<<<<

HARDEN AD

Secure your domain in minutes

Harden AD- formation AD cybersécurité

Sommaire

1 Instructions pour démarrer la formation Active Directory

1.1 Les prérequis

Vous devez disposer d'une machine Windows 10 / 11 avec un disque SSD, 150 Go d'espace disque libre et de 8 Go de mémoire (16 Go de mémoire recommandée).

Vous devez disposer des droits d'administration sur cette machine et de la possibilité de modifier les réglages du BIOS.

1.2 Configuration Hyper-V

Pour la réalisation des exercices de cette formation, nous allons déployer la fonctionnalité *Hyper-V* sur la machine.

Activer les instructions de virtualisation de votre machine au niveau du BIOS.

Installer d'Hyper-V sur une machine Windows 10 selon la procédure présentée à cette adresse :

https://www.easytutoriel.com/installer-hyper-v-windows.html

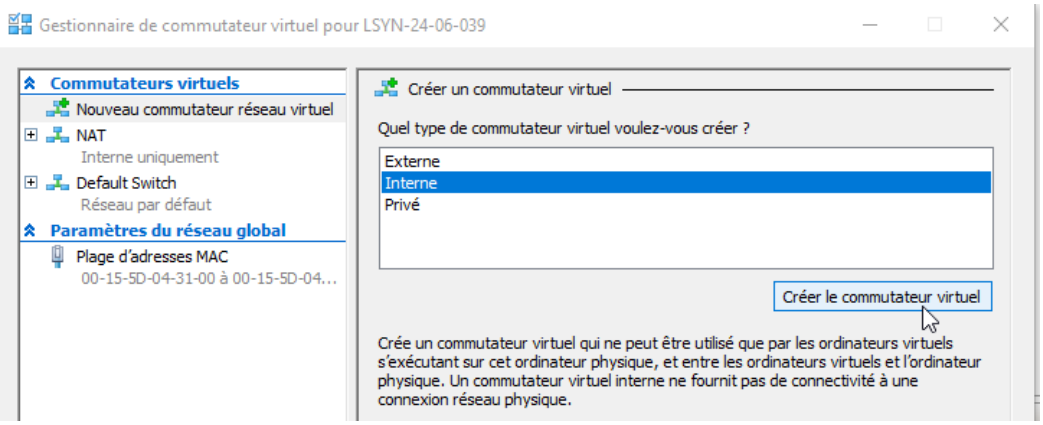
Créer un vSwitch appelé *NAT*.

Assigner à ce vSwitch l'adresse IP suivante : 192.168.140.1/24.

Configurer ce vSwitch pour disposer d'un réseau NAT dédié pour les machines virtuelles de l'environnement de maquette.

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/setup-nat-network

Créer un second vSwitch appelé *Interne* de type Interne.



Désactiver la mémoire dynamique sous Hyper-V

Désactiver les snapshots automatiques.

Vous pouvez suivre la formation Hyper-V du site web RDR-IT pour apprendre à utiliser Hyper-V :

https://rdr-it.com/howto/windows-server-2019-installation-du-role-hyper-v/

1.3 Télécharger les sources d'installation

Télécharger une version d'évaluation de Windows Server 2019 Server / Windows Server 2022 au format ISO à l'adresse suivante : https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2022

Télécharger une version d'évaluation de Windows 10 / 11 Enterprise au format ISO à l'adresse suivante : https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise

Télécharger les sources d'installation d'Exchange 2019 CU11 : https://www.microsoft.com/en-us/download/details.aspx?id=103477

1.4 Préparation de la maquette

Créer les 4 machines virtuelles ci-dessous.

Machine virtuelle DC1 :

- 2 vCPU
- Un disque de 60 Go d'espace disque (mode dynamique).
- Un second disque de 70 Go d'espace disque (mode dynamique)
- 1596 Mo (4096 Mo de mémoire recommandée)
- 1 carte réseau dans le vSwitch "NAT" créé à l'étape précédente.
- OS : Windows Server 2019 ou Windows Server 2022 avec interface graphique.
- La machine doit disposer d'un accès Internet et disposer de toutes les mises à jour de sécurité Windows.
- IP : 192.168.140.10
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.140.1
- Serveur DNS : 192.168.140.10 et 192.168.140.11

Machine virtuelle DC2 :

- 2 vCPU
- 60 Go d'espace disque
- 1596 Mo (4096 Mo de mémoire recommandée)
- 1 carte réseau dans le vSwitch "NAT" créé à l'étape précédente.
- OS : Windows Server 2019 ou Windows Server 2022 avec interface graphique.
- La machine doit disposer d'un accès Internet et disposer de toutes les mises à jour de sécurité Windows.
- IP : 192.168.140.11
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.140.1
- Serveur DNS : 192.168.140.10 et 192.168.140.11

Machine virtuelle RRAS1 :

- 2 vCPU
- 60 Go d'espace disque
- 1596 Mo (4096 Mo de mémoire recommandée)
- Carte réseau 1 dans le vSwitch "NAT" créé à l'étape précédente.
- Carte réseau 2 dans le vSwitch "Interne" créé à l'étape précédente.
- OS : Windows Server 2019 ou Windows Server 2022 avec interface graphique.
- La machine doit disposer d'un accès Internet et disposer de toutes les mises à jour de sécurité Windows.
- IP carte réseau 1 : 192.168.140.254
- Masque de sous réseau carte réseau 1 : 255.255.255.0
- Passerelle carte réseau 1 : 192.168.140.1
- IP carte réseau 2 : 192.168.141.254
- Masque de sous réseau carte réseau 1 : 255.255.255.0
- Passerelle carte réseau 1 : ne rien mettre
- Serveur DNS carte réseau 1 : ne rien mettre

Machine virtuelle VMK1 :

- 2 vCPU
- 60 Go d'espace disque
- 1024 Mo (4096 Mo de mémoire recommandée)
- 1 carte réseau dans le vSwitch "NAT" créé à l'étape précédente.
- OS : Windows 10 Enterprise ou Windows 11 Enterprise.
- La machine doit disposer d'un accès Internet et disposer de toutes les mises à jour de sécurité Windows.
- IP : 192.168.140.13
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.140.1
- Serveur DNS : 192.168.140.10 et 192.168.140.11

2 Notions fondamentales sur Active Directory

2.1 Vue d'ensemble de Windows Server et PowerShell et Active Directory

Vous devez disposer des connaissances générales sur Windows Server, PowerShell et Active Directory

Vous pouvez pour cela suivre les 3 formations gratuites suivantes :

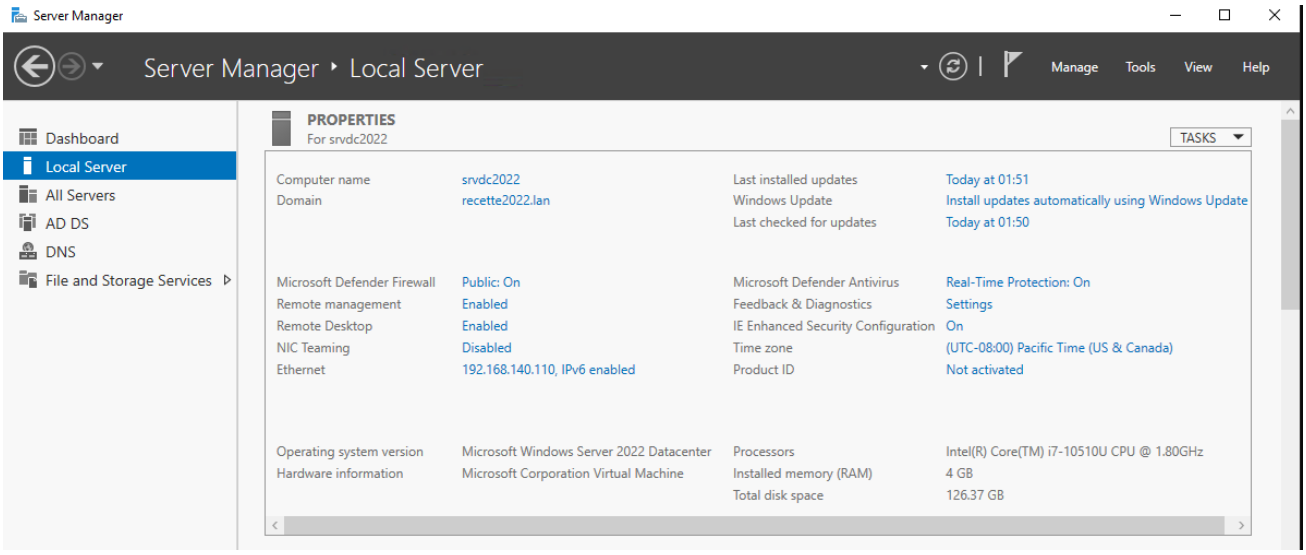
https://openclassrooms.com/fr/courses/2356306-prenez-en-main-windows-server

https://openclassrooms.com/fr/courses/6344196-planifiez-vos-taches-avec-des-scripts-powershell-sur-windows-server

https://rdr-it.com/active-directory/

Depuis le Gestionnaire de Server :

- Activer le bureau à distance avec authentification NLA.
- Installer les mises à jour Windows.
- Configurer le pare-feu Windows pour autoriser les accès RDP.
- Désactiver la protection renforcée Internet Explorer.
- Activer Windows.
- Paramétrer Microsoft Defender Antivirus.
- Installer la fonctionnalité *DFS Management Tools* (*Add roles and features | Remote Server Administration Tools | Roles Administration Tools | File Services Tools*).



Configurer le protocole IPV4 pour être prioritaire sur le protocole IPV6 (entrée de registre *DisabledComponents* à la valeur *32* (valeur décimale).

https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/configure-ipv6-in-windows

2.2 Choix du nom de domaine

Le nom du domaine ne doit pas contenir de caractères spéciaux comme le "_".

Exemple de nom DNS : *internal.harden.world*

Exemple de nom NETBOS : *INTHARDEN*

Dans la mesure du possible, il faut éviter d'utiliser le nom de l'entreprise dans le nom du domaine.

Il n'est pas possible de renommer un domaine. L'outil RENDOM est à proscrire.

https://redkaffe.com/2016/04/20/rendom-exe-ou-comment-renommer-son-adds/

Si vous utilisez un nom DNS résolvable par les serveurs DNS Internet (*HARDENAD.NET* par exemple), vous devez enregistrer ce domaine sur Internet.

Le nom DNS du domaine doit toujours contenir une extension (*harden.world*).

Si le nom de domaine DNS ne contient pas d'extension (Single Label DNS Name), appliquer cette procédure :

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/single-label-domains-support-policy

2.3 Création du domaine Active Directory FORMATIONXX.LAN

Configurer les machines DC1 et DC2 en tant que contrôleur de domaine et créer une forêt avec un domaine appelé *FORMATIONXX.INTRA* (où *XX* correspond à vos initiales).

Créer le domaine en mode natif 2008 R2.

Vous pouvez pour cela utiliser l'interface graphique ou PowerShell.

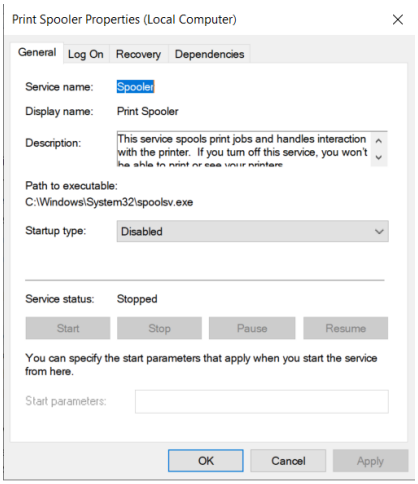
https://rdr-it.com/ajouter-un-controleur-de-domaine-ad-ds-dans-un-domaine-existant/

https://rdr-it.com/active-directory-ajouter-un-controleur-de-domaine-en-powershell/

2.4 Service spouleur d'impression

Les contrôleurs de domaine ne doivent pas être serveur d'impression : https://adsecurity.org/?p=4056

Si le contrôleur de domaine est serveur d'impression, migrer les imprimantes sur un serveur membre du domaine (qui n'est pas contrôleur du domaine).



2.5 Configuration du serveur d'administration en tant que machine membre du domaine

Configurer la machine WK01 en tant que membre du domaine.

https://rdr-it.com/joindre-un-ordinateur-a-un-domaine-windows-10-2016/

Installer les RSAT AD / AD LDS sur cette machine pour pouvoir gérer votre annuaire Active Directory depuis une machine Windows 10.

https://www.microsoft.com/en-us/download/details.aspx?id=45520

2.6 Déploiement de la sauvegarde Windows Server backup sur DC1

La sauvegarde Active Directory ne doit pas se faire avec des snapshots (surtout avec les anciennes versions de Windows Server). Dans le cas contraire, vous pouvez rencontrer des problèmes d'*USN ROOLBACK*.

https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/detect-and-recover-from-usn-rollback

Configurer Windows Server Backup pour effectuer une sauvegarde complète de DC1 (Etats du système, disque C, fichier de démarrage) vers le disque de 70 Go.

Ce dernier doit être exclu de la sauvegarde et sera reformaté.

Lancer le Gestionnaire de disque.

Vous noterez que le disque de 70 Go ne dispose pas de lettres de lecteur.

Les instructions pour déployer Windows Server Backup sont disponibles à cette adresse :

https://rdr-it.com/windows-backup-installation-et-configuration/

2.7 Le niveau fonctionnel du domaine et de la forêt

Active Directory permet de configurer un niveau fonctionnel pour le domaine et pour la forêt.

C'est le contrôleur du domaine avec la version la plus ancienne qui définit le niveau fonctionnel.

Un domaine AD en mode natif 2019 peut avoir des machines membres avec des OS anciens comme NT4 et Windows 2000 (si les paramètres de sécurité sont configurés pour supporter ces anciennes machines).

Le fait d'augmenter le niveau fonctionnel permet de bénéficier de nouvelles fonctionnalités :

- Le passage en mode 2008 R2 permet de disposer des nouveaux algorithmes de dérivation de clés Kerberos.
- A partir du mode natif 2008 R2, il est possible d'activer la corbeille Active Directory.
- A partir du mode natif 2008 R2, il est possible de monter ou descendre le mode fonctionnel de domaine et forêt.
- A partir du mode natif 2012 R2, le groupe *Protected Users* fonctionne.

Procédures de mise en œuvre :

https://www.it-connect.fr/chapitres/les-cinq-roles-fsmo/

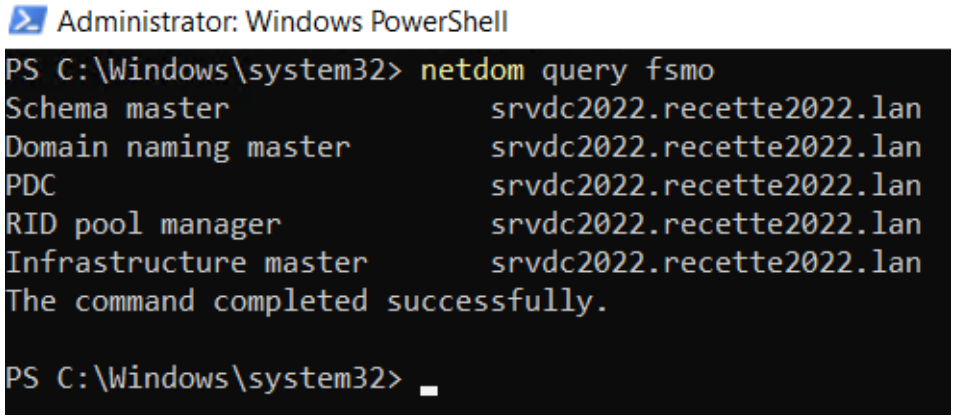
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels
https://azurecloudai.blog/2019/10/23/downgrading-active-directory-domain-and-forest-functional-levels-part-1/
https://azurecloudai.blog/2019/10/30/downgrading-active-directory-domain-and-forest-functional-levels-part-2/
https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/active-directory-functional-levels

Le mode natif 2008 permet d'activer les algorithmes de dérivation de clés AES 128 et AES 256.
Ce cas de problème, il sera nécessaire de désactiver ces algorithmes via la GPO *Configurer les types de chiffrement autorisées pour Kerberos*.
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos

A partir du mode natif 2008 R2, un retour arrière est possible (passage du mode natif 2016 au mode natif 2008 R2).
https://azurecloudai.blog/2019/10/30/downgrading-active-directory-domain-and-forest-functional-levels-part-2/

2.8 Les rôles FSMO

Active Directory dispose de 5 rôles FSMO.
Lancer la commande *NETDOM QUERY FSMO* pour vérifier que les rôles FSMO sont disponibles.



Pour plus d'informations sur ces 5 rôles :
https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles

Si vous disposez de plusieurs versions d'OS Windows, les rôles FSMO doivent être sur l'OS le plus récent.
La communauté Harden vous préconise d'héberger les rôles FSMO sur un contrôleur de domaine physique.

Transférer les rôles FSMO via les consoles MMC, PowerShell et l'outil NTDSUTIL sur le serveur DC2 puis les transférer de nouveau sur DC1.
https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/view-transfer-fsmo-roles
https://www.it-connect.fr/transfert-des-roles-fsmo-avec-ntdsutil/

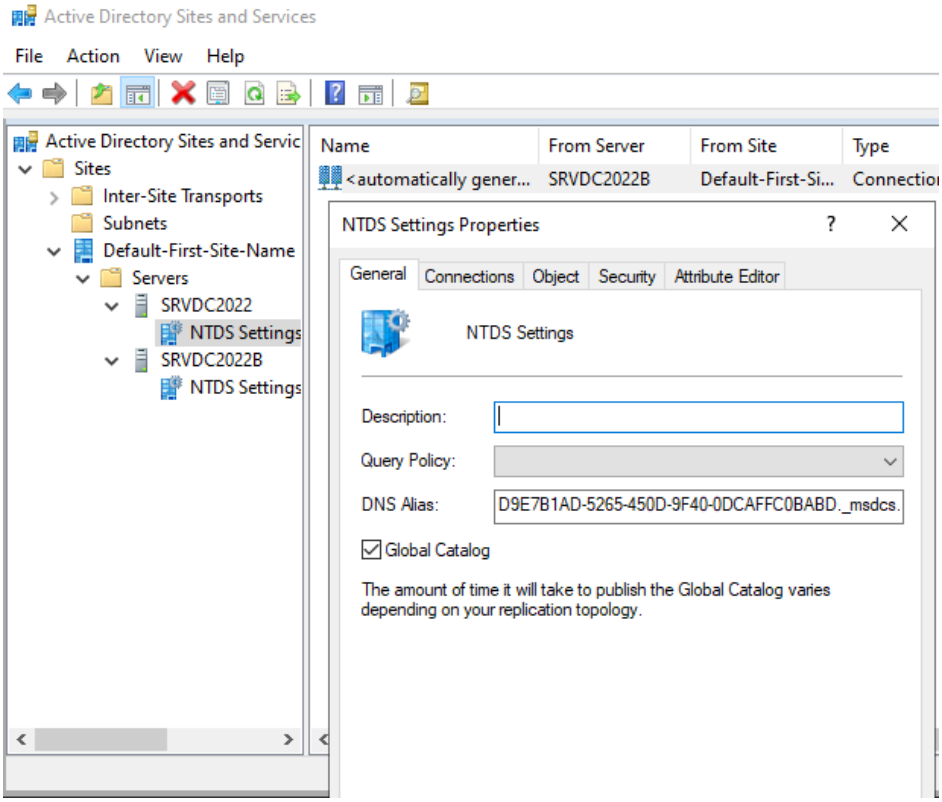
2.9 Le Catalog Global

L'intérêt du *serveur de Catalog Global* (résolution des groupes universelles principalement, optimisation des requêtes dans les forêts avec plusieurs domaines) est présenté en détail dans l'article ci-dessous :

https://www.it-connect.fr/chapitres/a-la-decouverte-du-catalogue-global/

Lancer la console *Sites et Services Active Directory*.

Vérifier que tous les contrôleurs de domaine sont *serveur de Catalogue Global*.



Quand plus aucun serveur de Catalog Global n'est disponible au niveau de la forêt, les utilisateurs ne peuvent plus ouvrir de session sur le domaine.

Pour cette raison, la communauté Harden vous préconise de configurer tous les contrôleurs de domaine en tant que serveur de *Catalog Global*.

Lancer la console Active Directory Sites and Services et configurer DC2 pour ne plus être Catalog Global via l'interface graphique. Faire ensuite l'opération inverse en PowerShell.

https://www.dtonias.com/enable-disable-global-catalog-server/

2.10 Synchronisation horaire

Le contrôleur de domaine avec le rôle FSMO *PDC Emulator* du domaine racine doit se synchroniser avec une source de temps externe comme *time.windows.com*.

Idéalement, ce contrôleur de domaine doit être une machine physique car les machines virtuelles peuvent rencontrer des problèmes de décalage de temps.

Toutes les autres machines du domaine devront se synchroniser via le processus standard Windows (NT5DS) et se synchroniser directement ou indirectement avec le contrôleur de domaine avec le rôle FSMO *PDC Emulator* du domaine racine.

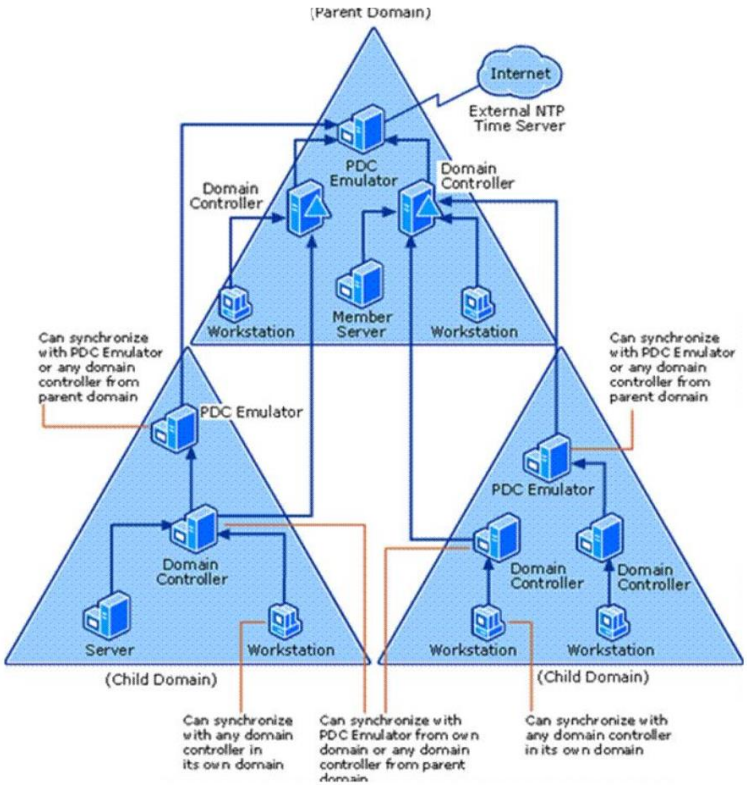
Sur le contrôleur de domaine avec le rôle *PDC Emulator* du domaine racine de la forêt :

```
w32tm /config /manualpeerlist:time.windows.com,0x8 /syncfromflags:manual /reliable:yes
/update
w32tm /resync /rediscover
net stop w32time
net start w32time
```

Sur les autres contrôleurs de domaine et machines membres du domaine :

```
net stop w32time
w32tm /unregister
w32tm /register
net start w32time
w32tm /config /syncfromflags:domhier /update
net stop w32time
net start w32time
```

Le schéma ci-dessous explique le fonctionnement de la synchronisation horaire Windows.



Lire ces 2 articles qui expliquent ce processus en détail.

https://www.renanrodrigues.com/post/how-to-configure-ntp-server-in-active-directory-step-by-step

https://teddycorp.net/ad-set-w32tm/

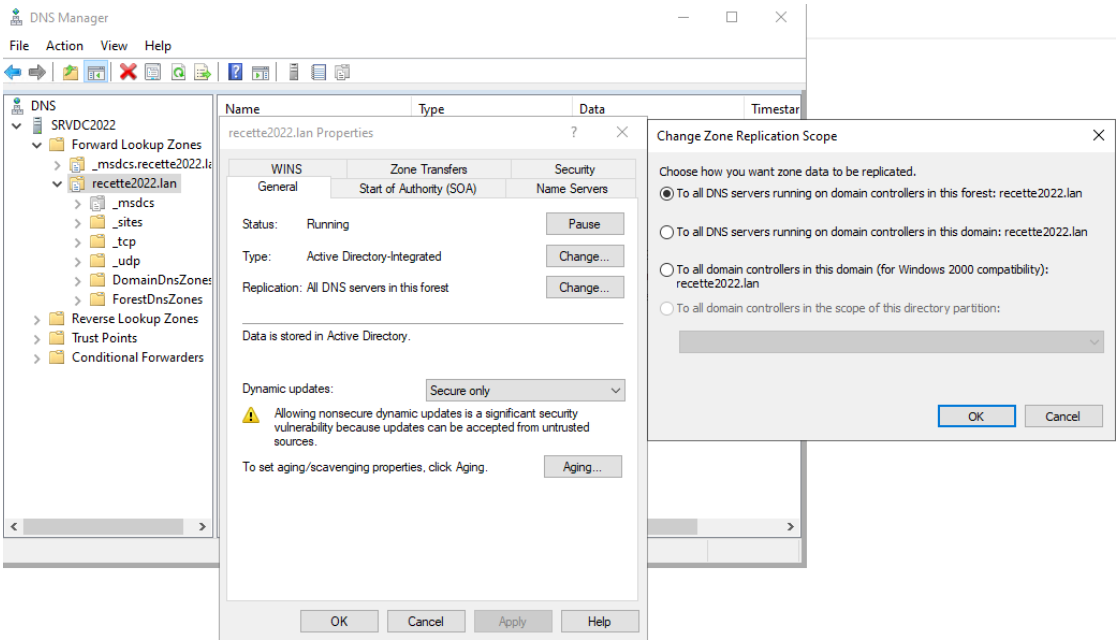
2.11 Configuration des zones DNS

Configurer tous les zones DNS intégrées dans l'annuaire AD pour répliquer sur tous les contrôleurs de tous les domaines de la forêt. Cela consiste à stocker toutes les zones DNS dans la partition Active Directory appelée *ForestDNSzones*.

Cela permettra que les zones DNS apparaissent sur tous les contrôleurs de tous les domaines de la forêt.

Le but est d'éviter des problèmes de réplication dans les environnements avec 1 forêt et plusieurs domaines.

Lancer la console DNS Manager. Aller dans les propriétés de la zone DNS et configurer *Replication* sur *All DNS servers in this forest*.

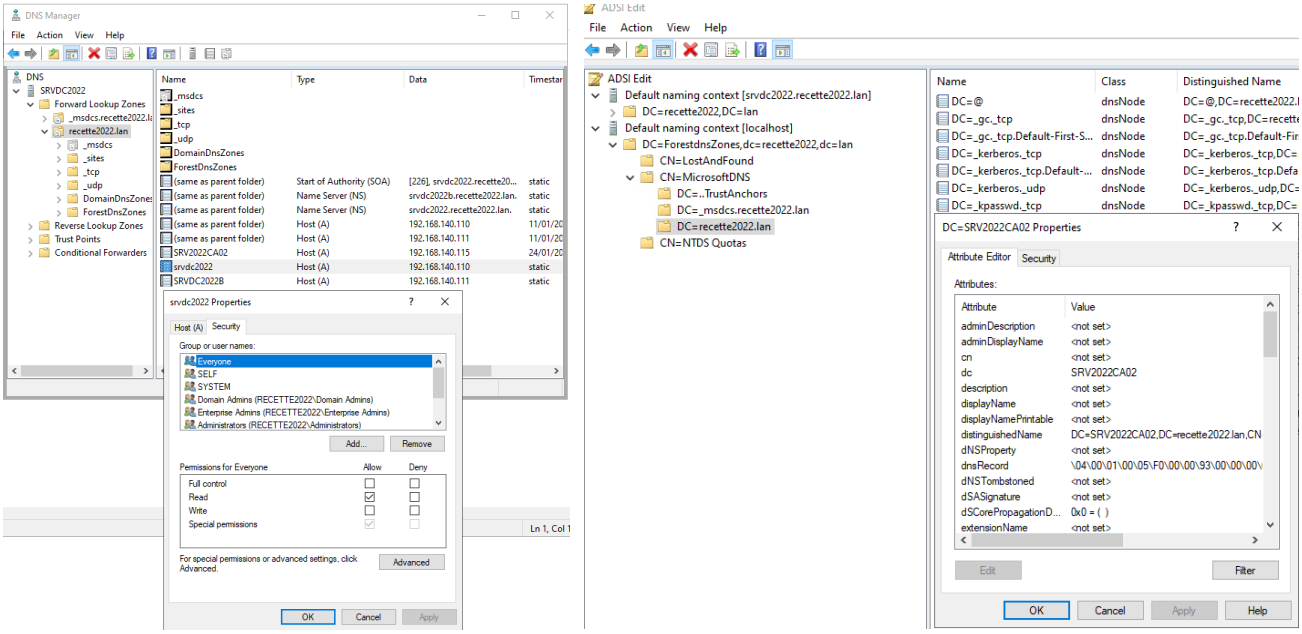


Configurer ensuite les zones DNS *Active Directory-Integrated* pour n'autoriser que les mises à jour dynamiques sécurisées.

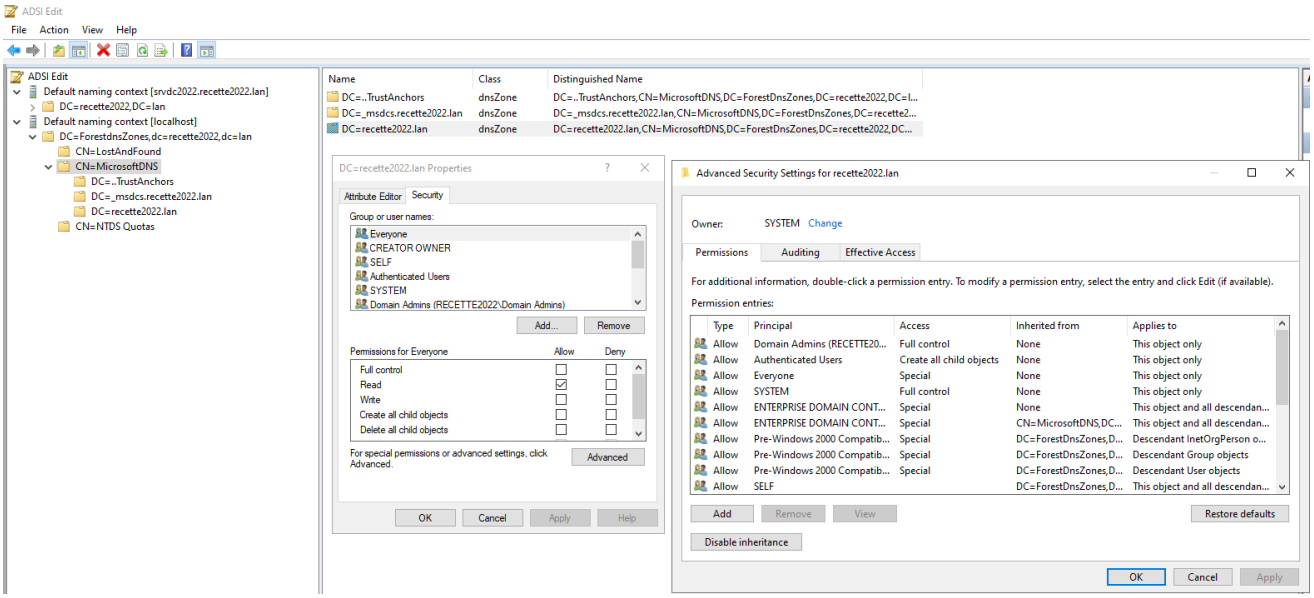
Lancer la console ADSIEDIT.MSC.

Chaque zone DNS intégrée à l'annuaire AD est un objet *dnsZone*.

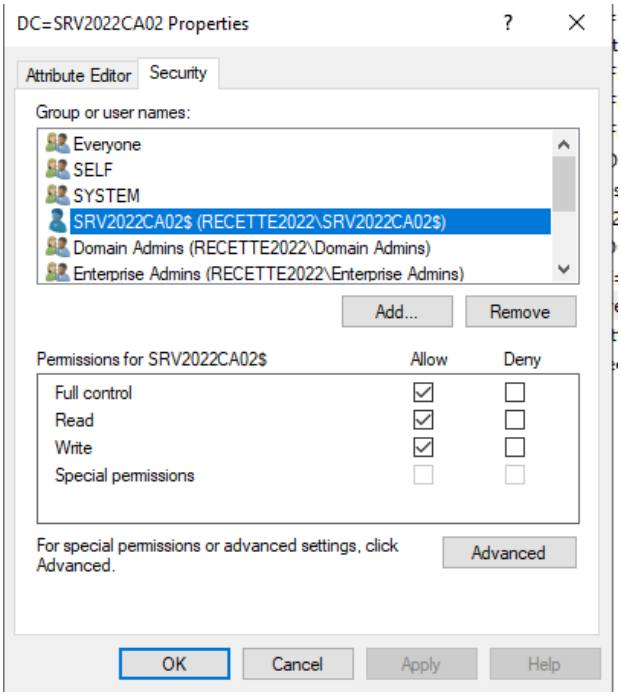
Chaque entrée DNS d'une zone DNS intégrée à l'annuaire AD est un objet *dnsNode*.



Chaque entrée DNS dispose donc d'ACL comme tous les autres objets Active Directory.



Cela permet par exemple que celle la machine SRV2022CA02 du domaine RECETTE2022.LAN puisse mettre à jour l'entrée DNS *SRV2022CA02.RECETTE2022.LAN*.



Le fait de changer ce paramètre peut générer des problèmes avec les serveurs DHCP qui peuvent avec un accès refusé lors qu'ils mettent à jour eux-mêmes les entrées DNS.

Il peut être utile d'ajouter le droit d'écrire de modifier les entrées DNS aux comptes ordinateurs correspondant aux serveurs DHCP.

Lire les 3 articles ci-dessous qui expliquent les problèmes de permissions avec le service DNS / DHCP :

http://msreport.free.fr/?p=208

http://msreport.free.fr/?p=429

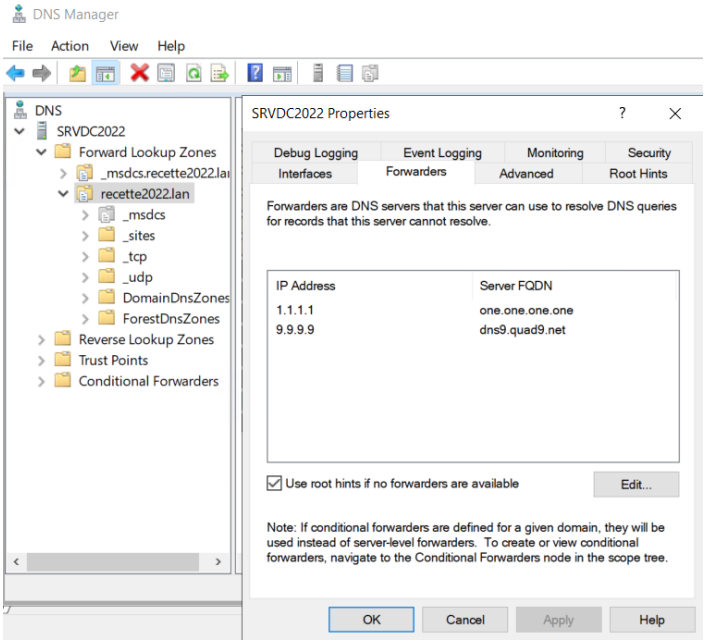
https://blogs.msmvps.com/acefekay/2009/09/02/using-adsi-edit-to-resolve-conflicting-or-duplicate-ad-integrated-dns-zones/

2.12 Configurer tous les contrôleurs de domaine en tant que serveur DNS et avec 1.1.1.1 et 9.9.9.9 comme serveur redirecteurs

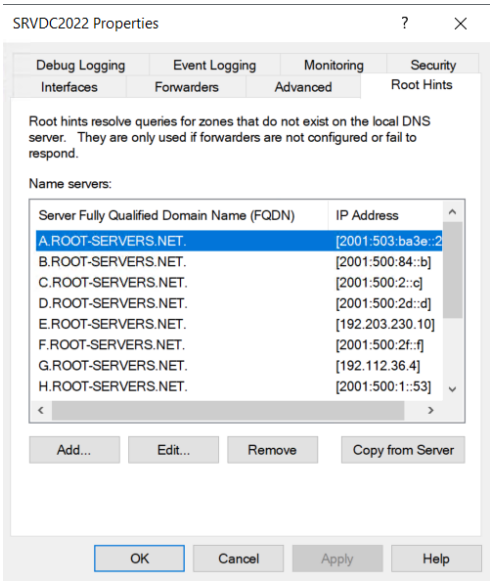
Quand un serveur DNS ne dispose pas de la zone DNS pour laquelle il doit résoudre un nom, il redirige cette demande vers un serveur de redirection.

Pour plus d'informations, voir la slide 22 du guide http://msreport.free.fr/articles/AdministrationAD.pdf.

Configurer DC1 et DC2 avec *1.1.1.1* et *9.9.9.9* comme serveurs DNS redirecteurs.



Les serveurs contrôleurs de domaine (qui sont aussi serveur DNS) doivent disposer d'un redirecteur DNS valide. S'il n'y en a pas, ce sont les serveurs racines DNS (présents dans l'onglets indications de racine) qui sont utilisés.



Par défaut, un nouveau contrôleur de domaine définit comme serveur DNS le contrôleur de domaine que vous avez défini comme serveur DNS principal lors du paramétrage de ce serveur en tant que contrôleur de domaine. Quand vous supprimez ce serveur, la résolution de nom ne se fait plus.

Appliquer pour cela la procédure ci-dessous :
https://rdr-it.com/dns-configuration-dun-redirecteur/

2.13 Mise à jour du schéma pour Exchange 2019

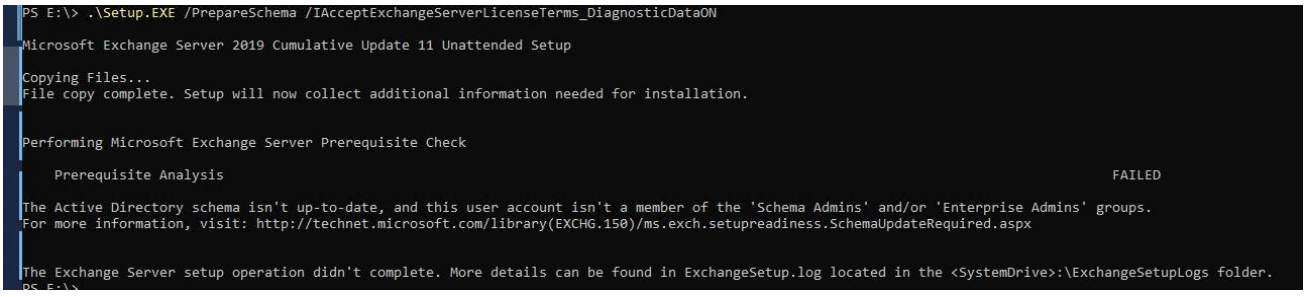
Mettre à jour le schéma Active Directory avec les extensions de schéma d'Exchange 2019 permet de disposer de nouveaux attributs comme *ExtensionAttribute1*. Ces attributs peuvent être intéressants pour stocker certaines informations.

Avant de mettre à jour le schéma Active Directory, vous devez tout d'abord apprendre à désactiver / réactiver la réplication AD : https://www.techieshelp.com/disable-enable-ad-replication/

En effet, la mise à jour du schéma Active Directory est une opération risquée qui n'est pas réversible (annulable). Windows Server 2022 ne prend pas en charge Exchange 2019 par exemple :
https://docs.microsoft.com/fr-fr/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019

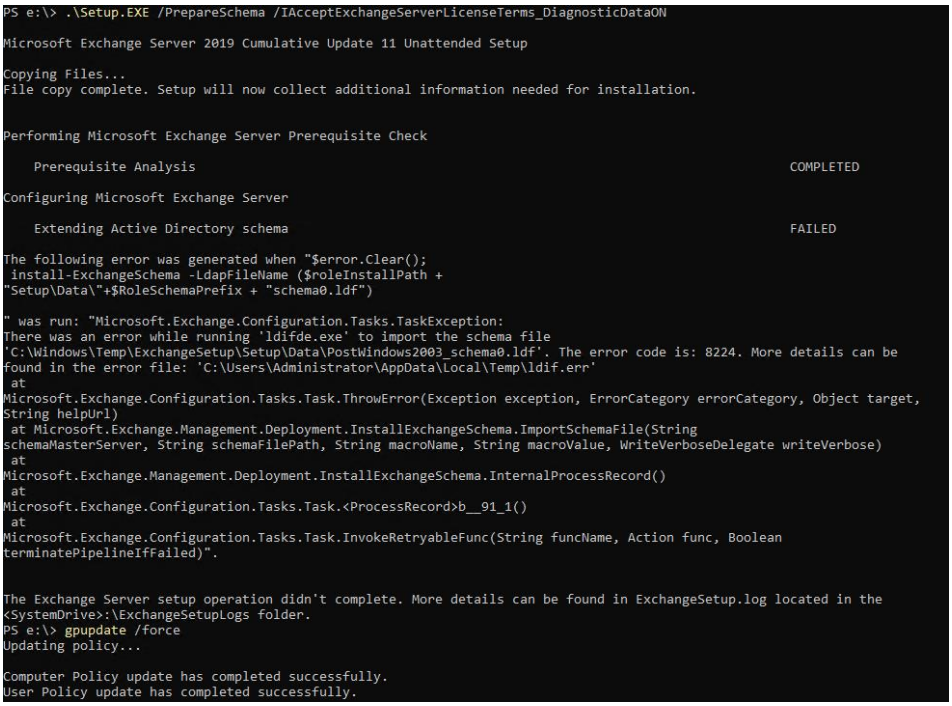
Télécharger les sources d'Exchange 2019 CU 11.
Les sources des CU Exchange 2019 sont en effet des installations complètes (5,8 Go).
https://www.microsoft.com/en-us/download/details.aspx?id=103477

Monter l'ISO.
Se connecter sur le contrôleur de domaine avec le rôle FSMO de maître de schéma.
Désactiver la réplication AD sur ce dernier.
Ajouter votre compte utilisateur en tant que membre des groupes *Enterprise Admins* et *Schema Admins*.
Penser à fermer et rouvrir votre session pour que les appartenances aux groupes soient prises en compte.
Dans le cas contraire, ce message apparaîtra.



Taper la commande suivante :
.\Setup.EXE /PrepareSchema /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

L'erreur ci-dessous apparaît, si le contrôleur de domaine ne peut pas répliquer avec un contrôleur de domaine.



Connecting to "srvdc2022.recette2022.lan"

Logging in as current user using SSPI

Importing directory from file "C:\Windows\Temp\ExchangeSetup\Setup\Data\PostWindows2003_schema0.ldf"

Loading entries

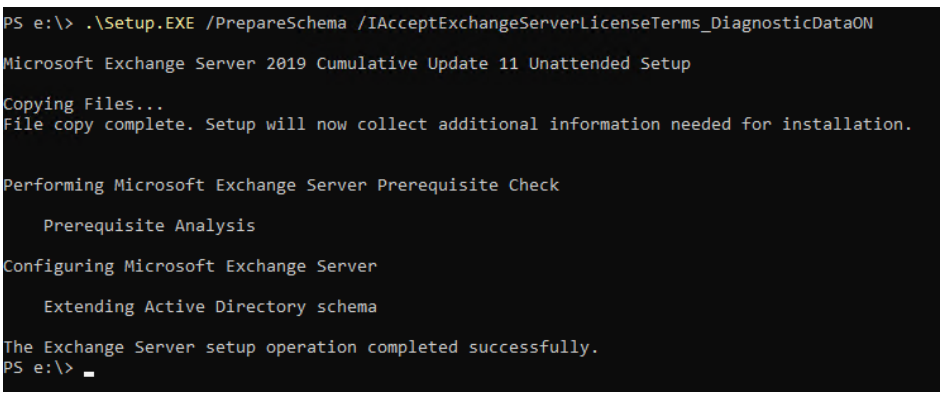
1: CN=ms-Exch-Access-Control-Map,CN=Schema,CN=Configuration,DC=recette2022,DC=lan

Entry DN: CN=ms-Exch-Access-Control-Map,CN=Schema,CN=Configuration,DC=recette2022,DC=lan

Add error on entry starting on line 1: Operations Error

The server side error is: 0x21a2 The FSMO role ownership could not be verified because its directory partition has not replicated successfully with at least one replication partner.

Le message suivant apparaît quand la mise à jour du schéma est réussie.



2.14 Configuration de la réplication inter-sites AD

Lire le guide RDR-IT sur les topologies avec plusieurs sites Active Directory.
https://rdr-it.com/active-directory-configuration-multi-sites-sous-reseau-et-replication/

Démarrer la machine RRAS1 et configurer cette machine comme un routeur.
https://msftwebcast.com/2020/02/configure-lan-routing-in-windows-server-2019.html

Configurer ensuite la carte réseau de la machine DC2 dans le vSwitch Interne et changer sa configuration réseau.

- IP : 192.168.141.11
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.141.254
- Serveur DNS : 192.168.140.10 et 192.168.141.11

Renommer le premier site AD par défaut en Paris.

Créer un nouveau site AD appelé *Tours* et configurer DC2 dans ce site.

Ajouter le sous réseau IP 192.168.141.0/24 et l'associer au site Tours.

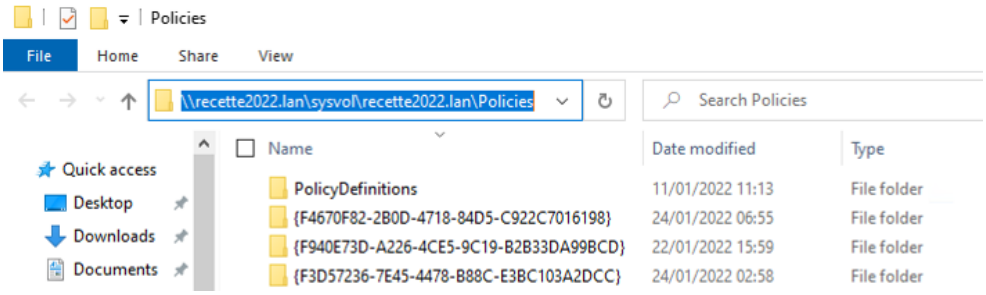
Créer le lien de site entre Paris et Tours.

Vérifier le bon fonctionnement de la topologie de sites AD.

Configurer ensuite les liens de transport inter-sites avec le paramètre *Change notification* :
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961787(v=technet.10)?redirectedfrom=MSDN
Cela permet d'accélérer la réplication des objets entre 2 contrôleurs de domaine qui sont dans 2 sites AD différents. En effet, c'est le trafic d'authentification (entre un client et un contrôleur de domaine) qui génère du trafic réseau. Le trafic réseau requis par la réplication AD consomme peu de bande passante.

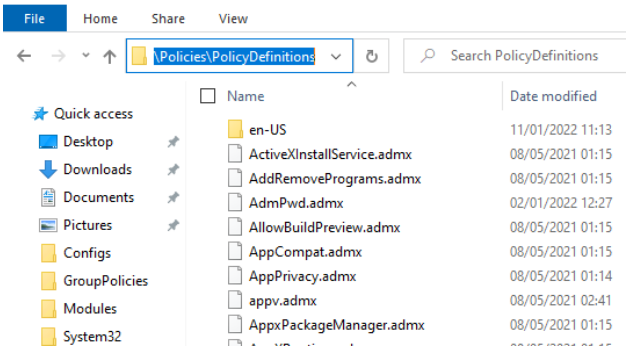
2.15 Activation du central Store

Les GPO sont des entrées de registre que les machines du domaine vont télécharger en se connectant sur \\nomdudomaine.dns\sysvol\nomdudomaine.dns\Policies.
Exemple pour le domaine *recette2022.lan* : \\recette2022.lan\sysvol\recette2022.lan\Policies



L'éditeur de stratégie de groupe s'appuie sur des fichiers ADMX / ADML pour permettre aux administrateurs de paramétrer simplement ces entrées de registre.

Ce mode de fonctionnement permet à des éditeurs tiers de créer des fichiers ADMX et ADML supplémentaires pour étendre les GPO.



Configurer l'éditeur de GPO pour utiliser le magasin central (central Store) selon la procédure ci-dessous :

https://rdr-it.com/magasin-central-mise-en-place/

2.16 Déployer la solution Microsoft LAPS pour modifier le mot de passe du compte administrateur par défaut de la base SAM sur les machines membres du domaine

Lire l'article https://rdr-it.com/laps-securisation-comptes-administrateur-local-installation-configuration/

Microsoft LAPS va mettre à jour le schéma Active Directory.

Il sera donc nécessaire d'appliquer la même méthodologie que pour la mise à jour du schéma Exchange 2019 CU11.

Télécharger Microsoft LAPS et le déployer la dll sur WK1.

https://www.microsoft.com/en-us/download/details.aspx?id=46899

2.17 Valider le bon fonctionnement de votre annuaire Active Directory et son niveau de sécurité

Lancer une invite de commande PowerShell (en tant qu'administrateurs pour ne pas être limité par l'UAC) et taper la commande *DCDIAG /v /e | Out-File -Append -FilePath c:\DCDIAG.TXT -Encoding UTF8* sur un de vos DC. Cet outil permet de tester le bon fonctionnement de l'annuaire Active Directory (réplication, services démarrés...).

Lancer la console Gestionnaire de Server et générer un *Best Practice Analyser* pour le rôle Active Directory.

2.18 Lister les comptes utilisateurs et ordinateurs inactifs

Vous pouvez vous appuyer sur le module PowerShell Active Directory pour lister les comptes utilisateurs non utilisés, lister les membres des principaux groupes d'administration ou lister les machines membres du domaine avec des versions d'OS non supportés.
Des exemples de scripts sont disponibles gratuitement depuis :
https://gallery.technet.microsoft.com/scriptcenter/Active-Directory-Reports-bb8c1cc7
https://github.com/edemilliere/BasicADReport/blob/master/ADReport.ps1
https://www.thelazyadministrator.com/2018/12/04/get-an-active-directory-interactive-html-report-with-powershell/

2.19 Bilan de sécurité de l'annuaire Active Directory avec Ping Castle

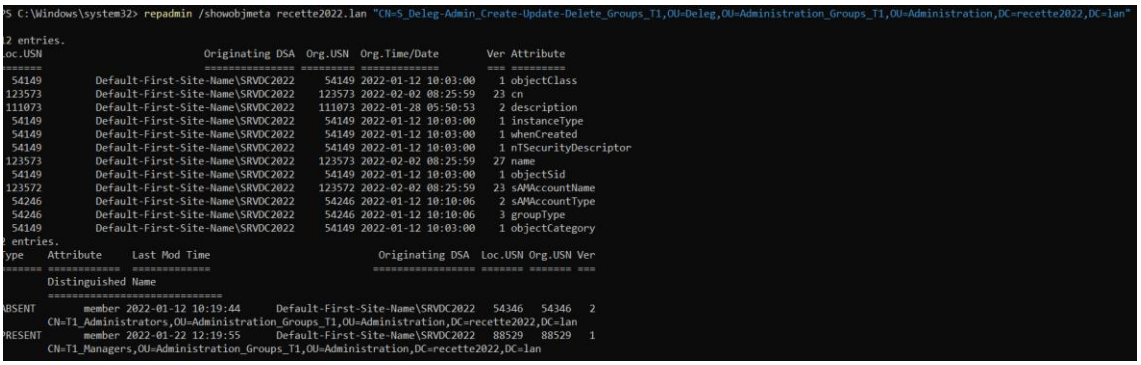
Lancer l'outil Ping Castle pour effectuer un bilan de sécurité de votre annuaire Active Directory.
https://www.pingcastle.com/

2.20 Bilan de sécurité avec l'outil de l'ANSSI ADTIMELINE et les métadonnées de chaque objet AD

Lancer la commande suivante

```
repadmin /showobjmeta recette2022.lan "CN=S_Deleg-Admin_Create-Update-Delete_Groups_T1,OU=Deleg,OU=Administration_Groups_T1,OU=Administration,DC=recette2022,DC=lan"
```

Elle permet de voir tous les changements effectués sur le groupe *S_Deleg-Admin_Create-Update-Delete_Groups_T1*.



Lancer ensuite l'outil AD Timeline.
https://github.com/ANSSI-FR/ADTimeline
https://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-ad_timeline.pdf

La vidéo ci-dessous explique comment fonctionne l'outil ADTIMELINE.
https://www.youtube.com/watch?v=N7tnKuXbpiQ&ab_channel=FIRST

2.21 Notions avancées

2.21.1 Un peu de lecture

Lire ensuite le guide *Tester la sécurité de son annuaire Active Directory*.
http://msreport.free.fr/articles/Securite-AD/TESTER_SECURITE_ACTIVE_DIRECTORY_V_2.0.pdf

Lire le guide d'administration de l'annuaire Active Directory.
http://msreport.free.fr/articles/AdministrationAD.pdf

Pourquoi il n'est pas recommandé de créer des forêts avec plusieurs domaines ?
Réponse : le groupe *AUTHENTICATED USERS* (tous les comptes utilisateurs et ordinateurs de la forêt) a des accès dans tous les domaines de la forêt.

2.21.2 Suffixe UPN

Ajouter le suffixe UPN *harden.world*.

Créer votre compte utilisateur avec comme suffixe UPN *harden.world*.

Créer un second utilisateur avec le module PowerShell Active Directory.
https://docs.microsoft.com/en-us/powershell/module/activedirectory/new-aduser?view=windowsserver2022-ps

2.21.3 Objet MSA et GMSA

Les objets MSA ou GMSA permettent de remplacer les comptes utilisateurs pour démarrer des services.
Toutes les applications ne prennent pas en charge les GMSA ou MSA. Il faut donc valider la compatibilité de ce type de comptes avant toute utilisation.
https://www.it-connect.fr/active-directory-utilisation-des-gmsa-group-managed-service-accounts/

Installer SQL Server 2019 sur une machine membre du domaine et configurer cette application pour utiliser un MSA comme compte de service.
https://www.mssqltips.com/sqlservertip/5334/using-managed-service-accounts-with-sql-server/

Les sources de SQL Server 2019 peuvent être télécharger à cette adresse :
https://www.microsoft.com/fr-fr/evalcenter/evaluate-sql-server

2.21.4 Comment les machines du domaine localisent leur contrôleur de domaine ?

Ouvrir une session sur WK1 et taper la commande *ipconfig /displaydns*. Comment une machine du domaine localise t'elle son contrôleur de domaine ?
Voir slide 27 du guide http://msreport.free.fr/articles/AdministrationAD.pdf.

Ouvrir le fichier *C:\Windows\System32\Config\Netlogon.dns* sur DC1.
Supprimer toutes les entrées DNS dans la zone *FORMATIONXX.LAN*.
Taper les commandes suivantes :


```
Ipconfig /registerdns
Net stop netlogon
Net start netlogon
```

Les entrées DNS sont chargées de nouveau. Pourquoi ?

2.21.5 Tombstone Life Time et Lingering Object

Que se passe t'il quand 2 contrôleurs de domaine ne répliquent pas pendant plus de 180 jours (60 jours si l'annuaire a été créé avec des contrôleurs de domaine sous Windows 2000 Server) ? Paramétrer la *Tombstone Life Time* sur 120 jours puis faire un retour arrière sur 180 jours.

Qu'est-ce qu'un objet *Lingering* ?

Indexer un attribut dans le Catalog Global

Indexer l'attribut *Title* dans le Catalog Global. Quel est l'intérêt de cette action ?

Voir slide 57 du guide http://msreport.free.fr/articles/AdministrationAD.pdf.

2.21.6 Corbeille Active Directory

La corbeille Active Directory permet de restaurer des objets supprimés.

Les objets supprimés passent tout d'abord dans la corbeille puis sont déplacés dans le conteneur ISDELETED (conteneur caché).

https://rdr-it.com/activer-corbeille-active-directory-windows-2012-2016-2019/

2.21.7 Configuration du conteneur par défaut pour les comptes ordinateurs et les comptes utilisateurs

Par défaut, les nouveaux comptes utilisateurs sont ajoutés dans le conteneur *Users*.

Par défaut, les nouveaux comptes ordinateurs sont ajoutés dans le conteneur *Computers*. C'est le cas quand nous joignons une machine dans le domaine sans avoir précréé son compte ordinateur.

Les conteneurs ne sont pas des unités d'organisations.

Il n'est pas possible de lier des GPO sur des conteneurs.

Pour cette raison, il est préconisé de créer une OU appelé *Provisionning* et de configurer Active Directory pour utiliser cette unité d'organisation comme emplacement par défaut pour les nouveaux comptes ordinateurs et utilisateurs.

https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/redirect-users-computers-containers

2.21.8 Relation d'approbation

Configurer DC2 en tant que serveur membre (suppression du rôle contrôleur de domaine).

Configurer DC2 en tant que contrôleur de domaine d'une nouvelle forêt avec un domaine appelé RESSOURCEXX.LAN.

Créer une relation d'approbation entre *FORMATIONXX.LAN* et *RESSOURCEXX.LAN*.

https://rdr-it.com/active-directory-relation-approbation-entre-deux-forets-domaines/

2.21.9 Migration des contrôleurs de domaine vers une nouvelle version de Windows Server

Pour pouvoir intégrer un contrôleur de domaine Windows Server 2019 / 2022 dans une forêt existante gérée par des contrôleurs de domaine avec une version antérieure de Windows, il est nécessaire d'effectuer les actions suivantes :

- Mise à niveau du schéma Active Directory avec la commande ADPREP /FORESTPREP
- Préparation du domaine avec la commande ADPREP / DOMAINPREP
- Ajout du ou des nouveaux contrôleurs de domaine Windows Server 2019 / 2022.
- Augmentation du niveau fonctionnelle du domaine et de la forêt (si applicable).
- Suppression des anciens contrôleurs de domaine

2.21.10 Migration de ressources entre 2 domaines

ADMT 3.2 permet de migrer des ressources entre 2 domaines Active Directory.

Il est cependant à noter que cet outil ne fonctionne plus avec les machines Windows 10.

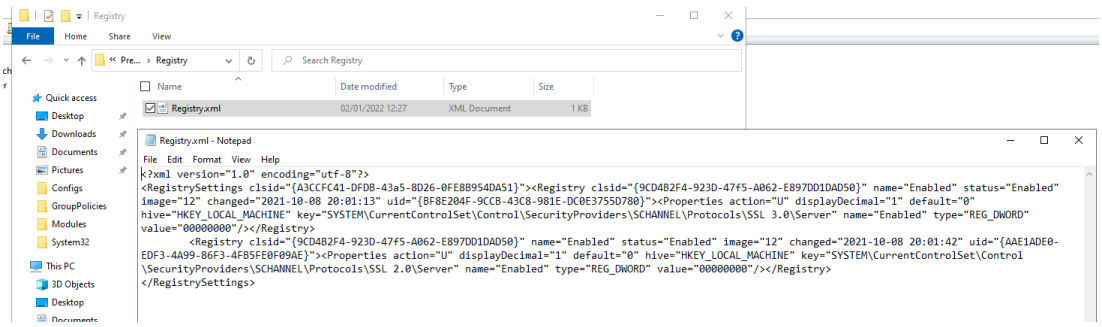
https://rdr-it.com/admt-outil-de-migration-de-domaine-active-directory/

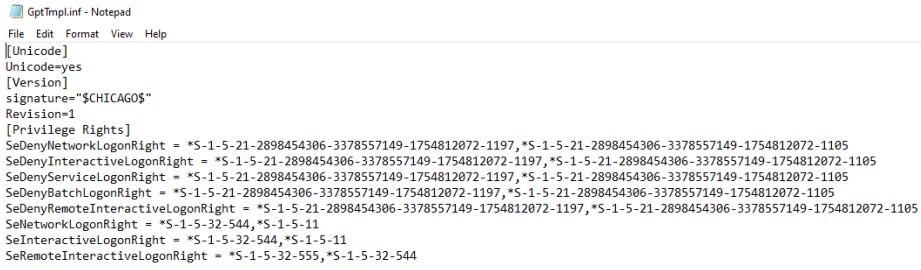
Il faudra utiliser un outil payant comme *Quest Migration Manager*.

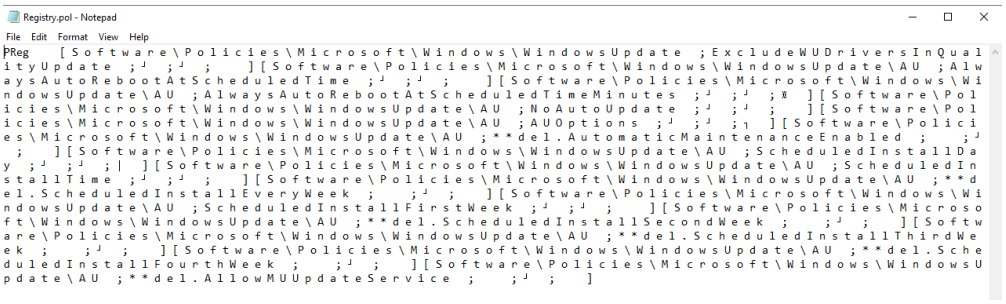
L'utilisation du *SID History* permet de migrer avec de la coexistence mais présente un risque de sécurité (voir paragraphe sur les attaques).

2.21.11 Comprendre le fonctionnement du dossier SYSVOL

Lorsqu'un ordinateur se connecte à l'annuaire Active Directory (il s'authentifie automatiquement après le chargement de la carte réseau), il applique les GPO qui sont liés au conteneur / unité d'organisation où il est placé. Une fois la liste des GPO récupérées, la machine va faire une requête dans l'AD pour déterminer où se trouve les fichiers des GPO (fichiers registry.xml, *GptTmpl.inf, Registry.pol*).



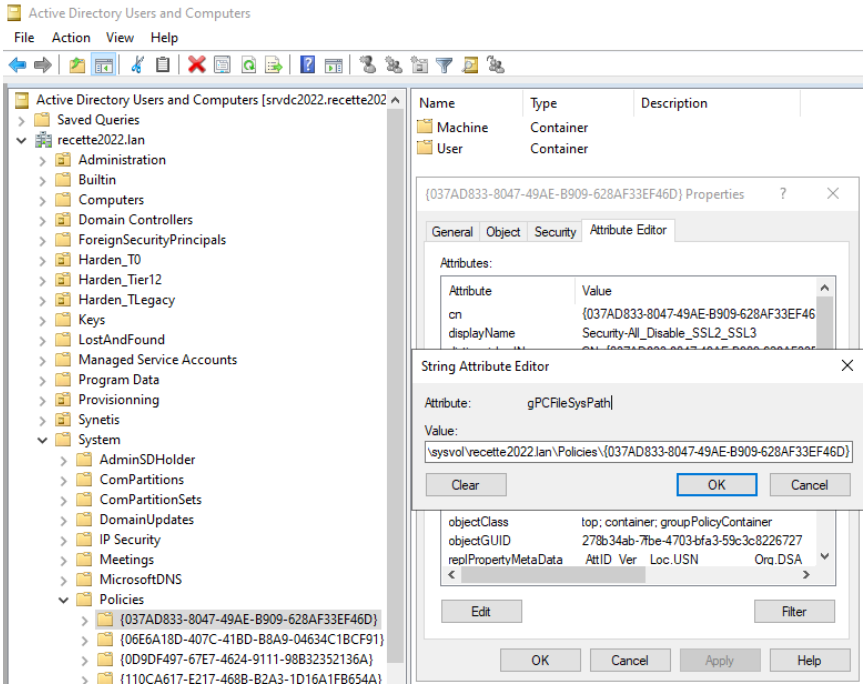




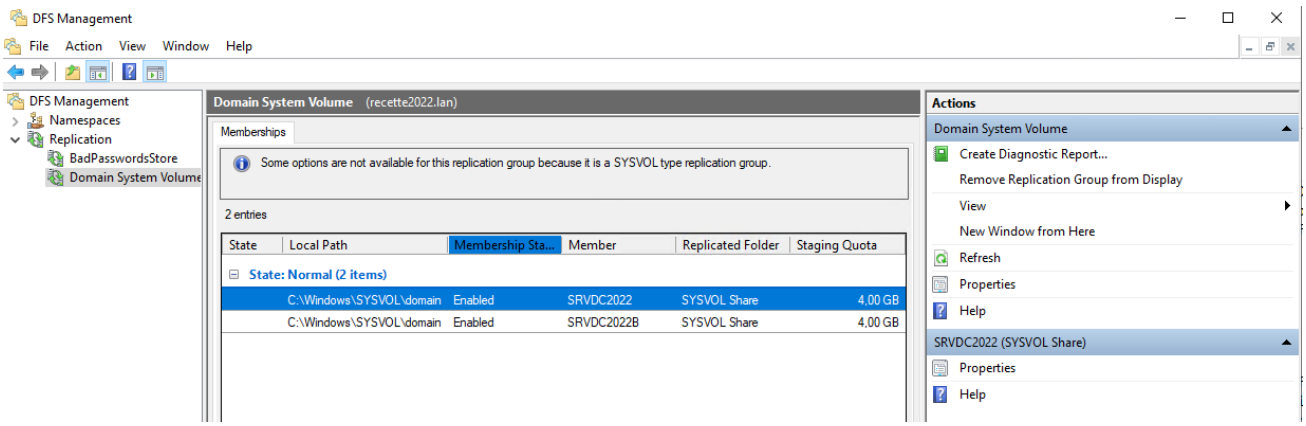
Windows va ensuite appliquer ces fichiers de configuration et modifier sa base de registre.

Dans l'exemple ci-dessous, la machine doit appliquer la GPO *Security-All_Disable_SSL2_SSL3*.
Cette GPO permet de désactiver les protocoles SSL2 et SSL3.
La valeur de l'attribut *ObjectGuid* de cette GPO est égale à *037AD833-8047-49AE-B909-628AF33EF46D*.

L'ordinateur doit alors télécharger les fichiers de la GPO depuis l'emplacement indiqué dans l'attribut *gPCFileSysPath*. Dans cet exemple, cet attribut à la valeur suivante :
\\recette2022.lan\sysvol\recette2022.lan\Policies\{037AD833-8047-49AE-B909-628AF33EF46D}



Le chemin ci-dessous fait référence à un espace de noms.
Pour voir cet espace de noms, il faut lancer la console *DFS Management* sur un contrôleur de domaine.



Dans cet exemple, nous pouvons voir que l'espace de noms \\recette2022.lan\sysvol est hébergé sur les 2 contrôleurs de domaine.

Le moteur DFS-R est utilisé dans cet exemple pour répliquer les changements du dossier *C:\Windows\SYSVOL\Domain* de 2 contrôleurs de domaine. En effet, ce dossier est modifié lors de l'ajout / modification ou suppression d'une GPO.

Historiquement, le moteur NTFRS était utilisé. Il a été remplacé avec Windows 2008 R2 par le moteur DFS-R.

Ce changement doit cependant être fait manuellement en appliquant cette procédure :

https://www.it-connect.fr/active-directory-migrer-sysvol-de-frs-a-dfsr/

C'est un prérequis pour migrer vers des contrôleurs de domaine Windows 2016 Server.

2.21.12 Dépannage de la réplication du dossier SYSVOL

Pour NTFRS, lire les articles ci-dessous :

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/use-burflags-to-reinitialize-frs

Pour DFS-R, lire les articles ci-dessous :

https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/force-authoritative-non-authoritative-synchronization

3 Savoir comment attaquer pour mieux se défendre

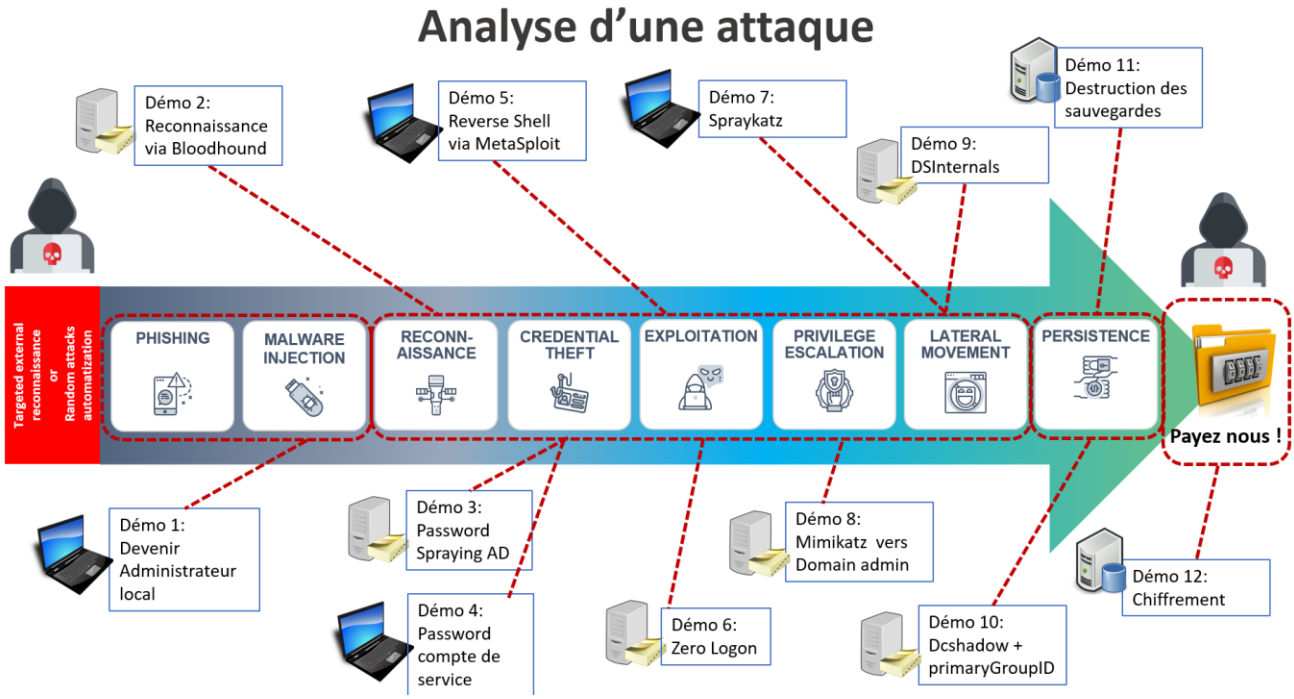
3.1 La méthodologie d'un attaquant pour déployer un rançongiciel (cryptolocker)

Le coût des cyberattaques explose partout dans le monde comme expliqué dans l'article ci-dessous :
https://www.lesechos.fr/amp/1005615

Le schéma ci-dessous explique la démarche d'un attaquant pour obtenir des accès d'administration sur un système, corrompre les sauvegardes et déployer un rançongiciel.

Ce qu'il faut en retenir :

- Très simple d'attaquer.
- Très complexe de défendre.



Chaque étape de l'attaque est documentée par une ou plusieurs vidéos :

Démo 1 : devenir administrateur local d'une machine Windows
https://youtu.be/yND1ZrTtZmQ
https://youtu.be/QhGfKKKxdjU

Démo 2 : Découverte automatique des chemins d'escalade de privilèges avec *BloodHound*
https://youtu.be/DzyCB5_gSaQ

Démo 3 : recherche de mot de passe simple sur tous les comptes AD (*Password Spraying AD*)
https://youtu.be/DhtUc4lej58

DEMO 4 : récupérer le mot de passe de comptes de services

Récupérer le login et mot de passe d'un compte de service via une authentification LDAP Bind Simple : https://youtu.be/bO1HtKdk-1c

Comprendre le rôle du compte de service et comment sont stockés les mots de passe des comptes de service : https://youtu.be/6PrHY9zYwyg

Utilisation de PSEXEC et SAPD.EXE pour afficher le mot de passe d'un compte de service Windows : https://youtu.be/tay2-dxTwH4

Démo 5 : utilisation de *METASPLOIT*

Générer un écran bleu sur un serveur Windows 2008 R2 avec le service RDP : https://youtu.be/zuelA0RsU3g

Obtenir un accès SYSTEM sur une machine Windows avec les outils d'administration Netgear : https://youtu.be/lhHF2kBF4uE

Démo 6 : utilisation de MIMIKATZ avec Zéro Logon et attaque DCSYNC pour générer un Golden Ticket

https://youtu.be/ydYC_kAtgFM

Démo 7 : mouvements latéraux avec SPRAYKATZ

https://youtu.be/40kyaOydv_s

Démo 8 : devenir administrateur du domaine avec MIMIKATZ

https://youtu.be/mwQgJTt33bk

Démo 9 : attaque DCSYNC avec le module PowerShell DSINTERNALS

https://youtu.be/htLgrX0fzjA

Démo 10 : attaque DCSHADOW avec MIMIKATZ

https://youtu.be/Okxzo03czyk

Démo 11 : comment détruire les sauvegardes VEEAM BACKUP & REPLICATION et utiliser un serveur de sauvegarde Veeam Backup pour effectuer une élévation de privilèges

https://youtu.be/4k6AVuOQqNk

Démo 12 : utilisation de DISKCRYPTOR comme un rançongiciel maison

https://youtu.be/IfmCeG0MfiE

Autres démonstrations non présentées dans cette slide :

Comment récupérer le NTHASH - LMHASH des utilisateurs avec LIBESEDB et NTDSXTRACT : https://youtu.be/S29XlCg5OHg

Comment faire une élévation de privilège via injection de SID History : https://youtu.be/FqSHLxBpY78

Démo en mode d'ensemble des attaques (vidéo de 2015) : https://youtu.be/5uQPfS3nmW4

Le guide Tester la sécurité de son annuaire Active Directory V2.0 présente le pas à pas de chacune de ces attaques et peut être téléchargé à l'adresse suivante :

http://msreport.free.fr/articles/TESTER_SECURITE_ACTIVE_DIRECTORY_V_2.0.pdf

La vidéo Les élévations de privilèges Active Directory et comment les détecter présente des attaques plus modernes avec des outils comme MIMIKATZ, DSINTERNALS.

https://youtu.be/qHKVQ76IpAU

3.2 Présentation de l'outil DSINTERNALS

Se loguer en tant qu'administrateur du domaine.
Installer l'outil DSINternals (https://www.dsinternals.com).

Cela s'effectue simplement avec PowerShell à l'aide des commandes suivantes :

```
Set-ExecutionPolicy Unrestricted
Install-module Dsinternals
```

La commande ci-dessous permet de sortir le mot de passe du compte KRBTGT et donc de générer un *Golden Ticket*.

```
Get-ADReplAccount -SamAccountName krbtgt -Domain FORMATION -Server DC1.formationXX.intra
Get-ADReplAccount -SamAccountName administrator -Domain FORMATION -Server
DC1.formationXX.intra
```

Où XX correspond à vos initiales.
Noter le NTHASH des comptes utilisateurs KRBTGT et ADMINISTRATOR.

Ils sont nécessaires pour la suite de l'exercice.

3.3 Présentation de l'outil MIMIKATZ

Télécharger l'outil MIMIKATZ : http://blog.gentilkiwi.com/mimikatz

Il sera nécessaire de désactiver l'antivirus Windows Defender sur la machine WK1 et d'utiliser Internet Explorer pour télécharger cet exécutable.

Attaque DCSYNC :

Lancer Mimikatz et exécuter les commandes suivantes :

```
privilege::debug
lsadump::dcsync /user:krbtgt
```

On notera que le module PowerShell DSINTERNALS permet de faire cela en PowerShell.

Attaque NTLM Pass The Hash :

Lancer Mimikatz et exécuter les commandes suivantes :

```
sekurlsa::pth /user:administrator /domain:FORMATION
/ntlm:abfc3e6527789f4b6ed36a63315a2ec8 /run:powershell
```

Remplacer *bfc3e6527789f4b6ed36a63315a2ec8* par la valeur du NTHASH du compte administrateur obtenu avec l'outil DSINTERNALS dans le paragraphe précédent

Attaque Golden Ticket :

Obtenir le SID de votre domaine avec la commande *Get-AdDomain*.

Lancer MIMIKATZ et exécuter les commandes suivantes :

```
privilege::debug
kerberos::golden /user:administrator /domain:formationXX.intra /sid:S-1-5-21-3815459336-2235161617-1670922636 /krbtgt:6f416c42b3e19a7b027d05ffd63146d1 /ptt
```

Vous devez saisir la valeur du SID du domaine et du compte KRBTGT obtenue aux étapes précédentes.

3.4 Présentation de l'outil METASPLOIT

ALPHORM propose 3 vidéos de formation sur METASPLOIT :

https://support.alphorm.com/hc/fr/articles/360002074478-Pentesting-avec-Metasploit-par-Hamza-KONDAH

4 Les contre-mesures à appliquer

4.1 Gouvernance de l'équipe IT

Visionner la vidéo Msreport – gouvernance Active Directory : https://youtu.be/1Dl6hLNJO5w

Elle explique l'importance d'avoir une équipe informatique centralisée pour gérer un annuaire Active Directory dans les sociétés de grande taille / multinationale.

4.2 Renforcer la sécurité de vos sauvegardes

Il est important de renforcer la sécurité du serveur de sauvegarde car ce dernier pourrait être utilisé pour faire une élévation de privilège au niveau du domaine Active Directory comme expliqué dans la vidéo suivante : https://youtu.be/4k6AVuOQqNk

Le serveur de sauvegarde doit être une machine physique (pas une machine virtuelle) afin de ne pas dépendre de l'infrastructure de virtualisation. Si cette dernière est compromise, le serveur de sauvegarde pourrait être compromis.

Le serveur de sauvegarde doit être membre d'un groupe de travail car il ne doit pas être compris si le domaine AD est compromis.

Si ce serveur doit être membre d'un domaine Active Directory, ce domaine Active Directory **doit être dédié** au serveur de sauvegarde.

Le plus important :

Vous devez disposer de sauvegardes déconnectées (disques durs externes, cartouches LTO) qui ne sont pas accessibles par l'attaquant si ce dernier prend le contrôle du serveur de sauvegarde.

De nombreuses sociétés perdent toutes leurs données car elles ne disposent pas de sauvegardes déconnectées.

4.3 Renforcer la sécurité de votre environnement de virtualisation

Votre environnement de virtualisation (Hyper-V, VMware ou autres) ne doit pas être administrable avec des comptes du domaine Active Directory de production. Si les serveurs de l'environnement de virtualisation doivent être membres d'un domaine Active Directory (cas avec un cluster Hyper-V), ce domaine Active Directory **doit être dédié** à l'environnement de virtualisation.

4.4 Sécuriser votre annuaire Active Directory

4.4.1 Vue d'ensemble

Vous pouvez pour cela appliquer le standard *Harden AD* et utiliser la solution *Harden AD* pour déployer automatiquement les actions de ce standard.

Cet outil est gratuit pour un usage personnel et peut être téléchargé à l'adresse suivante :

Https://hardenad.net

4.4.2 Réinitialiser KRBTGT

Cette tâche est effectuée par l'outil *Harden AD* V3 (développement en cours).

En cas de suspicion d'attaque Golden Ticket, il faut réinitialiser le mot de passe du compte KRBTGT 2 fois.

Attendre au minimum 10h (durée de vie d'un TGT) + temps de réplication de l'AD entre les 2 tentatives (en pratique attendre au minimum 24h).

Microsoft fournit un script qui vérifie tous les prérequis pour réinitialiser le mot de passe du compte KRBTGT à l'adresse suivante :

https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

C'est ce script qui doit être utilisé.

Le changement de mot de passe du compte utilisateur KRBTGT doit aussi être effectué régulièrement ensuite (tous les mois).

4.4.3 Exécuter l'outil Ping Castle

Télécharger Ping Castle. L'outil est gratuit pour un usage personnel.
Faire un bilan de santé de votre annuaire (paramètre par défaut).

4.4.4 Mise en place d'un modèle de Tiering

Visionner la vidéo *Déléguer l'administration d'Active Directory - les fondamentaux* :

https://youtu.be/vtqW4BWAP6I

Lire le chapitre 2 du guide Tester la sécurité de son annuaire Active Directory :

http://msreport.free.fr/articles/TESTER_SECURITE_ACTIVE_DIRECTORY_V_2.0.pdf

La mise en œuvre d'une politique de délégation et la création de station d'administration est un prérequis pour garantir un niveau de sécurité acceptable pour votre annuaire Active Directory.

Le principe est de séparer l'administration du service Active Directory (Tier 0), l'administration des serveurs et des applications (Tier 1) et l'administration des stations de travail et des stations de travail standards (Tier 2).

Le standard Harden propose justement un modèle de Tiering et la mise en place de stations d'administration (PAW).