

Procédure de configuration d'un Active Directory, DHCP, DNS et GPO



Gildas CHERAUD BOISTEAU

BTS Service Informatique aux Organisations option SISR

Sommaire

- 1 - Descriptif du projet
- 2 - Plan d'adressage du réseau
- 3 - Configuration du serveur
- 4 - Mise en place de l'Active Directory
- 5 - Configuration du service DNS
- 6 - Configuration du service DHCP
- 7 - Création des OU, utilisateurs et groupes
 - 8 - Déploiement des GPO
 - 9 - Conclusion

1. Descriptif du projet

L'objectif de ce projet est de créer, à la demande d'un CFA, un lab reprenant l'infrastructure de l'école, et cela, pour permettre aux élèves en première année de BTS SIO de s'entraîner sur divers sujets qui sont :

- Gestion des utilisateurs et des ressources via Active Directory
- Résolution de noms avec DNS
- Attribution automatique d'adresses IP via DHCP
- Application de stratégies de sécurité via GPO

2. Plan d'adressage réseau

Outil	Adresse associé
Réseau local LAN	192.168.1.x/24
Serveur AD/DNS/DHCP	192.168.1.10
Passerelle	192.168.1.1
Plage DHCP	192.168.1.50 à 192.168.1.200
Exclusions DHCP	192.168.1.1 ; 192.168.1.10
Domaine	sio2426.local

3. Configuration du serveur

3.1 Paramétrage réseau

Avant toute configuration, il est essentiel de définir une adresse IP fixe au serveur afin qu'il soit toujours joignable par les clients et les services réseau.

- Adresse IP : 192.168.1.10
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1
- DNS préféré : 127.0.0.1 (le serveur lui-même)
- Nom de la machine : SRV-AD

Ces paramètres doivent être configurés dans les propriétés de la carte réseau du serveur via le Centre Réseau et Partage ou via PowerShell.

3.2 Installation des rôles

Une fois le serveur configuré, il faut installer les rôles nécessaires à l'infrastructure :

- Active Directory Domain Services (AD DS) : pour gérer les utilisateurs, groupes et ordinateurs dans un domaine.
- DNS Server : pour la résolution de noms dans le réseau local.
- DHCP Server : pour attribuer dynamiquement des adresses IP aux clients.

Ces rôles peuvent être installés via le gestionnaire de serveur (Server Manager) ou en ligne de commande avec PowerShell.

4. Mise en place de l'Active Directory

4.1 Création du domaine

- Promouvoir ce serveur en contrôleur de domaine
- Créer une nouvelle forêt
- Nom du domaine : sio2426.local
- Définir le mot de passe MDPAdmin44*
- Redémarrer le serveur

*Le mot de passe, dans une vraie procédure technique utilisée en entreprise, serait stocké sur un coffre fort numérique sécurisé.

4.2 Vérification

- Ouvrir Active Directory Utilisateurs et Ordinateur
- Vérifier la présence du domaine sio2426.local
- Vérifier les enregistrements DNS avec nslookup

5. Configuration du service DNS

5.1 Zone directe

La zone directe permet de résoudre les noms de domaine vers des adresses IP.

- Ouvrir le gestionnaire DNS (dnsmgmt.msc).
- Vérifier que la zone "sio2426.local" a bien été créée automatiquement lors de la promotion du serveur en contrôleur de domaine.
- Ajouter manuellement des enregistrements de type A si nécessaire (ex. : PC01 → 192.168.1.51).

Cela garantit que les clients peuvent résoudre les noms internes du domaine.

5.2 Zone inverse

La zone inverse permet de résoudre les adresses IP vers des noms de domaine.

- Dans le gestionnaire DNS, créer une nouvelle zone principale.
- Choisir une zone de type “reverse lookup”.
- Saisir le réseau : 192.168.1.0/24.
- Valider et vérifier que les enregistrements PTR sont bien créés automatiquement pour les machines du domaine.

Cette zone est utile pour les diagnostics réseau et certains services qui nécessitent une résolution inverse.

6. Configuration du service DHCP

6.1 Création de l'étendue

L'étendue définit la plage d'adresses IP que le serveur DHCP peut attribuer aux clients.

- Nom de l'étendue : Etenduesio
- Plage d'adresses : de 192.168.1.50 à 192.168.1.200
- Adresses exclues : 192.168.1.1 (passerelle), 192.168.1.10 (serveur)
- Durée du bail : 8 jours

Cette configuration permet d'éviter les conflits d'adresses IP et de garantir une attribution dynamique efficace.

6.2 Options DHCP

Les options DHCP permettent de transmettre des paramètres réseau supplémentaires aux clients.

- Option 003 (Routeur) : 192.168.1.1
- Option 006 (Serveur DNS) : 192.168.1.10
- Option 015 (Nom de domaine) : sio2426.local

Ces options assurent que les clients reçoivent les bons paramètres pour communiquer sur le réseau et rejoindre le domaine.

6.3 Autorisation du serveur DHCP

Pour que le serveur DHCP puisse fonctionner dans un environnement Active Directory, il doit être autorisé dans le domaine.

- Ouvrir le gestionnaire DHCP.
- Clic droit sur le serveur → “Autoriser”.
- Vérifier que le serveur est bien reconnu comme autorisé dans le domaine.

Cette étape est indispensable pour éviter que le serveur soit bloqué par les contrôles de sécurité du domaine.

7. Création des OU, utilisateurs et groupes

7.1 Organisation du domaine

Une bonne organisation de l’annuaire Active Directory facilite la gestion des utilisateurs et des stratégies.

- Créer les unités d’organisation (OU) suivantes :
 - Admin
 - Profs
 - Eleves

Ces OU permettent de regrouper les comptes selon leur rôle et d’appliquer des GPO spécifiques à chaque groupe.

7.2 Création d'un utilisateur

- Nom : eleve01
- Prénom : Eleve
- Nom de famille : 01
- UPN : eleve01@sio2426.local
- OU : Eleves
- Mot de passe : MotDePasse123!
- Activer le compte

7.3 Création d'un groupe

Les groupes facilitent la gestion des droits et des accès.

- Nom du groupe : G_Eleves
- Type : Groupe global
- Emplacement : OU "Eleves"
- Ajouter l'utilisateur "eleve01" au groupe

Ce groupe pourra ensuite être utilisé pour appliquer des stratégies ou attribuer des autorisations sur les ressources réseau.

8. Déploiement des GPO

8.1 GPO Sécurité Élèves

La stratégie de groupe (GPO) “Sécurité_Élèves” est conçue pour renforcer la sécurité et limiter les actions des utilisateurs dans l’OU “Élèves”.

Étapes de création :

- 1 . **Ouvrir la console de gestion des stratégies de groupe** (gpmc.msc).
- 2 . **Créer une nouvelle GPO** nommée “Sécurité_Élèves”.
- 3 . **Configurer les paramètres suivants :**
 - **Interdiction d’accès au Panneau de configuration** Chemin : Configuration utilisateur → Modèles d’administration → Panneau de configuration Paramètre : “Interdire l’accès au Panneau de configuration et aux paramètres du PC”
 - **Définir un fond d’écran personnalisé** Chemin : Configuration utilisateur → Modèles d’administration → Bureau → Active Desktop Paramètre : “Activer Active Desktop” + “Définir le fond d’écran” (Le fichier image doit être accessible via un partage réseau ou local)
 - **Bloquer l’accès à l’invite de commandes** Chemin : Configuration utilisateur → Modèles d’administration → Système Paramètre : “Empêcher l’accès à l’invite de commandes”
- 4 . **Lier la GPO à l’OU “Élèves”** pour qu’elle s’applique uniquement aux utilisateurs de cette unité.
- 5 . **Sur un poste client** avec le CMD, forcer l’application des stratégies avec la commande : `/gpupdate /force*`

*Le /force permet de forcer le push des GPO sur le poste, sinon, il faut attendre le redémarrage ou un délai.

9. Conclusion

Ce projet a permis de mettre en place une infrastructure réseau pédagogique complète, fidèle à celle d'un environnement professionnel. Les élèves disposent désormais :

- D'un domaine Active Directory fonctionnel pour la gestion centralisée des comptes.
- D'un service DNS pour la résolution des noms internes.
- D'un serveur DHCP pour l'attribution automatique des adresses IP.
- De stratégies de groupe (GPO) pour encadrer l'usage des postes clients.

Cette infrastructure offre un cadre idéal pour les travaux pratiques en BTS SIO, tout en illustrant les principes fondamentaux de l'administration réseau sous Windows Server.