# Compte Rendu : Durcissement de l'Active Directory (AD)

## Réactiver les pare feux Windows :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement



A laisser activer si, pas de solution autre que Windows Defenders, EDR, Antivirus, ect

Une image contenant texte, logiciel, Page web, Police

Description générée automatiquement



## Spooler d’impression (ouvert à de nombreuse faille de sécurité) à désactiver.

Une image contenant texte, capture d’écran, affichage, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement



Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement



Après l’avoir arrêtez aller dans « Propriété » et changer le type de démarrage et mettez-le en désactivé pour qu’il ne se redémarre pas au prochain démarrage de la machine.

## Autre petite fonctionnalité qui peut être intéressante ce sont les clichés instantanés :

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement



Une fois dans la configuration des clichés instantanés vous pouvez cliquer sur « Activer ». Une fois activer vous pourrez créer des clichés qui peuvent être consulter en faisant un clique droit sur un dossier et « Voir les versions précédentes »

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement



Pour renforcer en plus votre Windows Serveur vous pouvez ajouter une fonctionnalité disponible sur Windows classique, BitLocker.

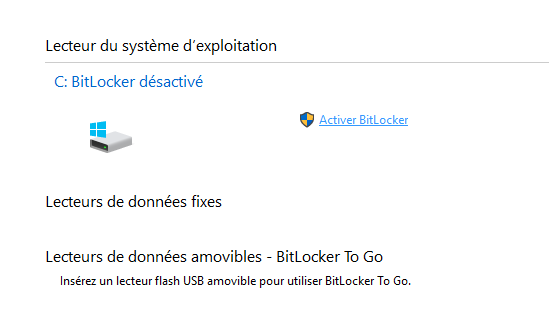
Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une fois l’installations terminées redémarrer la machine et aller dans « Gérer Bitlocker »



Pour continuer aller dans le centre d’administration de l’AD et activer la corbeille :

Une image contenant capture d’écran, texte, Police

Description générée automatiquement

Ensuite aller dans modification ADSI faite clique droite sur Modification ADSI et cliquer sur connexion, ne toucher à rien et faite OK

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Faite ensuite clic droit sur DC=nom de votre ad et cliquer sur propriéter

Une image contenant texte, logiciel, nombre, Page web

Description générée automatiquement

Chercher ensuite MachineAccountQuota et changer la valeur en 1 au lieu de 10.

Aller ensuite dans vos utilisateur et ordinateur de l’AD et aller dans la GO Builtin et cliquer sur le premier « Acces compatibles pré-Windows » et supprimé les utilisateurs authentifies.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Ensuite supprimer le compte Administrateur de « Administrateur du Schéma » contenu dans le GO Users.

Une image contenant texte, logiciel, affichage, Icône d’ordinateur

Description générée automatiquement

Dirigez vous ensuite vers la gestion des GPO, créer une GPO dans le Domain Contrôler et Appeler la Désactiver NTLM modifier ensuite cette même GPO et ensuite aller dans « Strategies » -> Parametre de sécurité -> Strategies locales -> Options de sécurités puis chercher cette options precise :



Puis cliquer sur « Définir ce parametre de strategies »

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

Puis choisissez cette option-là :

Une image contenant texte, Police, capture d’écran, information

Description générée automatiquement

Et cocher cette option :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

LAPS

Ouvrez en premier un PowerShell en administrateur et taper la commande suivante :

Une image contenant texte, capture d’écran, Police, Bleu électrique

Description générée automatiquement

Ensuite créer une GPO dans Ordinateurs et appeler la LAPS-Activation

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Modifier ensuite cette même stratégie et aller dans Stratégies -> Modèles d’administration -> Système puis LAPS et configurer le répertoire de sauvegarde de mot de passe

Cliquer sur Activé et choisissez Active Directory au lieu de Azure Active Directory

Une image contenant texte, logiciel, Page web, capture d’écran

Description générée automatiquement