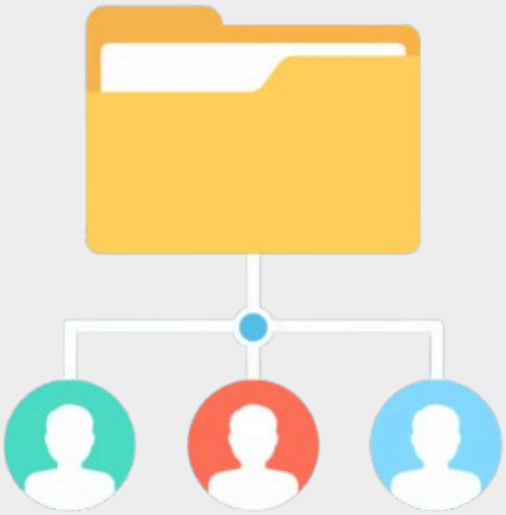


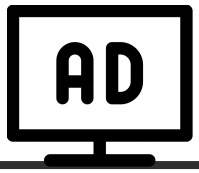
COMPTE RENDU ACTIVE DIRECTORY

NATHAN MARTIN
1SIO2

2024-2025

SOMMAIRE

INTRODUCTION



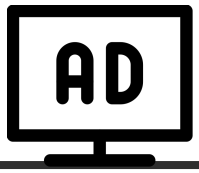
Dans le cadre de ce 4e TP en TC4, j'ai mis en place un domaine Active Directory. Ce travail avait pour objectif de comprendre et de manipuler les principaux éléments d'une infrastructure réseau professionnelle fonctionnant sous environnement Microsoft : serveur Active Directory, comptes utilisateurs, groupes de sécurité, unités d'organisation (OU), partages de ressources et stratégies de sécurité.

L'entreprise fictive utilisée dans le scénario est une société de formation composée de trois types de profils : le personnel administratif, les formateurs et les stagiaires.
L'objectif était de simuler un environnement proche du réel, dans lequel ces utilisateurs accèdent à un réseau structuré et sécurisé à partir de deux postes clients sous Windows 11.

Concrètement, j'ai installé un serveur Windows Server 2022, créé un domaine Active Directory, intégré des postes clients, configuré des comptes utilisateurs et des groupes, puis mis en place des partages réseau avec des droits d'accès adaptés à chaque profil.

Ce compte rendu présente l'ensemble des étapes suivies pour la mise en place complète du domaine Active Directory.

C'EST QUOI ACTIVE DIRECTORY ?



Active Directory (AD) est un service d'annuaire développé par Microsoft, utilisé dans les systèmes Windows Server. Il permet de centraliser et d'automatiser la gestion des utilisateurs, des ordinateurs, des groupes et des ressources (comme les imprimantes ou les dossiers partagés) dans un réseau professionnel.
Active Directory repose sur une structure hiérarchique appelée arborescence.

Cette arborescence est composée :

- d'une **forêt**, qui contient un ou plusieurs domaines (comme D-nathan.local)
- de **unités d'organisation (UO)**, qui permettent de classer les objets (utilisateurs, PC...) par service ou par type
- de **groupes de sécurité**, utilisés pour attribuer des droits d'accès à plusieurs utilisateurs en même temps.

AD utilise plusieurs technologies pour fonctionner :

- **DNS** : pour résoudre les noms des machines sur le réseau
- **LDAP** : pour interroger l'annuaire
- **Kerberos** : pour l'authentification sécurisée.

Grâce à AD, il est possible de gérer l'ensemble du réseau depuis un seul serveur, de déployer des stratégies de sécurité (GPO), et de faire gagner du temps aux administrateurs en évitant des configurations manuelles sur chaque poste. C'est la base de toute infrastructure professionnelle en environnement Windows.

Architecture du réseau interne

Ce schéma représente la topologie réseau simulée : un serveur contrôleur de domaine (SRV-nathan) et deux clients Windows 11 intégrés au domaine D-nathan.local via un réseau interne.

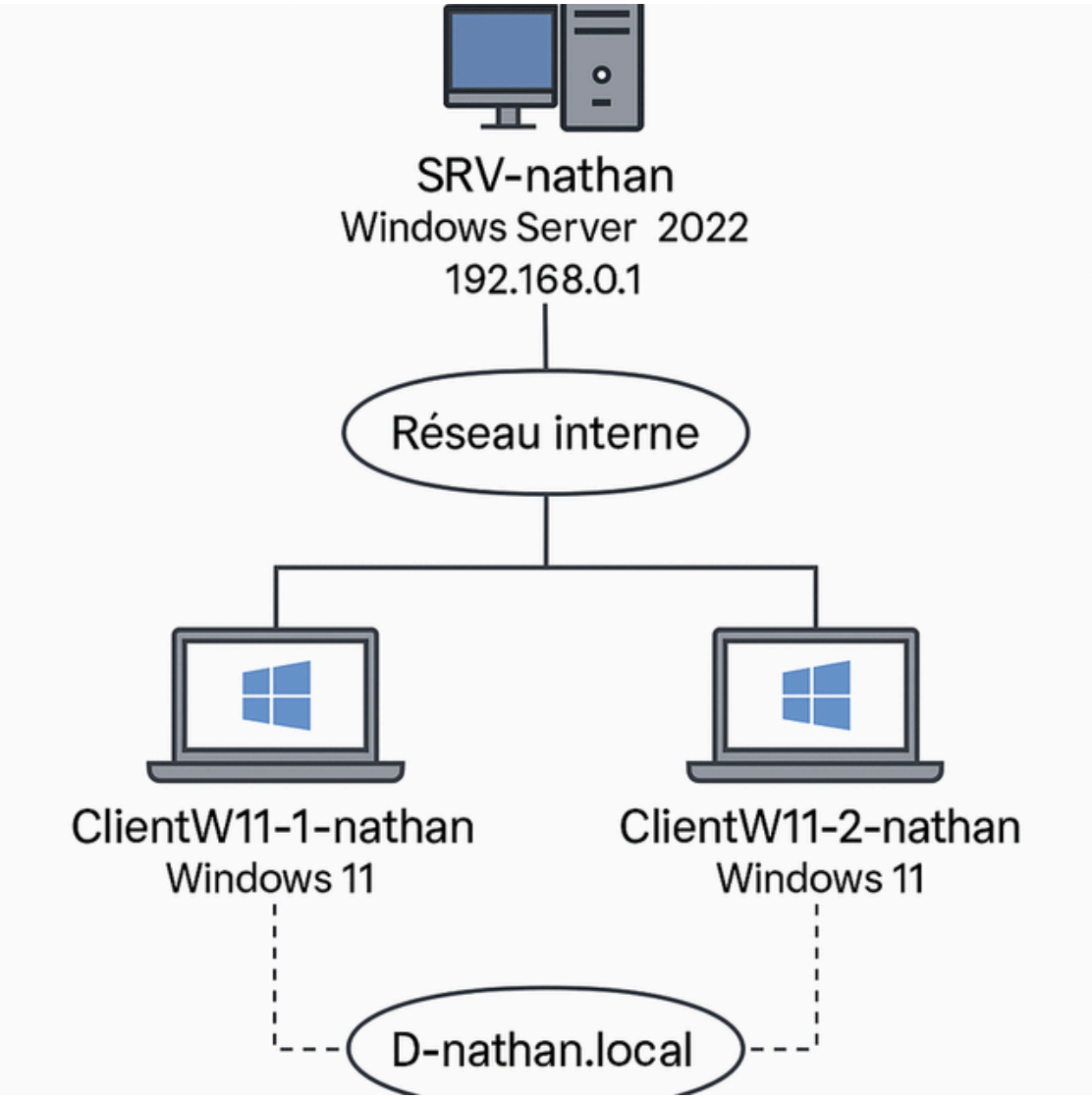


Schéma réalisé avec **Excalidraw**

INSTALLATION DU SERVEUR WINDOWS SERVER 2022

J’ai commencé par importer une machine virtuelle depuis l’image type T-W2022, disponible sur le réseau de l’établissement.

J’ai ensuite configuré l’adresse IP statique du serveur en 192.168.0.1/24, désactivé IPv6, puis défini le DNS sur 127.0.0.1 (localhost). Le serveur a été renommé SRV-nathan, comme demandé, puis redémarré. Après redémarrage, j’ai effectué les mises à jour du système via Windows Update.

J’ai ensuite modifié la stratégie de sécurité locale via secpol.msc pour assouplir les règles de mot de passe : complexité, longueur minimale, durée de validité. J’ai poursuivi en ajoutant le rôle AD DS (Active Directory Domain Services) depuis le Gestionnaire de serveur.

Une fois le rôle installé, j’ai promu le serveur en contrôleur de domaine, en créant une nouvelle forêt nommée D-nathan.local. L’installation a été laissée par défaut et s’est conclue par un redémarrage.

Après redémarrage, j’ai défini le mot de passe de l’administrateur du domaine (Azerty32), puis créé un compte d’administrateur de secours (admin / Azerty31). J’ai ensuite configuré un redirecteur DNS dans la console DNS.

Enfin, j’ai accédé aux outils d’administration (via le gestionnaire de serveur et MMC) en ajoutant les modules nécessaires : Utilisateurs et ordinateurs Active Directory, Stratégies de groupe, et DNS. Pour terminer, j’ai modifié la stratégie de mot de passe du domaine via la stratégie "Default Domain Policy", en cohérence avec les règles locales.

Le serveur est ainsi prêt à accueillir des clients et à gérer l’environnement Active Directory de l’entreprise.

AJOUT DES DEUX CLIENTS AU DOMAINE

Après la configuration du serveur, j'ai créé deux machines virtuelles sous Windows 11, que j'ai nommées respectivement ClientW11-1-nathan et ClientW11-2-nathan. Ces deux postes représentent les ordinateurs utilisés par les membres de l'entreprise simulée.

J'ai attribué à chaque machine une adresse IP statique dans le même sous-réseau que le serv eur, par exemple 192.168.0.2 et 192.168.0.3, avec un masque de sous-réseau de 255.255.255.0. Le DNS a été configuré pour pointer vers l'adresse IP du serveur (192.168.0.1) afin de permettre la jonction au domaine. Comme pour le serveur, j'ai désactivé IPv6 sur les deux clients pour éviter tout conflit réseau. J'ai ensuite lancé les mises à jour Windows sur chaque poste afin de stabiliser le système.

Sur chaque machine, j'ai créé un compte administrateur local de secours nommé adminloc, avec le mot de passe Azerty31, afin de conserver un accès local même après l'intégration au domaine.

L'étape suivante a été d'intégrer chaque poste au domaine D-nathan.local. Pour cela, je suis passé par le Panneau de configuration, puis dans Système et sécurité, et enfin Système. J'ai cliqué sur "Modifier les paramètres" dans les paramètres du nom d'ordinateur, puis sur le bouton "Modifier" dans l'onglet "Nom de l'ordinateur". J'ai sélectionné l'option "Membre de domaine" et saisi D-nathan.local. Une fenêtre m'a demandé les identifiants d'un compte autorisé à joindre un domaine, j'ai utilisé le compte administrateur du domaine. Après validation, la machine a demandé un redémarrage pour appliquer les changements.
J'ai répété la même procédure pour le deuxième poste.

Enfin, j'ai ouvert la console Utilisateurs et ordinateurs Active Directory sur le serveur pour vérifier que les deux machines ClientW11-1-nathan et ClientW11-2-nathan étaient bien présentes dans le domaine.

CONFIGURATION DES UO ET RESSOURCES PARTAGÉES

Dans cette partie du TP, j'ai organisé l'Active Directory en créant une hiérarchie logique adaptée à l'entreprise. J'ai commencé par créer une Unité d'Organisation principale (OU) nommée Nathan, qui représente l'entreprise. À l'intérieur, j'ai ajouté deux UO supplémentaires : Salle01 et Salle02, représentant les deux salles de formation. J'ai ensuite déplacé les objets ordinateurs ClientW11-1-nathan dans Salle01 et ClientW11-2-nathan dans Salle02, afin de structurer proprement les postes dans l'annuaire.

J'ai ensuite créé trois Unités d'Organisation pour les utilisateurs : Personnels, Formateurs et Stagiaires. Dans chacune, j'ai créé les comptes nécessaires avec les noms de mon choix : 2 comptes dans Personnels, 2 dans Formateurs et 4 dans Stagiaires. Tous les comptes ont reçu le mot de passe par défaut P@ssW0rd31, avec l'option de changement obligatoire à la première connexion activée. Ensuite, j'ai créé trois groupes de sécurité nommés G_Personnels, G_Formateurs et G_Stagiaires, et j'ai affecté chaque utilisateur au groupe correspondant à son profil.

Côté serveur, j'ai créé un dossier C:\Formation-Cisco que j'ai partagé sous le nom FormationCisco, avec les droits de contrôle total. Ce partage a été monté sur la lettre S: sur les postes clients via l'option "Connecter un lecteur réseau" en utilisant le chemin \\SRV-nathan\FormationCisco.
Dans ce dossier partagé, j'ai ensuite créé plusieurs sous-dossiers : Partage_professeur, Partage_stagiaires et home.
Les droits ont été définis de la manière suivante :

- Les formateurs ont un accès lecture/écriture sur Partage_professeur et Partage_stagiaires.
- Les stagiaires ont un accès lecture seule sur Partage_stagiaires.
- Chaque utilisateur dispose d'un dossier personnel dans S:\FormationCisco\home, avec un accès privé.

Enfin, pour automatiser le montage des dossiers à la connexion, j'ai préparé un script (connexion.bat) de connexion qui mappe les lecteurs selon le nom d'utilisateur (%username%). Ce script, au format .bat, est exécuté automatiquement lors de la connexion à une session utilisateur membre du domaine D-nathan.local.

```
@echo off
net use S: \\SRV-nathan\FormationCisco
net use T: \\SRV-nathan\FormationCisco\Partage_stagiaires
net use P: \\SRV-nathan\FormationCisco\Partage_professeur
net use H: \\SRV-nathan\FormationCisco\home\%username%
exit
```

Explication des commandes :

- @echo off

→ Ça empêche l'affichage des commandes dans la fenêtre, pour garder le script propre à l'exécution.

- net use S: \\SRV-nathan\FormationCisco

→ C'est pour monter le dossier partagé principal FormationCisco sur la lettre S

- net use T: \\SRV-nathan\FormationCisco\Partage_stagiaires

→ Monte le dossier partagé destiné aux stagiaires sur la lettre T

- net use P: \\SRV-nathan\FormationCisco\Partage_professeur

→ Monte le dossier partagé destiné aux formateurs sur la lettre P

- net use H: \\SRV-nathan\FormationCisco\home\%username%

→ Monte automatiquement un dossier personnel pour l'utilisateur connecté, en fonction de son nom d'utilisateur, sur la lettre H:. %username% est une variable système qui récupère dynamiquement le nom de la session.

- exit

→ Termine l'exécution du script proprement.

Une fois le script écrit, je l'ai placé dans le dossier spécial du domaine prévu pour les scripts de connexion. C'est à cet endroit que le contrôleur de domaine va chercher les scripts à exécuter lors de la connexion d'un utilisateur.

Pour que le script s'exécute automatiquement à chaque ouverture de session, je suis allé dans la console Utilisateurs et ordinateurs Active Directory, j'ai ouvert les propriétés de chaque utilisateur, puis dans l'onglet Profil, j'ai renseigné connexion.bat dans le champ Script de connexion. Cette configuration permet d'appliquer le script à l'utilisateur concerné, sans intervention supplémentaire.

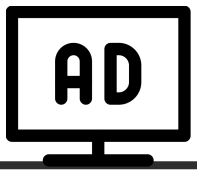
Grâce à cette mise en place, chaque utilisateur voit ses lecteurs réseau monter automatiquement dès qu'il se connecte au domaine. ça garantit une expérience simple, cohérente et bien organisée, tout en respectant la logique d'accès selon les profils définis (formateurs, stagiaires, personnels...).

Pour terminer, j'ai aussi mis en place les droits NTFS pour sécuriser l'accès aux dossiers partagés. J'ai trouvé ça plus logique et plus pratique de les gérer par groupe d'utilisateurs, plutôt que de le faire utilisateur par utilisateur. Une fois les groupes créés dans Active Directory, il suffit ensuite de les lier aux bons dossiers, et tous les membres du groupe ont directement les bons droits d'accès. C'est simple, efficace, et surtout plus facile à gérer si on rajoute ou retire des utilisateurs plus tard.

J'ai donc créé trois groupes : G_Personnels, G_Formateurs et G_Stagiaires, qui correspondent aux différents types de profils dans l'entreprise fictive du TP. Ensuite, j'ai attribué des droits spécifiques selon le groupe. Par exemple, les formateurs ont lecture et écriture sur Partage_professeur et Partage_stagiaires, alors que les stagiaires, eux, ont seulement un accès en lecture seule sur Partage_stagiaires. Ça permet d'éviter qu'ils modifient des fichiers qui ne leur sont pas destinés.

Pour les dossiers personnels, dans S:\FormationCisco\home, j'ai fait en sorte que seul l'utilisateur concerné (et les admins bien sûr) puisse y accéder. Chaque utilisateur a donc son propre espace sécurisé, ce qui est important même dans une petite structure comme celle du TP.

CE QUI N'A PAS MARCHÉ ET COMMENT J'AI RÉGLÉ ÇA



Pendant la mise en place de l'infrastructure, j'ai rencontré quelques problèmes techniques, surtout liés à la configuration réseau et à l'intégration des postes clients dans le domaine.

Le premier souci est arrivé quand j'ai voulu intégrer mes deux machines Windows 11 au domaine. Une erreur s'affichait en disant que le domaine était introuvable. J'ai vu que les clients n'avaient pas le bon DNS. En fait, ils ne pointaient pas vers l'adresse IP du serveur. J'ai donc modifié le paramétrage et mis manuellement 192.168.0.1 comme DNS, et là, ça a marché tout de suite.

Ensuite, j'ai eu un autre problème avec le script de connexion des lecteurs réseau. Les dossiers partagés ne se montaient pas automatiquement quand un utilisateur se connectait. En relisant le script, je me suis rendu compte qu'il y avait une faute dans le nom du dossier partagé : j'avais écrit FormationsCisco au lieu de FormationCisco.

Pour finir, j'avais au début mis tous les utilisateurs dans l'OU principale sans vraiment organiser. Mais en relisant la consigne, j'ai vu qu'il fallait créer des UO distinctes pour chaque type d'utilisateur. J'ai donc créé les UO Personnels, Formateurs et Stagiaires, et j'ai déplacé chaque utilisateur dans la bonne UO.

CONCLUSION

Ce TP m'a permis de découvrir concrètement comment mettre en place un domaine Active Directory dans un environnement réseau. J'ai pu installer un serveur Windows Server 2022, le configurer comme contrôleur de domaine, intégrer des clients, créer des utilisateurs, des groupes, des UO, et gérer des droits d'accès adaptés à chaque profil.
Même si certaines étapes ont posé quelques difficultés, comme la configuration réseau ou les scripts de connexion, elles m'ont justement permis de mieux comprendre le fonctionnement global d'un domaine et l'importance de chaque réglage. J'ai également pris conscience de l'intérêt de bien structurer l'annuaire Active Directory et de centraliser la gestion des utilisateurs pour gagner en efficacité.