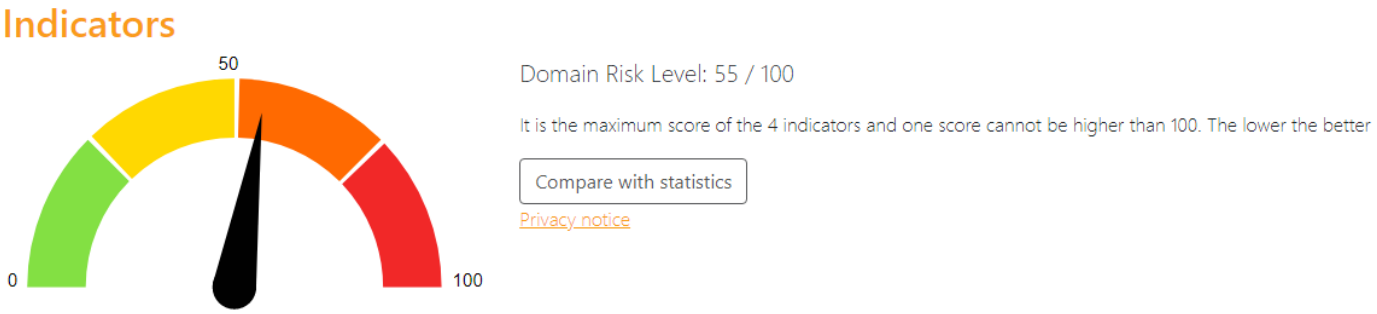
Active Directory - Security Hardening

Difficulté : Intermédiaire

Notions : Active directory, GPO, Sécurité

I. Introduction

> **Note** : Pour réaliser l'audit, c'est PingCastle qui sera utilisé. Il est téléchargeable Ici



Comme vu dans le rapport d'audit de sécurité, par défaut un Active Directory est moyennement vulnérable et certaines fonctionnalités risquent de ne pas être actives ou mal paramétrées. Il est donc bon de revoir certaines choses avant de réellement passer en production.

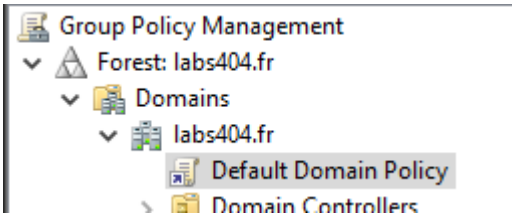
> **Astuce** : Le focus sera ici fait sur tous les points permettant de passer le score de risque à 0. Un certains nombres de points sont présents dans le rapport d'audit à titre informatif et

> peuvent également être corrigés.

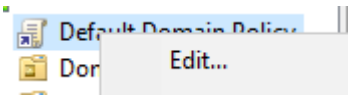
II. Modifier la stratégie de sécurité par défaut

Lancer l'éditeur de GPO :

Trouver la GPO '***Default Domain Policy***'



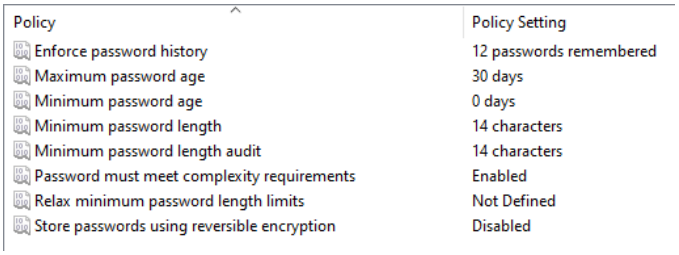
faire '***Clic droit --> Edit***'



2.1 Changer la politique des mots de passe

Dans la section '***Computer Configuration / Policies / Windows Settings / Security settings / Account Policies / Password Policy***'

- Password History : minimum 12
- Maximum password age : 30 jours
- Minimum password age : 0 jours
- Minimum password lenght : 14 caractères
- Minimum password lenght Audit : 14 caractères
- Must meet complexity requirements : Enabled

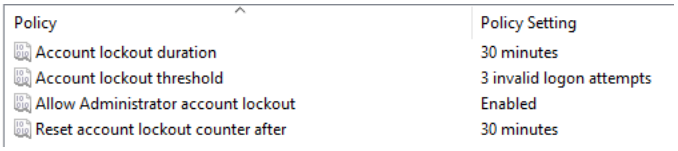


Policy	Policy Setting
Enforce password history	12 passwords remembered
Maximum password age	30 days
Minimum password age	0 days
Minimum password length	14 characters
Minimum password length audit	14 characters
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

2.2 Changer la politique de verrouillage des comptes

Dans la section '***Computer Configuration / Policies / Windows Settings / Security settings / Account Policies / Account Lockout Policy***'

- Account lockout duration : 30 minutes
- Account lockout threshold : 3 essais
- Allow Administrator Account Lockout : Enabled
- Reset Account Lockout count after : 30 minutes



Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	30 minutes

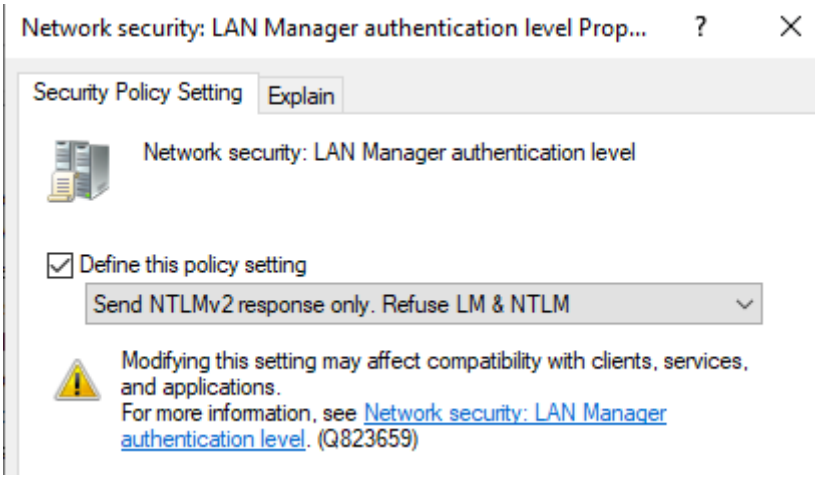
III. Corriger les 'Stale Objects'

3.1 Désactiver NTLMv1

> **Attention** : Les postes inférieurs à windows 7 ou effectuant leurs connections en NTLMv1 ne pourront plus se connecter sur le domaine.

Éditer la '***Default Domain Policy***' et modifier le paramètre suivant :

'***Settings / Security Settings / Local Policies / Security Options / Network Security: LAN Manager authentication level***'

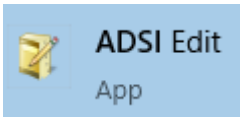


3.2 Retirer aux utilisateurs le droits d'ajouter des machines

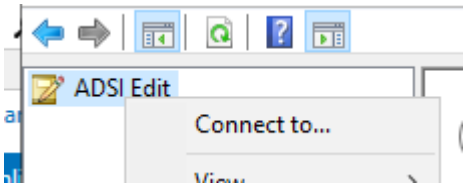
> **Note** : cela n'affectera que les comptes utilisateurs, mais les administrateurs de domaines garderons tout de même ce privilège.

En mode GUI

Ouvrir la console '***ADSI Edit***'

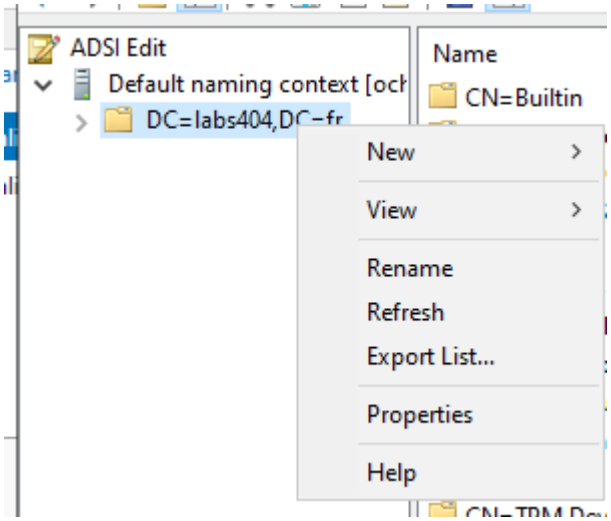


Faire un clic droit puis '***Connect To...***'

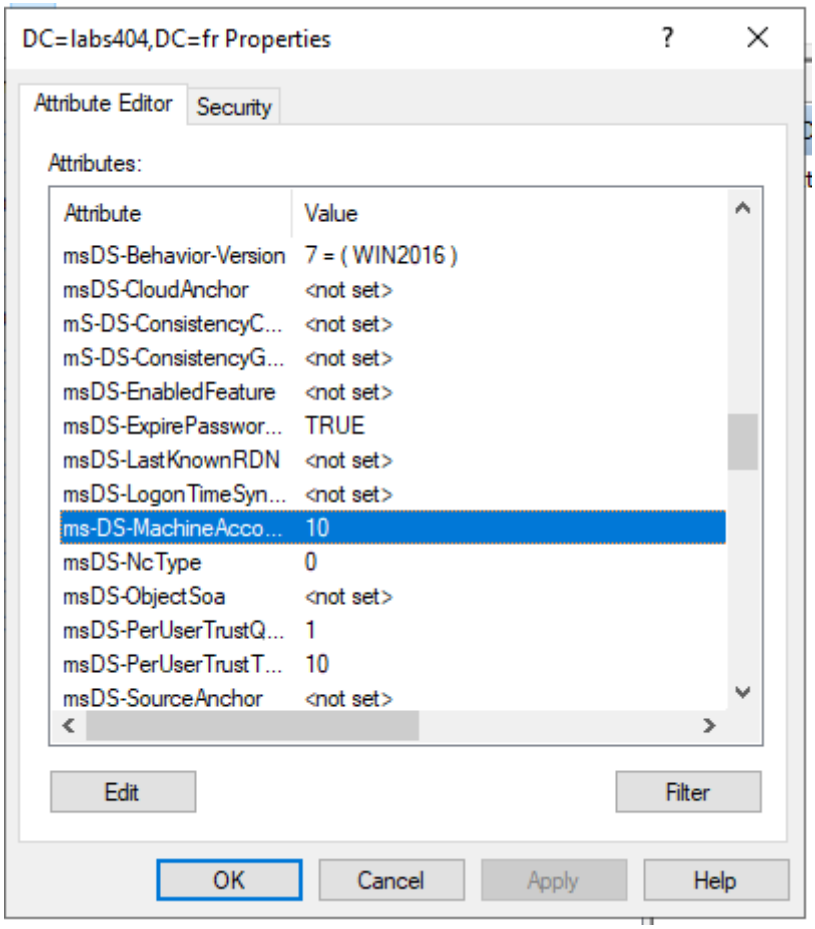


Choisir le contexte par défaut et faire '***OK***'.

Sélectionner l'objet racine du domaine, puis clic droit --> '***Properties***'



Dans l'editeur d'attributs, trouver l'attribut '***ms-DS-MachineAccountQuota***'



Fixer sa valeur à '***0***'.

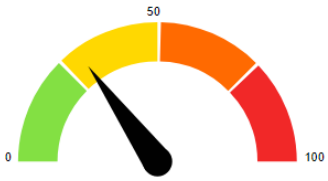
En mode console

```
Set-ADDomain -Identity "DC=<domain>,DC=<ext>" -Replace @{"ms-DS-MachineAccountQuota"="0"}
```

```
[OCH-LAB-ADDS01.labs404.fr]: PS C:\Users\Administrator\Documents> Set-ADDomain -Identity "DC=LABS404,DC=FR" -Replace @{"ms-DS-MachineAccountQuota"="0"
[OCH-LAB-ADDS01.labs404.fr]: PS C:\Users\Administrator\Documents>
```

IV. Corriger les 'Privileged Accounts'

Privileged Accounts



Privileged Accounts : 30 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [3 rules matched on a total of 45]

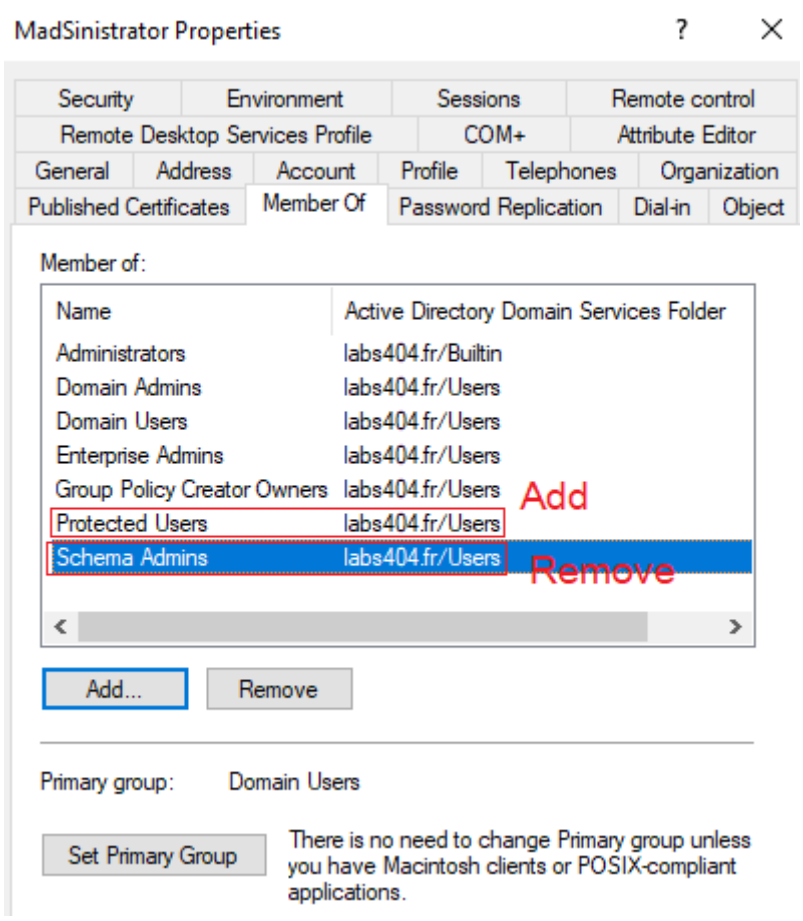
Presence of Admin accounts which do not have the flag "This account is sensitive and cannot be delegated": 1	+ 20 Point(s)
The group Schema Admins is not empty: 1 account(s)	+ 10 Point(s)

Les deux points suivants peuvent être corrigés en une fois.

- ***Ajouter*** les comptes à protéger dans le groupe Builtin '***Protected Users***'
- ***Retirer*** les comptes admins du groupe '***Shema Admins***'

> ***Attention*** : Sortir l'administrateur du domaine du group administrateur de schéma signifie qu'il faudra l'y ré-ajouter pour toute modification / mise à jour du schéma Active Directory.

En mode GUI



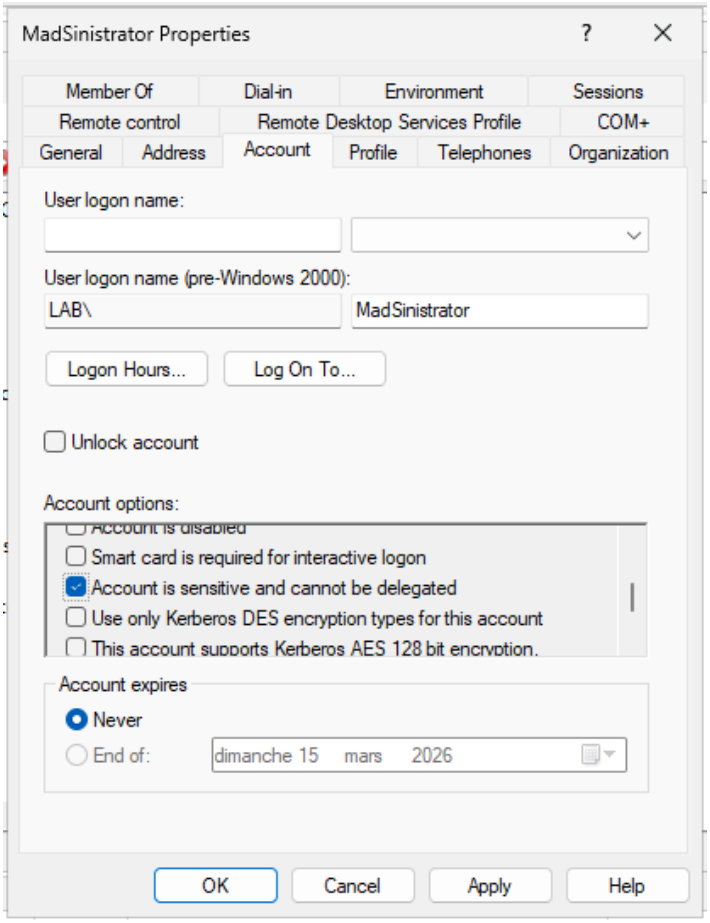
En mode console

```
Remove-ADGroupMember -Identity "Schema Admins" -Members "<Compte Admin>"
Add-ADGroupMember -Identity "Protected Users" -Members "<Compte Admin>"
```

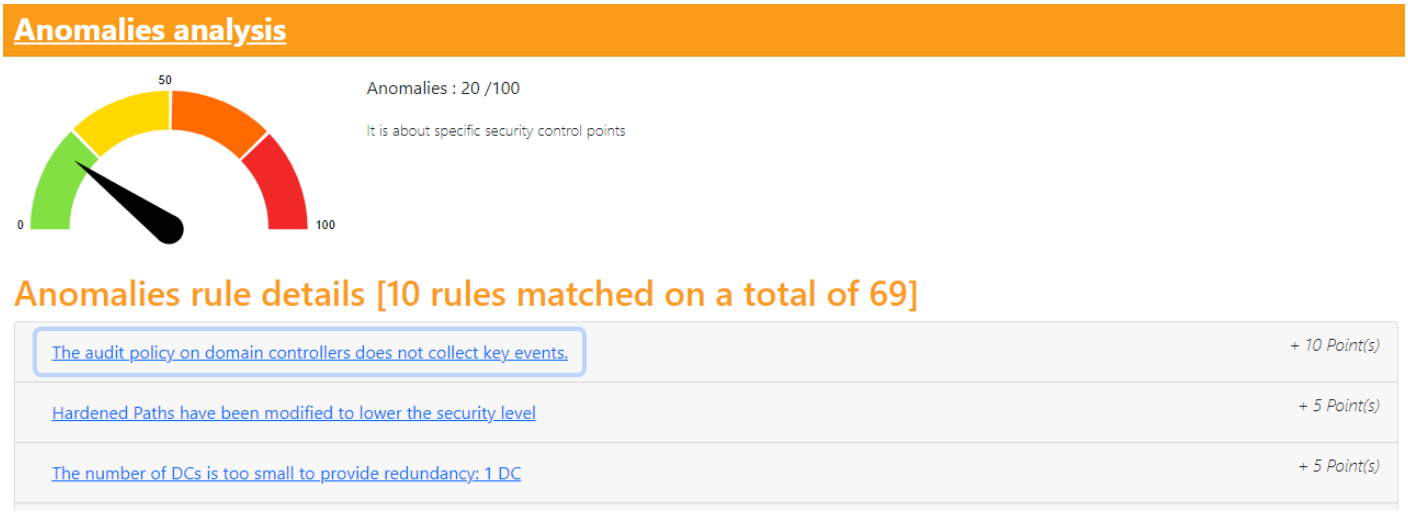
```
[OCH-LAB-ADDS01.labs404.fr]: PS C:\Users\Administrator\Documents> Remove-ADGroupMember -Identity "Schema Admins" -Members "MadSinistrator"

Confirm
Are you sure you want to perform this action?
Performing the operation "Set" on target "CN=Schema Admins,CN=Users,DC=labs404,DC=fr".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"): y
[OCH-LAB-ADDS01.labs404.fr]: PS C:\Users\Administrator\Documents> Add-ADGroupMember -Identity "Protected Users" -Members "MadSinistrator"
[OCH-LAB-ADDS01.labs404.fr]: PS C:\Users\Administrator\Documents>
```

Sur l'utilisateur Administrator, Faire un '***clic droit --> Properties***', dans l'onglet '***Account***', cocher également l'attribut : '***Account is sensitive and cannot be delegated***'.

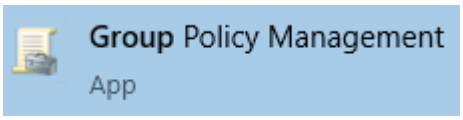


V. Corriger les derniers points

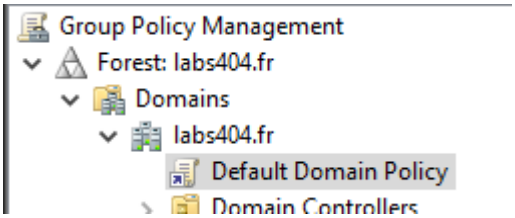


5.1 Activer les audits d'évènements

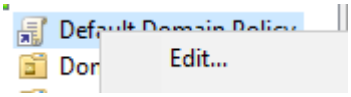
Lancer l'éditeur de GPO :



Trouver la GPO '***Default Domain Policy***'

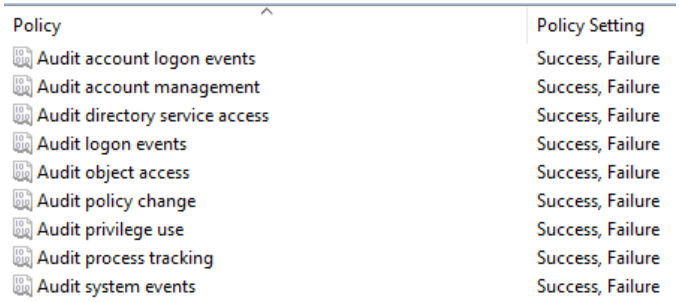


faire '***Clic droit --> Edit***'



Dans la section '***Computer Configuration / Policies / Windows Settings / Security settings / Local Policy / Audit Policy***'

Tout Passer en 'success & failure'

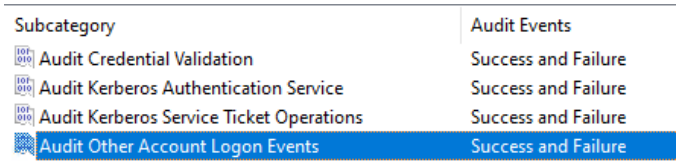


Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Dans la section '***Computer Configuration / Policies / Windows Settings / Security settings / Advanced Audit Policy Configuration / Audit Policy***'

Activer les audits de comptes '***Account Logon***':

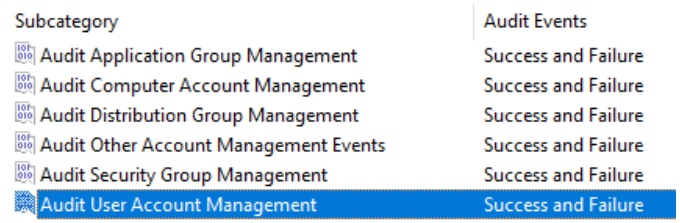
Tout Passer en 'success & failure'



Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure

Activer les audits de management des comptes '***Account Management***':

Tout Passer en 'success & failure'

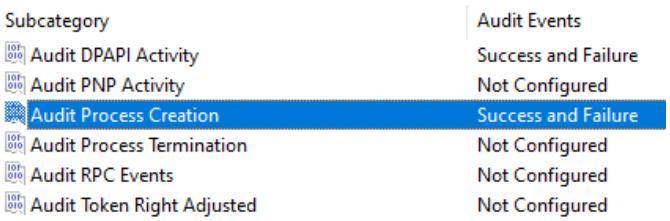


Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

Activer les audits de tracking '***Detailed Tracking***':

A minima :

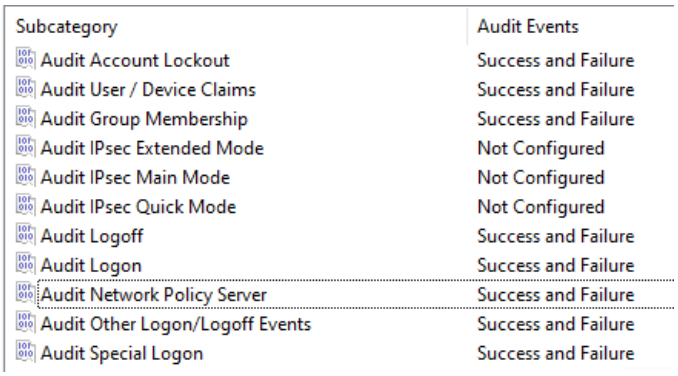
- Audit DPAPI Activity
- Audite Process Creation



Subcategory	Audit Events
Audit DPAPI Activity	Success and Failure
Audit PNP Activity	Not Configured
Audit Process Creation	Success and Failure
Audit Process Termination	Not Configured
Audit RPC Events	Not Configured
Audit Token Right Adjusted	Not Configured

Activer les audits des événements '***Logon,Logoff***':

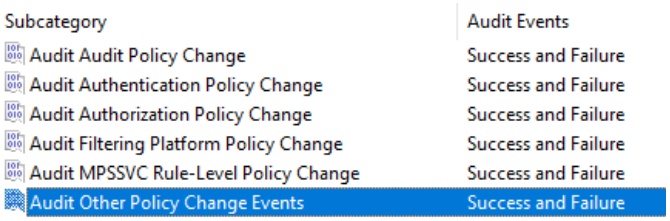
Tout Passer en 'success & failure' sauf les events IPsec



Subcategory	Audit Events
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Success and Failure
Audit Group Membership	Success and Failure
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Activer les audits de changements de politiques '***Policy change***':

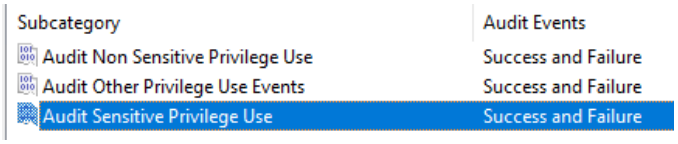
Tout Passer en 'success & failure'



Subcategory	Audit Events
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success and Failure
Audit Authorization Policy Change	Success and Failure
Audit Filtering Platform Policy Change	Success and Failure
Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure

Activer les audits d'utilisation de privilèges '***Privilege use***':

Tout Passer en 'success & failure'

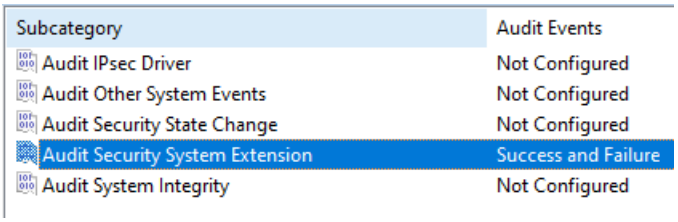


Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Success and Failure
Audit Other Privilege Use Events	Success and Failure
Audit Sensitive Privilege Use	Success and Failure

Activer les audits systèmes '***System***':

A minima :

- Audit Security System Extention

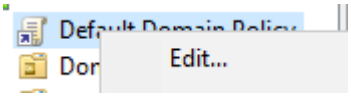


5.2 Activer le 'Path Hardening' sur le netlogon et le sysvol

Lancer l'éditeur de GPO :

Créer une GPO et la placer sur chaque OU contenant des Ordinateurs.

faire '***Clic droit --> Edit***'

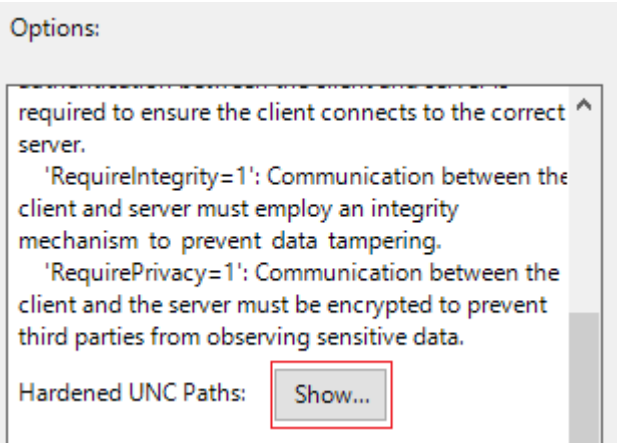


Dans la section '***Computer Configuration / Policies / Administrative Templates / Network / Network Provider***'

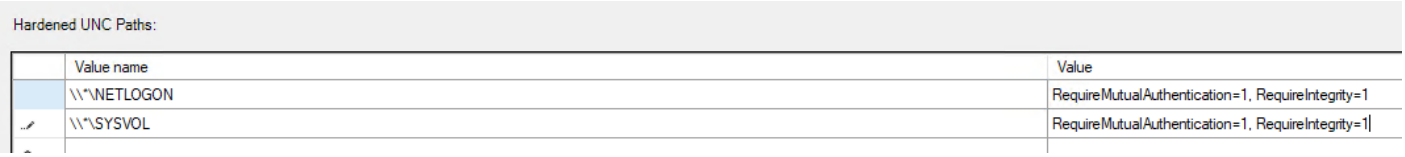
Editer l'option '***Hardened UNC Paths***'

Activer le paramétrage en cochant '***Enabled***'

Puis cliquer sur '***Show***'



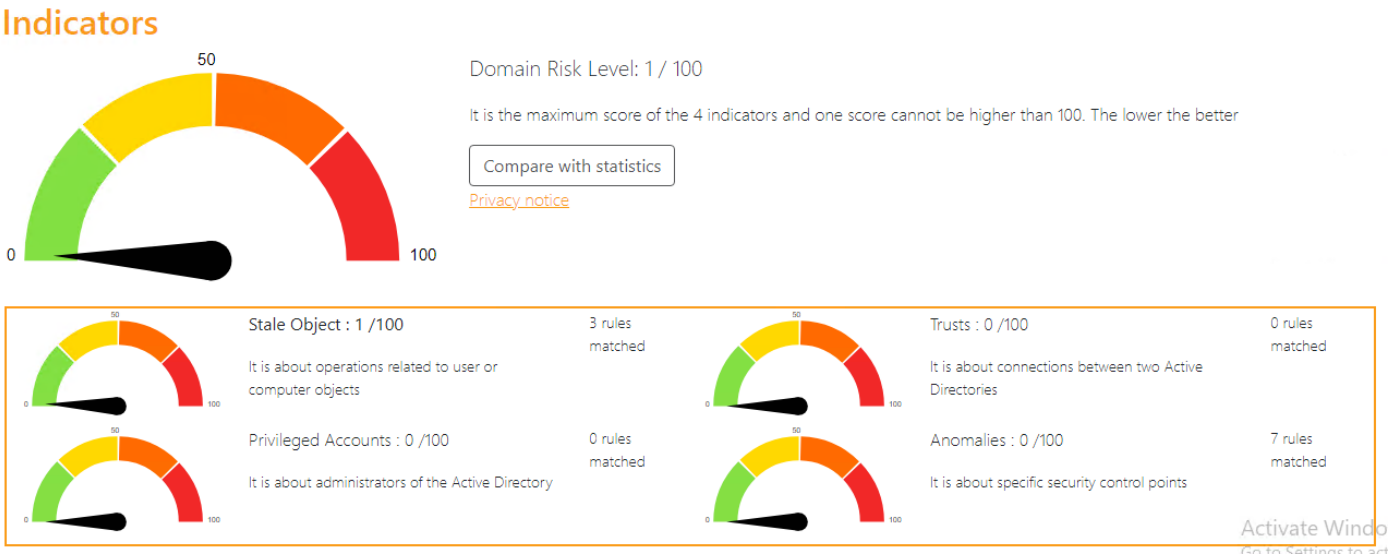
Ajouter les valeurs suivantes



5.4.3 Ajouter une redondance de contrôleur de domaine.

> **Note** : Voir la page Active directory - Ajout d'un DC

VI. Conclusion



Le point restant est dû à un compte dont le mot de passe n'expire pas. Celui-ci sera révisé pour être éliminé et remplacé par un compte GMSA.

Il peut toujours être utile de correiger les eventuels points soulevés ultérieurement par l'audit, même si ceux-ci ne coûtent pas de points.

Revision #2
Created 2026-07-30 08:30:09 UTC by Olivier
Updated 2026-07-30 08:39:56 UTC by Olivier