REALISATIONS

Activité professionnelle n°1

Mise en place d'un contrôleur de domaine Active Directory sous Windows Server

1. Présentation du contexte

Dans de nombreuses entreprises, la gestion des utilisateurs et des ressources informatiques doit être centralisée afin de faciliter l'administration du système d'information.

Lorsque plusieurs postes de travail sont présents sur un réseau, il devient rapidement difficile de gérer individuellement les comptes utilisateurs, les accès aux ressources ou encore les stratégies de sécurité.

Afin de répondre à ces problématiques, les entreprises utilisent généralement un service d'annuaire permettant de centraliser la gestion des identités et des ressources du réseau.

Dans l'environnement Microsoft, ce rôle est assuré par Active Directory Domain Services (AD DS).

Active Directory permet de gérer de manière centralisée :

- les utilisateurs
- les ordinateurs
- les groupes
- les politiques de sécurité
- les ressources réseau

Dans le cadre de cette activité professionnelle réalisée en environnement de laboratoire, l'objectif est de mettre en place une infrastructure Active Directory permettant de centraliser la gestion des utilisateurs d'un réseau informatique.

Cette infrastructure repose sur un serveur Windows Server 2022 configuré en contrôleur de domaine, ainsi que sur plusieurs postes clients intégrés au domaine.

2. Problématique

Dans un réseau informatique comportant plusieurs postes de travail, l'administration locale de chaque machine peut rapidement devenir complexe et chronophage.

Chaque ordinateur possède ses propres comptes utilisateurs et ses propres paramètres de sécurité, ce qui rend difficile :

- la gestion des accès
- la sécurisation des comptes
- l'administration globale du réseau

La problématique est donc la suivante :
Comment centraliser la gestion des utilisateurs et des ressources d'un réseau informatique afin de simplifier l'administration et améliorer la sécurité ?

La solution consiste à mettre en place un contrôleur de domaine Active Directory permettant de centraliser l'authentification et l'administration des comptes utilisateurs.

3. Analyse de la solution

Plusieurs solutions existent pour gérer les utilisateurs dans un réseau informatique.

Gestion locale des comptes
Chaque ordinateur possède ses propres comptes utilisateurs.

Avantages :

- mise en place simple

Inconvénients :

- administration difficile
- absence de centralisation
- gestion complexe dans les grandes infrastructures

Utilisation d'un annuaire LDAP
Certaines infrastructures utilisent un annuaire LDAP sous Linux.

Avantages :

- solution flexible
- open source

Inconvénients :

- configuration plus complexe
- moins intégré aux environnements Windows

Active Directory

Active Directory est une solution développée par Microsoft permettant de gérer les utilisateurs et les ressources d'un réseau.

Avantages :
- gestion centralisée
- administration simplifiée
- intégration native avec Windows
- gestion des stratégies de sécurité (GPO)

Inconvénients :
- nécessite un serveur Windows

Solution retenue
La solution retenue est Active Directory Domain Services, car elle permet de répondre efficacement aux besoins de centralisation de la gestion des utilisateurs et des ressources.

4. Architecture technique

L'infrastructure mise en place est composée des éléments suivants :

Équipement	Rôle
Windows Server 2022	Contrôleur de domaine
Poste client Windows	Ordinateur membre du domaine
Réseau local	Communication entre les machines

Schéma simplifié :

Poste client 1
|
Poste client 2
|
Réseau
|
Windows Server 2022
Contrôleur de domaine
Active Directory

Le serveur assure les fonctions suivantes :
- authentification des utilisateurs
- gestion des comptes
- administration des ressources réseau

5. Mise en œuvre technique

Installation de Windows Server

La première étape consiste à installer le système d'exploitation Windows Server 2022 sur une machine virtuelle.

Les paramètres suivants sont configurés :

- nom du serveur
- adresse IP fixe
- configuration réseau

Exemple de configuration réseau :

Paramètre	Valeur
Adresse IP	192.168.1.10
Masque	255.255.255.0
Passerelle	192.168.1.1
DNS	192.168.1.10

Installation du rôle Active Directory

Depuis le Gestionnaire de serveur, le rôle Services de domaine Active Directory est installé.

Étapes :

1. ouvrir le gestionnaire de serveur
2. sélectionner Ajouter des rôles et fonctionnalités
3. choisir Services AD DS
4. lancer l'installation

Une fois le rôle installé, le serveur doit être promu en contrôleur de domaine.

Promotion du serveur en contrôleur de domaine
La promotion du serveur permet de créer une nouvelle forêt Active Directory.
Paramètres configurés :

- nouveau domaine
- nom du domaine

Exemple : btssiogv.local

Un mot de passe de restauration des services d'annuaire est également défini.
Une fois la configuration terminée, le serveur redémarre et devient contrôleur de domaine.

Création d'unités organisationnelles (OU)

Les unités organisationnelles permettent d'organiser les objets dans Active Directory.

Exemple d'organisation :

```
Entreprise
  |
  |---- Utilisateurs
  |---- Ordinateurs
  |---- Administrateurs
```

Cette structure facilite l'administration et l'application des stratégies.

Création d'utilisateurs

Des comptes utilisateurs sont ensuite créés dans l'annuaire.

Exemple :

Nom	Identifiant
Jean Dupont	jdupont
Marie Martin	mmartin

Chaque utilisateur dispose :

- d'un identifiant
- d'un mot de passe
- de droits d'accès spécifiques

Intégration d'un poste au domaine

Un poste client Windows est ensuite intégré au domaine.

Étapes :

1. ouvrir les paramètres système
2. modifier l'appartenance au domaine
3. saisir le nom du domaine

Exemple : btssiogv.local

Après redémarrage, les utilisateurs peuvent se connecter avec leur compte Active Directory.

6. Tests et validation

Plusieurs tests sont réalisés afin de vérifier le bon fonctionnement de l'infrastructure.

Test d'authentification
Connexion d'un utilisateur au poste client avec un compte Active Directory.

Résultat : connexion réussie.

Test de communication réseau

Commande utilisée : ping serveur

Résultat : communication fonctionnelle.

Test de gestion des utilisateurs
Création d'un nouvel utilisateur dans Active Directory.

Résultat : le compte est immédiatement utilisable sur le réseau.

7. Résultats obtenus

La mise en place du contrôleur de domaine permet de centraliser la gestion des utilisateurs et des ressources du réseau.

Les avantages observés sont :

- administration simplifiée
- gestion centralisée des comptes
- amélioration de la sécurité
- meilleure organisation des ressources

Les utilisateurs peuvent désormais se connecter sur n'importe quel poste du domaine avec leurs identifiants.

8. Conclusion

La mise en place d'un contrôleur de domaine Active Directory constitue une étape essentielle dans la gestion d'une infrastructure informatique.

Cette activité professionnelle a permis de comprendre le fonctionnement d'un annuaire Active Directory ainsi que les différentes étapes nécessaires à sa mise en place.

Elle a également permis de mettre en pratique plusieurs compétences liées à l'administration des systèmes Windows et à la gestion d'un réseau informatique.

Compétences mobilisées

- installer un serveur Windows
- configurer un contrôleur de domaine
- administrer Active Directory
- gérer les utilisateurs et les groupes
- intégrer un poste client dans un domaine