**Installation de l’Active Directory**

**Objectifs**

* Installer le rôle AD DS (Active Directory Domain Services) sur le SERVEUR1
* Joindre le SERVEUR2 au domaine

**Matériels**

* L'ordinateur réel avec deux ordinateurs virtuels avec "Windows Server 2019"

**Étape 1 - Vérification du contrôleur de domaine**

Démarrer l'ordinateur virtuel "SERVEUR1" et connectez-vous avec l’usager Administrateur.

Vérifier la configuration du serveur virtuel "SERVEUR1"

* Le nom du serveur est **SERVEUR1**
* Modifier la configuration DNS de la carte réseau

DNS: **127.0.0.1**

**Étape 2 - Création d’un domaine**

Démarrer la console "Gestionnaire de serveur", dans le menu "Gérer"

Installer le rôle "Services AD DS"

* Lire les informations qui vous sont données
* Cocher "Redémarrer automatiquement le serveur de destination, si nécessaire"
* Quand les fonctionnalités seront installées, fermer la fenêtre et cliquez sur le triangle jaune qui est en haut et à droite, à côté du drapeau
* Il faut effectuer la configuration post-déploiement (choisir "Promouvoir ce serveur en contrôleur de domaine")

Répondre aux questions de la post-configuration du domaine

* Écran "Configuration de déploiement"
* Choisir "Ajouter une nouvelle forêt"
* Le nom de domaine racine est **FORMATION.LOCAL**
* Écran "Options du contrôleur de domaine"
* Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe: AAAaaa111

Confirmer le mot de passe: AAAaaa111

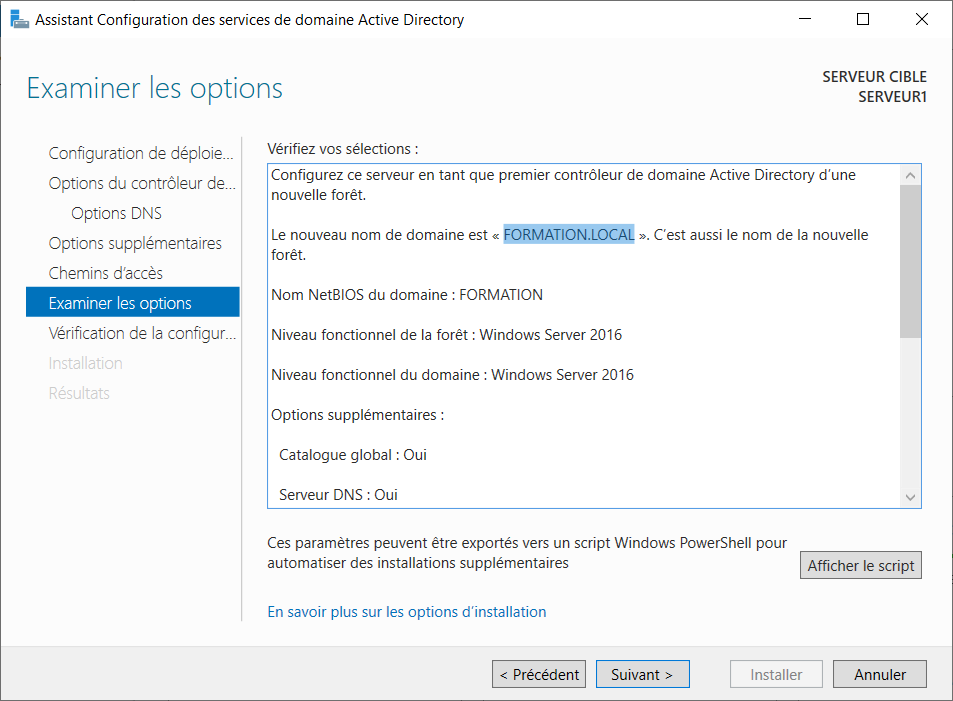
* Vous aurez un avertissement "Il est impossible de créer une délégation pour ce serveur DNS …"

**Ne vous en occupez pas et cliquer sur le bouton "Suivant".**

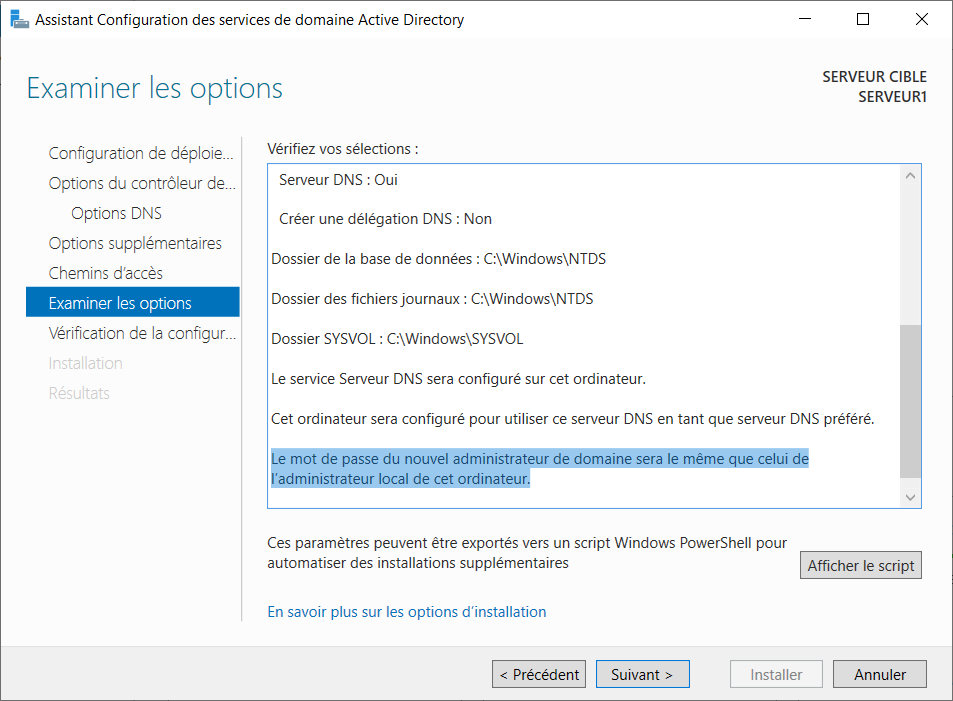
* Écran "Options supplémentaires"
* Le nom de domaine NetBIOS: **FORMATION**

**Vous aurez besoin de cette information pour joindre le SERVEUR2 au domaine.**

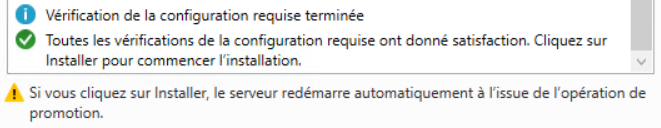
* Écran "Chemins d’accès"
* Ne pas changer l'emplacement des dossiers proposés par défaut
* Écran "Examiner les options"



Il est important de vérifier que le nom du domaine est **FORMATION.LOCAL**



* Écran "Vérification de la configuration requise"



* Il est important de vérifier que la dernière ligne confirme que la configuration minimale requise est satisfaite.
* Démarrer l'installation
* Le serveur va redémarrer à la fin de l’installation.

**Étape 3 - Validation du domaine**

Connectez-vous sur le contrôleur de domaine.

Dans la console DNS (Gestionnaire de serveur / Outils / DNS)

* Sélectionner "SERVEUR1 / Zones de recherche directes" / FORMATION.LOCAL"

pour vérifier la présence d’un enregistrement de type "A" au nom de votre serveur SERVEUR1

Dans une invite de commandes exécuter la commande suivante

**ping SERVEUR1.FORMATION.LOCAL -4**

Vérifier la présence des partages: NETLOGON et SYSVOL

* exécuter "net share" dans une "Invite de commandes"
* tester l'accès aux partages SYSVOL et NETLOGON

\\FORMATION.LOCAL\NETLOGON

\\FORMATION.LOCAL\SYSVOL

**Étape 4 - Joindre le SERVEUR2 au domaine**

Connectez-vous sur le "SERVEUR2" en utilisant le compte Administrateur.

Vérifier la configuration du serveur virtuel "SERVEUR2"

* Le nom du serveur 2 est **SERVEUR2**
* Modifier la configuration DNS de la carte réseau

DNS: 192.168.1.10 (adresse IP du "Contrôleur de Domaine")

**Joindre l'ordinateur à votre domaine**

( + Pause) permet d'afficher la fenêtre "Propriétés système"

Cliquer sur "Modifier les paramètres"

* Choisir l’option "Membre d'un Domaine:"
* Taper le nom de domaine NetBIOS qui est **FORMATION**

Authentifiez-vous avec le compte Administrateur du domaine avec FORMATION\administrateur

* Après le message de bienvenue, vous devez redémarrer l'ordinateur client.

**Canal sécurisé entre un ordinateur et le contrôleur de domaine**

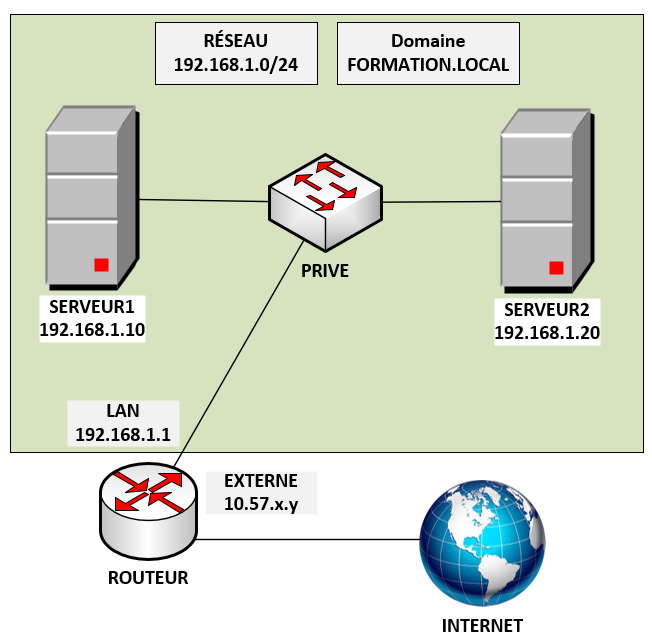
Lorsqu'un ordinateur est joint au domaine, un compte ordinateur est créé.

Le compte ordinateur possède un nom (samAccountName ) et un mot de passe.

Le samAccountName d’un ordinateur de l’Active Directory se termine toujours par un $.

Le mot de passe est enregistré sous forme de secret LSA (Local Security Account) et est changé à chaque 30 jours.

**Le schéma de nos serveurs.**



**Toujours sur le "SERVEUR2", connectez-vous au domaine.**

Utilisation d'un compte de l'Active Directory

* FORMATION\Administrateur utilise le compte Administrateur du domaine
* Administrateur@formation.local utilise le compte Administrateur du domaine



"**Connectez-vous à FORMATION**" indique vous utilisez un compte de l'Active Directory.

**Pour le cours, il ne sera pas nécessaire de se connecter avec un compte local sur le SERVEUR2.**

Utilisation d'un compte local du SERVEUR2

* Administrateur utilise le compte Administrateur local
* .\Administrateur utilise le compte Administrateur local

.\ fait référence à l'ordinateur local

* SERVEUR2\Administrateur utilise le compte Administrateur local

SERVEUR2\ force l'utilisation du compte Administrateur local



"**Connectez-vous à SERVEUR2**" indique que vous utilisez un compte local du SERVEUR2.

**Étape 5 – Renommer le compte "Administrateur" local sur le SERVEUR2**

Pour éviter de se connecter par erreur avec le compte "Administrateur" local sur le SERVEUR2, je vous conseille de renommer le compte "Administrateur" local.

**Le nom de l'utilisateur dont le SID se termine par 500 varie selon la langue.**

* En français, le nom de l'utilisateur est "Administrateur".
* En anglais, le nom de l'utilisateur est "Administrator".
* En espagnol, le nom de l'utilisateur est "Administrador".
* …

**# Le code doit s’exécuter sur le SERVEUR2**

**$NewAdminName = "AdminLocal"**

**$Objet = Get-LocalUser | Where-Object { $PSItem.SID -like "S-1-5-21-\*-500" }**

**Rename-LocalUser -InputObject $Objet -NewName $NewAdminName**

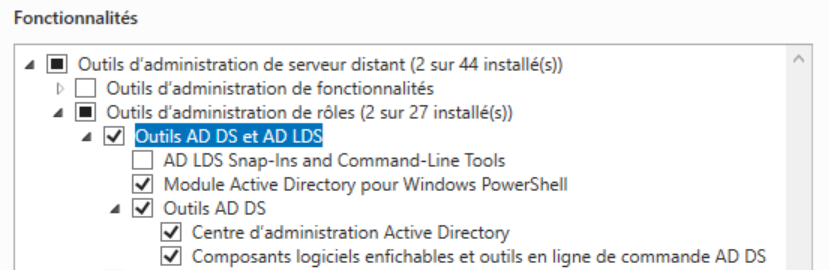
**Étape 6 – Installer la console UOAD sur le SERVEUR2**

Par défaut, la console UOAD n'est pas installée sur un serveur qui est joint à un domaine Active Directory.

**Installer les outils d'administration**

Dans la fonctionnalité "Outils d'administration de serveur distant", développer "Outils d'administration de rôles".

* ajouter les composants suivants



**Si tout s’est bien passé, la console UOAD (Utilisateurs et Ordinateurs Active Directory) sera installée sur le SERVEUR2.**

**ANNEXE**

Comment sortir un ordinateur du domaine

**Vous devez utiliser ces commandes en cas de besoin seulement.**

Cette commande permet de sortir un ordinateur du domaine si le contrôleur de domaine existe.

Cette commande demande le mot de passe du compte " **NomDuDomaine\Administrateur**".

**Remove-Computer -ComputerName NomDeLordinateur `**

**-UnjoinDomainCredential NomDuDomaine\Administrateur `**

**-WorkgroupName NomDuGroupeDeTravail `**

**-Force `**

**-Restart**

Cette commande permet de sortir un ordinateur du domaine même si le contrôleur de domaine n'existe plus.

Après l'exécution de la commande, le groupe de travail portera le nom du domaine.

**netdom.exe remove NomDeLordinateur /Domain:NomDuDomaine /Force /Reboot**