Korantin Horuckowa

PRÉVISION

une vision, des valeurs, la passion d'entreprendre

Modification de l'Active Directory

Table des matières

Après la sécurisation des BIOS/UEFI et de la procédure de démarrage, le but est désormais de travailler sur l'Active Directory de l'entreprise. Environ 65 points ont été soulevés lors de l'audit, des points plus ou moins importants et plus ou moins long à corriger ou à mettre en place.
Le but de cette mission est d'apporter des améliorations, des correctifs ou des explications aux différents points soulevés par Ping Castle sur l'Active Directory pour les techniciens.

I Activer les logs

A Prise en main du sujet

Qu'est-ce qu'un log?

Le concept d'historique des événements ou de journalisation désigne l'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique…). Le journal (en anglais log file ou log), désigne alors le fichier contenant ces enregistrements. Généralement datés et classés par ordre chronologique, ces derniers permettent d'analyser pas à pas l'activité interne du processus et ses interactions avec son environnement.

Sofimat, Magsi, Oxymax, Emily, Tubomax, JEM				
Type	Audit	Problem	Rationale	DC
Advanced	Policy Change / Authentication Policy Change	No GPO check for audit success	Collect events 4713, 4716, 4739, 4867, to track trust modifications	Tous
Advanced	Account Management / Computer Account Management	No GPO check for audit success	Collect events 4741, 4742 to track computer changes	Tous
Advanced	Detailed Tracking / DPAPI Activity	No GPO check for audit success	Collect event 4692 to track the export of DPAPI backup key	Tous
Advanced	Account Logon / Kerberos Authentication Service	No GPO check for audit success	Collect events 4768, 4771 for kerberos authentication	Tous
Advanced	Account Logon / Kerberos Service Ticket Operations	No GPO check for audit success	Collect events 4769 for kerberos authentication	Tous
Advanced	Logon/Logoff / Logoff	No GPO check for audit success	Collect events 4634 for account logoff	Tous
Advanced	Logon/Logoff / Logon	No GPO check for audit success	Collect events 4624, 4625, 4648 for account logon	Tous
Advanced	Detailed Tracking / Process Creation	No GPO check for audit success	Collect event 4688 to get the history of executed programs	Tous
Advanced	Account Management / Security Group Management	No GPO check for audit success	Collect events 4728, 4732, 4756 for group membership change	Tous
Advanced	System / Security System Extension	No GPO check for audit success	Collect events 4610, 4697 to track lsass security packages and services	Tous
Advanced	Privilege Use / Sensitive Privilege Use	No GPO check for audit success	Collect events 4672, 4673, 4674 for privileges tracking such as the debug one	Tous
Advanced	Logon/Logoff / Special Logon	No GPO check for audit success	Collect event 4964 for special group attributed at logon	Tous
Advanced	Account Management / User Account Management	No GPO check for audit success	Collect events 4720,22,23,38,65,66,80,94 for user account mamangement	Tous

Listes Ping Castle

a) Active Directory

"*Un annuaire est une structure hiérarchique stockant les informations sur les objets du réseau. Un service d'annuaire, tel que le service de domaine Active Directory (AD DS), fournit des méthodes de stockage des données d'annuaire et de mise à disposition de ces données aux utilisateurs et administrateurs réseau.*"

"*L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information.*"

Pour simplifier c'est un annuaire LDAP pour les systèmes d'exploitation Windows.
Un annuaire AD permet une administration centralisée et simplifiée, l'identification des différents objets et classes d'objet :

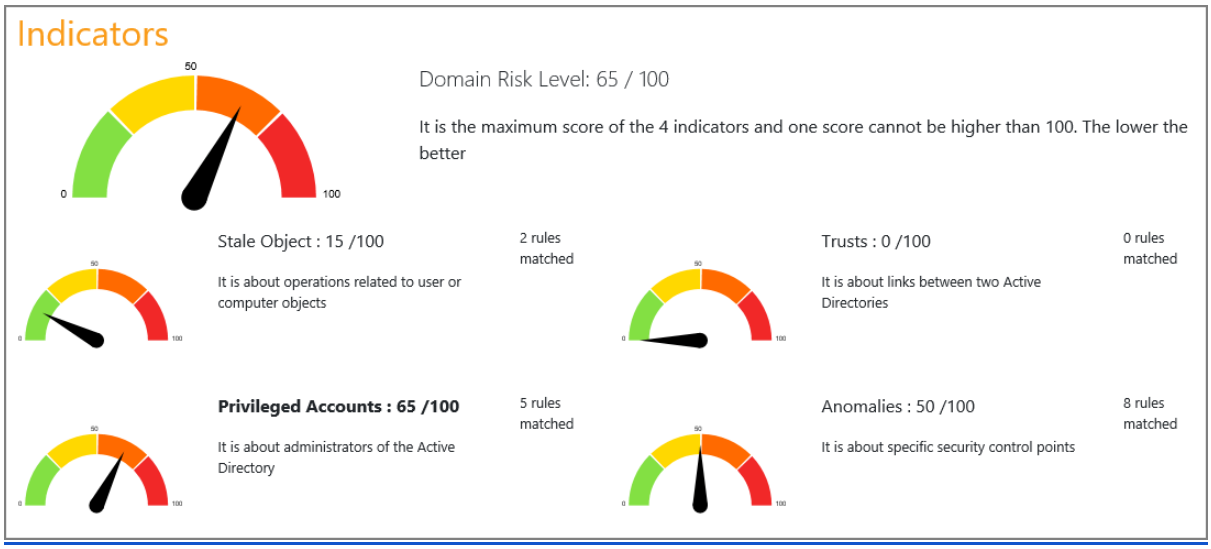
1. Ordinateurs : qui sont les ordinateurs, serveurs et contrôleurs de domaine intégrés au domaine.
2. Contact : enregistrer des contacts sans autorisation d'identification
3. Groupe : regrouper les objets dans un groupe pour simplifier l'administration
4. UO ou Unité d'Organisation : dossier pour créer une arborescence et organiser les objets
5. Imprimante : pour administrer les imprimantes

6. Utilisateur : comptes utilisateurs qui permettent de s'authentifier sur le domaine et ainsi d'accéder aux ressources, aux ordinateurs

(Liste non exhaustive)

b) Ping Castle

Les différents points présents dans ce tableau ont été relevés via *Ping Castle*, logiciel permettant d'auditer son AD (Active Directory) de manière autonome. Une fois l'audit terminé, des fichiers sont générés et permettent de prendre connaissance des forces et faiblesse de l'AD.



Résultat d'un audit sur un AD quelconque

Stale Object : points de sécurité liés aux utilisateurs ou aux ordinateurs
Privileged Accounts : points de sécurité liés aux comptes avec des privilèges élevés (Administrateurs du domaine Active Directory
Trusts : point de sécurité liés aux relations d'approbations entre les domaines Active Directory
Anomalies : points de sécurité liés à d'autres aspects de la configuration qui peuvent impacter la sécurité de l'annuaire

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or 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

"*Risk model" quelconque*

B Recherche

Le but de la mise en place est de prendre connaissance de l'Active Directory de Magsi, l'une des société prise en charge par Prévision et de voir comment faire une GPO pour activer les logs présents dans les tableaux ci-dessous. Tout cela sera fait sur un environnement de test avec une copie du contrôleur de domaine pour éviter les conséquences d'une mauvaise manipulation.

a) Événement et correspondance

Premièrement regardons à quoi font référence les évènements présents dans la matrice Ping Castle

Ligne 1

Type	Audit	Problem	Rationale	DC
Advanced	Policy Change / Authentication Policy Change	No GPO check for audit success	Collect events 4713, 4716, 4739, 4867, to track trust modifications	Tous

Au vus du message d'erreur "Problem" présent dans la colonne 3 ligne 3, l'action à mettre en œuvre est une stratégie de groupe sur l'AD DS permettant de récupérer ses événements.

L'événement n°	correspond à
4713	la stratégie Kerberos à été modifiée
4716	les informations de domaine approuvé ont été modifiée
4739	la stratégie de domaine à été modifiée
4867	une entrée d'information de forêt à été modifiée

Ligne 2

Advanced	Account Management / Computer Account Management	No GPO check for audit success	Collect events 4741, 4742 to track computer changes	Tous

L'événement n°	correspond à
4741	un compte d'ordinateur à été créé
4742	un compte d'ordinateur à été modifié
4743	un compte d'ordinateur à été supprimé

Ligne 3

Advanced	Detailed Tracking / DPAPI Activity	No GPO check for audit success	Collect event 4692 to track the export of DPAPI backup key	Tous

L'événement n°	correspond à
4692	la sauvegarde de la clé principale de protection des données à été tentée

Ligne 4

Advanced	Account Logon / Kerberos Authentication Service	No GPO check for audit success	Collect events 4768, 4771 for kerberos authentication	Tous

L'événement n°	correspond à
4768	un ticket d'authentification Kerberos (TGT) à été demandé
4771	échec de la pré-authentification Kerberos

Ligne 5

Advanced	Account Logon / Kerberos Service Ticket Operations	No GPO check for audit success	Collect events 4769 for kerberos authentication	Tous

L'événement n°	correspond à
4769	un ticket de service Kerberos à été demandé

Ligne 6

Advanced	Logon/Logoff / Logoff	No GPO check for audit success	Collect events 4634 for account logoff	Tous

L'événement n°	correspond à
4634	un compte à été déconnecté

Ligne 7

Advanced	Logon/Logoff / Logon	No GPO check for audit success	Collect events 4624, 4625, 4648 for account logon	Tous

L'événement n°	correspond à
4624	un compte à été correctement connecté
4625	échec d'ouverture de session d'un compte
4648	une tentative d'ouverture de session à été effectuée à l'aide d'informations d'identification explicite

Ligne 8

Advanced	Detailed Tracking / Process Creation	No GPO check for audit success	Collect event 4688 to get the history of executed programs	Tous

L'événement n°	correspond à
4688	un nouveau processus à été créé

Ligne 9

Advanced	Account Management / Security Group Management	No GPO check for audit success	Collect events 4728, 4732, 4756 for group membership change	Tous

L’événement n°	correspond à
4728	introuvable
4732	un membre à été ajouté à un groupe local avec sécurité
4756	introuvable

Ligne 10

Advanced	System / Security System Extension	No GPO check for audit success	Collect events 4610, 4697 to track lsass security packages and services	Tous

L’événement n°	correspond à
4610	un package d’authentification a été chargé par l’autorité de sécurité locale
4697	un service à été installer dans le système

Ligne 11

Advanced	Privilege Use / Sensitive Privilege Use	No GPO check for audit success	Collect events 4672, 4673, 4674 for privileges tracking such as the debug one	Tous

L’événement n°	correspond à
4672	privilège spéciaux attribués à la nouvelle ouverture de session
4673	un service privilégié à été appelé
4674	une opération à été tentée sur un objet privilégié

Ligne 12

Advanced	Logon/Logoff / Special Logon	No GPO check for audit success	Collect event 4964 for special group attributed at logon	Tous

L’événement n°	correspond à
4964	des groupes spéciaux ont été affecté à une nouvelle ouverture de session

Ligne 13

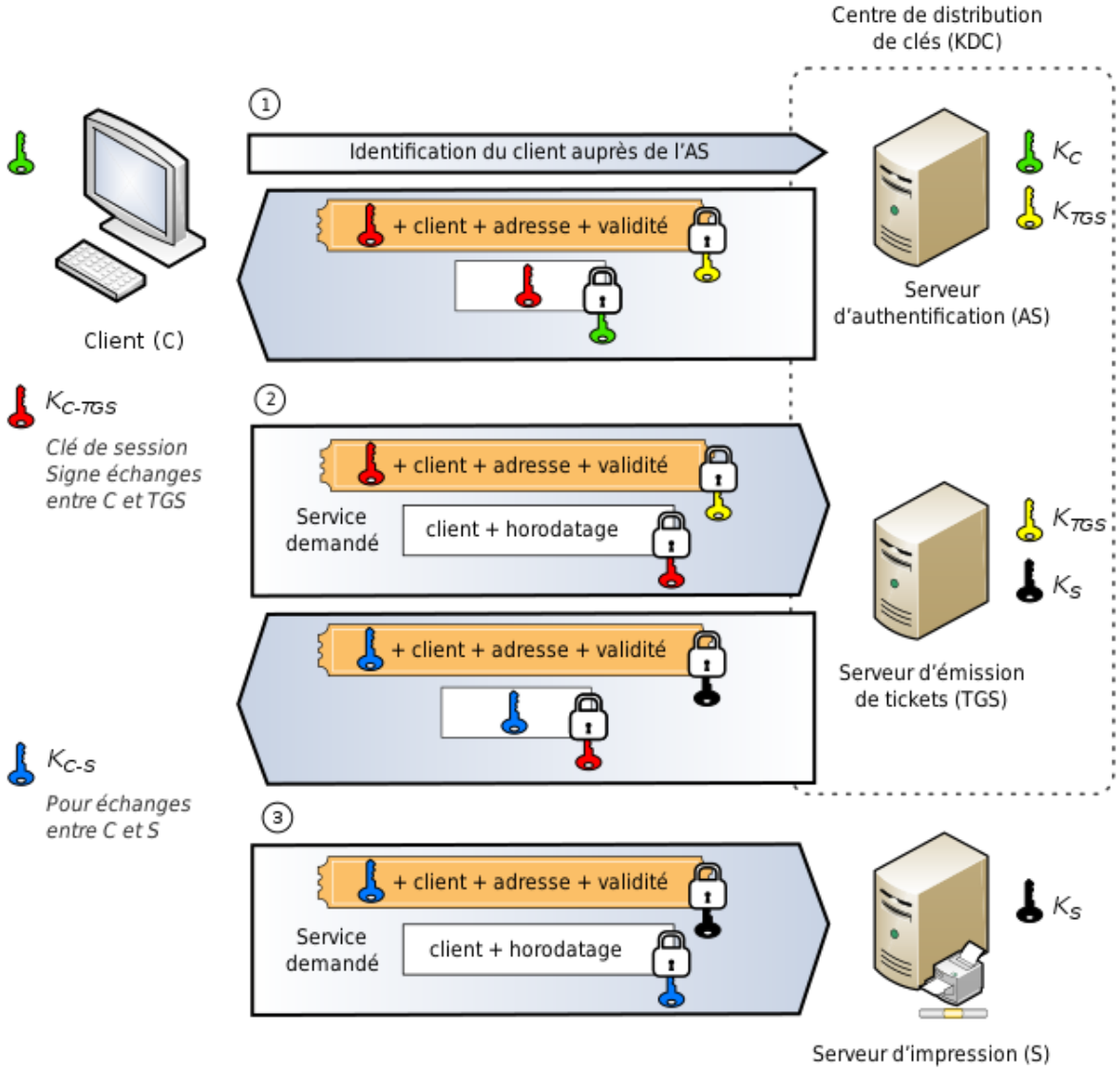
Adva	Account Management / User	No GPO check	Collect events 4720,22,23,38,65,66,80,94	T

nced	Account Management	for audit success	for user account management	ou s

L’événement n°	correspond à
4720	un compte utilisateur à été créé
4722	un compte utilisateur à été activé
4723	une tentative de modification du mot de passe d’un compte à été effectué
4738	un compte d’utilisateur à été modifié
4765	l’historique sid à été ajouté à un compte
4766	une tentative d’ajout de l’historique du SID à un compte a échoué
4780	la liste de contrôle d’accès a été définis sur les comptes qui sont membres de groupes d’administrateur
4794	une tentative à été effectuée pour définir le mot de passe administrateur du mode de restauration des services d’annuaire

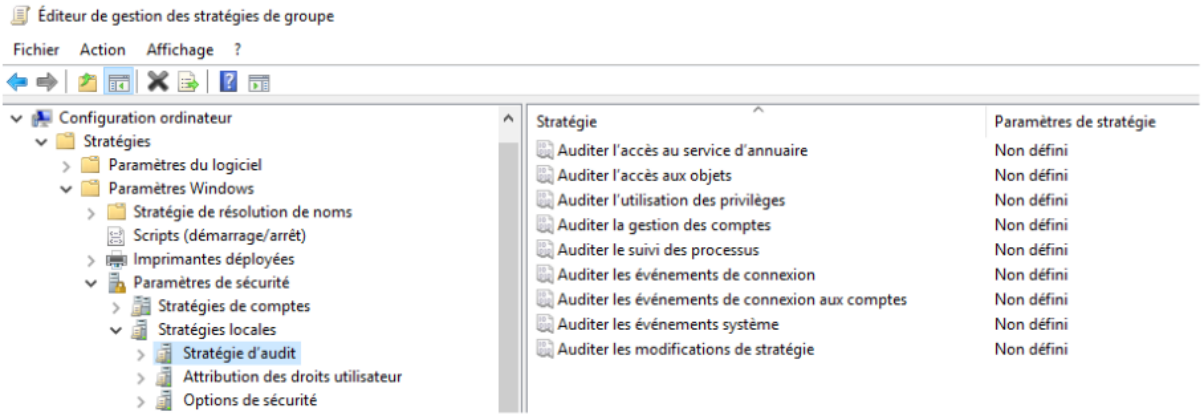
b) Kerberos

Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.



C Mise en place de la solution

Pour mettre en place la GPO, comme précisé plus tôt, un environnement de test à été créé. Une connexion au serveur AD test est faite via le bureau a distance, permettant l'administration à distance de celui-ci et donc dans mon cas, depuis mon poste de travail.
Première GPO, l'activation des logs de connexion, que ce soit un échec ou bien une réussite. Pour cela rendez-vous sur le serveur Active Directory>Gestion de stratégie de groupe>Clic droit sur le domaine>Créer un objet GPO dans ce domaine et le lier ici>Donner le nom souhaité>Clic droit sur la GPO>Modifier>Sur le panneau de gauche de l'Éditeur de gestion de stratégie de groupe>Configuration ordinateur>Stratégies>Paramètres Windows>Paramètres de sécurité>Stratégies locales>Stratégie d'audit

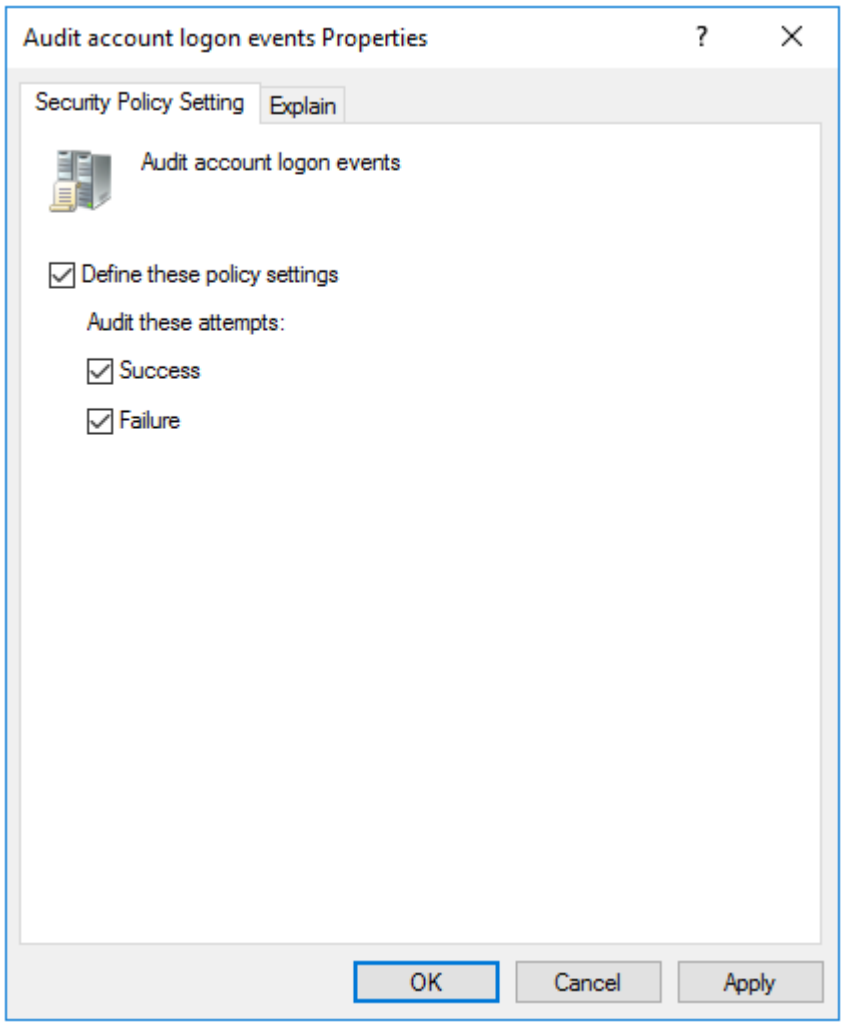


Editeur de gestion des stratégies, stratégie d'audit

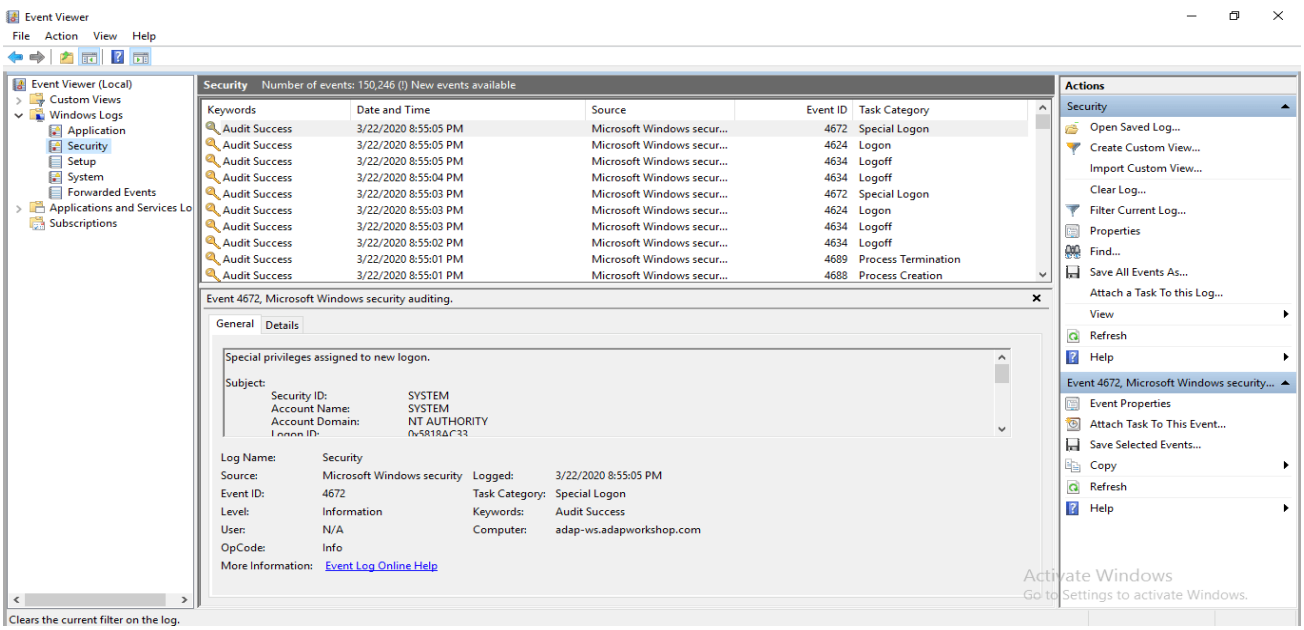
Contenue dans stratégie d'audit

Nous pouvons constater que ces paramètres sont indéfinis "Not Defined", pour les activer : Sur le panneau de droite>Double clic gauche>Cocher la case "Définir ces paramètres de stratégie">Cocher "Réussite" et "Échec"

Cela active la journalisation des connexion utilisateur, réussite ou échec.
Il est ensuite nécessaire de faire un "Appliquer" ou "Apply" et "Ok", pour appliquer les paramètres à la GPO.
Nous devons ensuite chercher à voir si des numéros d'événements présents dans les tableaux se retrouvent dans l'observateur d'évènement du serveur. Pour cela rendez-vous sur : Observateur d'événements>Journaux Windows>Sécurité



Finalisation de la GPO



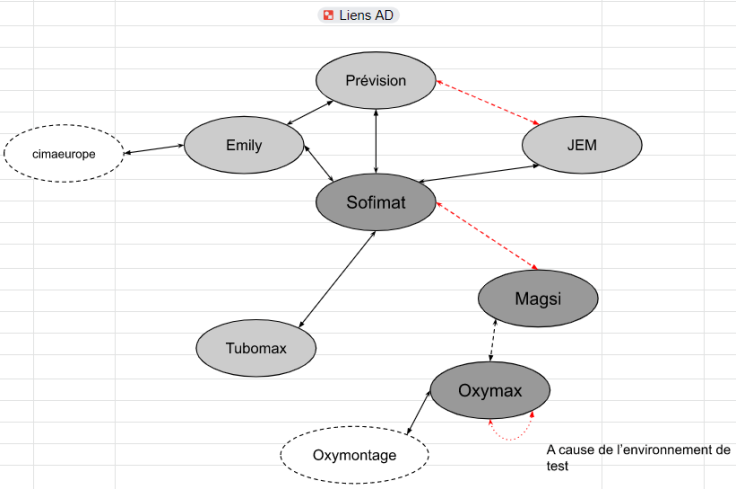
Journal d'événements de sécurité Windows

II Voir les procédures et impacts du changement Kerberos

a) Changer d'algorithme de chiffrement

Cette feuille liste les comptes qui ont des problèmes avec l'algorithme d'authentification Kerberos (les Trusts et les PC)

Trust		
Sofimat		
Partenaire	**Actif**	**Algorithme Kerberos**
magsiagri.fr	NON	RC4 (Par défaut)
emily.fr	OUI	RC4 (Par défaut)
tubomax.fr	OUI	RC4 (Par défaut)
prevision.fr	OUI	RC4 (Par défaut)
jem-tp.fr	OUI	RC4 (Par défaut)
Magsi		
Partenaire	**Actif**	**Algorithme Kerberos**
oxymax.fr	NON	RC4 (Par défaut)
sofimat.fr	NON	RC4 (Par défaut)
Oxymax		
Partenaire	**Actif**	**Algorithme Kerberos**
sofimat.fr	NON	RC4 (Par défaut)
oxymontage.com	OUI	RC4 (Par défaut)
oxymax.fr	OUI	RC4 (Par défaut)
Emily		
Partenaire	**Actif**	**Algorithme Kerberos**
cimaeurope.fr	OUI	RC4 (Par défaut)
sofimat.fr	OUI	RC4 (Par défaut)
prevision.fr	OUI	RC4 (Par défaut)
Tubomax		
Partenaire	**Actif**	**Algorithme Kerberos**
sofimat.fr	OUI	RC4 (Par défaut)



Matrice Kerberos

Le but premier est l'activation de l'algorithme Kerberos (qui est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs) avec comme méthode de chiffrement AES256_HMAC_SHA1 ou bien AES128_HMAC_SHA1 et au minimum RC4. Je n'active pas seulement AES256 ou AES128 car cela peut poser des problèmes comme signaler sur le support Windows.

Ce problème se produit si vous sélectionnez uniquement la case à cocher **AES256_HMAC_SHA1** ou **AES128_HMAC_SHA1** dans le **sécurité réseau : configurer des types de cryptage autorisés pour Kerberos** paramètre stratégie de groupe.

Remarque : Le paramètre de stratégie de groupe se trouve sous **ordinateur\Paramètres Windows\Paramètres de Sécurité\stratégies \Security Options**.

Support Windows, arrêt du système automatique à cause du chiffrement Kerberos

AES 128 et 256 : pour Advanced Encryptions Standard ou Norme de Chiffrement Avancé, est un algorithme de chiffrement symétrique travaillant avec des clés comprises entre 128 et 256 bits. Il remplace le DES (Data Encryptions Standard) qui ne prend que des clés de 56 bits et est donc plus vulnérable et plus lent.

Le principe est donc le même que pour l'activation des logs d'audit, nous créons une nouvelle GPO pour cela rendez-vous sur le serveur Active Directory>Gestion de stratégie de groupe>Clic droit sur le domaine>Créer un objet GPO dans ce domaine et le lier ici>Donner le nom souhaité>Clic droit sur la GPO>Modifier>Sur le panneau de gauche de l'Éditeur de gestion de stratégie de groupe>Configuration ordinateur>Stratégies>Paramètres Windows>Paramètres de sécurité>Stratégies locales>Options de sécurité>Sécurité réseau: configurer des types de cryptage autorisés pour Kerberos.
Cette stratégie, étant créée au niveau du domaine s'appliquera à tous les utilisateurs authentifiés.

b) Le mot de passe Kerberos

Reste désormais la procédure de changement de mots de passe Kerberos. Pour pouvoir exécuter le script je l'ai copié sur un document PowerShell ISE et l'ai mis sur clé puis je l'ai exécuté sur le serveur AD. De plus, le script pour son bon fonctionnement nécessite des prérequis tels que la présence de modules PowerShell.
Par ailleurs le script est bien fait et est très détaillé mais il reste compliqué, l'étude avec un technicien peut être intéressante. Une fois appliquer, une autre modification du mot de passe doit se faire après 10 jours pour que Kerberos soit fonctionnel.
Il n'est pas possible de mettre le script dans ce document à cause de sa longueur. En revanche, le lien GitHub est disponible dans les sources du II.
Changer ce mot de passe est plutôt compliqué et il n'existe aucun moyen mis en œuvre par Microsoft pour le faire. De plus, il nécessite un script (script énoncé plus tôt) et il n'est pas possible de le faire en interface graphique du moins cela est fortement déconseillé.

Pourquoi changer le mot de passe Kerberos ?
Pour une raison de sécurité, de manière à protéger l'environnement Active Directory lors d'une attaque par Golden Ticket par exemple.

Après avoir fait un premier bilan sur la modification de l'Active Directory, le technicien référent m'a demandé de lui faire part du processus pour modifier le mot de passe Kerberos et les avantages et inconvénients à le faire. L'atout principal d'un changement de mot de passe Kerberos est la sécurité de l'Active Directory, mais des inconvénients persistent à savoir la complexité de mise en œuvre, le temps de correction et le fait de devoir renouveler l'opération tous les 6 mois si l'on veut être optimal. Le renouvellement du mot de passe du compte Kerberos n'est donc pas envisagé pour le moment.

III Comptes administrateurs délégables

a) Délégation

La délégation est en générale utilisée pour donner des droits d'admin pour une tâche bien spécifique à un utilisateur ou un groupe d'utilisateurs à l'image de la réinitialisation de mots de passe pour une personne qui travaille dans une école et qui doit changer les mots de passe d'étudiant, l'ajout d'un poste utilisateur dans un domaine pour les techniciens en charge des déploiements, ajouter un utilisateur à un groupe pour le support par exemple ou encore désactiver des compte utilisateurs…

Celle-ci peut être activée à plusieurs niveaux de l'Active Directory, l'intégralité du domaine, un site, une unité d'organisation spécifique ou encore un objet spécifique de l'annuaire.
Nous pouvons voir en effet que des utilisateurs ont des droits administrateurs, la question est est-ce que cela est voulu ou non.

Ici sont répértoriés tous les comptes inconnus (autre domaine/suppression de compte) qui ont des droits de délégation

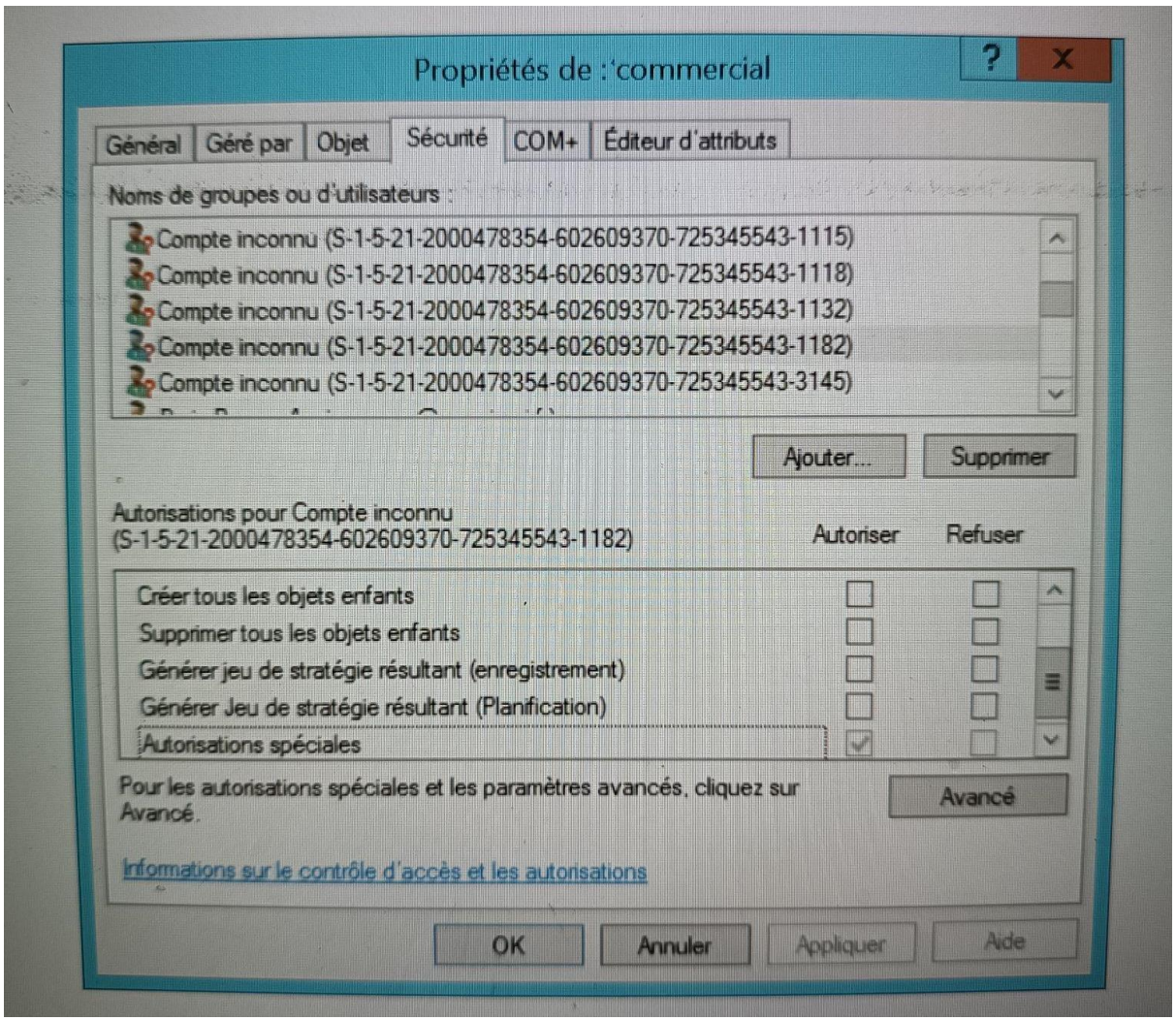
	Sofimat
DN	**delegation**
CN=Computers,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1113
CN=WinsockServices,CN=System,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1108
CN=Gestion du système,CN=System,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-4159
OU=contacts,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1118
OU=contacts,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1632
OU=Guiclan,OU=Sofimat,OU=Utilisateurs,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1632
OU=Briec,OU=Sofimat,OU=Utilisateurs,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1632
OU=Plouguin,OU=Sofimat,OU=Utilisateurs,DC=sofimat,DC=fr	S-1-5-21-682003330-1993962763-839522115-1632
	Magsi
DN	**delegation**
OU=Magsi,OU=Utilisateurs,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1182
OU=Magsi,OU=Utilisateurs,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-3145
OU=commercial,OU=Magsi,OU=Utilisateurs,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1115
OU=commercial,OU=Magsi,OU=Utilisateurs,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1118
OU=commercial,OU=Magsi,OU=Utilisateurs,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1132
	Oxymax
DN	**delegation**
OU=commercial,OU=Magsi,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1115
OU=commercial,OU=Magsi,DC=magsiagri,DC=fr	S-1-5-21-2000478354-602609370-725345543-1118

Matrice délégation

b) Comptes inconnus

Grâce à ce document nous pouvons constater que l'unité d'organisation "Commercial" présent dans l'unité d'organisation Magsi elle-même se trouvant dans l'unité d'organisation "Utilisateurs" sur le contrôleur de domaine "magsiagri.fr" possède une délégation d'administration sur le dossier. Or, pour Magsi, il est fort probable que cette délégation soit légitime puisque comme nous l'avons vu précédemment cela permet de donner un droit à un objet donc ici un utilisateur pour réaliser des tâches diverses à l'image de la création d'un utilisateur par exemple. Il est possible de voir toutes les délégations de l'Active Directory. Pour cela, il faut se rendre dans l'Active Directory>Affichage>Cocher "Fonctionnalités avancées">Propriétés. Pour modifier une délégation, il faut ensuite cliquer sur celle choisie>modifier/supprimer>Autoriser>Refuser.

Ainsi avec un répertoire complet, il est possible de voir quelles délégations existent et d'adapter en conséquence. Dans notre cas, nous devons nous cibler sur l'ou commercial qui se trouve dans l'ou Magsi elle-même dans l'ou user sur le domaine magsiagri.fr. Pour cela nous nous plaçons sur cette ou et faisons un clic droit>Propriétés>Sécurité et nous pouvons constater que les message S-1-5-21-2000478354-602609370-725345543-1182 présent dans la matrice se rapportent à des comptes inconnus.



Comptes correspondants aux SID S-1-5-21-2000478354-602609370-725345543-XXXX

IV Lister les comptes de services SPN avec des droits administrateurs

SPN signifie “Service Principal Name” lié à la notion de Kerberos. “*Lorsqu’un client souhaite accéder à un service, il va d’abord chercher à savoir qui porte le service. Dans Active Directory, cette information est stockée dans l’attribut multivalué « servicePrincipalName » d’objets computer ou user.”*
Le but de cette tâche est le listing des comptes SPN ayant un droit administrateur. Un service correspond à une classe de service (ex ldap pour un service LDAP), l’hôte lui peut-être soit son nom NETBIOS (ce service sert à associer un nom d’ordinateur à une adresse IP), l’unicité n’étant alors pas garantie.

Pourquoi il ne faut pas avoir de services avec des droits d’administrateur ?
Le but de l’attaque Kerberoast est de viser des comptes services, avec des mots de passe générer par des humains et donc plus ou moins faible suivant la politique de mot de passe de l’entreprise. Le mot de passe étant forcément plus faible, il devient plus facile d’avoir accès au comptes services qui s’ils ont des droits administrateurs peuvent donner libre accès au domaine.

Pour lister ces comptes un filtre de l’annuaire LDAP peut être utilisé avec l’attribut “servicePrincipalName”.

```
&(objectCategory=person)(objectClass=user)(servicePrincipalName=*)
```

Attribut

```
$search = New-Object DirectoryServices.DirectorySearcher([ADSI]"")
$search.filter =
"(&(objectCategory=person)(objectClass=user)(servicePrincipalName=
*))"
$results = $search.Findall()
foreach($result in $results)
{
      $userEntry = $result.GetDirectoryEntry()
      Write-host "User : " $userEntry.name "("
$userEntry.distinguishedName ")"
      Write-host "SPNs"
      foreach($SPN in $userEntry.servicePrincipalName)
      {
            $SPN
      }
      Write-host ""
}
```

Exemple de script PowerShell permettant de trouver un service SPN

Ainsi pour se prémunir de ce genre d’attaque il est nécessaire d’éviter d’avoir des comptes de services avec des droits administrateur ou si cela est nécessaire de mettre un mot de passe fort et renouvelé de façon régulière via MSA de Microsoft qui permet de renforcer le mot de passe et de le changer régulièrement et automatiquement via PowerShell.

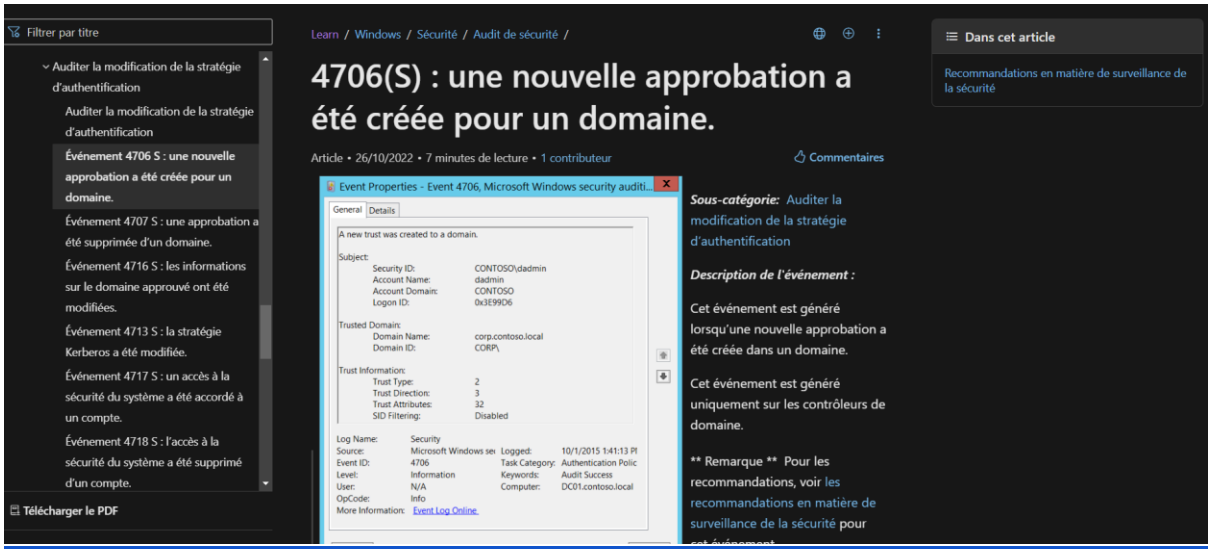
Sources et bibliographie :

Les documents, citations présentes dans ce compte rendu comportent un lien retournant soit sur le document, la vidéo ou bien le site qui traite du sujet. Ce n'est pas le cas pour les screenshots de l'Active Directory et les photos d'écrans.

Source I

Article Wikipédia:
Kerberos
Rapports et matrices:
Listes Ping Castle
Article Wikipédia:
Historique ou journal de log
Vidéo:
Playlist active directory

Article IT Connect :
Active Directory
PingCastle un outil pour auditer l'Activ Directory
Piste I:
Microsoft



Site :
Comment activer les logs d'audits

Sources II

Article Learn Microsoft
Modification de la GPO Kerberos
Article IT Connect
Mot de passe Kerberos
GitHub:
Script du changement du mot de passe Kerberos

Source III

Article IT Connect :
La délégation
Héritage et délégation d'administration
Article Learn Microsoft :
Identificateur de sécurité

Source IV

Site Web:
Qu'est ce qu'un SPN ?
Kerberoast