Le contrôleur de domaine dans un réseau local

Table des matières

L'intégralité du brief se fera dans Windows Server 2019, sans licence, installé dans une machine virtuelle Hyper-V pour simuler un ordinateur(Service intégré dans windows, dans les faits plus stable que Oracle Vbox) .

Le but du brief est de configurer un contrôleur de domaine et de manipuler les comptes utilisateur dans le domaine créé. Ainsi nous pourrons répondre à différentes questions :

Livre 1

1. Quels sont les pré-requis à l'installation d'un Contrôleur de domaine
2. L'intérêt de l'AD-DS
3. Quels sont les protocoles nécessaires au bon fonctionnement d'un Active Directory et leur utilité à chacun d'eux ?
4. Quel est l'intérêt d'activer le bureau à distance sur ce serveur ?

Livre 2

1. Pouvez-vous utiliser le compte « chefinfo » de votre domaine pour vous connecter au domaine de votre voisin ?
2. Quelle est la politique des mots de passe, par défaut sur votre domaine ?
3. Donnez une raison justifiant la désactivation d'un compte utilisateur de votre domaine
4. Quel compte utilisateur devrez-vous utiliser pour joindre un poste utilisateur à votre domaine ?

Livre 3

La Partie 3 porte sur la validation des parties précédentes, c'est-à-dire s'assurer du bon fonctionnement des actions réalisées par le test.

LIVRE I

Action 1 :Installation/configuration de votre serveur (VM windows server 2019) puis Activer / Configurer le service ADDS

Nous commençons sur le bureau de windows server (*screenshot_001)*. Je **renomme** la machine dans **Information système** pour que serveur aie le nom "**SRV-MATSUYAMA**" (*screenshot_002*), puis je **redémarre** pour appliquer.

Puis je vais Activer Le service AD-DS mais avant cela quelques prérequis :

Q1 :Liste des prérequis pour le contrôleur de domaine(Q.1)

J'ai trouver une liste un peu ancienne (2009) des prérequis donc j'ai cherché d'autre sources autour de moi avant d'ajouter un contrôleur de domaine :

Le serveur est sur une partition NTFS avec 250Mb disponible (*screenshot_003)*. Je suis connecté en tant qu'Administrateur. Ensuite la **version est à jour**, j'ai déjà effectué la MàJ et je suis donc **connecté au réseau** par l'intermédiaire d'un switch virtuel dans hyper V (*screenshot_004)* *(screenshot_005*). J'ai ensuite installé le rôle "**DNS**" un service nécessaire au bon fonctionnement de L'ADDS. J'ai aussi besoin d'un **nom de domaine** à utiliser, la contrainte est d'utiliser un nom de ville, J'ai choisit la ville de Matsuyama (ville de l'île de shikoku, Japon), mon nom de domaine sera **MATSUYAMA.local**. Enfin j'ai besoin d'une **IP fixe** donc je la configure manuellement (*screenshot_006*).

Dans le gestionnaire de serveur > gérer > ajouter des rôles et fonctionnalités :

On valide les étapes pour installer "Serveur DNS" et "Service AD DS" , suivit de la configuration de L'AD-DS après installation.

Pour résumé les prérequis :

- Avoir un compte et mot de passe administrateur pour avoir le droit d'installation sur le serveur
- Nommer le serveur
- configurer une adresse IP fixe
- vérifier que le serveur résout le domaine active directory
- installer les mise à jours (connexion internet)
- espace disponible sur le disque dur

Q2 :Intérêt de l'ADDS

L'ADDS est un Annuaire mais possèdes de nombreux avantage dans la gestion en entreprise.

Son objectif est d'être l'outil permettant de superviser différentes fonctionnalités :

- la centralisation d'identification et d'authentification à un réseau d'ordinateurs utilisant le système MS, APPL ou LNX. De nos jour on utilise le protocole Kerberos qui est sécurisé par un système de clé secrète (chiffrement symétrique).
- La stratégie de groupe (ou GPO) qui peuvent être multiples, puis lié a l'active directory afin d'inclure une gestion :
    1. des ordinateurs déconnectés
    2. des utilisateurs itinérants
    3. la redirection de dossier et la gestion des fichiers en mode déconnectés.

    Elle permet aussi de restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction à la lecture l'écriture l'exécution de certains dossiers/fichiers , la d2sactivation de l'utilisation de certains exécutables (exemples : console ou powershell).
- L'installation de mises à jour (par l'administrateur)
- Répertorie les éléments d'un réseau : comptes utilisateurs, les serveurs, les postes de travail les dossiers partagées.
- Interroger l'annuaire pour obtenir des informations à l'aide d'une demande concrête, par exemple toute les imprimantes couleur au « $8^{ème}$ étage »
- Stockage des informations et paramètres dans une base de données distribuée sur un ou plusieurs contrôleur de domaine.

Q3 :Les protocoles.

Voici la liste des protocoles nécessaires pour le bon fonctionnement de L'AD :

2.3 Protocol Relationships

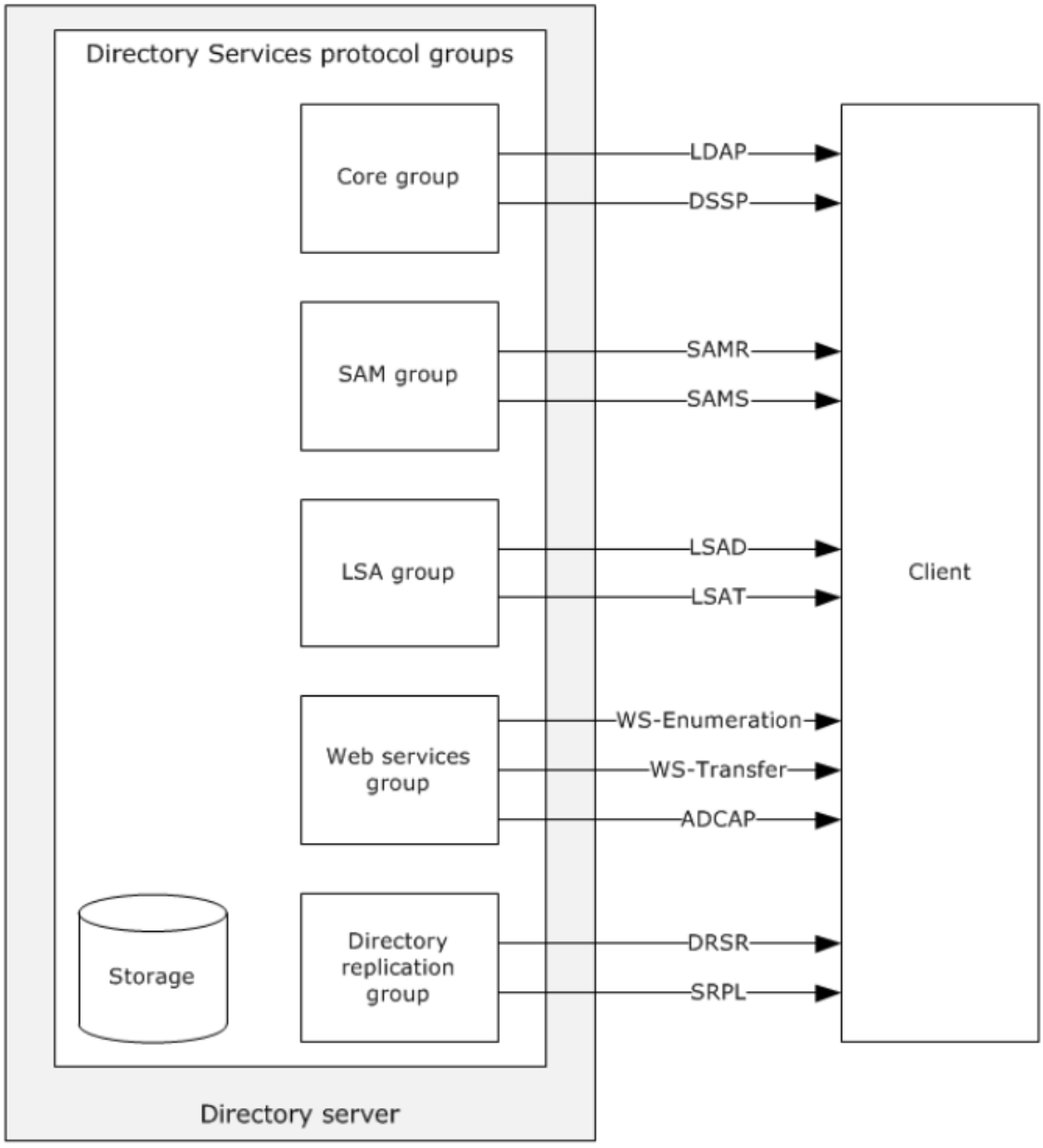


Figure 3: Active Directory protocol grouping

Détail :

LDAP-[MS-ADTS]:Lightweight Directory Acess Protocol membership

[MS-DRDR] :Directory Replication Remote Protocol (drsuapi) -Replication

[MS-SRPL] :SMTP Replication Protocol Extensions

[MS-DSSP] :Directory Services Setup Remote Protocol

ces quatre protocoles activent le "cœur" du système de l'AD , les fonctionnalités de base : accès aux arbres , réplications de ceux-ci, adhésions aux groupes, statuts du contrôleur de domaine.

[MS-SAMR] :Security Account Manager (SAM) Remote Protocol (client-to-server)

[MS-SAMS] :Security Account Manager Remote protocol

Ces deux protocoles activent la maintenances des comptes lorsque le système Acticve Directory exploite le mode AD-DS. Cela comprend la création, la modification, la récupération et la suppression d'utilisateurs et de groupes.

[MS-LSAD] :Local Security Authority (Domain policy) Remote Protocol

[MS-LSAT] :Loacal Security Authority (Translation Methods) Remote Protocol

Ces deux protocoles permettent au client d'extraire des informations sur les politiques de sécurité et de traduire les identifiants de sécurité (SID) qui identifient principalement les utilisateurs en noms lisible par l'homme.

[MS-ADCAP]:Active Directory Web Service Custom Action

[MS-WSTIM] : Identity Management Operations for Drirectory Acces Extensions

[WSENUM] :WS-Enumeration

[WXFR] :WS-Transfer

[MS-WSDS] :WS-Enumeration: Directory Services Protocol Extensions

[MS-WSPELD] :WS-Transfer and WS-Enumeration Protocol Extension for Lightweight Directory Access Protocol v3 Controls

[MS-ADDM] : Active Directory Web Services: Data Model And Common Elements

Ces sept protocoles activent les services Web pour que le system AD ait accès à l'arborescence des répertoires et la gestion des informations et des topologies des comptes Active Directory.

Action 2 :Activer le Bureau à distance.

(*screenshot_007*)

Q4 :Intérêt du Bureau a distance (Remote Desktop Protocol)

Le bureau a distance (RDP remote desktop protocol) permet à un utilisateur agréé de contrôler la machine serveur par le biais d'un réseau local ou externe. L'utilisateur pourras alors depuis son poste (contrôle :clavier écran souris) obtenir le contrôle total du poste et ainsi installer les *màj*, vérifier les paramètres ajouter des fonctionnalité, gérer les groupe ou GPO, etc ... peux importe d'où il travail.

Q5 :Vigilance: Attention à qui à accès au RDP et l'attaque man in the middle

Donc les bonnes pratiques sont :

- désactiver le service si il n'est pas utilisé
- configurer Account Lockout Threshold : le seuil de verrouillage de compte (erreurs répétées des mots de passe)
- configurer une politique de mots de passe forte
- restriction d'IP pour l'accès à distance
- utiliser un Port différent du port par défaut
- offrir le moins de droits possible au utilisateurs du RDP
- utiliser un VP ou une authentification à multiple facteurs pour protéger la connexion.

on peux aussi Activer le Mode « Restricted Admin » pour les Connexions Bureau à distance »

LIVRE II Création de comptes utilisateurs

Action 3 et 4

Création chefinfo et gilbert

Centre d'administration Active directory > Users > [Tâche] nouveau >utilisateur

(screenshot_008)

Pour que chefinfo soit administrateur, on clique sur l'utilisateur,

Depuis le centre d'administration précédemment ouvert on clique sur users > dossier "Users" > on clique sur chefinfo (*screenshot_008*)

Depuis le gestionnaire de serveur on va sur outils > utilisateurs et ordinateur active directory > (nom de domaine) > dossier Users > chefinfo

Pour les deux : dans l'onglet "Membre de" suivre (screenshot_009) (désolé pour le labyrinthe).

Action 5

Import de la liste des apprenants , script pour powershell, crédit:Nathan Bude. (*screenshot_010*).

Q6 :Connexion au domaine voisin

Le domaine d'un autre apprenant n'est pas accessible avec mon compte chefinfo, il est administrateur, certes, mais il n'est pas dans l'annuaire du domaine voisin.

La nuance est que deux compte du même nom ne sont pas identiques, le domaine dans lequel il est créé est la source du problème. Créer une relation d'approbation entre les deux domaine permettrais aux utilisateurs chefinfo de se connecter respectivement aux "domaines voisins liés".

Q7 :Politique des mots de passe

Outils > Stratégie de sécurité locale > stratégie de mot passe

nous donne la stratégie en place, par défaut car je ne l'ai pas modifié.

Stratégie	Paramètre de sécurité
Audit de la longueur minimale de mot de passe	*N/A*
Conserver l'historique des mots de passe	*24 mots de passe mémorisés*
Durée de vie maximale du mot de passe	*42 jours*
Durée de vie minimale du mot de passe	*1 jour*
Enregistrer les mots de passe en utilisant un chiffrement réversible	*Désactivé*
Les mots de passe doit respecter des exigences de complexité	*Activé*
Longueur minimale du mot de passe	*7 caractères*

Action 6 :Panneau de configuration\Système et sécurité\Outils d'administration

Gestion des stratégies de groupe (C:\Windows\system32\gpmc.msc)

(screenshot_011)

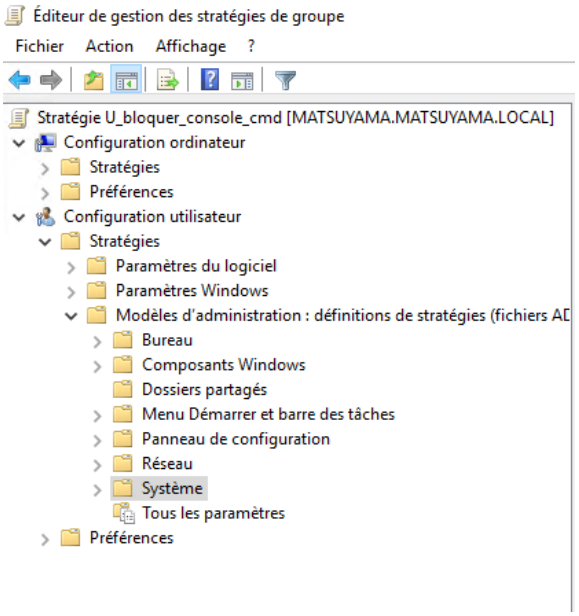
une fois créée , la GPO u_bloquer_console_cmd : on clique droit → modifier

on va centrer la gpo sur bloquer l'invite de commande CMD

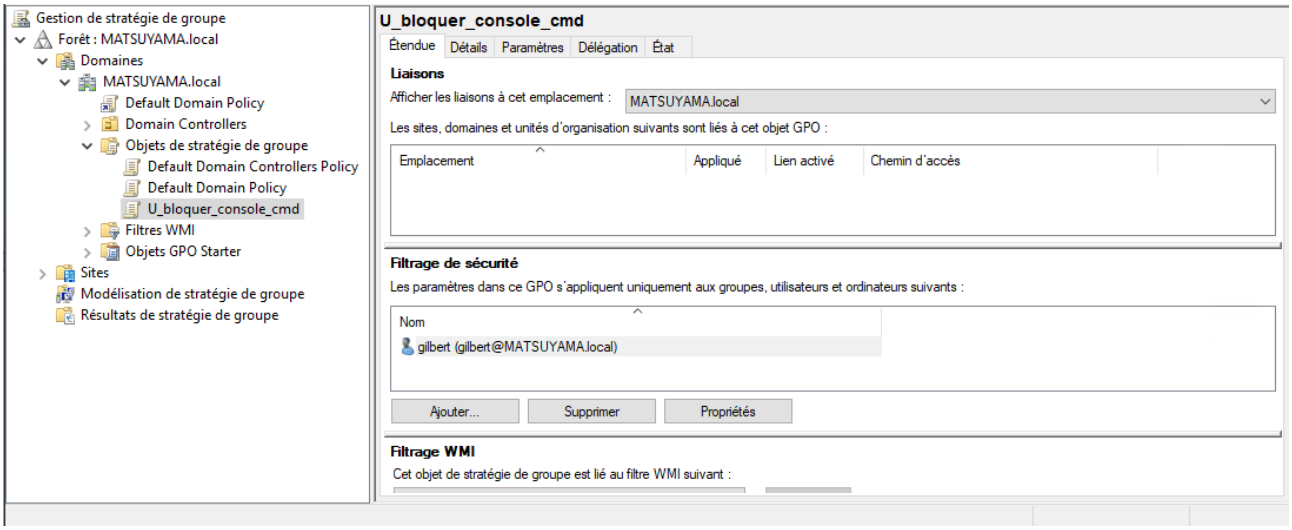
Donc on clique sur désactivé l'accès à l'invite de commande

Puis 3 boutons d'activation permette de désactiver/activer le paramètre

On valide , désormais pour nôtre nouvelle GPO l'invite de commande est désactivé.



Pour terminer l'action on retourne dans la stratégie de groupe :



Dans filtrage de sécurité on supprime les champs par défaut et on ajoute l'utilisateur gilbert.

Q8 :Désactivation un compte utilisateur de domaine

Un utilisateur quittant l'organisation ou prenant congés pendant une longue durée n'as plus besoin d'un accès au domaine, pour éviter que le compte soit "recyclé", utilisé par un tier (un autre employé, un inconnu du domaine ayant trouvés les identifiants ou autre)

Q9 :Joindre un poste au domaine

Il faut utiliser le compte unique administrateur pour joindre un poste utilisateur au domaine.

Livre III ?

Q10 :Test de vérification des actions

Action 1	Dans cmd : • « hostname » pour vérifier le nom du serveur • $ ping MASTUYAMA.local $ ping 192.168.1.177 doivent répondre pour vérifier que l'AD à bien été configurer et est fonctionnel
Action 2	• Se connecter depuis la machine hôte avec le bureau à distance • demander au voisin(e)s de se connecter en bureau a distance
Action 3	• Se connecter depuis un autre poste (on ne peux pas lancer la vm et se connecter depuis le même poste) avec le compte chefinfo au domaine • essayer d'ajouter un poste au domaine avec le compte chefinfo
Action 4	• Se connecter depuis un autre poste avec le compte gilbert au domaine
Action 5	• Dans le menu Utilisateur et ordinateur Active Directory : parcourir la liste des utilisateurs et vérifier si ils sont tous présents
Action 6	• Ouvrir une sessions avec le compte gilbert et essayer et ouvrir l'invite de commande si le message «**l'invite de commandes a été désactiver par votre administrateur**.» la stratégie de groupe fonctionne bien.

SOURCES :

Installation & protocol

- ajouter un ADDS
- what do you need to install active directory
- MS AD documentation

Vigilance AD

- Activer le Mode "Restricted Admin" pour les Connexions Bureau à distance
- Securing Remote Desktop (RDP) for System Administrators

Créer sa GPO

- IT connect

Illustration I: (bonus) Ogma