



# MOLECULIS

AT THE HEART OF INNOVATION

---

MOLECULIS™  
Connectés pour innover

---

Gwendal  
Hamissou  
Ahmed  
Jean-Félix



<b>INTRODUCTION</b>	5
1. Contexte Général	5
2. Objectifs	6
3. Évaluation des Besoins	6
3.1. Présentation Organisationnelle et Infrastructure Physique	6
3.1.1. Structure Organisationnelle	6
3.1.2. Infrastructure Physique	7
3.2. Fiabilité et Disponibilité	7
3.3. Connectivité et Collaboration	7
3.4. Scalabilité	8
3.5. Sécurité	8
3.6. Performances	8
4. Cahier des Charges	9
4.1. Objectifs du Projet	9
4.2. Conception du Réseau	9
4.2.1 Segmentation des VLAN	9
4.2.2 Sous-Réseaux	10
4.2.3 Topologie Réseau	10
4.3. Contraintes Techniques	10
4.3.1 Environnement Virtuel	10
4.3.2 Choix des équipements Simulés	11
4.3.3 Connectivité et Sécurité	11
4.3.4 Performances Attendues	11
5. Tests et Validation	12
5.1 Tests Fonctionnels	12
<b>I - INFRASTRUCTURE</b>	13
1.Un réseau informatique pour le laboratoire: un défi crucial	13
2.Vue d'ensemble	14
3.VLan Service Administratif	16
4.VLan Services de Recherches et Plateformes Techniques	18
5.Les Serveurs	20
5.1.Serveur DNS/DHCP/Active Directory : Un cœur de réseau	21
5.2.Serveur de Supervision : Un œil vigilant sur l'infrastructure	22
6.Connexion au WAN	23
6.1.Le routeur	24
6.2.Le pare-feu	24
7. Plan d'adressage	25
<b>II - SWITCH FEDERATEUR</b>	26
1.Introduction	26
2.Choix du matériel	27
3.Configuration du Switch Fédérateur	27
4.Fichier de configuration	30
<b>III - ROUTEUR</b>	31

<u>1.Introduction</u>	31
<u>2.Choix du matériel</u>	31
<u>3.Configuration du Routeur</u>	32
<u>3.1.Câblage</u>	32
<u>3.2.Configuration terminal</u>	32
<u>Configuration du NAT</u>	34
<u>IV - GESTION DU SYSTÈME</u>	36
<u>1.Active Directory</u>	36
<u>2.Fonctionnement d'Active Directory</u>	36
<u>3.Services DNS et DHCP dans AD DS</u>	37
<u>4.Choix de l'Active Directory</u>	37
<u>5.Prérequis Matériels</u>	38
<u>6.Création du Gestionnaire de Domaine</u>	38
<u>6.1.Prérequis initiaux</u>	38
<u>6.2.Installation d'un rôle du gestionnaire du domaine</u>	38
<u>6.3.Configuration du rôle ADDS</u>	40
<u>7.Configuration du service DNS</u>	42
<u>8.Configuration du DHCP</u>	43
<u>9.Configuration de l'autorité de Certification (ADCS)</u>	49
<u>9.1.Rôle du service de Certification</u>	49
<u>9.2.Installation et configuration de l'autorité de certification</u>	49
<u>9.3.Génération d'un certificat</u>	51
<u>10.Architecture de l'Active Directory</u>	54
<u>10.1.Notre politique concernant les Unités organisationnelles (OU)</u>	54
<u>10.2.Schéma structurel du domaine MOLECULIS.LAN</u>	55
<u>10.3.Création d'un OU</u>	56
<u>11.Politiques de Sécurité</u>	57
<u>11.1.Introduction aux GPO</u>	57
<u>11.2.Création et gestion des GPO</u>	58
<u>11.3.Organisation des GPO</u>	60
<u>12.Partage des ressources</u>	62
<u>13.Répartition des Rôles FSMO</u>	65
<u>13.1.Préparation des machines</u>	68
<u>13.2.Répartition des rôles</u>	71
<u>V - PARE-FEU</u>	74
<u>1.Objectifs du pare-feu</u>	74
<u>2.Choix de pfSense</u>	74
<u>3.Prérequis matériels</u>	76
<u>4.Organisation globale du pare-feu</u>	77
<u>5.Installation du pare-feu</u>	78
<u>6.Configuration initiale via l'interface Web</u>	80
<u>7.Configuration de la DMZ</u>	82
<u>7.1.Création de la DMZ via la Web UI</u>	82
<u>7.2.Définition des règles de filtrage associées à la DMZ</u>	83

<u>8.Délégation de l'authentification par Active Directory</u>	86
<u>9.Règles de filtrage</u>	92
<u>9.1.Politique de filtrage</u>	92
<u>9.2.Création d'une règle de filtrage</u>	92
<u>9.3.Politique de filtrage du pare-feu</u>	93
<u>VI - VIRTUAL PRIVATE NETWORK</u>	94
<u>1.Objectifs de l'accès VPN</u>	94
<u>2.Choix d'OpenVPN</u>	94
<u>3.Prérequis matériels et logiciels</u>	95
<u>4.Installation et configuration d'OpenVPN</u>	96
<u>4.1.Création d'une autorité de certification interne à pfSense</u>	96
<u>4.2.Création du certificat interne à pfSense</u>	98
<u>4.3.Configuration du serveur openVPN</u>	99
<u>4.4.Règles de filtrage relatives au VPN</u>	102
<u>4.5.Authentification et déploiement par l'Active Directory</u>	103
<u>4.6 Test de la connection depuis un hôte du WAN</u>	103
<u>VII - Supervision</u>	104
<u>1.Supervision des systèmes</u>	104
<u>2.Sélection de Centreon comme solutions de supervision</u>	104
<u>3.Prérequis logiciels et matériels</u>	105
<u>3.1.Prérequis logiciels</u>	105
<u>3.2.Prérequis matériels</u>	106
<u>4.Installation de Centreon</u>	107
<u>4.1.Installation du serveur MySQL</u>	107
<u>4.2.Installation Web</u>	108
<u>5.Intégration du serveur dans le domaine Active Directory</u>	112
<u>6.Configuration de Centreon</u>	114
<u>6.1.Création d'un Poller et utilisation (Local)</u>	114
<u>6.2.Création d'un Hôte</u>	116
<u>6.3.Création d'un Service</u>	117
<u>6.4.Gestion de l'interface graphique</u>	119
<u>IX - BILAN DU PROJET</u>	121
<u>1.Bilan des Réalisations</u>	121
<u>2.Axes d'amélioration</u>	122
<u>3.Conclusion</u>	123
<u>ANNEXES</u>	124

# INTRODUCTION

## 1. Contexte Général

Le laboratoire **Moleculis**, un centre de recherche scientifique de pointe spécialisé dans la chimie et l'innovation scientifique, connaît une croissance rapide. Cette expansion a entraîné des besoins accrus en termes d'infrastructure réseau pour soutenir ses activités critiques. Avec plus de 930 membres permanents, comprenant des chercheurs, des équipes techniques et du personnel administratif, ainsi qu'un flux constant de stagiaires et de collaborateurs externes, l'infrastructure actuelle doit être entièrement repensée pour répondre aux exigences techniques et fonctionnelles élevées imposées par cette évolution.

Les travaux de recherche du laboratoire s'appuient sur des plateformes techniques d'analyse et de calcul intensif, produisant un volume conséquent de données critiques qui transitent entre divers services et systèmes. Parallèlement, la gestion administrative d'un personnel dépassant les 1 000 personnes, incluant la gestion des comptes, des finances et des ressources humaines, renforce la nécessité de disposer d'une infrastructure performante, évolutive et sécurisée.

Cette dynamique impose une refonte complète du réseau, avec une infrastructure capable de répondre à plusieurs critères fondamentaux :

- **Fiabilité** : garantir une connectivité continue et stable pour toutes les activités critiques.
- **Sécurité** : protéger efficacement les données sensibles, qu'elles soient scientifiques, administratives ou financières.
- **Évolutivité** : permettre une croissance sans entrave, intégrant facilement de nouveaux utilisateurs, services et technologies.
- **Performance** : répondre aux besoins croissants en matière de traitement, de transfert et d'analyse des données.

## 2. Objectifs

Ce projet vise à concevoir une infrastructure réseau moderne et optimisée, capable de répondre aux besoins actuels du laboratoire Moleculis tout en anticipant les défis futurs liés à son expansion et à ses exigences croissantes en matière de performance, sécurité et évolutivité.

Pour atteindre cet objectif, le projet a suivi une approche méthodique et structurée, comprenant les étapes suivantes :

- **Analyse des besoins** pour définir les priorités fonctionnelles et techniques.
- **Choix des équipements** pour garantir performance et fiabilité.
- **Conception de la topologie réseau**, incluant la segmentation stratégique par VLAN et des mécanismes de sécurité avancés.
- **Implémentation dans un environnement virtualisé** pour simuler, tester et valider les configurations dans des conditions réalistes.
- **Documentation complète** pour assurer la transparence et la facilité de mise en production.

La virtualisation joue un rôle clé dans la validation des choix techniques et fonctionnels. Elle permet d'ajuster les configurations dans un cadre contrôlé, tout en offrant la flexibilité nécessaire pour intégrer des solutions modernes. L'ensemble des configurations, y compris les paramètres des équipements réseau, les commandes CLI et les réglages spécifiques des machines virtuelles, sera soigneusement documenté afin de garantir la transparence et de faciliter la mise en production.

L'objectif final de ce projet est de produire une documentation complète décrivant une infrastructure réseau robuste, performante et évolutive, capable de répondre aux besoins actuels du laboratoire Moleculis tout en facilitant une transition fluide vers une mise en production future adaptée à ses exigences croissantes.

## 3. Évaluation des Besoins

### 3.1. Présentation Organisationnelle et Infrastructure Physique

#### 3.1.1. Structure Organisationnelle

Le laboratoire Moleculis, avec ses activités de recherche et d'innovation de pointe, repose sur une organisation structurée en trois principaux pôles fonctionnels :

- Direction : 10 personnes.
- Administration et logistique : 53 personnes (secrétariat (20), finance (10), logistique (15), sécurité-Hygiène (8), informatique (8)).
- Recherche : 6 équipes totalisant 860 personnes (équipe 1 (210), équipe 2 (150), équipe 3 (160), équipe 4 (130), équipe 5 (100), équipe 6 (109)).

Total : 930 membres permanents, plus des invités et stagiaires.

### 3.1.2. Infrastructure Physique

L'infrastructure physique du laboratoire Moleculis est conçue pour répondre aux exigences variées des activités administratives et scientifiques :

- Bureaux dédiés (direction, administration, informatique, service supports).
- 3 salles de réunion.
- Plateaux techniques : 6 plateformes d'analyse et 1 plateforme de calcul intensif.
- Une zone des serveurs centralisée regroupant :
  - Serveurs critiques : Active Directory (AD), DNS et DHCP.
  - Supervision : Serveur Centreon.
  - Stockage : Serveurs de stockage Windows
- DMZ (zone démilitarisée) : serveur web.

### 3.2. Fiabilité et Disponibilité

L'infrastructure réseau doit garantir une haute disponibilité afin d'assurer la continuité des activités critiques du laboratoire Moleculis. Les besoins identifiés incluent :

- **Performance** : Une topologie capable de supporter le trafic généré par plus de 1 000 utilisateurs, répartis entre les plateformes de recherche analytique, de calcul intensif et les services administratifs.
- **Redondance** : Mise en place de mécanismes de tolérance aux pannes pour éviter tout point unique de défaillance, en particulier pour les composants critiques comme le routeur central et les switches de distribution.
- **Sauvegardes automatiques** : Conservation des configurations des équipements réseau et des données critiques, afin de permettre une restauration rapide en cas de problème.

### 3.3. Connectivité et Collaboration

L'infrastructure réseau doit favoriser une collaboration fluide entre les différentes équipes tout en maintenant une isolation et une sécurité robustes. Les besoins incluent :

- **Connectivité centralisée** : Une infrastructure qui relie efficacement les services administratifs, techniques et de recherche pour un partage fluide des données et des ressources.
- **Accès distant sécurisé** : Implémentation d'un VPN performant pour garantir un accès sécurisé aux données et outils internes pour les collaborateurs travaillant à distance.
- **Partage sécurisé des ressources** : Les données critiques doivent être accessibles aux équipes concernées, tout en assurant une limitation stricte des accès non autorisés grâce à la segmentation des flux.

### 3.4. Scalabilité

Pour accompagner la croissance du laboratoire, l'infrastructure doit être conçue de manière à s'adapter facilement aux évolutions futures. Les besoins incluent :

- **Ajout d'utilisateurs et d'équipements** : Capacité à intégrer de nouveaux utilisateurs, périphériques et services sans nécessiter de refonte majeure.
- **Extensions techniques** : Préparation à la croissance des plateformes techniques et à l'intégration de nouvelles technologies telles que l'IoT (Internet des Objets) pour les équipements de recherche ou les protocoles émergents comme la 5G.
- **Flexibilité d'adressage** : Réservation de plages d'adresses IP pour les futurs sous-réseaux et VLANs.

### 3.5. Sécurité

La protection des données sensibles, tant scientifiques qu'administratives, est une priorité pour le laboratoire. Les besoins incluent :

- **Segmentation réseau** : Une isolation rigoureuse des flux grâce à l'utilisation de VLAN dédiés (administration et recherche), zone serveurs et DMZ.
- **Pare-feu robuste** : Mise en place d'un pare-feu pour filtrer les flux entrants et sortants, tout en offrant une supervision avancée.
- **Surveillance continue** : Intégration d'outils de supervision pour détecter les anomalies en temps réel et permettre une réaction rapide.
- **Contrôle d'accès** : Application de politiques strictes pour limiter les accès aux ressources en fonction des profils d'utilisateurs.

### 3.6. Performances

L'infrastructure doit répondre aux exigences élevées des plateformes techniques et administratives, notamment en termes de débit et de latence. Les besoins incluent :

- **Débit élevé** : Connexions internes d'au moins 1 Gbps pour les postes de travail, et un backbone (partie centrale et à haut débit d'un réseau informatique) d'au moins 10 Gbps pour les flux critiques entre les switches de cœur et d'accès.
- **Faible latence** : Indispensable pour garantir une performance optimale des plateformes de calcul intensif et des applications sensibles.
- **Backbone robuste** : Architecture optimisée pour le transfert de données volumineuses entre les plateformes techniques et les centres de stockage.

## 4. Cahier des Charges

Le but de ce cahier des charges est de définir les spécifications techniques et fonctionnelles nécessaires à la conception, la mise en place et la validation d'une infrastructure réseau performante, évolutive et sécurisée. Il servira de document de référence pour orienter toutes les étapes du projet, depuis l'analyse des besoins jusqu'à la mise en production, tout en assurant une compréhension claire des objectifs et des contraintes du projet.

### 4.1. Objectifs du Projet

Le projet vise à concevoir, configurer, tester et documenter une infrastructure réseau complète, basée sur une architecture définie par l'équipe. Cette infrastructure virtuelle servira de référence pour une mise en production future.

Les objectifs incluent :

- **Connectivité fiable** : Assurer une communication fluide entre les différents segments du réseau.
- **Sécurité renforcée** : Garantir l'isolation des flux critiques grâce à une segmentation réseau stricte et un pare-feu robuste. Assurer une supervision continue.
- **Évolutivité intégrée** : Préparer des configurations permettant l'ajout futur de services, utilisateurs ou équipements.
- **Performance optimale** : Valider la capacité de l'infrastructure à supporter des charges critiques.

### 4.2. Conception du Réseau

L'infrastructure réseau a été conçue en respectant les besoins spécifiques du laboratoire. Elle repose sur une **architecture segmentée** avec des VLAN dédiés, une zone des serveurs et une DMZ.

#### 4.2.1 Segmentation des VLAN

Les VLAN suivants ont été définis pour garantir une isolation logique des flux réseau et assurer la performance ainsi que la sécurité des différentes entités fonctionnelles du laboratoire :

- **VLAN Administration** : Inclut les services administratifs, logistiques, la direction, l'accueil, les équipes informatiques et les salles de réunion.
- **VLAN Recherche et Technique** : Regroupe les plateformes d'analyse et de calcul intensif.
- **Zone des Serveurs** :
  - **Serveurs critiques** : Active Directory (AD), DNS, DHCP.
  - **Supervision** : Centreon.
  - **Stockage** : Serveurs NAS ou équivalents.
- **DMZ** : héberge le serveur web accessible depuis l'extérieur.

#### 4.2.2 Sous-Réseaux

Pour chaque entité fonctionnelle du laboratoire, des sous-réseaux dédiés ont été créés afin de garantir la performance, l'isolation des flux et la sécurité :

- **Sous-réseaux pour les équipes de recherche** : 6 sous-réseaux (1 par équipe).
- **Sous-réseaux pour les plateformes d'analyse et de calcul** : 2 sous-réseaux (1 pour l'analyse, 1 pour le calcul intensif).
- **Sous-réseau pour les salles de réunion** : 1 sous-réseau.
- **Sous-réseau pour la salle informatique** : 1 sous-réseau.
- **Sous-réseau pour le bureau de l'équipe informatique** : 1 sous-réseau.
- **Sous-réseaux pour les bureaux administratifs et de direction** : 2 sous-réseaux (1 pour l'administration, 1 pour la direction).
- **Sous-réseau pour l'accueil** : 1 sous-réseau.

Cette segmentation par sous-réseaux permet une meilleure gestion des flux réseau, un contrôle strict des accès et une isolation des différentes unités fonctionnelles du laboratoire.

#### 4.2.3 Topologie Réseau

L'infrastructure réseau est conçue autour d'une architecture simplifiée mais performante, offrant une solution à la fois robuste et économique :

- **Routeur** : Il joue un rôle central en assurant le routage inter-VLAN et la gestion de la connexion vers le WAN.
- **Switch fédérateur** : Ce switch centralise les VLANs et fait office d'intermédiaire entre le routeur et les switches d'accès, garantissant une distribution efficace du trafic réseau.
- **Switches d'accès** : Ils connectent directement les terminaux tels que les postes de travail, imprimantes, et points d'accès Wi-Fi, permettant une connexion fluide des utilisateurs au réseau.

### 4.3. Contraintes Techniques

#### 4.3.1 Environnement Virtuel

Toutes les configurations et tests seront effectués dans un environnement virtualisé sur un poste sous Windows 11, avant la mise en production physique.

- **Logiciel de virtualisation** : VMware, VirtualBox, GNS3, Cisco Packet Tracer...
- **Ressources minimales** :
  - 16 Go de RAM disponibles sur l'hôte (Windows 11), répartis entre les différentes machines virtuelles selon les besoins.
  - Processeur compatible avec la virtualisation (minimum 4 à 8 cœurs logiques nécessaires pour les performances de l'environnement).
  - Espace disque : 500 Go alloués pour héberger les images VM et les fichiers système.

#### 4.3.2 Choix des équipements Simulés

Les équipements virtuels représenteront des matériels physiques réels pour garantir la compatibilité avec une implémentation future. Ces équipements incluent :

- **Routeurs :**
  - **Cisco ISR 4451-X** : Routeur haute performance adapté aux grandes infrastructures.
- **Switch de Cœur (Fédérateur) :**
  - **Cisco Catalyst 9300** : Switch L3 robuste avec gestion VLAN avancée.
- **Switchs d'Accès :**
  - **Cisco Catalyst 2960-X** : Fiable et économique pour les terminaux utilisateurs.
- **Serveurs :**
  - **Windows Server 2022** : Pour les services Active Directory (AD), DNS et DHCP.
  - **Linux** : Pour la supervision via **Centreon**.
  - **Serveur de ressources partagées**: Windows server 2022 pour le partage via **Active Directory**

#### 4.3.3 Connectivité et Sécurité

- **WAN** : Connexion simulée avec un débit d'au moins 500 Mbps.
- **VPN** : Mise en place d'une solution **OpenVPN** pour les accès distants.
- **Pare-feu** : Configuration avec PfSense pour sécuriser les flux internes et externes.
- **Câblage virtuel** : Simuler des connexions Ethernet (Cat6) et fibres optiques.

#### 4.3.4 Performances Attendues

- Connexions internes d'au moins **1 Gbps** pour les utilisateurs.
- Backbone réseau supportant **10 Gbps** pour les flux critiques entre les VLANs.
- Isolation stricte des flux grâce à des règles ACL et au pare-feu.

## 5. Tests et Validation

### 5.1 Tests Fonctionnels

- **Connectivité :**
  - Vérifier les communications entre les VLANs et les différentes zones réseau (Serveurs, DMZ, VLAN Administration, VLAN Technique & Recherche).
  - S'assurer que les équipements et postes connectés communiquent correctement au sein de leur VLAN respectif et avec les zones partagées.
- **Sécurité :**
  - Tester les règles ACL entre les VLANs pour vérifier l'isolation des flux réseau.
  - Simuler des attaques réseau (tentatives d'accès non autorisées) pour valider l'efficacité des mécanismes de sécurité, notamment du pare-feu PfSense.
  - Contrôler l'accès aux services critiques (serveurs AD, DNS, DHCP) depuis les segments autorisés.
- **Services :**
  - DHCP : Valider l'attribution dynamique des adresses IP à chaque VLAN selon les plages définies.
  - DNS : Tester la résolution de noms internes et externes pour les équipements et les utilisateurs.
  - **Active Directory (AD) :**
    - Vérifier l'authentification des utilisateurs, la gestion des groupes et les droits d'accès.
    - Tester les interactions avec les postes clients connectés.
- **Supervision (Centreon) :**
  - Vérifier que Centreon détecte et surveille correctement les équipements critiques (routeurs, switches, serveurs).
  - Simuler des alertes (pannes ou seuils dépassés) pour s'assurer que le système génère des notifications en temps réel.
- **VPN** : Tester les accès distants via OpenVPN pour garantir une connectivité sécurisée et performante.
- **Performance** : Simuler des charges réseau pour évaluer le débit et la latence.

# I - INFRASTRUCTURE

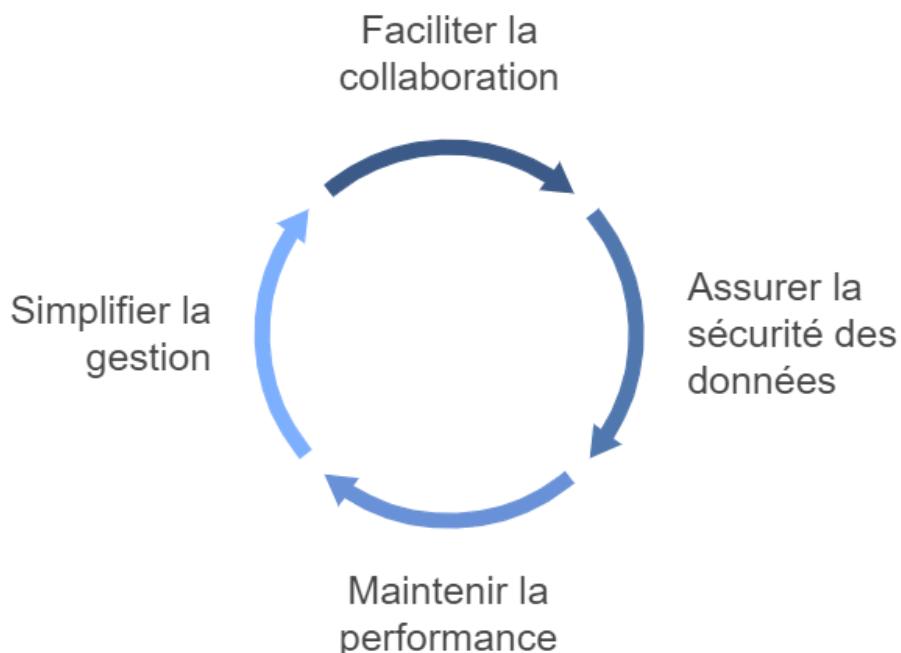
## 1. Un réseau informatique pour le laboratoire: un défi crucial

**Moleculis** représente un écosystème complexe où la collaboration, le partage d'informations et la sécurité des données sont des enjeux majeurs. Le réseau informatique devient alors un élément crucial, agissant comme le système nerveux de l'organisation. Il doit être capable de supporter un volume important de trafic, de garantir une accessibilité constante aux ressources et de protéger les données sensibles.

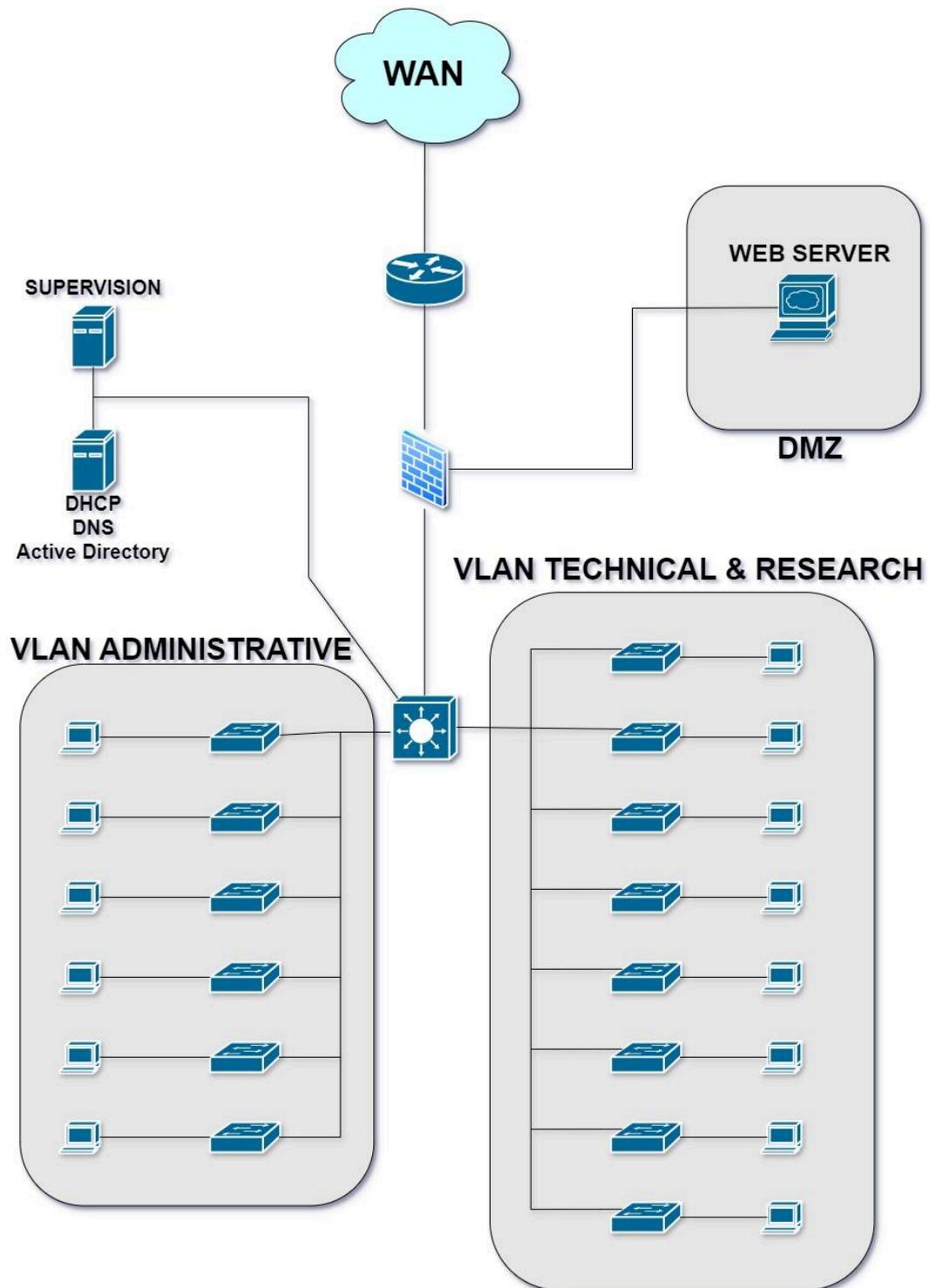
Ce réseau doit être **fiable, performant** et **sécurisé** pour permettre aux chercheurs, aux techniciens et à l'ensemble du personnel de travailler efficacement et en toute sécurité.

**Les enjeux clés d'un réseau informatique dans un laboratoire de cette envergure sont :**

- **La collaboration et le partage d'informations** : Le réseau doit permettre une communication fluide entre les différents départements et équipes, favorisant la collaboration et l'échange d'informations.
- **La sécurité des données** : Les données scientifiques et les informations sensibles doivent être protégées contre les accès non autorisés et les cybermenaces.
- **La performance et la fiabilité** : Le réseau doit être capable de supporter un volume important de trafic et de garantir une accessibilité constante aux ressources, notamment pour les applications scientifiques gourmandes en ressources.
- **La gestion et l'administration** : Le réseau doit être facile à gérer et à administrer, permettant une maintenance efficace et une évolution continue.



## 2. Vue d'ensemble



### **Réseau local:**

- Ce LAN héberge les serveurs liés à l'administration du réseau.
- On y retrouve des outils de gestion, de surveillance et de configuration du réseau.

### **VLAN Service Administratif:**

- Ce VLAN est dédié aux différentes équipes des services Administratifs et IT.

### **VLAN Services Recherches et Techniques:**

- Ce VLAN est dédié aux équipes de recherche et aux plateformes techniques.
- On y retrouve des postes de travail des chercheurs ainsi que les postes et outils métier présents dans les différents locaux techniques.

### **DMZ:**

- La DMZ (Zone démilitarisée) est un segment de réseau isolé du réseau interne et exposé à internet.
- Dans notre cas, la DMZ héberge un serveur web accessible depuis l'extérieur.

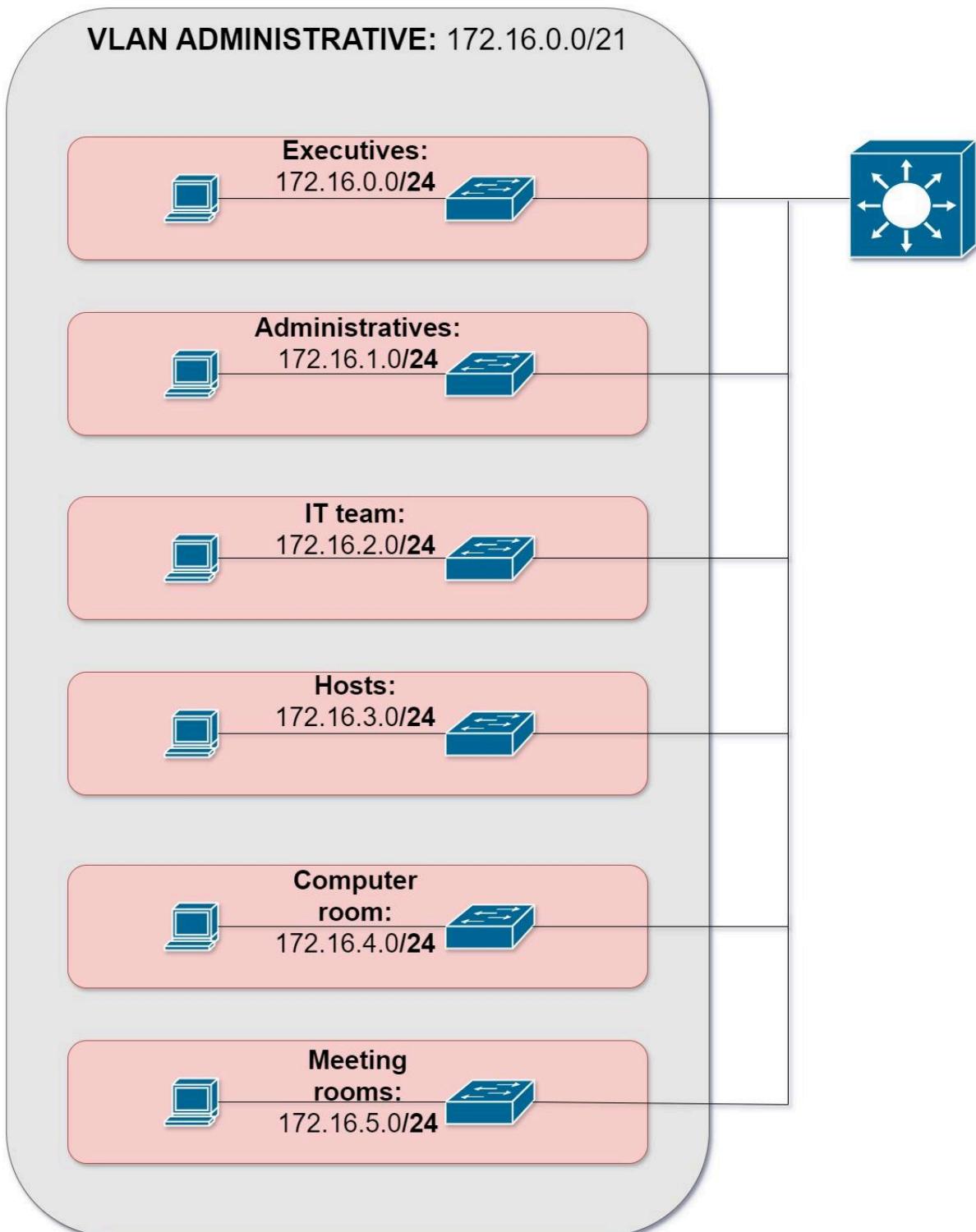
### **Connexions et équipements:**

- **Routeur:** Le réseau est connecté à internet via un routeur qui assure la bonne redirection du trafic vers l'extérieur de notre réseau.
- **Pare-Feu:** Élément essentiel à notre infrastructure, il filtre le trafic entrant et sortant du réseau.
- **Switch Fédérateur:** Un switch central interconnecte les différents VLAN et assure la communication entre eux.
- **Serveurs DHCP/DNS/Active Directory:** Un serveur dédié fournit les services DHCP, DNS et Active Directory pour le réseau.
- **Serveur de supervision:** Un serveur dédié assure la supervision du réseau.

### **Sécurité:**

- La segmentation du réseau en VLAN permet d'isoler le trafic et d'améliorer la sécurité.
- Le firewall protège le réseau des accès non autorisés depuis l'extérieur.
- La DMZ permet d'isoler le serveur web du réseau interne, limitant ainsi les risques en cas d'attaque.

### 3.VLan Service Administratif



Le **VLAN Service Administratifs** est un segment du réseau dédié à l'administration du laboratoire en lui-même. Il est isolé des autres VLAN, ce qui assure une sécurité accrue pour les outils de gestion et les données sensibles qui y sont stockées.

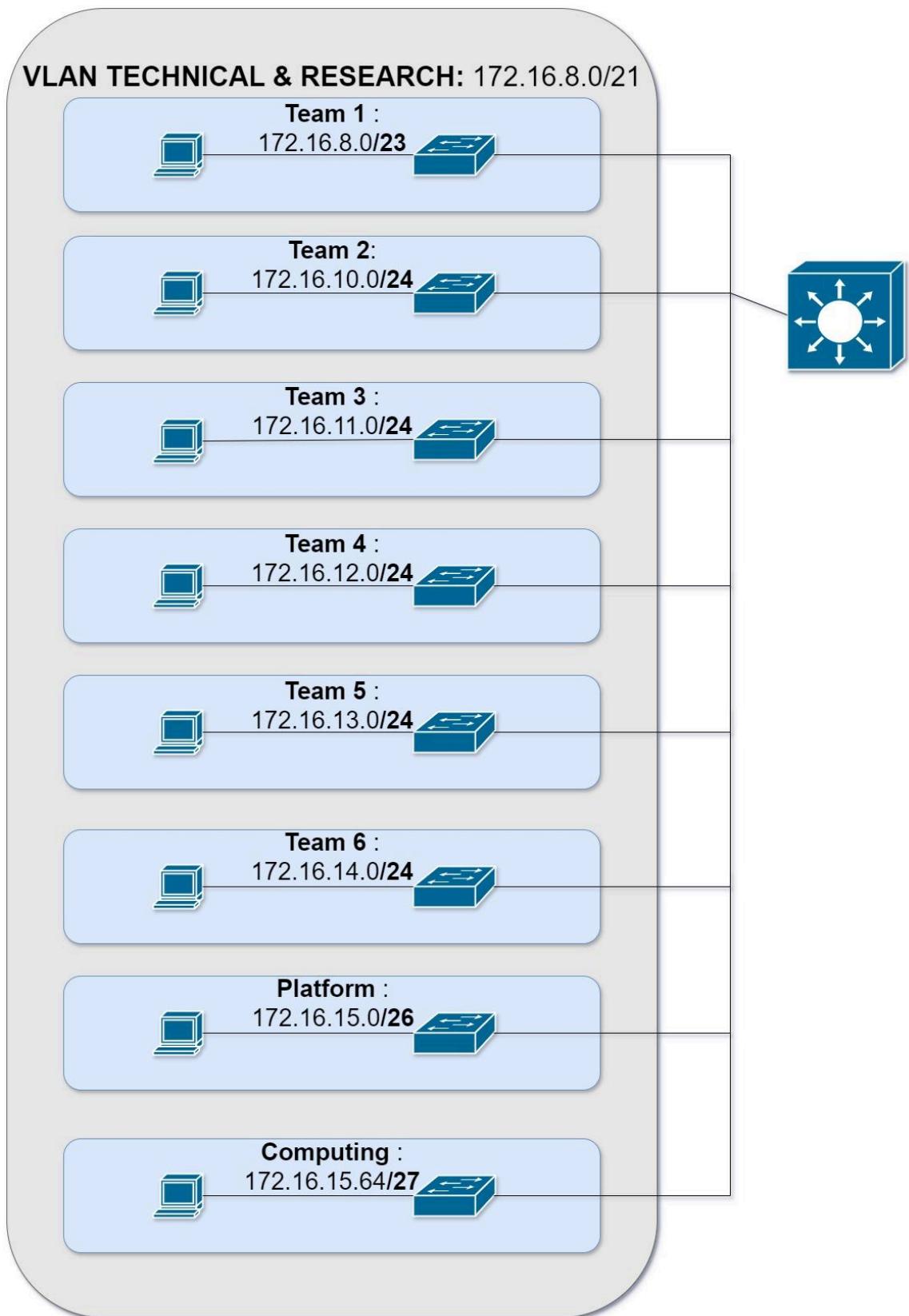
Ce VLAN abrite:

- **Postes de travail des administrateurs réseau:** Ces postes sont utilisés pour configurer, surveiller et gérer le réseau.
- **Postes de travail des équipes administratives:** Ces postes sont utilisés par les services manipulant des données sensibles de l'entreprise (informations personnelles des employés, comptabilité, bilans etc...)

Le VLAN, adressé en 172.16.0.0/21, est découpé en **6 sous-réseaux** distincts, basé sur la structure fonctionnelle des services concernés:

EQUIPE / SERVICE	ADRESSE DU SOUS-RÉSEAU
Direction	172.16.0.0/24
Administration	172.16.1.0/24
Equipe IT	172.16.2.0/24
Accueil	172.16.3.0/24
Salle informatique	172.16.4.0/24
Salles de réunions	172.16.5.0/24

## 4.VLan Services de Recherches et Plateformes Techniques



Le **VLAN Services de Recherche et Plateformes Techniques** est un segment du réseau dédié aux chercheurs et à leurs outils. Il est isolé des autres VLAN, ce qui assure une sécurité accrue pour les outils de laboratoire et les données sensibles qui y sont stockées.

Ce VLAN abrite:

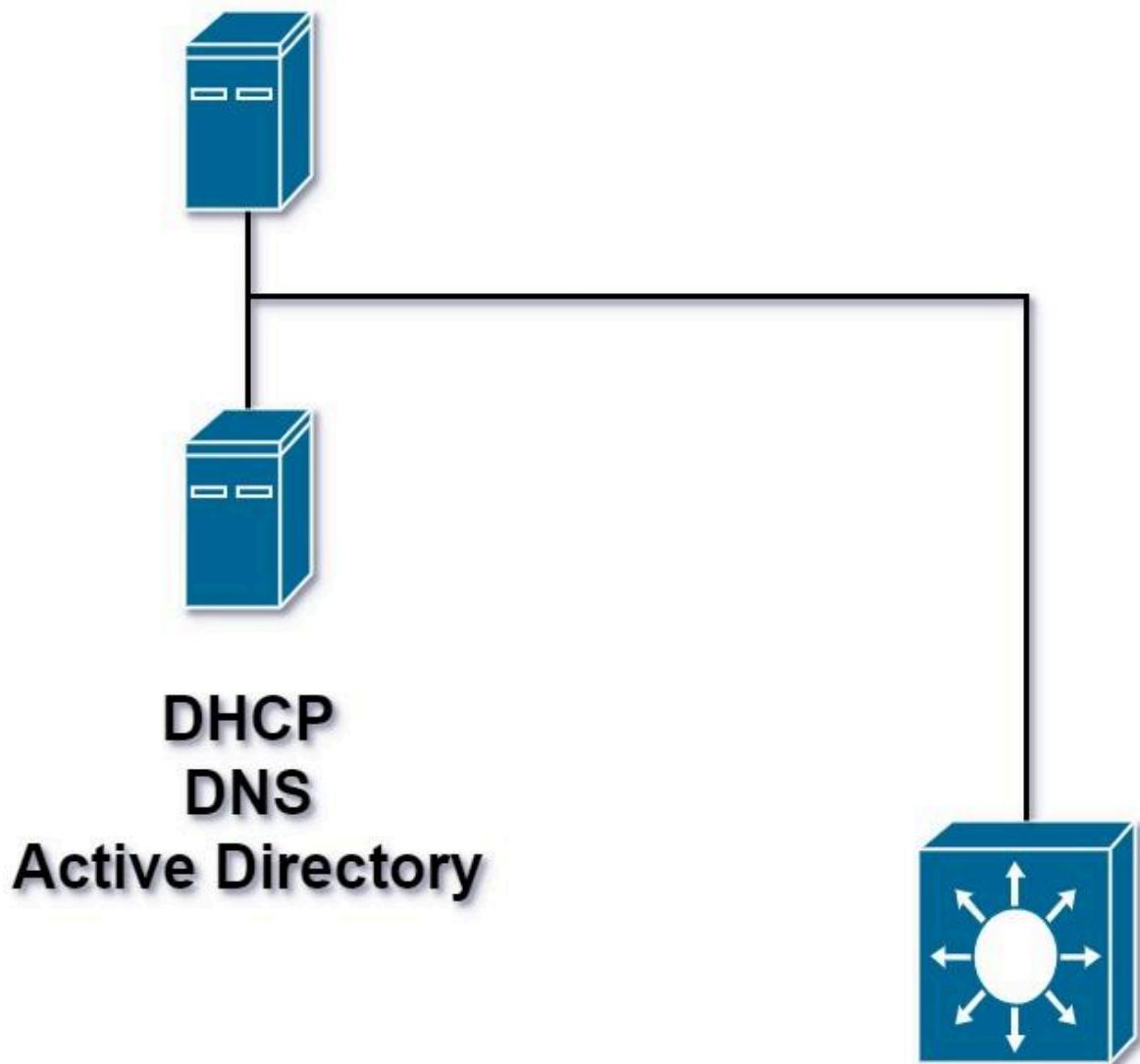
- **Postes de travail des chercheurs:** Ces postes sont utilisés par les équipes scientifiques pour leur usage bureautique.
- **Postes métier:** Ces postes sont situés dans les plateformes techniques pour un usage purement métier (expérimentations, analyse etc...).
- **Postes de calcul:** Ces postes à forte puissance de calcul sont utilisés pour l'analyse et le traitement de grandes quantités d'informations complexes.

Le VLAN, adressé en 172.16.8.0/21, est découpé en **8 sous-réseaux** distincts, basé sur la structure fonctionnelle des services concernés:

EQUIPE / SERVICE	ADRESSE DU SOUS-RÉSEAU
Equipe de recherche 1	172.16.8.0/ <b>23</b>
Equipe de recherche 2	172.16.10.0/ <b>24</b>
Equipe de recherche 3	172.16.11.0/ <b>24</b>
Equipe de recherche 4	172.16.12.0/ <b>24</b>
Equipe de recherche 5	172.16.13.0/ <b>24</b>
Equipe de recherche 6	172.16.14.0/ <b>24</b>
Plateformes Techniques	172.16.15.0/ <b>26</b>
Salle de calcul	172.16.15.64/ <b>27</b>

## 5.Les Serveurs

### SUPERVISION



## 5.1. Serveur DNS/DHCP/Active Directory : Un cœur de réseau

Ce serveur est le pilier central de notre réseau, gérant l'accès aux ressources et la communication entre les différents appareils. Il combine trois fonctions essentielles :

- **DNS (Domain Name System)** : Traduit les noms de domaine (ex: google.com) en adresses IP numériques (ex: 172.217.160.142), permettant aux utilisateurs de naviguer sur internet et d'accéder aux services réseau.
- **DHCP (Dynamic Host Configuration Protocol)** : Attribue automatiquement des adresses IP aux appareils du réseau, simplifiant la configuration et l'administration.
- **Active Directory** : Gère les utilisateurs, les groupes, les ordinateurs et les ressources du réseau, assurant un contrôle d'accès centralisé et une sécurité renforcée.

### Avantages :

- **Simplicité d'administration** : Un seul point de contrôle pour gérer les utilisateurs, les autorisations et les configurations réseau.
- **Sécurité accrue** : Contrôle d'accès précis, gestion des mots de passe et authentification centralisée.
- **Fiabilité et performance** : Gestion centralisée des ressources et optimisation des performances réseau.
- **Scalabilité** : Adaptable aux besoins croissants du réseau, avec la possibilité d'ajouter des serveurs supplémentaires.

Les rôles sont répartis sur 5 serveurs distincts:

NOM / RÔLE	ADRESSE IP
Contrôleur de domaine	192.168.1.2/16
Maître RID	192.168.1.3/16
Contrôleur de schéma	192.168.1.4/16
Maître d'attribution de noms de domaine	192.168.1.5/16
Emulateur PDC	192.168.1.6/16

## 5.2. Serveur de Supervision : Un œil vigilant sur l'infrastructure

Ce serveur est un outil indispensable pour surveiller en temps réel l'état de notre infrastructure informatique. Il collecte des données sur les performances, la disponibilité et la sécurité de vos serveurs, applications et réseaux.

### Fonctionnalités :

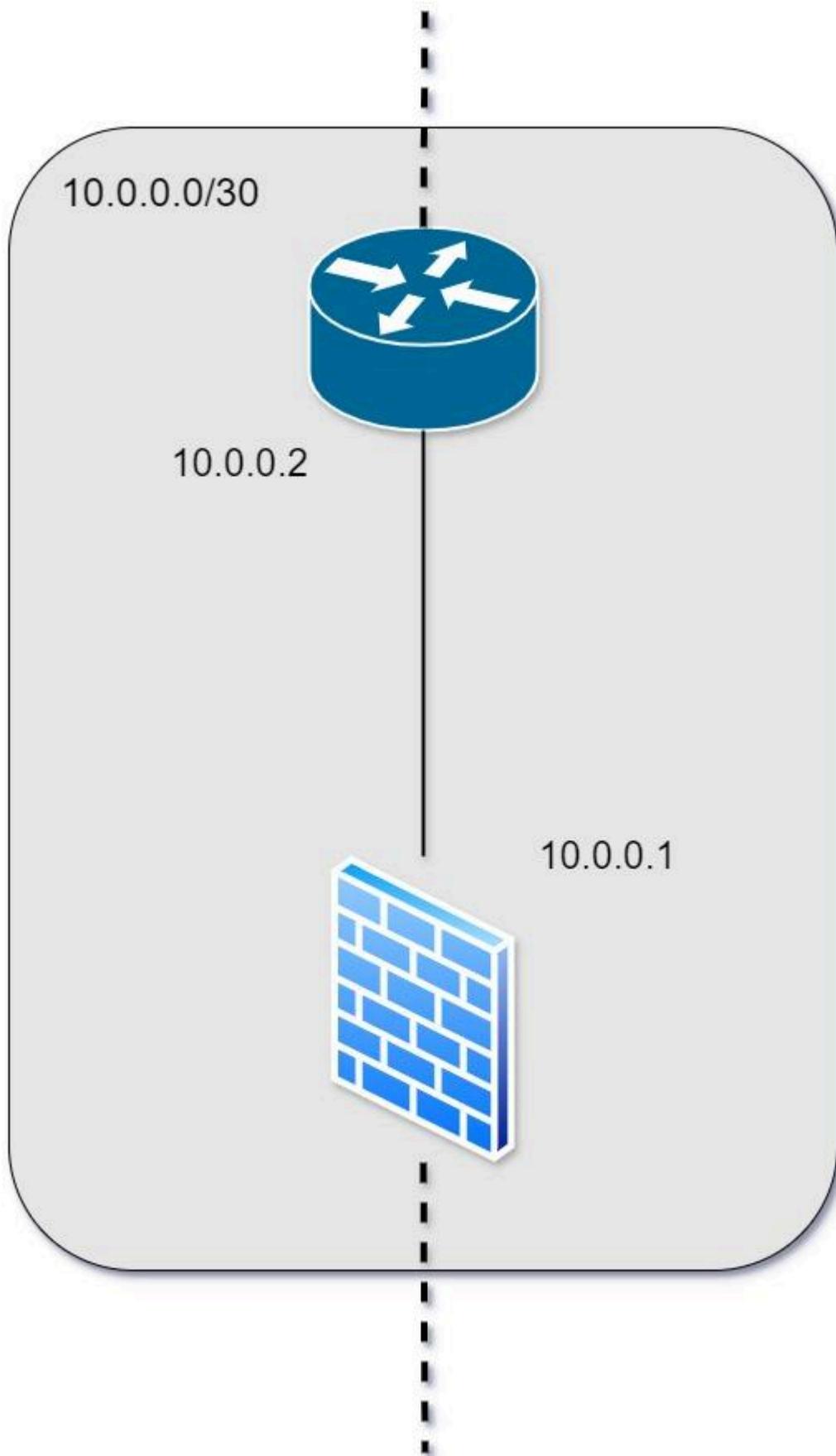
- **Surveillance des performances** : Analyse de l'utilisation du CPU, de la mémoire, du disque dur et des connexions réseau.
- **Détection des erreurs** : Alerte en cas de panne de serveur, d'interruption de service ou d'autres anomalies.
- **Gestion des événements** : Collecte et analyse des événements système pour identifier les problèmes et les tendances.
- **Rapports et analyses** : Génération de rapports détaillés sur l'état de l'infrastructure et l'identification des points faibles.

### Avantages :

- **Proactivité** : Détection des problèmes avant qu'ils ne deviennent critiques.
- **Réduction des temps d'arrêt** : Intervention rapide en cas de panne ou d'incident.
- **Optimisation des performances** : Identification des goulets d'étranglement et des points d'amélioration.
- **Sécurité renforcée** : Détection des attaques et des intrusions.

On lui attribue l'adresse **192.168.0.40**.

## 6.Connexion au WAN



## 6.1.Le routeur

**Le routeur** est un appareil réseau qui a pour rôle principal de **diriger les paquets de données** entre les réseaux. Il utilise des **protocoles de routage** pour déterminer le meilleur chemin pour envoyer les paquets à leur destination. **En résumé, le routeur est un appareil essentiel pour connecter les réseaux et gérer le trafic réseau.**

Il sera détaillé dans la rubrique dédiée.

Il est adressé en **10.0.0.2**.

## 6.2.Le pare-feu

Un **pare-feu** est un élément essentiel de la sécurité des réseaux informatiques. C'est un système de sécurité qui surveille et contrôle le trafic réseau entrant et sortant. Il peut être sous forme de matériel (dispositif physique) ou de logiciel (application installée sur un ordinateur ou un serveur).

**Fonctionnalités principales :**

- **Filtrage du trafic** : Le pare-feu décide d'autoriser ou de bloquer le trafic en fonction de règles de sécurité prédéfinies. Cela permet de protéger le réseau contre les accès non autorisés et les menaces potentielles.
- **Prévention des intrusions** : Il agit comme une première ligne de défense, empêchant les attaques et les intrusions avant qu'elles n'atteignent les systèmes internes.
- **Surveillance** : Les pare-feux peuvent enregistrer et analyser le trafic pour détecter des comportements suspects ou des tentatives d'intrusion.

**Importance** : En raison de l'augmentation des cybermenaces, un pare-feu est crucial pour maintenir la sécurité des données et des systèmes d'information. Il contribue à la protection des informations sensibles et à la continuité des opérations.

Il possède 3 interfaces, et donc autant d'adresses IP:

INTERFACE	ADRESSE IP
LAN	192.168.0.1
WAN	10.0.0.1
DMZ	10.0.0.9

## 7. Plan d'adressage

Vous trouverez le [plan d'adressage complet](#) en suivant ce lien.

*Si pour quelque raison, le lien n'est pas fonctionnel, nous fournissons une copie du fichier avec la documentation*

**Il est destiné à être mis à jour par les équipes techniques à chaque ajout de matériel adressé en statique!**

## II - SWITCH FEDERATEUR

### 1. Introduction

Dans le monde des réseaux informatiques, les **switchs de couche 3**, également appelés **switchs intelligents**, jouent un rôle crucial en permettant des connexions plus efficaces et intelligentes. Contrairement aux **switchs de couche 2** qui opèrent uniquement au niveau des adresses MAC, les **switchs de couche 3** exploitent les **adresses IP** pour diriger le trafic réseau. Cette capacité leur permet de :

- **Routage intelligent du trafic:** En analysant les adresses IP de destination, les **switchs de couche 3** peuvent acheminer les données vers le bon chemin, optimisant ainsi le flux de communication.
- **Segmentation du réseau:** Ils permettent de diviser un réseau en plusieurs réseaux virtuels (**Vlan**), améliorant la sécurité et la performance en isolant les différents segments.
- **Gestion du trafic:** Grâce à des fonctionnalités avancées comme la **QoS (Quality of Service)**, les **switchs de couche 3** peuvent prioriser le trafic critique et garantir une bande passante suffisante aux applications sensibles.
- **Connectivité inter-réseaux:** Ils facilitent la communication entre différents réseaux en agissant comme des passerelles, permettant ainsi de partager des ressources et des informations entre des segments distincts.

En résumé, les **switchs de couche 3** offrent une solution flexible et performante pour gérer le trafic réseau complexe, en assurant une connectivité optimale et une sécurité renforcée.

## 2.Choix du matériel

Choisir un **switch Cisco** présente de nombreux avantages qui peuvent optimiser la performance et la sécurité du réseau:

1. **Fiabilité et Performance** : Les switches Cisco sont réputés pour leur robustesse et leur capacité à gérer des volumes de données élevés sans compromettre la performance.
2. **Technologie Avancée** : Ils intègrent des technologies avancées qui permettent une gestion intelligente du trafic réseau, garantissant ainsi une répartition efficace des données.
3. **Sécurité Renforcée** : Cisco offre des fonctionnalités de sécurité avancées, telles que le contrôle d'accès et la segmentation du réseau, ce qui aide à protéger les données contre les menaces.
4. **Forte présence dans son secteur**: Cisco étant un acteur majeur dans le monde de l'infrastructure réseau, il est aisément de trouver une équipe ayant les compétences pour travailler sur ces systèmes.
5. **Évolutivité** : Les solutions Cisco sont conçues pour évoluer avec votre entreprise, vous permettant d'ajouter facilement des fonctionnalités ou d'augmenter la capacité à mesure que vos besoins changent.

En résumé, opter pour un switch Cisco est un choix stratégique pour garantir la performance, la sécurité et la gestion efficace du réseau.

## 3.Configuration du Switch Fédérateur

**Toute la configuration du switch s'effectue dans le terminal Cisco**

- Dans le terminal du switch, activez le vlan 2 et nommez le **vlan-administrative**

```
Press RETURN to get started!

FEDERATEUR>en
FEDERATEUR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
FEDERATEUR(config)#vlan 2
FEDERATEUR(config-vlan)#name vlan-administrative
FEDERATEUR(config-vlan)#end
FEDERATEUR#
```

- Faites de même avec le vlan 3 et le nommer **vlan-research**

```
FEDERATEUR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
FEDERATEUR(config)#vlan 3
FEDERATEUR(config-vlan)#name vlan-research
FEDERATEUR(config-vlan)#end
FEDERATEUR#
```

- Attribuez l'interface FastEthernet0/9 au vlan 2

```
FEDERATEUR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
FEDERATEUR(config)#int
FEDERATEUR(config)#interface FastEthernet0/9
FEDERATEUR(config-if)#switchport access vlan 2
FEDERATEUR(config-if)#no shutdown
FEDERATEUR(config-if)#end
FEDERATEUR#
```

Répétez l'opération pour les interfaces de FastEthernet0/10 jusqu'à 0/16

- Maintenant, attribuez l'interface FastEthernet0/17 au vlan 3

```
FEDERATEUR(config)#int FastEthernet0/17
FEDERATEUR(config-if)#switchport access vlan 3
FEDERATEUR(config-if)#no shutdown
FEDERATEUR(config-if)#exit
FEDERATEUR(config)#
```

Répétez l'opération pour les interfaces de FastEthernet0/18 jusqu'à 0/24

- Activez l'interface virtuelle **VLAN 1** (vlan créé par défaut sur le switch, symbolise le réseau LAN) et paramétrez l'adresse 192.168.0.3/16

```
FEDERATEUR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
FEDERATEUR(config)#int vlan 1
FEDERATEUR(config-if)#no shutdown

FEDERATEUR(config-if)#ip address 192.168.0.3 255.255.0.0
FEDERATEUR(config-if)#
```

- Activez l'interface virtuelle **VLAN 2** et paramétrez l'adresse 172.16.0.1/21

```
FEDERATEUR(config)#int vlan 2
FEDERATEUR(config-if)#ip address 172.16.0.1 255.255.248.0
FEDERATEUR(config-if)#no shutdown
FEDERATEUR(config-if)#
```

- Activez l'interface virtuelle **VLAN 3** et paramétrez l'adresse 172.16.8.1/21

```
FEDERATEUR(config)#int vlan 3
FEDERATEUR(config-if)#ip address 172.16.8.1 255.255.248.0
FEDERATEUR(config-if)#no shutdown
FEDERATEUR(config-if)#+
```

- Activez le relais DHCP sur l'interface Vlan 2

```
FEDERATEUR(config)#int vlan 2
FEDERATEUR(config-if)#ip helper-address 192.168.0.2
FEDERATEUR(config-if)#+
```

Répétez l'opération sur le Vlan 3

- Paramétrez la **passerelle par défaut**

```
FEDERATEUR(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
FEDERATEUR(config)#+
```

- Vérifiez les routes

```
FEDERATEUR#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

      172.16.0.0/21 is subnetted, 2 subnets
C        172.16.0.0 is directly connected, Vlan2
C        172.16.8.0 is directly connected, Vlan3
C        192.168.0.0/16 is directly connected, Vlan1
S*      0.0.0.0/0 [1/0] via 192.168.0.1
```

- Activez le **routage inter-vlan**

```
FEDERATEUR(config)#int vlan 1
FEDERATEUR(config-if)#ip routing
FEDERATEUR(config)#int vlan 2
FEDERATEUR(config-if)#ip routing
FEDERATEUR(config)#int vlan 3
FEDERATEUR(config-if)#ip routing
```

- Finalisez en copiant la **running-config** en **startup-config**

```
FEDERATEUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
FEDERATEUR#
```

## 4.Fichier de configuration

Vous pouvez aussi charger directement le [fichier de configuration](#).

*Si le lien ne fonctionne pas, une copie du fichier est fournie avec cette documentation.*

# III - ROUTEUR

## 1. Introduction

Dans un environnement professionnel, la connectivité et la sécurité des données sont cruciales. Un routeur devient alors un élément central de votre infrastructure réseau, offrant des avantages considérables :

- **Gestion centralisée du réseau** : Un routeur permet de contrôler l'accès à votre réseau, de gérer les utilisateurs et les appareils connectés, et de définir des règles de sécurité strictes.
- **Sécurité renforcée** : Avec des fonctions de pare-feu intégrées, de filtrage d'adresses IP et de VPN, un routeur professionnel protège votre réseau des intrusions et des cyberattaques.
- **Performances optimales** : Un routeur professionnel est conçu pour gérer un trafic réseau important et garantir une connexion stable et rapide pour tous vos collaborateurs.
- **Fiabilité accrue** : Les routeurs professionnels sont conçus pour une utilisation intensive et offrent une grande fiabilité, minimisant les interruptions de service.
- **Flexibilité et évolutivité** : Un routeur professionnel peut être adapté aux besoins spécifiques de votre entreprise et évoluer en fonction de votre croissance.

En résumé, un routeur professionnel est un investissement judicieux pour toute entreprise qui souhaite garantir la sécurité, la performance et la fiabilité de son réseau.

## 2. Choix du matériel

En plus de partager les avantages du switch précédemment présenté, les **routeurs Cisco** présentent d'autres avantages :

1. **Fiabilité et Performance** : Cisco est reconnu comme le premier constructeur mondial de routeurs et de commutateurs. Leurs équipements sont conçus pour offrir des performances constantes et fiables, même dans des environnements exigeants.
2. **Technologie Avancée** : Les routeurs Cisco intègrent des technologies de pointe, comme les plans de contrôle et de données indépendants, permettant des débits constants quelles que soient les fonctions utilisées.
3. **Protocoles Propriétaires** : Cisco utilise des protocoles propriétaires qui optimisent la gestion du réseau (comme par exemple **EIGRP**) et améliorent la sécurité. Cela permet une meilleure intégration et une gestion simplifiée des réseaux complexes.

4. **Support et Documentation** : Cisco offre un excellent support technique et une documentation exhaustive, ce qui facilite la configuration et la gestion des équipements. Cela est un atout majeur pour les entreprises qui souhaitent minimiser les temps d'arrêt.
5. **Évolutivité** : Les routeurs Cisco sont conçus pour évoluer avec les besoins de votre entreprise. Que vous soyez une petite entreprise ou une grande organisation, il existe des solutions adaptées à chaque taille et à chaque besoin.
6. **Sécurité** : Les routeurs Cisco intègrent des fonctionnalités de sécurité avancées, ce qui est essentiel pour protéger les données sensibles et garantir la sécurité des communications au sein de votre réseau.

En résumé, choisir un routeur Cisco, c'est opter pour une solution robuste, sécurisée et évolutive, idéale pour répondre aux défis modernes des réseaux d'entreprise.

## 3.Configuration du Routeur

### 3.1.Câblage

Il est important de connecter l'interface **GigabitEthernet0/0** au WAN.  
L'interface **GigabitEthernet0/1** sera quant à elle connectée au pare-feu, et donc indirectement au réseau de l'entreprise

### 3.2.Configuration terminal

**Toute la configuration du routeur s'effectue dans le terminal Cisco**

- Attribuez l'adresse IP publique à l'**interface GigabitEthernet0/0** (Remplacer l'IP dans la capture par l'IP attribuée par le FAI)

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int Gi
Router(config)#int GigabitEthernet0/0
Router(config-if)#ip address 88.156.12.55 255.255.255.240
Router(config-if)#no shutdown

Router(config-if)#

```

- Attribuez l'adresse IP 10.0.0.2/30 à l'interface GigabitEthernet0/1

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int Gi
Router(config)#int GigabitEthernet0/1
Router(config-if)#ip address 10.0.0.2 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#

```

---

- Ajoutez les routes et la passerelle par défaut:

Réseau cible	Masque	Passerelle
0.0.0.0	0.0.0.0	GigabitEthernet0/0
192.168.0.0	255.255.0.0	10.0.0.1
172.16.0.0	255.255.248.0	10.0.0.1
172.16.8.0	255.255.248.0	10.0.0.1

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 Gi
Router(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
Router(config)#ip route 192.168.0.0 255.255.0.0 10.0.0.1
Router(config)#ip route 172.16.0.0 255.255.248.0 10.0.0.1
Router(config)#ip route 172.16.8.0 255.255.248.0 10.0.0.1
Router(config)#

```

- Vérifiez les routes

```

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/30 is directly connected, GigabitEthernet0/1
L        10.0.0.2/32 is directly connected, GigabitEthernet0/1
  88.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        88.156.12.48/28 is directly connected, GigabitEthernet0/0
L        88.156.12.55/32 is directly connected, GigabitEthernet0/0
  172.16.0.0/21 is subnetted, 2 subnets
S          172.16.0.0/21 [1/0] via 10.0.0.1
S          172.16.8.0/21 [1/0] via 10.0.0.1
S          192.168.0.0/16 [1/0] via 10.0.0.1
S*        0.0.0.0/0 is directly connected, GigabitEthernet0/0

Router#

```

## Configuration du NAT

- Définissez l'interface GigabitEthernet0/1 comme **interface interne**:

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int GigabitEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#

```

- Définissez l'interface **GigabitEthernet0/0** comme **interface externe**:

```

Router(config)#int GigabitEthernet0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#

```

- Configurez le NAT Overload pour traduire les adresses IP internes en utilisant l'interface externe:

```

Router(config)#ip nat inside source list 1 interface GigabitEthernet0/0 overload
Router(config)#

```

- Créez les listes d'accès autorisant les réseaux locaux:

```
Router(config)#access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255
Router(config)#

```

---

- Copiez la **running-config** dans la **startup-config**

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

```

---

# IV - GESTION DU SYSTÈME

## 1. Active Directory

**Active Directory** (AD) est une implémentation par Microsoft des services d'annuaire LDAP pour Windows. Il comprend une base de données structurée qui recense les utilisateurs, ordinateurs et leurs autorisations d'accès.

AD gère l'authentification des utilisateurs pour garantir l'accès uniquement aux ressources autorisées.

### Rôles et avantages

- **Pour les administrateurs** : Gestion centralisée des utilisateurs et des droits d'accès, contrôle de la configuration via la Stratégie de groupe AD.
- **Pour les utilisateurs** : Authentification unique pour accéder à toutes les ressources autorisées.

### Stockage et partage des fichiers

- Les fichiers sont stockés de manière centralisée, permettant leur partage entre utilisateurs pour une meilleure collaboration et l'application de GPO permettant de déployer facilement des services et des programmes sur des groupes d'utilisateurs.
- Ces fichiers sont sécurisés et sauvegardés pour assurer la continuité de l'activité.

## 2. Fonctionnement d'Active Directory

### Service principal et Contrôleurs de domaine

- AD repose sur Active Directory Domain Services (AD DS) intégré à Windows Server.
- Les serveurs exécutant AD DS sont appelés contrôleurs de domaine, avec plusieurs contrôleurs dans une organisation, assurant la synchronisation des modifications (par exemple, mise à jour de mots de passe).

### Serveur de catalogue global

- Un contrôleur de domaine spécial qui stocke une copie complète des objets de son domaine et une copie partielle des objets d'autres domaines dans la forêt, permettant la recherche d'objets à travers la forêt.

### Appareils Windows et Protocoles utilisés

- Les appareils Windows, tels que les ordinateurs de bureau et portables, peuvent rejoindre un domaine Active Directory mais ne possèdent pas AD DS.
- AD utilise des protocoles standards tels que LDAP, Kerberos et DNS pour fonctionner efficacement.

### 3.Services DNS et DHCP dans AD DS

#### DNS (Domain Name System)

- Utilisé pour localiser les contrôleurs de domaine et faciliter la communication entre eux.
- L'intégration facile de l'espace de noms Active Directory dans un espace DNS existant simplifie la gestion.
- Les zones DNS intégrées à Active Directory éliminent la nécessité de configurer des zones secondaires et des transferts de zones.

#### DHCP (Dynamic Host Configuration Protocol)

- Attribue automatiquement des adresses IP aux appareils du réseau.
- Facilite la gestion des adresses IP dans des environnements complexes, permettant aux clients de se connecter au domaine sans configuration manuelle des adresses IP.

### 4.Choix de l'Active Directory

Nous avons choisi l'Active Directory comme solution robuste et évolutive pour gérer les infrastructures de notre réseau pour les raisons suivantes :

1. Gestion centralisée des utilisateurs, groupes et ordinateurs simplifiant l'administration et les configurations,
2. Authentification unique (SSO) pour un accès facile aux ressources du domaine et une meilleure productivité,
3. Sécurité avancée avec des protocoles comme Kerberos, une gestion des permissions d'accès et des Stratégies de groupe pour renforcer la sécurité.
4. Haute disponibilité grâce à la redondance des contrôleurs de domaine, garantissant la continuité des services,
5. Intégration DNS et DHCP pour la gestion des ressources réseau et l'attribution dynamique des adresses IP, et
6. Audit, traçabilité et facilité d'expansion, permettant de suivre les actions des utilisateurs et d'étendre facilement l'infrastructure à différents sites géographiques.

## 5. Prérequis Matériels

Pour un réseau comprenant un millier d'utilisateurs nous recommandons les configurations suivantes :

Ressource	Minimum	Recommandé
CPU	8 cœurs	12-16 cœurs
RAM	16 Go	32 Go
Stockage	500 Go SSD	500 Go SSD NVMe
Réseau	1 Gbps	10 Gbps
Serveurs	HPE DL360 / Dell R640	HPE DL360 / Dell R640

## 6. Création du Gestionnaire de Domaine

### 6.1. Prérequis initiaux

Nous allons voir ici comment créer le premier contrôleur de domaine et par là même créer la forêt MOLECULIS.

Sur le serveur Windows, vérifier que les dernières mises à jour sont correctement installées, que le serveur est configuré avec une IP statique et que la machine sur laquelle l'installation va être faite possède un nom approprié.

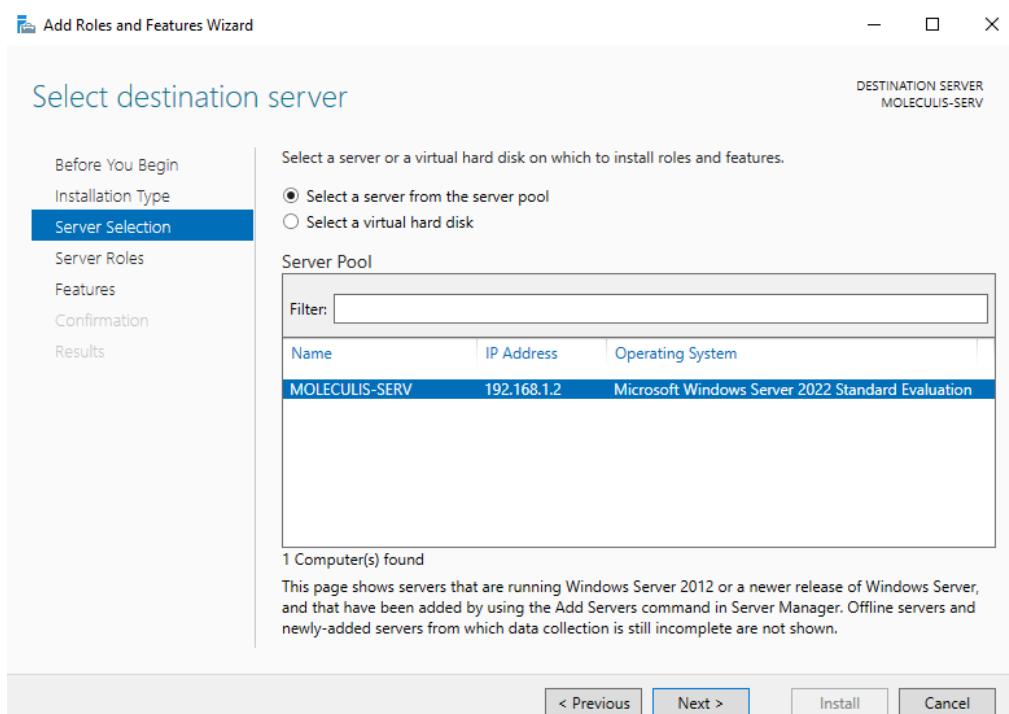
### 6.2. Installation d'un rôle du gestionnaire du domaine

Nous allons voir ici comment ajouter un service un rôle à notre domaine en commençant par l'**ADDS**. Nous verrons dans les rubriques suivantes les rôles **DNS**, **DHCP** et **Certification** qui suivront globalement la même procédure d'installation.

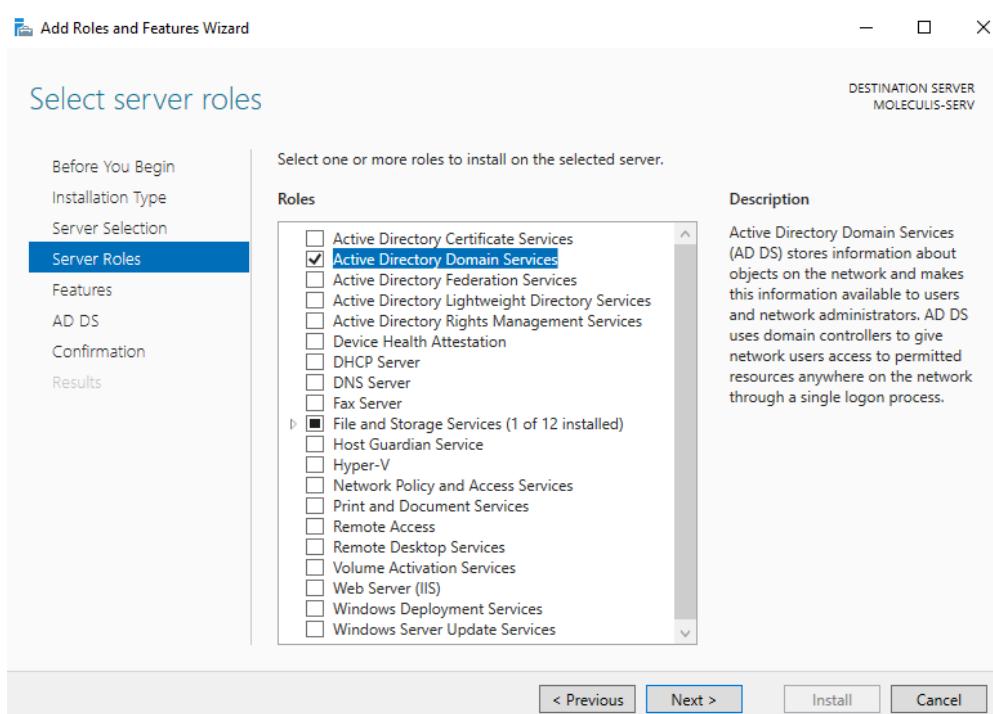
Dans le **Gestionnaire de serveur**, cliquez sur **Manage** et sélectionnez **Ajouter des rôles et fonctionnalités**.

Vous accédez dès lors à l'assistant d'installation du rôle. Cliquez sur **Suivant** sur la page de bienvenue puis choisissez **Installation basée sur un rôle ou une fonctionnalité**.

Sélectionnez ensuite le serveur local et cliquez sur **Suivant**.

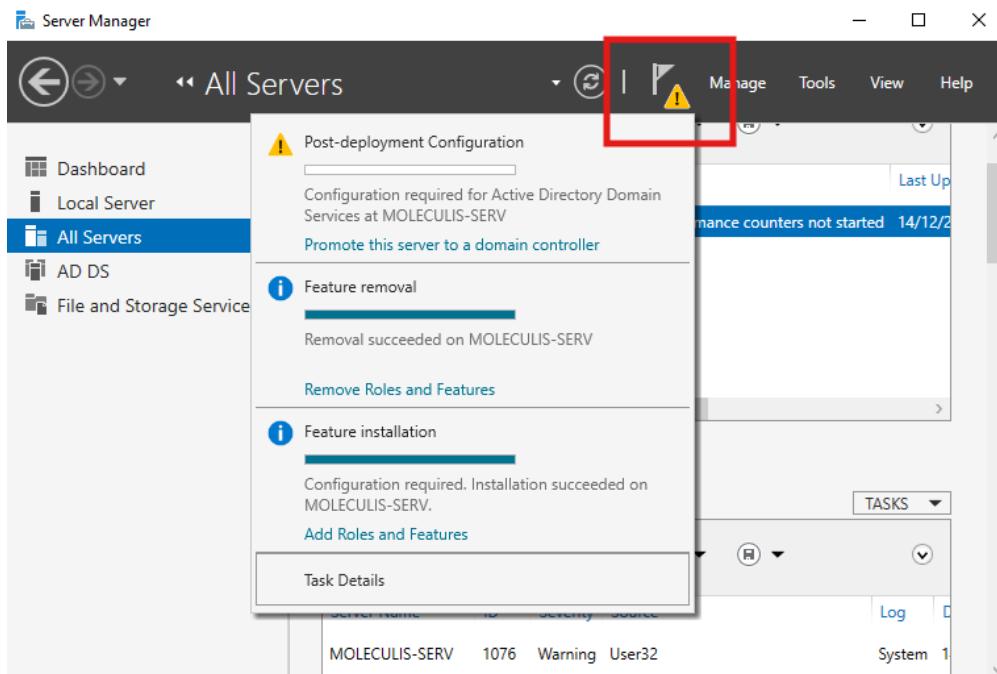


Dans la sélection du rôle, cliquez sur **Service de domaine Active Directory** puis **Ajouter les fonctionnalités** et enfin **Suivant**.



Laissez ensuite les fonctionnalités par défaut, cliquez sur **Suivant** puis sur **Installer** après avoir passé en revue les informations.

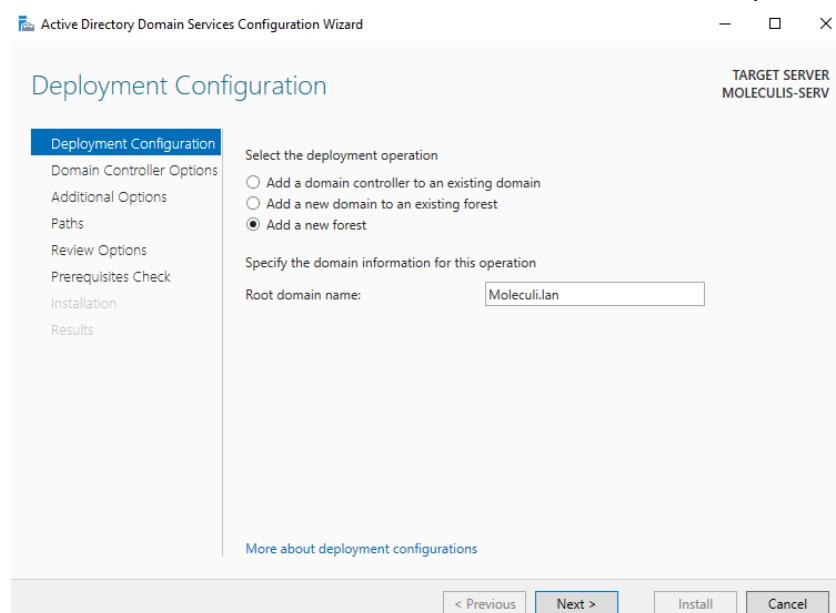
Une fois l'installation terminée, cliquez sur le lien en haut à gauche **Promouvoir ce serveur en contrôleur de domaine** pour effectuer la post-installation.



### 6.3. Configuration du rôle ADDS

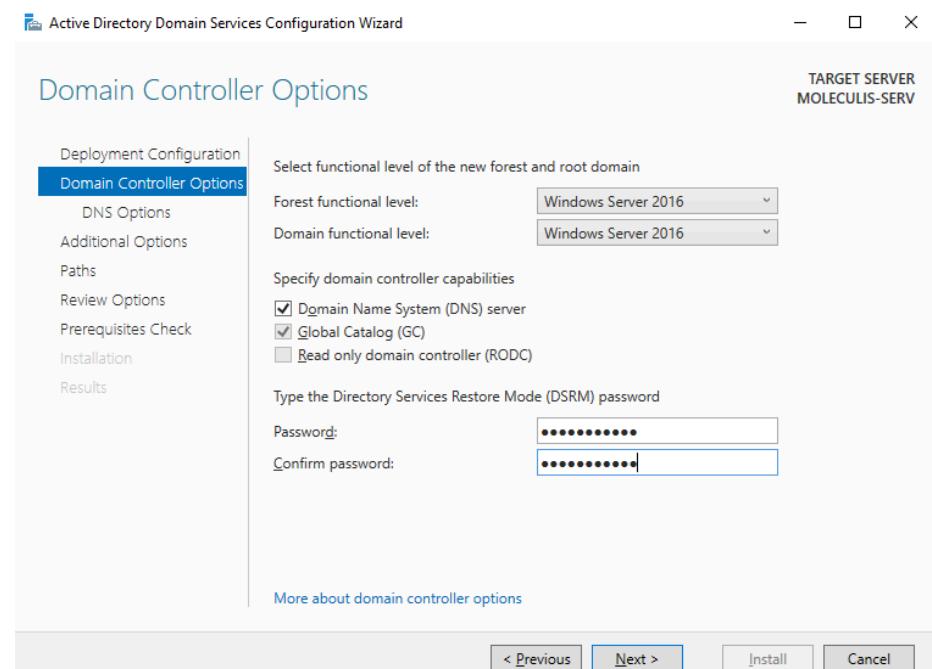
Un assistant de configuration va maintenant permettre de configurer le contrôleur de domaine.

S'il s'agit du premier contrôleur et que le domaine n'existe pas encore, choisissez **Ajouter une nouvelle forêt** et entrez le nom DNS **Moleculis.lan** puis cliquez sur **Suivant**.



Choisissez ensuite le niveau fonctionnel de la forêt et du domaine ainsi créé, dans notre cas **Windows Server 2016**.

Cochez Serveur **DNS** et **Catalogue global**. La configuration du serveur DNS sera détaillée dans une autre rubrique de ce guide. Précisez aussi un mot de passe pour le service de restauration.



Ne sélectionnez pas d'option de délégation DNS et entrez par la suite MOLECULIS comme nom **NETBIOS**. Laissez les **Paths** par défaut proposés par l'assistant d'installation.

Contrôlez ensuite le résumé des options choisies et lancez la vérification des prérequis. Si ces derniers sont corrects, vous allez pouvoir cliquer sur **Installer**.

Une fois l'installation du rôle terminée, le serveur va redémarrer automatiquement. Une fois le redémarrage terminé, connectez-vous au domaine avec le **compte administrateur par défaut** (MOLECULIS/administrateur).

Vérifiez la fonctionnalité du domaine avec l'outil **Utilisateurs et Ordinateurs Active Directory**.

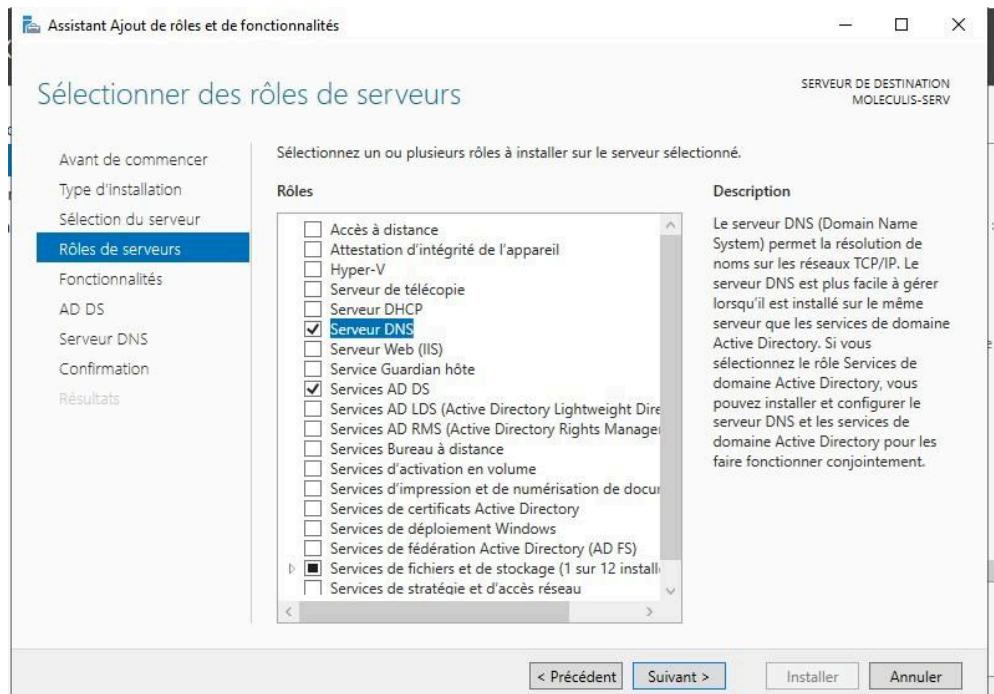
Le domaine est créé et il va maintenant être possible de :

- configurer le service DNS associé à l'ADDS
- créer et configurer le rôle DHCP
- créer et configurer un rôle de certification (ACDS)
- organiser le domaine avec des Unité d'Organisation, des utilisateurs et des membres
- organiser une politique de sécurité avec les GPO

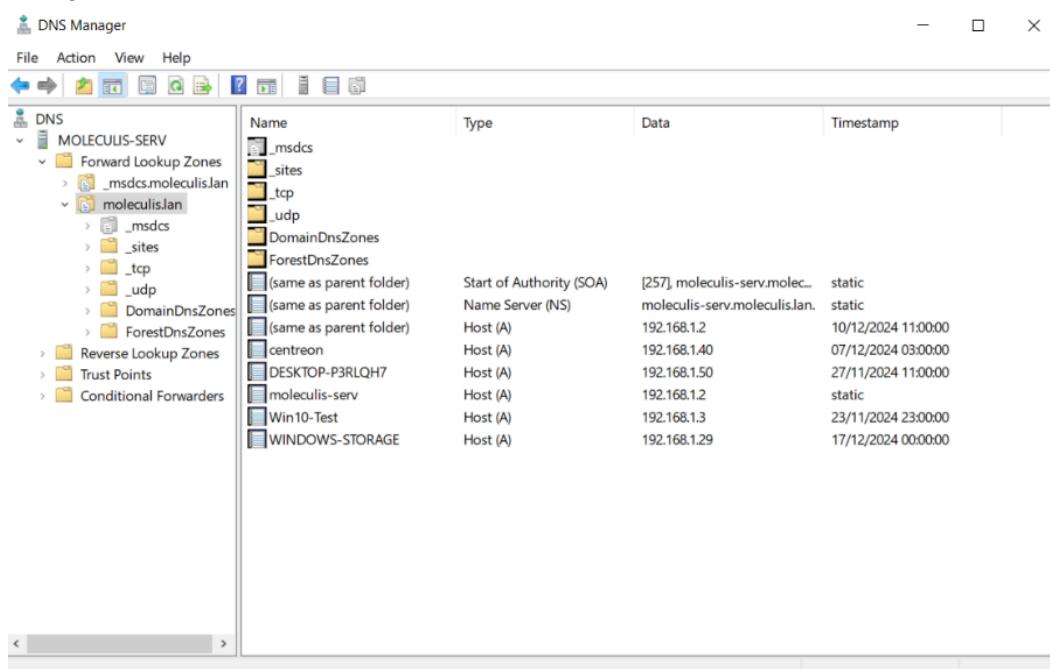
Toutes ces configurations vont être traitées dans la suite de ce guide.

## 7. Configuration du service DNS

- L'installation du rôle Active Directory Domain Services (AD DS) sur Windows Server 2022 permet d'installer et de configurer automatiquement les services nécessaires pour la gestion d'un domaine, tels que le DNS. Il faut s'assurer de sélectionner le serveur DNS :



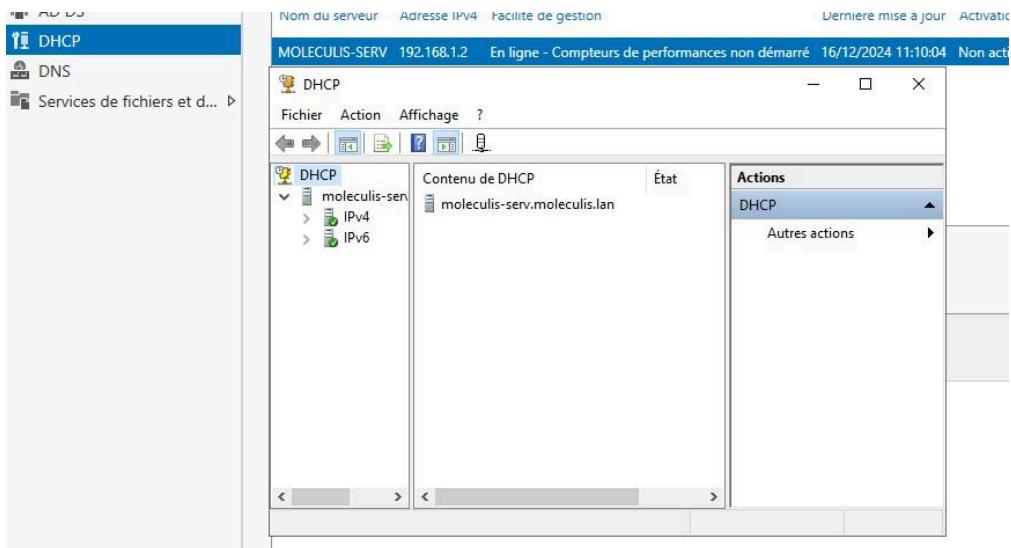
- Aperçu du domaine DNS après création :



## 8. Configuration du DHCP

### Installation du rôle DHCP :

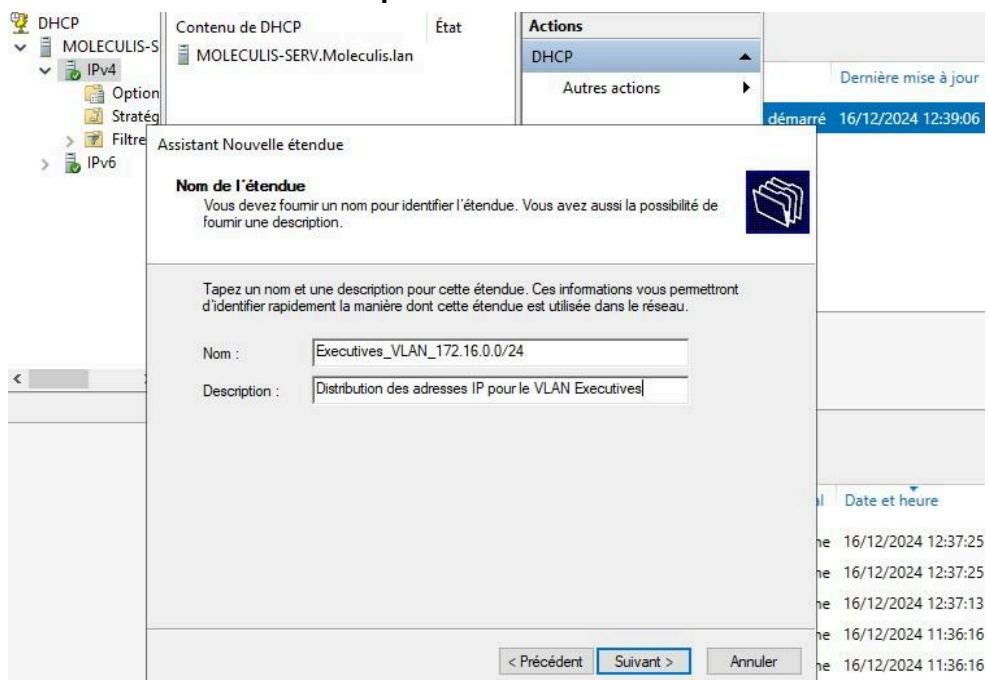
- Dans Gestionnaire de serveur → Ajouter des rôles et fonctionnalités.
- Sélectionnez "Serveur DHCP" et suivez les étapes. On obtient après configuration :



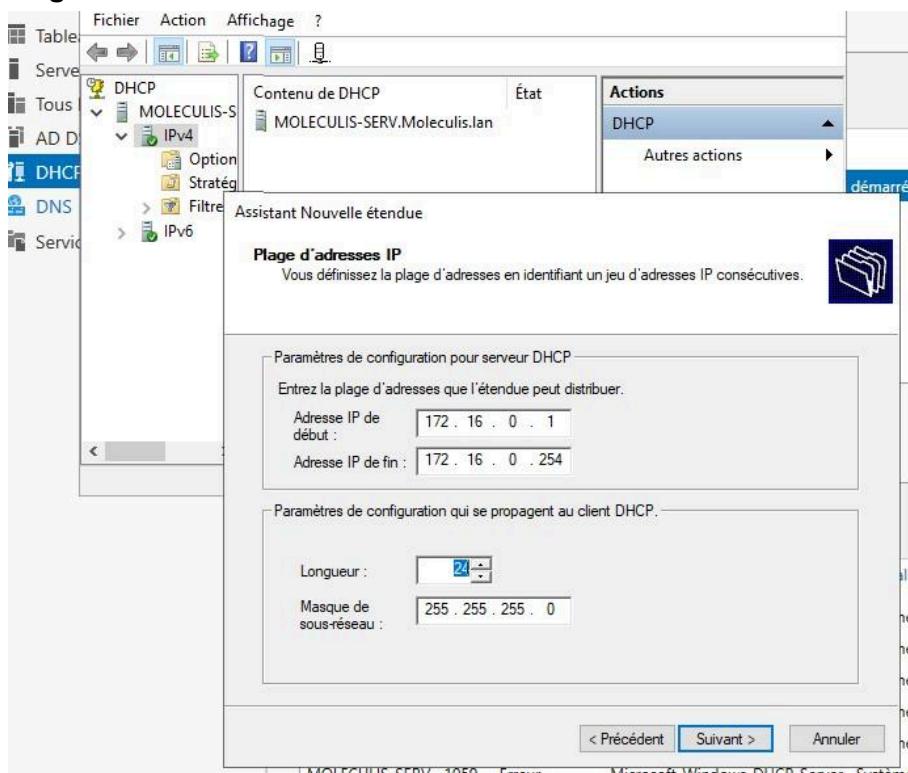
## Création d'une nouvelle étendue DHCP pour le réseau interne

Exemple de création d'une étendue (scope) pour le Vlan Administratif :

- Cas concret avec le Vlan de la direction (Executives\_VLAN) :
- **Création d'un nouveau scope :**

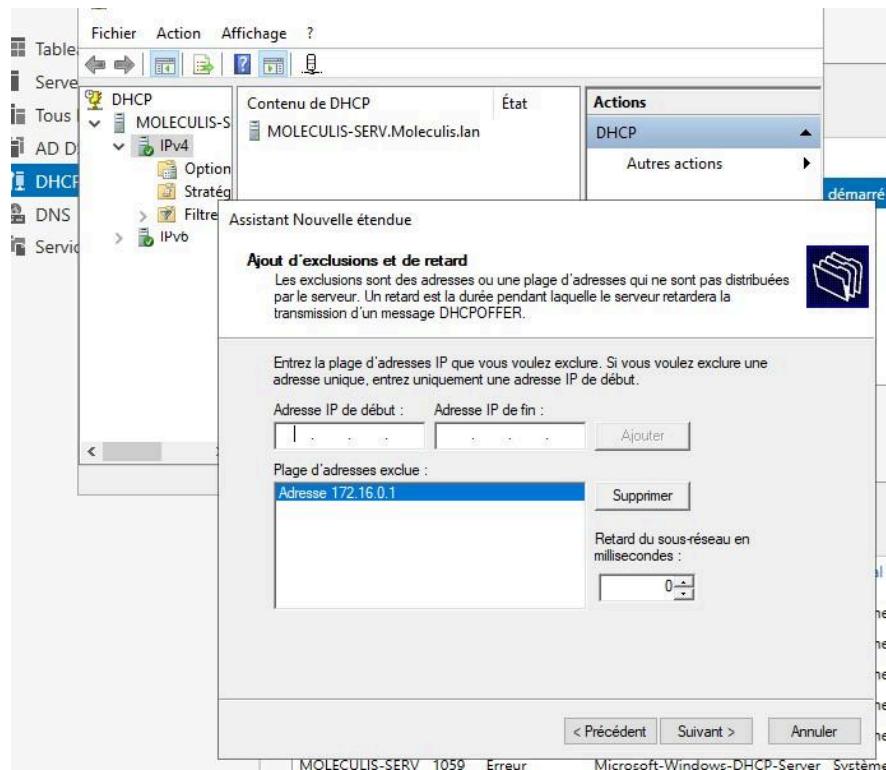


- **Plage d'adresses :**



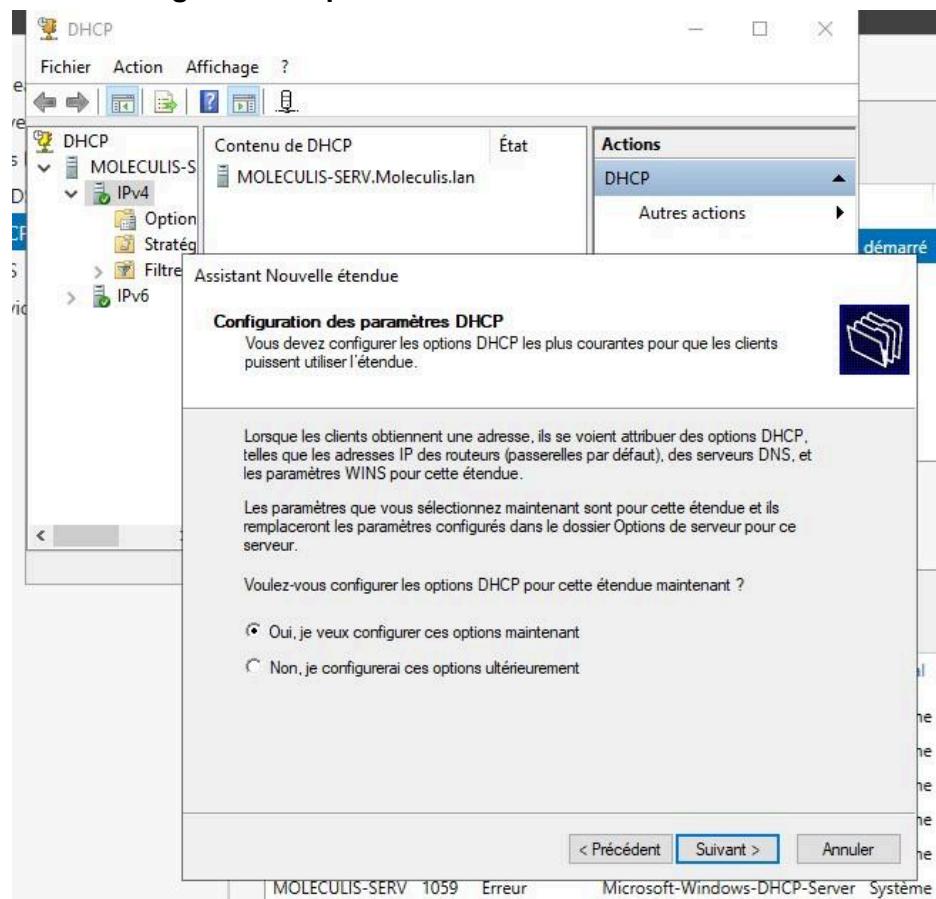
→ **Exclusions (adresses réservées) :**

- Exemple de passerelles (Switch/Routeur) :
- Pour tous les serveurs ou équipements réseau ajoutés on fera une exclusion dans la plage.

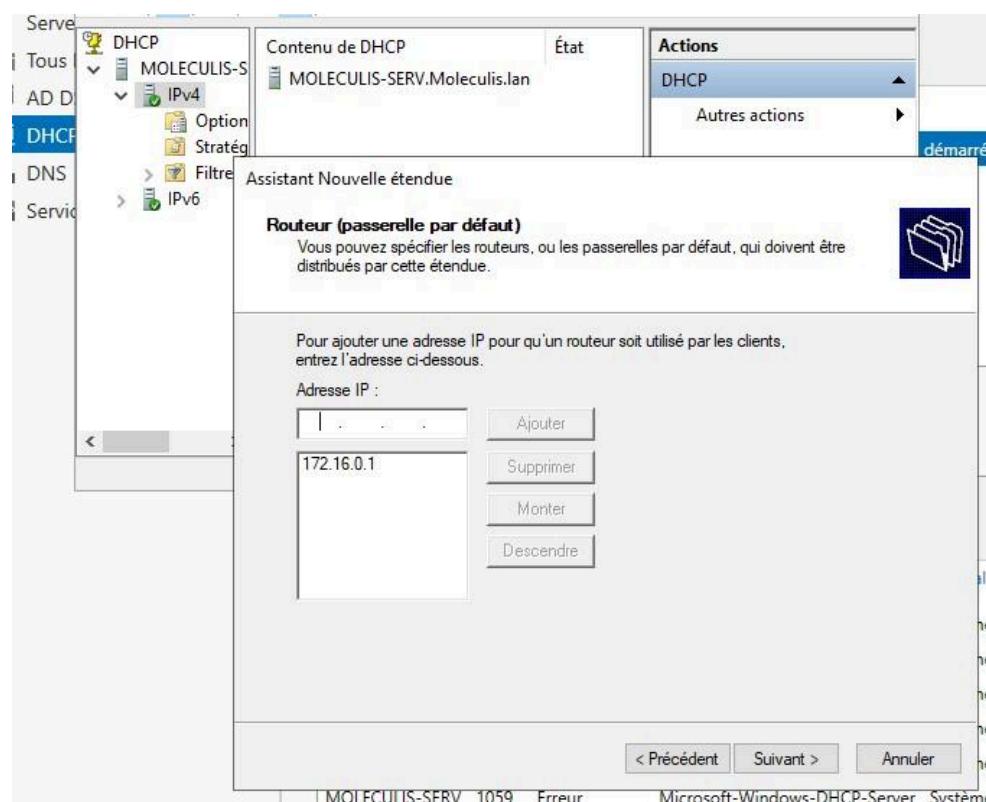


→ **Durée du Bail : Valeur par défaut : 8 jours.**

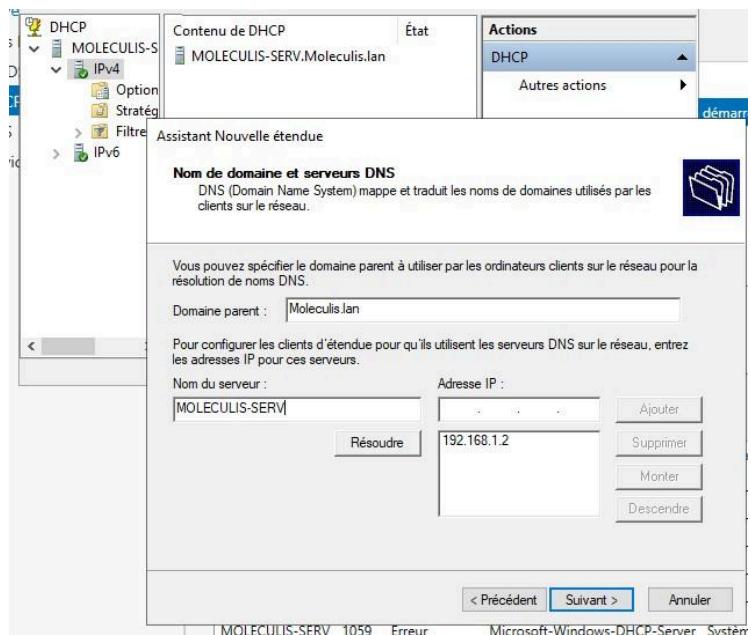
## → Configurer les Options DHCP :



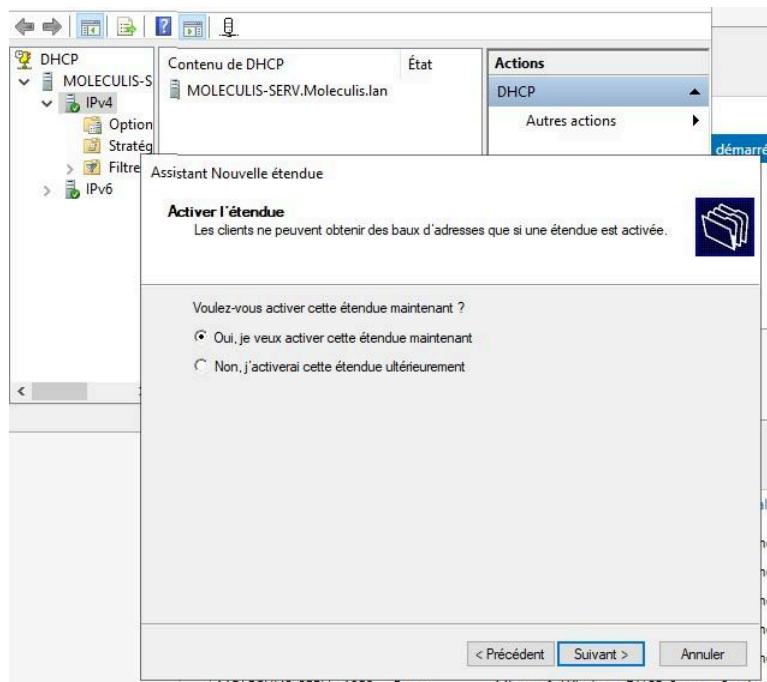
## ● Passerelle (Routeur) :



- Serveur DNS :



- Activer le Scope :

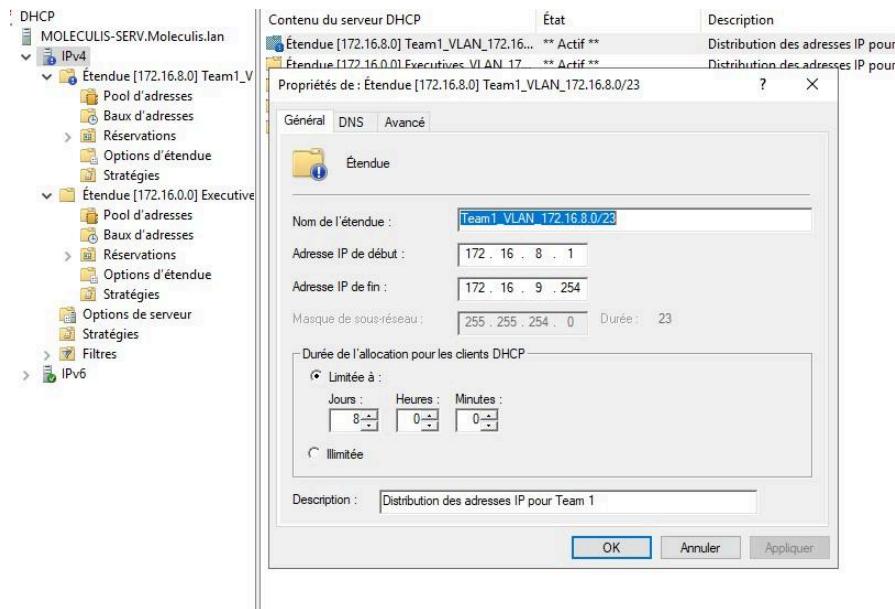


→ Résumé du Scope Executives :

Paramètre	Valeur
Nom du Scope	Executives_VLAN_172.16.0.0/24
Plage d'adresses	172.16.0.1 - 172.16.0.254
Masque	255.255.255.0 (/24)
Passerelle	172.16.0.1 (exclusion)
Serveur DNS	192.168.1.2
Nom de Domaine	moleculis.lan

- Répétition de la procédure pour chaque sous-réseaux des deux VLAN :

Exemple pour le VLAN recherche et technique : Team 1



## 9.Configuration de l'autorité de Certification (ADCS)

### 9.1.Rôle du service de Certification

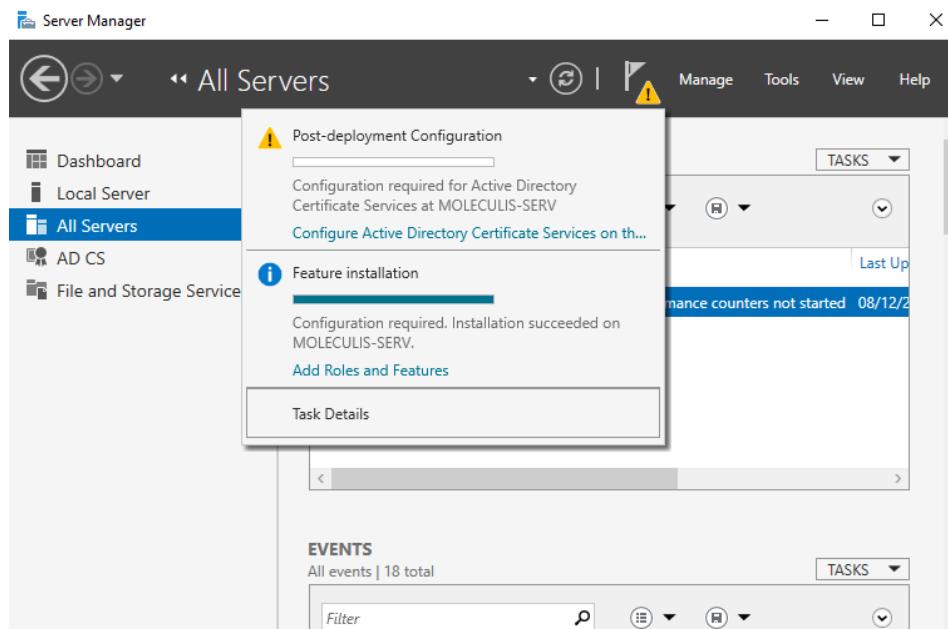
Ce service est responsable de l'émission, de la gestion et la révocation de certificats numériques. Ces certificats permettent de **sécuriser les communications, d'authentifier les utilisateurs, les ordinateurs ou les services et de garantir l'intégrité des données.**

Dans le système livré, il intervient notamment dans l'authentification des administrateurs et des techniciens ayant accès au **pare-feu**, en temps qu'autorité de certification remote, ainsi que dans le contrôle des accès au serveur **VPN**.

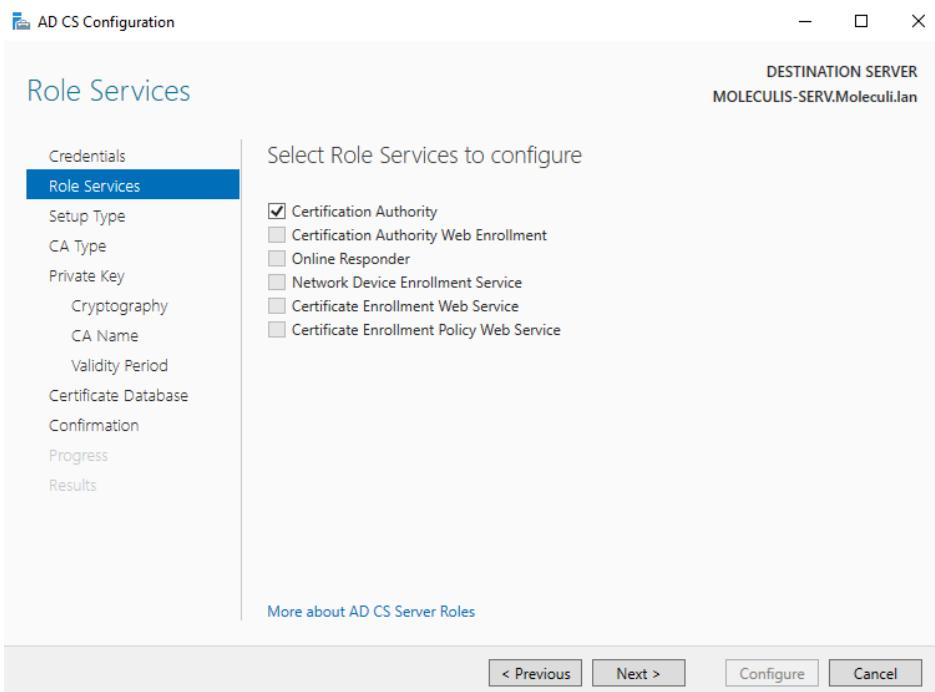
### 9.2.Installation et configuration de l'autorité de certification

L'installation du rôle est identique à celle des autres rôles, se référer à Installation d'un rôle décrite en détail plus haut dans la création du gestionnaire de domaine. Choisissez **Autorité de Certification (ADCS)** et gardez les valeurs par défaut jusqu'à l'installation.

Vous accéderez ensuite, comme lors de la création du rôle ADDS à la configuration après déploiement du rôle de certification.



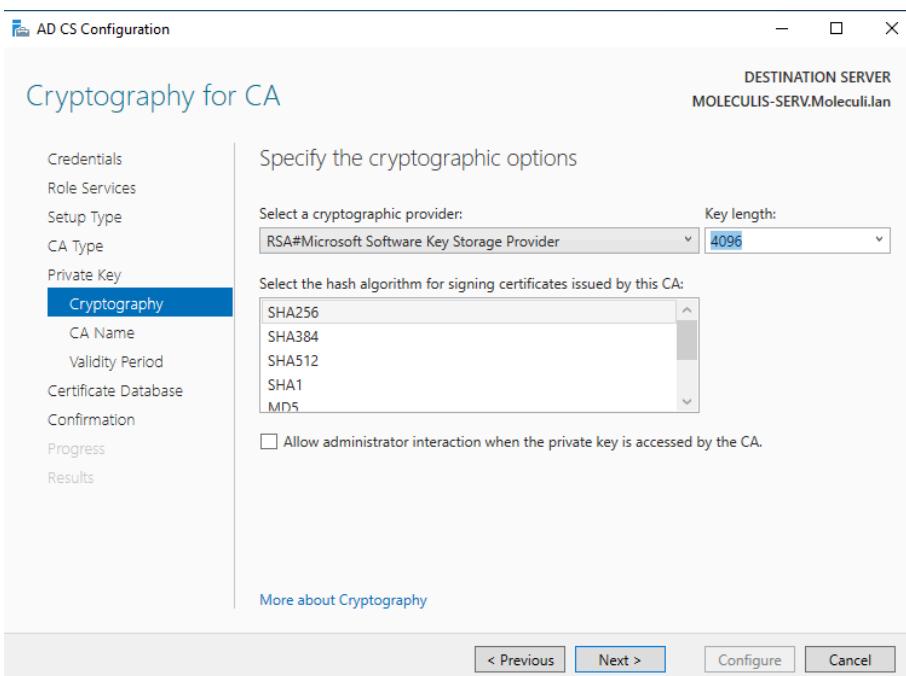
Vous allez pouvoir continuer la configuration de l'autorité de certificat grâce à l'assistant d'installation. Choisir tout d'abord **Autorité de Certification**.



Puis sélectionnez le type **CA d'entreprise** et **Root CA**.

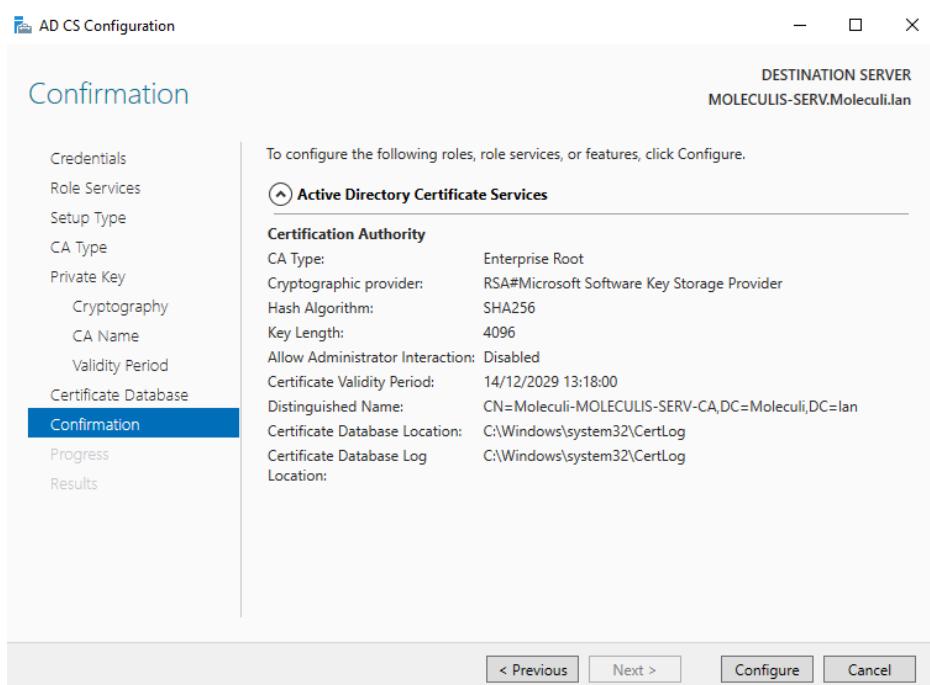
Choisissez ensuite de créer une **Nouvelle clé privée** et configurer de la manière suivante :

- Fournisseur de la clé : gardez l'option par défaut
- Longueur de la clé : choisissez **4096** bits pour renforcer la sécurité
- Algorithme : **SHA256**



Gardez ensuite les noms par défaut et une période de validité de **10 ans**.  
Laissez les emplacements par défaut pour les bases de données et les logs de l'autorité de certification.

Valider ensuite les paramètres précisés plus tôt et lancer l'installation de la configuration en cliquant sur **Configurer**.



Un message de confirmation doit s'afficher. **Le rôle ACDS est maintenant actif.**  
Nous allons voir maintenant comment générer un certificat qui pourra être utilisé par la suite dans la gestion du domaine MOLECULIS.

### 9.3.Génération d'un certificat

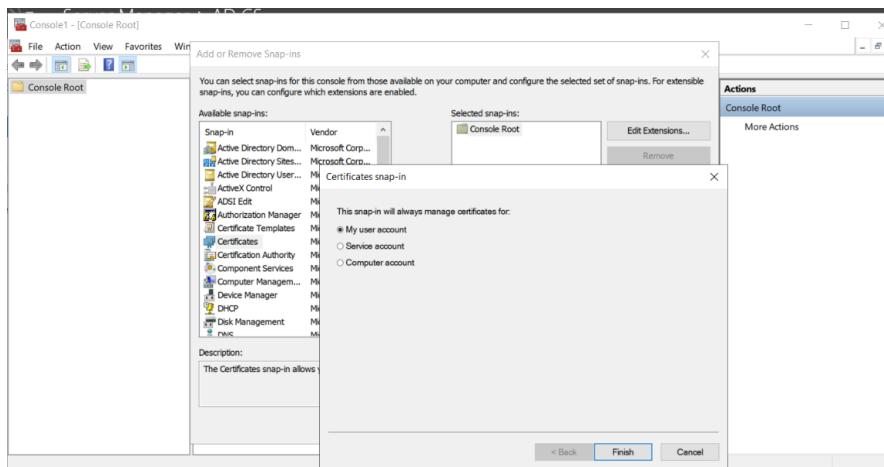
**Lancer la console MMC pour accéder à la gestion des certificats :**

Appuyez sur Window + R puis tapez mmc et faites Entrée

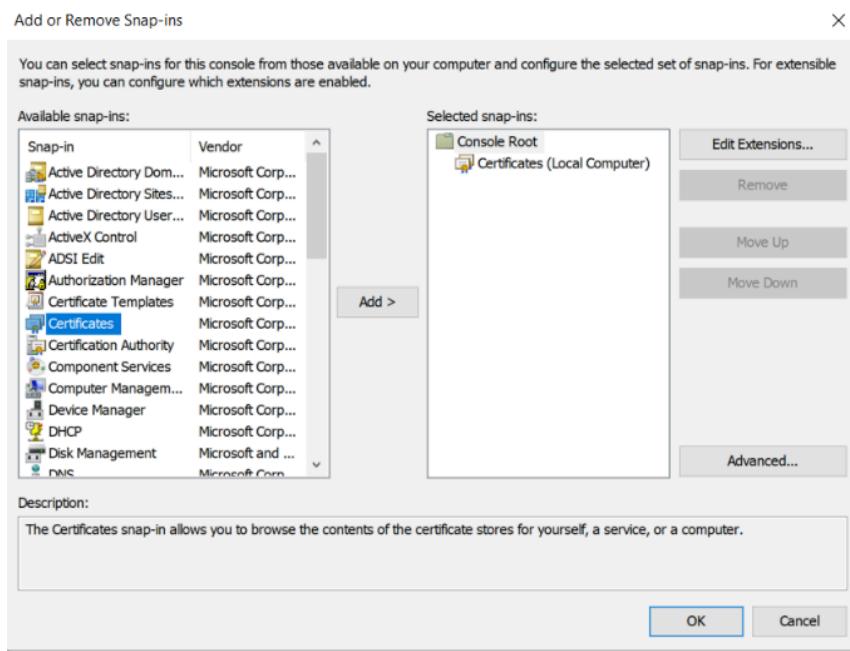
Ajouter le composant logiciel enfichable pour les certificats en allant dans le menu **Fichier**, puis cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.

Sélectionnez **Certificats**, puis cliquez sur **Ajouter**.

Choisissez **Compte d'ordinateur**, **Compte utilisateur** ou **Service** (ici Service donc pour l'utilisateur-service pfSense créé dans l'AD), puis cliquez sur **Terminer** et **OK**.



Sélectionnez ensuite **Certificats**, faites **Ajouter** et sélectionnez le **Certificat local**



Vous retrouverez le certificat créé lors de l'installation de l'**Active Directory Certificate Service** (ici *moleculis-Moleculis-SERV-CA*).

Issued To	Issued By	Expiration Date	Intended Pur
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stampin
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Client Auther
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Client Auther
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Client Auther
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Client Auther
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10/11/2031	Time Stampin
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Auther
ISRG Root X1	ISRG Root X1	04/06/2035	Client Auther
Microsoft Authenticode(tm) Root	Microsoft Authenticode(tm) Root	01/01/2000	Secure Email
Microsoft ECC Product Root Cert	Microsoft ECC Product Root Cert	27/02/2043	<All>
Microsoft ECC TS Root Certificate	Microsoft ECC TS Root Certificate	27/02/2043	<All>
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>
Microsoft Root Certificate Author	Microsoft Root Certificate Authority	10/05/2021	<All>
Microsoft Root Certificate Author	Microsoft Root Certificate Authority	23/06/2035	<All>
Microsoft Root Certificate Author	Microsoft Root Certificate Authority	22/03/2036	<All>
Microsoft Time Stamp Root Cert	Microsoft Time Stamp Root Cert	22/10/2039	<All>
<b>moleculis-MOLECULIS-SERV-CA</b>	<b>moleculis-MOLECULIS-SERV-CA</b>	<b>28/11/2034</b>	<b>&lt;All&gt;</b>
moleculis-MOLECULIS-SERV-CA	moleculis-MOLECULIS-SERV-CA	28/11/2034	<All>
NO LIABILITY ACCEPTED. (c)97 Veri	NO LIABILITY ACCEPTED. (c)97 Veri	08/01/2004	Time Stampin
Symantec Enterprise Mobile Ro	Symantec Enterprise Mobile Root	15/03/2032	Code Signing
Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Time Stampin
USERTrust RSA Certification Auth	USERTrust RSA Certification Authority	19/01/2038	Client Auther

Sélectionnez **Exporter** et indiquez le chemin vers lequel la partie publique du certificat va être enregistrée.

**File to Export**  
Specify the name of the file you want to export

File name:

**Next** **Cancel**

Vous pouvez dorénavant récupérer la partie publique du certificat localement. Celle-ci va pouvoir être copiée afin de définir l'**authentification remote** effectuée par l'Active Directory.

La clé doit être de la forme :  
**-----BEGIN CERTIFICATE-----**  
**<Chaîne\_alphanumérique>**  
**-----END CERTIFICATE-----**

## 10. Architecture de l'Active Directory

### 10.1. Notre politique concernant les Unités organisationnelles (OU)

Nous avons décidé, concernant l'organisation de l'Active Directory Moleculis.lan, une structuration en Unités Organisationnelles (OU) permettant d'offrir une gestion claire, centralisée et sécurisée des utilisateurs et des ordinateurs du laboratoire.

Cette organisation repose trois grandes divisions reflétant la séparation des rôles entre les différents départements. Le découpage initial dédie chaque OU à un domaine spécifique pour ensuite faciliter le déploiement et la gestion de politiques de sécurité (GPO, dont les détails seront traités dans la prochaine rubrique) adaptés aux utilisateurs.

On retrouve le premier découpage suivant :

- Administrative : Employés des bureaux administratifs, de l'accueil etc..
- Research : Bureaux des chercheurs et plateaux techniques
- IT : Administrateurs et techniciens informatiques

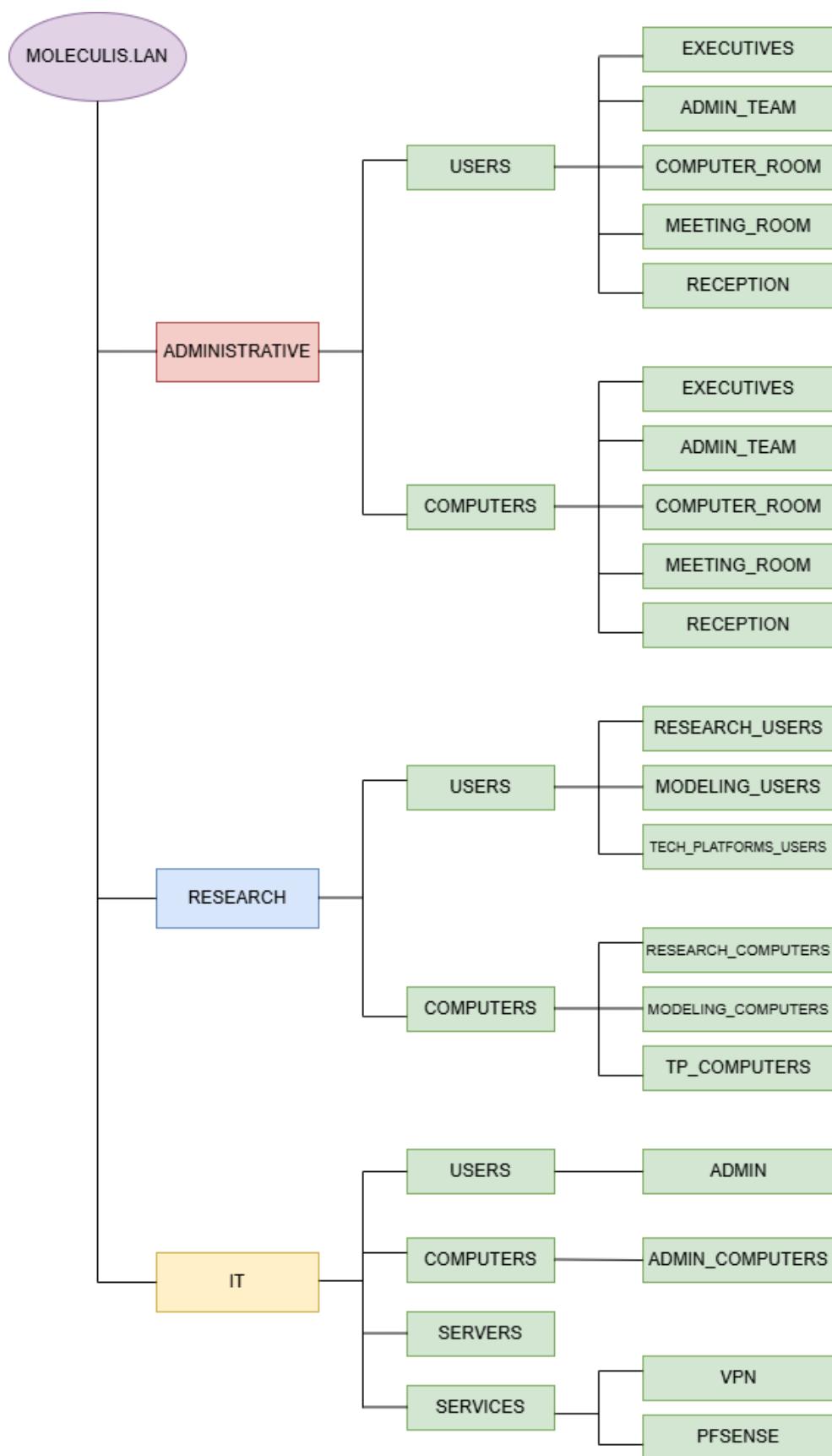
Chacune de ces unités possède des sous-unités adaptées aux rôles spécifiques des utilisateurs et des équipements. On retrouve dans chaque département une sous-unité pour les utilisateurs ou le matériel, afin d'appliquer de manière distincte des politiques sur des utilisateurs spécifiques (généralement regroupés au sein d'un groupe commun) ou sur les postes de manière plus globale.

**Les OU Administrative et Research** ont des accès restreint au réseau (ces priviléges étant réservés aux administrateurs) mais il va être possible d'appliquer des déploiements de logiciels et de services ainsi que de contrôler l'accès aux ressources partagées afin de faire évoluer l'environnement de travail des chercheurs et des employés administratifs selon leurs besoins.

**L'OU IT** est isolé des deux autres groupes d'employés et regroupe les éléments cruciaux pour les informaticiens du réseau comme les serveurs, des ordinateurs possédant des accès plus larges aux ressources ainsi que des outils d'administrations.

On retrouve aussi dans cet OU IT une sous-unité **Network\_Services** contenant les éléments liés au pare-feu **pfSense** et au service **OpenVPN**.

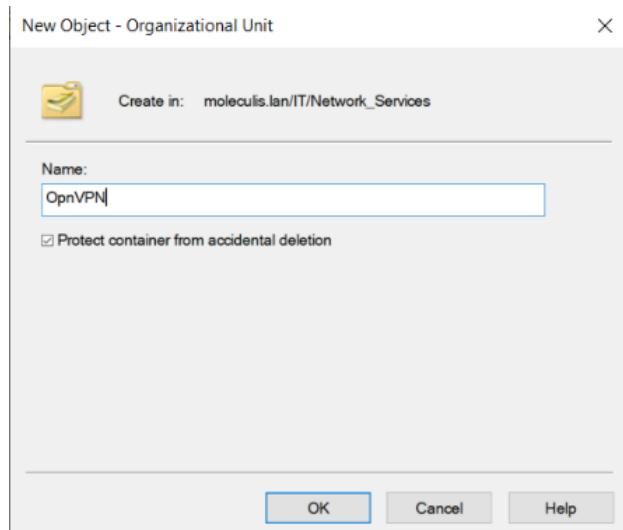
## 10.2.Schéma structurel du domaine MOLECULIS.LAN



### 10.3.Création d'un OU

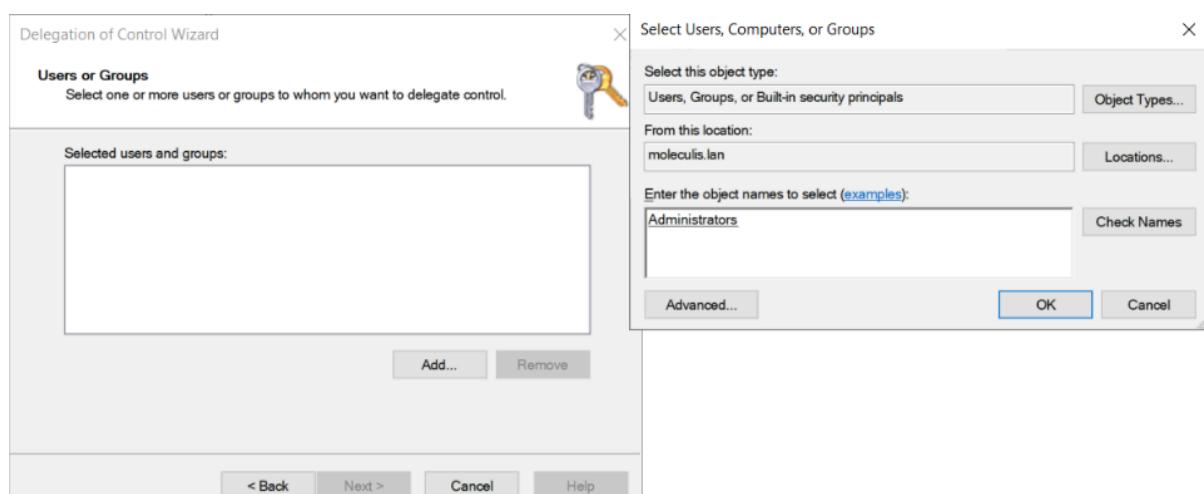
Nous allons voir ici comment créer une OU ainsi que des utilisateurs et des groupes en prenant exemple sur l'OU OpenVPN.

Dans l'arborescence Moleculis.lan allez dans **IT/Network\_Services** et cliquez droit, sélectionnez **Nouvelle** puis **Unité Organisationnelle**.  
Entrez le nom de cette nouvelle OU, à savoir OpenVPN.



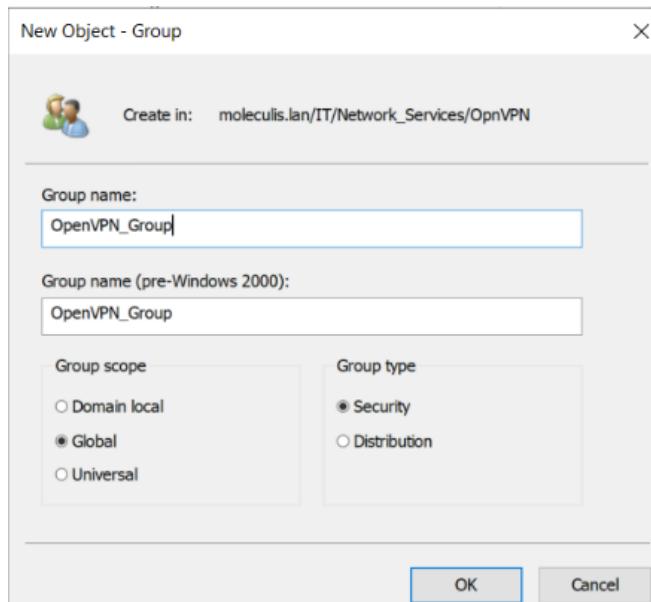
Vous pouvez ensuite cliquer sur l'OU fraîchement créée et **déléguer** son administration. Nous garderons ici un contrôle strict pour l'administrateur.

Il sera possible de cette manière de déléguer des droits de lecture (et uniquement de lecture) pour l'utilisateur-service pfSense, afin que celui-ci puisse amorcer l'authentification entre le pare-feu pfSense et l'Active Directory.



Dans un premier temps nous allons créer un groupe OpenVPN\_Group ainsi qu'un utilisateur OpenVPN\_User.

Pour le groupe choisir un scope **Global** et un type **Sécurité**.



Créez de même un utilisateur et ajoutez le à ce groupe. Il va maintenant être possible d'appliquer des politiques (GPO) propres à cet OU ou au utilisateurs VPN membres du groupe pour faciliter la gestion du de l'accès VPN.

Il sera notamment possible de **déployer le client OpenVPN et les configurations de connexion remote** lors de la prochaine connexion dans l'utilisateur dans le domaine.

Nous allons maintenant présenter les politiques associées à la hiérarchie et aux groupes du domaine MOLECULIS détaillés précédemment.

## 11. Politiques de Sécurité

### 11.1. Introduction aux GPO

Un **GPO (Group Policy Object)** est un objet dans Active Directory qui définit des paramètres de configuration pour des utilisateurs, ordinateurs ou groupes. Il permet de centraliser l'administration du domaine du laboratoire, en appliquant des politiques de sécurité, des paramètres de configuration, et des scripts.

Les GPO sont structurés en deux sections principales :

- **Configuration de l'ordinateur:** Appliquée aux ordinateurs membres du domaine, cette section inclut des stratégies (sécurité, mot de passe), des paramètres logiciels (installation de logiciels) et des scripts (exécution au démarrage/arrêt des ordinateurs).
- **Configuration de l'utilisateur:** Appliquée aux utilisateurs, cette section gère des stratégies de bureau, des paramètres logiciels et des scripts (exécution lors de la connexion/déconnexion).

Cette structuration ordinateur/utilisateur est la raison pour laquelle nous avons choisi de dissocier dans l'organisation du domaine MOLECULIS abordée plus haut, chaque département en unités Users et Computers afin de faciliter leur gestions.

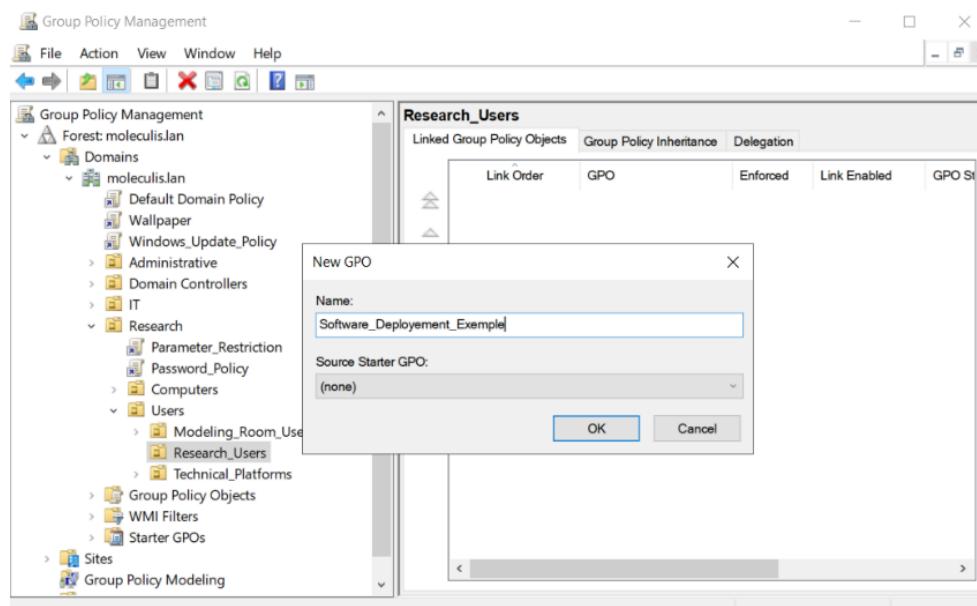
Les GPO ont une **priorité** qui dépend de leur niveau : les GPO appliqués en bas (niveau plus spécifique, comme l'OU) ont priorité. L'option **No Override** peut empêcher un GPO de plus bas niveau d'être remplacé. L'option **Block Inheritance** permet d'empêcher l'héritage des GPO d'un niveau supérieur.

## 11.2. Création et gestion des GPO

Nous allons voir dans cette partie la création d'un GPO, en l'occurrence, pour cet exemple, le déploiement d'un logiciel pour sur les sessions de l'équipe de recherche.

La gestion des GPO se fait via la **Group Policy Management Console (GPMC)**.

**Création d'un GPO :** Dans l'outil de management, cliquez sur l'OU concernée par la GPO que vous voulez appliquer, sélectionnez Créeer une GPO et nommez la.



**Liaison d'un GPO :** Associez un GPO à une **Unité Organisationnelle (OU)**, un **site** ou un **domaine** ou un groupe.

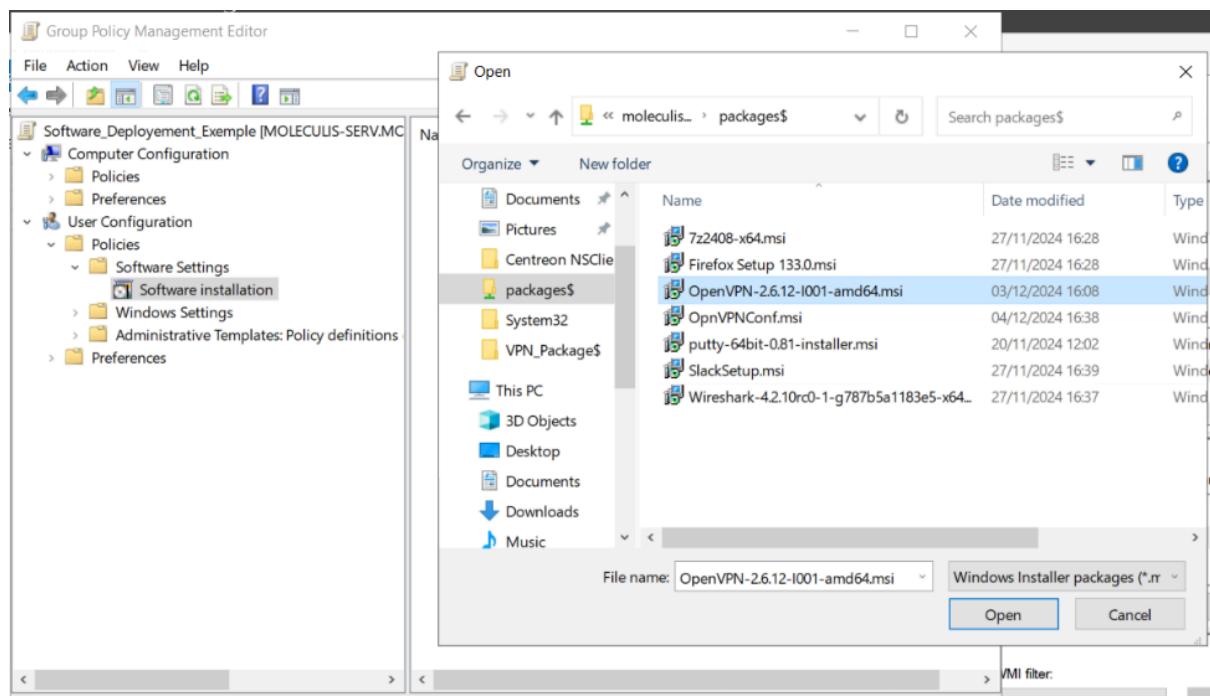
#### **Modification d'un GPO :**

Nous allons ici configurer la GPO pour qu'elle applique le déploiement du logiciel.

Cliquez sur la GPO puis **Éditer**

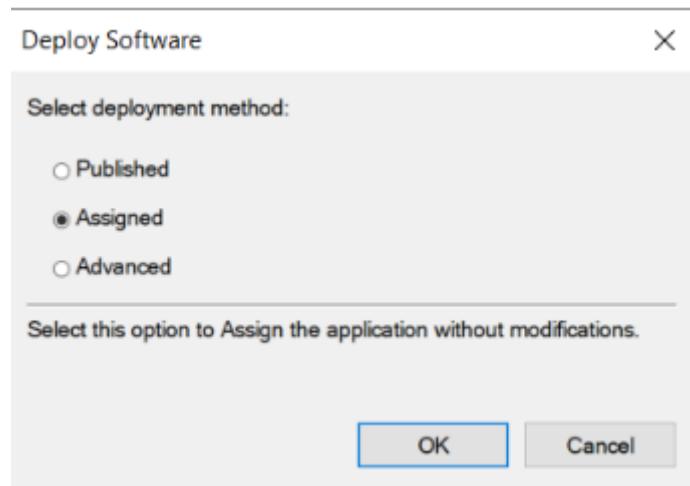
Allez ensuite dans **Configuration Utilisateur** car il s'agit d'un GPO que nous voulons uniquement déployer sur une session utilisateur, puis dans **Politique -> Logiciel -> Installation d'un logiciel**.

Sélectionnez l'installateur (idéalement en .msi) du client OpenVPN placé préalablement dans un fichier de partage réseau et faites **Ouvrir**.



Différents choix de déploiement vont être proposés :

- **Publier** permet de déployer sans installer, à charge de l'utilisateur de le faire ou non.
- **Assigner** en revanche va forcer l'installation.



Lors de la prochaine connexion d'un chercheur dans le domaine MOLECULIS, le client openvpn sera automatiquement installé par l'Active Directory.

**Délégation des droits** : Il est possible, de la même manière que pour les OU, d'accorder des permissions particulières pour modifier ou gérer un GPO.

**Mise à jour** : Forcez la mise à jour des GPO avec la commande powershell **gpupdate /force** manuellement ou attendre une actualisation automatique.

Les outils principaux pour gérer les GPO sont :

**GPMC** : Gestion des GPO dans le domaine.

**gpresult** : Affichage des GPO appliqués à un utilisateur ou un ordinateur via ligne de commande.

**rsop.msc** : Outil graphique permettant de visualiser les stratégies appliquées sur un poste ou un utilisateur.

### 11.3.Organisation des GPO

#	Nom de la GPO	Description	Application sur	Paramètres principaux
1	<b>Admin_Password_Policy</b>	Définit la politique de mot de passe pour les administrateurs.	<b>OU : IT</b> <b>Groupe :</b> Administrators	Complexité des mots de passe, expiration, longueur minimale.

#	Nom de la GPO	Description	Application sur	Paramètres principaux
2	<b>User_Password_Policy</b>	Politique de mot de passe pour les utilisateurs dans certaines OU.	OU : Research, Administrative	Complexité, expiration, longueur minimale.
3	<b>Admin_Software_Deployment</b>	Déploie des logiciels pour les administrateurs.	OU : IT Groupe : Administrator	Installation automatique des logiciels pré-configurés.
4	<b>User_Software_Deployment</b>	Déploie des logiciels pour les utilisateurs du domaine.	Groupe : Domain Users	Déploiement automatique de logiciels pour tous les utilisateurs.
5	<b>Windows_Update_Policy</b>	Configuration des mises à jour automatiques de Windows.	OU : Domain Groupe : Users	Mises à jour automatiques, planification des heures de mise à jour.
6	<b>pfSense_Forbid_Local_Session</b>	Interdit les sessions locales pour les utilisateurs du domaine.	OU : Moleculis.lan Groupe : Users	Désactivation des connexions locales sur pfSense.
7	<b>SNMP_Configurations</b>	Configure SNMP sur les serveurs pour la gestion du réseau.	OU : Moleculis.lan	Configuration de SNMP pour la gestion et la surveillance des serveurs.
8	<b>OpenVPN_Configuration_Deployment</b>	Déploie la configuration d'OpenVPN pour un groupe spécifique.	Groupe : OpenVPN_Group_Users	Configuration automatique d'OpenVPN pour les utilisateurs spécifiés.
9	<b>Users_Parameters_Restriction</b>	Restreint les paramètres d'utilisation pour les utilisateurs.	OU : Research, Administrative	Restriction d'accès à certains paramètres système.

#	Nom de la GPO	Description	Application sur	Paramètres principaux
10	<b>Corporate_Wallpaper</b>	Applique un fond d'écran d'entreprise sur les postes utilisateurs.	OU : Domain Groupe : Users	Application d'un fond d'écran corporatif sur tous les postes utilisateurs.
11	<b>Automatic_Network_Drive_Policy</b>	Déploie des lecteurs réseau automatiques pour le groupe des chercheurs	OU : Research Groupe : Researchers	Assignation automatique des lecteurs réseau aux chercheurs.
12	<b>Automatic_Network_Drive_Policy_Administrative</b>	Déploie des lecteurs réseau pour les employés administratifs.	OU : Administrative Groupe : Administrative_Employee	Assignation automatique des lecteurs réseau aux employés administratifs.

## 12. Partage des ressources

Concernant le partage des ressources, nous avons décidé d'utiliser un système de dossiers partagés sauvegarder sur un serveur de stockage Windows Server.

Nous recommandons d'utiliser des **RAID5** (et c'est cette méthode qui sera détaillée par la suite) qui semble le meilleur compromis au vue des avantages et inconvénients décrits ci-après.

Pour	Contre
Tolérance aux pannes	Reconstruction lente
Bonne performance en lecture	Performance d'écriture réduite
Efficacité de stockage	Vulnérabilité pendant la reconstruction
Faible coût de redondance	Nécessite au moins 3 disques
Scalable	Risque en cas de panne multiple

Le RAID5 offre de nombreux avantages pour le partage des ressources entre chercheurs, une tolérance aux pannes efficace.

### Explication du système :

Nous avons testé les GPO sur un raid5 installé sur un Windows Server 2022.

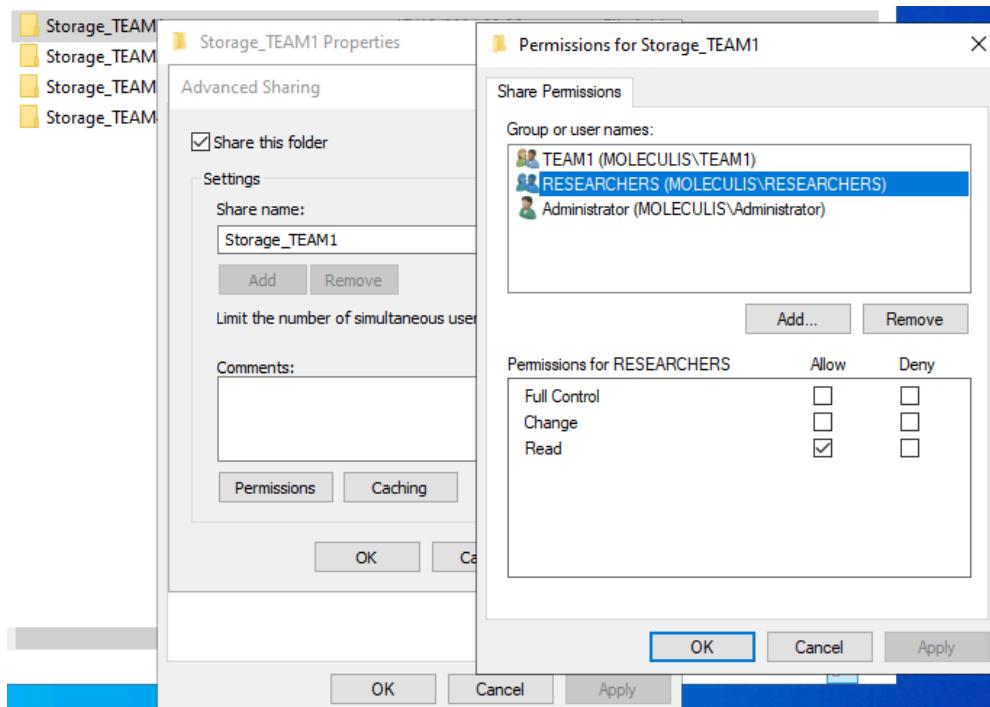
Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...)	29,37 GB	19,41 GB	66 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...)	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...)	524 MB	524 MB	100 %
New Volume (E:)	RAID-5	Dynamic	NTFS	Healthy	9,96 GB	9,93 GB	100 %
SSS_Xb4FREE_EN...	Simple	Basic	UDF	Healthy (P...)	4,70 GB	0 MB	0 %



Appliquez ensuite les **droits NTFS** sur les dossiers partagés en correspondance avec la politique que nous proposons ici.

- **Lecture (L)**
- **Écriture (E)**
- **Suppression (S)**
- **Administration (A)**

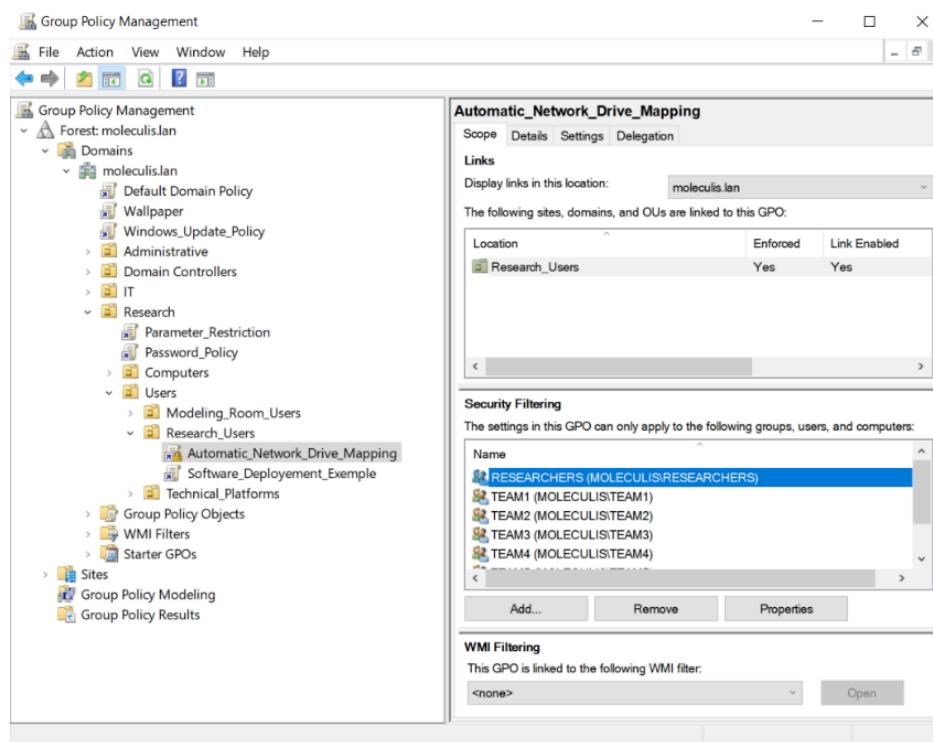
Ressource/ Utilisateur	ADMIN	RESEAR- CHERS	T1	T2	T3	T4	T5	T6	TEAM MANAGER
TEAM1_Storage	A, E	L	L, E	L	L	L	L	L	L, E
TEAM2_Storage	A, E	L	L	L, E	L	L	L	L	L, E
TEAM3_Storage	A, E	L	L	L	L, E	L	L	L	L, E
TEAM4_Storage	A, E	L	L	L	L	L, E	L	L	L, E
TEAM5_Storage	A, E	L	L	L	L	L	L, E	L	L, E
TEAM6_Storage	A, E	L	L	L	L	L	L	L, E	L, E



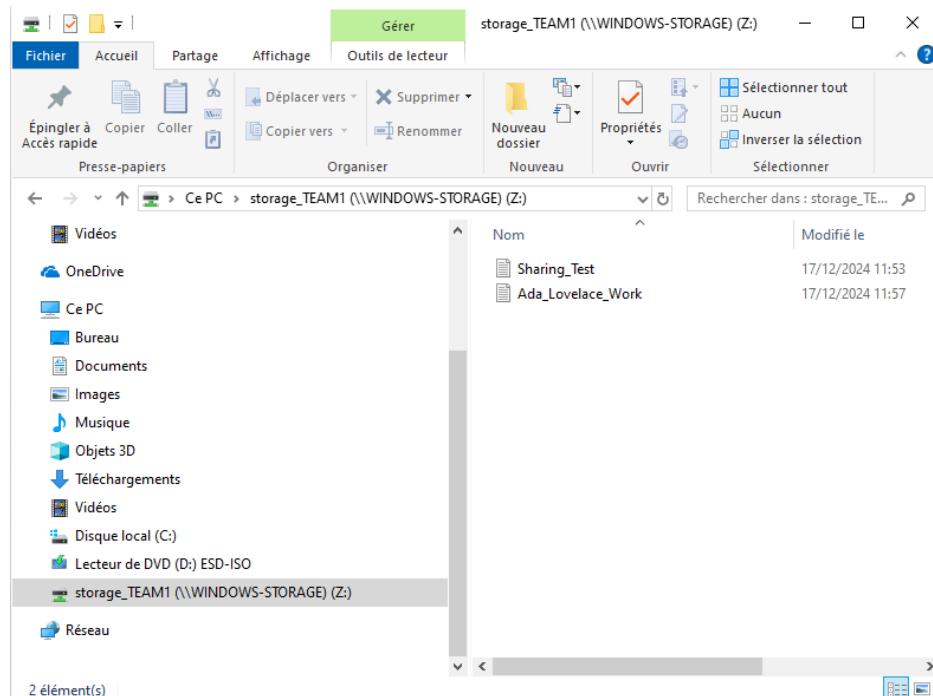
Organisez ensuite le partage des ressources via une GPO pour monter automatiquement les dossiers partagés accessibles sur les sessions des membres des groupes de recherches avec l'exécution d'un script bash au démarrage de la session.

Par exemple :

```
net use Z: \\WINDOWS-STORAGE\TEAM1_Storage /persistent:yes
```

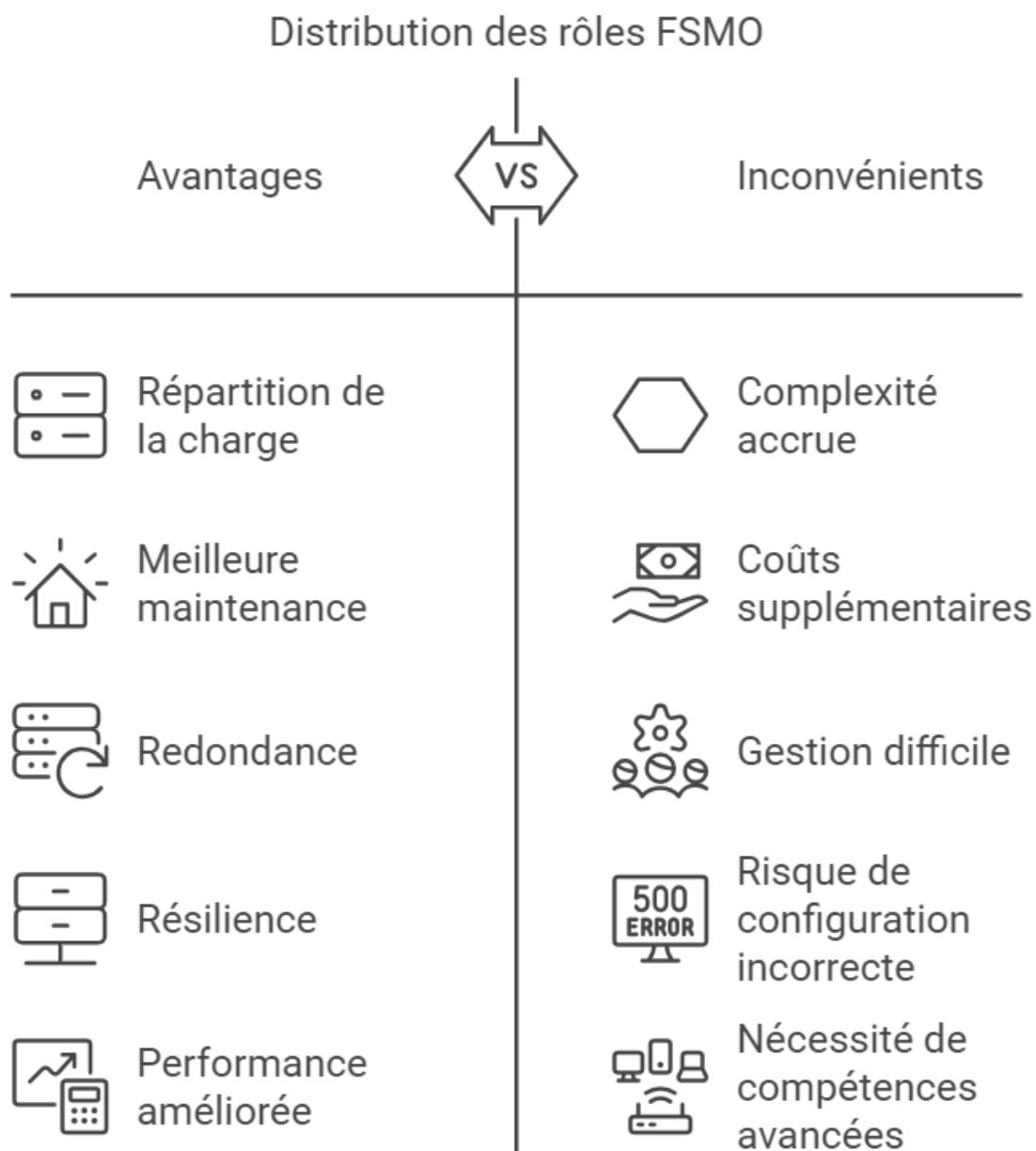


Testez ensuite la configuration en vous connectant sur le compte d'un membre de l'équipe de recherche.



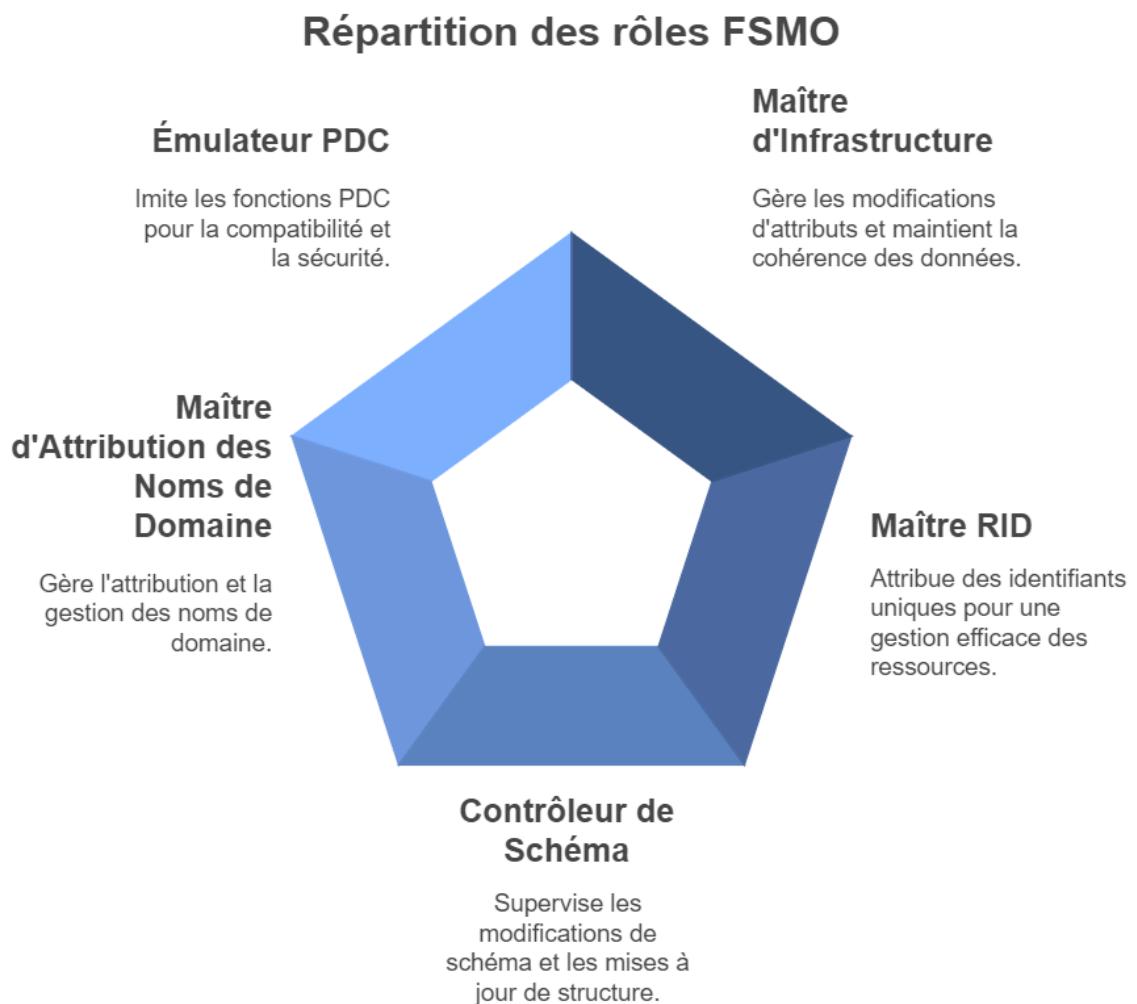
## 13. Répartition des Rôles FSMO

Nous avons précédemment configuré le **contrôleur de domaine** pour notre Active Directory. Néanmoins, une bonne pratique consiste à **répartir les rôles FSMO** sur plusieurs contrôleurs, permettant une répartition de la charge ainsi qu'une meilleure remise en service en cas de panne.



Il y a **5** rôles à répartir:

- Le Maître d'Infrastructure (Notre serveur précédemment configuré)
- Le Maître RID
- Le Contrôleur de schéma
- Le Maître d'attribution des noms de domaine
- L'Emulateur PDC



### 13.1.Préparation des machines

- Dans un premier temps, installez **4 autres serveurs Windows Core** en configurant les noms et adresses IP comme ceci:

NOM / RÔLE	ADRESSE IP
MOLECULIS-SERV (Contrôleur de domaine )	192.168.1.2/16
RID-SERV (Maître RID)	192.168.1.3/16
SCHEME-SERV (Contrôleur de schéma)	192.168.1.4/16
NAME-SERV (Maître d'attribution de noms de domaine)	192.168.1.5/16
PDC-SERV (Emulateur PDC)	192.168.1.6/16

Par exemple pour le serveur **Maître RID**:

```
c:\Administrator: C:\Windows\system32\cmd.exe
=====
          Network adapter settings
=====

NIC index:      1
Description:   Intel(R) PRO/1000 MT Desktop Adapter
IP address:    169.254.117.118,
                fe80::d153:39b4:55a6:7576
Subnet mask:   255.255.0.0
DHCP enabled: True

Default gateway:
Preferred DNS server: 10.0.2.3
Alternate DNS server:

  1) Set network adapter address
  2) Set DNS servers
  3) Clear DNS server settings

Enter selection (Blank=Cancel): 1
Select (D)HCP or (S)tatic IP address (Blank=Cancel): S
Enter static IP address (Blank=Cancel): 192.168.1.3
Enter subnet mask (Blank=255.255.255.0): 255.255.0.0
Enter default gateway (Blank=Cancel): 192.168.0.3
Setting NIC to static IP...
Successfully released DHCP lease.
Successfully enabled static addressing. DHCP for this network adapter is disabled.
Successfully set gateway.
Successfully set network adapter address.
(Press ENTER to continue):
```

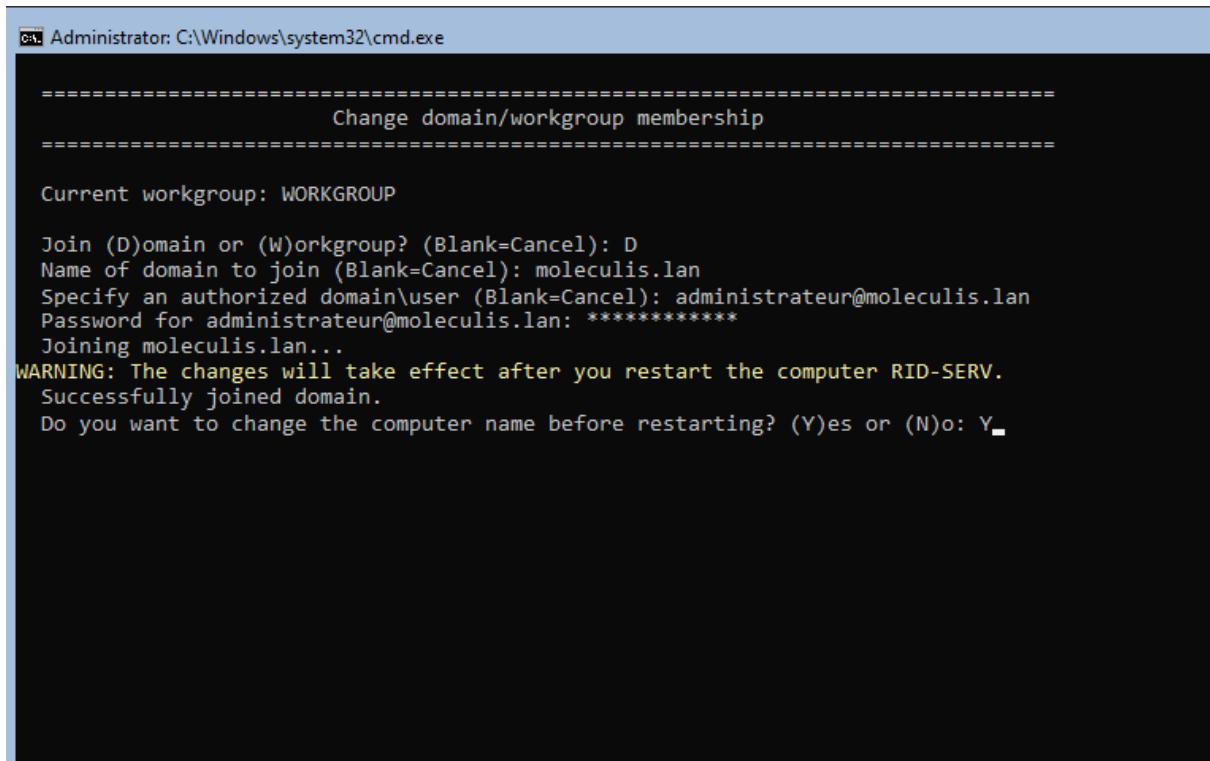
- Dans un second temps, installez les rôles Active Directory comme précédemment.  
**POINT DE VIGILANCE** : Il ne faut pas créer de nouvelle forêt!

- Ouvrez la **console PowerShell** en tapant **15**
- Tapez dans l'ordre:

```
Add-WindowsFeature -Name "RSAT-AD-Tools" -IncludeManagementTools  
-IncludeAllSubFeature
```

```
Add-WindowsFeature -Name "AD-Domain-Services"  
-IncludeManagementTools -IncludeAllSubFeature
```

- Rejoignez le domaine **moleculis.lan** en tapant **1** :



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command "netdom join" is being run to change the computer's membership from a workgroup to a domain. The user is prompted to enter the domain name, which is "moleculis.lan". They also provide a domain administrator account and password. A warning message states that changes will take effect after restarting the computer. The user then asks if they want to change the computer name before restarting, and responds with "Y".

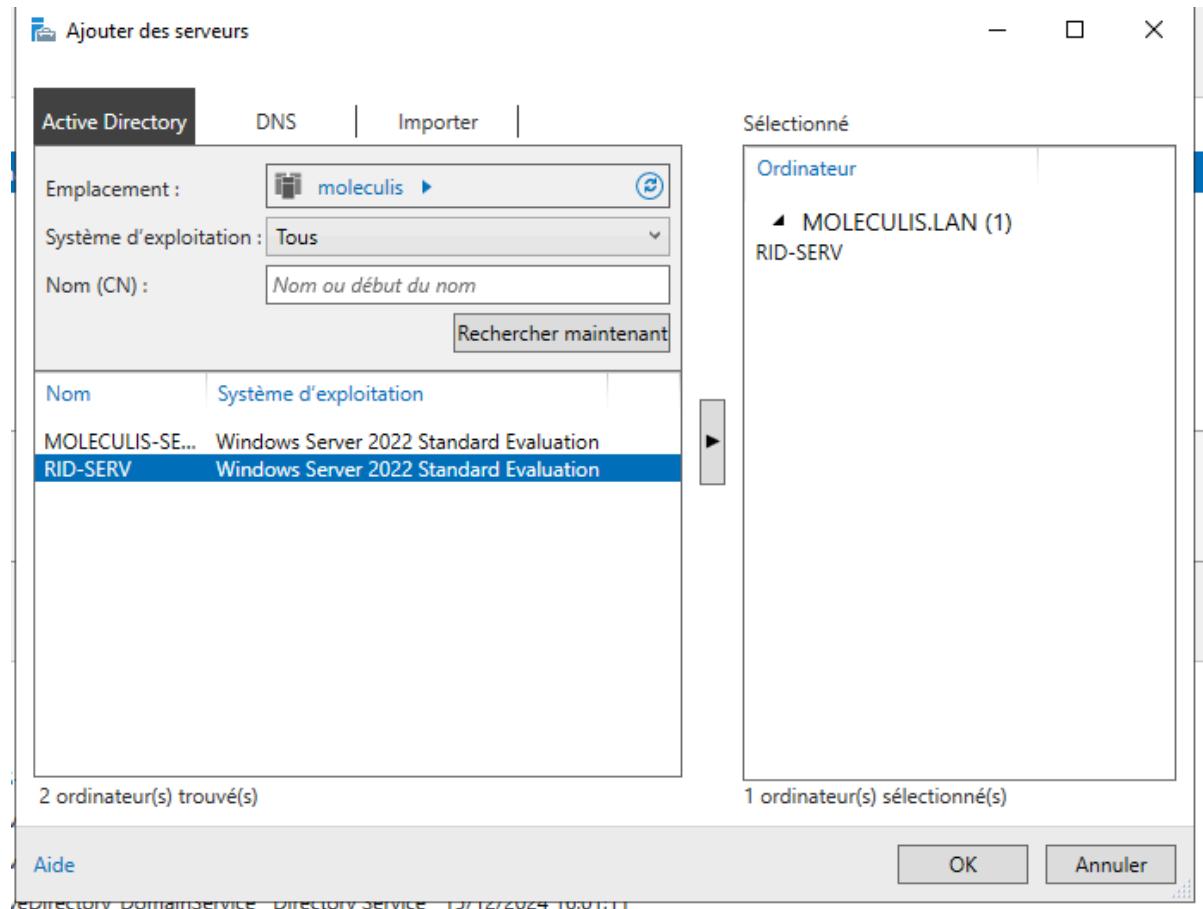
```
c:\> Administrator: C:\Windows\system32\cmd.exe
=====
          Change domain/workgroup membership
=====

Current workgroup: WORKGROUP

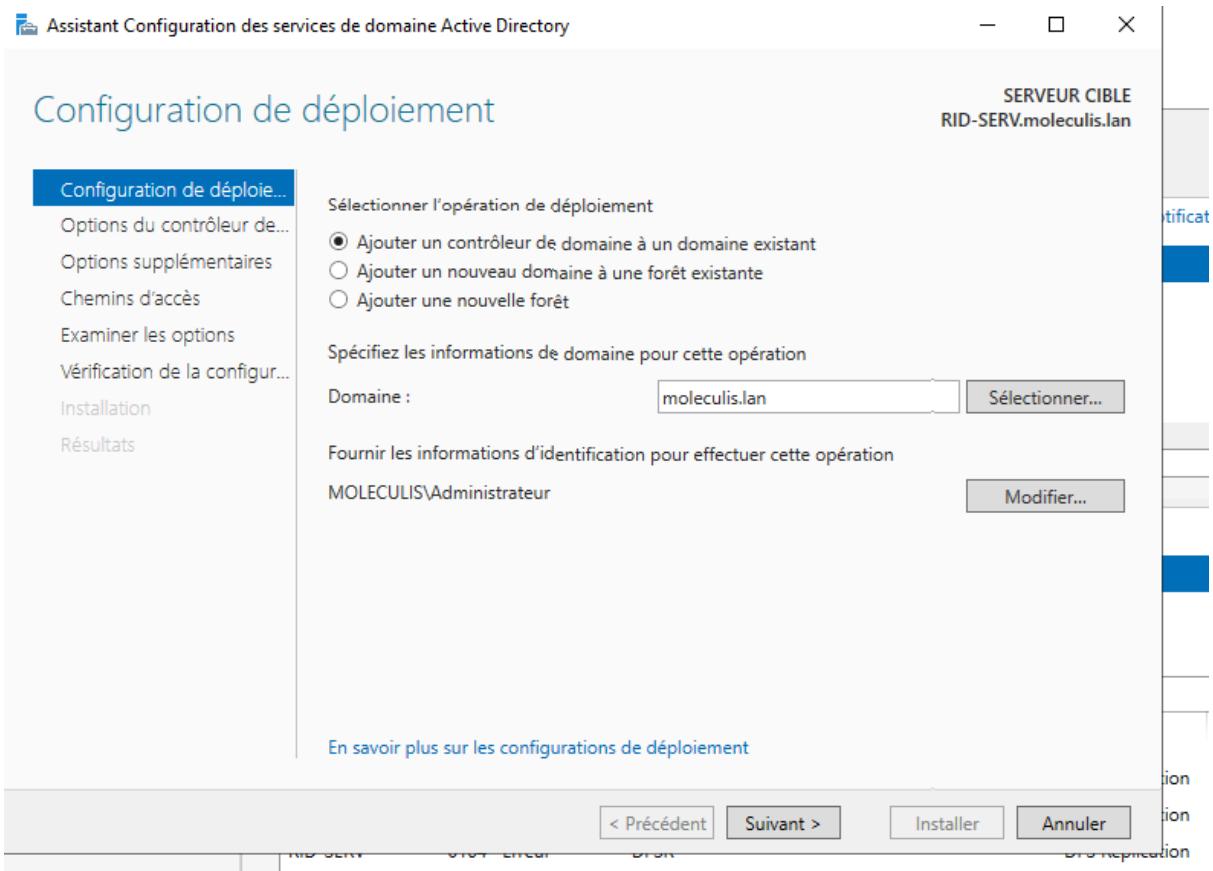
Join (D)omain or (W)orkgroup? (Blank=Cancel): D
Name of domain to join (Blank=Cancel): moleculis.lan
Specify an authorized domain\user (Blank=Cancel): administrateur@moleculis.lan
Password for administrateur@moleculis.lan: *****
Joining moleculis.lan...
WARNING: The changes will take effect after you restart the computer RID-SERV.
Successfully joined domain.
Do you want to change the computer name before restarting? (Y)es or (N)o: Y
```

- Sur le contrôleur principal, ajoutez les serveurs pour pouvoir les administrer à distance:

Cliquez sur **manage** > **add server**



- Finalisez la configuration du serveur en contrôleur de domaine



### 13.2. Répartition des rôles

- Sur le contrôleur de domaine ayant actuellement **tous les rôles**:

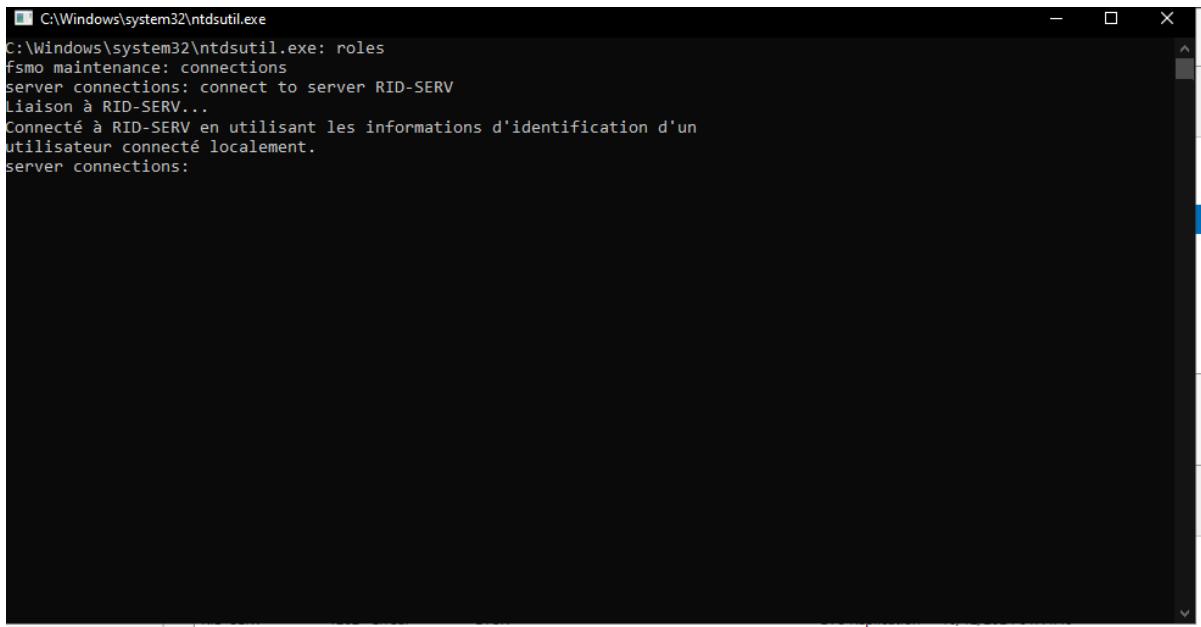
- Ouvrez un invite de commande powershell et tapez **ntdsutil.exe**.  
Un prompt va apparaître.

```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe:
```

- Tapez **Roles** pour passer en mode *maintenance FSMO*
- Passez ensuite en mode connexion avec la commande **connections**

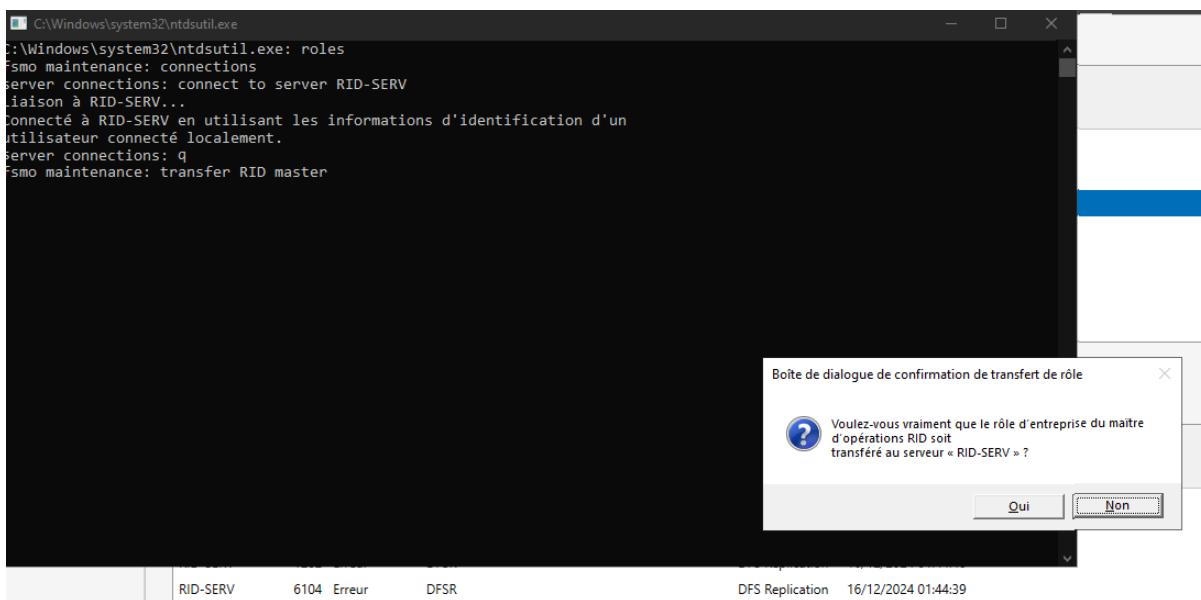
Tapzr ensuite **connect to server RID-SERV** pour vous connecter au serveur destiné à être le maître RID.

Lorsque la connexion est établie, vous pouvez taper **q** pour repasser à l'écran précédent.



```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server RID-SERV
Liaison à RID-SERV...
Connecté à RID-SERV en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections:
```

- Tapez ensuite **transfer RID master**. Confirmez lorsque la boîte de dialogue apparaît.



```
C:\Windows\system32\ntdsutil.exe
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server RID-SERV
Liaison à RID-SERV...
Connecté à RID-SERV en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections: q
fsmo maintenance: transfer RID master
```

Boîte de dialogue de confirmation de transfert de rôle

Voulez-vous vraiment que le rôle d'entreprise du maître d'opérations RID soit transféré au serveur « RID-SERV » ?

Qui      Non

RID-SERV	6104 Erreur	DFSR	DFS Replication	16/12/2024 01:44:39
----------	-------------	------	-----------------	---------------------

- Effectuez les actions pour les **autres serveurs**
  - Pour **SCHEME-SERV**, tapez `transfer schema master`
  - Pour **NAME-SERV**, tapez `transfer domain naming master`
  - Pour **PDC-SERV**, tapez `transfer pdc`
- Ensuite, quittez l'utilitaire en tapant `q` jusqu'à ce que la fenêtre se ferme.
- Enfin, vérifiez la configuration en tapant la commande PowerShell:

```
NETDOM QUERY /Domain:moleculis.lan FSMO
```

Les rôles vont s'afficher avec les serveurs correspondants.

# V - PARE-FEU

## 1. Objectifs du pare-feu

Un **pare-feu** est un dispositif de sécurité réseau, matériel ou logiciel, qui va contrôler et réguler le trafic entre les différentes zones du système.

Il répond à plusieurs objectifs :

### 1. Protection contre les menaces externes

- Les tentatives d'intrusion (piratage).
- Les logiciels malveillants comme les virus et les ransomwares.

### 2. Contrôle du trafic réseau

- Filtrer les paquets de données pour autoriser uniquement ceux conformes aux règles établies.
- Bloquer des applications ou des sites non autorisés.

### 3. Prévention des accès non autorisés par application de filtrages sur :

- Les zones sources ou de destination
- L'adresse IP
- Les utilisateurs locaux et/ou authentifié par l'AD
- Les ports utilisés
- Les protocoles

### 4. Surveillance et journalisation

- Identifier les menaces potentielles.
- Auditer et analyser les événements réseau.

### 5. Renforcement des politiques de sécurité

## 2. Choix de pfSense

Dans un souci de réduire les coûts liés à l'achat d'une licence, il a été décidé d'utiliser un pare-feu gratuit et open-source. Ces pare-feu représentent tout de même une solution fiable et sécurisée et possédant, pour les plus emblématiques, une large communauté, ils bénéficient d'un support important ainsi que d'une documentation riche permettant des supports techniques variés.

Dans notre réflexion concernant la solution à utiliser, en lien avec les connaissances de l'équipe, notre choix s'est arrêté sur deux candidats potentiels, IPFire et pfSense.

Critère	pfSense	IPFire
Type de licence	Gratuit (communauté) ou payant via Netgate	Gratuit, open source
Support commercial	Disponible via Netgate (plans de support variés)	Non, uniquement via la communauté
Interface utilisateur	Intuitive, riche et moderne	Plus simple mais moins intuitive
Fonctionnalités VPN	OpenVPN, IPsec, WireGuard	OpenVPN, IPsec
Fonctionnalités avancées	IDS/IPS (Snort/Suricata), QoS, Load Balancing	IDS/IPS (via add-ons), QoS basique
Personnalisation	Très modulable (packages : Snort, Squid, etc.)	Modulable mais moins riche en extensions
Performance	Optimisée pour les environnements complexes	Adaptée aux environnements modestes
Communauté	Large communauté et documentation détaillée	Communauté plus restreinte
Cas d'usage	Convient aux PME, grandes entreprises et filiales	Principalement PME et environnements simples
Matériel recommandé	Large compatibilité, options Netgate optimisées	Compatibilité limitée à certains matériels
Gestion centralisée	Disponible (via outils tiers ou Netgate)	Non

**pfSense** se distingue par sa flexibilité, ses fonctionnalités avancées, et son adaptabilité à des environnements variés, y compris ceux nécessitant un support commercial.

**IPFire** est en revanche plus adaptée aux petites entreprises ou aux besoins modestes. Il manque de certaines fonctionnalités clés et d'un support dédié, nous avons donc décidé, pour des raisons d'évolutivité et de maintenance, d'écartier cette solution. Le pare-feu pfSense a donc été retenu pour assurer la sécurité du réseau.

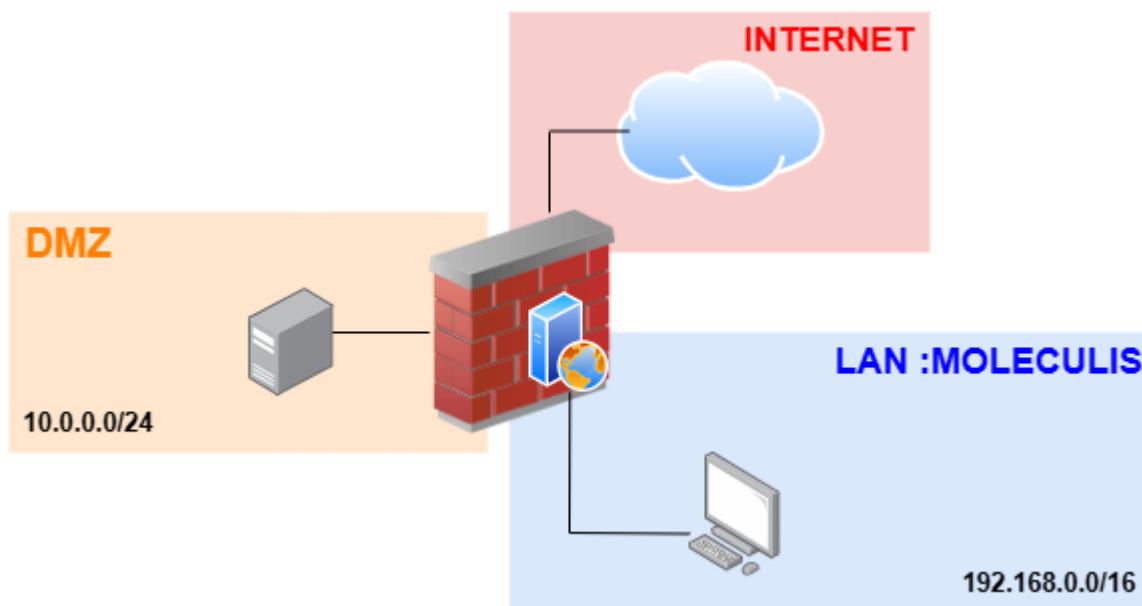
**La solution pfSense a donc été retenue** et nous vous proposons ici les détails de son installation et de sa configuration.

### 3. Prérequis matériels

Les prérequis matériels suivants sont adaptés à un réseau de 900 employés et 100 usagers en remote lors d'un pic de trafic.

Composant	Exigence Minimale	Recommandation
<b>CPU</b>	Multi-cœurs modernes (Intel Xeon/i7 ou AMD Ryzen)	4 cœurs minimum, 8 cœurs ou plus pour de meilleures performances
<b>RAM</b>	8 Go	16 Go ou plus pour un grand nombre de connexions simultanées
<b>Stockage</b>	SSD de 120 Go minimum	SSD de 240 Go ou plus pour plus d'espace et de vitesse
<b>Interface Réseau</b>	2 interfaces réseau (1 pour LAN, 1 pour WAN)	Interfaces Gigabit Ethernet ou 10 GbE si trafic élevé
<b>Bandé passante</b>	Dépend de la connexion Internet disponible	1 Gbps minimum pour gérer 100 employés distants

## 4. Organisation globale du pare-feu



### Interfaces du pare-feu :

WAN (Internet) : Zone externe non sécurisée. Le trafic entrant est strictement limité aux services publics en DMZ (serveurs web, serveurs de messagerie).

DMZ (Demilitarized Zone) : Contient des serveurs exposés (web, email). La communication avec le LAN est bloquée et strictement réglementée pour un accès admin pour éviter des attaques latérales.

LAN (Réseau interne) : Zone sécurisée pour les employés du laboratoire et les données sensibles. Les connexions vers la DMZ et le WAN sont limitées aux besoins spécifiques.

## 5. Installation du pare-feu

Nous allons dans un premier temps détailler l'installation de pfSense sur une machine qui doit initialement, au minimum, posséder deux interfaces réseaux.

Nous verrons ensuite, en accédant à la webUI de pfSense, les configurations minimales à effectuer via l'agent d'installation.

Tout d'abord récupérer une **image** de pfSense sur disponible aux liens suivants :

[Site officiel](#)

[Site d'archive](#)

L'agent d'installation de pfSense analyse la configuration matérielle de la machine hôte au démarrage.

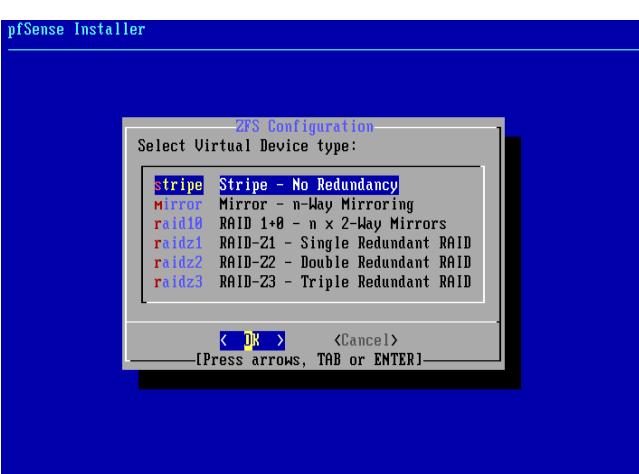
Une fois l'analyse matérielle terminée, l'assistant d'installation vous guidera pour les premières étapes. Acceptez les termes du contrat d'utilisation en appuyant sur **Entrée**.



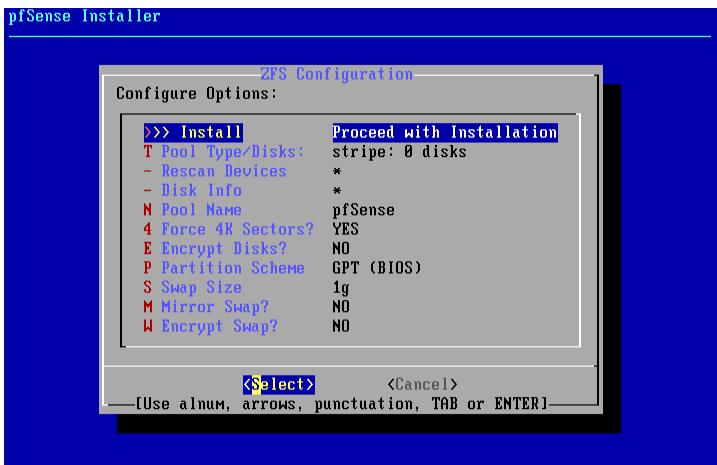
Sélectionnez "Install pfSense" et faites Entrée.



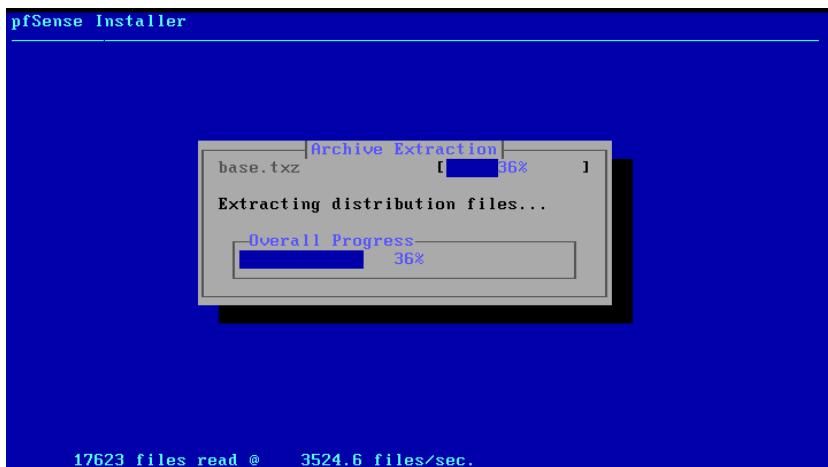
Concernant le mode de partitionnement, nous utiliserons le mode automatique (**Auto-ZFS**).



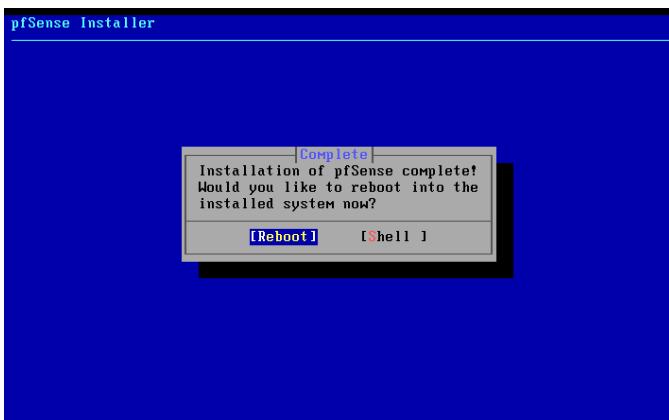
Valider ensuite le partitionnement sans redondance.



Valider ensuite les options définies ultérieurement.



Le pare-feu pfSense va maintenant s'installer.



A la fin de l'installation, exécutez un redémarrage.

Comme on peut le voir, la configuration IP de l'interface WAN a été attribuée par le serveur DHCP du réseau WAN.

Nous allons en revanche configurer l'interface LAN avec sa configuration IP adéquate avant de poursuivre les configurations via l'interface web.

Choisissez l'**option 2**.

Selectionnez l'interface LAN en entrant l'option 2 et ne pas autoriser l'adressage DHCP.

Définissez la configuration IP de l'interface statiquement: **192.168.0.1/16**

Ne pas définir de passerelle ni de configuration IPV4.

Ne pas définir également de serveur DHCP, ce rôle étant dévolue dans le LAN à l'Active directory.

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: da756c837e93aaaf6135

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

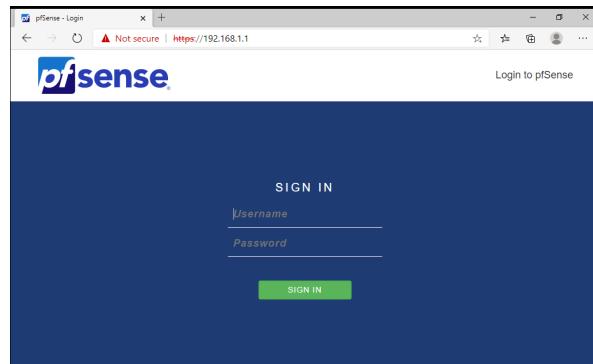
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.128.96/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Connectez-vous maintenant sur un poste dans le même réseau que l'interface LAN de pfSense afin d'accéder à l'interface WEB pour continuer la configuration.

## 6. Configuration initiale via l'interface Web



Connectez-vous avec l'admin local prédéfini de pfSense -> **Admin** (password : pfsense)

L'agent d'installation va permettre la configuration des premiers éléments du pare-feu.

Définissez le nom de l'host : **pfSense**

Modifiez le nom de domaine : **moleculis.lan**

Définissez le DNS primaire : **192.168.1.2** (Serveur Active Directory)

Définissez le DNS secondaire : **localhost**

Step 2 of 9

### General Information

On this screen the general pfSense parameters will be set.

<b>Hostname</b>	pfSense	Name of the firewall host, without domain part.
<b>Domain</b>	home.arpa	Domain name for the firewall.
Examples: pfsense, firewall, edgefw		
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.		
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.		
<b>Primary DNS Server</b>	192.168.1.2	
<b>Secondary DNS Server</b>	127.0.0.1	
<b>Override DNS</b>	<input checked="" type="checkbox"/>	Allow DNS servers to be overridden by DHCP/PPP on WAN

### RFC1918 Networks

**Block RFC1918 Private Networks**  Block private networks from entering via WAN  
 When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

### Block bogon networks

**Block bogon networks**  Block non-Internet routed networks from entering via WAN  
 When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

**>> Next**

Décochez le blocage des IP publiques via le WAN

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

### Configure LAN Interface

On this screen the Local Area Network information will be configured.

<b>LAN IP Address</b>	192.168.0.1	Type dhcp if this interface uses DHCP to obtain its IP address.
<b>Subnet Mask</b>	16	

**>> Next**

Configurez l'interface LAN de pfSense

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

### Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

<b>Admin Password</b>	.....
<b>Admin Password AGAIN</b>	..... 

**>> Next**

Modifiez le mot de passe par défaut du compte **admin**.

Relancez enfin pfSense pour effectuer les changements apportés précédemment.  
**La configuration initiale de pfSense est maintenant terminée.**

The screenshot shows the pfSense Status / Dashboard interface. On the left, the "System Information" section displays details such as Name (pfSense.home.arpa), User (admin@192.168.0.2), System (VMware Virtual Machine, Netgate Device ID: da756c837e93aaf6135), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020), and Version (2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023). It also indicates that the system is on the latest version and provides a timestamp for the version update. On the right, the "Interfaces" section lists two interfaces: WAN (1000baseT <full-duplex>, IP 192.168.128.96) and LAN (1000baseT <full-duplex>, IP 192.168.0.1).

## 7. Configuration de la DMZ

Pour les besoins du déploiement d'un serveur web, la demande de l'installation d'une zone démilitarisée a été formulée.

Elle va permettre de créer une **zone de partage accessible par internet**, contrôlée par le pare-feu et **isolée du réseau interne** qui doit rester sécurisée afin de protéger les données sensibles.

Des filtrages vont pouvoir être appliqués spécifiquement sur cette DMZ afin de réduire la surface d'attaque et organiser la gestion des accès et des flux autorisés ou non à y accéder.

### 7.1. Création de la DMZ via la Web UI

Dans cette partie nous allons créer l'interface DMZ sur une troisième interface réseau, définir des règles de filtrages associés à des tests vers un serveur web Nginx installé sur une distribution Ubuntu en 10.0.0.10/24

The screenshot shows the pfSense Interfaces / DMZ (em2) configuration page. Under the "General Configuration" tab, the "Enable" checkbox is checked. The "Description" field is set to "DMZ" with the note "Enter a description (name) for the interface here." The "IPv4 Configuration Type" is set to "Static IPv4" and the "IPv6 Configuration Type" is set to "None".

## 7.2. Définition des règles de filtrage associées à la DMZ

Configurer les règles de filtrage associées à la DMZ, dans **Firewall -> Rules**

Pour une explication plus approfondie, se référer à **Création d'une règle de filtrage** vue précédemment.

Tout d'abord, interdire tous les accès externes vers la DMZ, pour ensuite autoriser, de manière précise, les clients et les protocoles autorisés.

### Règle : Accès du WAN vers la DMZ

**Source** : Any

**Destination** : DMZ subnet

**Protocole** : TCP

**Port** : 8080

**Action** : Passer

**Description** : Autoriser l'accès HTTP à la DMZ pour le serveur NGINX

Composant	Valeur
Source	Any
Destination	DMZ Subnet
Protocole	Any
Action	Bloquer
Interface	DMZ (ou l'interface associée à la DMZ)
Destination Port Range	Any

### Résultat dans la Web UI

 0/135 IPv4 TCP \* \* 10.0.0.10 8080 \* none NAT Redirection from WAN to Web-Server    

Nous allons ensuite autoriser l'accès provenant du WAN vers la DMZ. Pour cela nous allons également établir une redirection de port de l'interface extérieure vers le serveur web.

#### Redirection : port 8080 de l'interface WAN vers la DMZ

Configurez la redirection, dans **Firewall -> NAT -> Port Forward**

Sélectionnez l'interface WAN et choisir le protocol IPv4

Choisir comme destination l'adresse de l'interface WAN sur le port 8080 et choisir de rediriger la requête sur l'adresse du serveur web (10.0.0.10).

Composant	Valeur
Source	WAN Subnet
Destination	WAN Address (interface du pare-feu)
Protocole	ipv4 TCP
Action	Autoriser
Interface	DMZ
Destination Port Range	8080

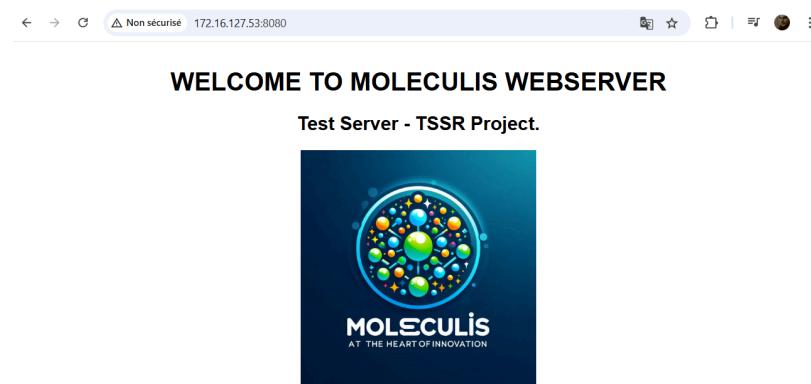
#### Résultat dans la WEB UI

0/135 IPv4 TCP \* \* 10.0.0.10 8080 \* none NAT Redirection from WAN to Web-Server     

#### TEST ASSOCIÉ

Connectez-vous depuis un poste distant sur le serveur web de test installé dans la DMZ en utilisant : [http://<ip\\_serveur\\_nginx>:8080](http://<ip_serveur_nginx>:8080) afin de confirmer son accessibilité et la redirection.

**Résultat : Le poste du wan se connecte bien au serveur web. Il n'est en revanche pas accessible par un autre port ou un autre protocole.**

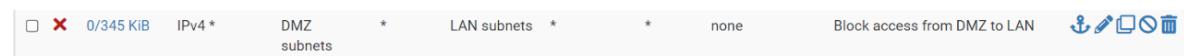


### Règle : accès du LAN vers la DMZ

Objectif: Autoriser SSH du LAN vers la DMZ pour l'administration

Composant	Valeur
Source	Adresse Host Admin
Destination	DMZ subnet
Protocole	TCP
Action	Passer
Interface	DMZ
Destination Port Range	22

### Résultat dans la WEB UI



### Test associé: Tester la connectivité entre un host du LAN et la DMZ

Ping 10.0.0.10 / curl 10.0.0.10 / connexion via un navigateur en http etc..

### Résultat : Il n'est pas possible d'accéder à des host dans la DMZ

```
PS C:\Users\Administrator> ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

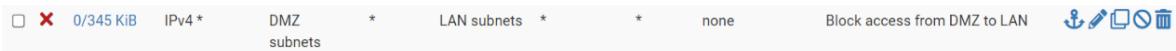
Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
```

Règle : accès de la DMZ vers le LAN

**Objectif:** Bloquer l'accès de la DMZ vers le LAN

Composant	Valeur
Source	DMZ subnet
Destination	LAN subnet
Protocole	TCP
Action	Bloquer
Interface	DMZ
Destination Port Range	Any

#### Résultat dans la WEB UI



0/345 KiB IPv4 \* DMZ subnets \* LAN subnets \* \* none Block access from DMZ to LAN

**Test associé:** Tester la connectivité à partir d'un host de la DMZ vers le LAN

Ping 192.168.1.2

**Résultat : Il n'est pas possible d'accéder au LAN via la DMZ**

```
gwen@gwen-VMware-Virtual-Platform:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
48 packets transmitted, 0 received, 100% packet loss, time 48127ms

gwen@gwen-VMware-Virtual-Platform:~$
```

## 8.Délégation de l'authentification par Active Directory

Il va nous falloir, pour commencer, générer un certificat. La génération de certificat est détaillée dans la partie **Active Directory -> Configuration de l'autorité de certificat -> Génération d'un certificat** et créer un certificat de type Service pour l'utilisateur-service pfSense créé dans l'Active Directory.

Une fois le certificat généré, retournez maintenant dans l'interface web de pfSense.  
Le certificat créé va permettre le chiffrement des requêtes LDAP entre pfSense et le serveur Active Directory.  
Pour cela allez dans **System->User Manager->Authentication Server** et créez

**LDAP Server Settings**

<u>Hostname or IP address</u>	MOLECULIS-SERV.moleculis.lan
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.	
<u>Port value</u>	636
<u>Transport</u>	SSL/TLS Encrypted
<u>Peer Certificate Authority</u>	ADCS
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.	
<u>Protocol version</u>	3
<u>Server Timeout</u>	25
Timeout for LDAP operations (seconds)	
<u>Search scope</u>	Level Entire Subtree
<u>Base DN</u> DC=moleculis,DC=lan	
<u>Authentication containers</u>	OU=OpenVPN,OU=IT,DC=moleculis,DC=lan;OU=pfSense,OU=IT,DC=moleculis,DC=lan
<input type="button" value="Select a container"/>	
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers	

Définir l'utilisateur-service pfSense créé dans dans l'Active Directory, ainsi que son mot de passe, pour effectuer la connexion initiale avec l'annuaire LDAP.

<u>Extended query</u>	<input type="checkbox"/> Enable extended query
<u>Bind anonymous</u>	<input type="checkbox"/> Use anonymous binds to resolve distinguished names
<u>Bind credentials</u>	CN=pfSense,OU=pfSense,OU=IT,DC=moleculis,DC=lan *****
<u>User naming attribute</u>	samAccountName
<u>Group naming attribute</u>	cn
<u>Group member attribute</u>	memberOf

Dans la partie conteneur, sélectionnez **le scope d'OU** dans lequel l'utilisateur-service pfSense effectuer ses correspondances.

- OU=Meeting\_Room,OU=Users,OU=Administrative,DC=moleculis,DC=lan
- OU=Meeting\_Room\_Computers,OU=Computers,OU=Administrative,DC=moleculis,DC=lan
- OU=Modeling\_Room,OU=Computers,OU=Research,DC=moleculis,DC=lan
- OU=Modeling\_Room\_Users,OU=Users,OU=Research,DC=moleculis,DC=lan
- OU=Network\_Services,OU=IT,DC=moleculis,DC=lan
- OU=OpenVPN,OU=IT,DC=moleculis,DC=lan
- OU=OpenVPN,OU=Network\_Services,OU=IT,DC=moleculis,DC=lan
- OU=pfSense,OU=IT,DC=moleculis,DC=lan
- OU=Reception,OU=Users,OU=Administrative,DC=moleculis,DC=lan
- OU=Reception\_Computers,OU=Computers,OU=Administrative,DC=moleculis,DC=lan
- OU=Research,DC=moleculis,DC=lan
- OU=Research\_Computers,OU=Computers,OU=Research,DC=moleculis,DC=lan
- OU=Research\_Users,OU=Users,OU=Research,DC=moleculis,DC=lan

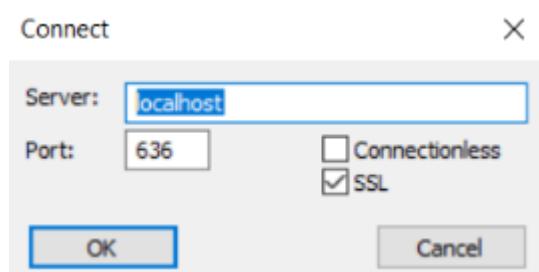
Le serveur d'authentification LDAP est maintenant créé.

The screenshot shows the pfSense User Manager Authentication Servers page. The navigation bar at the top includes links for System, User Manager, and Authentication Servers. The Authentication Servers tab is selected, indicated by a red underline. Below the tabs is a table titled "Authentication Servers" with the following data:

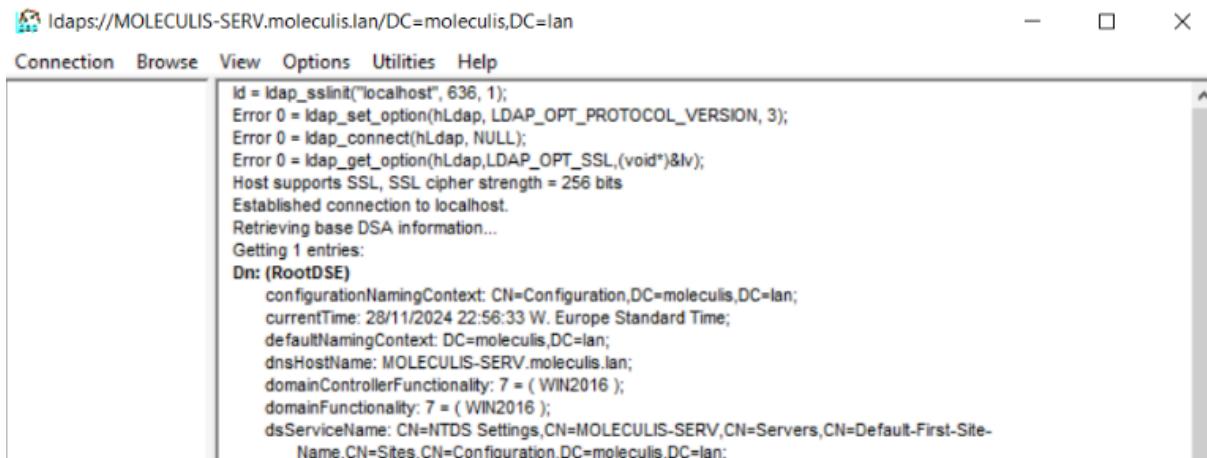
Server Name	Type	Host Name	Actions
DC-Moleculis.lan	LDAP	192.168.1.2	
Local Database		pfSense	

A green "Add" button with a plus sign is located at the bottom right of the table area.

Pour vérifier l'effectivité du chiffrement TLS, il est possible d'utiliser **ldp.exe** sur le serveur Active Directory. Sélectionnez le port 636 SSL.

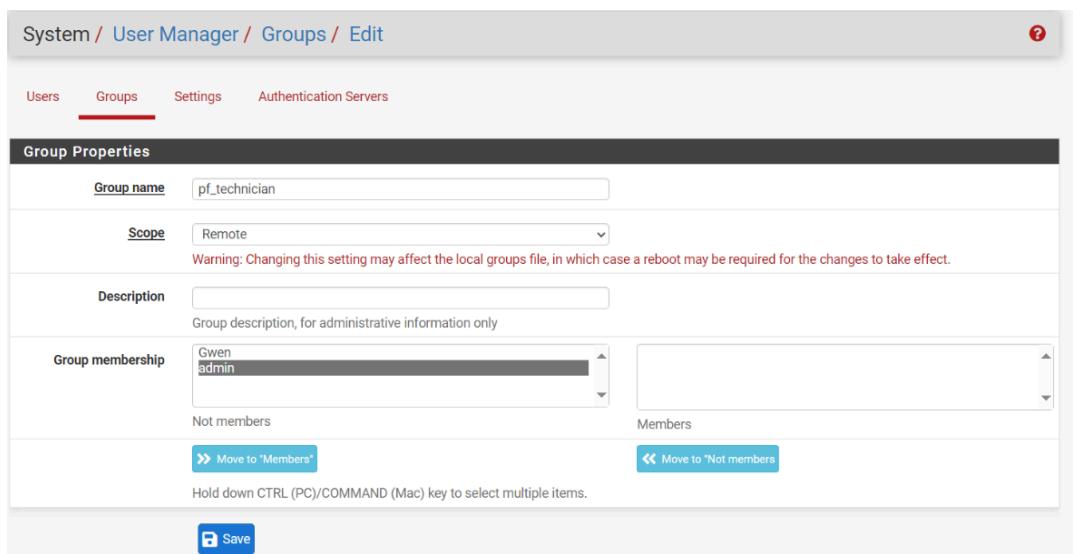


Si les configurations sont correctes, l'exécution du programme ne doit pas renvoyer d'erreurs.



```
Idaps://MOLECULIS-SERV.moleculis.lan/DC=moleculis,DC=lan
Connection  Browse  View  Options  Utilities  Help
Id = ldap_sslinit("localhost", 636, 1);
Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
Host supports SSL, SSL cipher strength = 256 bits
Established connection to localhost.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
configurationNamingContext: CN=Configuration,DC=moleculis,DC=lan;
currentTime: 28/11/2024 22:56:33 W. Europe Standard Time;
defaultNamingContext: DC=moleculis,DC=lan;
dnsHostName: MOLECULIS-SERV.moleculis.lan;
domainControllerFunctionality: 7 = ( WIN2016 );
domainFunctionality: 7 = ( WIN2016 );
dsServiceName: CN=NTDS Settings,CN=MOLECULIS-SERV,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=moleculis,DC=lan;
```

Il est bien entendu aussi possible d'analyser les requêtes et les réponses entre l'AD et le pare-feu avec **Wireshark** et s'assurer que le protocole TLS est bien utilisé.



The screenshot shows the 'Group Properties' page for a group named 'pf\_technician'. The 'Groups' tab is selected in the navigation bar. The 'Scope' is set to 'Remote'. The 'Group membership' section lists members 'Gwen' and 'admin' under the 'Not members' list. A note at the bottom says: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.' A 'Save' button is at the bottom.

Nous allons maintenant créer des groupes locaux dont le nom doit être **identique** à ceux présents dans le serveur LDAP (ici l'Active Directory) pour que pfSense puisse les associer à ces derniers. Nous voyons ici qu'ils ne contiennent aucun membres locaux et il ne sera pas nécessaire d'en créer, la gestion des utilisateurs étant dorénavant déléguée à l'Active Directory.

The screenshot shows the 'Groups' section of the User Manager. The table has columns for Group name, Description, Member Count, and Actions. The actions column contains icons for edit, copy, and delete. A green 'Add' button is at the bottom right.

Groups			
Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	2	
pf_administrator		0	
pf_technician		0	

La création locale de ses groupes va en revanche permettre de définir **des politiques de restrictions locales propres** à ces groupes.

Nous pouvons par exemple donner des droits globaux aux administrateurs mais restreindre les droits uniquement à l'écriture aux techniciens réseaux.

The screenshot shows the 'Group Privileges' page for the 'pf\_administrator' group. A dropdown menu titled 'Assigned privileges' is open, listing various WebCfg and Diagnostics options. A note at the bottom says 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'

- WebCfg - AJAX: Get Queue Stats
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages**
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access).
- WebCfg - Diagnostics: ARP Table
- WebCfg - Diagnostics: Authentication
- WebCfg - Diagnostics: Backup & Restore
- WebCfg - Diagnostics: Command
- WebCfg - Diagnostics: Configuration History
- WebCfg - Diagnostics: CPU Utilization
- WebCfg - Diagnostics: DNS Lookup
- WebCfg - Diagnostics: Edit File
- WebCfg - Diagnostics: Factory defaults
- WebCfg - Diagnostics: GEOM Mirrors
- WebCfg - Diagnostics: Halt system
- WebCfg - Diagnostics: Interface Traffic
- WebCfg - Diagnostics: Limiter Info

Ici le groupe des techniciens n'a accès qu'au dashboard, aux diagnostics ping/traceroute et la lecture des graphiques et des logs.

Assigned Privileges		
Name	Description	Action
WebCfg - Dashboard (all)	Allow access to all pages required for the dashboard.	
WebCfg - Diagnostics: Ping	Allow access to the 'Diagnostics: Ping' page.	
WebCfg - Diagnostics: Traceroute	Allow access to the 'Diagnostics: Traceroute' page.	
WebCfg - Status: Traffic Graph	Allow access to the 'Status: Traffic Graph' page.	
WebCfg - Status: Logs: Firewall	Allow access to the 'Status: Logs: Firewall' page.	
WebCfg - Status: Logs: Settings	Allow access to the 'Status: Logs: Settings' page.	

+ Add

Dans l'Active Directory nous il va nous falloir créer des utilisateurs associés aux groupes locaux de pfSense. L'Active Directory, via une requête LDAP initiée par utilisateur-service pfSense, va authentifier le mot de passe lors de la connexion au pare-feu et permettre la lecture du scope défini.

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the tree structure of the domain: Active Directory Users and Computers [MOLE], moleculis.lan, Administrative, Computers, Domain Controllers, ForeignSecurityPrincipals, IT, Managed Service Accounts, Research, and Users. Under the 'IT' folder, there is a 'pfSense' folder which is currently selected. On the right, a list view shows the following users and groups:

Name	Type	Description
pf_admin	User	
pf_administrator	Security Group ..	
pf_tech	User	
pf_technician	Security Group ..	
pfsense	User	

Il sera par ailleurs aussi possible d'appliquer des GPO sur ces utilisateurs dans le domaine MOLECULIS.

En revanche l'Active Directory ne pourra pas appliquer de GPO pour des actions internes au pare-feu. Les groupes locaux de pfSense pallient cette faiblesse, le pare-feu n'étant pas membre du domaine MOLECULIS.

## 9.Règles de filtrage

### 9.1.Politique de filtrage

La **politique de filtrage** dans une entreprise est un cadre destiné à réguler et contrôler l'accès aux ressources et services du réseau informatique de l'entreprise, notamment l'accès à Internet, les services, les sites web et les protocoles.

La politique générale est de bloquer tous les accès et ensuite appliquer, en fonction des sources, des destinations, des protocoles et des ports, différentes autorisations pour des utilisations précises. Cela va permettre de filtrer et contrôler de façon fine et sécurisée les différents flux qui traversent les différentes zones du système.

Le pare-feu pfSense permet de configurer les politiques de filtrage de façon simple et ordonnée via sa web UI.

Rules (Drag to Change Order)											
□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓ 0/0 B	IPv4 TCP	192.168.1.2	22 (SSH)	DMZ subnets	22 (SSH)	*	none		SSH access from admin host to DMZ	
□	✗ 0/0 B	IPv4 TCP	*	*	WAN subnets	*	*	none		Block access from DMZ to Internet	
□	✗ 0/185 KiB	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Block access from DMZ to LAN	
□	✓ 0/10 KiB	IPv4 TCP/UDP	DMZ subnets	*	*	53 (DNS)	*	none		DNS Resolution from DMZ	
□	✓ 0/57.31 MiB	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	none		Access from DMZ to WAN (443)	
□	✓ 0/3 KiB	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none		Access from DMZ to WAN (80)	

Buttons at the bottom: Add, Add, Delete, Toggle, Copy, Save, Separator.

Par défaut, il autorise tous les flux sortant du LAN et interdit tous les flux provenant du LAN. Nous allons voir comment appliquer une règle de filtrage dans la rubrique suivante.

### 9.2.Création d'une règle de filtrage

Dans le panneau de configuration de la web UI de pfSense, allez dans Firewall puis Rules. Pour effectuer un filtrage, différents éléments sont essentiels à définir:

#### 1- L'interface :

C'est généralement l'interface réseau sur laquelle le filtrage va être effectué. Cela peut aussi être un service (par exemple le serveur VPN comme vu dans la partie OpenVPN de ce dossier).

#### 2- La source et la destination

Cela peut être une IP, un réseau, une zone ou même une interface.

#### 3- Le protocole et le port

Permet d'affiner le filtrage selon la nature des paquets transmis.

### 9.3. Politique de filtrage du pare-feu

Source	Destination	Port/Protocole	Action	Commentaires
Global	Tous	Tous	✗	Politique par défaut
WAN	DMZ	Tous	✗	Bloquer le trafic entrant
WAN	LAN	Tous	✗	Bloquer le trafic entrant vers le LAN.
WAN	10.0.0.10	HTTP (80), HTTPS (443)	✓	Exception serveur Web
WAN	WAN address	UDP (4050)	✓	Accès WAN vers le serveur OpenVPN
OpenVPN	LAN	Tous	✓	Accès OpenVPN vers le LAN
DMZ	WAN	HTTP (80), HTTPS (443)	✓	Autoriser les connexions sortantes des serveurs.
DMZ	LAN	Tous	✗	Interdire les connexions directes vers le LAN.
LAN	LAN Adress (Interface du pare-feu)	SSH (22), HTTPS(443)	✓	Accès admin à la console et à la Web UI
LAN (Poste ou utilisateur admin)	DMZ	SSH (22)	✓	Restreindre aux admins.
LAN	WAN	DNS (53)	✓	Permettre les résolutions DNS
Interne	Pare-feu	SSH (22), HTTPS (443)	✓	Autoriser uniquement les administrateurs.

# VI - VIRTUAL PRIVATE NETWORK

## 1. Objectifs de l'accès VPN

La configuration de l'accès VPN répond à la nécessité pour les employés en remote de bénéficier des avantages et des ressources de l'intranet du laboratoire tout en maintenant la sécurité de l'intranet.

Il répond à des objectifs multiples qui sont :

1. **La sécurisation des communications** : le chiffrement des flux entre les employés en remote et le serveur VPN afin de se prémunir contre l'interception et les attaques de type "man-in-the-middle".
2. **La flexibilité** : il permet aux employés du laboratoire ainsi que les clients autorisés à accéder de n'importe où aux ressources du laboratoire. Il apporte aussi une solution permettant la continuité de nombreux services en cas de circonstances graves (et nous l'avons vécu récemment avec la pandémie du Covid).
3. **La simplicité de la gestion** : la centralisation de l'accès sur un serveur uniquement facilite la gestion des utilisateurs à distance.
4. **Une réduction des coûts** : permet le travail à distance pour augmenter la productivité.

## 2. Choix d'OpenVPN

Nous avons choisi OpenVPN car c'est une solution open-source gratuite, fiable et reconnue, utilisée dans des environnement d'entreprise et qui a fait preuve de son efficacité.

De plus, et nous dirons même surtout, il s'intègre facilement à la topologie présentée, étant notamment très complémentaire avec la solution de pare-feu pfSense sur lequel le serveur est installé. Le pare-feu pfSense apporte en effet une certification locale et sécurisée ainsi qu'une authentification déléguée par l'Active Directory.

Il permet enfin un filtrage appliqué directement sur les groupes d'utilisateurs de l'Active Directory, ce qui permet d'affiner les accès aux services présents dans le LAN de MOLECULIS.

Le pare-feu pfSense propose aussi une autre solution de serveur VPN avec IPSec. Nous l'avons choisi plutôt que le VPN IPSec pour plusieurs raisons :

1. Plus grande **compatibilité** aux différents environnements
2. Configuration et gestion pour les administrateurs plus simple ainsi qu'une intégration simplifiée
3. **Sécurité** supérieure et plus moderne, notamment s'agissant du chiffrement. IPSec nécessite, pour atteindre le même niveau de sécurité, une configuration plus complexe.
4. IPSec est plus orienté sur les connexions **site à site**, ce qui ne répond globalement pas à notre besoin.
5. Configuration simplifiée pour les utilisateurs finaux, notamment la **gestion d'export** de configurations.

### 3. Prérequis matériels et logiciels

Concernant les prérequis matériels, se référer aux configurations détaillées dans le chapitre **Pfsense -> Prérequis matériels**.

Concernant les prérequis logiciels, assurez-vous de l'effectivité des :

**Version de pfSense** : Assurez-vous d'utiliser une version de pfSense qui supporte OpenVPN et l'intégration avec Active Directory. Les versions récentes pfSense (2.4.x et supérieures) sont compatibles.

**Serveur Windows avec AD** : Un serveur AD actif sur lequel vous pouvez authentifier vos utilisateurs

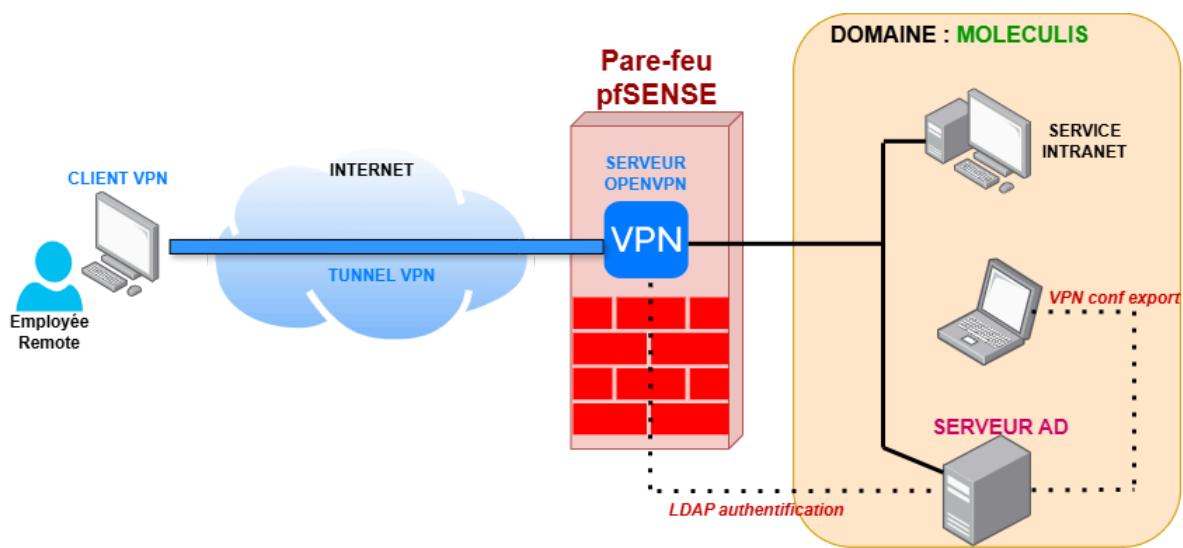
**Accès LDAPS** : Votre serveur AD doit être configuré pour accepter les connexions LDAPS pour assurer le chiffrement des échanges avec pfSense (voir le Chapitre **pfSense -> Délégation de l'authentification**)

**OpenVPN** : Ce paquet est généralement installé par défaut sur pfSense, mais vous devrez vous assurer qu'il est activé.

**OpenVPN Client Export Utility** : Nécessaire pour exporter les configurations utilisables par les clients.

## 4. Installation et configuration d'OpenVPN

Les instructions présentes dans ce guide vont permettre d'assurer cet accès en s'appuyant sur la solution OpenVPN offerte par pfSense ainsi qu'une authentification et un déploiement orchestrés par le contrôleur de domaine Active Directory comme présenté ci-dessous.



La procédure d'installation va suivre le déroulement suivant :

- La création de l'autorité de certification interne
- La génération d'un certificat interne
- La configuration du serveur OpenVPN
- L'authentification délégué à l'Active Directory via l'ACDS
- Le déploiement des configurations par GPO sur les postes locaux
- Les procédures de test

## 4.1.Création d'une autorité de certification interne à pfSense

Il s'agit ici de créer une autorité de certification interne à pfSense qui va permettre de générer et signer des certificats pour les clients et serveurs VPN afin d'assurer une connexion sécurisée. Cette autorité de certification interne servira à vérifier la validité des certificats utilisés dans le VPN, que nous allons créer dans la partie suivante.

Allez dans **User Manager -> Certificates Authority**

Create / Edit CA

<u>Descriptive name</u>	CA-MOLECULIS-OPNVPN
The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '	
<u>Method</u>	Create an internal Certificate Authority
<u>Trust Store</u>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
<u>Randomize Serial</u>	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Choisir une clé **RSA2048**, un algorithme **SHA256**.

Contrairement au certificat, l'autorité de certificat peut avoir une **durée de 10 ans**.

Définir les informations sociales liées au laboratoire Moleculis.

Internal Certificate Authority

<u>Key type</u>	RSA
<input type="checkbox"/> 2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest Algorithm</u>	sha256
The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.	
<u>Lifetime (days)</u>	3650
<u>Common Name</u>	internal-ca
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	FR
<u>State or Province</u>	Loire-Atlantique
<u>City</u>	Nantes
<u>Organization</u>	Moleculis
<u>Organizational Unit</u>	e.g. My Department Name (optional)

L'autorité est maintenant créée et peut être retrouvée dans **user manager-> authorities**.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-MOLECULIS	✓	self-signed	2	CN=moleculis-ca ⓘ Valid From: Mon, 25 Nov 2024 14:07:58 +0100 Valid Until: Thu, 23 Nov 2034 14:07:58 +0100		🔧 🌐 🔍 🗃
ADCS	✗	self-signed	0	DC=moleculis, DC=lan, CN=moleculis-MOLECULIS-SERV-CA ⓘ Valid From: Thu, 28 Nov 2024 15:09:56 +0100 Valid Until: Tue, 28 Nov 2034 15:19:56 +0100	LDAP Server	🔧 🌐
CA-MOLECULIS-VPN	✓	self-signed	1	ST=Loire-Atlantique, O=Moleculis, L=Nantes, CN=internal-ca, C=FR ⓘ Valid From: Wed, 04 Dec 2024 12:28:26 +0100 Valid Until: Sat, 02 Dec 2034 12:28:26 +0100		🔧 🌐 🔍 🗃

## 4.2. Création du certificat interne à pfSense

A partir de l'autorité de certification interne précédemment établie, créez un certificat interne

**Add/Sign a New Certificate**

**Method:** Create an internal Certificate

**Descriptive name:** CERT-MOLECULIS-OPNVPN  
The name of this entry as displayed in the GUI for reference.  
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, , '.

**Internal Certificate**

**Certificate authority:** CA-MOLECULIS-OPNVPN

**Key type:** RSA

**2048**  
The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm:** sha256  
The digest method used when the certificate is signed.  
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

**Lifetime (days):** 365  
The length of time the signed certificate will be valid, in days.  
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

**Common Name:** vpn.moleculis.lan

Choisir l'autorité précédemment créée comme autorité de certification.  
 Choisir une clé RSA 2048 et un algorithme de type SHA256.  
 La période de validité ne doit pas dépasser un an pour des raisons de sécurité.

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6742783812831) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6742783812831  Valid From: Sun, 24 Nov 2024 01:50:00 +0100 Valid Until: Sat, 27 Dec 2025 01:50:00 +0100	webConfigurator	
VPN-GJ User Certificate CA: No Server: No	CA-MOLECULIS	CN=Gwen  Valid From: Mon, 25 Nov 2024 15:07:55 +0100 Valid Until: Thu, 23 Nov 2034 15:07:55 +0100	User Cert	
ADCS-Certificate CA: Yes Server: No	self-signed	DC=moleculis, DC=lan, CN=moleculis-MOLECULIS-SERV-CA  Valid From: Thu, 28 Nov 2024 15:09:56 +0100 Valid Until: Tue, 28 Nov 2034 15:19:56 +0100		
CERT2-MOLECULIS-OPNVPN Server Certificate CA: No Server: Yes	CA-MOLECULIS-VPN	ST=Loire-Atlantique, O=Moleculis, L=Nantes, CN=vpn.moleculis.lan, C=FR  Valid From: Wed, 04 Dec 2024 12:30:21 +0100 Valid Until: Sun, 09 Nov 2025 12:30:21 +0100	OpenVPN Server	

### 4.3. Configuration du serveur openVPN

Vous allez ici **configurer le serveur OpenVPN sur pfSense** pour accepter les connexions VPN. Cela va inclure :

- La définition des interfaces
- Les protocoles utilisés
- Les paramètres de certificats (certificats et clé de chiffrement)

Aller dans **VPN -> OpenVPN -> Servers** et cliquer sur **Add**.

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions

Sélectionnez l'**autorité d'authentification Active Directory** (voir le chapitre pfSense -> déléгation de l'authentification) . La création des utilisateurs autorisés à utiliser le serveur OpenVPN sera réalisée par les administrateurs de l'AD.

**General Information**

**Description**: SERV-OPENVPN-MOLECULIS  
A description of this VPN for administrative reference.

**Disabled**:  Disable this server  
Set this option to disable this server without removing it from the list.

**Mode Configuration**

**Server mode**: Remote Access (User Auth)

**Backend for authentication**: DC-Moleculis.lan  
Local Database

**Device mode**: tun - Layer 3 Tunnel Mode  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Choisir l'interface **WAN** et modifier le port par défaut pour des raisons de sécurité.

**Endpoint Configuration**

**Protocol**: UDP on IPv4 only

**Interface**: WAN  
The interface or Virtual IP address where OpenVPN will receive client connections.

**Local port**: 4050  
The port used by OpenVPN to receive client connections.

Choisir ensuite l'utilisation du chiffrement **TLS** et choisir l'autorité de certification locale ainsi que le certificat associé précédemment créé.

**Cryptographic Settings**

**TLS Configuration**

- Use a TLS Key  
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
- Automatically generate a TLS Key.

**Peer Certificate Authority**: CA-MOLECULIS-OPNVPN

**Peer Certificate Revocation list**: No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

**OCSP Check**:  Check client certificates with OCSP

**Server certificate**: CERT-MOLECULIS-OPNVPN (Server: Yes, CA: CA-MOLECULIS-OPNVP)  
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

## Choisir SHA256 comme type chiffrage et forcer

<b>Fallback Data Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)	The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
<b>Auth digest algorithm</b>	SHA256 (256-bit)	The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
<b>Hardware Crypto</b>	No Hardware Crypto Acceleration	
<b>Certificate Depth</b>	One (Client+Server)	When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
<b>Client Certificate Key Usage Validation</b>	<input checked="" type="checkbox"/> Enforce key usage	Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

## Ensuite, paramétrez les configurations réseaux.

- Le tunnel VPN : 10.0.8.0/24
- Le réseau de destination : Le sous-réseau du LAN Moleculis vers lequel le client va pouvoir se connecter.

Tunnel Settings		
<b>IPv4 Tunnel Network</b>	10.0.8.0/24	This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.  A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
<b>IPv6 Tunnel Network</b>		This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
<b>Redirect IPv4 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.	
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.	
<b>IPv4 Local network(s)</b>	192.168.1.0/24	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

## Configurez ensuite les informations relatives au VPN, en définissant le domaine et le serveur DNS.

Advanced Client Settings		
<b>DNS Default Domain</b>	<input checked="" type="checkbox"/> Provide a default domain name to clients	
<b>DNS Default Domain</b>	moleculis.lan	
<b>DNS Server enable</b>	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.	
<b>DNS Server 1</b>	192.168.1.2	

**OpenVPN Server**

Remote Access Server	SERV-OPENVPN-MOLECULIS UDP4:4050
<b>Client Connection Behavior</b>	
Host Name Resolution	Other
Host Name	vpn.moleculis.lan
Enter the hostname or IP address the client will use to connect to this server.	
Verify Server CN	Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.	

Le serveur OpenVPN est maintenant créé et accessible dans la liste des serveurs.

VPN / OpenVPN / Servers

Servers	Clients	Client Specific Overrides	Wizards	Client Export												
<b>OpenVPN Servers</b> <table border="1"> <thead> <tr> <th>Interface</th> <th>Protocol / Port</th> <th>Tunnel Network</th> <th>Mode / Crypto</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>any</td> <td>UDP4 / 1194 (TUN)</td> <td>10.0.8.0/24</td> <td> <b>Mode:</b> Remote Access ( User Auth )  <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC  <b>Digest:</b> SHA256  <b>D-H Params:</b> 2048 bits                 </td> <td>OpenVPN2-MOLECULIS</td> <td> </td> </tr> </tbody> </table>					Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions	any	UDP4 / 1194 (TUN)	10.0.8.0/24	<b>Mode:</b> Remote Access ( User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	OpenVPN2-MOLECULIS	
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions											
any	UDP4 / 1194 (TUN)	10.0.8.0/24	<b>Mode:</b> Remote Access ( User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	OpenVPN2-MOLECULIS												

Rendez-vous maintenant dans la rubrique **Client Export** pour récupérer la configuration client qui va permettre de se connecter au serveur OpenVPN.

**OpenVPN Clients**

User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none"> <li>- Inline Configurations:             </li> <li>- Bundled Configurations:            </li> <li>- Current Windows Installer (2.6.7-lx001):            </li> <li>- Previous Windows Installer (2.5.9-lx601):            </li> <li>- Legacy Windows Installers (2.4.12-lx601):            </li> <li>- Viscosity (Mac OS X and Windows):            </li> </ul>

## 4.4.Règles de filtrage relatives au VPN

Créez deux règles de filtrage pour assurer les communications du serveur VPN avec l'extérieur et le LAN.

Voir pfSense -> règles de filtrages pour plus de détails.

### Autorisez la connection au serveur VPN par le WAN

The screenshot shows the 'WAN' tab selected in the top navigation bar. Below it, a table lists a single rule for OpenVPN traffic:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/235 KIB	IPv4 UDP	*	*	WAN address	4050	*	none		Allow traffic to OpenVPN server	

### Autorisez la connection du serveur VPN vers le LAN

The screenshot shows the 'OpenVPN' tab selected in the top navigation bar. Below it, a table lists a single rule for traffic from OpenVPN to the LAN:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 UDP	10.0.8.0/24	*	LAN subnets	*	*	none		Allow traffic from OpenVPN to LAN	

At the bottom of the interface, there are several action buttons: Add, Delete, Toggle, Copy, Save, and Separator.

## 4.5.Authentification et déploiement par l'Active Directory

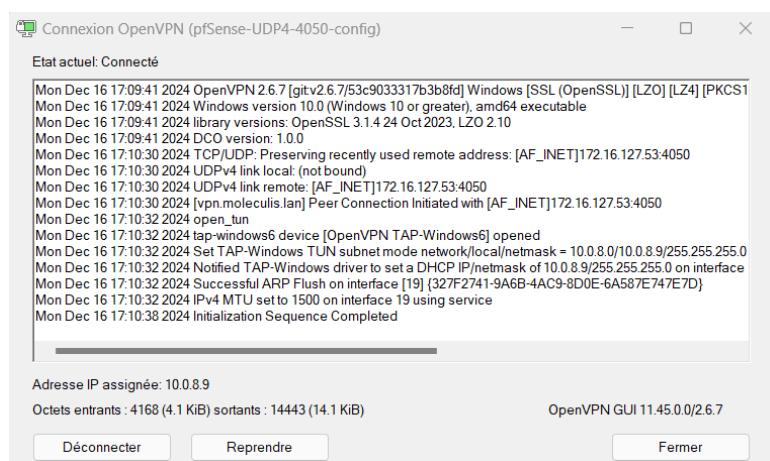
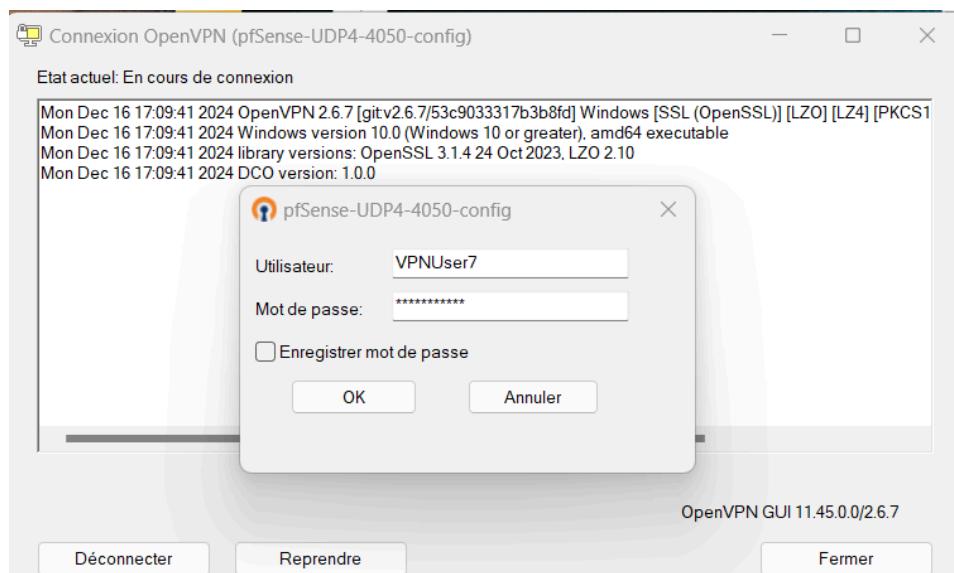
Comme nous l'avons vu précédemment, l'Active Directory est responsable de l'authentification concernant les VPN.

Dans l'OU **Network\_Services**, vous allez pouvoir créer des utilisateurs OpenVPN qui pourront être ensuite s'authentifier à distance via une validation entre le pare-feu

Ils pourront de même récupérer les configurations grâce à un script de déploiement powershell orchestré par l'Active Directory.

## 4.6 Test de la connection depuis un hôte du WAN

Connectez-vous localement dans le domaine avec un laptop sur une session appartenant au groupe OpenVPN. A la connexion, la GPO d'export va installer le client OpenVPN et exporter le fichier de configuration. Il sera ensuite possible de se connecter via le WAN en rentrant le nom d'utilisateur et le mot de passe définis par le service de l'AD.



## VII - Supervision

### 1. Supervision des systèmes

La supervision désigne le suivi du bon fonctionnement d'un système ou d'une activité. Elle vise à contrôler, rapporter et signaler les états normaux ou anormaux des systèmes informatiques. Ce processus repose sur une surveillance en temps réel des valeurs et des événements, garantissant ainsi que les systèmes opèrent de manière efficace, sécurisée et conforme aux paramètres préalablement définis.

En cas d'incident ou de dysfonctionnement, le système de supervision peut envoyer des notifications via la console, par email, ou encore par SMS, ce qui permet une disponibilité de surveillance en continu, 24h/24 et 7j/7, notamment dans les entreprises qui gèrent des cellules de crise.

Les outils de supervision sont des logiciels qui permettent aux administrateurs de contrôler leurs infrastructures. Ils communiquent avec l'environnement IT via divers protocoles comme SNMP, WMI, SSH ou HTTP. Le choix du protocole varie en fonction de l'outil, du fournisseur d'application ou du fabricant de l'équipement concerné.

### 2. Sélection de Centreon comme solutions de supervision

Avec l'expansion continue des réseaux informatiques, il est devenu indispensable d'assurer leur bon fonctionnement, car chaque dysfonctionnement peut entraîner des coûts considérables. Le choix d'une solution de supervision efficace est donc crucial.

Bien que plusieurs options existent, telles que Nagios, Zabbix, Shinken, et Centreon, nous avons opté pour Centreon, convaincus de sa robustesse, de sa flexibilité et de sa capacité à répondre parfaitement aux besoins de ce projet pour les raisons suivantes :

- **Open-source et gratuit** : Centreon est une solution open-source, accessible gratuitement, permettant une personnalisation totale et une réduction des coûts.
- **Tableau de bord en temps réel** : Il fournit un tableau de bord dynamique pour surveiller l'état des systèmes et des services en temps réel, facilitant la détection rapide des problèmes.
- **Interface conviviale** : Son interface est intuitive et simple à utiliser, même pour des utilisateurs non techniques, ce qui simplifie la gestion des alertes et des performances.
- **Flexibilité et personnalisation** : Centreon offre une grande souplesse dans la configuration, avec des options de personnalisation pour répondre aux besoins spécifiques de chaque organisation.

Développé en France, Centreon est un outil de supervision largement utilisé pour surveiller des infrastructures critiques, comme celles du Ministère de la Justice.

Le fonctionnement global est résumé dans le schéma (voir Figure 1), qui montre les interactions entre les différents éléments.

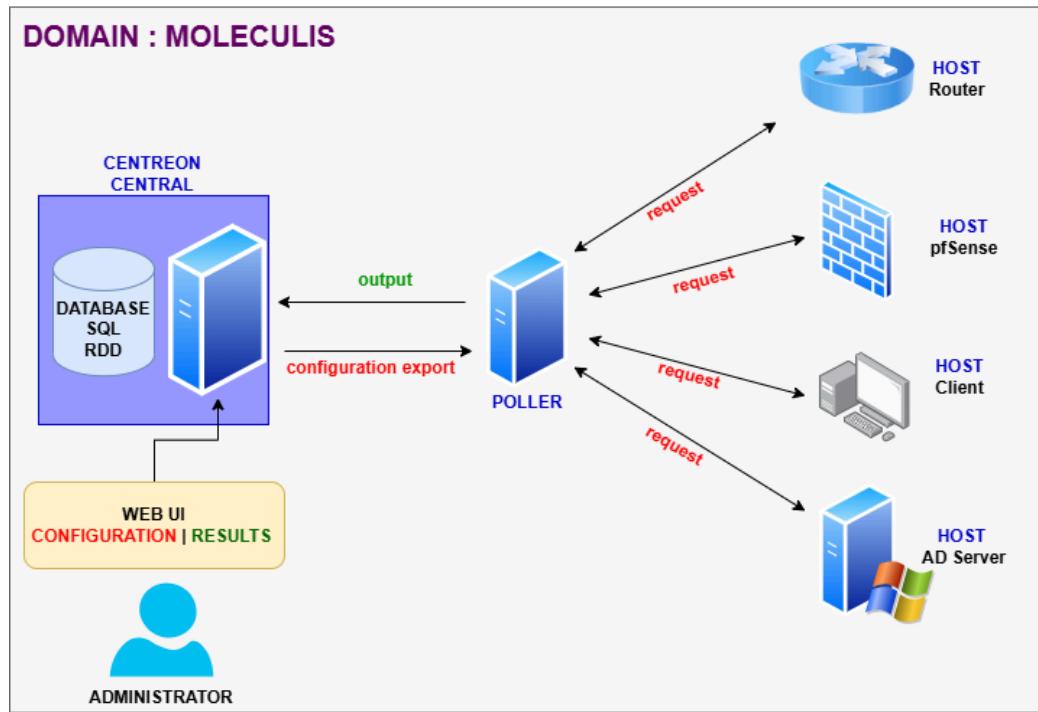


Figure 1 : Fonctionnement de Centreon

### 3.Prérequis logiciels et matériels

#### 3.1.Prérequis logiciels

##### **Base de données**

Centreon prend en charge **MariaDB (version 10.5.x)**. L'utilisation d'autres bases de données sur MySQL est possible mais uniquement prise en charge par la communauté.

##### **Dépendances logicielles**

Les logiciels suivants sont nécessaires pour Centreon :

Logiciel	Version minimale
Apache	2.4
GnuTLS	$\geq 2.0$
Net-SNMP	5.7
OpenSSL	$\geq 1.0.1k$
PHP	8.0
RRDtools	1.4.7
Zlib	1.2.3

### 3.2. Prérequis matériels

Nombre de services	Hôtes estimés	Pollers nécessaires	Central (vCPU / RAM)	Poller (vCPU / RAM)
< 500	50	1 central	1 vCPU / 1 Go	-
500 - 2000	50 - 200	1 central	2 vCPU / 2 Go	-

### Espace disque recommandé

Nombre de services	/var/lib/mysql (en Go)	/var/lib/centreon (en Go)
500	10	2.5
2000	42	10

### Système de fichiers

- Serveur Centreon

Système de fichiers	Taille minimale
swap	1 à 1,5 fois la taille de la RAM
/	Au moins 20 Go
/var/log	Au moins 10 Go
/var/lib/centreon	Selon la taille des données
/var/cache/centreon/backup	Au moins 10 Go (export et purge quotidiens)

- **Pollers de supervision**

Système de fichiers	Taille minimale
swap	1 à 1,5 fois la taille de la RAM
/	Au moins 20 Go
/var/log	Au moins 10 Go
/var/lib/centreon-broker	Au moins 5 Go

## 4. Installation de Centreon

L'installation suivante est réalisée dans un environnement de test Oracle LINUX 9

### 4.1. Installation du serveur MySQL

L'installation de MySQL pour Centreon consiste à configurer une base de données relationnelle pour stocker les informations de surveillance. Voici un résumé des étapes :

1. Installer MySQL avec :

```
apt-get install mysql-server ou yum install mysql-server selon la distribution.
```

2. Démarrer le service MySQL avec :

```
systemctl start mysql.
```

3. Sécuriser l'installation avec :

```
mysql_secure_installation.
```

4. Créer une base de données dédiée à Centreon, par exemple :

```
CREATE DATABASE centreon;
```

5. Créer un utilisateur MySQL pour Centreon avec des privilèges suffisants :

```
CREATE USER 'centreon'@'localhost' IDENTIFIED BY 'password';).
```

6. Accorder les droits nécessaires à l'utilisateur avec :

```
GRANT ALL PRIVILEGES ON centreon.* TO 'centreon'@'localhost';.
```

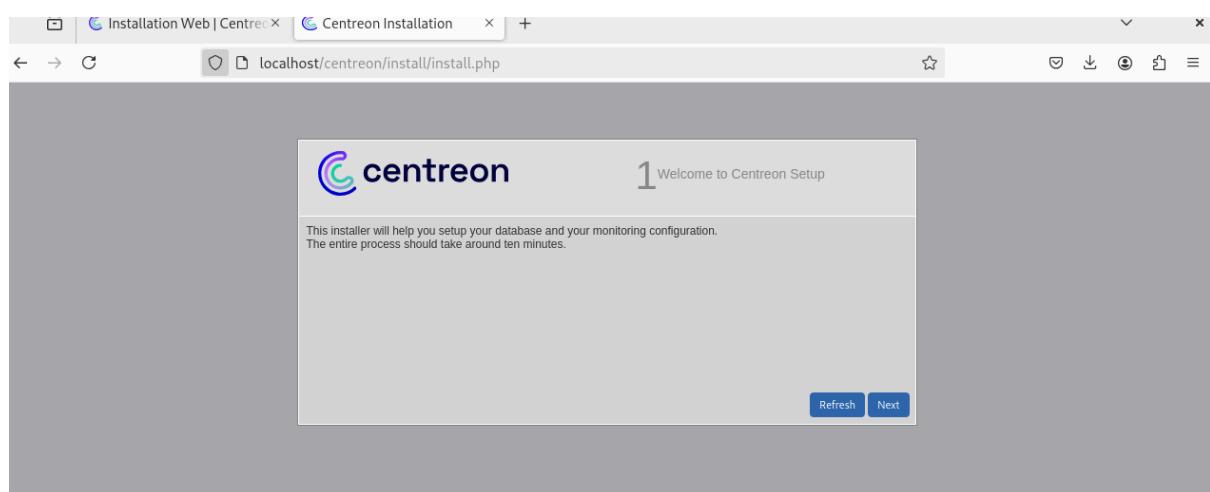
7. Charger la base de données Centreon via les scripts SQL fournis dans l'archive d'installation.
8. Configurer Centreon pour utiliser MySQL en modifiant le fichier de configuration centreon.conf.
9. Vérifier la connectivité de la base de données à partir de Centreon.
10. Redémarrer les services Centreon pour appliquer la configuration.

## 4.2. Installation Web

Connectez-vous à l'interface web via <http://<ip du serveur>/centreon>.

### Étape 1 : Welcome to Centreon setup

L'assistant de configuration de Centreon s'affiche. Cliquez sur Next.



## Étape 2 : Dependency check up

Les modules et les prérequis nécessaires sont vérifiés. Ils doivent tous être satisfais. Cliquez sur Refresh lorsque les actions correctrices nécessaires ont été effectuées. Puis cliquez Next.

Module name	File	Status
MySQL	pdo_mysql.so	Loaded
GD	gd.so	Loaded
LDAP	ldap.so	Loaded
XML Writer	xmlwriter.so	Loaded
MB String	mbstring.so	Loaded
SQLite	pdo_sqlite.so	Loaded
INTL	intl.so	Loaded

Back    Refresh    Next

## Étape 3 : Monitoring engine information

Définissez les chemins utilisés par le moteur de supervision. Nous recommandons d'utiliser ceux par défaut. Puis cliquez sur Next.

Monitoring engine information	
Centreon Engine Stats binary *	/usr/sbin/centenginestats
Centreon Engine var lib directory *	/var/lib/centreon-engine
Centreon Engine Connector path	/usr/lib64/centreon-connector
Centreon Engine Library (*.so) directory *	/usr/lib64/centreon-engine
Centreon Plugins Path *	/usr/lib/centreon/plugins/

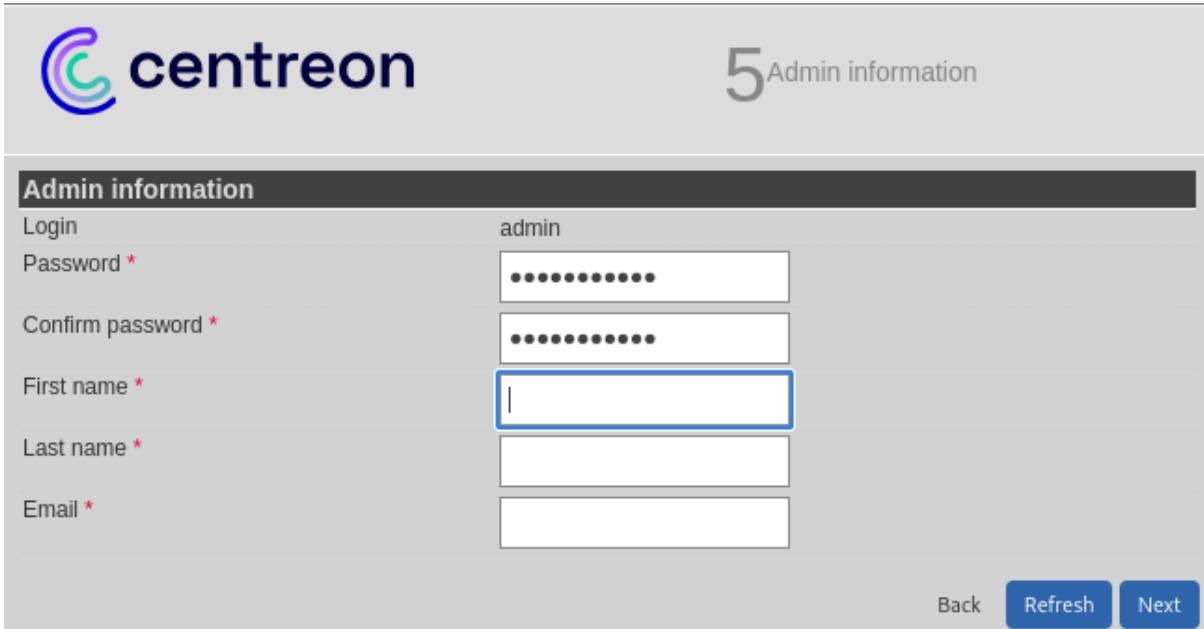
Back    Refresh    Next

## Étape 4 : Broker module information

Définissez les chemins utilisés par le multiplexeur. Nous recommandons d'utiliser ceux par défaut. Puis cliquez sur Next.

## Étape 5 : Admin information

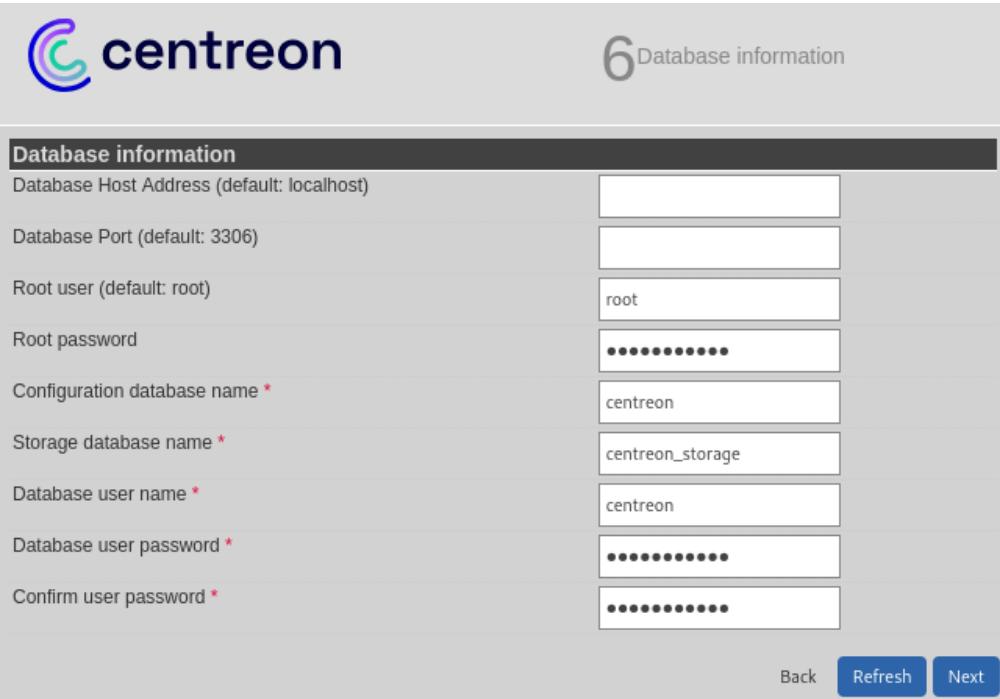
Définissez les informations nécessaires pour la création de l'utilisateur par défaut, admin. Vous utiliserez ce compte pour vous connecter à Centreon la première fois. Le mot de passe doit être conforme à la politique de sécurité de mot de passe par défaut : 12 caractères minimum, lettres minuscules et majuscules, chiffres et caractères spéciaux. Vous pourrez changer cette politique par la suite. Puis cliquez sur Next.



The screenshot shows the 'Admin information' configuration screen. It includes fields for Login (admin), Password, Confirm password, First name, Last name, and Email. The 'First name' field is currently active, indicated by a blue border around its input box. At the bottom right are 'Back', 'Refresh', and 'Next' buttons.

## Étape 6 : Database information

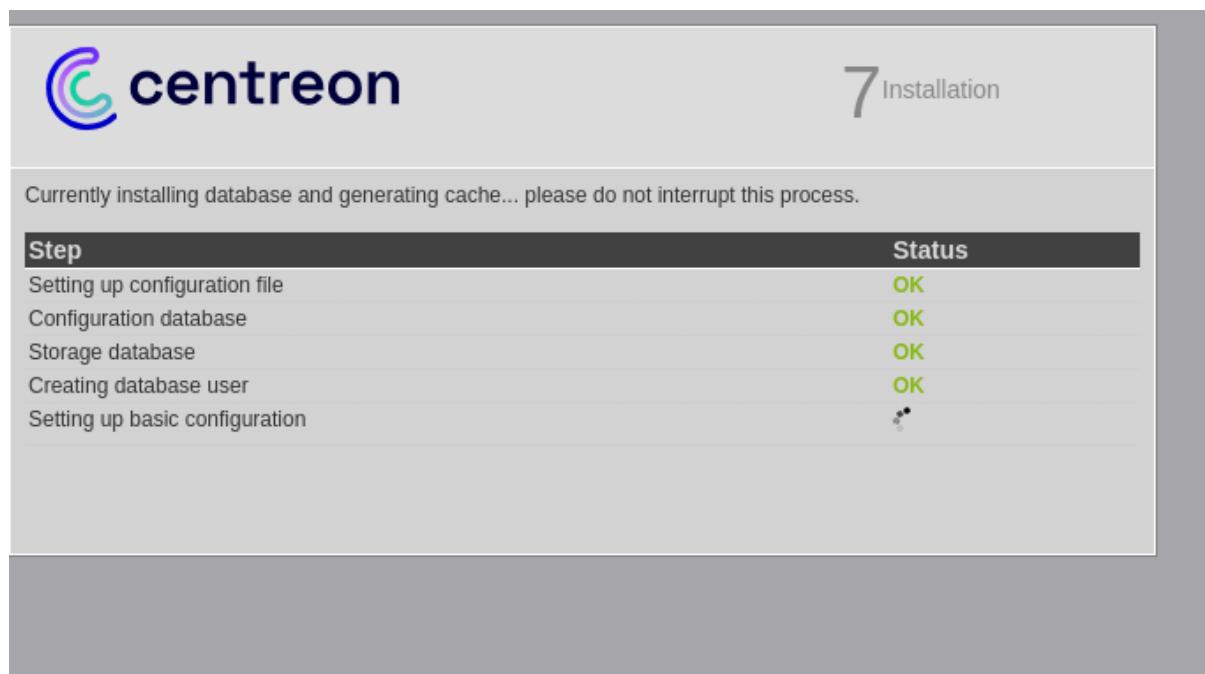
Fournissez les informations de connexion à l'instance de base de données. Puis cliquez sur Next.



The screenshot shows the 'Database information' configuration screen. It includes fields for Database Host Address, Database Port, Root user (set to root), Root password, Configuration database name (set to centreon), Storage database name (set to centreon\_storage), Database user name (set to centreon), Database user password, and Confirm user password. At the bottom right are 'Back', 'Refresh', and 'Next' buttons.

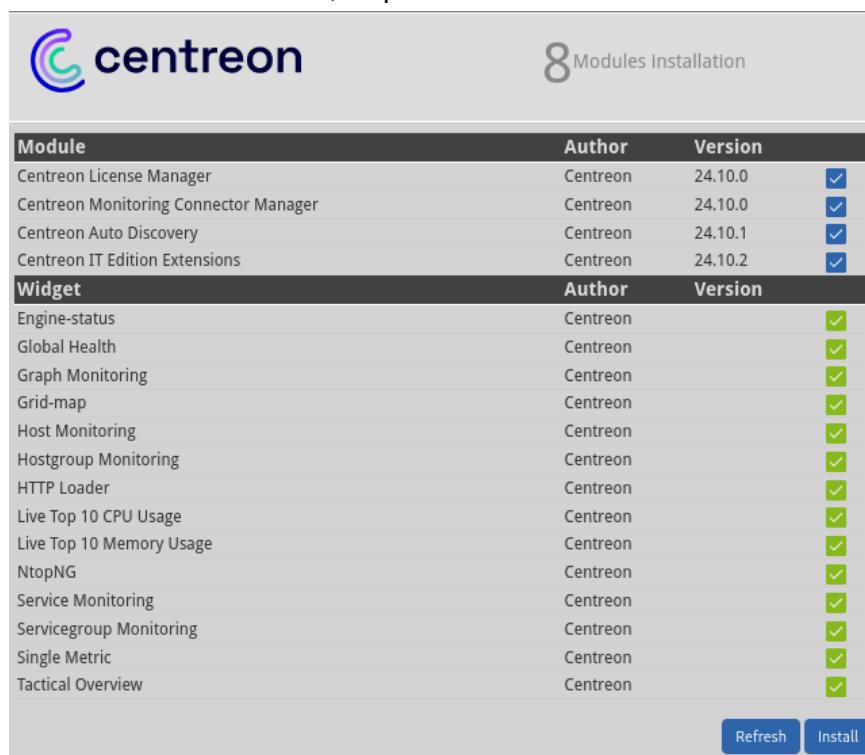
## Étape 7 : Installation

L'assistant de configuration crée les fichiers de configuration et les bases de données. Quand le processus est terminé, cliquez sur Next.



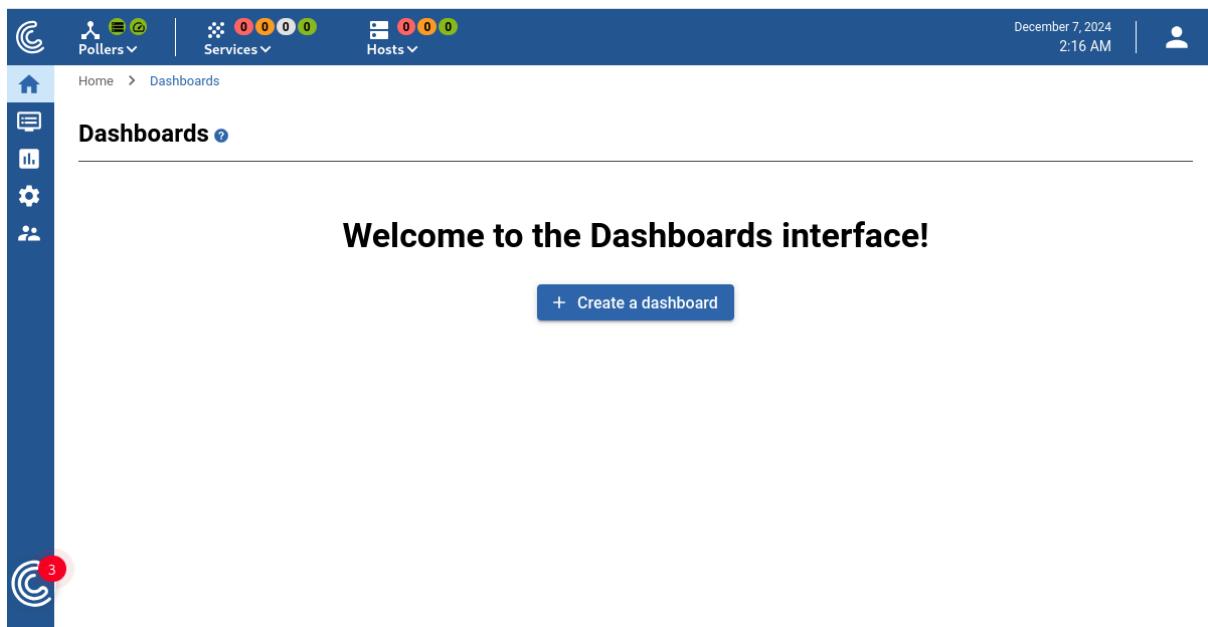
## Étape 8 : Modules installation

Selectionnez les modules et widgets disponibles à l'installation. Puis cliquez sur Install. Une fois les modules installés, cliquez sur Next.



L'installation est terminée, cliquez sur **Terminer**.

Vous pouvez maintenant vous connecter en utilisant le compte admin, et initialiser la supervision.



## 5. Intégration du serveur dans le domaine Active Directory

L'intégration du serveur Centreon dans un domaine Active Directory permet de centraliser la gestion des utilisateurs et des ressources, facilitant ainsi l'administration et la sécurité du système.

### Étape 1 : Installation des Paquets Nécessaires

Commande : sudo yum install realmd sssd adcli krb5-workstation samba-common-tools

```
[root@centreon ~]# yum install realmd sssd adcli krb5-workstation samba-common-tools
Dernière vérification de l'expiration des métadonnées effectuée il y a 1:25:38 le sam. 07 déc. 2024 01:58:03.
Le paquet realmd-0.17.1-2.el9.x86_64 est déjà installé.
Le paquet sssd-2.9.5-4.0.1.el9_5.1.x86_64 est déjà installé.
Le paquet adcli-0.9.2-1.el9.x86_64 est déjà installé.
Dépendances résolues.
=====
Paquet           Architecture      Version       Dépôt        Taille
=====
Installation:
krb5-workstation   x86_64  1.21.1-4.0.1.el9_5  ol9_baseos_latest  660 k
samba-common-tools  x86_64  4.20.2-2.0.1.el9_5  ol9_baseos_latest  497 k
Installation des dépendances:
krb5-pkinit        x86_64  1.21.1-4.0.1.el9_5  ol9_baseos_latest   56 k
libkadm5          x86_64  1.21.1-4.0.1.el9_5  ol9_baseos_latest   76 k
libnetapi         x86_64  4.20.2-2.0.1.el9_5  ol9_baseos_latest  142 k
samba-ldb-ldap-modules x86_64  4.20.2-2.0.1.el9_5  ol9_baseos_latest   27 k
samba-libs        x86_64  4.20.2-2.0.1.el9_5  ol9_baseos_latest  135 k
Résumé de la transaction
=====
Installer 7 Paquets

Taille totale des téléchargements : 1.6 M
Taille des paquets installés : 5.6 M
Voulez-vous continuer ? [o/N] : o
```

## Étape 2 : Découverte du Domaine Active Directory

Commande : realm discover moleculis.lan

```
[root@centreon ~]# realm discover moleculis.lan
moleculis.lan
  type: kerberos
  realm-name: MOLECULIS.LAN
  domain-name: moleculis.lan
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
```

## Étape 3 : Configuration du Fichier SSSD

Commande : nano /etc/sssd/sssd.conf

```
[root@centreon ~]# nano /etc/sssd/sssd.conf
```

## Étape 4 : Rejoindre le Domaine Active Directory

Commande : realm join --user=<domain\_admin> moleculis.lan

```
[root@centreon ~]# realm join --user=a.nady moleculis.lan
Password for a.nady@MOLECULIS.LAN:
 * Installing necessary packages: oddjob oddjob-mkhomedir
[root@centreon ~]#
```

## Étape 5 : Vérification de l'Intégration

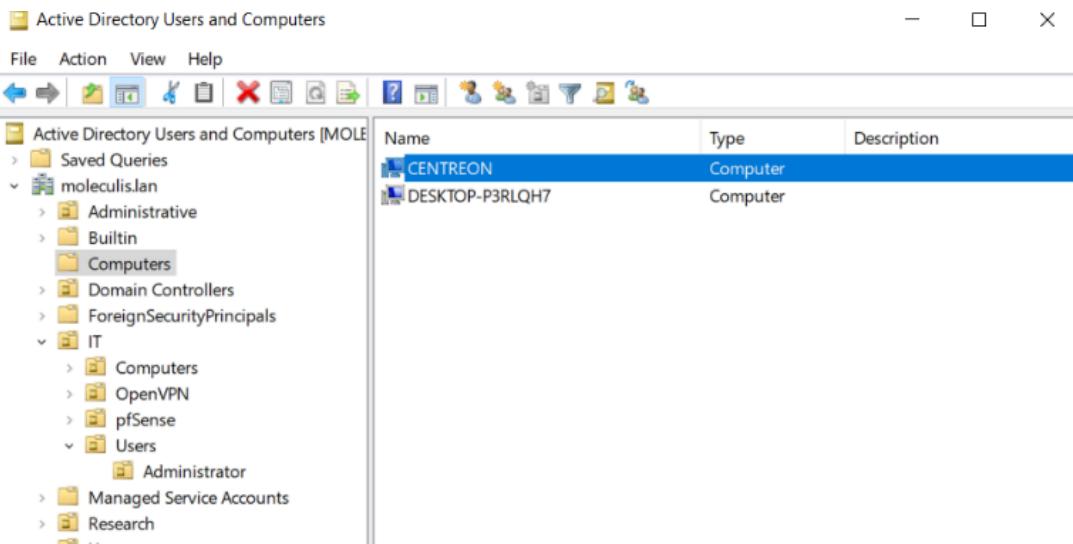
Commande : id <domain\_admin>

```
sssd
domains = moleculis.lan
config_file_version = 2
services = nss, pam

[domain/moleculis.lan]
default_shell = /bin/bash
krb5_store_password_if_offline = True
tcache_credentials = True
krb5_realm = MOLECULIS.LAN
realm_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = moleculis.lan
use_fullyQualifiedNames = True
ldap_id_mapping = True
access_provider = ad
```

## Vérification de l'Intégration dans Active Directory

Utilisez l'outil **Active Directory Users and Computers** sur un serveur Windows pour vérifier que le serveur Centreon est bien intégré dans le domaine "Moleculis".



## 6. Configuration de Centreon

### 6.1. Crédit d'un Poller et utilisation (Local)

#### Création d'un poller

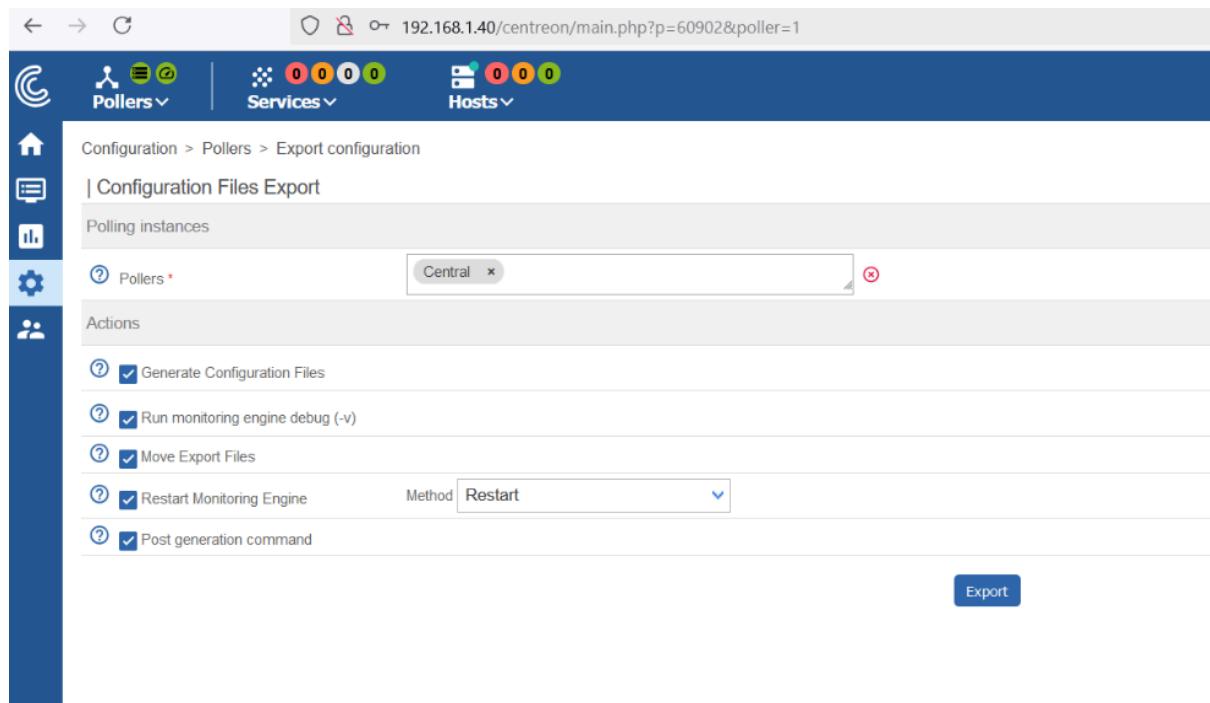
Accédez à l'interface web de Centreon : Allez dans Configuration > Pollers > Add. Remplissez les informations nécessaires (Nom, IP, etc.) Sauvegardez et déployez la configuration.

Il s'agit ici d'un collecteur local, la configuration d'un collecteur externe n'a pas été expérimenté, il s'agirait d'une installation sur une autre machine similaire à celle du serveur Central Centreon.

Pollers												30	
<input type="checkbox"/>	Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Options
<input checked="" type="checkbox"/>	Central	127.0.0.1	Central	<span>YES</span>	<span>NO</span>	1872	5 hours 34 minutes	December 11, 2024 4:51:29 PM	Centreon Engine 24.10.2	Yes	<span>ENABLED</span>		<span>1</span>

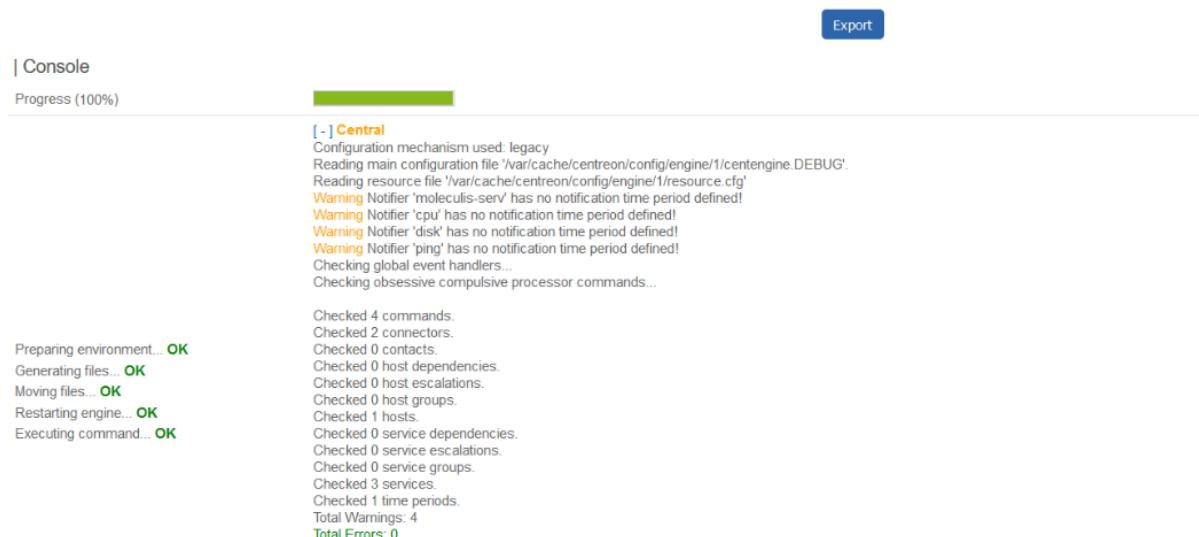
## Export de la configuration vers le Poller

Le poller est l'intermédiaire entre le serveur central et les host. Il va effectuer les requêtes vers les agents installés sur les host à superviser. Chaque configuration d'host et de services associés doit être exportée vers le poller afin d'établir ou modifier la supervision.



## Résultat de l'export

Le serveur central va générer les configurations établies, analyser les éventuelles erreurs liées à la configuration et fournir un compte rendu de l'exportation.



## 6.2.Création d'un Hôte

Accédez à l'interface web de Centreon : Allez dans **Configuration > Hosts > Add.**

The screenshot shows the Centreon web interface with a dark blue header. In the top left, there are icons for Pollers (with 0 items), Services (with 0 items), and Hosts (with 0 items). Below the header, a sidebar on the left contains icons for Home, Pollers, Services, Hosts, Notifications, Relations, Data Processing, and Host Extended Infos. The main content area shows the path 'Configuration > Hosts > moleculis-serv'. The 'Host Configuration' tab is selected. The form is titled '| Modify a Host' and contains the following fields:

- Host basic information**
  - Name: moleculis-serv
  - Alias: (empty)
  - Address: 192.168.1.2 Resolve
  - SNMP Community & Version: (empty) ▼
  - Monitoring server: Central
  - Timezone: Timezone ▼ (X)
- Templates**
  - A host or host template can have several templates. See help for more details.
  - + Add a new entry
  - OS-Windows-SNMP ▼ (+) (edit) (X)
- Create Services linked to the Template too**
  - Yes  No

Remplissez les informations nécessaires :

- Hostname
- Adresse IP de l'host
- Serveur de monitoring

La validation de l'effectivité de la connexion à l'host est effectuée ensuite après l'export, via un simple ping.

Associez l'hôte au poller créé précédemment. Sauvegardez.

## 6.3.Création d'un Service

Accédez à l'interface web de Centreon : Allez **dans Configuration > Services > Add.**  
Remplissez les informations nécessaires :

- Le nom custom du service
- Le nom de l'host précédemment créé
- Templates de supervisions
- Commandes et valeurs de seuils
- Réglages des fréquences de requêtes

The screenshot shows the 'Services by host' section of the Centreon configuration interface. The 'General Information' tab is selected. In the 'Service Basic Information' section, the 'Name' field is set to 'disk' and the 'Hosts' dropdown contains 'moleculis-serv'. The 'Template' dropdown is set to 'OS-Windows-Disk-Global-SNMP'. The 'Service Check Options' section contains several entries under 'Check Command':

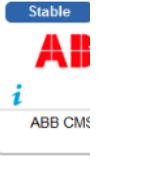
- Name: FILTER, Value: .\*
- Name: TRANSFORMSRC, Value: ^(..)\*
- Name: TRANSFORMDST, Value: \$1
- Name: WARNING, Value: 80
- Name: CRITICAL, Value: 90
- Name: EXTRAOPTIONS, Value: --verbose --filter-perfdata='stora'

Below this, the 'Args' section indicates 'No argument found for this command'. On the left sidebar, there are icons for Pollers, Services, and Hosts.

Les templates sont des **packs de services** (requêtes et méthodes d'applications associées) à effectuer dans votre supervision. Ces templates sont récupérables via l'interface web comme présenté ci-après.

Configuration > Monitoring Connector Manager

### Monitoring Connector Manager ?

Keyword	Category	Status				
 Base Pack	 Centreon Central	 Linux SNMP	 Centreon Database	 Centreon Poller	 Centreon-HA	 Cisco STA
 UPS Standard	 Windows SNMP	 Alcatel-Lucent	 Omniswitch 6850	 3COM	 3CX	 A10 AX
 ABB CMS						

Configurez les services associés à un host en fonction des besoins du laboratoire. Priorisez une surveillance accrue sur les éléments vitaux du réseau :

- Serveurs
- Pare-feu
- Switch fédérateur
- Routeur
- Services AD

Analysez et modulez les surveillances spécifiques adaptés à chaque service :

- Performance : surveillance des ressources systèmes (CPU, RAM, utilisation des disques, bande passante réseau..)
- Services : disponibilité des services et des applications
- Logs : vérification des alertes et erreurs dans les journaux des systèmes ou des applications
- Seuils d'alerte : évaluer les seuils critiques ou d'avertissement associés à chaque services

Sauvegardez et déployez la configuration comme vu précédemment dans la partie Poller.

## 6.4. Gestion de l'interface graphique

L'interface est organisée autour de plusieurs modules qui permettent de gérer les configurations, la visualisation des métriques et l'analyse des performances.

Les techniciens ou administrateurs du laboratoire pourront ainsi créer et configurer des objets de supervision (hôtes, services, équipements) et gérer les alertes en temps réel. Cela va permettre une intervention **proactive** en amont des pannes éventuelles mais aussi de **mieux distribuer les ressources** sur le système.

La WebUI offre des **dashboards** personnalisables, permettant d'afficher les informations les plus essentielles sous forme de graphiques ou de tableaux.

Centreon facilite également la gestion des **alertes et notifications** en temps réel, avec des options de personnalisation pour définir les seuils d'alerte et les actions associées (e-mails, SMS, etc.).

### Vue des services

	Status	Resource	Parent	G	Duration	Last check	Information	Tries
□	Warning	S Memory	① moleculis-serv	■	22m 26s	5m 26s	WARNING: Ram Total: 2.00GB Used: 1.68GB (84.17%) Free: 324.00MB (15.83%)	3/3 (H)
□	Warning	S Swap	① centreon	■	5h 26m	9m 41s	WARNING: Used : 12.45 %	3/3 (H)
□	Unknown	S Test3	① pfSense.moleculis.lan	■	5h 26m	24m 21s	UNKNOWN: No storage found. Can be filters, cache file.	3/3 (H)
□	Unknown	S Service-Windows-Test	① Windows10-Test	■	19h 1m	26m 26s	UNKNOWN: SNMP Table Request: Timeout	3/3 (H)
□	OK	S Swap-AD	① moleculis-serv	■	5h 7m	7m 36s	OK: Swap Total: 3.31 GB Used: 2.31 GB (69.65%) Free: 1.00 GB (30.34%)	1/3 (H)
□	OK	S CPU	① pfSense.moleculis.lan	■	5h 25m	12s	OK: CPU Usage: User 0.03 %, Nice 0.05 %, System 0.66 %, Idle 98.60 %, Wait 0.00 %, Kernel 0.64 %, Interrup...	1/3 (H)
□	OK	S Load	① centreon	■	19h 27m	1m 41s	OK: Load average: 0.10, 0.08, 0.07	1/3 (H)
□	OK	S Cpu	① centreon	■	19h 27m	1m 36s	OK: 2 CPU(s) average usage is 3.50 %	1/3 (H)
□	OK	S Memory	① centreon	■	19h 28m	36s	OK: Ram Total: 2.46 GB Used (+buffers/cache): 1.01 GB (41.10%) Free: 1.45 GB (58.90%), Buffer: 24.00 KB,...	1/10 (H)
□	OK	S CPU-pfSense	① pfSense.moleculis.lan	■	19h 43m	1m 32s	OK: 2 CPU(s) average usage is 0.00 %	1/3 (H)
□	OK	S Test	① pfSense.moleculis.lan	■	22h 4m	3m 11s	OK: All pflnterfaces are ok	1/3 (H)
□	OK	S Ping	① pfSense.moleculis.lan	■	1d 5h	1m 31s	OK - 192.168.1.1 rta 0,469ms lost 0%	1/3 (H)
□	OK	S runtime	① pfSense.moleculis.lan	■	1d 5h	26m 31s	OK: PfSense running since : 5h 19m 8s	1/3 (H)
□	OK	S Ping	① centreon	■	4d 11h	1m 31s	OK - 127.0.0.1 rta 0,030ms lost 0%	1/3 (H)
□	OK	S ping	① moleculis-serv	■	4d 12h	1m 31s	OK - 192.168.1.2 rta 0,326ms lost 0%	1/3 (H)

### Vue des hôtes

	Status	Resource	Parent	G	Duration	Last check	Information	Tries
□	Down	Windows10-Test	■	■	18h 36m	3m 33s	CRITICAL - 192.168.1.144: Host unreachable @ 192.168.1.40 rta nan, lost 100%	1/3 (H)
□	Up	moleculis-serv	■	■	19h 8m	4m 48s	OK - 192.168.1.2 rta 0,602ms lost 0%	1/3 (H)
□	Up	pfSense.moleculis.lan	■	■	21h 18m	2m 18s	OK: All pflnterfaces are ok	1/3 (H)
□	Up	centreon	■	■	4d 11h	1m 3s	OK - 127.0.0.1 rta 0,056ms lost 0%	1/3 (H)

## Rapport d'analyse d'un service

The screenshot shows the Centreon monitoring interface. At the top, there are three navigation links: 'Pollers' (0 green, 2 yellow, 2 orange, 11 red), 'Services' (1 red, 0 green, 3 yellow), and 'Hosts' (1 red, 0 green, 3 yellow). On the left, a vertical sidebar contains icons for Home, Overview, Configuration, and User Management.

The main area displays a 'Services Grid' under 'Monitoring > Status Details'. A search bar at the top right of this grid shows 'Swap' and 'centreon'. The grid lists four hosts: 'centreon' (UP, Swap), 'moleculis-serv' (UP, Memory), 'pfSense.moleculis.lan' (UP, Test3), and 'Windows10-Test' (DOWN, Service).

A detailed service analysis is shown for 'Swap' on 'centreon'. The 'Display' tab is selected, showing the following information:

- Output:** WARNING: Used : 12.45 %
- Status Information:**
  - Last State Change: December 11, 2024 11:22:57 AM
  - Current State Duration: 5h 24m
  - State Type: HARD
- Extended Status Information:**
  - Performance Data:  
'used'=401080320B;0;3221221376  
'free'=2820141056B;0;3221221376  
'used\_prct'=12.45%;0:10;0:30;0:100
- Check information:**
  - Last Check: December 11, 2024 4:39:57 PM
  - Next Check: December 11, 2024 4:54:57 PM
  - Latency: 0.01 s
  - Execution Time: 0.104888 s
  - In Scheduled Downtime?: No
- Notification Information:**
  - Last Notification: N/A
- Last Status Change:**

# IX - BILAN DU PROJET

## 1. Bilan des Réalisations

Le projet d'infrastructure informatique a abouti à la mise en place d'une solution complète et performante, répondant aux besoins de sécurité, de fiabilité et de performance du laboratoire. Voici un résumé des réalisations clés :

### Réseau:

- **Infrastructure réseau complète:** Mise en place d'un réseau local sécurisé avec un câblage structuré et des équipements performants.
- **Active Directory:** Implémentation d'un Active Directory centralisé pour la gestion des utilisateurs, des groupes, des ordinateurs et des ressources du réseau.
- **Pare-feu pfSense:** Installation et configuration d'un pare-feu pfSense pour sécuriser l'accès au réseau et filtrer le trafic internet.
- **Accès VPN:** Mise en place d'un accès VPN sécurisé permettant aux utilisateurs distants d'accéder au réseau du laboratoire.
- **DMZ:** Création d'une zone démilitarisée (DMZ) pour héberger les serveurs web et autres services exposés à l'internet, permettant d'isoler ces services du réseau interne.
- **Serveur de supervision Centreon:** Installation et configuration d'un serveur de supervision Centreon pour surveiller l'état de l'infrastructure et détecter les anomalies.

### Avantages clés:

- **Sécurité renforcée:** Le pare-feu, l'Active Directory et la DMZ garantissent une protection optimale contre les menaces externes.
- **Gestion centralisée:** L'Active Directory facilite la gestion des utilisateurs et des ressources du réseau.
- **Fiabilité et performance:** L'infrastructure réseau est conçue pour garantir une fiabilité et des performances optimales.
- **Supervision proactive:** Centreon permet de détecter et de résoudre les problèmes potentiels avant qu'ils ne causent des interruptions de service.
- **Flexibilité et évolutivité:** L'infrastructure est conçue pour être évolutive et adaptable aux besoins futurs du laboratoire.

## 2.Axes d'amélioration

L'infrastructure informatique de **Moleculis** est déjà solide et performante, mais il est toujours possible d'améliorer certains aspects pour maximiser son efficacité et sa sécurité. Voici quelques axes d'amélioration potentiels :

### Sécurité:

- **Mise en place d'un système de détection d'intrusion (IDS):** Un IDS peut détecter les activités malveillantes en temps réel et alerter les administrateurs, renforçant la sécurité du réseau.
- **Intégration d'un système de gestion des vulnérabilités (VMS):** Un VMS permet de scanner régulièrement l'infrastructure pour identifier les vulnérabilités et de les corriger rapidement, réduisant les risques d'exploitation.

### Performance:

- **Optimisation du réseau:** Analyse du trafic réseau avec **Centreon** et optimisation des configurations pour améliorer les performances et réduire les temps de latence.
- **Mise en place d'un système de stockage partagé:** Un système de stockage partagé performant peut améliorer les performances des applications et faciliter le partage de données entre les chercheurs.

### Gestion et maintenance:

- **Automatisation des tâches de maintenance:** Automatisation des tâches répétitives de maintenance pour réduire la charge de travail des administrateurs et garantir la fiabilité du système.
- **Formation des utilisateurs:** Formation des utilisateurs aux bonnes pratiques de sécurité et d'utilisation de l'infrastructure.

### Evolutivité:

- **Mise en place d'une infrastructure cloud hybride:** L'utilisation d'un cloud hybride permet de bénéficier des avantages du cloud computing tout en conservant le contrôle sur les données sensibles.
- **Intégration de nouvelles technologies:** Intégration de nouvelles technologies émergentes pour améliorer la performance et la sécurité de l'infrastructure.

En intégrant ces axes d'amélioration, **Moleculis** pourra garantir une infrastructure informatique encore plus performante, sécurisée et évolutive, favorisant la recherche et l'innovation au sein du laboratoire.

### 3. Conclusion

L'infrastructure proposée, comprenant **un réseau local sécurisé, un serveur centralisé, des postes de travail performants et des logiciels spécialisés**, permettra aux chercheurs de **Moleculis** de mener leurs travaux de manière optimale.

Ce projet a également permis de mettre en place des **processus de gestion de l'infrastructure**, garantissant ainsi sa **fiabilité, sa sécurité et sa maintenance à long terme**.

La mise en place de cette infrastructure permettra à **Moleculis** de :

- **Améliorer la collaboration entre les chercheurs** grâce à un accès partagé aux données et aux outils.
- **Accélérer la recherche** en offrant aux chercheurs des outils performants et une infrastructure stable.
- **Renforcer la sécurité des données** grâce à un système de sauvegarde et de protection des données.
- **Réduire les coûts** en optimisant l'utilisation des ressources informatiques.

La mise en place de cette **infrastructure informatique complète** a permis d'améliorer significativement la **sécurité, la fiabilité et la performance** du laboratoire. Elle constitue un investissement stratégique pour le développement de la recherche et garantit un environnement informatique optimal pour les chercheurs de **Moleculis**, lui permettant de **s'adapter aux exigences de la recherche moderne et de se positionner comme un acteur majeur dans son domaine**.

# ANNEXES

- [Plan d'adressage complet](#)
- [Fichier de configuration du switch](#)
- [Lien vers le dépôt GitHub du projet](#)
- [Documentation officielle de pfSense](#)
- [Documentation officielle de Centreon](#)
- [Guide de l'ANSSI pour la cybersécurité](#)