Mise en place d’un Active Directory

FOUR Lucas
Conseil départemental de la Drôme

Table des matières

Cahier des charges – Expression des besoins

| Descriptif de l'existant |

L'infrastructure de départ étant inexistante, je ne dispose d'aucun service réseau préconfiguré. Mon environnement se limite à un accès à Internet via le réseau local (LAN) du GRETA, qui me permet de télécharger les ressources nécessaires à la mise en place du projet.

| Besoin(s) |

Ce travail pratique a pour objectif de mettre en place une infrastructure de domaine permettant la centralisation de la gestion des utilisateurs, des ordinateurs et des ressources réseau au sein d'un réseau d'entreprise. Cette infrastructure doit offrir une authentification centralisée, une gestion des droits d'accès ainsi que l'application de stratégies de sécurité sur l'ensemble des postes du domaine.

| Contrainte(s) |

La réalisation de ce travail pratique est soumise aux contraintes suivantes :

- **Contrainte de temps** : l'ensemble de l'infrastructure doit être déployé en quatre heures.
- **Contrainte logicielle** : la solution retenue est Active Directory, déployée sur les services de rôle Windows Server.
- **Contrainte système** : l'architecture repose sur deux machines virtuelles — un serveur sous Windows Server faisant office de contrôleur de domaine, et un poste client de référence intégré au domaine.
- **Contrainte fonctionnelle** : l'infrastructure doit permettre l'authentification centralisée, l'application de stratégies de groupe (GPO) et la gestion des droits d'accès au sein du domaine.
- **Contrainte de validation** : le TP sera validé sur le bon fonctionnement du contrôleur de domaine, l'intégration du poste client au domaine et l'application effective des GPO.

Ressources

| Ressources mises à disposition |

Pour la réalisation de ce travail pratique, je dispose d'une machine hôte équipée de l'hyperviseur Hyper-V, utilisé comme solution de virtualisation.
De plus, cette machine est connectée au réseau local (LAN) du GRETA, ce qui me permet de bénéficier d'un accès à Internet nécessaire au téléchargement et à la configuration des différents composants du projet.

| Ressources nécessaires à la mise en place |

Pour la mise en œuvre de ce travail pratique, plusieurs éléments matériels et logiciels sont nécessaires :

- Une machine hôte équipée d'un logiciel de virtualisation (dans ce cas, Hyper-V), afin de créer et gérer les différentes machines virtuelles ;
- Un accès à Internet, indispensable pour le téléchargement des mises à jour, des rôles et des fonctionnalités nécessaires à l'installation et à la configuration d'Active Directory ;
- Les images ISO de Windows Server (destinée à l'installation du contrôleur de domaine) et de Windows 10 ou Windows 11 (utilisées pour les postes clients du domaine) ;
- Les outils d'administration Active Directory, intégrés à Windows Server, permettant la gestion des utilisateurs, des ordinateurs, des groupes et des stratégies de groupe (GPO).

| Gestion des ressources |

Étant donné que le temps imparti pour ce travail pratique est limité à quatre heures, et qu'il inclut l'installation complète d'un serveur Windows Server destiné à héberger Active Directory, ainsi que la mise en place des postes clients intégrés au domaine, j'ai procédé au pré-téléchargement des images ISO nécessaires. Cette préparation en amont permet de gagner du temps lors de la création des machines virtuelles et d'optimiser le déroulement du travail pratique.

Analyse

| Descriptifs des solutions |

- **Active Directory** est un service d'annuaire développé par Microsoft, destiné à la gestion centralisée des utilisateurs, des ordinateurs et des ressources réseau au sein d'un domaine. Installé sur un serveur Windows Server, il repose sur plusieurs services intégrés tels que LDAP, Kerberos et DNS. Active Directory se distingue par sa facilité d'administration, son intégration native avec les systèmes Windows et l'utilisation des stratégies de groupe (GPO) permettant d'appliquer des règles de sécurité et de configuration de manière centralisée. Il s'agit de la solution la plus couramment utilisée dans les environnements professionnels sous Windows.

- **OpenLDAP** est une solution libre et open source fournissant un service d'annuaire basé sur le protocole LDAP. Installé principalement sur des systèmes Linux, OpenLDAP permet également la centralisation des comptes utilisateurs et des informations d'authentification. Il se distingue par sa grande flexibilité et son indépendance vis-à-vis d'un éditeur, mais nécessite une configuration plus complexe et une bonne maîtrise technique. Contrairement à Active Directory, OpenLDAP ne propose pas nativement de mécanismes équivalents aux GPO et requiert l'ajout d'outils complémentaires pour atteindre un niveau de gestion comparable.

| Comparaison des solutions |

Solutions	Active Directory	OpenLDAP
Coûts	Inclus avec Windows Server (solution propriétaire Microsoft)	Gratuit (open source)
OS d'installation	Windows Server	Serveur Linux / Unix
Points forts	Gestion centralisée des utilisateurs et ordinateurs, authentification sécurisée, stratégies de groupe (GPO), intégration native Windows	Solution libre et flexible, basée sur LDAP, indépendante d'un éditeur, adaptable à des environnements variés
Interface / utilisation	Interface graphique conviviale, administration simplifiée via consoles Microsoft	Administration principalement en ligne de commande ou via outils tiers, plus technique
Mise en place	Relativement simple et bien guidée, intégration DNS automatique	Plus complexe, nécessite une configuration manuelle et une bonne maîtrise de LDAP
Communauté / Support	Support officiel Microsoft, documentation abondante	Communauté open source active, documentation communautaire
Idéal pour	Entreprises majoritairement sous Windows, infrastructures réseau structurées	Environnements Linux ou mixtes, structures recherchant une solution libre
Limites	Dépendance à l'écosystème Microsoft, coût des licences Windows Server	Pas de gestion native des GPO, fonctionnalités moins intégrées que Active Directory

| Choix d'une solution – Argumentation |

J'ai choisi d'utiliser **Active Directory** pour ce travail pratique, car il s'agit d'une solution robuste et largement utilisée en environnement professionnel pour la gestion centralisée des utilisateurs et des ressources réseau. Son fonctionnement basé sur une infrastructure de domaine permet d'administrer efficacement les comptes utilisateurs, les ordinateurs et les droits d'accès à partir d'un point central. De plus, Active Directory offre des fonctionnalités avancées telles que l'authentification centralisée, la gestion des stratégies de groupe (GPO) et une intégration native avec les systèmes Windows, facilitant ainsi l'application de règles de sécurité et de configuration sur l'ensemble des postes du domaine.

| Plan d'adressage réseau |

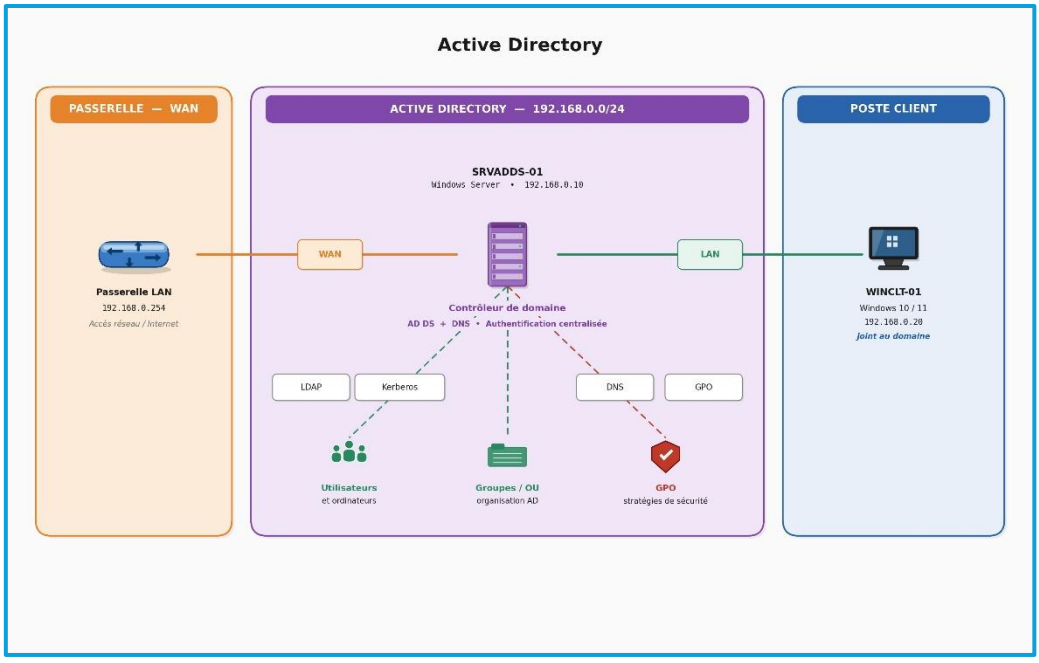
Tableau d'adressage :

Nom du réseau	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
LAN	192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.254	192.168.0.255

Tableau des adresses IP :

Machines	Adresses IP	Masque de sous réseau	Passerelle par défaut	DNS
SRVADDS-01	192.168.0.10	255.255.255.0	192.168.0.254	192.168.0.10
WINCLT-01	192.168.0.20	255.255.255.0	192.168.0.254	192.168.0.10

Schéma réseau :



| Etude de l'impact sur le SI existant |

Étant donné que ce travail s'inscrit dans un contexte de formation, il n'existe aucun système d'information (SI) préexistant, mis à part l'accès à Internet. L'ensemble de l'infrastructure nécessaire à la mise en place d'un domaine Active Directory doit donc être créé et configuré intégralement dans le cadre de ce travail pratique. L'installation d'un serveur Active Directory au sein d'une entreprise permettrait de centraliser la gestion des utilisateurs, des ordinateurs et des ressources réseau, d'améliorer la sécurité grâce à l'authentification centralisée et aux stratégies de groupe (GPO), et de simplifier l'administration du parc informatique. Cette solution contribue également à la standardisation des configurations et à une gestion plus efficace des postes clients.

| Phasage de l'intervention |

Dans un premier temps, j'installerai les machines virtuelles nécessaires à la mise en place d'une infrastructure Active Directory. Cela comprend une machine virtuelle sous Windows Server, destinée à héberger le rôle de contrôleur de domaine, ainsi qu'une machine virtuelle sous Windows 10 qui servira de poste client intégré au domaine. Sur le serveur Windows Server, les services indispensables au fonctionnement d'Active Directory seront installés et configurés, notamment Active Directory Domain Services (AD DS) et le service DNS, essentiels à l'authentification centralisée et à la résolution de noms au sein du domaine. Selon les besoins, le service DHCP pourra également être mis en place afin d'automatiser l'attribution des adresses IP aux postes clients. Une fois l'environnement prêt, je procéderai à la promotion du serveur en contrôleur de domaine, puis à la création du domaine Active Directory. Je joindrai ensuite le poste client au domaine afin de vérifier le bon fonctionnement de l'authentification centralisée. Enfin, je mettrai en place différents objets Active Directory tels que des utilisateurs, des groupes et des unités d'organisation, ainsi que des stratégies de groupe (GPO), dans le but de tester la gestion centralisée des comptes, des postes clients et des règles de sécurité au sein du domaine.

| Prévision des tests et validation |

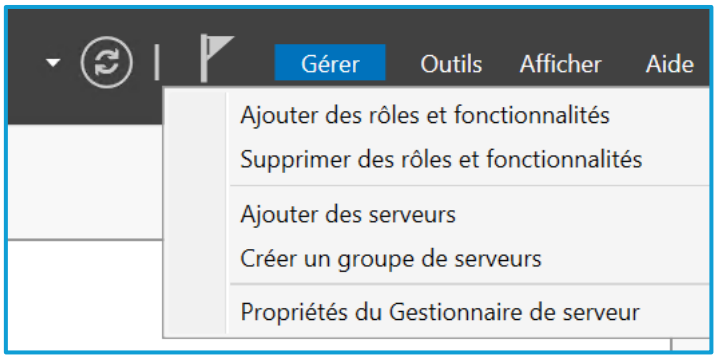
Lors de l'installation des services nécessaires au fonctionnement d'Active Directory, je procéderai à différentes vérifications afin de m'assurer de leur bon fonctionnement. Je contrôlerai notamment que les services Active Directory Domain Services (AD DS) et DNS sont correctement installés, démarrés et opérationnels. Par la suite, lors de l'intégration des postes clients au domaine, je vérifierai que chaque machine rejoint correctement le domaine Active Directory et qu'elle apparaît bien dans la console d'administration Active Directory, au sein des objets ordinateurs ou des unités d'organisation prévues. Enfin, une fois la configuration du domaine finalisée, je testerai la communication entre le serveur et les postes clients, l'authentification des utilisateurs ainsi que l'application des stratégies de groupe (GPO), afin de garantir le bon fonctionnement de la gestion centralisée et de la sécurité au sein de l'infrastructure Active Directory.

Mise en place

| Installer le rôle ADDS |

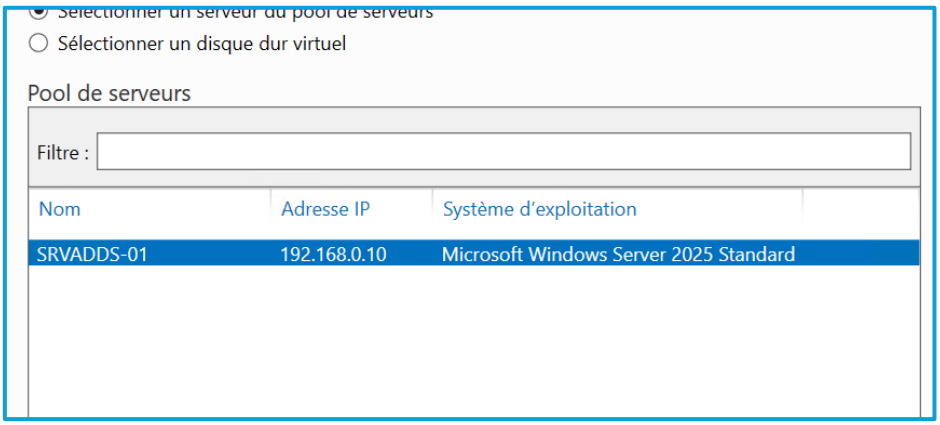
La première étape, avant de créer le domaine Active Directory, consiste à installer le rôle « **ADDS** » : **Active Directory Domain Services**. Il s'agit du rôle permettant de créer un domaine Active Directory.

Ouvrez le Gestionnaire de serveur, puis cliquez sur « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** ».

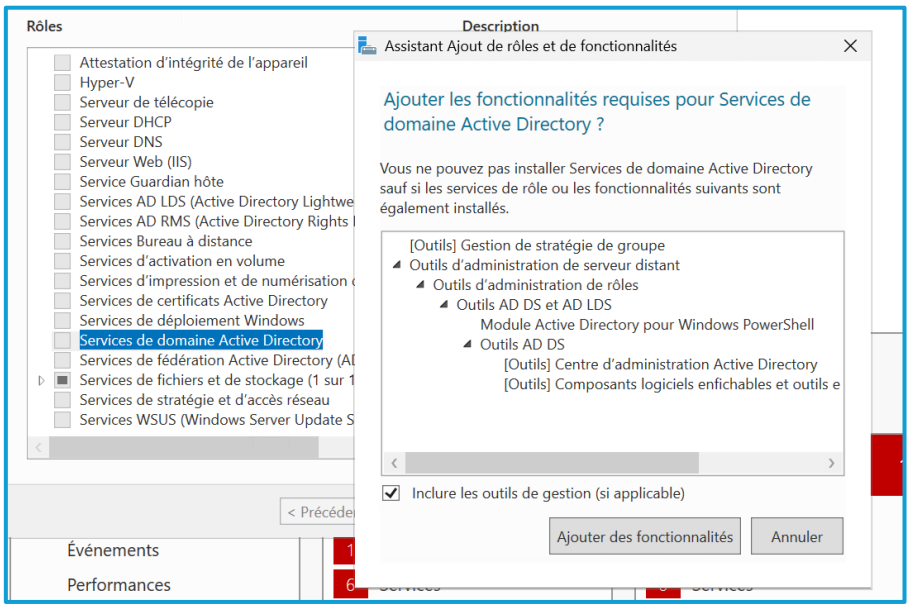


Passez l'étape « **Avant de commencer** » et poursuivez ensuite en laissant le type d'installation sur le choix « **Installation basée sur un rôle ou une fonctionnalité** ».

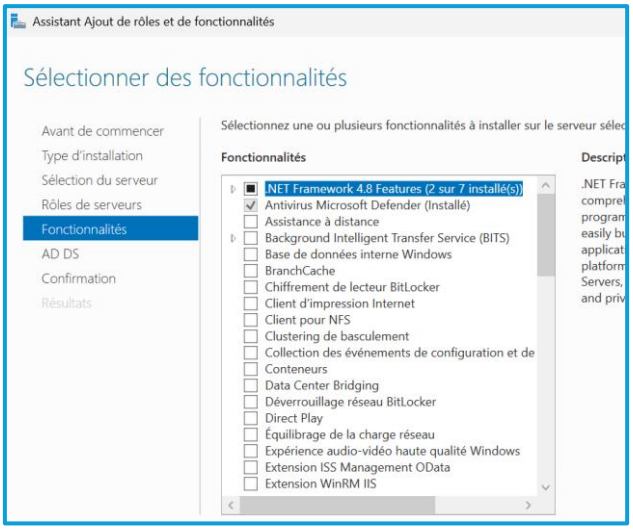
Sélectionnez votre serveur local. En principe, c'est le choix par défaut.



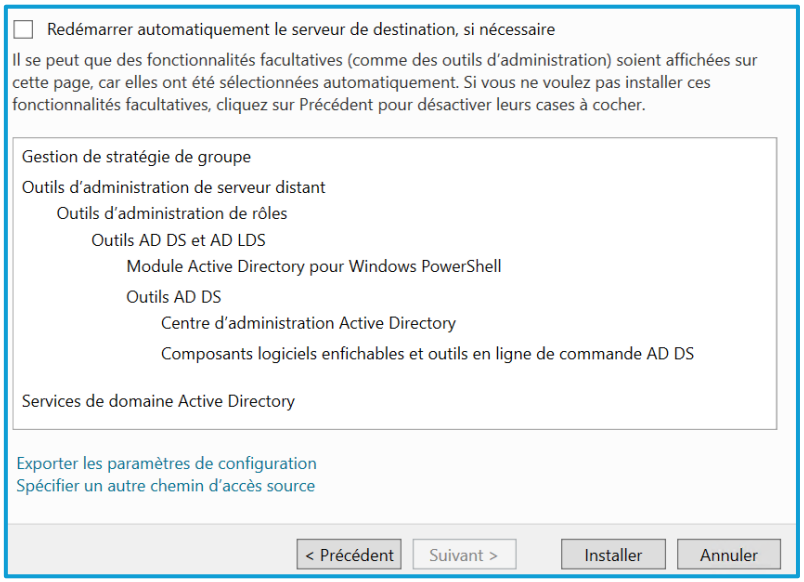
L'étape cruciale de l'installation du rôle est ici, puisqu'il va falloir cocher « **Services AD DS** » dans la liste. Une seconde fenêtre va apparaître pour vous proposer d'installer les outils de gestion : validez. Qui dit outils de gestion, dit console d'administration comme « **Utilisateurs et ordinateurs Active Directory** » mais aussi le module PowerShell pour Active Directory.



Nous n'installons pas de fonctionnalités en plus, donc poursuivez sans rien sélectionner.



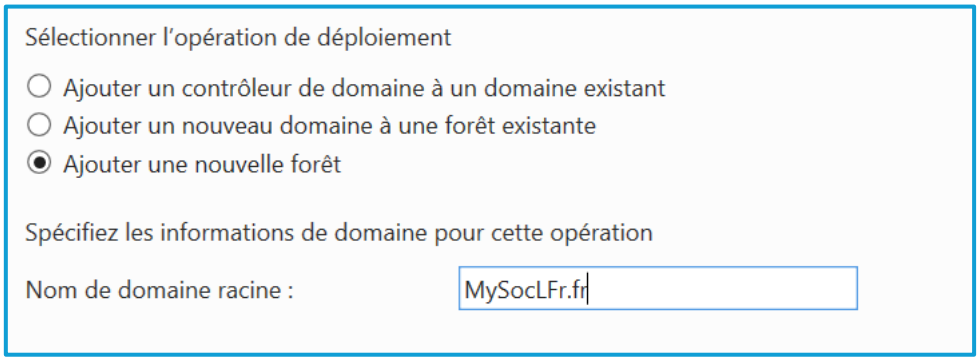
Cliquez sur « **Installer** » pour démarrer l'installation, qui peut prendre quelques minutes.



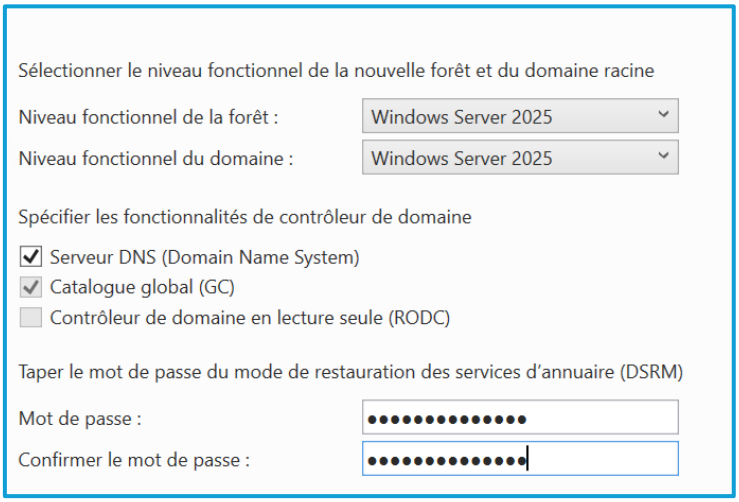
| Créer un domaine Active Directory |

La fameuse commande « **dcpromo** » n'existe plus et laisse place à un message dans le gestionnaire de serveur qui permet de promouvoir le serveur en tant que contrôleur de domaine

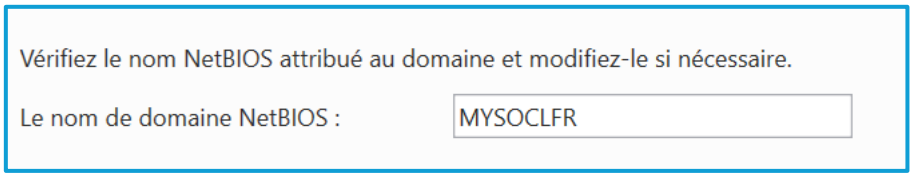
Comme il s'agit d'un nouveau domaine dans une nouvelle forêt, choisissez « **Ajouter une nouvelle forêt** » et indiquez le nom de domaine.



Lors de la création du domaine, le niveau fonctionnel est défini sur Windows Server 2016, ce qui impose l'utilisation de Windows Server 2025 ou supérieur pour les contrôleurs de domaine. Le serveur est configuré comme serveur DNS et Catalogue global. Un mot de passe de restauration de l'annuaire (DSRM) est également défini, distinct du mot de passe Administrateur du domaine.

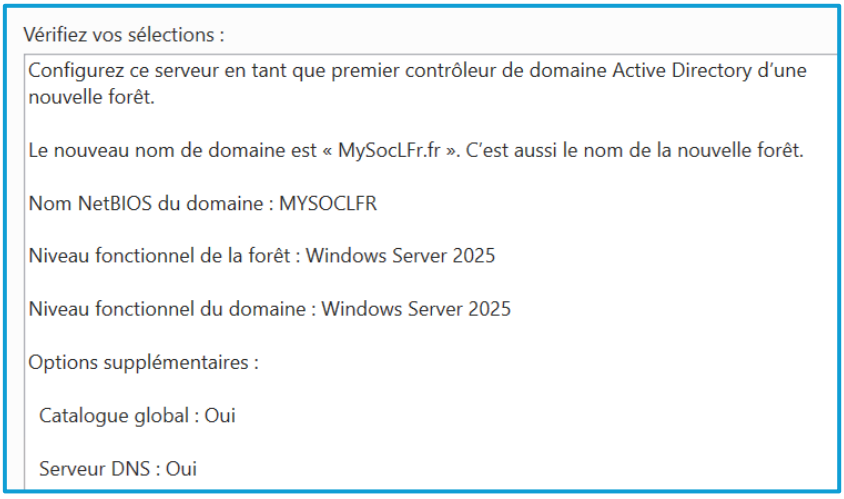


Indiquez un nom NETBIOS pour le domaine, à savoir un nom court et qui ne s'appuie pas sur DNS pour être résolu.



Laissez les chemins par défaut et poursuivez.

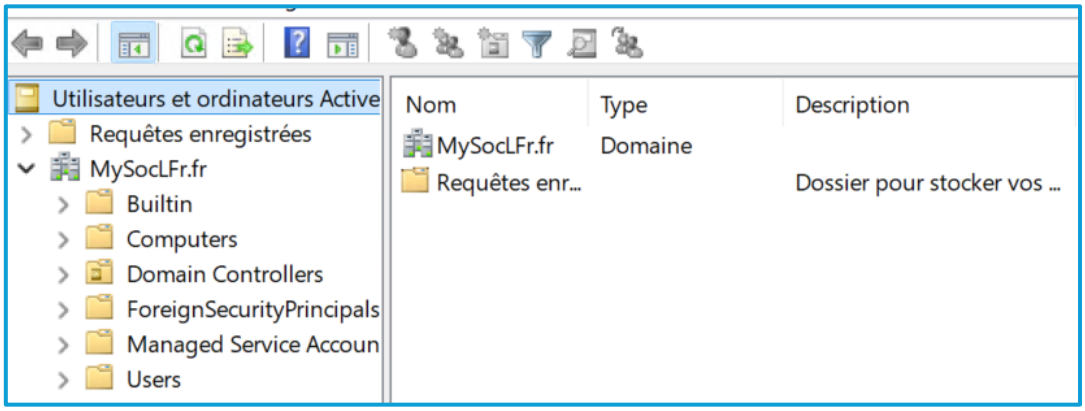
Vérifiez les options et continuez.



Finissez en cliquant sur installer pour démarrer la création de votre domaine et la configuration du DC.

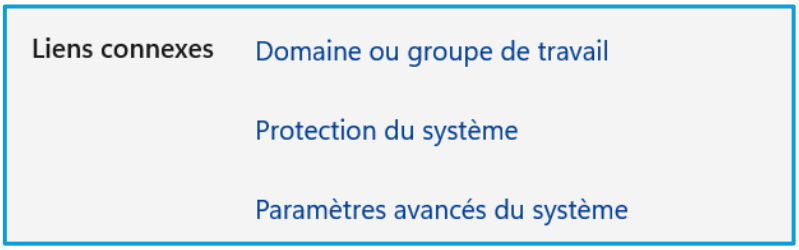
Patientez pendant l'installation. Une fois celle-ci terminée, le serveur redémarre automatiquement.

Après le redémarrage, le domaine Active Directory est opérationnel. Il peut être administré à l'aide des consoles Utilisateurs et ordinateurs Active Directory et Centre d'administration Active Directory, permettant de gérer les utilisateurs, ordinateurs et autres objets du domaine.

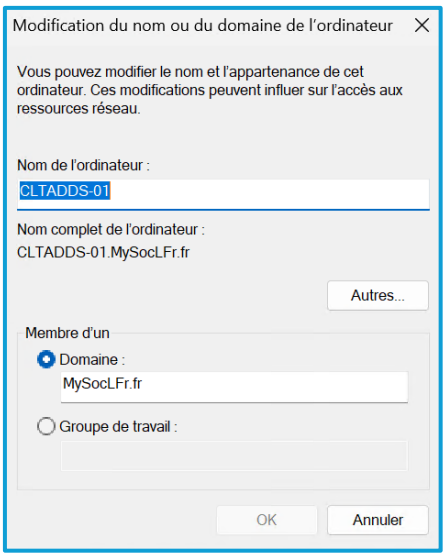


| Ajout du poste client dans le domaine |

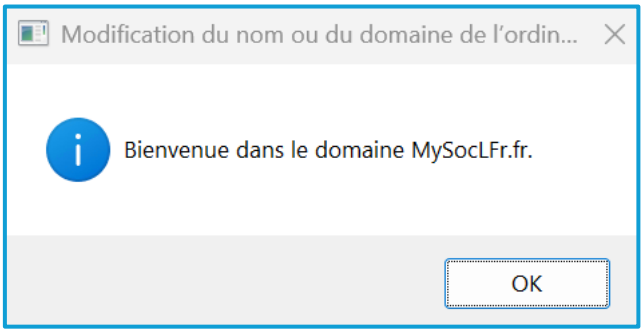
Il faut se rendre dans **« Système »** puis cliquer sur **« Domaine ou groupe de travail »**



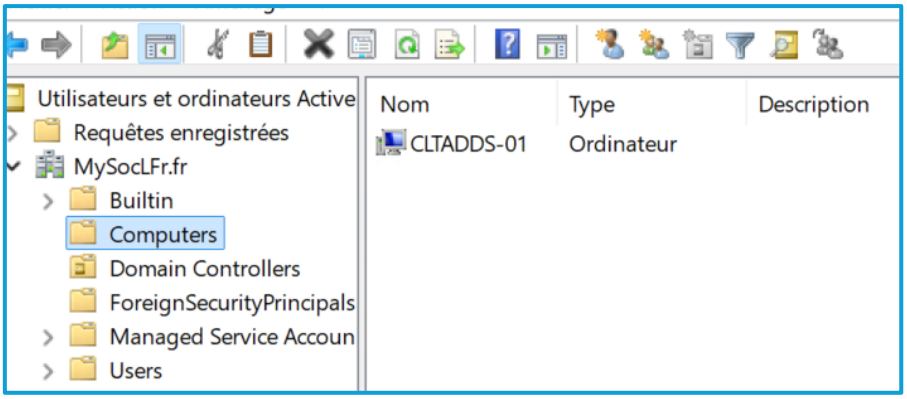
Ensuite il faut cliquer sur **« Modifier »** puis sélectionner **« Domaine »**. Rentrer votre nom de domaine et cliquer sur **« ok »**



Vous allez voir un message apparaitre en vous demandant de rentrer vos identifiants administrateur pour pouvoir ajouter votre client sur le domaine. Une fois rentrer, un message vous dit que votre client et bien sur le domaine.



Sur l'Active Directory, dans le dossier « **Computers** » on peut voir que le poste client est bien remonter dans l'AD.



Conclusion

La mise en place du serveur Active Directory, accompagnée de l'installation et de la configuration de ses différents services, m'a permis de déployer une infrastructure de domaine fonctionnelle et cohérente. Les tests réalisés, notamment l'intégration des postes clients au domaine, l'authentification des utilisateurs et l'application des stratégies de groupe (GPO), ont confirmé le bon fonctionnement et la fiabilité de l'environnement mis en place. Grâce à Active Directory, il est possible de centraliser la gestion des utilisateurs, des ordinateurs et des ressources réseau, tout en renforçant la sécurité et en simplifiant l'administration des postes clients au sein d'un environnement Windows.

Auto-évaluation

Le temps imparti de quatre heures a été respecté, grâce à une bonne préparation en amont, notamment le téléchargement anticipé des ISO et la connaissance préalable de la procédure d'installation. Cette anticipation m'a permis d'optimiser le déroulement du TP et d'atteindre les objectifs fixés dans les délais.