TP Active Directory et sécurisation des accès

Phase 2

Objectif du TP (*réseau de type domaine AD)*

- Installation/configuration d'un deuxième contrôleur de domaine Active Directory
- Gestion des comptes et des groupes d'un domaine
- Gestion des autorisations NTFS sur les fichiers et dossiers
- Gestion des autorisations de partage des dossiers.
- Se connecter en local et à distance sur un dossier partagé.
- Administration à distance serveur Linux et Windows
- Gestion des services sous Linux
- Installer des logiciels sous Linux
- Sécuriser les accès via ssh

Chaque groupe de 2 étudiants, composé de 4 machines virtuelles, installera un **domaine unique d'une nouvelle forêt**. Un domaine est composé de 2 contrôleurs de domaine (Windows 2022) et 2 stations de travail (Windows 10) qui devront être jointes au domaine et d'une machine Linux debian 11 non intégrée au domaine. L'utilisation d'unités organisationnelles est possible afin de représenter au mieux la structure de votre entreprise et de permettre une administration plus fine.

Attention : vous penserez bien à actualiser votre schéma réseau

ADMINISTRATION du contrôleur de domaine

Les contraintes suivantes sont toujours en vigueur :

- Installer le service Active Directory sur le deuxième serveur Windows 2019 et vérifier que la réplication s'est correctement effectuée.
- Installer un nouveau serveur 2022 **core** puis le configurer pour être membre du domaine. Justifier la mise en œuvre.
- L'entreprise est composée de 4 services (*étude*, *exploitation*, *personnel* et *comptabilité*) comprenant chacun un responsable et 3 employés.
- Les employés ont tous ont un répertoire de base individuel.
- Les dossiers de base seront stockés sur le contrôleur de domaine numéro 2.
- Un dossier commun par service ainsi qu'un dossier commun pour l'entreprise doivent être mis en place et accessibles par les utilisateurs concernés.
- Créer l'arborescence correspondant aux dossiers de base sur une partition NTFS Windows :

  - ➔ Tous les responsables doivent pouvoir accéder en lecture au dossier de base responsable *étude* et à ses sous-dossiers.
  - ➔ Tous les employés doivent pouvoir lire les informations du dossier commun de l'entreprise et surtout ne pas pouvoir écrire ni supprimer.
  - ➔ Les employés de chaque service doivent pouvoir lire et écrire dans leur dossier de travail et ses sous-dossiers.
  - ➔ Les dossiers des responsables de service ne doivent pas être accessibles par les employés.
  - ➔ Le dossier administrateur n'est accessible et peut être entièrement géré que par l'administrateur et le directeur.
  - ➔ Le directeur doit pouvoir déplacer ou copier les fichiers du service personnel dans son propre dossier.

- Un dossier partagé sur la machine du service personnel et contenant les notes de service doit être accessible par l'ensemble des membres de l'entreprise mais avec des droits différents :
  - ➔ Les responsables, directeur et l'administrateur en ont le contrôle total
  - ➔ Les employés du service étude peuvent corriger certains fichiers
  - ➔ Les autres employés ne peuvent que consulter
- Accéder à un partage qui se trouve sur votre machine Linux. Expliquez comment vous allez mettre en place cet accès

Services

- Comment en mode commande et service visualise t-on les services sous Windows ?
- Comment en mode commande visualise t-on les services sous Linux ?
- Comment connaitre l'état du service cron sous Linux ? Arrêter puis démarrer le.
- Comment connaitre l'état du service station de travail en mode commande et graphique sous Windows 10?
- Comment visualise t-on les journaux sous Linux et Windows server?
- Mettre à jour votre système Linux.

Administration à distance

- Administrer votre serveur Linux d'un client en W10 avec Webmin. Justifier l'installation et tester le bon fonctionnement.
- Administrer votre serveur Windows 2019 depuis un client Windows 10.

Tests

Faire les tests sous Windows, en créant les sous-dossiers et les fichiers nécessaires et en vous connectant en tant qu'employé, directeur et administrateur, Liam localement et à distance (avec les droits nécessaires).

Chaque étape du TP fera l'objet d'un rapport consignant les manipulations effectuées.

💣 **Attention** : avant toute manipulation informatique se rapportant au TP, vous présenterez au professeur responsable votre architecture Active Directory sur papier (à l'aide de Visio) ainsi que les grandes lignes des configurations à mettre en œuvre. **Après acceptation** du responsable, *le show must go on ….*💣

Sécurisation des accès

- Installer le service ssh (openssh-server) sous Linux. Comment fonctionne l'installation de programmes sous Linux. Vérifier l'état du service après installation.
- Administrer votre serveur Linux à partir d'un client Windows avec Putty et winscp. Justifier et expliquer l'utilisation de ssh. A quoi sert ssh dans la communication.
- Utiliser le client filezilla pour vous connecter en sftp au serveur Linux et effectuer un transfert de fichiers sécurisés.
- Administrer un serveur Linux debian 11 à partir d'un serveur Linux debian 11 avec ssh en mode commande. Justifier.
- Montrer avec wireshark que les données sont chiffrées (exemple protocole rdp3389 et ssh 22)
- Les employés ne peuvent pas se connecter en dehors des heures de travail des jours ouvrables.

Tests

Faire les tests sous Windows, en créant les sous-dossiers et les fichiers nécessaires et en vous connectant en tant qu'employé, directeur et administrateur, Liam localement et à distance (avec les droits nécessaires).

GPO

- Création d'une GPO Bureau SrvEtude lié à l'UO Etude pour les employés seulement et qui configure les paramètres suivants :
  - ✓ Supprimer le menu Exécuter du menu Démarrer
  - ✓ Empêcher l'accès au Panneau de configuration
  - ✓ Cacher l'icône Favoris réseau sur le bureau
  - ✓ Supprimer les Connexions réseau du menu Démarrer
  - ✓ Supprimer « connecter un lecteur réseau » et « Déconnecter un lecteur réseau ».

- Les stratégies de mots de passe seront sur 8 caractères dans le domaine et de 6 caractères dans l'unité d'organisation personnel

- Laquelle de ces stratégies est appliquée ?

- Les membres de l'unité d'organisation personnel devront accéder sur leur bureau au strict minimum (pas accès à exécuter, à rechercher, ….):

- Création d'une GPO ***CxCommun*** afin que chaque ordinateur du domaine ait un lecteur ***N:*** connecté au dossier partagé ***Commun*** de l'entreprise

- L'application **putty-64bit-0.80-installer.msi** dans \\dataetud\commun1I\B1-B3 sera déployée pour chaque client de l'unité Id'organisation personnel.

Chaque étape du TP fera l'objet d'un rapport consignant les manipulations effectuées.
💣 **Attention** : avant toute manipulation informatique se rapportant au TP, vous présenterez au professeur responsable votre architecture Active Directory sur papier (à l'aide de Visio) ainsi que les grandes lignes des configurations à mettre en œuvre. **Après acceptation** du responsable, *le show must go on ….*💣

Exemple :

- **Bien définir vos tâches dans azuredevops**
- serveur Core : A quoi cela sert, la mise en oeuvre, à mettre dans le réseau (commande sconfig) - version standard et 1 partition (mettre un nom au serveur, configurer le réseau, l'adhérer au domaine Administrer Server Core | Microsoft Docs
- Attention de bien actualiser le schéma réseau
- travail sur les uo et comptes
- travail sur répertoire de base, commun et permissions ntfs

Azuredevops :
création d'un nouveau projet agile: B1-B3 JLT&AT
ajouter les compte des JL Turrel et Arthur Trouillon en les mettant project administrator
créer des feature --> userstory-->tâches-->compétence-->cpte rendu -->temps
exemple : la réplication active directory
La **réplication** automatique de la base de données d'annuaire entre contrôleurs de domaine, n'a pas d'autre vocation que d'assurer une disponibilité permettant la continuité de l'activité. (PCA)
La Feature : plan continuité d'activité mettre une description
userstory :
les étapes de la réplication active directory
Tâches

- création du premier contrôleur AD
- création du deuxième contrôleur AD avec mise en place de la réplication
- tests montrant la réplication
- tests montrant l'arrêt d'un contrôleur AD
- ....

Compétences : Gérer le patrimoine informatique - Vérifier les conditions de la continuité d'un service informatique