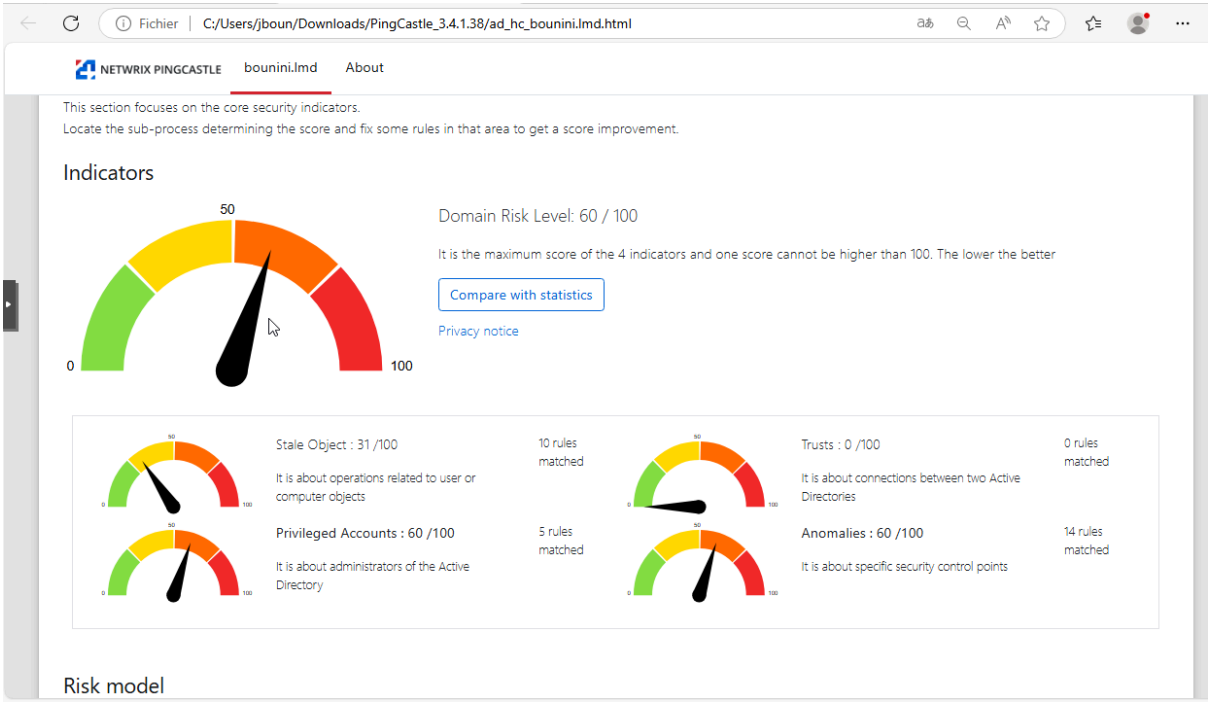
AP : PingCastle

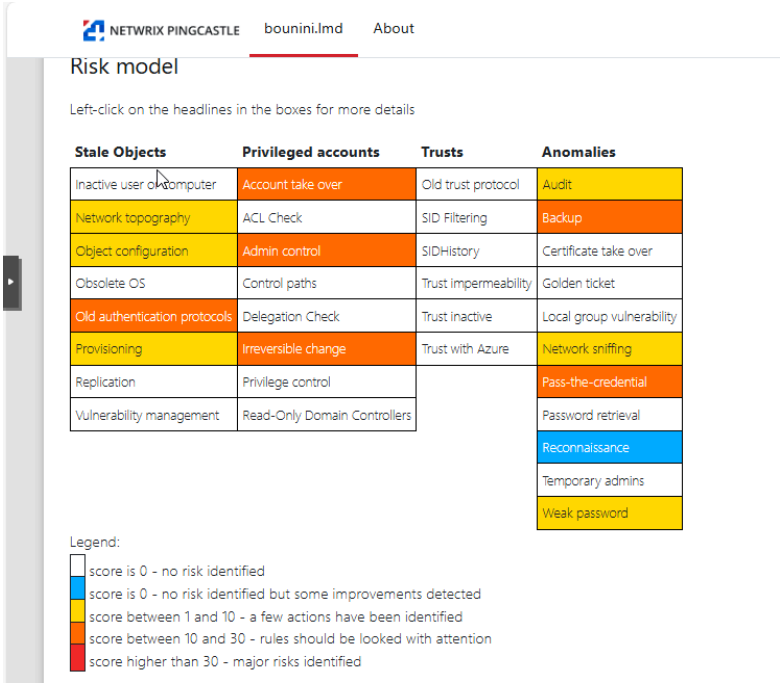
Une capture d'écran du résumé de l'audit en début de séance :



On peut constater que le score est de 60/100.

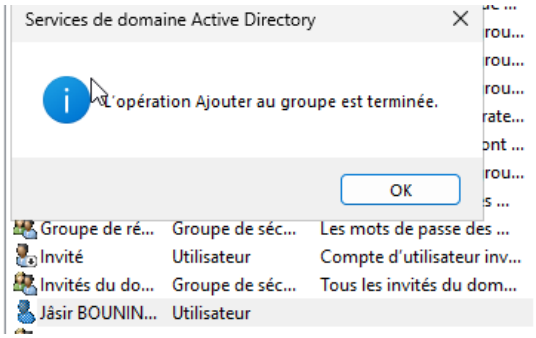
Des explications sur quelques failles qui vous paraissent majeures et/ou abordables :

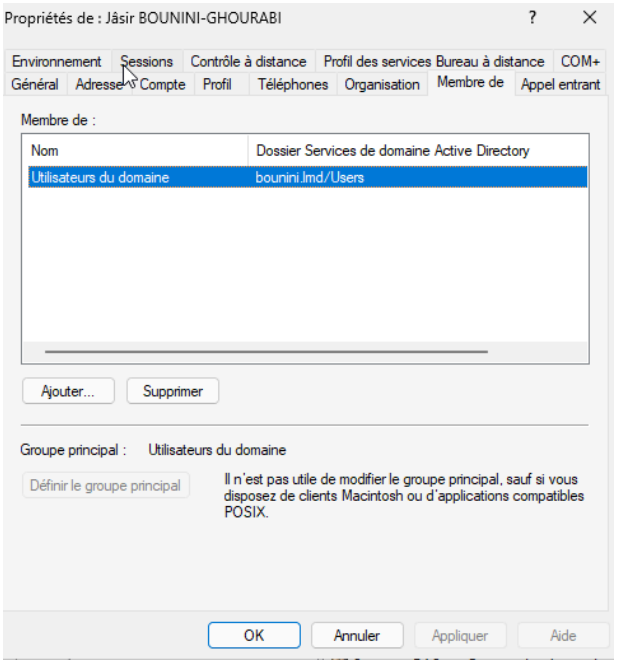
- On voit plus en détail les difference failles :

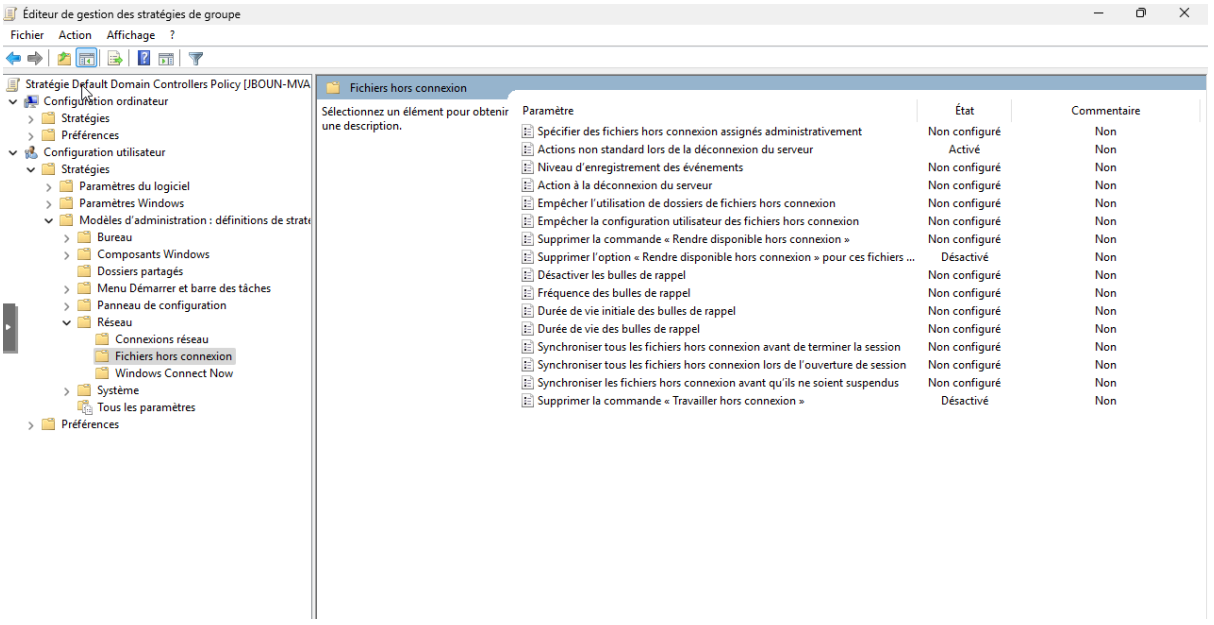


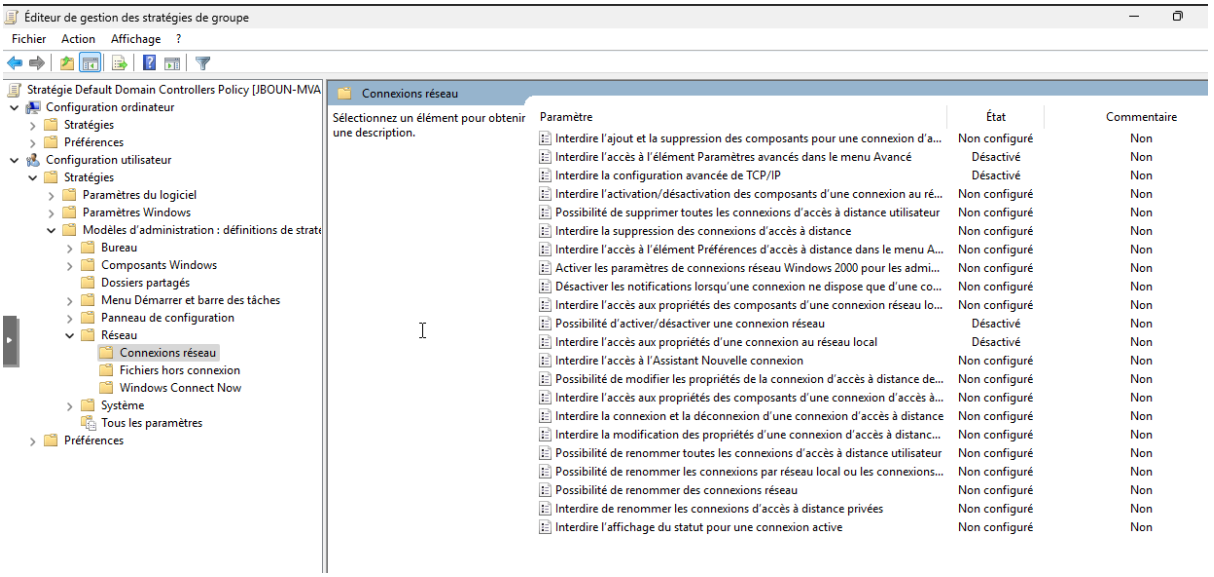
Je vais alors les règles pour faire baissé le score:

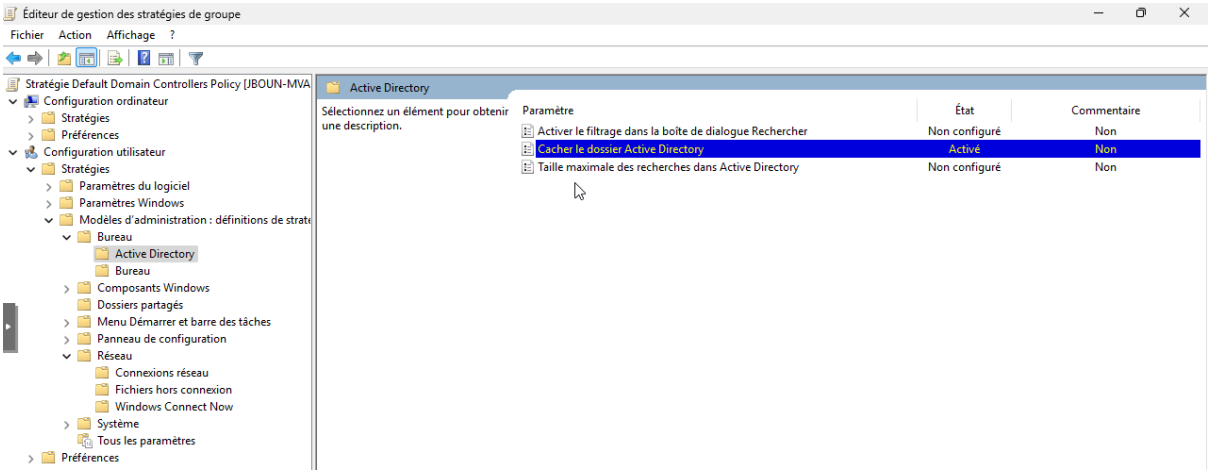
1. **Affecter utilisateur à un groupe et reduire ces droits.**











Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

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

Stale Object : 41 /100

It is about operations related to user or computer objects

11 rules matched

Privileged Accounts : 40 /100

It is about administrators of the Active Directory

4 rules matched

Trusts : 0 /100

It is about connections between two Active Directories

0 rules matched

Anomalies : 55 /100

It is about specific security control points

13 rules matched

Ajout du groupe "Protected Users”

Le groupe de sécurité "Protected Users" (introduit avec Windows Server 2012 R2) est une mesure de sécurité essentielle pour protéger les comptes sensibles (administrateurs, services privilégiés).

Son mécanisme vise à contrer les attaques Pass-the-Hash (PtH) en renforçant l'authentification et en réduisant la durée de vie des identifiants.

Principales protections activées :

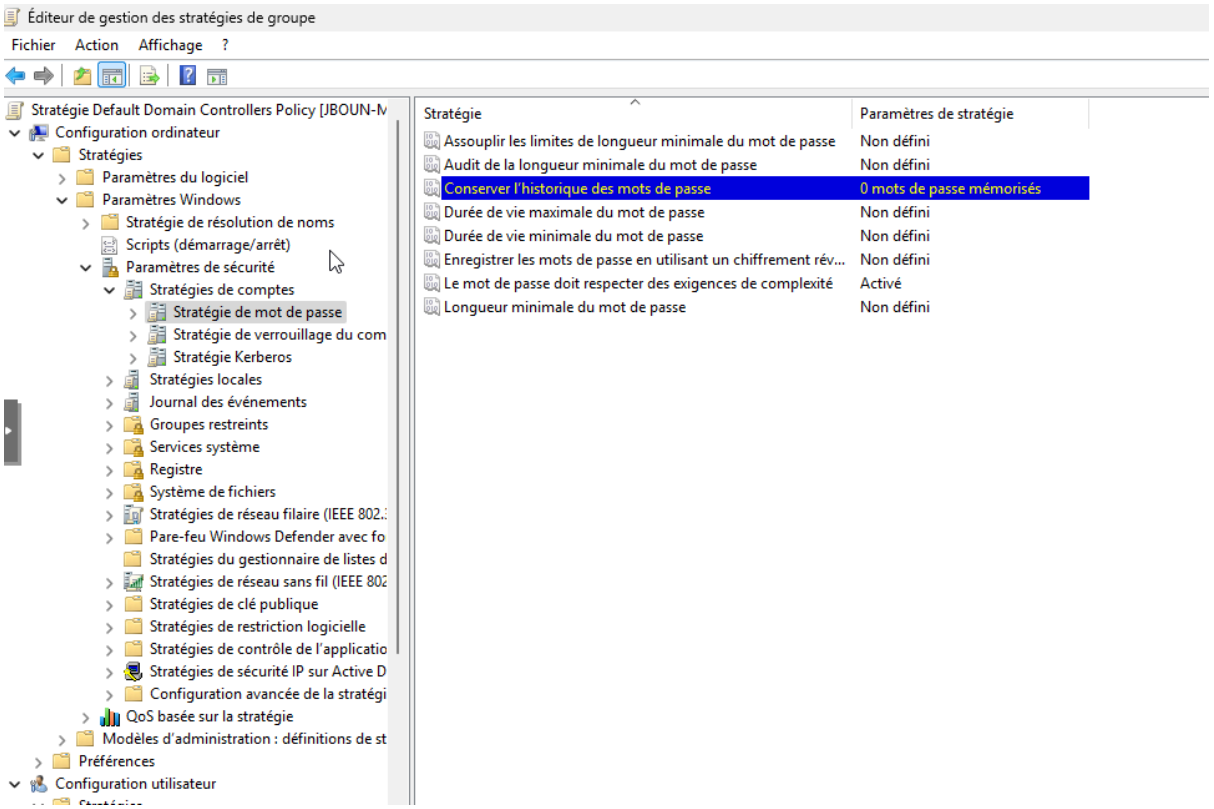
Interdiction du stockage d'identifiants délégables (Délégation non contrainte).

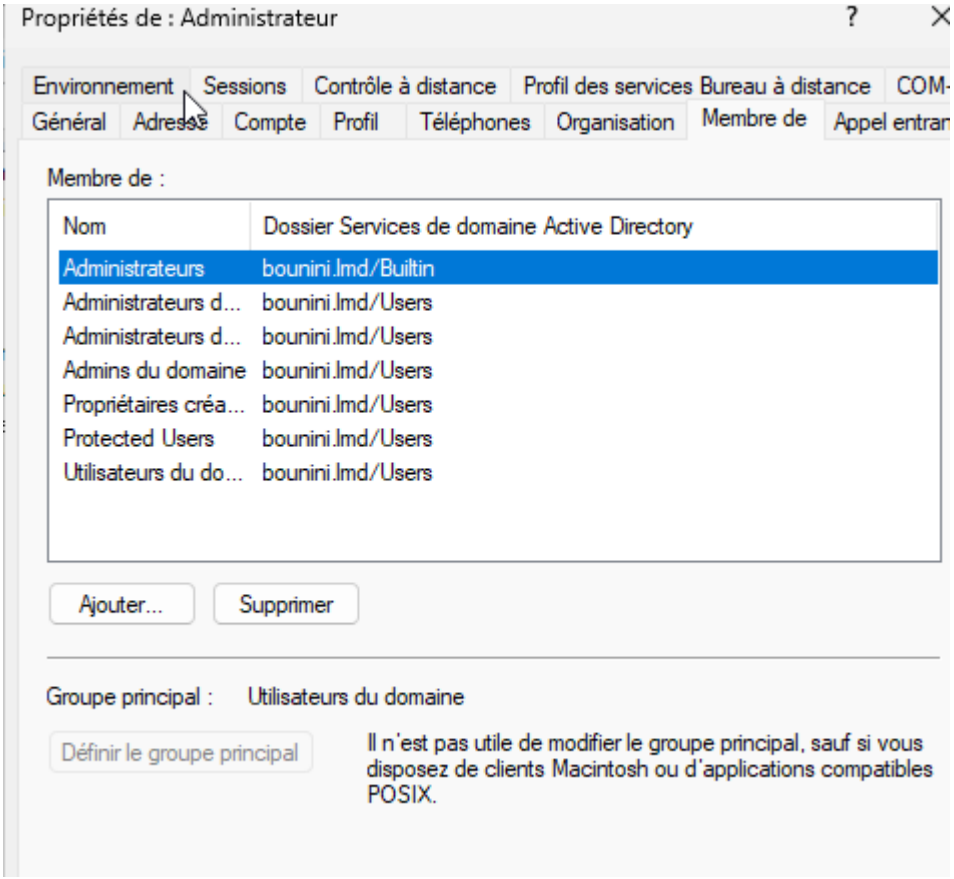
Désactivation des algorithmes faibles (DES, NTLM) au profit d'algorithmes forts comme AES.

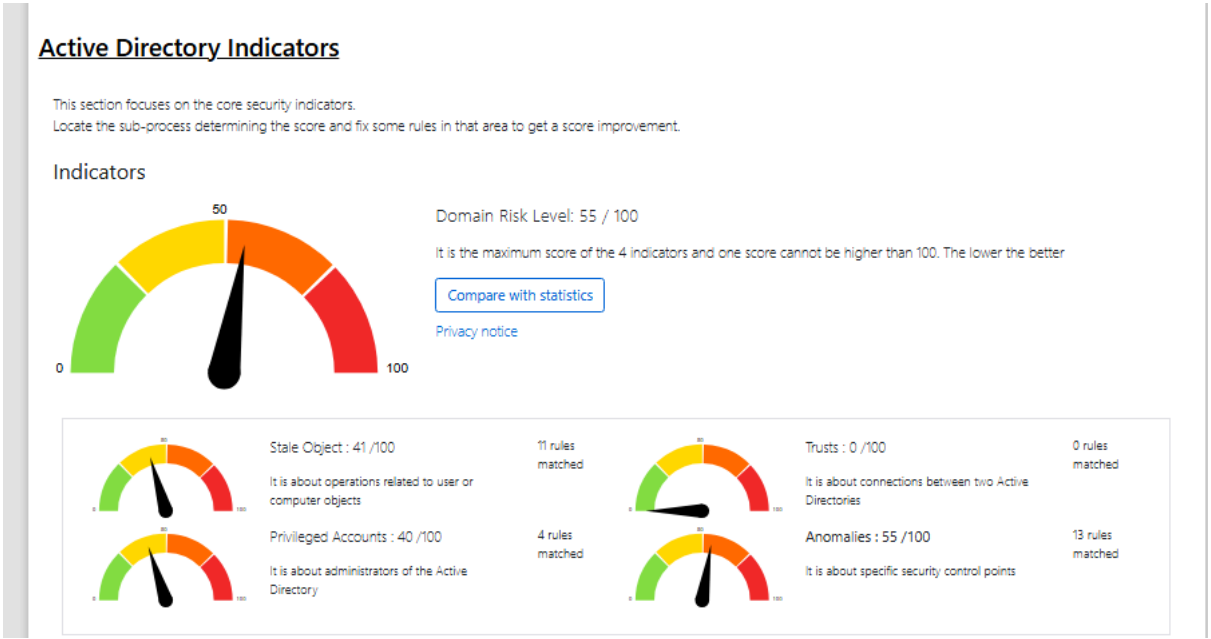
Interdiction du stockage de clés de session de longue durée, forçant une nouvelle authentification.

Restriction de l'utilisation des identifiants mis en cache.

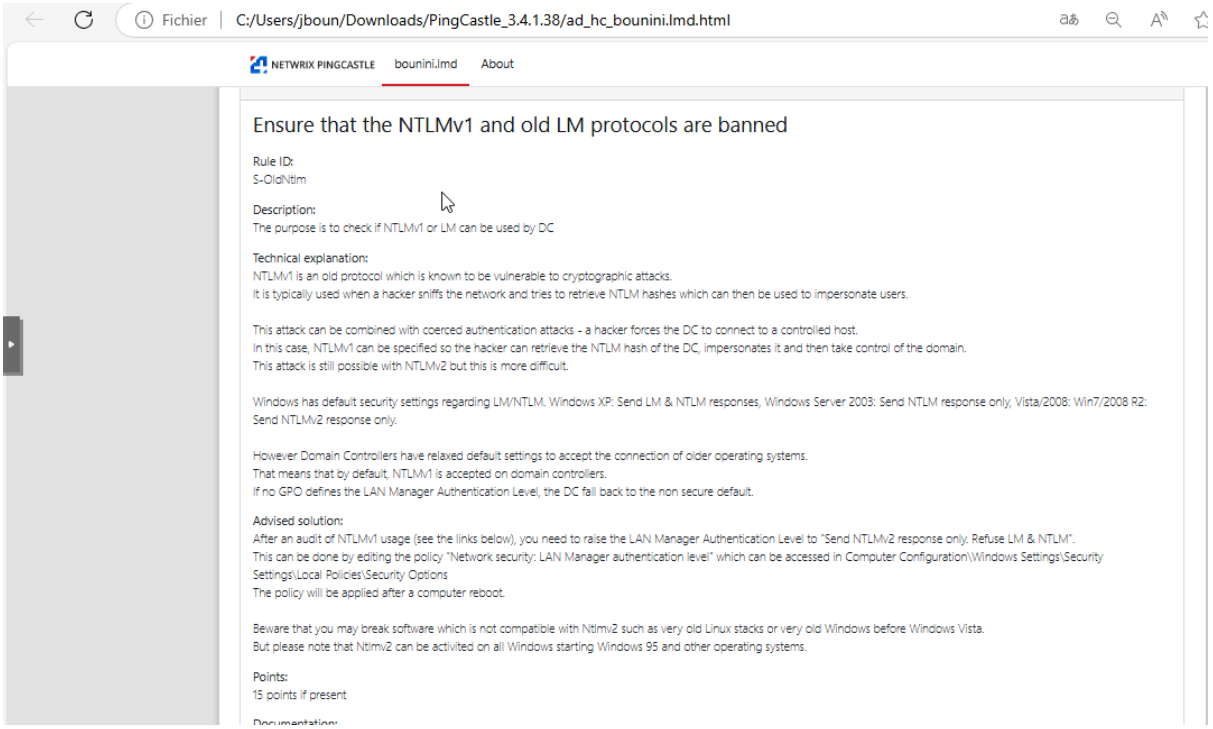
Mise en œuvre : L'ajout de comptes à ce groupe doit cibler les comptes à droits élevés, principaux vecteurs de mouvement latéral. Ces protections nécessitent un **niveau fonctionnel adéquat** de l'environnement Active Directory.



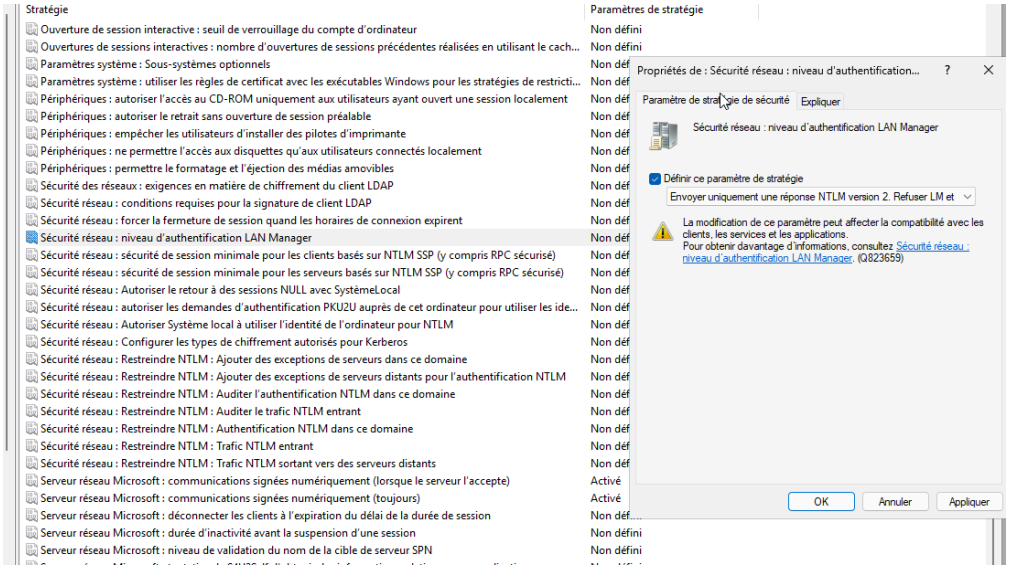

Propriétés de : Administrateur
Environnement
Sessions
Contrôle à distance
Profil des services Bureau à distance
COM-
Général
Adresse
Compte
Profil
Téléphones
Organisation
Membre de
Appel entran
Membre de :
Nom
Dossier Services de domaine Active Directory
Administrateurs
bounini.lmd/Builtin
Administrateurs d...
bounini.lmd/Users
Administrateurs d...
bounini.lmd/Users
Admins du domaine
bounini.lmd/Users
Propriétaires créa...
bounini.lmd/Users
Protected Users
bounini.lmd/Users
Utilisateurs du do...
bounini.lmd/Users
Ajouter...
Supprimer
Groupe principal :
Utilisateurs du domaine
Définir le groupe principal
Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

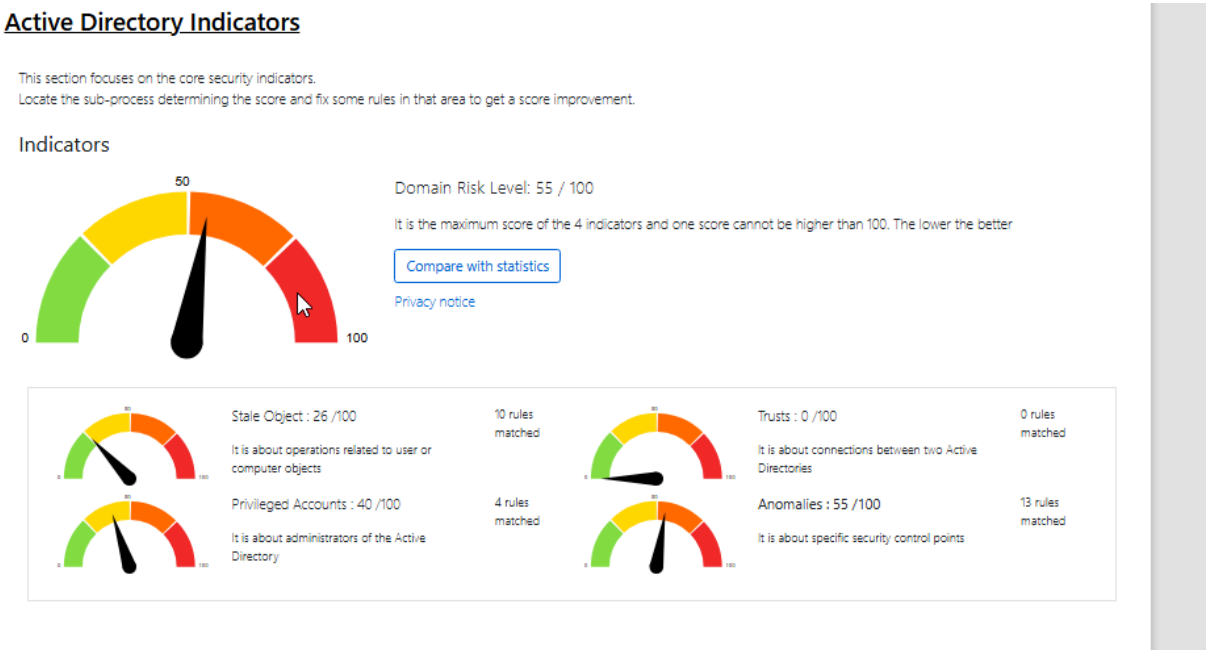

Active Directory Indicators
This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.
Indicators
50
0
100
Domain Risk Level: 55 / 100
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better
Compare with statistics
Privacy notice
Stale Object : 41 /100
It is about operations related to user or computer objects
11 rules matched
Privileged Accounts : 40 /100
It is about administrators of the Active Directory
4 rules matched
Trusts : 0 /100
It is about connections between two Active Directories
0 rules matched
Anomalies : 55 /100
It is about specific security control points
13 rules matched

Sécurisation des flux d'authentification (Désactivation NTLMv1/LM)



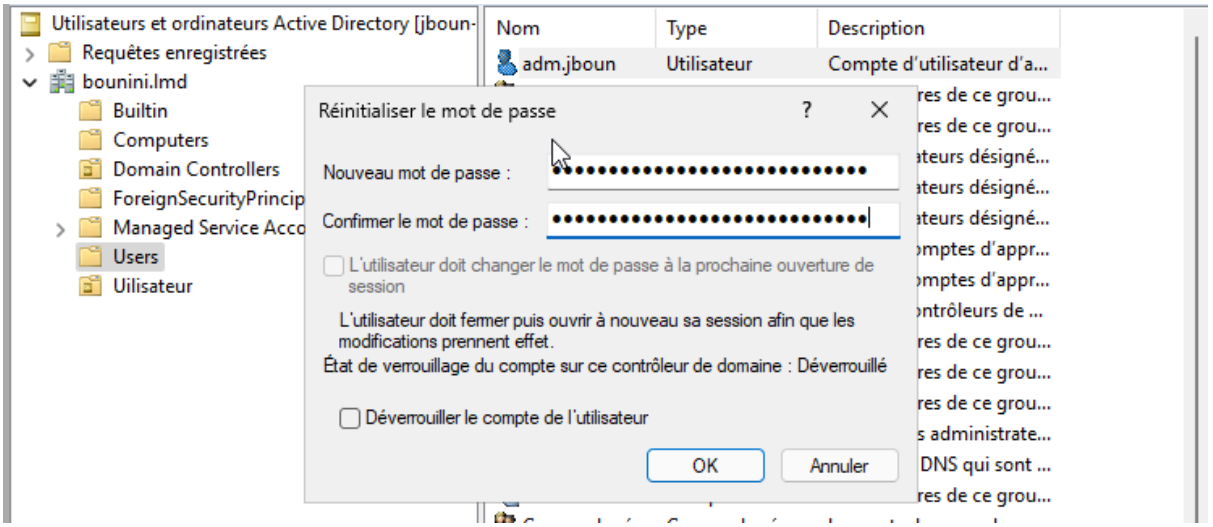
Dans la strategie :Default Domain Controllers Policy

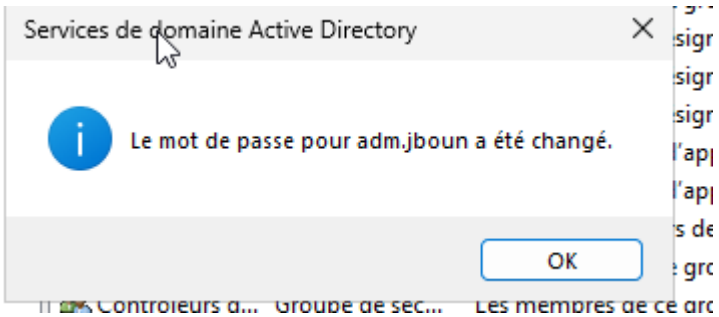


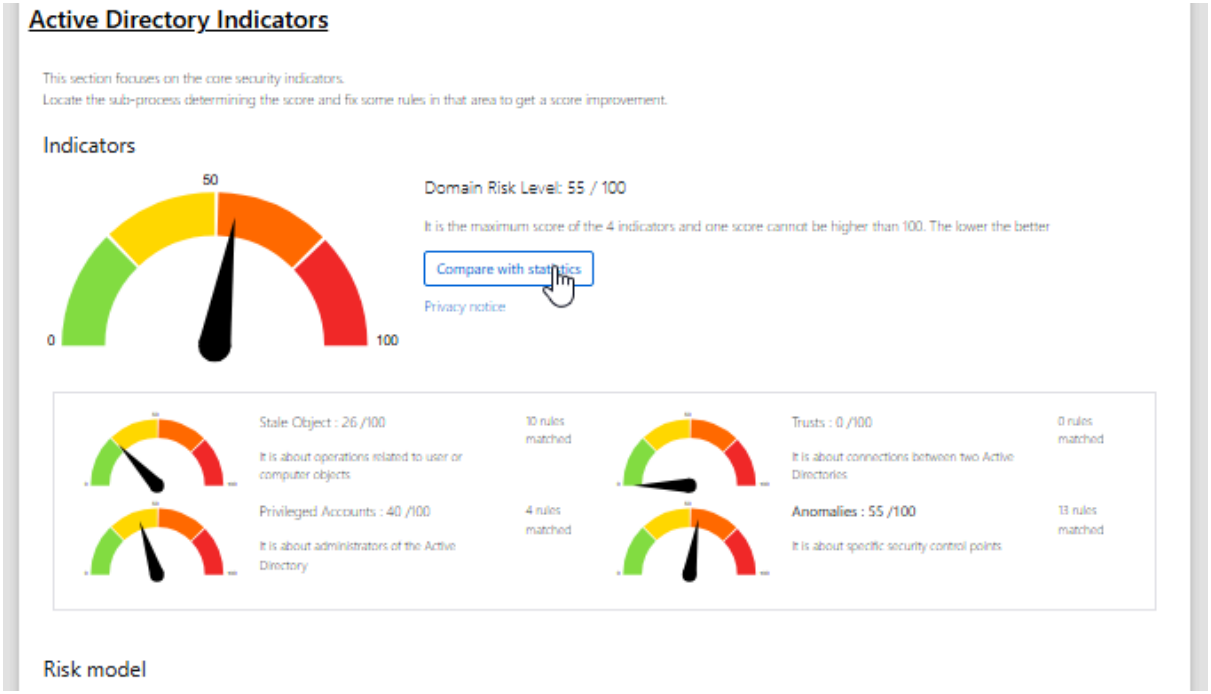


Correction de la vulnérabilité PingCastle `P-AdminLogin`

changement du mdp administrateur et aussi du nom remplacer par adm.jboun avec le mdp : JesuisenSISRmartiniere2025@.

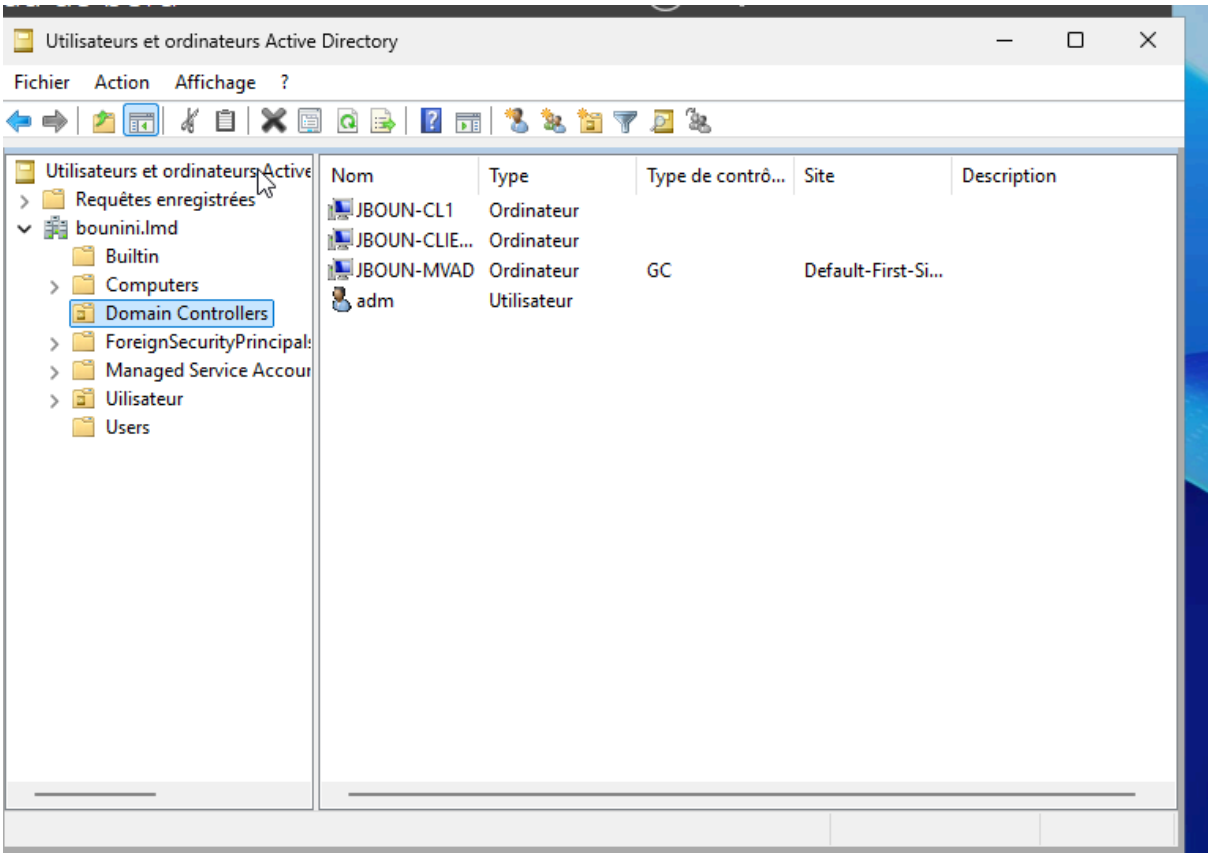


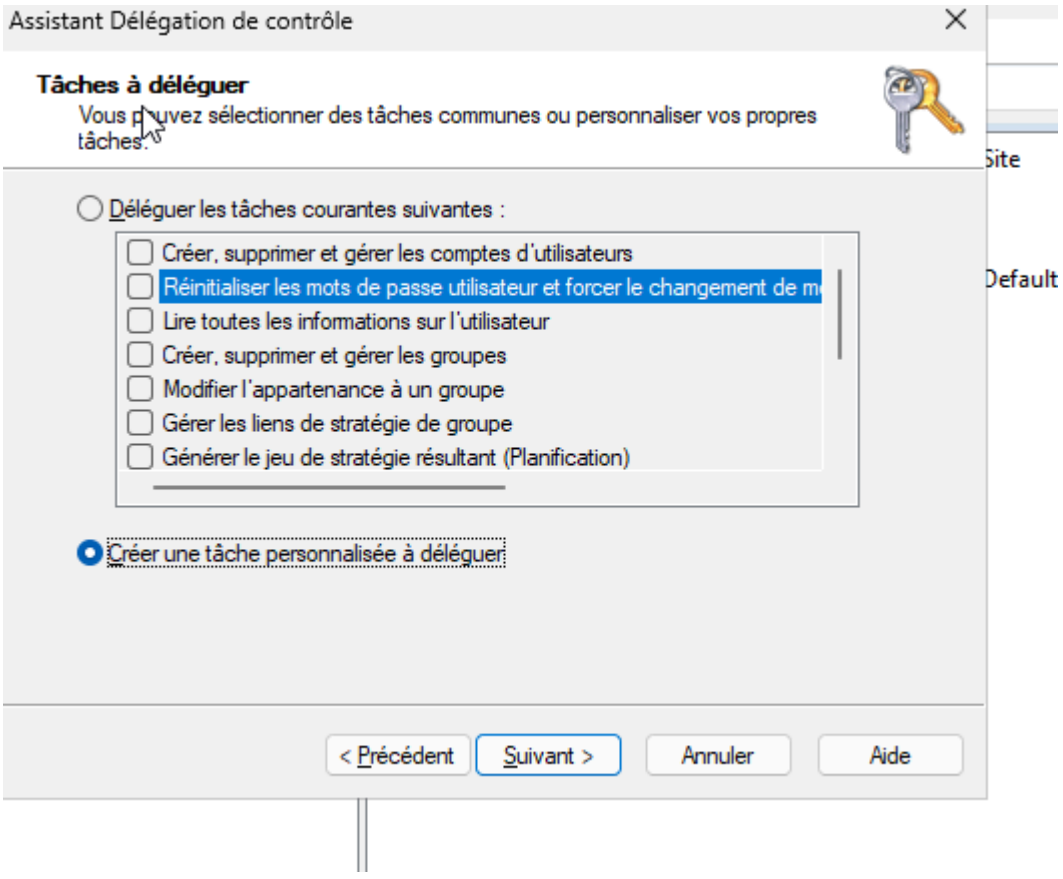




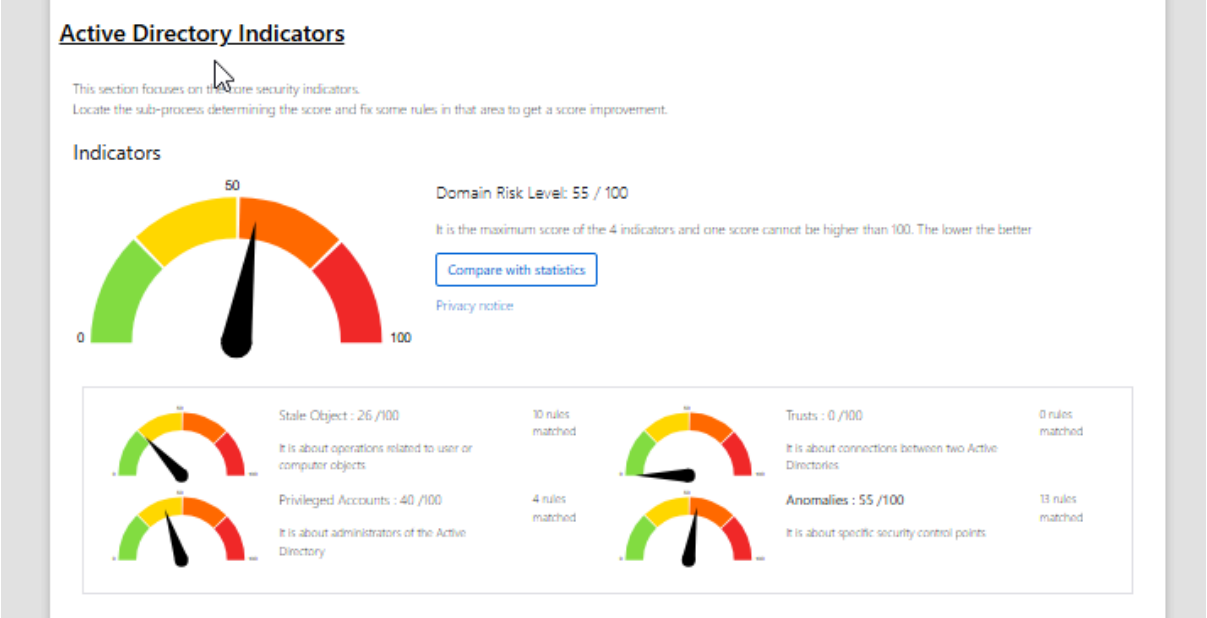
Cela n'a rien changé.

je continue :

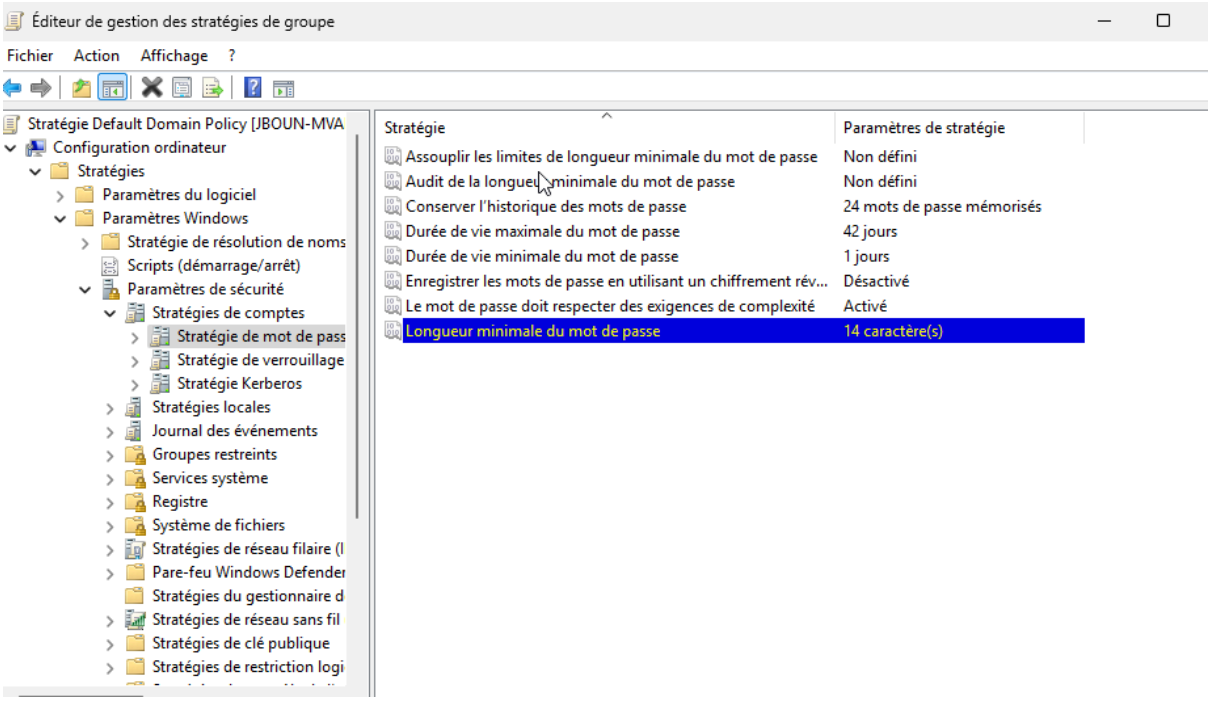

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
bounini.lmd
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Uilisateur
Users
Nom Type Type de contrô... Site Description
JBOUN-CL1 Ordinateur
JBOUN-CLIE... Ordinateur
JBOUN-MVAD Ordinateur GC Default-First-Si...
adm Utilisateur

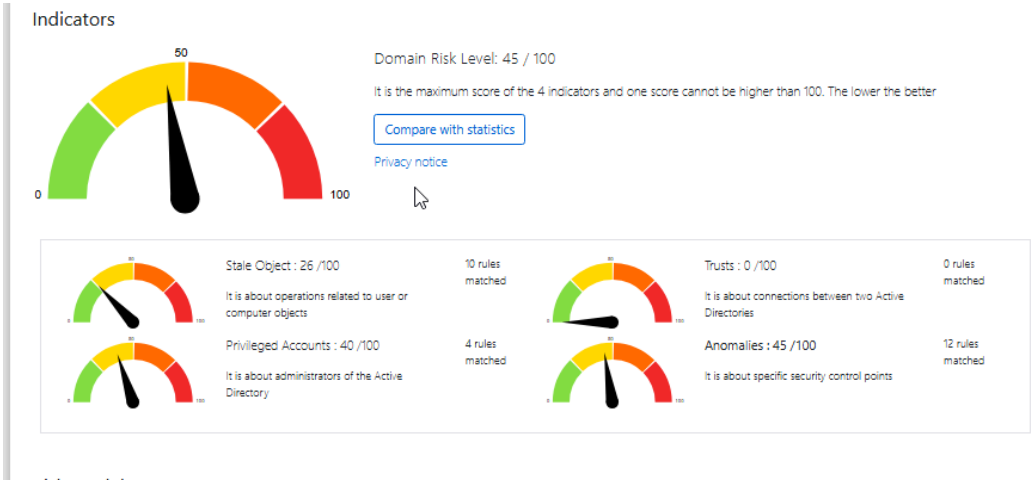

Assistant Délégation de contrôle
Tâches à déléguer
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.
Déléguer les tâches courantes suivantes :
Créer, supprimer et gérer les comptes d'utilisateurs
Réinitialiser les mots de passe utilisateur et forcer le changement de m
Lire toutes les informations sur l'utilisateur
Créer, supprimer et gérer les groupes
Modifier l'appartenance à un groupe
Gérer les liens de stratégie de groupe
Générer le jeu de stratégie résultant (Planification)
Créer une tâche personnalisée à déléguer
< Précédent
Suivant >
Annuler
Aide

→ j'ai fait en sorte de donner à un seul admin de pouvoir sauver l'ad en cas d'urgence comme les mot de passe ect ..

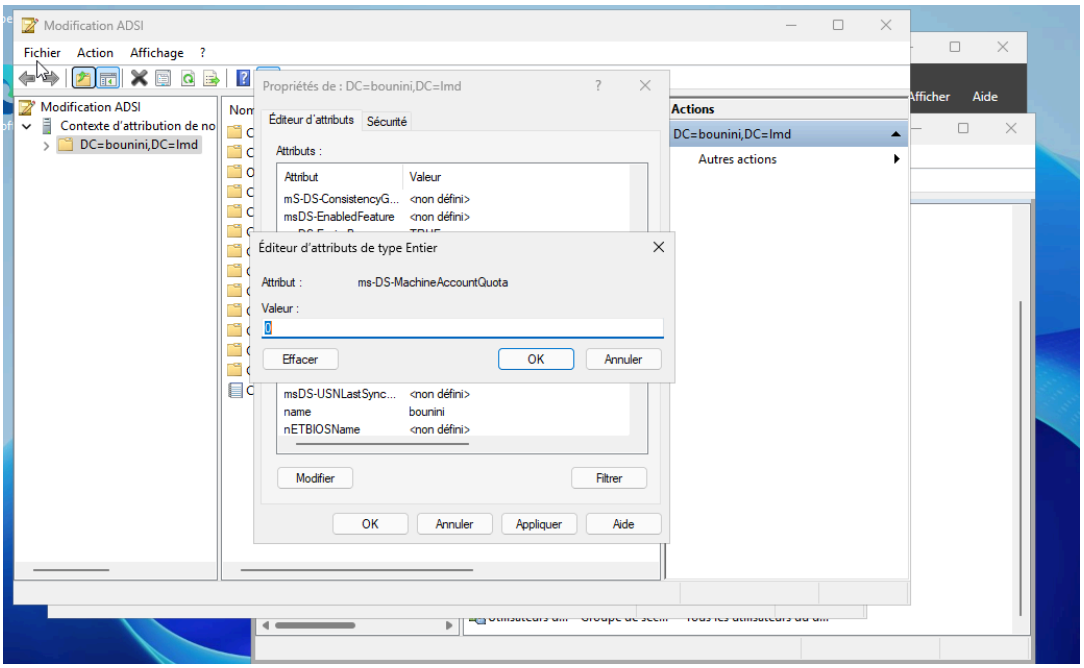


→ J'ai changer la stratégie de mdp ; longueurs de mot de passe pour plus de sécurité





→ maintenant on à s'assurer que les utilisateurs ne puissent pas enregistrer d'ordinateurs supplémentaires dans le domaine.



je met à 0 pour que seul l'administrateur puisse ajouter des machine sur l'AD