

Active Directory - Security Hardening



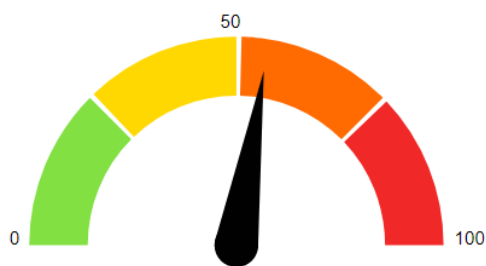
Difficulté : Intermédiaire

Notions : Active directory, GPO, Sécurité

I. Introduction

Note : Pour réaliser l'audit, c'est PingCastle qui sera utilisé. Il est téléchargeable [Ici](#)

Indicators



Domain Risk Level: 55 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)

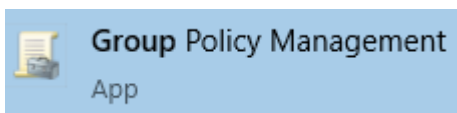
Comme vu dans le rapport d'audit de sécurité, par défaut un Active Directory est moyennement vulnérable et certaines fonctionnalités risquent de ne pas être actives ou mal paramétrées. Il est donc bon de revoir certaines choses avant de réellement passer en production.

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

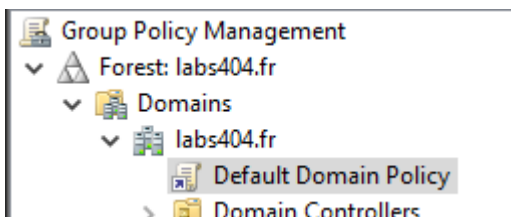
peuvent également être corrigés.

II. Modifier la stratégie de sécurité par défaut

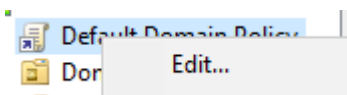
Lancer l'éditeur de GPO :



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 length : 14 caractères
- Minimum password length 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

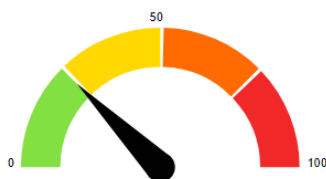
Dans la section '**Computer Configuration / Policies / Windows Settings / Security settings / Account Policies / Account Lockout Policy**'

- 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'

Stale Objects



Stale Objects : 25 /100

It is about operations related to user or computer objects

Stale Objects rule details [4 rules matched on a total of 50]

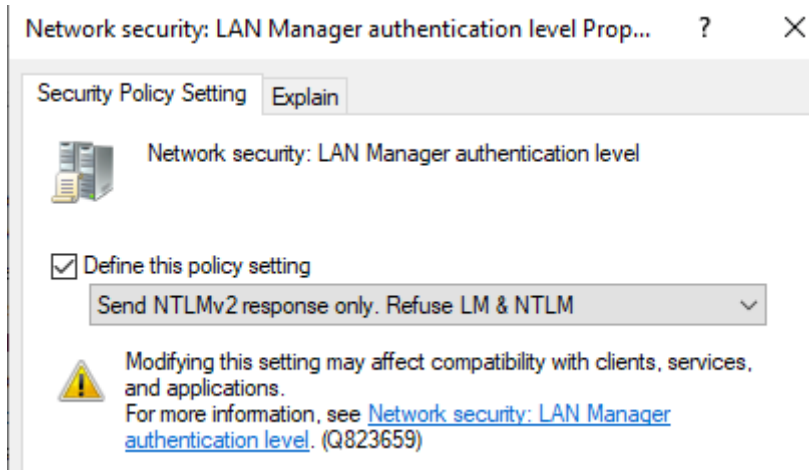
The LAN Manager Authentication Level allows the use of NTLMv1 or LM.	+ 15 Point(s)
Non-admin users can add up to 10 computer(s) to a domain	+ 10 Point(s)

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'

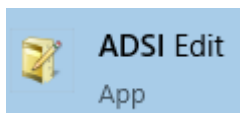


3.2 Retirer aux utilisateurs le droits d'ajouter des machines

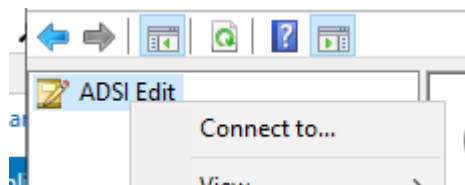
Note : cela n'affectera que les comptes utilisateurs, mais les administrateurs de domaines garderons tout de même ce privilège.

En mode GUI

Ouvrir la console '**ADSI Edit**'

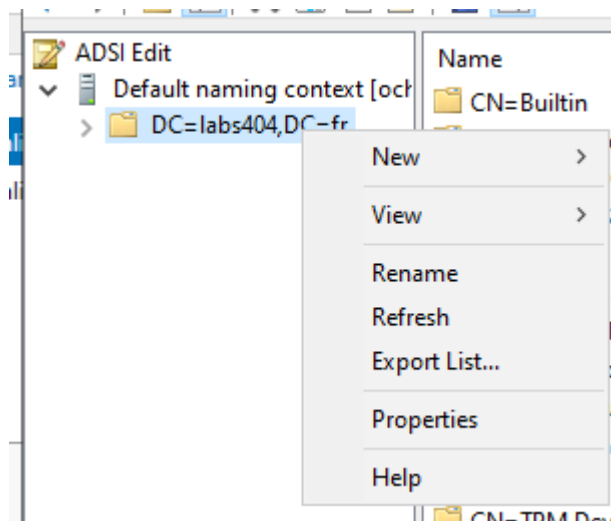


Faire un clic droit puis '**Connect To...**'

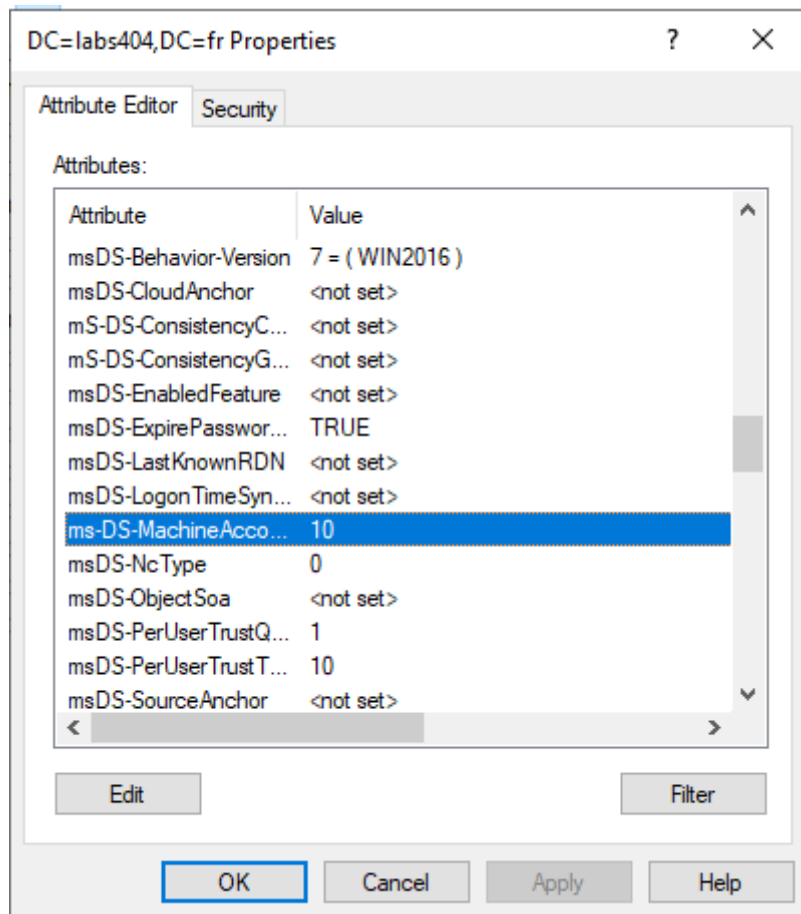


Choisir le contexte par défaut et faire '**OK**'.

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'.

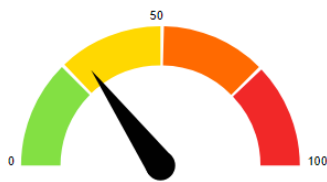
En mode console

```
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 '**Schema 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

MadSistrator Properties

? X

Security	Environment	Sessions	Remote control
Remote Desktop Services Profile	COM+	Attribute Editor	
General	Address	Account	Profile
Published Certificates	Member Of	Password Replication	Dial-in
		Object	

Member of:

Name	Active Directory Domain Services Folder
Administrators	labs404.fr/Builtin
Domain Admins	labs404.fr/Users
Domain Users	labs404.fr/Users
Enterprise Admins	labs404.fr/Users
Group Policy Creator Owners	labs404.fr/Users
Protected Users	labs404.fr/Users
Schema Admins	labs404.fr/Users

Add

Remove

Add...

Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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 '**clik droit --> Properties**', dans l'onglet '**Account**', cocher également l'attribut : '**Account is sensitive and cannot be delegated**'.

The screenshot shows the 'MadSinistrator Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'LAB\'. The 'User logon name (pre-Windows 2000)' is 'MadSinistrator'. The 'Logon Hours...' and 'Log On To...' buttons are visible. Under 'Account options', the checkbox 'Account is sensitive and cannot be delegated' is checked. The 'Account expires' section shows 'Never' selected.

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	

General Address Account Profile Telephones Organization

User logon name: [LAB\] [v]

User logon name (pre-Windows 2000): [LAB\] [MadSinistrator]

[Logon Hours...] [Log On To...]

☐ Unlock account

Account options:

- ☐ Account is disabled
- ☐ Smart card is required for interactive logon
- ☒ Account is sensitive and cannot be delegated
- ☐ Use only Kerberos DES encryption types for this account
- ☐ This account supports Kerberos AES 128 bit encryption.

Account expires

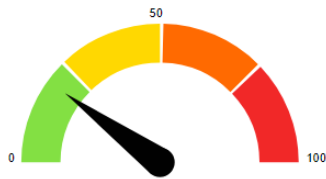
☒ Never

☐ End of: [dimanche 15 mars 2026] [calendar icon]

[OK] [Cancel] [Apply] [Help]

V. Corriger les derniers points

Anomalies analysis



Anomalies : 20 /100

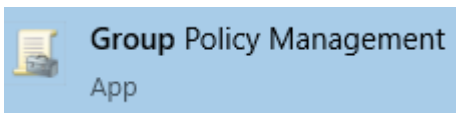
It is about specific security control points

Anomalies rule details [10 rules matched on a total of 69]

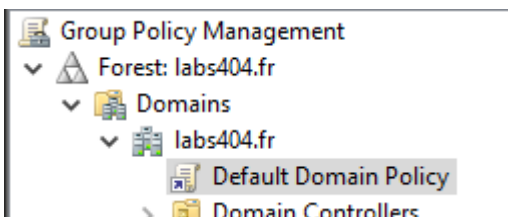
The audit policy on domain controllers does not collect key events.	+ 10 Point(s)
Hardened Paths have been modified to lower the security level	+ 5 Point(s)
The number of DCs is too small to provide redundancy: 1 DC	+ 5 Point(s)

5.1 Activer les audits d'évènements

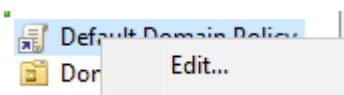
Lancer l'éditeur de GPO :



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**' :

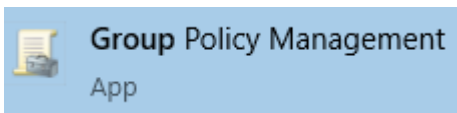
A minima :

- Audit Security System Extension

Subcategory	Audit Events
 Audit IPsec Driver	Not Configured
 Audit Other System Events	Not Configured
 Audit Security State Change	Not Configured
 Audit Security System Extension	Success and Failure
 Audit System Integrity	Not Configured

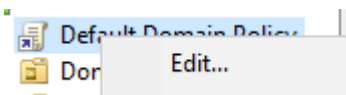
5.2 Activer le 'Path Hardening' sur le netlogon et le sysvol

Lancer l'éditeur de GPO :



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

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



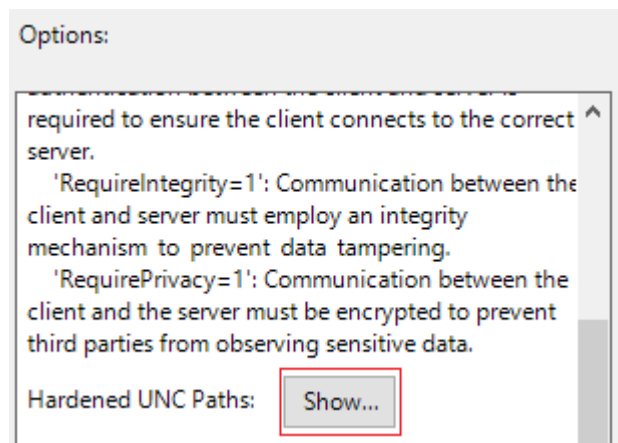
Dans la section '**Computer Configuration / Policies / Administrative Templates / Network / Network Provider**'

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

Setting	State	Comment
 Hardened UNC Paths	Not configured	No

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

Puis cliquer sur '**Show**'



Ajouter les valeurs suivantes

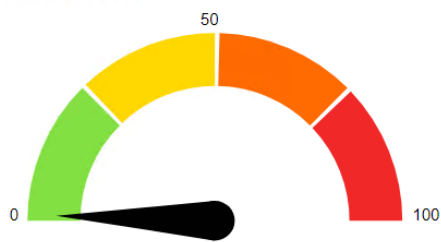
Hardened UNC Paths:		
	Value name	Value
	*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1
	*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1

5.4.3 Ajouter une redondance de contrôleur de domaine.

Note : Voir la page [Active directory - Ajout d'un DC](#)

VI. Conclusion

Indicators

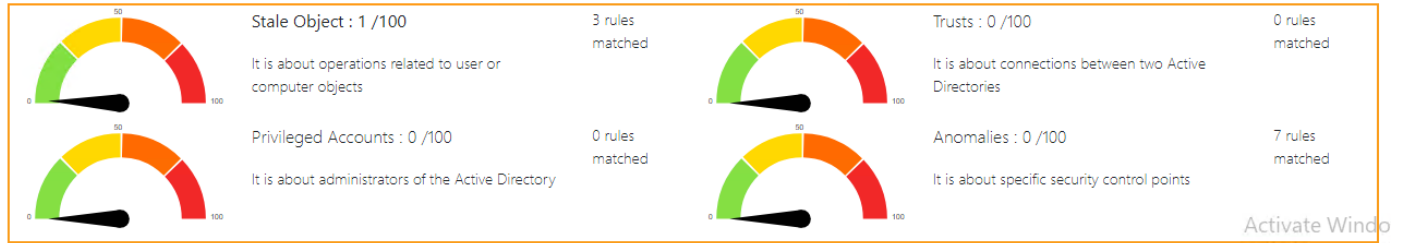


Domain Risk Level: 1 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)



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 corriger 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