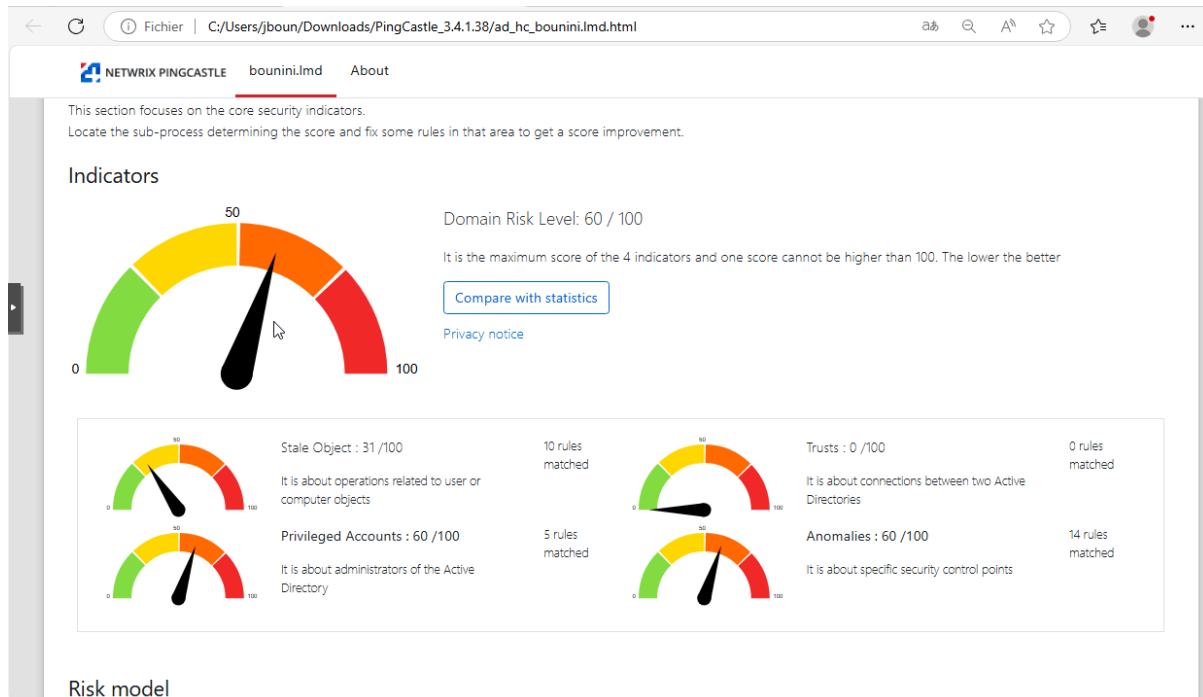


AP : PingCastle

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 :

Risk model

Left-click on the headlines in the boxes for more details

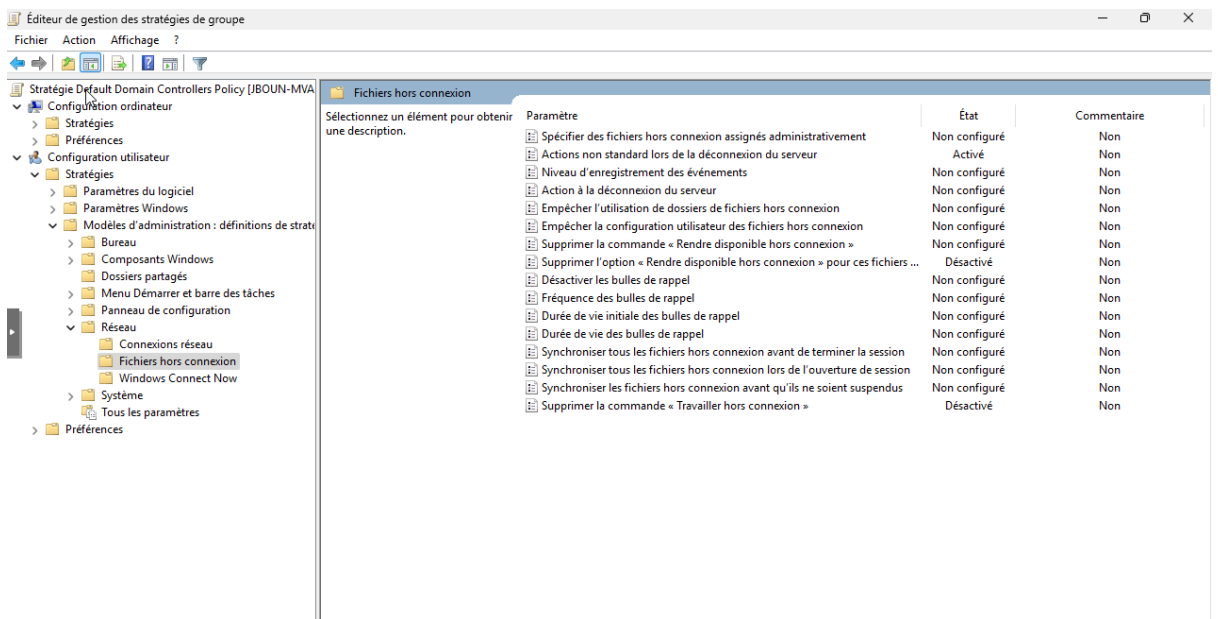
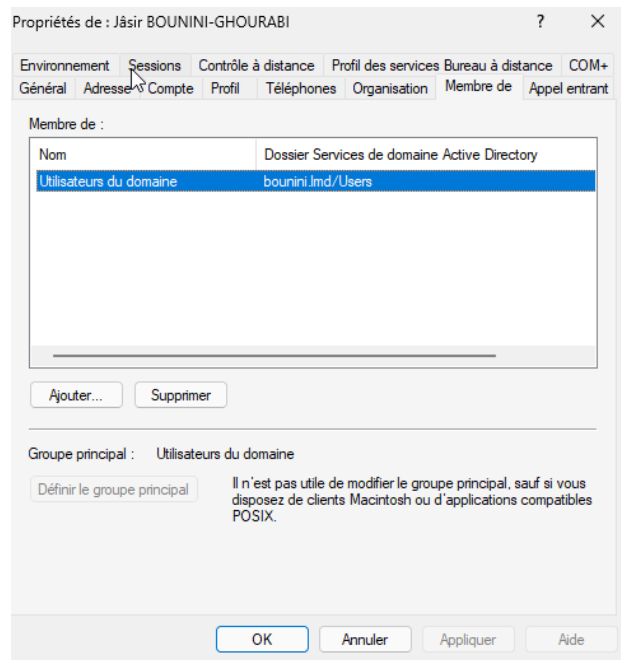
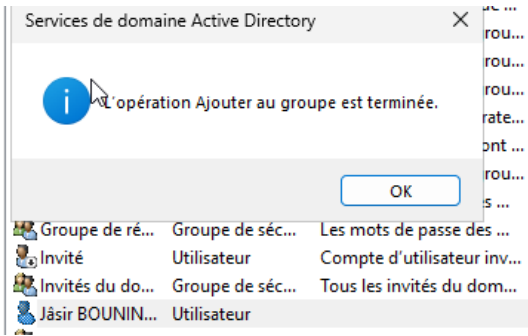
Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user on computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust Impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

- score is 0 - no risk identified
- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

Je vais alors les règles pour faire baissé le score:

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



Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Controllers Policy (JBOUN-MVA)

- Configuration ordinateur
 - Stratégies
 - Préférences
- Configuration utilisateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Modèles d'administration : définitions de strate...
 - Bureau
 - Composants Windows
 - Dossiers partagés
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Connexions réseau
 - Fichiers hors connexion
 - Windows Connect Now
 - Système
 - Tous les paramètres
 - Préférences

Connexions réseau

Sélectionnez un élément pour obtenir une description.

Paramètre	État	Commentaire
Interdire l'ajout et la suppression des composants pour une connexion d'a...	Non configuré	Non
Interdire l'accès à l'élément Paramètres avancés dans le menu Avancé	Désactivé	Non
Interdire la configuration avancée de TCP/IP	Désactivé	Non
Interdire l'activation/désactivation des composants d'une connexion au ré...	Non configuré	Non
Possibilité de supprimer toutes les connexions d'accès à distance utilisateur	Non configuré	Non
Interdire la suppression des connexions d'accès à distance	Non configuré	Non
Interdire l'accès à l'élément Préférences d'accès à distance dans le menu A...	Non configuré	Non
Activer les paramètres de connexions réseau Windows 2000 pour les admini...	Non configuré	Non
Désactiver les notifications lorsqu'une connexion ne dispose que d'une co...	Non configuré	Non
Interdire l'accès aux propriétés des composants d'une connexion réseau lo...	Non configuré	Non
Possibilité d'activer/désactiver une connexion réseau	Désactivé	Non
Interdire l'accès aux propriétés d'une connexion au réseau local	Désactivé	Non
Interdire l'accès à l'Assistant Nouvelle connexion	Non configuré	Non
Possibilité de modifier les propriétés de la connexion d'accès à distance de...	Non configuré	Non
Interdire l'accès aux propriétés des composants d'une connexion d'accès à...	Non configuré	Non
Interdire la connexion et la déconnexion d'une connexion d'accès à distance	Non configuré	Non
Interdire la modification des propriétés d'une connexion d'accès à distanc...	Non configuré	Non
Possibilité de renommer toutes les connexions d'accès à distance utilisateur	Non configuré	Non
Possibilité de renommer les connexions par réseau local ou les connexions...	Non configuré	Non
Possibilité de renommer des connexions réseau	Non configuré	Non
Interdire de renommer les connexions d'accès à distance privées	Non configuré	Non
Interdire l'affichage du statut pour une connexion active	Non configuré	Non

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Controllers Policy (JBOUN-MVA)

- Configuration ordinateur
 - Stratégies
 - Préférences
- Configuration utilisateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Modèles d'administration : définitions de strate...
 - Bureau
 - Active Directory
 - Bureau
 - Composants Windows
 - Dossiers partagés
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Connexions réseau
 - Fichiers hors connexion
 - Windows Connect Now
 - Système
 - Tous les paramètres
 - Préférences

Active Directory

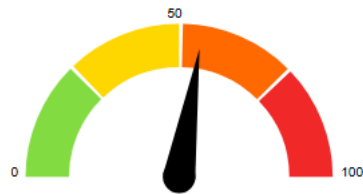
Sélectionnez un élément pour obtenir une description.

Paramètre	État	Commentaire
Activer le filtrage dans la boîte de dialogue Rechercher	Non configuré	Non
Cacher le dossier Active Directory	Activé	Non
Taille maximale des recherches dans Active Directory	Non configuré	Non

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



Trusts : 0 /100
It is about connections between two Active Directories

0 rules matched



Privileged Accounts : 40 /100
It is about administrators of the Active Directory

4 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 :

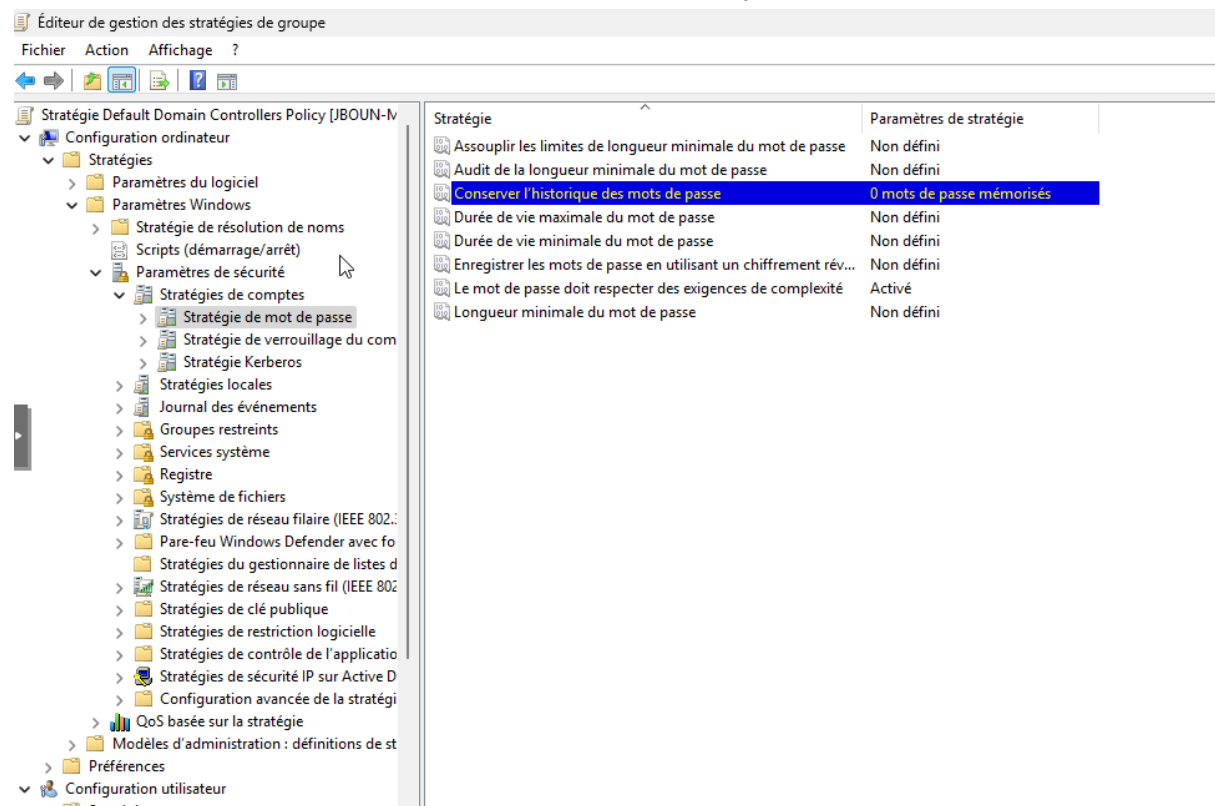
Interdiction du stockage d'identifiants déléguables (Délégation non contrainte).

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.



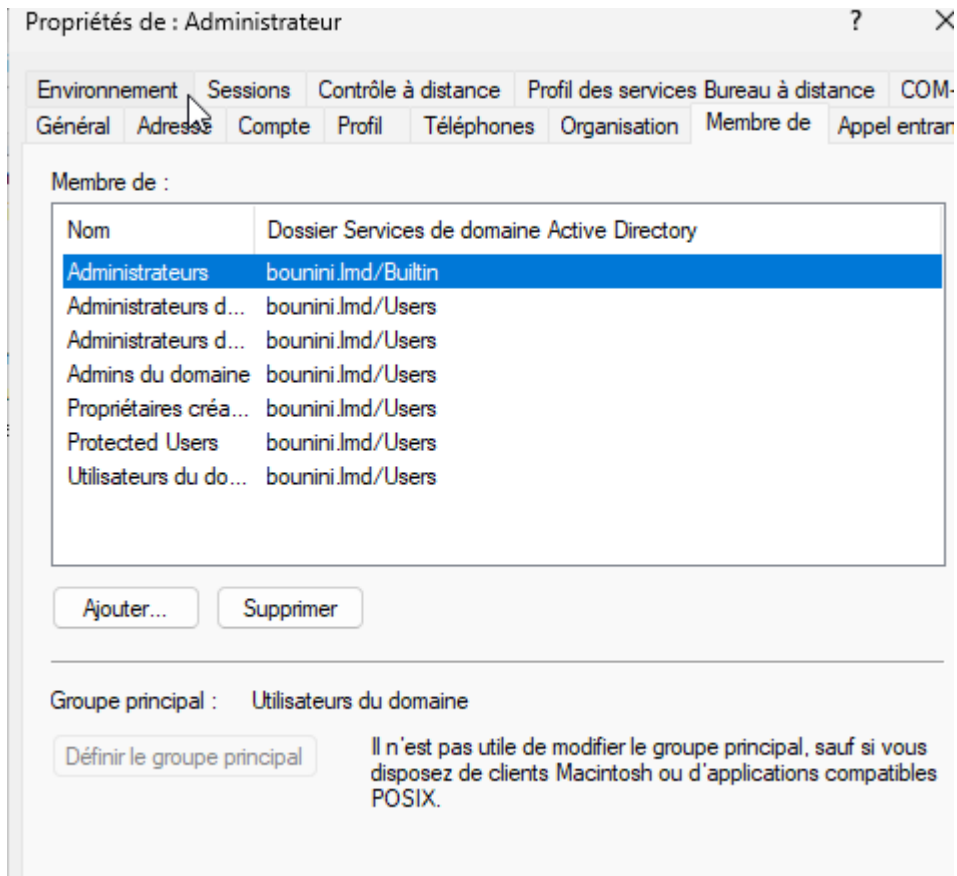
Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Controllers Policy [JBOUN-IV]

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Paramètres de sécurité
 - Stratégies de comptes
 - Stratégie de mot de passe
 - Stratégie de verrouillage du com
 - Stratégie Kerberos
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
 - Stratégies de réseau filaire (IEEE 802.11)
 - Pare-feu Windows Defender avec fonctionnalités avancées
 - Stratégies du gestionnaire de listes de diffusion
 - Stratégies de réseau sans fil (IEEE 802.11)
 - Stratégies de clé publique
 - Stratégies de restriction logicielle
 - Stratégies de contrôle de l'application
 - Stratégies de sécurité IP sur Active Directory
 - Configuration avancée de la stratégie
 - QoS basée sur la stratégie
 - Modèles d'administration : définitions de stratégie
 - Préférences
 - Configuration utilisateur

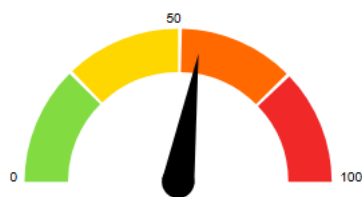
Stratégie	Paramètres de stratégie
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	0 mots de passe mémorisés
Durée de vie maximale du mot de passe	Non défini
Durée de vie minimale du mot de passe	Non défini
Enregistrer les mots de passe en utilisant un chiffrement réversible	Non défini
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	Non défini



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

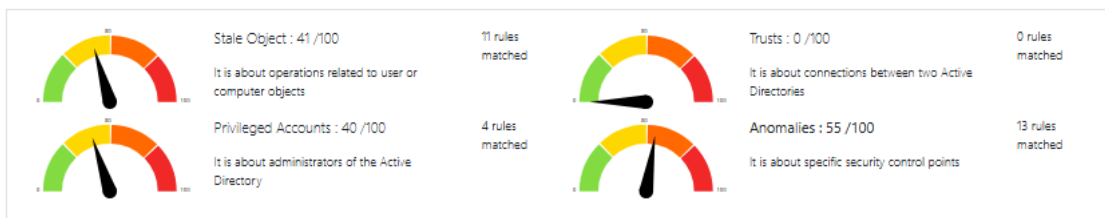


Domain Risk Level: 55 / 100

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](#)



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

Ensure that the NTLMv1 and old LM protocols are banned

Rule ID: S-QiaNtim

Description: The purpose is to check if NTLMv1 or LM can be used by DC

Technical explanation: NTLMv1 is an old protocol which is known to be vulnerable to cryptographic attacks. It is typically used when a hacker sniffs the network and tries to retrieve NTLM hashes which can then be used to impersonate users.

This attack can be combined with coerced authentication attacks - a hacker forces the DC to connect to a controlled host. In this case, NTLMv1 can be specified so the hacker can retrieve the NTLM hash of the DC, impersonates it and then take control of the domain. This attack is still possible with NTLMv2 but this is more difficult.

Windows has default security settings regarding LM/NTLM. Windows XP: Send LM & NTLM responses; Windows Server 2003: Send NTLM response only; Vista/2008: Win7/2008 R2: Send NTLMv2 response only.

However Domain Controllers have relaxed default settings to accept the connection of older operating systems. That means that by default, NTLMv1 is accepted on domain controllers. If no GPO defines the LAN Manager Authentication Level, the DC fall back to the non secure default.

Advised solution: After an audit of NTLMv1 usage (see the links below), you need to raise the LAN Manager Authentication Level to "Send NTLMv2 response only; Refuse LM & NTLM". This can be done by editing the policy "Network security: LAN Manager authentication level" which can be accessed in Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. The policy will be applied after a computer reboot.

Beware that you may break software which is not compatible with Ntlmv2 such as very old Linux stacks or very old Windows before Windows Vista. But please note that Ntlmv2 can be activated on all Windows starting Windows 95 and other operating systems.

Points: 15 points if present

Documentation:

Dans la strategie :Default Domain Controllers Policy

Stratégie

- Ouverture de session interactive : seuil de verrouillage du compte d'ordinateur
- Ouvertures de sessions interactives : nombre d'ouvertures de sessions précédentes réalisées en utilisant le cach...
- Paramètres système : Sous-systèmes optionnels
- Paramètres système : utiliser les règles de certificat avec les exécutables Windows pour les stratégies de restricti...
- Périphériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session localement
- Périphériques : autoriser le retrait sans ouverture de session préalable
- Périphériques : empêcher les utilisateurs d'installer des pilotes d'imprimante
- Périphériques : ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement
- Périphériques : permettre le formatage et l'éjection des médias amovibles
- Sécurité des réseaux : exigences en matière de chiffrement du client LDAP
- Sécurité réseau : conditions requises pour la signature de client LDAP
- Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent
- Sécurité réseau : niveau d'authentification LAN Manager**
- Sécurité réseau : sécurité de session minimale pour les clients basés sur NTLM SSP (y compris RPC sécurisé)
- Sécurité réseau : sécurité de session minimale pour les serveurs basés sur NTLM SSP (y compris RPC sécurisé)
- Sécurité réseau : Autoriser le retour à des sessions NULL avec SystèmeLocal
- Sécurité réseau : autoriser les demandes d'authentification PKU2U auprès de cet ordinateur pour utiliser les ide...
- Sécurité réseau : Autoriser Système local à utiliser l'identité de l'ordinateur pour NTLM
- Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos
- Sécurité réseau : Restreindre NTLM : Ajouter des exceptions de serveurs dans ce domaine
- Sécurité réseau : Restreindre NTLM : Ajouter des exceptions de serveurs distants pour l'authentification NTLM
- Sécurité réseau : Restreindre NTLM : Auditer l'authentification NTLM dans ce domaine
- Sécurité réseau : Restreindre NTLM : Auditer le trafic NTLM entrant
- Sécurité réseau : Restreindre NTLM : Authentification NTLM dans ce domaine
- Sécurité réseau : Restreindre NTLM : Trafic NTLM entrant
- Sécurité réseau : Restreindre NTLM : Trafic NTLM sortant vers des serveurs distants
- Serveur réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)
- Serveur réseau Microsoft : communications signées numériquement (toujours)
- Serveur réseau Microsoft : déconnecter les clients à l'expiration du délai de la durée de session
- Serveur réseau Microsoft : durée d'inactivité avant la suspension d'une session
- Serveur réseau Microsoft : niveau de validation du nom de la cible de serveur SPN

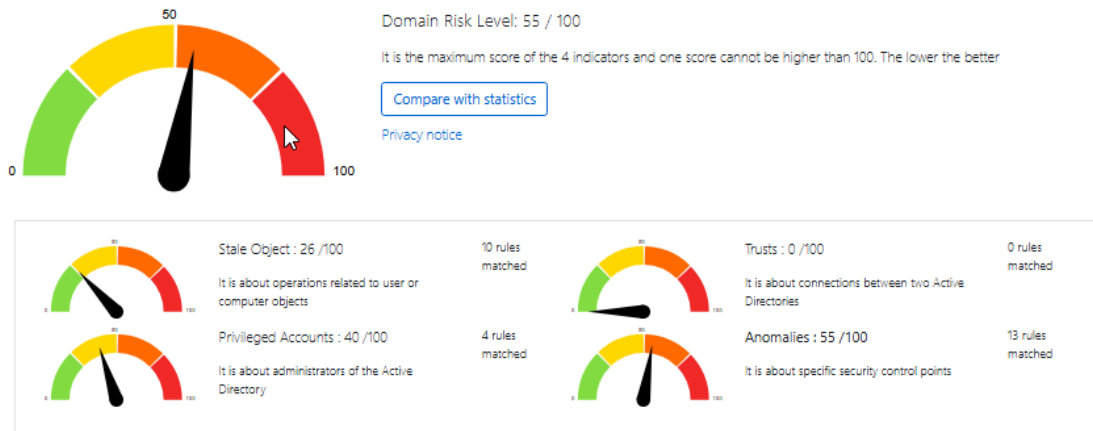
Paramètres de stratégie

Non défini	Non défini
Non défini	Non défini
Non défini	Propriétés de : Sécurité réseau : niveau d'authentification...
Non défini	Paramètre de stratégie de sécurité
Non défini	Sécurité réseau : niveau d'authentification LAN Manager
Non défini	<input checked="" type="checkbox"/> Définir ce paramètre de stratégie
Non défini	Envoyer uniquement une réponse NTLM version 2. Refuser LM et
Non défini	La modification de ce paramètre peut affecter la compatibilité avec les clients, les services et les applications. Pour obtenir davantage d'informations, consultez Sécurité réseau : niveau d'authentification LAN Manager (8823659)
Non défini	OK Annuler Appliquer

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



Correction de la vulnérabilité PingCastle P-AdminLogin

changement du mdp administrateur et aussi du nom remplacer par adm.jboun avec le mdp : JesuisenSISmartiniere2025@.

Utilisateurs et ordinateurs Active Directory [jboun-...]

Nom	Type	Description
adm.jboun	Utilisateur	Compte d'utilisateur d'a...

Réinitialiser le mot de passe

Nouveau mot de passe : [masqué]

Confirmer le mot de passe : [masqué]

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur doit fermer puis ouvrir à nouveau sa session afin que les modifications prennent effet.

État de verrouillage du compte sur ce contrôleur de domaine : Déverrouillé

Déverrouiller le compte de l'utilisateur

OK Annuler

Services de domaine Active Directory

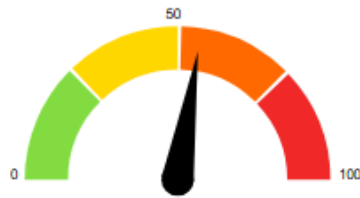
Le mot de passe pour adm.jboun a été changé.

OK

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](#)

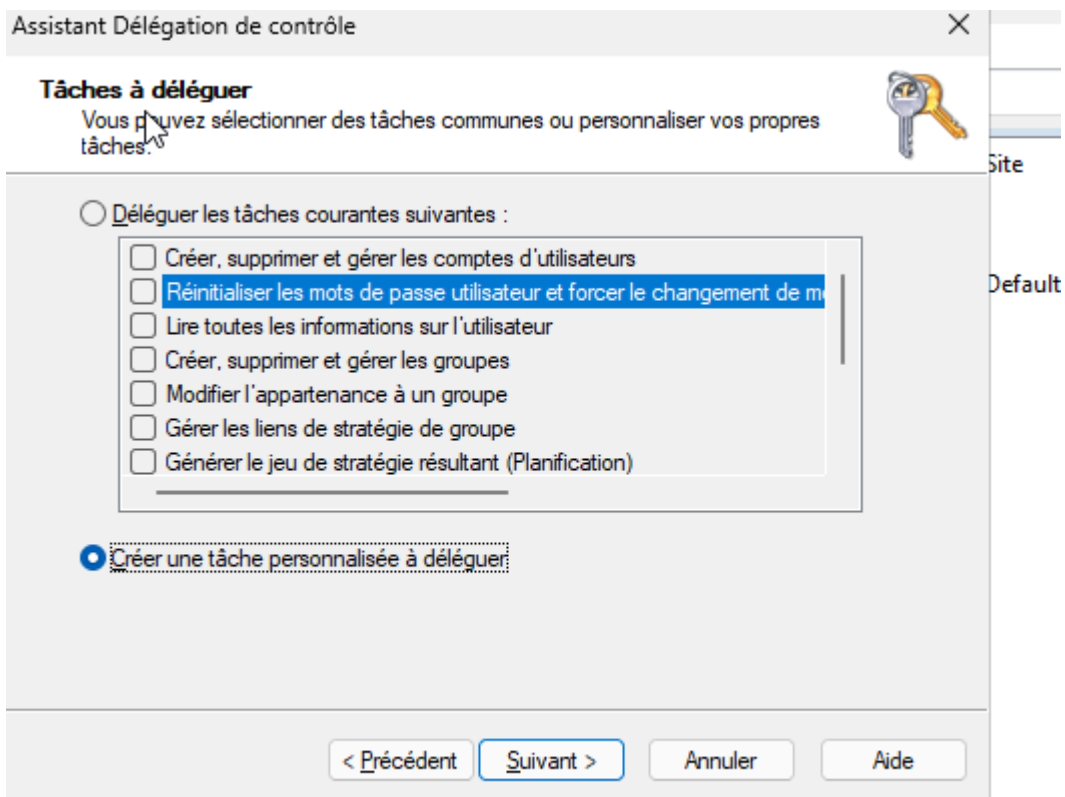
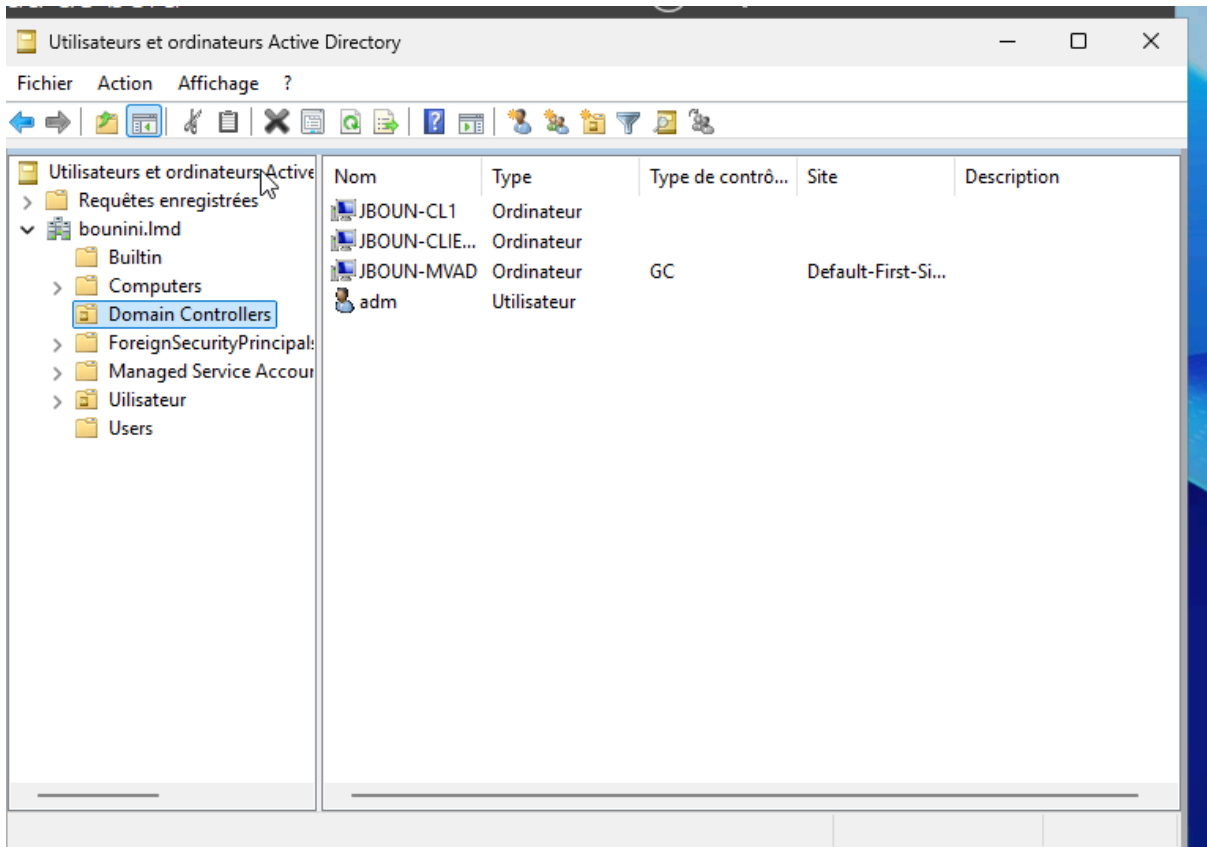
[Privacy notice](#)



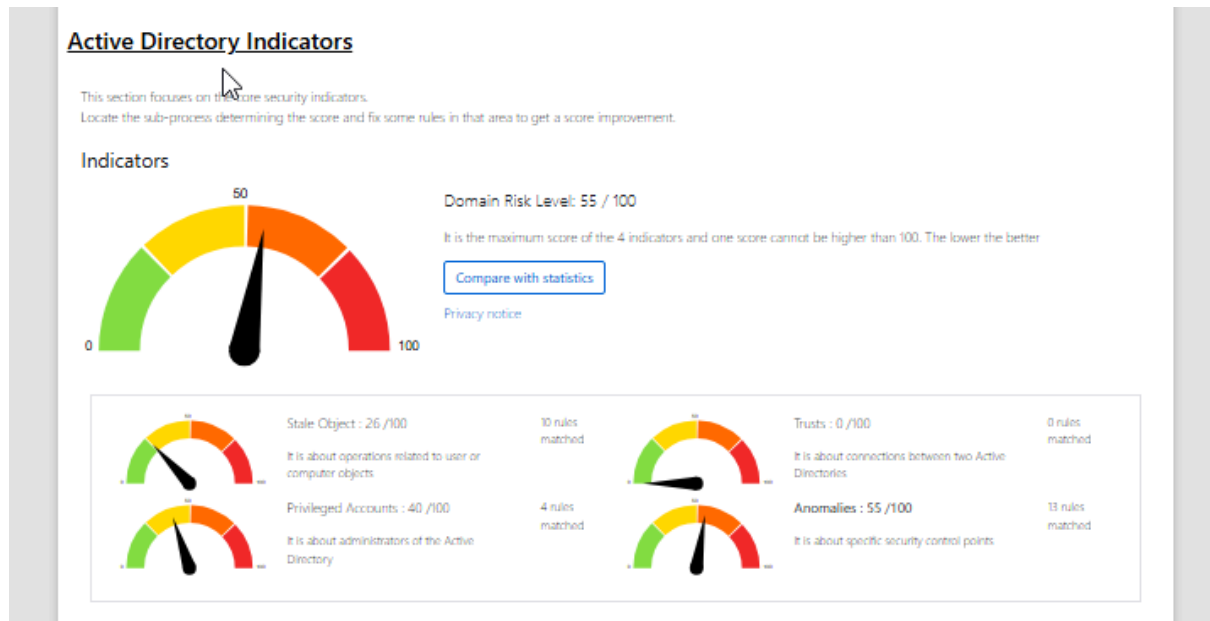
Risk model

Cela n'a rien changé.

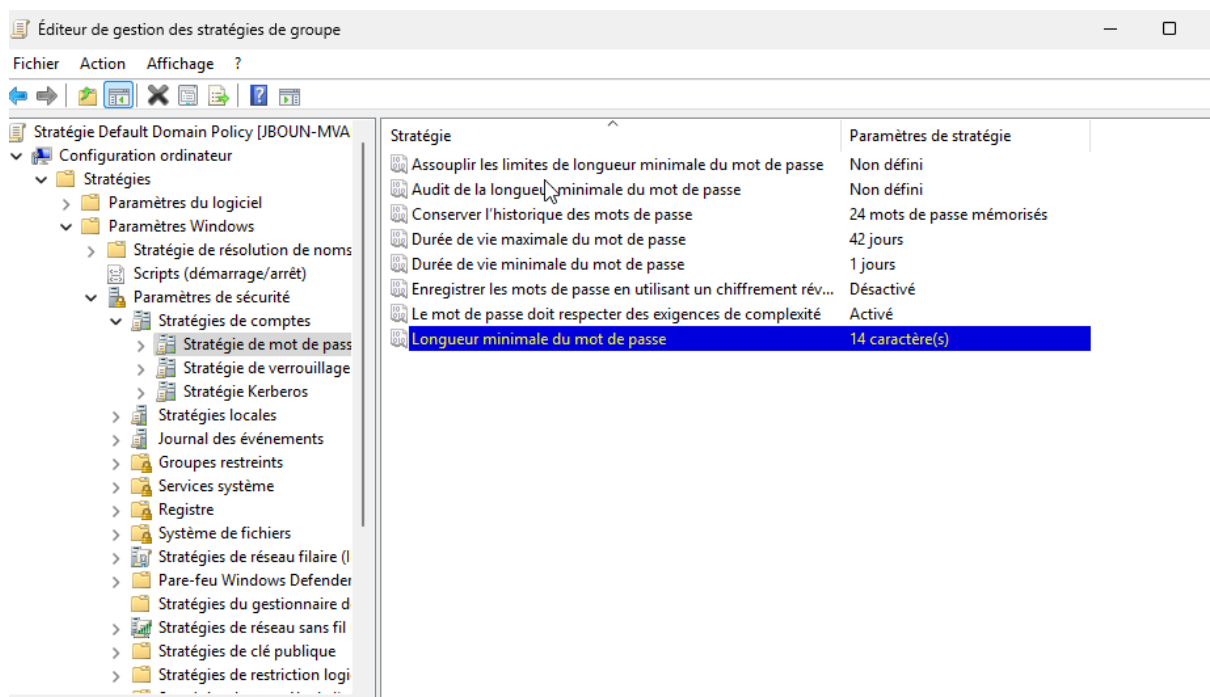
je continue :

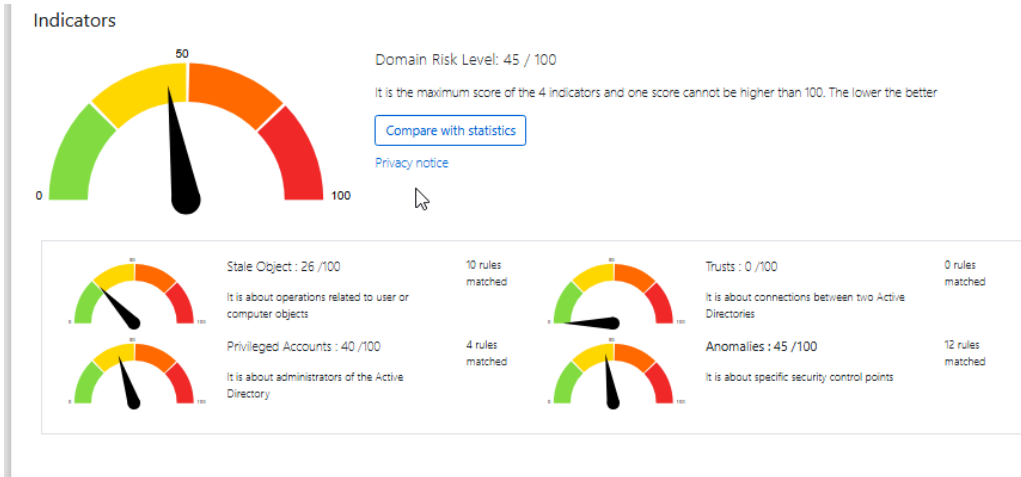


→ j'ai fait en sorte de donner à un seul admin de pouvoir sauver l'ad en cas d'urgence comme les mot de passe ect ..

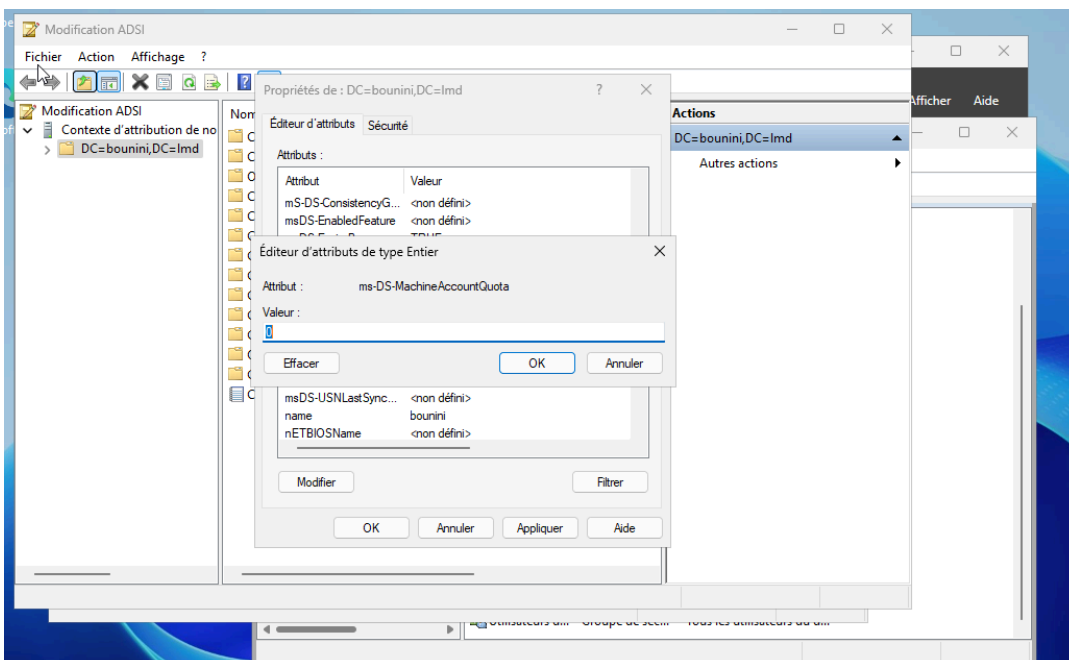


→ J'ai changer la stratégie de mdp ; longueurs de mot de passe pour plus de sécurité





→ 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

