CRÉER UNE COPIE AVANT DE REMPLIR

Installation de l'Active Directory

Installation Active Directory

Sur votre serveur SRVSTORDC fraîchement installé faites un tour dans les **outils d'administration** (cliquez sur outils) et listez-les ci-dessous en indiquant une brève description

Outil d'administration	Brève description
Analyseur de performances	Surveille les performances du système
Configuration du système	Affiche les informations sur le matériel
Défragmenter et optimiser les lecteurs	Optimisation du disque dur
Diagnostic de mémoire Windows	Vérifie le bon fonctionnement de la mémoire
Gestion de l'impression	Gestion des imprimantes
Gestion de l'ordinateur	Outil centralisé pour la gestion (réseaux, disque)
Informations système	Information détaillée sur le (matériel, os, pilote)
Initiateur iSCSI	Connection aux périphériques réseaux ISCSI
Moniteur de ressources	Surveillance de l'utilisation des ressources systèmes
Nettoyage de disque	Nettoyage des fichiers temporaires et inutile
Observateur d'évènements	Affiche les journaux d'évènement systèmes
Pare-feu Windows avec fonctions avancées de sécurité	Configuration avancée des pares-feux
Planificateur de tâches	Automatisation de programmes/scripts
Sauvegarde Windows Server	Permet la sauvegarde et restauration du systèmes
Services	Gestion des services en cours sur le serveur
Services de composants	Gestion des services COM+
Services Microsoft Azure	Gestion de services Cloud
Sources de données ODBC (32 bits)	Gestion des sources de données installé sur le serveur (32bit)
Sources de données ODBC (64 bits)	Gestion des sources de données installé sur le serveur (64bit)
Stratégie de sécurité locale	Gestion de sécurité (compte user, droit)
Windows PowerShell	Administration via ligne de commande
Windows PowerShell (x86)	Version systèmes 32bits
Windows PowerShell ISE	Editeur et gestion de script
Windows PowerShell ISE (x86)	Version pour systèmes 32bits

- Cliquez maintenant sur **gérer** puis **ajouter des rôles et fonctionnalités**
- Choisir installation basée sur un rôle ou une fonctionnalité, suivant
- Sur l'écran sélectionner le serveur de destination, ne rien changer, suivant
- Dans sélection des rôles de serveur, choisir **services AD DS** ainsi que **serveur DNS.** Une fenêtre Assistant ajouter les fonctionnalités s'ouvre, cliquez sur Ajouter des fonctionnalités.
- Sur l'écran suivant Sélectionner les fonctionnalités, ne sélectionnez rien et cliquez sur suivant.
- Faites la même chose avec le rôle serveur DNS
- Allez jusqu'au bout de l'installation en conservant les options par défaut

- Si besoin redémarrez le serveur
- Une fois l'installation terminée, sur la page « Gestionnaire de serveur », cliquez sur le drapeau avec un triangle jaune.
- Cliquez ensuite sur « Promouvoir ce serveur en contrôleur de domaine » pour commencer la configuration de déploiement.

- Qu'est-ce qu'un contrôleur de domaine ?

Le contrôleur de domaine est un serveur informatique qui gère l'authentification et l'autorisation des utilisateurs et des ordinateurs dans un réseau Windows. Il permet de centraliser la gestion des comptes utilisateurs, des groupes de sécurité.

- Comme il s'agit d'un nouveau domaine dans une nouvelle forêt, Cochez « Ajouter une nouvelle forêt » et renseignez un nom dans le champ « Nom de domaine racine ».
    - storXX.local (XX est votre numéro de candidat)
- Ensuite cliquez sur le bouton « Suivant ».
- Tapez un mot de passe (Azerty/123) pour le mode de restauration des services de d'annuaire (DSRM), puis cliquez sur « Suivant ».
- Sur la fenêtre de l'option DNS, cliquez sur « Suivant ».
- Vérifiez votre nom de domaine du NetBIOS puis cliquez sur « Suivant ».
- Qu'est-ce que le NetBIOS ?

NetBIOS (Network Basic Input/Output System) est un protocole de communication réseau utilisé principalement dans les systèmes d'exploitation Windows.

Le NetBIOS est un protocole ancien qui facilite l'identification et la communication entre les ordinateurs sur un réseau local.

- Sur la fenêtre des chemins d'accès, cliquez sur « Suivant ».
- A quoi sert le répertoire sysvol ?

Le répertoire SYSVOL (Système volume) est un élément essentiel dans un environnement Active Directory. Il est situé dans le répertoire C :\Windows\SYSVOL.

Il stocke des données qui doivent être répliquées entre les contrôleurs de domaine ou accessible par des ordinateurs clients. Son répertoire contient principalement deux types de données.

1 Les scripts de connexion, qui s'exécutent lors de l'ouverture de session de l'utilisateur

2 Les Stratégies de groupes (GPO), qui sont récupérés par les clients et appliqués pour personnaliser l'espace de travail de l'utilisateur.

Le répertoire SYSVOL est répliqué entre le contrôleur de domaine pout garantir que le contenu soit identique et que les clients bénéficient des mêmes données à jour.

En résumé, le répertoire SYSVOL est crucial pour le bon fonctionnement de l'Active Directory

- Cliquez sur « Suivant », après avoir examiné les options.

- Après la vérification de la configuration par le système, cliquez sur le bouton « Installer ».
- Une fois l'installation terminée, votre machine va redémarrer automatiquement.
- Retournez maintenant dans les outils d'administration et listez les nouveaux outils apparus

Outil d'administration AD	Brève description
Centre d'administration Active Directory	Interface centralisée pour gérer les objets Active Directory.
DNS	Gère et enregistrements DNS et la résolution de noms
Domaine et approbation Active Directory	Gère les relations de confiance entre domaines et approbations
Editeur de registre	Permet de modifier les paramètres du registre Windows
Gestion des stratégies de groupe	Ajouter, modifier et appliquer les stratégies de groupe
Gestion de serveur	Gère les rôles et fonctionnalités du serveur
Information système	Affiche des informations détaillées sur le système
Lecteur de récupération	Permet de démarrer à partir d'un support de récupération.
Modification ADSI	Outil pour gérer les objets de l'AD via l'interface ADSI
Module Active Directory (PowerShell)	Gérer l'AD via PowerShell
Moniteur de ressources	Surveille l'utilisation des ressources système
Sites et services Active Directory	Gérer les sites, les sous réseaux et les connexions entre les contrôleurs de domaine.
Stratégie et sécurité locale	Configure les paramètres de sécurité locaux.
Utilisateurs et ordinateurs Active directory	Gère les comptes d'utilisateur et d'ordinateurs dans AD

C'est le moment de faire une petite pause cours : qu'est-ce que l'Active Directory ?
Active Directory est un *annuaire* au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Il est possible d'interroger l'annuaire pour obtenir une liste des **objets** possédant des **attributs**, en formulant par exemple une requête du type : " Trouver toutes les imprimantes couleur de l'étage 2 ".

Les stratégies de groupe (GPO) sont des paramètres de configuration appliqués aux ordinateurs ou aux utilisateurs lors de leur initialisation, ils sont également gérés dans *Active Directory*.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans *Active Directory*, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger *Active Directory* ou pour y ajouter, modifier ou supprimer des données.

L'*Active Directory* permet de hiérarchiser les utilisateurs et les ordinateurs en groupes et sous-groupes afin de faciliter l'administration des droits et restrictions utilisateurs. C'est aussi *Active Directory* qui se charge de stocker tous les comptes utilisateurs et de gérer l'authentification des utilisateurs sur le domaine Windows.

Vous l'avez donc compris, Active Directory contient des objets représentant des éléments de différents types décrits par des attributs. Cherchez un peu et citez quelques objets possibles ?

Objets utilisateur Objets ordinateurs

Prenez maintenant l'objet utilisateur, citez quelques attributs le concernant ?

Nom principal Information de connexion Description Control du compte Date d'expiration

Le compte administrateur

Vous allez maintenant créer un utilisateur pour chacun d'entre vous en respectant la nomenclature de l'entreprise que vous avez définie. Dans Utilisateurs et ordinateurs Active Directory vous allez créer votre compte en copiant celui de l'administrateur (afin que votre compte possède les mêmes attributs que l'administrateur notamment l'appartenance aux bons groupes). Cliquez droit sur le compte administrateur et faites copier. Définissez votre mot de passe. Indiquez que celui-ci n'expire jamais. Ajoutez en commentaire « Administrateur STOR ».

Nous allons maintenant auditer ce compte administrateur : Activez la stratégie d'audit pour vérifier qui se connecte en erreur sur votre serveur. Pour cela :

- Dans les outils d'administration, lancez Stratégie de sécurité locale puis configuration avancée de la stratégie d'audit
- Dans connexion de compte :
    - Auditer la validation des informations… sur échec
    - Auditer le service d'authentification Kerberos sur échec
- Dans ouvrir / fermer la session
    - Auditer l'ouverture de session sur échec

Déconnectez-vous (fermer la session) et reconnectez-vous en administrateur en simulant une erreur de mot de passe. Une fois connecté, cherchez dans l'observateur d'événements l'erreur qui a été générée.

Désactivez maintenant le compte administrateur. A votre avis, pourquoi faire cela ?

Désactiver le compte administrateur par défaut et utiliser des comptes d'administration dédiés permet de renforcer la sécurité du serveur en réduisant la surface d'attaque et en améliorant la traçabilité et l'audit des actions d'administration.

Nous reviendrons un peu plus tard sur la gestion des mots de passe.

Paramétrer le DNS

Pour cela :

- Outils puis DNS
- La zone de recherche directe a été créée. Développez votre zone de recherche directe puis cliquez sur le nom de votre domaine. Si tout va bien, vous devez voir votre serveur.
- Vous allez créer maintenant une zone de recherche inversée
- Cliquez avec le bouton droit sur zone de recherche inversée et sélectionnez nouvelle zone.
- Sélectionnez zone principale puis zone de recherche inversée IPV4
- Dans ID réseau vous inscrivez les 3 premiers octets de l'adresse IP de votre serveur
- Voilà, c'est terminé pour le DNS. Vous y reviendrez régulièrement au fur et à mesure que vous rentrerez des machines dans le domaine
- Mais au fait, qu'est-ce qu'une zone de recherche inversée et quelle est la différence avec la zone de recherche directe

Une zone de recherche directe mappe un nom d'hôte à une adresse IP. C'est le fonctionnement DNS standard.
Une zone de recherche inversée fait l'inverse : elle mappe une adresse IP à un nom d'hôte. Elle utilise un espace de noms spécial
La différence principale est que la zone directe résout un nom en adresse IP, tandis que la zone inversée résout une adresse IP en nom d'hôte.

Intégration de vos machines dans le domaine

Vous allez maintenant intégrer votre client Windows 10 dans le domaine créé. Vous devez tout d'abord renommer votre client Windows 10 de façon à ce qu'il respecte la nomenclature de votre entreprise. Veuillez aussi respecter l'adressage IP ! Vous devez redémarrer votre machine.

Vous devez ensuite intégrer le domaine. Attention : pour pouvoir entrer une machine dans un domaine, il faut connaître l'adresse du serveur DNS du domaine et l'inscrire dans les paramètres TCP IP de la carte réseau de la machine que vous voulez rentrer dans le domaine. Pourquoi cela ?

La configuration correcte du serveur DNS dans les paramètres TCP/IP est cruciale pour permettre à une machine de trouver et de communiquer avec les contrôleurs de domaine Active Directory.

Pour cela, à l'endroit où vous avez changé le nom, vous cliquez sur Domaine et vous entrez le nom de votre domaine sous la forme storXX.local

Le système va vous demander de vous authentifier avec un compte autorisé pour intégrer une machine dans un domaine. Utilisez votre compte personnel administrateur en y ajoutant les informations de votre domaine. Par exemple : jdupont@storXX.local

Vous devez voir s’afficher un message de bienvenue dans le domaine

Redémarrez une nouvelle fois votre machine.

Vérifiez l’existence de vos machines dans le domaine :

2 possibilités :

- Dans les outils de gestion, utilisateurs et ordinateurs Active Directory, dans la partie Computers
- Dans les outils de gestion toujours, DNS et vous regardez dans vos zones de recherches (directe ou inversée)