Sécurisation d'une infrastructure SI d'entreprise

IMPLÉMENTATION TECHNIQUE DES POLITIQUES DE DURCISSEMENT ET CONFIGURATIONS DE SÉCURITÉ

YMB - TECH

PRÉSENTÉ PAR

YEBGA MIYOGOG Brayan

NOVEMBRE 2025

Table des matières

Résumé

Ce projet s'inscrit dans une démarche de conception et de sécurisation d'une infrastructure réseau segmentée, intégrant des mécanismes de filtrage, de durcissement et de gestion centralisée des identités. L'objectif principal était de mettre en œuvre un système d'information conforme aux recommandations de l'ANSSI, aux normes internationales telles que l'ISO/IEC 27001, aux bonnes pratiques du NIST Cybersecurity Framework ainsi qu'aux exigences réglementaires du RGPD. La méthodologie adoptée repose sur une approche systémique et scientifique : chaque étape a été pensée comme une expérimentation validée par des tests et documentée pour assurer la reproductibilité. La segmentation du réseau et la configuration du pare-feu Ubuntu avec iptables ont permis de cloisonner les flux inter-VLAN, garantissant une défense en profondeur. Le durcissement du serveur Linux Apache, avec la création d'un utilisateur restreint webadmin, la mise en place du chiffrement HTTPS et la désactivation des modules non essentiels, illustre l'application concrète du principe du moindre privilège et des guides de configuration sécurisée. La mise en œuvre d'Active Directory sur Windows Server 2025, avec la création du domaine mondomaine.local, a centralisé l'authentification et la gestion des identités. La jointure des postes clients et administrateurs au domaine a renforcé la cohérence et la sécurité globale. L'édition et la gestion des stratégies de groupe GPO ont permis d'imposer des règles homogènes : stratégie de mots de passe robuste, verrouillage des comptes après tentatives infructueuses, restrictions RDP et désactivation des services inutiles. Les livrables produits, script webadmin.sh et fichier GPO.pdf, constituent des preuves tangibles de la reproductibilité, de la traçabilité et de la conformité des configurations. Ce projet démontre la capacité à articuler rigueur scientifique, pertinence technique et vision stratégique dans le domaine de la cybersécurité. Enfin, il ouvre des perspectives de recherche appliquée : intégration de solutions de supervision et de détection d'intrusion SIEM, automatisation avancée par Ansible, mise en place de mécanismes de haute disponibilité, adaptation aux exigences du RGPD et exploration des approches modernes de micro-segmentation en environnements cloud et hybrides. En définitive, ce travail illustre la convergence entre pratique professionnelle et exigence académique et constitue une base solide pour des recherches futures en cybersécurité appliquée, dans un contexte global marqué par la complexité et l'interconnexion des systèmes.

Abstract

This project is part of a broader effort to design and secure a segmented network infrastructure, integrating mechanisms for filtering, hardening, and centralized identity management. The primary objective was to implement an information system compliant with the recommendations of the French National Cybersecurity Agency (ANSSI), international standards such as ISO/IEC 27001, best practices from the NIST Cybersecurity Framework, and regulatory requirements of the GDPR. The methodology adopted relied on a systemic and scientific approach: each stage was conceived as an experiment, validated through testing, and documented to ensure reproducibility. Network segmentation and the configuration of the Ubuntu firewall with iptables enabled strict isolation of inter-VLAN traffic, ensuring defense-in-depth. The hardening of the Linux Apache server, with the creation of a restricted user account webadmin, the implementation of HTTPS encryption, and the deactivation of non-essential modules, illustrates the concrete application of the principle of least privilege and secure configuration guidelines. The deployment of Active Directory on Windows Server 2025, with the creation of the domain mondomaine.local, centralized authentication and identity management. The integration of client and administrator workstations into the domain reinforced overall coherence and security. The editing and management of Group Policy Objects (GPOs) enforced uniform rules: strong password policies, account lockout after failed attempts, RDP restrictions, and deactivation of unnecessary services. The deliverables produced, including the webadmin.sh script and the GPO.pdf file, serve as tangible evidence of reproducibility, traceability, and compliance with configuration standards. This project demonstrates the ability to combine scientific rigor, technical relevance, and strategic vision in the field of cybersecurity. Finally, it opens avenues for applied research: integration of supervision and intrusion detection solutions (SIEM), advanced automation with Ansible, implementation of high-availability mechanisms, adaptation to GDPR requirements, and exploration of modern micro-segmentation approaches in cloud and hybrid environments. Ultimately, this work illustrates the convergence between professional practice and academic rigor, and provides a solid foundation for future applied cybersecurity research in a global context characterized by complexity and interconnectivity of systems.

Introduction générale

À l'ère de la transformation numérique globale, les systèmes d'information constituent désormais les piliers invisibles mais essentiels de toute organisation, qu'elle soit publique ou privée, industrielle ou tertiaire. Cette dépendance croissante aux infrastructures numériques s'accompagne, en parallèle, d'une exposition accrue aux risques cyber, qu'ils soient d'origine technique, humaine ou organisationnelle. Dans ce contexte, la conception d'une infrastructure réseau sécurisée ne peut plus être envisagée comme une simple opération technique ; elle représente, au contraire, un véritable acte d'ingénierie stratégique mobilisant des compétences transversales en architecture système, cybersécurité, gouvernance et conformité réglementaire.

C'est dans cette dynamique que s'inscrit le projet intitulé *« Mon beau réseau »*. Il consiste à concevoir, déployer et sécuriser une infrastructure IT complète pour une entreprise nouvellement installée, laquelle ne dispose pas encore de Politique de Sécurité des Systèmes d'Information (PSSI). Cette entreprise exprime des priorités claires : d'une part, garantir la confidentialité et l'intégrité des données ; d'autre part, assurer la disponibilité des services critiques ; enfin, mettre en place une traçabilité fiable des événements. Bien que ces exigences soient classiques, elles posent un défi particulier dans un contexte de départ à zéro, où tout est à construire : segmentation réseau, services de base, mécanismes de contrôle d'accès, supervision, documentation.

Dès lors, la problématique centrale de ce projet peut être formulée ainsi : **comment concevoir une infrastructure réseau virtualisée, segmentée et sécurisée, conforme aux bonnes pratiques de l'ANSSI, tout en assurant sa maintenabilité, sa traçabilité et sa transférabilité à un futur administrateur ?** Cette question implique de répondre à plusieurs sous-enjeux : en premier lieu, comment structurer logiquement le réseau pour limiter les risques de propagation ? En second lieu, comment sécuriser les services exposés (web, DNS, AD) sans compromettre leur accessibilité ? En troisième lieu, comment garantir une gestion centralisée des identités et des droits ? Et surtout, comment documenter l'ensemble de manière claire, exploitable et durable ?

Afin de répondre à ces enjeux, une démarche méthodique a été adoptée, articulée autour de quatre axes majeurs. Tout d'abord, la modélisation et le déploiement de l'architecture cible ont permis de définir les VLAN, le plan d'adressage, les choix d'hyperviseurs, la création des machines virtuelles et la configuration des interfaces réseau. Ensuite, la mise en œuvre des services fondamentaux a conduit à l'installation et à la configuration du pare-feu Linux, du

serveur web Apache, du domaine Active Directory, ainsi que des postes clients. Par la suite, une sécurisation multi-niveau de l'infrastructure a été réalisée, reposant sur l'application du principe du moindre privilège, le durcissement des services, la mise en place de certificats SSL/TLS, la configuration des GPO et le filtrage réseau via iptables. Enfin, la documentation, la validation et la transférabilité ont été assurées par la rédaction de scripts d'automatisation, de fiches de validation, de captures d'écran et par la structuration d'un livrable complet à destination d'un futur administrateur.

Ce document présente l'ensemble des livrables issus de cette démarche. Il est conçu comme un guide technique et stratégique, permettant à tout professionnel de comprendre, maintenir et faire évoluer l'infrastructure déployée. Il s'adresse à la fois aux administrateurs système, aux auditeurs sécurité et aux décideurs souhaitant disposer d'une vision claire et justifiée de l'environnement numérique de l'entreprise.

I. Contexte et objectifs

L'entreprise concernée par ce projet est nouvellement installée et ne dispose, à ce stade, d'aucune Politique de Sécurité des Systèmes d'Information (PSSI), ni d'infrastructure technique préexistante. Ce contexte de départ vierge constitue à la fois une opportunité stratégique, permettant de concevoir une architecture propre, cohérente et conforme dès l'origine et un défi opérationnel, dans la mesure où toutes les briques du système doivent être pensées, déployées et sécurisées sans héritage technique ni documentation préalable.

Dans ce cadre, les priorités exprimées par l'entreprise sont claires et alignées avec les principes fondamentaux de la cybersécurité :

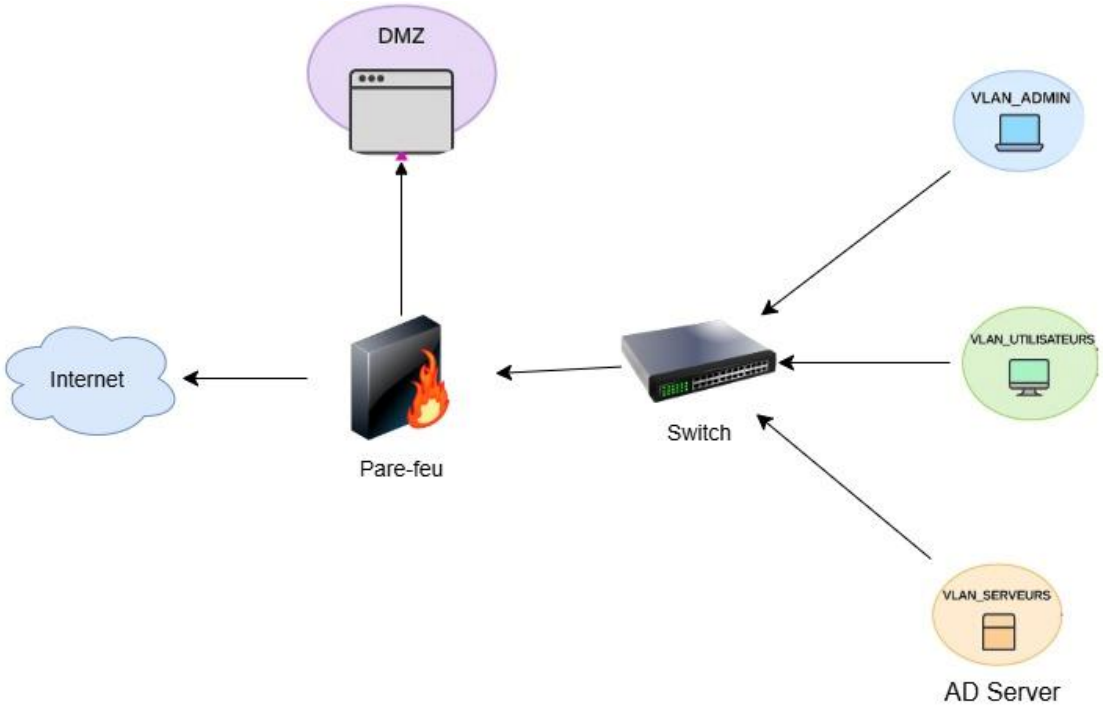
- **Confidentialité** : garantir que les données sensibles ne soient accessibles qu'aux utilisateurs autorisés, notamment par le filtrage des flux, l'authentification forte et la gestion centralisée des identités.
- **Intégrité** : assurer que les données et les configurations ne puissent être altérées de manière non autorisée, en appliquant des restrictions de privilèges, des politiques de groupe (GPO) et des mécanismes de contrôle d'accès.
- **Disponibilité** : maintenir l'accès aux services critiques en toutes circonstances, notamment par la redondance des composants, la segmentation réseau et la supervision des flux.
- **Traçabilité** : permettre l'audit des actions et des événements, via la centralisation des journaux, l'activation des stratégies d'audit et la journalisation des accès.

Face à ces exigences, le projet vise à concevoir une infrastructure virtualisée, segmentée et sécurisée, reposant sur les principes suivants :

- **Déploiement d'un pare-feu Linux multi-interface**, assurant le cloisonnement des VLAN (DMZ, Serveurs, Administration, Utilisateurs) et le filtrage des flux inter-segments.
- **Mise en place d'un serveur web sécurisé (Linux/Apache)**, accessible en HTTPS depuis l'extérieur et l'intérieur du réseau, avec gestion fine des permissions et des certificats.

- **Intégration d'un domaine Active Directory (Windows Server)**, assurant la gestion centralisée des utilisateurs, des machines et des droits, avec application de GPO conformes aux recommandations de l'ANSSI.
- **Configuration de postes clients Windows 11**, intégrés au domaine, sécurisés par le principe du moindre privilège, et supervisés via des outils d'administration à distance.
- **Documentation complète et transférable**, incluant les scripts, les configurations, les schémas d'architecture, les plans d'adressage, les fiches de validation et les captures d'écran.

L'objectif final est de livrer une infrastructure opérationnelle, conforme aux standards de sécurité, et accompagnée d'un dossier technique clair, structuré et exploitable par tout administrateur en charge de sa maintenance ou de son évolution.



II. Architecture cible

L'architecture cible du système d'information repose sur une infrastructure entièrement virtualisée, segmentée en plusieurs zones fonctionnelles, chacune associée à un VLAN spécifique. Cette segmentation vise à limiter les surfaces d'attaque, à cloisonner les flux réseau,

et à faciliter l'application de politiques de sécurité différenciées selon les rôles des machines. Le déploiement est réalisé à l'aide d'un hyperviseur de type 2 (VirtualBox ou VMware), permettant une flexibilité dans la gestion des machines virtuelles et une reproductibilité du scénario.

1. Composition de l'infrastructure

L'environnement cible comprend les éléments suivants :

- **Un pare-feu Linux (Ubuntu)** configuré avec cinq interfaces réseau, jouant le rôle de routeur et de filtre entre les VLAN.
- **Un serveur web Linux (Apache)** situé en DMZ, accessible en HTTPS depuis l'extérieur et l'intérieur du réseau.
- **Un serveur Windows Server 2025**, promu en contrôleur de domaine Active Directory, assurant la gestion centralisée des utilisateurs, des machines et des politiques de sécurité.
- **Un poste d'administration Windows 11**, réservé aux tâches de supervision, configuration et maintenance.
- **Un poste utilisateur Windows 11**, intégré au domaine, utilisé pour les opérations courantes.
- **Un téléphone VoIP par utilisateur**, connecté au réseau via le VLAN utilisateur.

2. Segmentation réseau et VLAN

La segmentation est réalisée selon les principes de sécurité en profondeur. Chaque rôle est isolé dans un VLAN dédié :

VLAN	Rôle	Exemple IP	Interface VM
WAN	Accès Internet simulé	DHCP ou NAT	enp0s3
DMZ	Serveur web Linux	192.168.10.10	enp0s18
SERVEURS	Serveur Windows AD/DNS	192.168.20.10	enp0s9

ADMINISTRATION	Poste d'administration	192.168.30.10	enp0s17
UTILISATEURS	Postes clients + VoIP	192.168.40.10	enp0s16

Chaque interface du pare-feu est associée à un VLAN, et configurée avec un mode réseau spécifique (pont, NAT, interne) selon les besoins de communication et d'isolation. L'attribution des adresses IP est réalisée manuellement via Netplan (Linux) ou via les outils Windows Server.

3. Justification des choix techniques

- **Virtualisation** : permet de simuler un environnement complet, reproductible et modulaire, facilitant les tests et la maintenance.
- **Segmentation par VLAN** : réduit les risques de latéralisation en cas de compromission, et permet un contrôle fin des flux.
- **Pare-feu multi-interface** : centralise le filtrage, le routage et la journalisation des flux inter-VLAN.
- **Active Directory** : assure une gestion centralisée des identités, des droits et des politiques de sécurité.
- **HTTPS sur Apache** : garantit la confidentialité des échanges avec le serveur web, même en environnement local.

III. Segmentation logique : Mise en place des VLAN dans Cisco Packet Tracer

La segmentation réseau constitue une mesure de sécurité fondamentale dans toute architecture d'entreprise. Elle permet de cloisonner les flux, de limiter les déplacements latéraux en cas de compromission, et de renforcer l'application du principe du moindre privilège. Dans le cadre de ce projet, la segmentation est réalisée à l'aide de VLAN configurés sur un switch Cisco simulé dans l'environnement Cisco Packet Tracer. Cette étape vise à isoler les différentes zones fonctionnelles du système d'information : DMZ, serveurs internes, postes

utilisateurs et administration, en leur attribuant des VLAN distincts, conformément au plan d'adressage défini précédemment.

1. Objectifs de la segmentation

Les Objectifs de la segmentation sont les suivants :

- **Isoler les flux réseau** entre les zones critiques (serveurs, DMZ) et les zones exposées (utilisateurs, Internet)
- **Réduire la surface d'attaque** en limitant la portée des broadcasts et des attaques ARP
- **Préparer le filtrage inter-VLAN** via le pare-feu Ubuntu
- **Structurer le réseau** pour faciliter la maintenance, l'audit et l'évolution

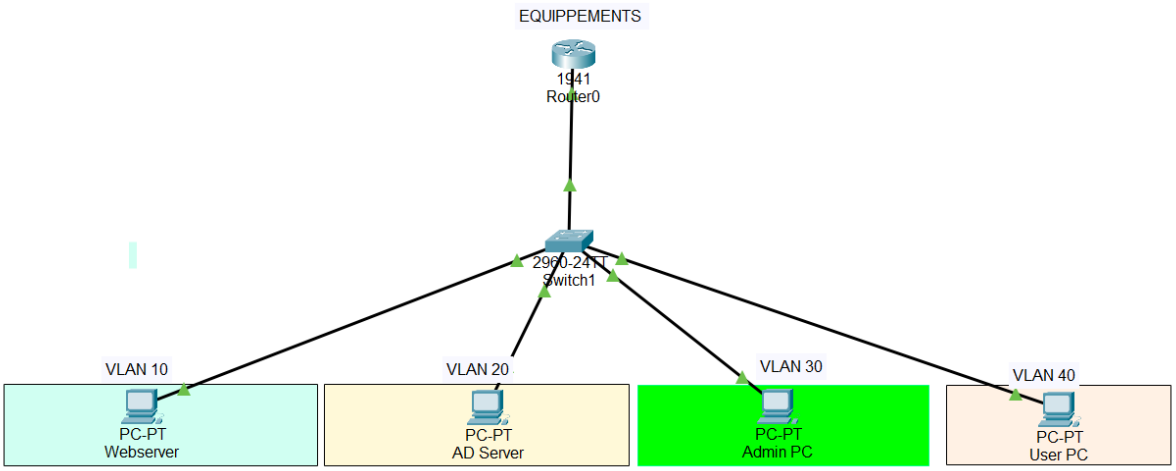
2. Définition des VLAN

Les VLANs ont été définis selon les usages métier suivants :

VLAN ID	Nom	Usage métier
10	DMZ	Serveur Web
20	SERVEURS	Active Directory / DNS
30	ADMINISTRATION	Poste d'administration
40	UTILISATEURS	Postes clients + VoIP

Chaque VLAN est associé à une plage IP dédiée, une interface du pare-feu, et un port spécifique sur le switch.

3. Ajout des équipements et configuration du switch Cisco



❖ **Ajout des équipements**

- 1 Switch (2960)
- 1 Routeur
- 4 PC (1 par VLAN)
- Câbles droits pour les connexions

❖ **Création des VLAN sur le switch**

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name DMZ
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name SERVEURS
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name ADMIN
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name UTILISATEURS
```

❖ **Affectation des ports**

```
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#swithport mode access
                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode access
Switch(config-if)#switchport access wlan 10
                                 ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport access vlan 10
Switch(config-if)#description "Webserver"
Switch(config-if)#int fa0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#description "AD Server"
Switch(config-if)#int fa0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#description "Admin PC"
Switch(config-if)#int fa0/4
Switch(config-if)#switchport access vlan 40
Switch(config-if)#description "User PC"
Switch(config-if)#
```

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/5 - 23
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively dow
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively dow
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively dow
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively dow
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively dow
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively do
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively do
Switch(config-if-range)#description "Ports dsactivs pour securite"
```

- **Configuration du port trunk**

```
Switch(config-if-range)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport port-secutity
                                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

- **Plan d'adressage simulé**

VLAN	Adresse réseau	Exemple IP	Passerelle
VLAN 10 (DMZ)	192.168.10.0/24	192.168.10.10	192.168.10.1
VLAN 20	192.168.20.0/24	192.168.20.10	192.168.20.1
VLAN 30	192.168.30.0/24	192.168.30.10	192.168.30.1
VLAN 40	192.168.40.0/24	192.168.40.10	192.168.40.1

IV. Mesures de sécurité appliquées

❖ **Désactivation des ports inutilisés**

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/5 - 23
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administrativel

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administrativel

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administrativel

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administrativel

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administrativel

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administrative

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administrative

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administrative

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administrative
```

Nous l'avons fait car cela empêche tout branchement non autorisé sur les ports libres.

❖ **Limitation du nombre d'équipements par port (Port Security)**

L'objectif ici, est d'empêcher les attaques de type ARP spoofing ou le branchement de plusieurs appareils sur un même port.

```
Switch(config-if-range)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport port-secutity
                                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Dans la continuité de la segmentation réseau réalisée via la configuration des VLAN dans Cisco Packet Tracer, l'étape suivante consiste à mettre en œuvre le routage inter-VLAN afin de permettre la communication contrôlée entre les différentes zones fonctionnelles du système d'information. Pour ce faire, nous adoptons la méthode classique dite ***router-on-a-stick***, largement utilisée dans les environnements pédagogiques et professionnels. Cette approche repose sur l'utilisation d'une seule interface physique du routeur, laquelle est

subdivisée en plusieurs sous-interfaces logiques, chacune associée à un VLAN spécifique. Chaque sous-interface est configurée avec une adresse IP correspondant à la passerelle du VLAN concerné, ce qui permet au routeur de gérer le trafic entre les segments tout en conservant une isolation logique. L'objectif de cette configuration est de permettre la communication entre les VLAN DMZ, SERVEURS, ADMINISTRATION et UTILISATEURS, tout en maintenant une maîtrise fine des flux et une traçabilité des échanges inter-zones.

❖ Étapes de configuration du routeur

La première étape de la configuration du routage inter-VLAN consiste à établir la liaison physique entre le switch et le routeur. Pour ce faire, le port FastEthernet 0/24 du switch, préalablement configuré en mode trunk afin de transporter les trames de plusieurs VLAN, est relié au port GigabitEthernet 0/0 du routeur à l'aide d'un câble droit. Cette connexion constitue le point d'entrée unique du trafic inter-VLAN vers le routeur, conformément à la méthode ***router-on-a-stick***. Elle permet d'acheminer les trames VLAN taguées vers les sous-interfaces logiques du routeur, qui assurera ensuite le routage entre les différents segments du réseau.

❖ Accéder au routeur et créer les sous-interfaces VLAN

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

L'encapsulation utilisée sur les sous-interfaces du routeur est de type **IEEE 802.1Q (dot1Q)**, ce qui permet d'identifier de manière explicite le VLAN auquel chaque trame appartient. Cette encapsulation est indispensable dans le cadre d'un routage inter-VLAN via une interface trunk, car elle assure la reconnaissance des balises VLAN par le routeur. Par ailleurs, **chaque sous-interface est configurée avec une adresse IP spécifique**, correspondant

à la passerelle du VLAN concerné. Cette adresse joue un rôle central dans le routage, puisqu'elle représente le point de sortie logique pour les machines du VLAN, et permet au routeur de gérer les échanges entre segments tout en maintenant une isolation fonctionnelle. Cette configuration garantit une communication fluide entre les VLANs tout en respectant les principes de sécurité et de traçabilité du projet.

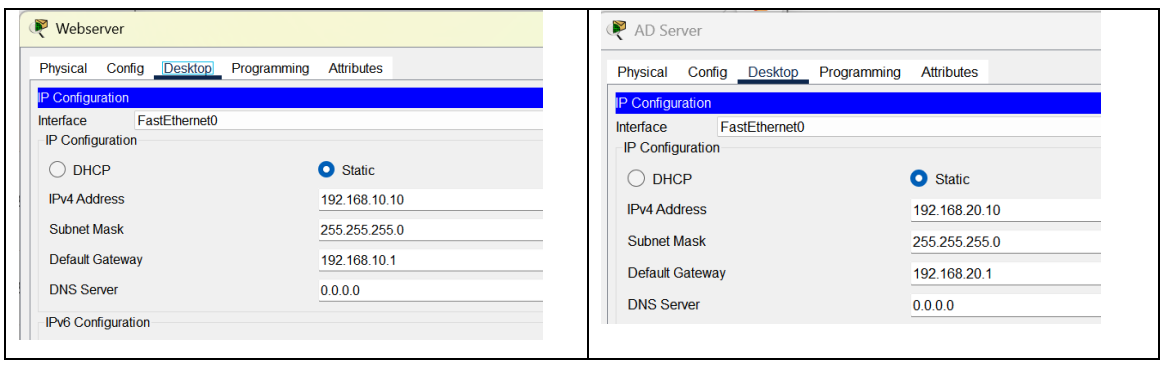
❖ Activer l'interface physique

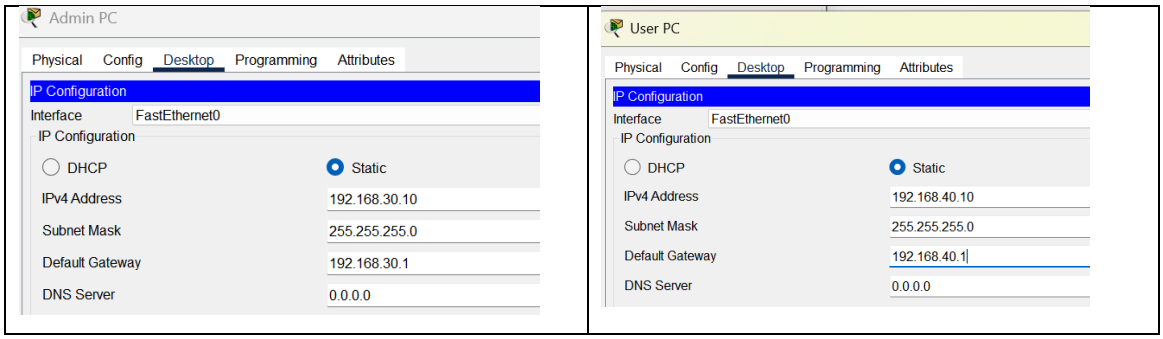
```
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
```

❖ Vérification de la configuration

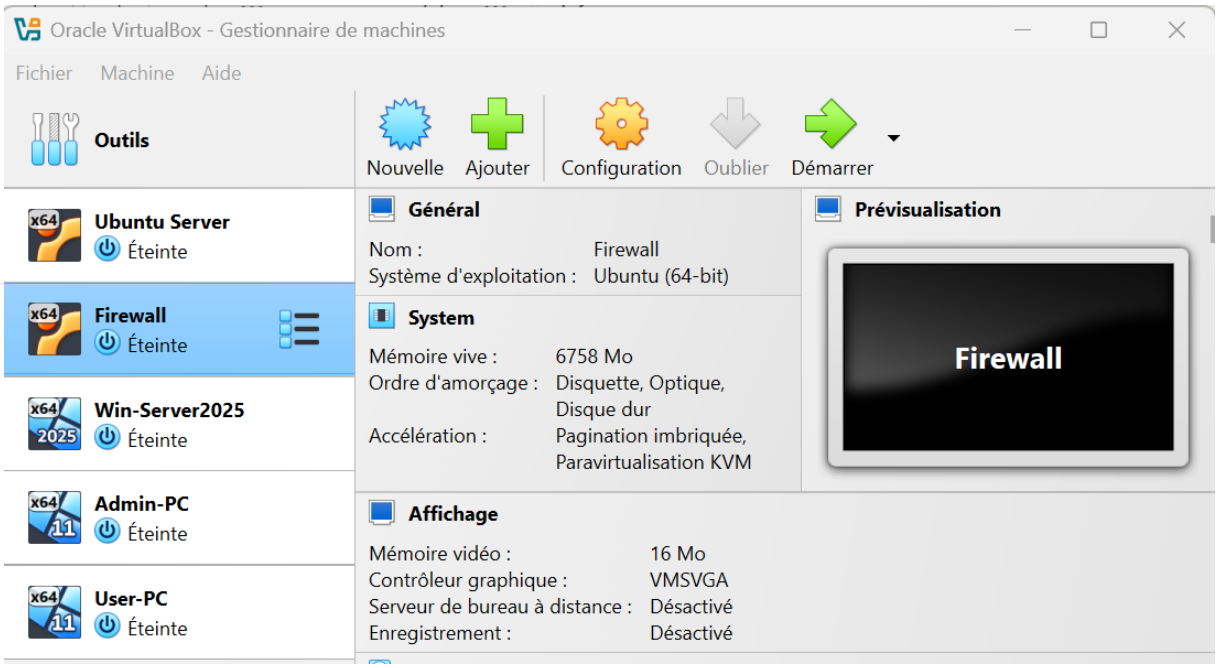
```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.40  192.168.40.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
Router>
```

❖ Configuration des PC





V. Création des machines virtuelles



La mise en place des machines virtuelles constitue une étape centrale dans le déploiement de l'infrastructure cible. Elle permet de simuler un environnement complet, cohérent et segmenté, tout en assurant la flexibilité nécessaire aux tests, à la configuration et à la sécurisation des services. Les machines ont été créées dans VirtualBox (ou VMware selon la configuration locale), en respectant les contraintes de performance de la machine hôte, sans nécessairement suivre les préconisations maximales du cahier des charges.

1. Prérequis techniques

Avant la création des machines, les éléments suivants ont été validés :

- L'architecture cible a été définie
- Le plan d'adressage est opérationnel

- L'hyperviseur VirtualBox est installé et fonctionnel
- Les images ISO des systèmes d'exploitation ont été récupérées :
  - Ubuntu Server (pour le pare-feu et le serveur web)
  - Windows Server 2025 (version d'évaluation 180 jours)
  - Windows 11 (version d'évaluation 90 jours)

2. Machines virtuelles créées

Nom VM	Système d'exploitation	Rôle	VLAN associé	Adresse IP
VM-Firewall	Ubuntu Server	Pare-feu multi-VLAN	Trunk	5 interfaces IP
VM-WebServer	Ubuntu Server	Serveur Web (Apache)	DMZ	192.168.10.10
VM-AD-DNS	Windows Server 2025	AD/DNS	SERVEURS	192.168.20.10
VM-Admin	Windows 11	Poste d'administration	ADMINISTRATION	192.168.30.10
VM-User	Windows 11	Poste utilisateur	UTILISATEURS	192.168.40.10

---

3. Paramètres techniques des VM

Les ressources ont été ajustées selon la capacité de la machine hôte :

VM	RAM (Mo)	CPU	Disque (Go)	Cartes réseau activées
VM-Firewall	1024	1	10	5 interfaces (VLANs)
VM-WebServer	1024	1	10	1 interface (DMZ)
VM-AD-DNS	2048	2	30	1 interface (SERVEURS)

VM-Admin	2048	2	25	1 interface (ADMIN)
VM-User	2048	2	25	1 interface (UTILISATEURS)

4. Ajout de la cinquième interface réseau sur le pare-feu

Dans le cadre de la segmentation réseau, chaque VLAN est associé à une interface dédiée sur le pare-feu Ubuntu. Après avoir configuré les quatre premières interfaces pour les VLAN DMZ, SERVEURS, ADMINISTRATION et WAN, l'ajout d'une **cinquième interface** est nécessaire pour intégrer le VLAN UTILISATEURS (VLAN 40), qui regroupe les postes clients et les équipements VoIP. Nous avons réalisé cela en ligne de commande à l'aide de l'outil **VBoxManage**, permettant une configuration précise et scriptable de la machine virtuelle. L'interface est ajoutée en tant que réseau interne, avec un nom cohérent (**VLAN40**) pour assurer l'isolation logique et la compatibilité avec les autres machines du segment.

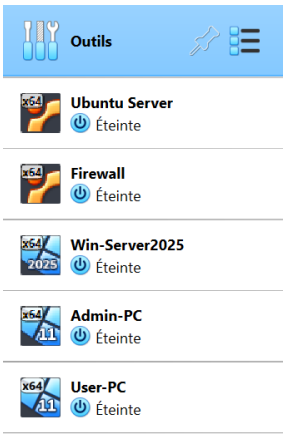
La commande utilisée est la suivante :

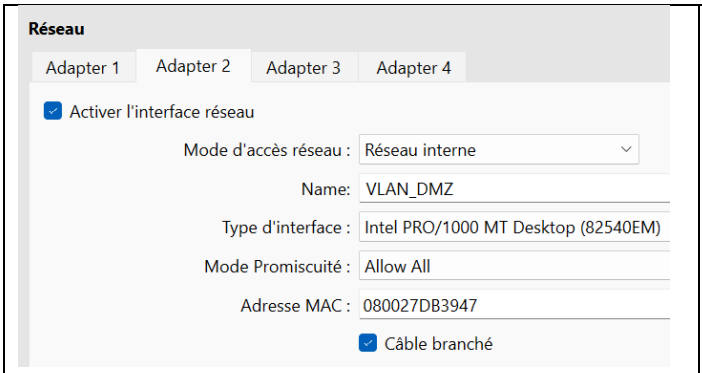
```
PS C:\Users\PC> VBoxManage modifyvm "Firewall" --nic
5 intnet
PS C:\Users\PC> VBoxManage modifyvm "Firewall" --int
net5 "VLAN_UTILISATEURS"
PS C:\Users\PC>
```

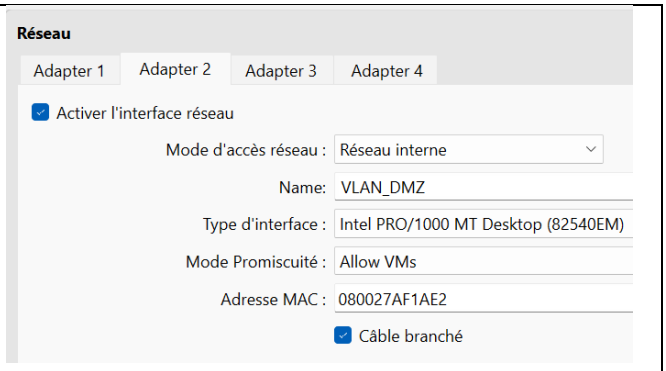
Cette instruction a modifié la machine virtuelle nommée "**VM-Firewall**" en lui ajoutant une cinquième carte réseau (**nic5**) configurée en mode **réseau interne** (**intnet**) et associée au réseau logique nommé "**VLAN40**". Ce réseau interne est ensuite utilisé pour connecter le poste utilisateur Windows 11 au pare-feu, via le VLAN 40. Une fois l'interface ajoutée, elle a été détectée dans Ubuntu sous le nom **enp0s16.**L'ajout de cette interface complète la structure logique du pare-feu, qui dispose désormais d'une interface dédiée pour chaque segment fonctionnel, conformément à l'architecture cible du projet.

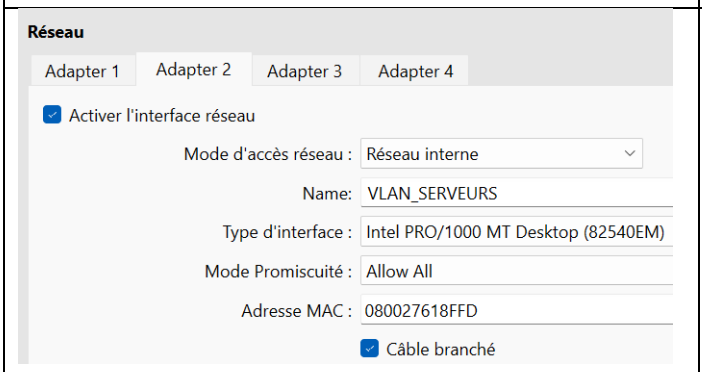
5. Segmentation réseau

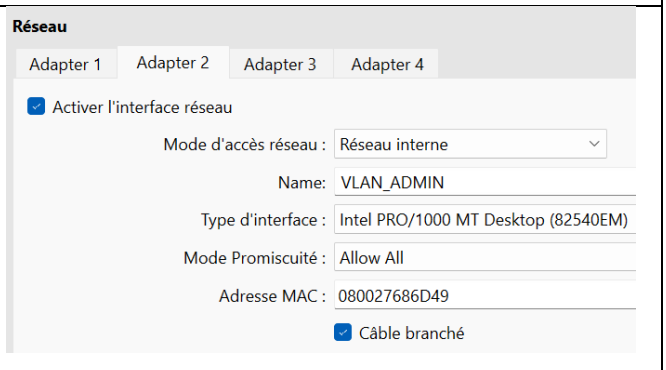
Cela s'est fait dans l'ordre :

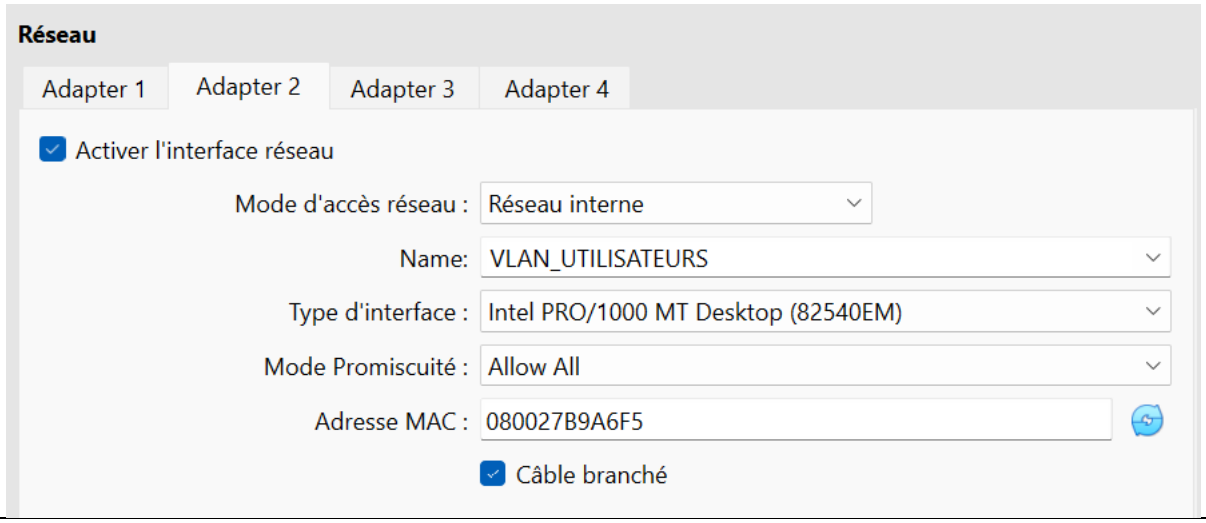

Outils
Ubuntu Server
Éteinte
Firewall
Éteinte
Win-Server2025
Éteinte
Admin-PC
Éteinte
User-PC
Éteinte


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau interne
Name: VLAN_DMZ
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 080027DB3947
Câble branché


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau interne
Name: VLAN_DMZ
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow VMs
Adresse MAC : 080027AF1AE2
Câble branché

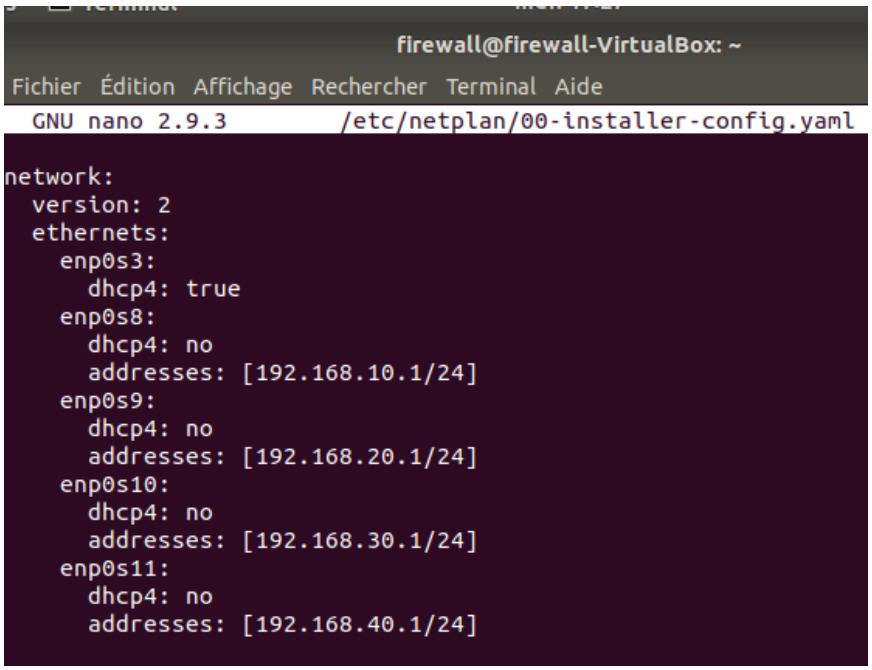

Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau interne
Name: VLAN_SERVEURS
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 080027618FFD
Câble branché


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau interne
Name: VLAN_ADMIN
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 080027686D49
Câble branché


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau interne
Name: VLAN_UTILISATEURS
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 080027B9A6F5
Câble branché

VI. Configuration du pare-feu Ubuntu et Filtrage inter-VLAN avec iptables

Nous avons débuté par l'adressage du pare-feu **via Netplan** et appliqué grâce à la commande : **« sudo netplan apply »**



Le pare-feu Ubuntu constitue le point névralgique de la sécurité réseau de l'infrastructure. Il assure à la fois le **routage inter-VLAN** et le **filtrage des flux** entre les différentes zones fonctionnelles du système d'information. Sa configuration repose sur l'activation du routage IP, la définition explicite des interfaces réseau, et la mise en œuvre de règles iptables strictes, conformes aux principes de cloisonnement, de traçabilité et de sécurité en profondeur.

1. Objectifs

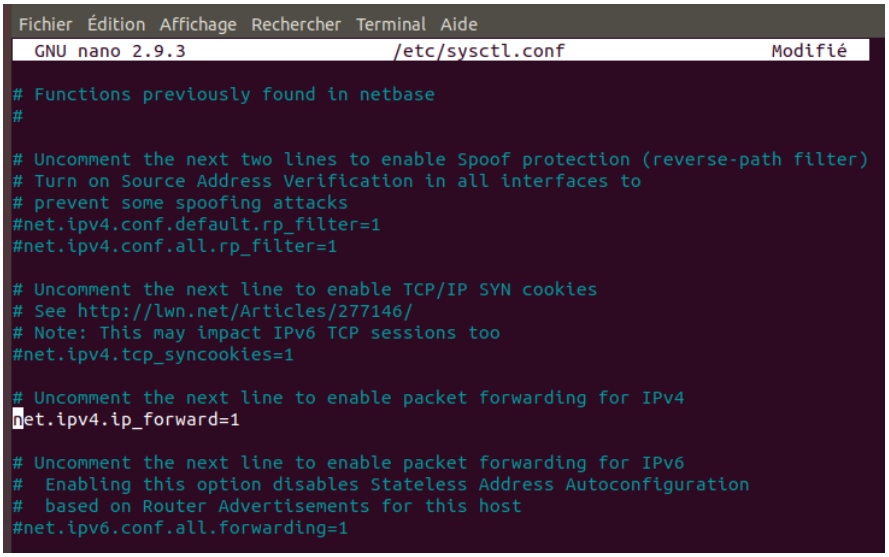
Les objectifs sont les suivants :

- Activer le routage IP entre les VLANs
- Contrôler les flux inter-segments selon les rôles métier
- Bloquer par défaut tout trafic non autorisé
- Journaliser les paquets rejetés pour supervision
- Préparer l'intégration de mesures de sécurité complémentaires

2. Activation du routage IP

Le routage IP est activé de manière persistante via la modification du fichier **/etc/sysctl.conf** :

echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p



Cette commande permet au noyau Linux de transférer les paquets entre interfaces réseau, condition indispensable au fonctionnement du routage inter-VLAN.

3. Politique de sécurité par défaut

Le pare-feu applique une politique restrictive dès le démarrage :

- **INPUT :** seuls les paquets explicitement autorisés sont acceptés
- **FORWARD :** les flux inter-VLAN sont filtrés selon des règles précises
- **OUTPUT :** les connexions sortantes depuis le pare-feu sont autorisées

```
    link/ether 08:00:27:54:e9:58 brd ff:ff:ff:ff:ff:ff
firewall@firewall-VirtualBox:~$ sudo nano /etc/netplan/00-installer-config.yaml
[sudo] Mot de passe de firewall :
firewall@firewall-VirtualBox:~$ sudo netplan apply
firewall@firewall-VirtualBox:~$ sudo nano /etc/sysctl.conf
firewall@firewall-VirtualBox:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
firewall@firewall-VirtualBox:~$ sudo iptables -P INPUT ACCEPT
firewall@firewall-VirtualBox:~$ sudo iptables -P FORWARD ACCEPT
firewall@firewall-VirtualBox:~$ sudo iptables -P OUTPUT ACCEPT
firewall@firewall-VirtualBox:~$ sudo apt install iptables-persistent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  netfilter-persistent
Les NOUVEAUX paquets suivants seront installés :
  iptables-persistent netfilter-persistent
0 mis à jour, 2 nouvellement installés, 0 à enlever et 707 non mis à jour.
Il est nécessaire de prendre 13,1 ko dans les archives.
Après cette opération, 81,9 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de:1 http://fr.archive.ubuntu.com/ubuntu bionic-updates/universe amd6
4 netfilter-persistent all 1.0.4+nmu2ubuntu1.1 [6 748 B]
```

4. Règles de filtrage inter-VLAN

Les règles suivantes ont été définies pour autoriser uniquement les flux nécessaires à l'infrastructure :

```
firewall@firewall-VirtualBox: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
  GNU nano 2.9.3                /root/iptables.sh                Modifié

#!/bin/bash

echo " Réinitialisation des règles existantes"
iptables -F  # Supprime toutes les règles de filtrage
iptables -X  # Supprime toutes les chaînes personnalisées

echo "  Application des politiques par défaut"
iptables -P INPUT DROP    # Bloque toutes les connexions entrantes par défaut
iptables -P FORWARD DROP  # Bloque le routage entre interfaces par défaut
iptables -P OUTPUT ACCEPT # Autorise toutes les connexions sortantes

echo "🔌 Règles système de base"
iptables -A INPUT -i lo -j ACCEPT  # Autorise le trafic local (loopback)
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  # Auto$
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  # Au$
iptables -A INPUT -p icmp -j ACCEPT  # Autorise les pings vers le pare-feu
iptables -A FORWARD -p icmp -j ACCEPT  # Autorise les pings entre VLANs

echo "🌐 Accès Internet depuis VLAN_UTILISATEURS"
iptables -A FORWARD -s 192.168.40.0/24 -o enp0s3 -p tcp --dport 443 -j ACCEPT $

echo "🌍 Accès au site web hébergé en DMZ"
iptables -A FORWARD -i enp0s3 -d 192.168.10.10 -p tcp --dport 443 -j ACCEPT  #$
```

Pour assurer la traçabilité des flux bloqués, nous avons ajouté une règle de journalisation été ajoutée grâce à la commande : **iptables -A FORWARD -j LOG --log-prefix "DROP-FORWARD: "** et les journaux sont consultables via la commande :

sudo tail -f /var/log/syslog . Et enfin, Les règles sont sauvegardées pour être restaurées automatiquement au démarrage grâce à la commande inséré à la fin du fichier iptables :

- **sudo apt install iptables-persistent**
- **sudo netfilter-persistent save**

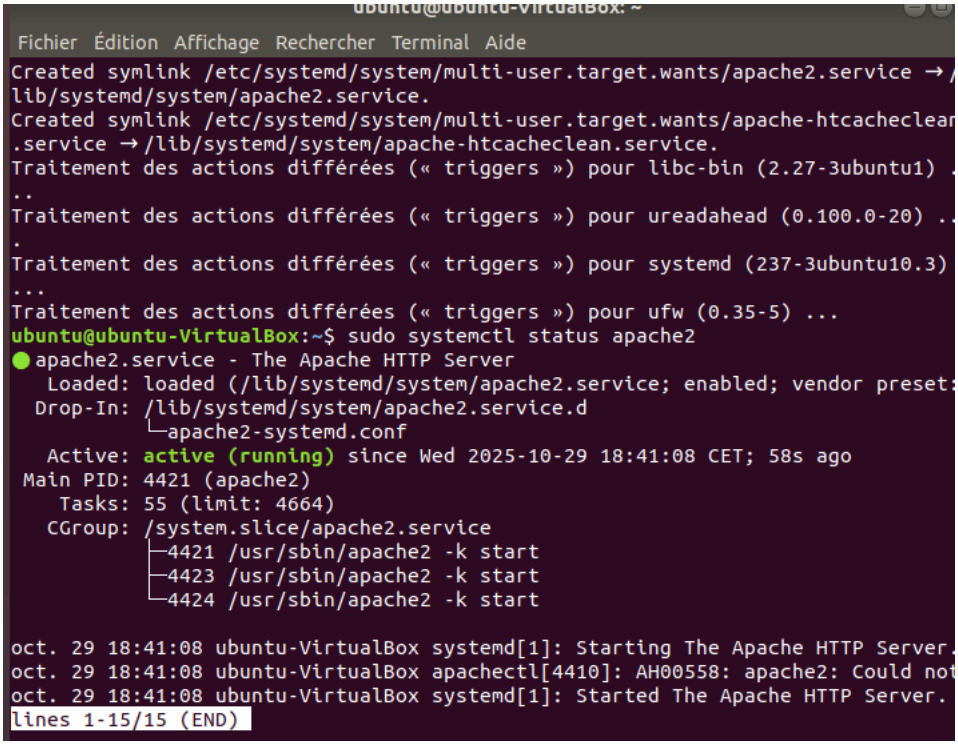
VII. Installation et sécurisation du serveur Linux (Apache)

Il était question, d'installer le serveur web Apache sur la machine Ubuntu située dans la DMZ, puis de le sécuriser selon les recommandations de l'ANSSI. Nous avons procédé à une installation minimale, à la création d'un utilisateur dédié, à la mise en place du chiffrement HTTPS, et à la désactivation des modules non essentiels.

1. Installation du serveur Apache

Nous avons installé Apache via le gestionnaire de paquets grâce aux commandes :

sudo apt update && sudo apt install apache2 -y puis, le service a été démarré et vérifié avec : **sudo systemctl status apache2**



2. Personnalisation de la page d'accueil Apache

Il était question, dans cette étape, de remplacer la page par défaut d'Apache par une page personnalisée, afin de donner une identité propre au serveur web et de mettre en valeur

le contexte académique et pédagogique du projet. Nous avons donc modifié le fichier index.html situé dans le répertoire /var/www/html pour afficher une page adaptée. Nous avons procédé comme suite :

- Nous avons conservé une copie de la page initiale afin de pouvoir la restaurer si nécessaire, puis nous avons ensuite créé un nouveau fichier index.html

```
root@ubuntu-VirtualBox:/home/ubuntu# cd /var/www/html
root@ubuntu-VirtualBox:/var/www/html# sudo mv index.html index.html.bak
root@ubuntu-VirtualBox:/var/www/html# sudo nano index.html
root@ubuntu-VirtualBox:/var/www/html#
```

- Il ne restait plus qu'ajouter, le contenu suivant :

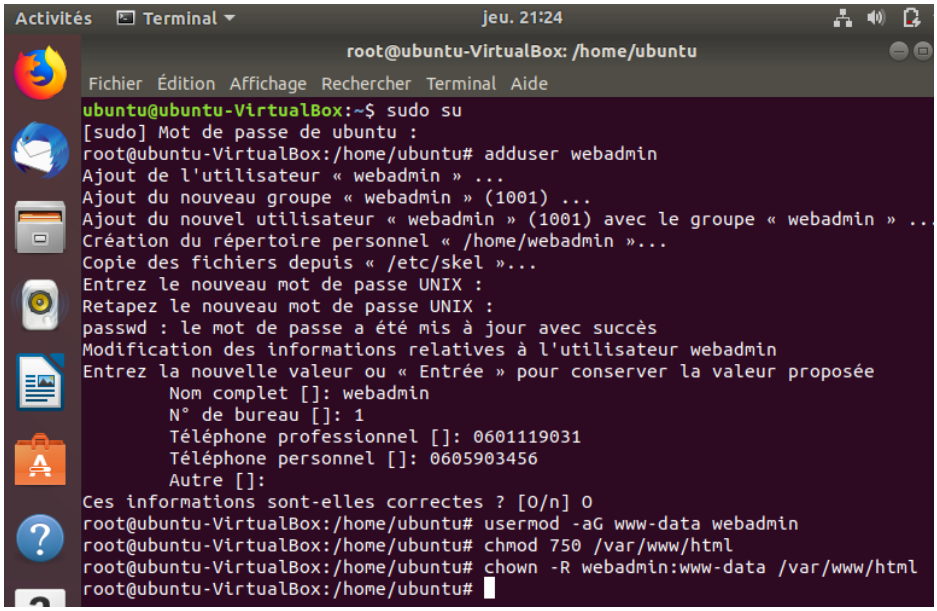
3. Vérification de l'affichage

Depuis un de nos poste client, nous avons ouvert un navigateur et saisi l'URL :
« **https://mondomaine.local** » et avons pu voir le résultat suivant :

4. Création de l'utilisateur webadmin

Un utilisateur dédié à l'administration du site web a été créé grâce à :

- **sudo adduser webadmin**
- **sudo usermod -aG www-data webadmin**



Nous avons volontairement limité ses droits : Pas d'accès sudo, accès restreint au répertoire /var/www/html, aucune permission sur les fichiers système.

```
root@ubuntu-VirtualBox:/home/ubuntu# usermod -aG www-data webadmin
root@ubuntu-VirtualBox:/home/ubuntu# chmod 750 /var/www/html
root@ubuntu-VirtualBox:/home/ubuntu# chown -R webadmin:www-data /var/www/html
root@ubuntu-VirtualBox:/home/ubuntu# a2dismod autoindex
WARNING: The following essential module will be disabled.
This might result in unexpected behavior and should NOT be done
unless you know exactly what you are doing!
 autoindex

To continue type in the phrase 'Yes, do as I say!' or retry by passing '-f': Ye
s
Aborting
root@ubuntu-VirtualBox:/home/ubuntu# a2dismod status
Module status disabled.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu-VirtualBox:/home/ubuntu# systemctl restart apache2
root@ubuntu-VirtualBox:/home/ubuntu#
```

Cette mesure nous a permis de cloisonner les privilèges et de réduire les risques en cas de compromission.

3. Mise en place du chiffrement HTTPS

Il était impératif de sécuriser les échanges entre clients et serveur. Nous avons généré un certificat auto-signé :

```
root@ubuntu-VirtualBox:/home/ubuntu# openssl req -x509 -nodes -days 365 -newkey
 rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/ap
ache-selfsigned.crt
Generating a 2048 bit RSA private key
.....................................................................
.....................+++++
.....................................................+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:HERAULT
Locality Name (eg, city) []:Montpellier
Organization Name (eg, company) [Internet Widgits Pty Ltd]:openclassroom
Organizational Unit Name (eg, section) []:eg
Common Name (e.g. server FQDN or YOUR name) []:yebga brayan
Email Address []:yebgabrayan@gmail.com
root@ubuntu-VirtualBox:/home/ubuntu#
```

Puis nous avons activé le module SSL et configuré le virtual host sécurisé :

```
root@ubuntu-VirtualBox:/home/ubuntu# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu-VirtualBox:/home/ubuntu# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@ubuntu-VirtualBox:/home/ubuntu#
```

Le serveur est désormais accessible en HTTPS sur le port 443, avec un certificat valide.

VIII. Sécurisation du domaine Active Directory

Il était question, de renforcer la sécurité du domaine Active Directory hébergé sur le serveur Windows Server 2025. Ce domaine constitue le socle de l'authentification centralisée, de la gestion des identités et des politiques de sécurité. Nous avons mis en œuvre une série de mesures visant à limiter les privilèges, à durcir les accès, à appliquer des stratégies conformes aux recommandations de l'ANSSI, et à désactiver les services non essentiels.

1. Installation du rôle AD DS

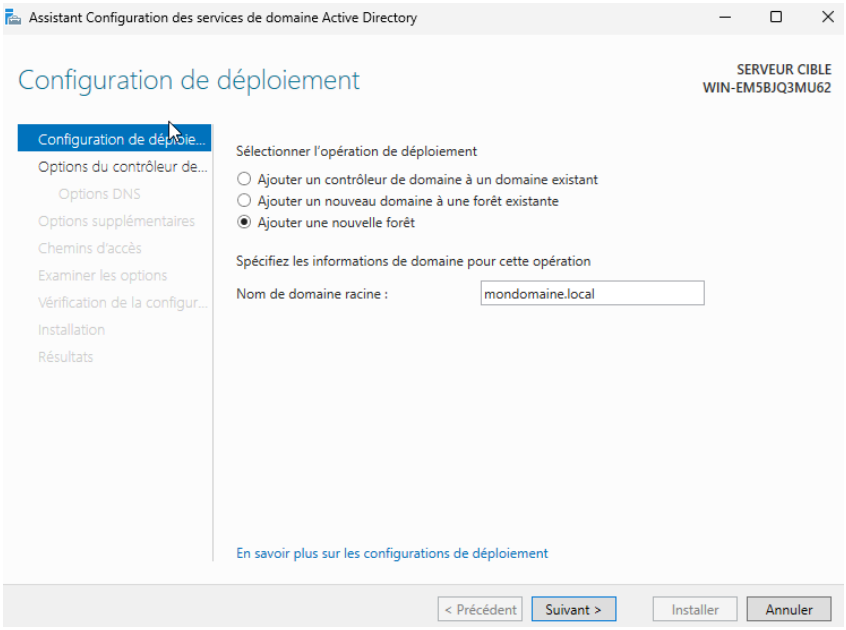
L'installation a été réalisée via l'interface graphique Server Manager :

- Ajout du rôle Active Directory
- Menu : Manage → Add Roles and Features
- Sélection du rôle : Active Directory Domain Services
- Validation des dépendances (notamment DNS)
- Lancement de l'installation

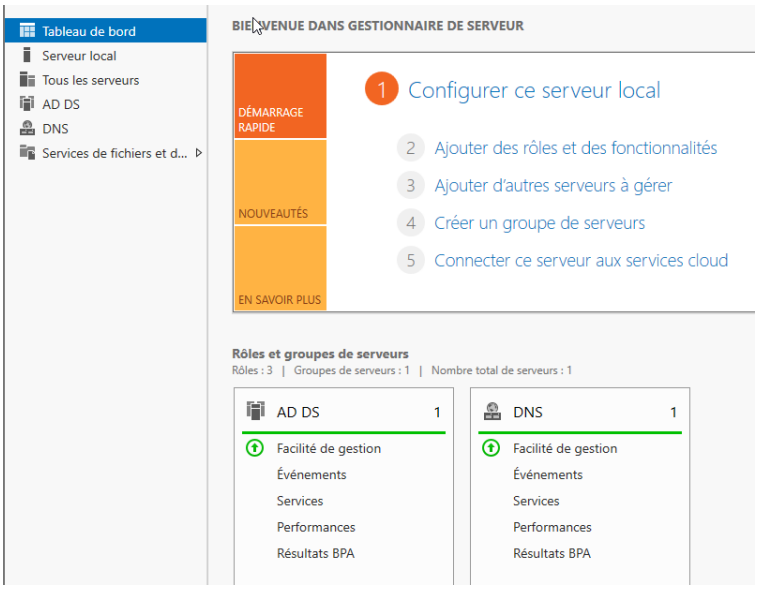
2. Promotion en contrôleur de domaine

- Une fois le rôle installé, nous avons cliqué sur « ***Promote this server to a domain controller*** »
- Choix : *Créer une nouvelle forêt*

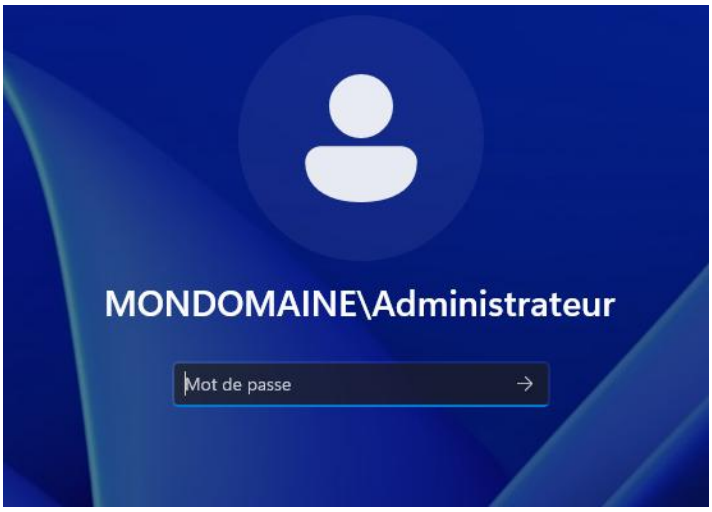
- Nom du domaine : **mondomaine.local**



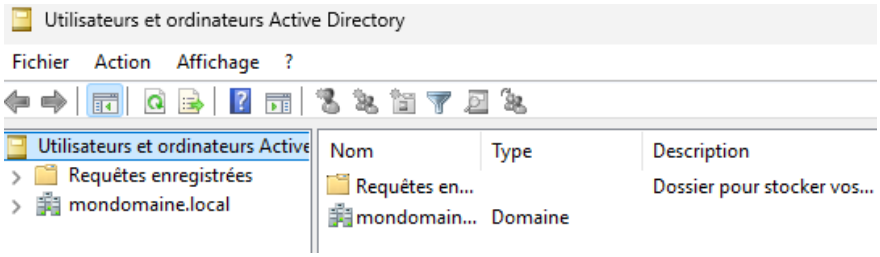
- Définition du mot de passe DSRM (Directory Services Restore Mode)



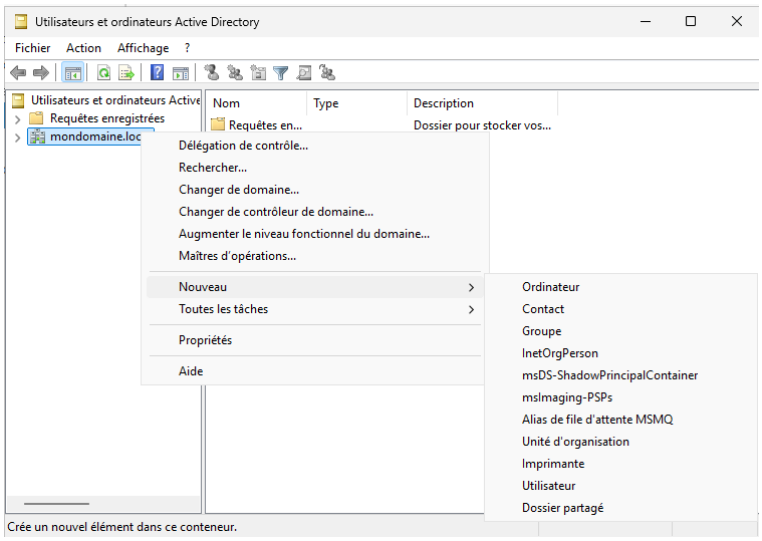
Nous avons observé un changement sur l'écran d'accueil de Windows notamment, le nom du domaine « **mondomaine** » devant le nom du serveur.



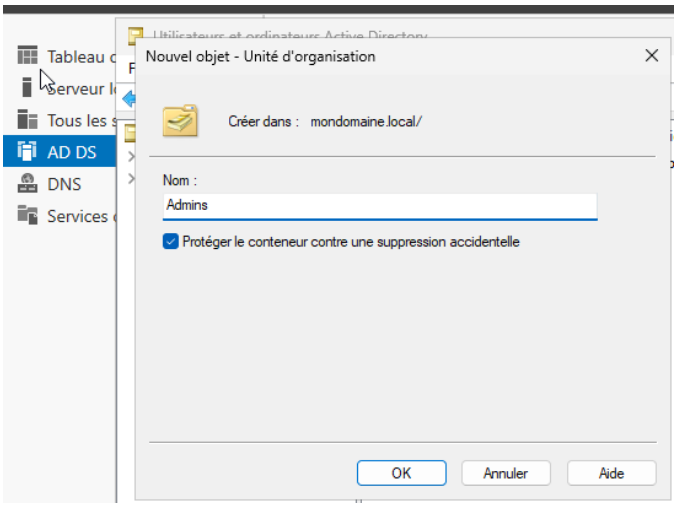
Maintenant, il était question de crée une unité d'organisation et pour cela, nous devons aller dans « **Utilisateurs et ordinateurs Active Directory** »



Nous avons fait un clic droit sur notre nom de domaine « **mondomaine »,** puis sur « **Nouveau »** et enfin sur « **Unité d'organisation ».**

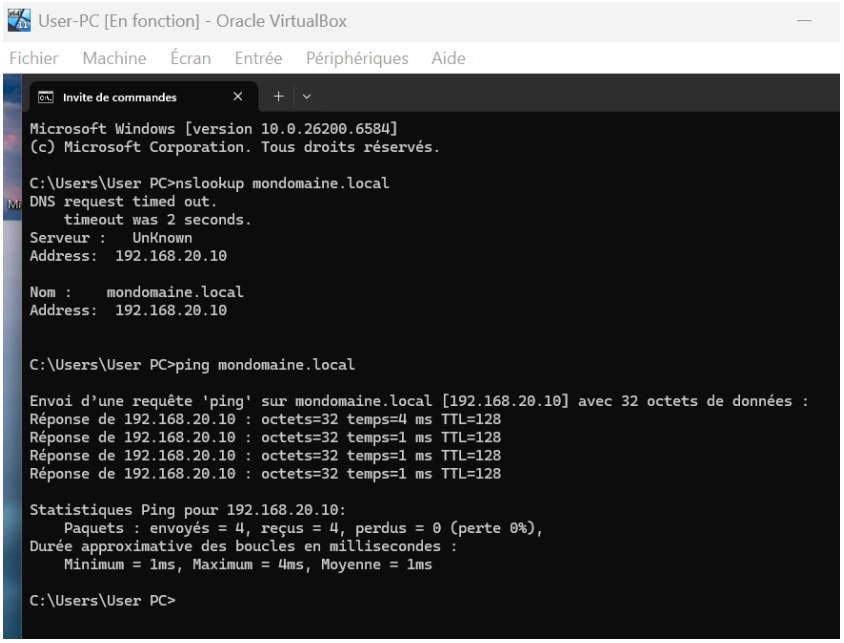


Il ne restait plus qu'à créer de nouveau objet d'unité d'organisation à savoir :



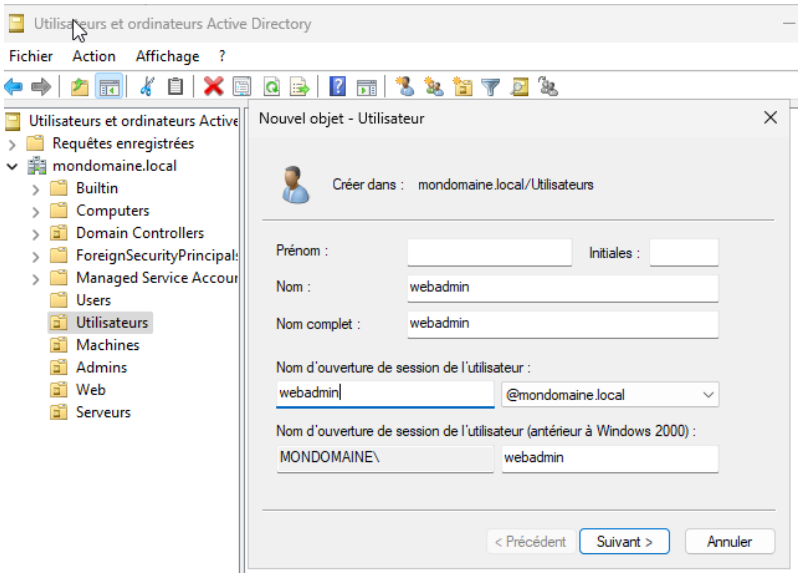
5. Vérification des configuration DNS intégrée

La vérification passe par les commandes **nslookup** et ping **mondomaine.local**

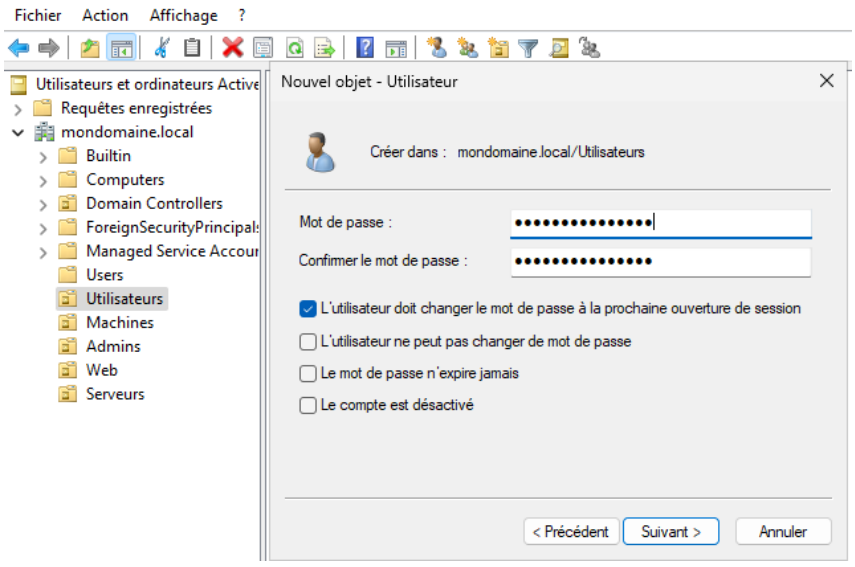


6. Création des utilisateurs

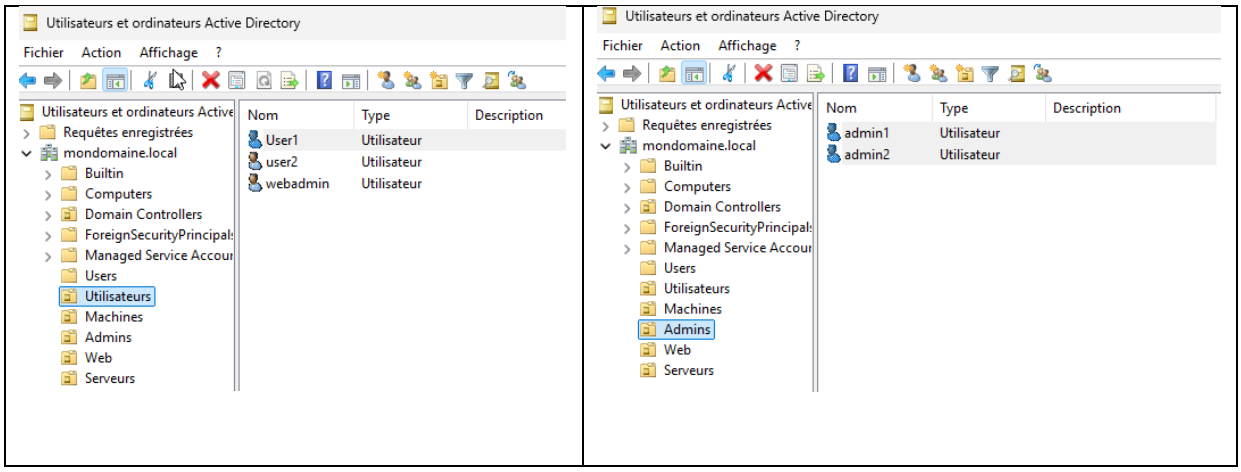
Nous avons débuté par la création du compte **webdamin**



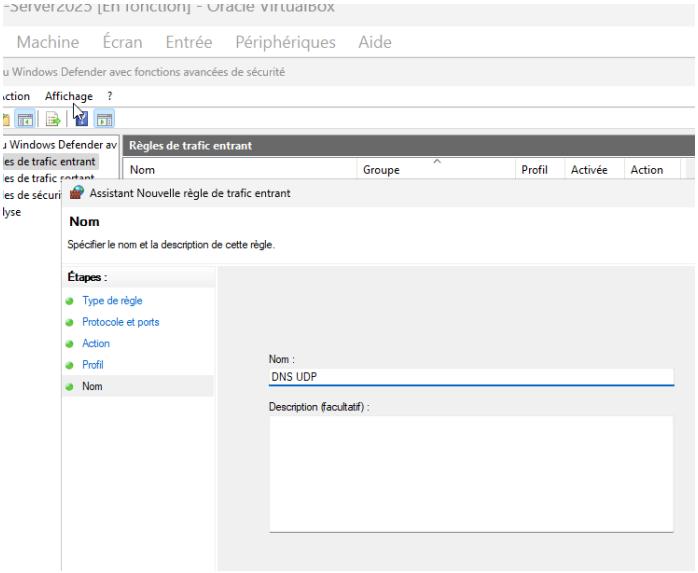
Par la suite il fallait définir un mot de passe par défaut qui seras changé par l'utilisateur l'or de ça toute première connexion.



Nous avons eu les résultats suivants :



Il ne restait plus qu'ajouter une nouvelle règle pour autoriser le trafic entrant **DNS** et **UDP**

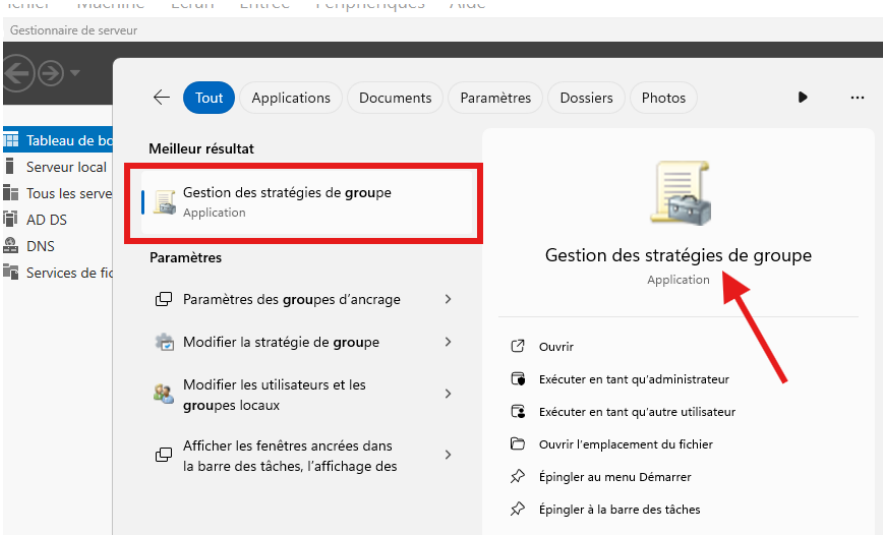


7. Jointure des postes clients et administrateurs au domaine

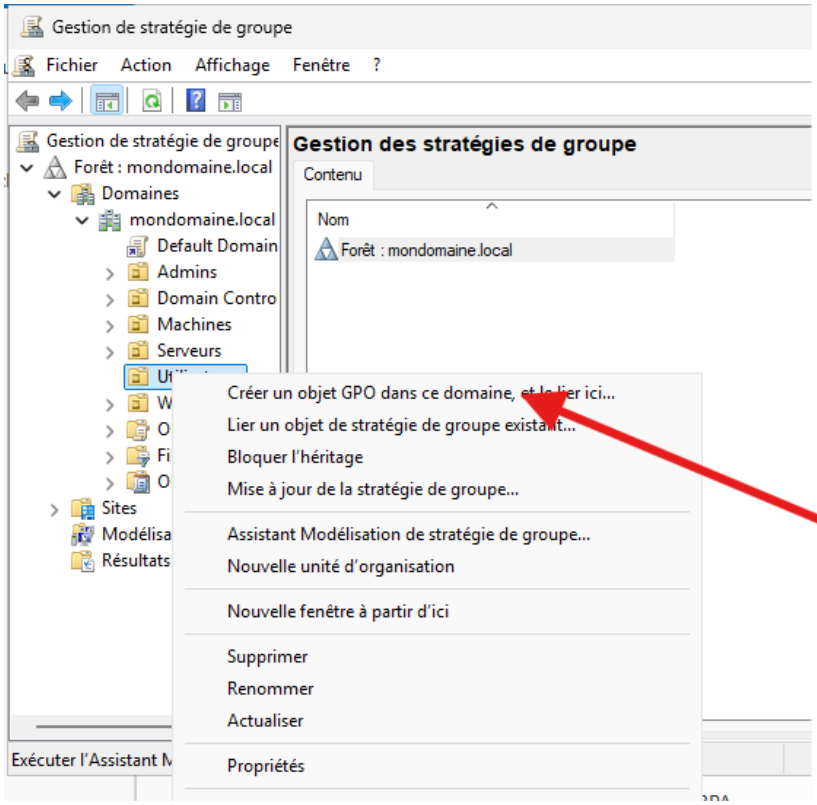
Pour cette partie, nous avons intégré les machines Windows (poste utilisateur et poste administrateur) au domaine Active Directory « **mondomaine.local** ». Cette opération avait pour but de centraliser l'authentification, d'appliquer les stratégies de groupe (GPO), et de renforcer la cohérence de la sécurité dans l'infrastructure.

Nous avons procédé comme suite :

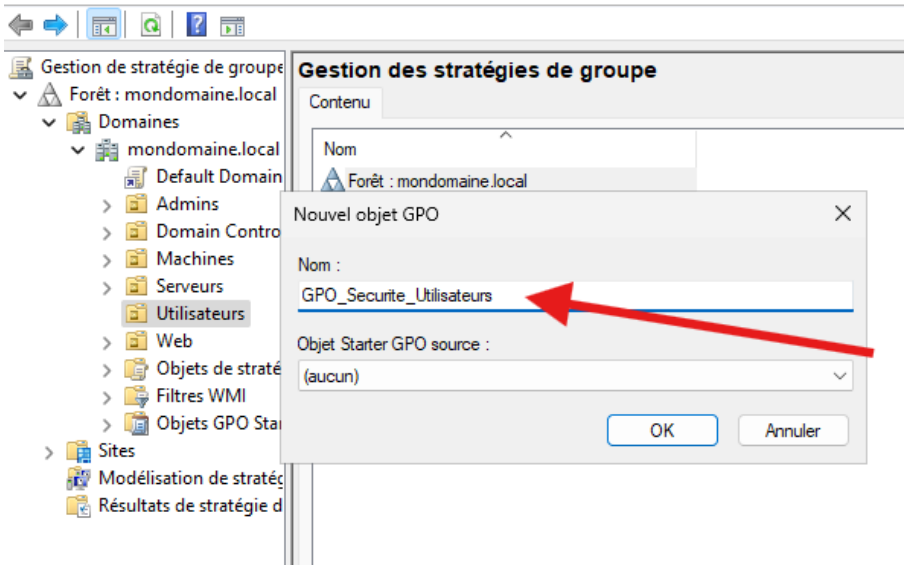
- Nous avons recherché dans le menu Windows « **Gestion des stratégies de groupe** » puis presser la touche « **Entrée** »



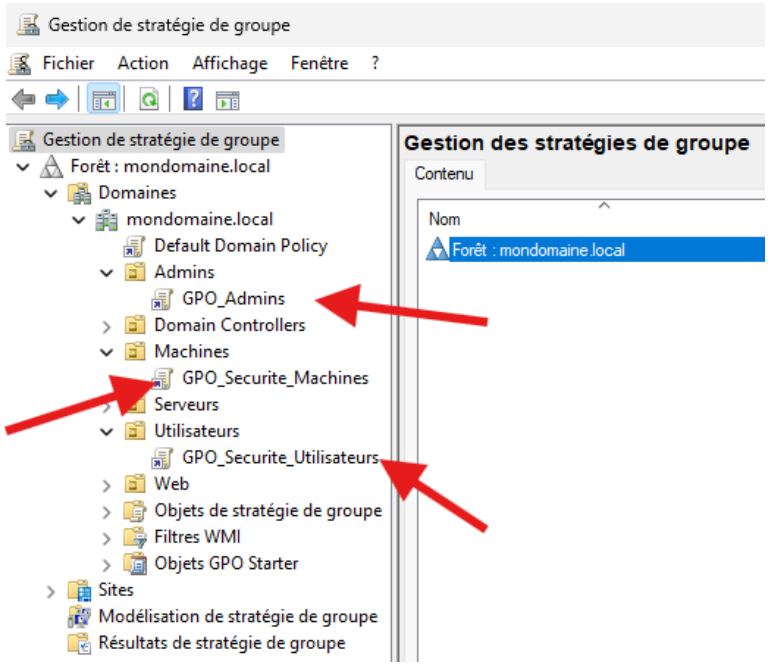
- Ensuite, nous avons fait un clic droit sur « **Utilisateurs** », puis sur « **Créer un objet GPO dans ce domaine** »



- Il ne restait plus cas définir le nom de dernier comme suite :

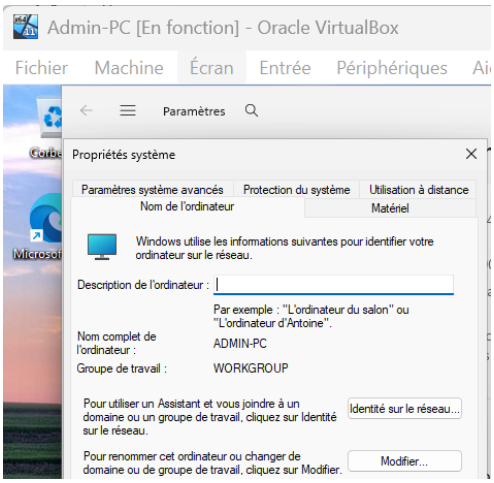


- Et enfin, nous avons répliquées la procédure pour les autres groupes

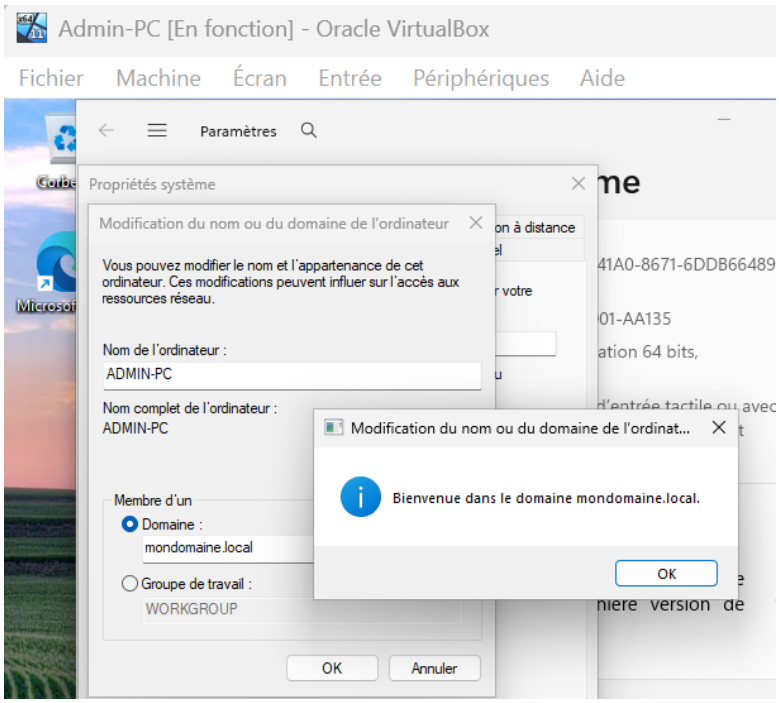


8. Modification du nom de domaine de l'ordinateur

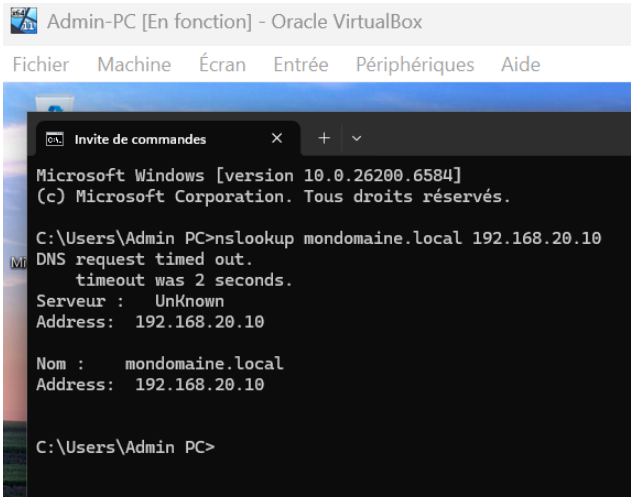
Pour le réaliser, nous somme aller dans propriétés du système et nous avons cliqué sur « **identité sur le réseau** »



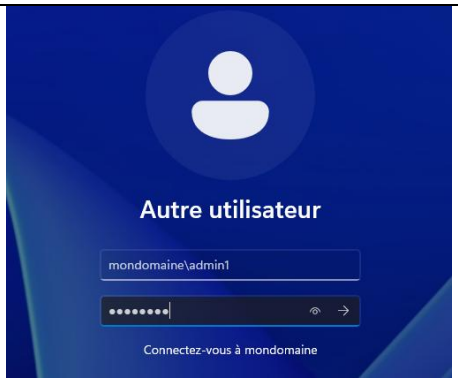
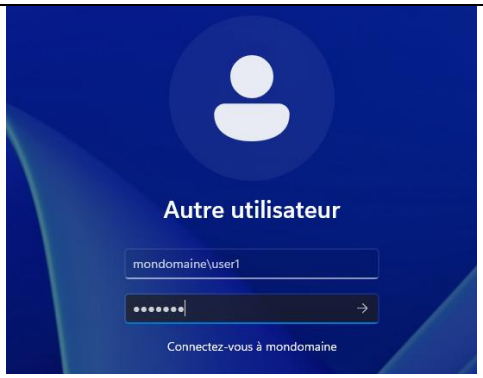
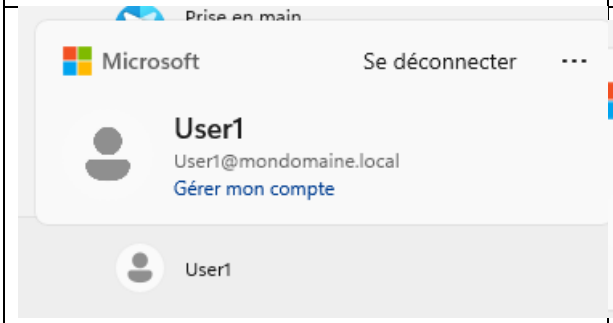
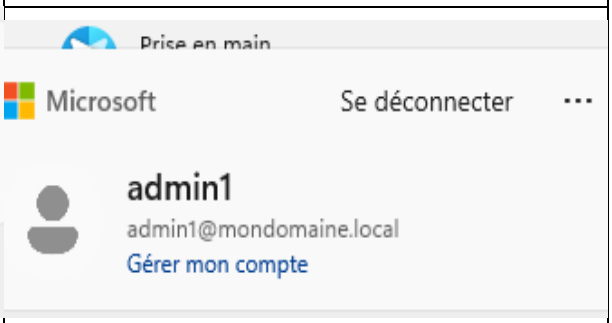
Nous avons entré le nom de notre domaine et la connexion à été établie sans souci



Une petite visite dans le « **CMD** » de constater que nos pc clients reconnaisse notre nom de domaine « **mondomaine.local** »

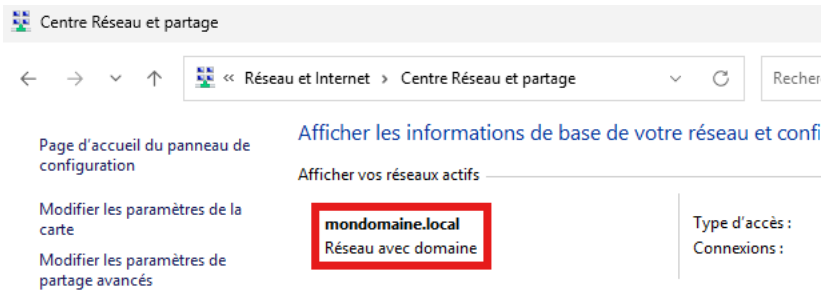


Il ne restait plus qu'à redémarrer la machine cliente et nous avons constaté des changements.

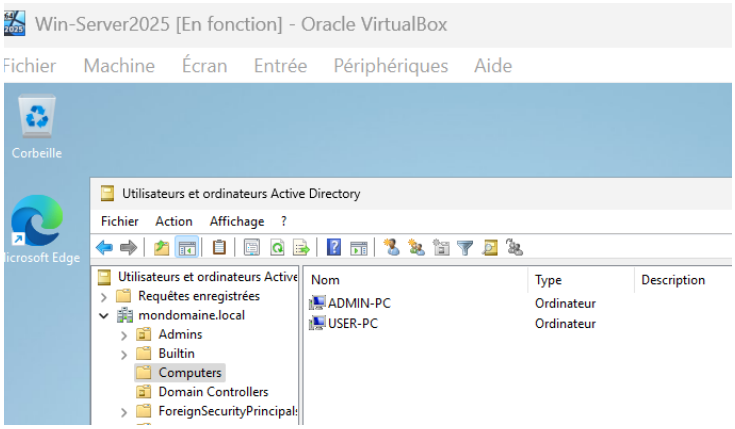
PC User1	PC Admin1
	
	

Nous avons également pu observer plusieurs changements :

- Dans le « **Centre réseau et partage »,** nous constatons que notre réseau à bien été identifié



- Aussi, dans « **L'Utilisateur et ordinateur active directory**



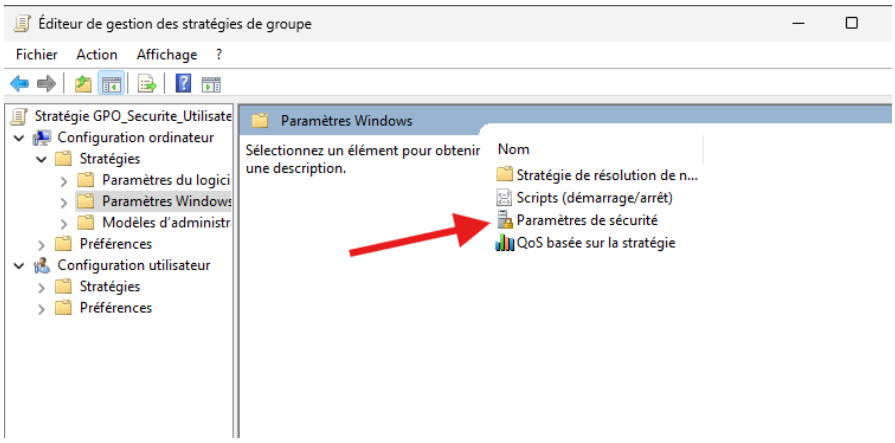
9. Editer la gestion des stratégies de groupe (GPO)

Pour cette partie, nous avons configurée et éditer les stratégies de groupe (Group Policy Object) afin de renforcer la sécurité du domaine Active Directory et d'assurer une homogénéité des paramètres sur l'ensemble des postes clients et administrateurs. Nous avons utilisé la console Group Policy Management pour créer, modifier et appliquer les règles. Les objectifs étaient de :

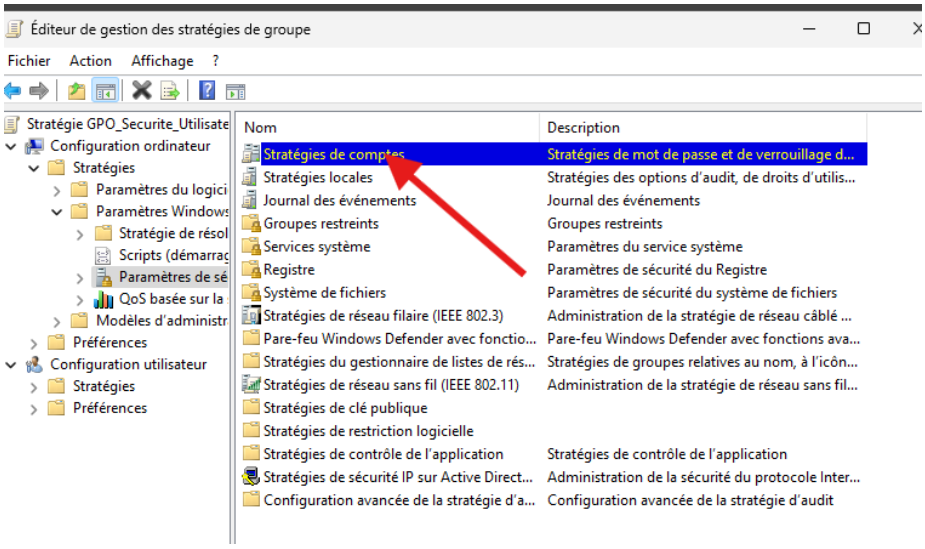
- Centraliser la gestion des paramètres de sécurité et de configuration
- Appliquer une stratégie de mots de passe conforme aux recommandations ANSSI
- Restreindre les accès administratifs (notamment RDP)
- Désactiver les services non essentiels
- Documenter et exporter les GPO pour traçabilité

Pour réaliser ces objectifs, nous avons :

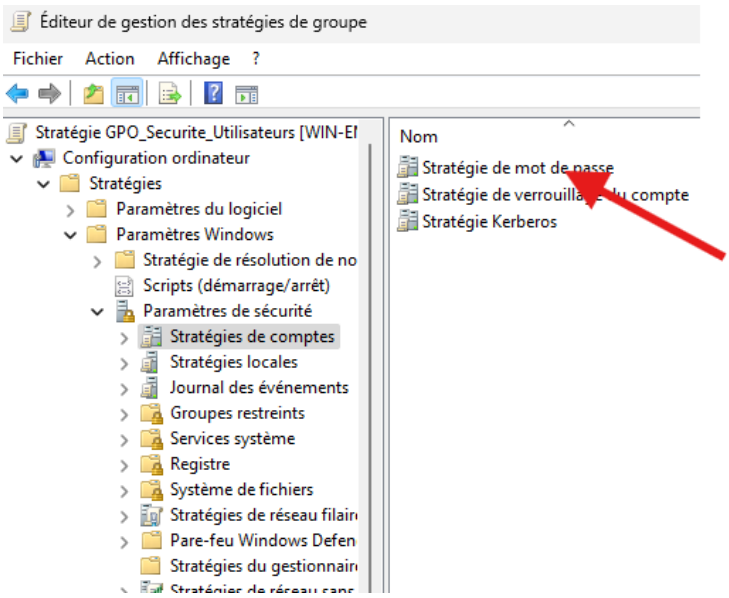
- Ouvert la console GPO et nous nous sommes rendus dans le menu « **Outils d'administration** » suivi de « **Gestion des stratégies de groupe** » ou nous accédé aux éléments suivants **:**



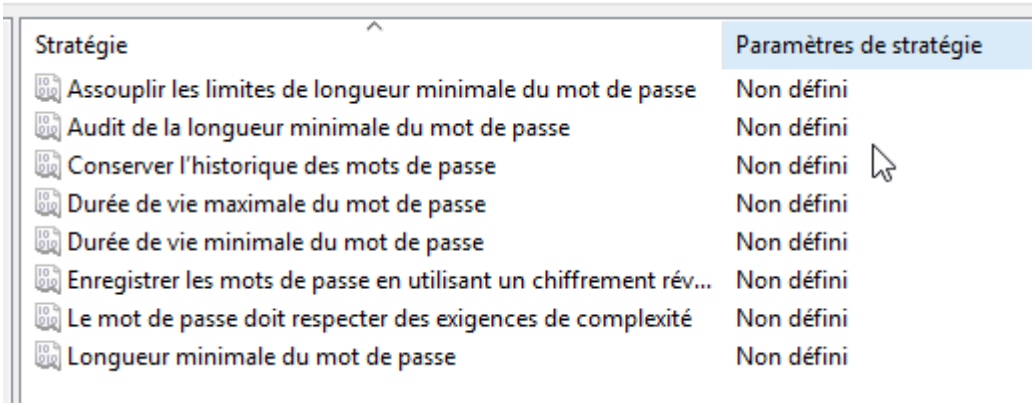
- Une fois entré dans paramètre de sécurité dans les configurations des paramètres Windows, nous avons opté pour l'option « **stratégies de compte** »



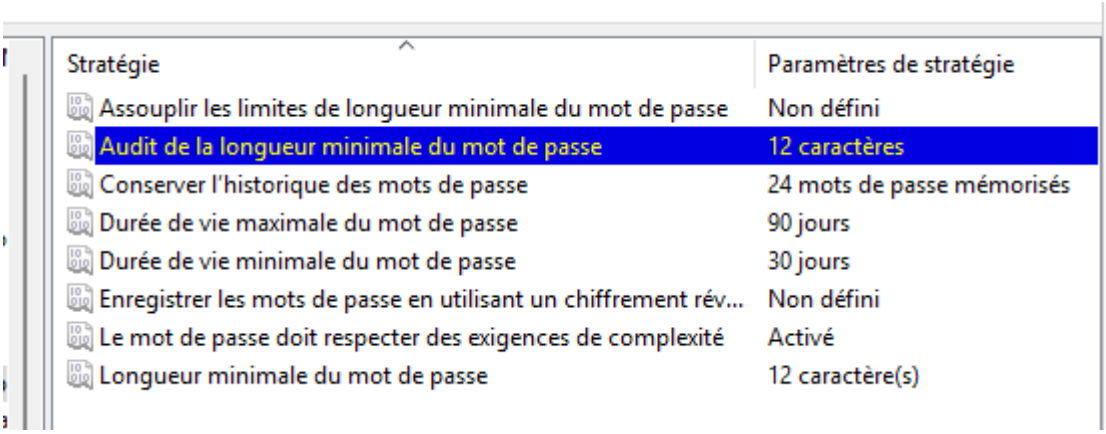
- Puis sur « **stratégie de mot de passe** »



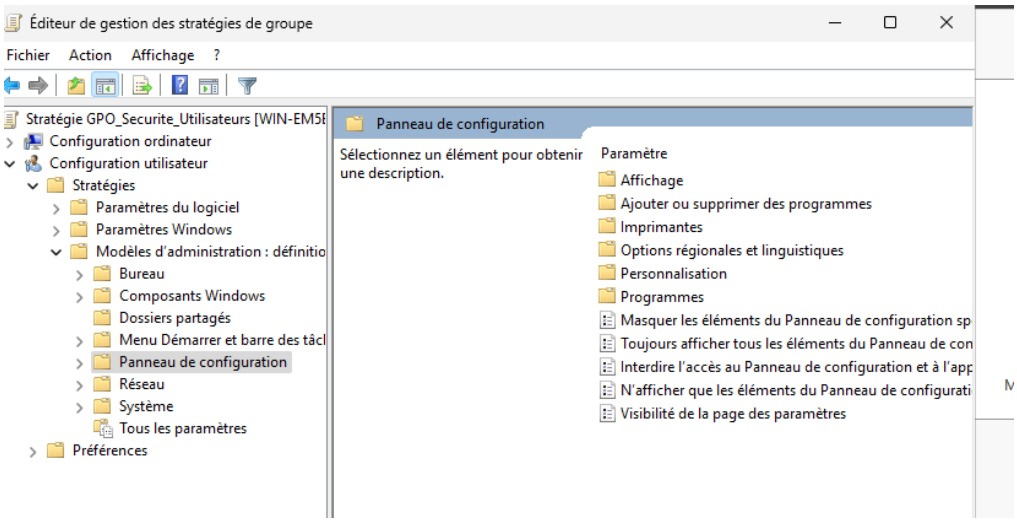
- Nous avons eu le rendu suivant ou tous les paramètre de stratégie était désactivé



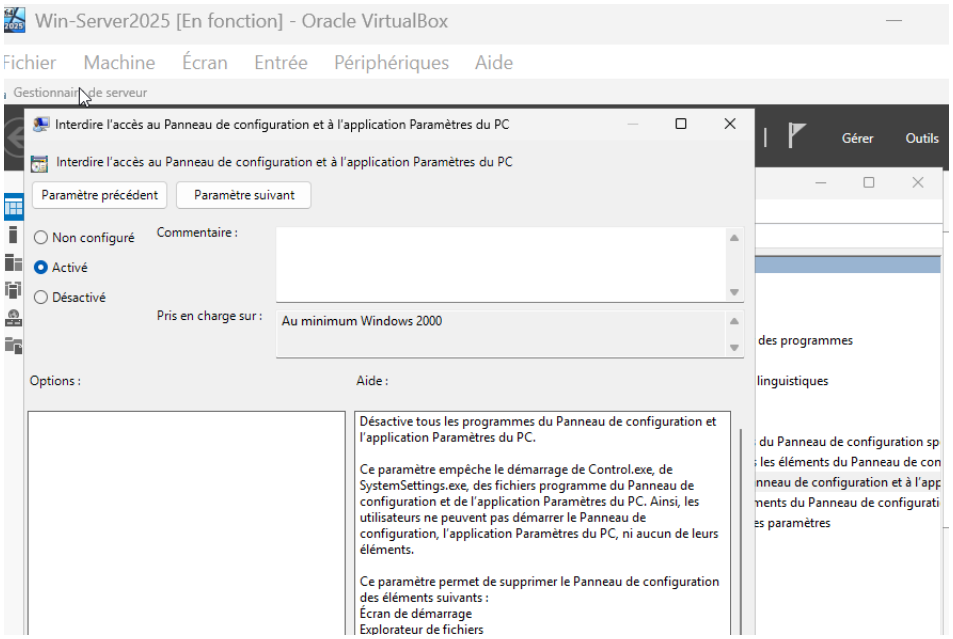
- Nous avons défini quelques stratégies comme représenté plus bas



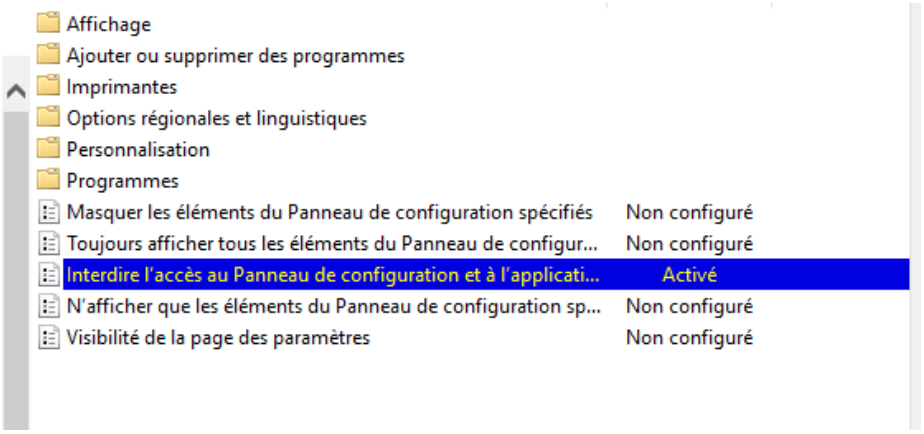
Pour clôturer cela en beauté, nous avons appliqué quelques couches de précautions supplémentaires comme interdire l'accès aux panneaux de configuration. Pour ce fait, nous somme aller dans « **Modèle d'administration »** se trouvant lui-même dans « **Configuration Utilisateur »**



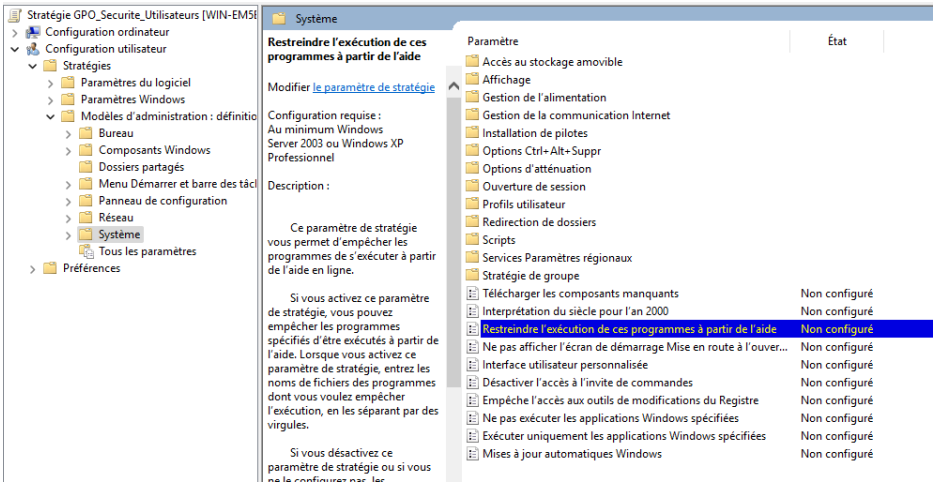
Là nous l'avons activé comme suite :



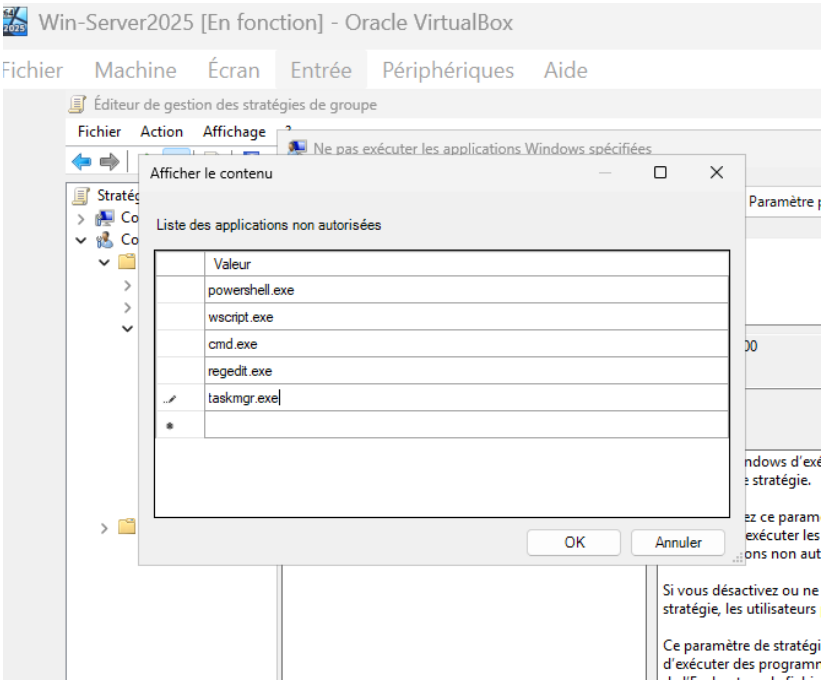
- Voici le rendu obtenu en question :



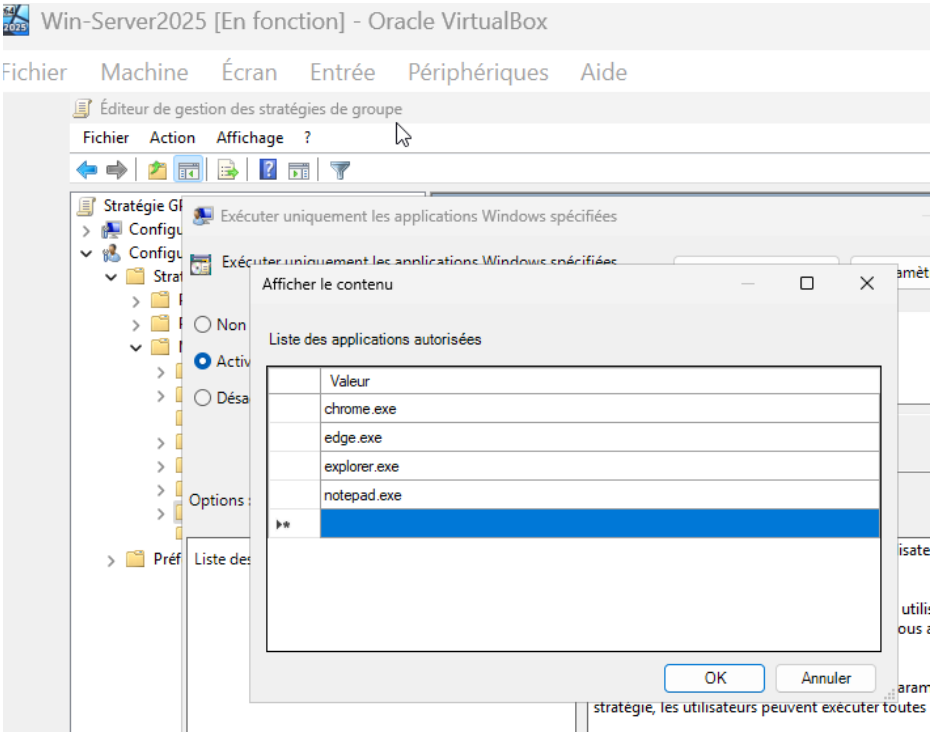
- Nous avons également restreint l'exécution de certain programme



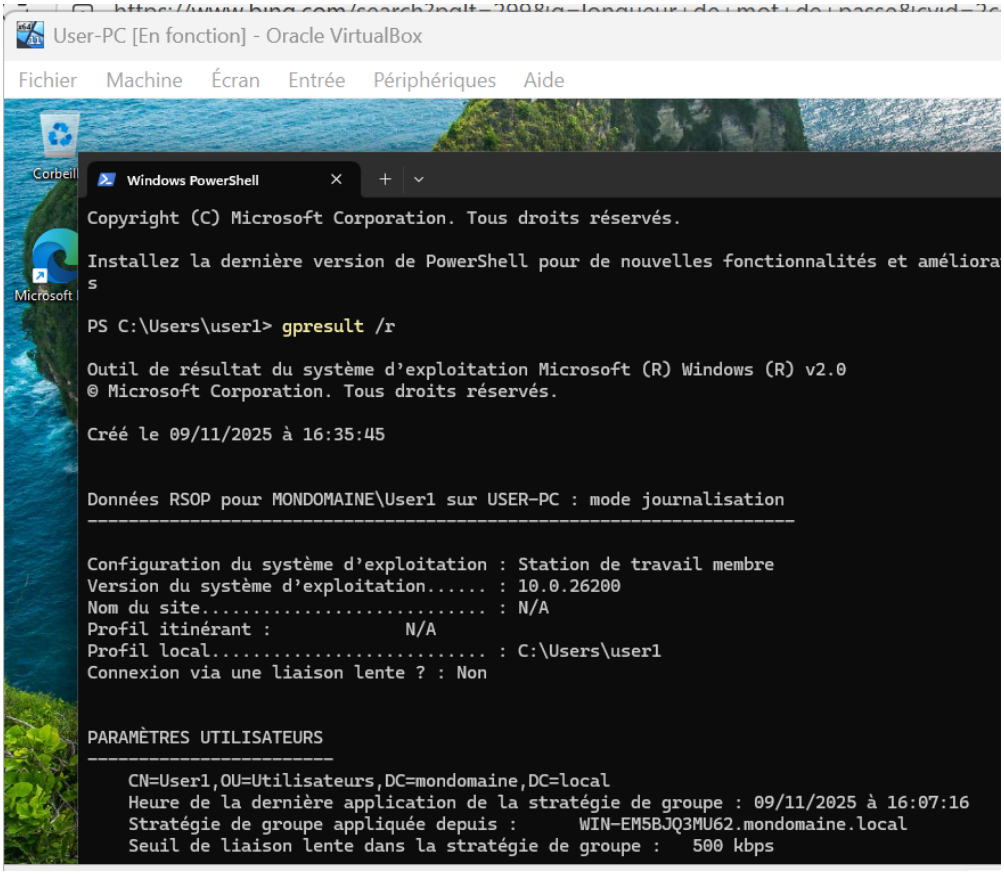
Il s'agissait des programmes tels : **powershell.exe, wscript.exe, cmd.exe, regedit.exe et bien d'autres encore.**



- A cela s'ajoute des restrictions sur certaine application Windows



- La dernière étape est la v**érification s**ur un poste client avec la commande « **gpresult /r »**

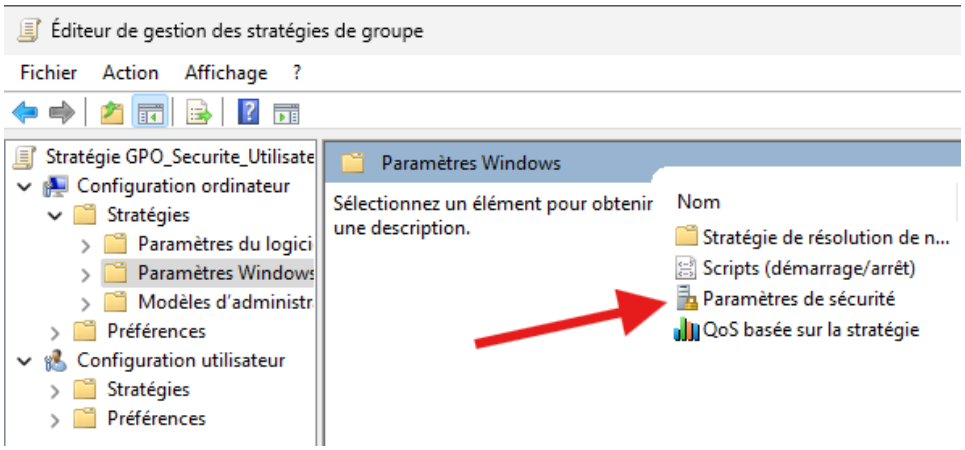


10. Interdiction de la connexion à distance en tant qu'administrateur local

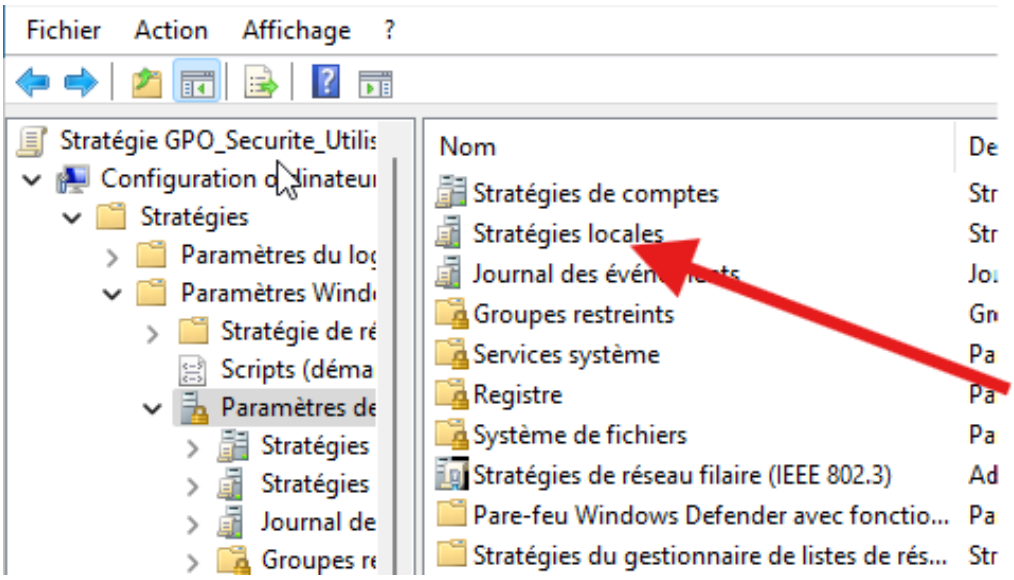
La mesure visant à interdire la connexion à distance en tant qu'administrateur local s'inscrit dans une logique de durcissement des postes Windows et de réduction de la surface d'attaque. En pratique, elle consiste à appliquer une stratégie de groupe (GPO) qui refuse l'ouverture de session par les services Bureau à distance pour le compte Administrateur local, tout en limitant l'accès RDP aux seuls groupes du domaine explicitement autorisés. Cette restriction empêche l'exploitation d'un compte privilégié souvent ciblé par les attaques par force brute et renforce le principe de moindre privilège recommandé par l'ANSSI et l'ISO/IEC 27001. Associée à des bonnes pratiques comme le renommage du compte Administrateur intégré, l'utilisation de LAPS pour gérer les mots de passe locaux et la journalisation des tentatives de connexion, cette mesure garantit une meilleure sécurité des environnements Windows tout en assurant la conformité aux standards de cybersécurité.

Pour cela, nous avons procédé comme suite :

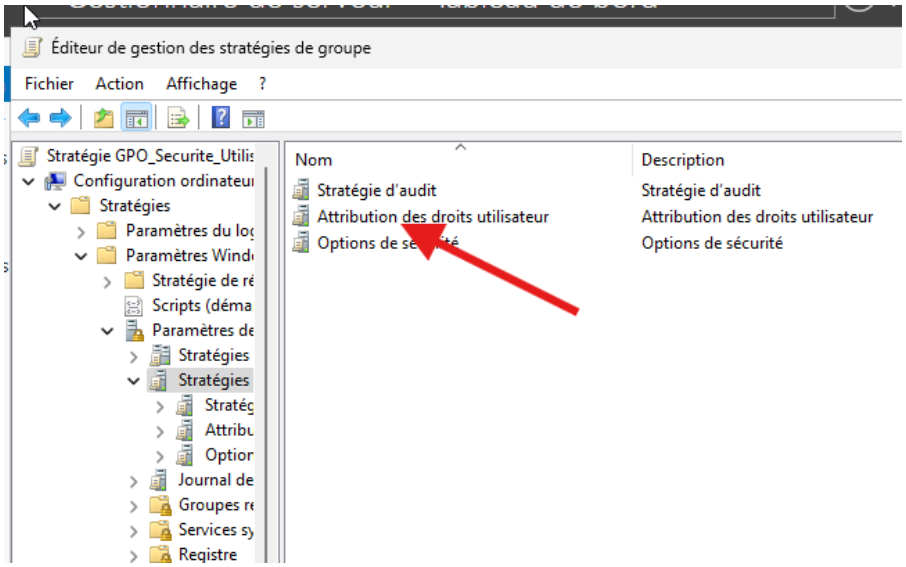
- Nous sommes entrés dans les paramètres Windows, puis dans les paramètres de sécurité.



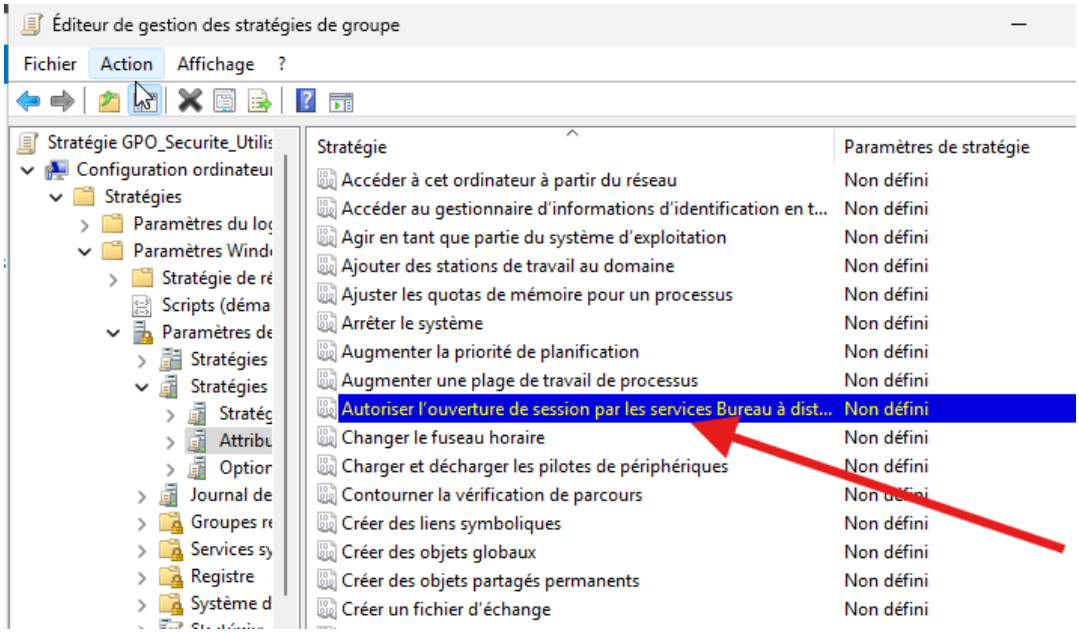
- Puis dans stratégies locales



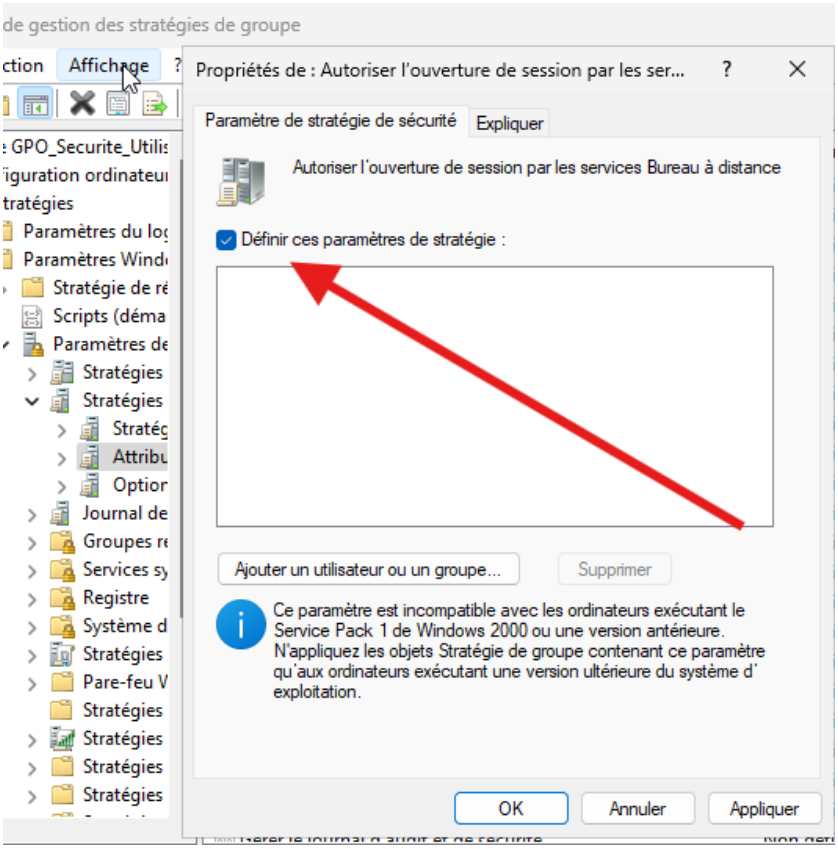
- Nous somme entrés dans attribution des droits utilisateurs



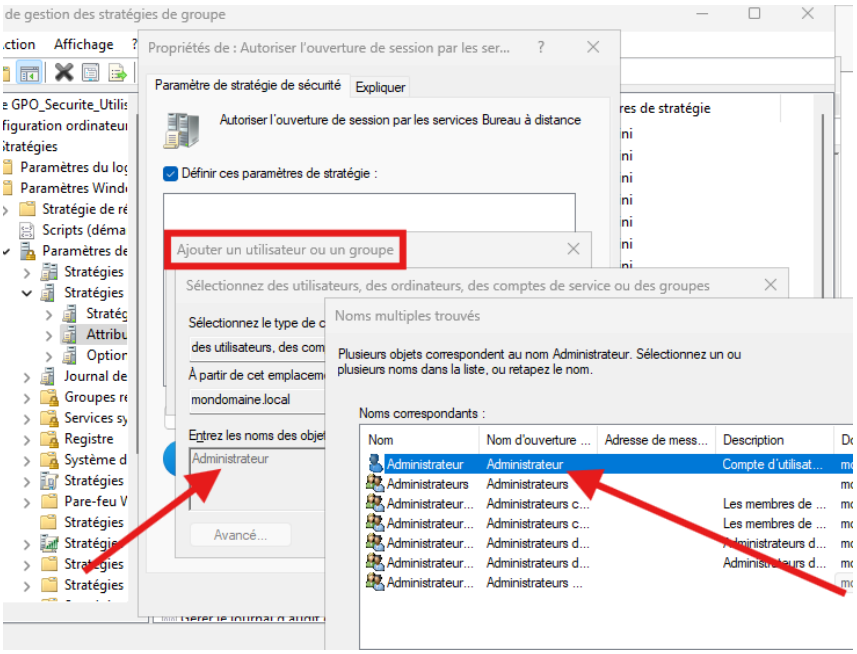
- Nous devons définir quelque paramètre notamment, refuser l'ouverture de session par les services Bureau à distance. Là, il est non défini nous allons le paramétrer.



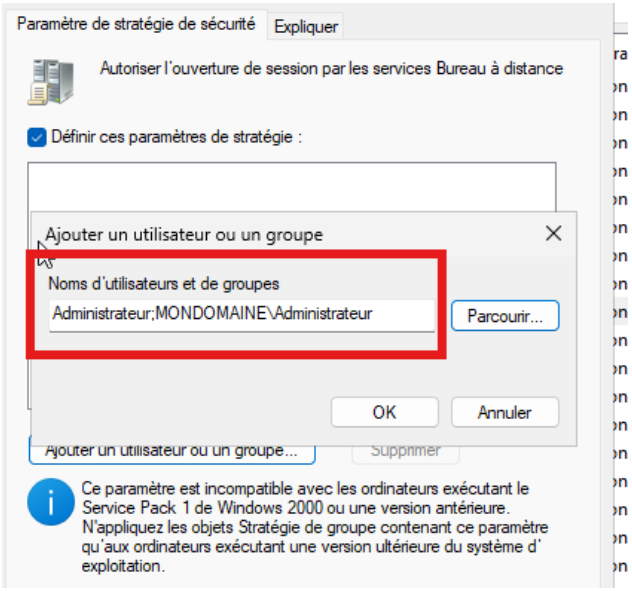
- Nous avons coché la case « **Définir ces paramètres de stratégies** »



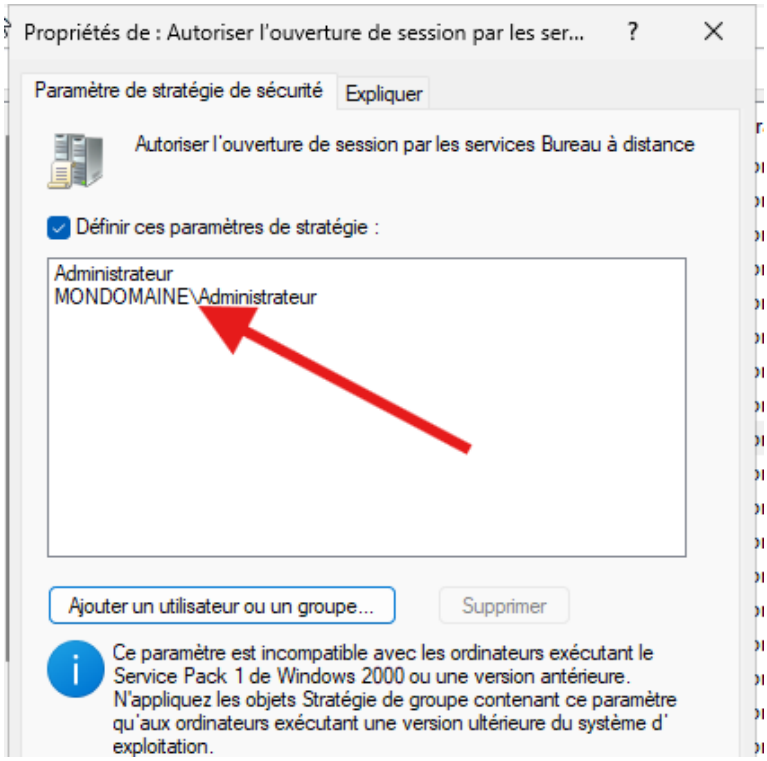
➢ Nous avons « **Ajouter un utilisateur ou un groupe** »



➢ Nous avons ajouté **Administrateur** du domaine **MONDOMAINE**



- Résultat aperçu



11. Désactivation du Directory Listing Apache

Nous allons empêcher la divulgation non autorisée de la structure des répertoires via le serveur Apache, afin de réduire la surface d'attaque et protéger les informations sensibles exposées par la liste des fichiers. Pour cela, nous avons :

- Modifier la configuration Apache, généralement dans le fichier apache2.conf ou dans les fichiers de configuration des sites (.conf dans /etc/apache2/sites-available/).
- Nous avons localisé le fichier de configuration principal (apache2.conf).
- Ouvrir le fichier avec un éditeur de texte en mode administrateur, avec : **sudo nano /etc/apache2/apache2.conf**
- Nous avons recherché les directives **<Directory>** correspondant aux répertoires accessibles publiquement notamment, /**var/www/html**.
- Enfin, nous avons désactiver l'option d'indexes dans les directives, puis redémarrer le service Apache pour appliquer les modifications : **sudo systemctl restart apache2**

Conclusion générale

Il était question, dans ce projet, de concevoir, déployer et sécuriser une infrastructure réseau segmentée et documentée, en intégrant des mécanismes de filtrage, de durcissement et de gestion centralisée des identités, afin de répondre aux exigences contemporaines de la cybersécurité et aux standards académiques les plus élevés. Nous avons progressivement construit une architecture cohérente, validé chaque étape technique et produit des livrables conformes aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), aux normes internationales ISO/IEC 27001 relatives au management de la sécurité de l'information, ainsi qu'aux bonnes pratiques du NIST Cybersecurity Framework. La segmentation du réseau et la configuration du pare-feu Ubuntu avec iptables ont permis de mettre en œuvre un cloisonnement strict des flux inter-VLAN, garantissant une défense en profondeur et une maîtrise des communications entre zones fonctionnelles, conformément au principe de « **least privilege** » et aux recommandations de l'ANSSI en matière de segmentation et de filtrage. Le durcissement du serveur Linux (Apache), avec la création d'un utilisateur restreint webadmin, la mise en place du chiffrement HTTPS et la désactivation des modules non essentiels, a illustré l'application concrète des mesures de sécurité préconisées par les guides de configuration sécurisée de l'ANSSI et par les benchmarks CIS (Center for Internet Security). La promotion du serveur Windows en contrôleur de domaine pour **mondomaine.local** a centralisé l'authentification et la gestion des identités, tandis que la jointure des postes clients et administrateurs au domaine a renforcé la cohérence et la sécurité globale, conformément aux principes de gouvernance des identités et des accès (IAM). L'édition et la gestion des stratégies de groupe (GPO) ont permis d'imposer des règles homogènes et conformes aux recommandations de l'ANSSI et aux exigences du RGPD en matière de protection des données personnelles : stratégie de mots de passe robuste, verrouillage des comptes après tentatives infructueuses, restrictions RDP, désactivation des services inutiles. Les livrables produits, script webadmin.sh pour l'automatisation des tâches Linux et fichier GPO.pdf pour la documentation des politiques Windows, constituent des preuves tangibles de la reproductibilité, de la traçabilité et de la conformité des configurations, répondant aux exigences de l'ISO/IEC 27001 en matière de documentation et de gestion des preuves de conformité.

Ce projet illustre une démarche scientifique appliquée à la cybersécurité, fondée sur une approche systémique, une logique de défense en profondeur et une documentation exhaustive,

et démontre la capacité à articuler rigueur méthodologique, pertinence technique et vision stratégique. Il s'inscrit dans une perspective académique de haut niveau, où chaque étape est pensée comme une expérimentation validée par des tests, et où la reproductibilité des résultats est assurée par une documentation exhaustive. La méthodologie adoptée repose sur une articulation entre théorie et pratique : d'une part, l'intégration des recommandations normatives et des standards de sécurité (ANSSI, ISO/IEC 27001, NIST CSF, RGPD) ; d'autre part, la mise en œuvre technique concrète dans un environnement virtualisé et contrôlé. Cette double dimension confère au projet une valeur académique et professionnelle, en démontrant que la cybersécurité ne se limite pas à des configurations ponctuelles, mais qu'elle constitue un champ de recherche appliquée, où la rigueur scientifique et l'innovation technique doivent coexister.

À notre niveau, il est essentiel de ne pas s'arrêter au résultat immédiat, mais d'ouvrir des perspectives de recherche et d'amélioration. Ce projet constitue une base solide pour des travaux futurs dans plusieurs directions : l'intégration de solutions de supervision et de détection d'intrusion (IDS/IPS, SIEM) afin de corréler les événements et détecter les anomalies ; le développement de scripts et de playbooks Ansible pour industrialiser le déploiement et la sécurisation ; la mise en place de mécanismes de résilience et de haute disponibilité (clusters AD, load balancing Apache) pour garantir la continuité de service ; l'adaptation de l'infrastructure aux exigences réglementaires du RGPD et aux normes ISO/IEC 27001 ; enfin, l'exploration des liens entre la segmentation réseau classique et les approches modernes de micro-segmentation en environnements cloud et hybrides. Ces perspectives ouvrent la voie à une recherche appliquée en cybersécurité, où l'objectif n'est pas seulement de sécuriser un système d'information, mais de penser sa résilience, son évolutivité et sa conformité dans un contexte global marqué par la complexité et l'interconnexion des systèmes.

En définitive, nous avons atteint les objectifs fixés : un système d'information segmenté, sécurisé et documenté, prêt à être soutenu et évalué, et qui constitue une base solide pour des recherches futures en cybersécurité appliquée. Ce projet met en avant la double dimension pédagogique et académique, valorisant ainsi la convergence entre pratique professionnelle et exigence académique. Il démontre la capacité à concevoir, sécuriser et administrer un système d'information complexe, en respectant les standards académiques et professionnels, et s'inscrit pleinement dans une perspective doctorale, en articulant rigueur scientifique, pertinence technique et vision stratégique pour répondre aux enjeux contemporains de la sécurité des systèmes d'information.

BIBLIOGRAPHIE

[1] ANSSI : Guide d'hygiène informatique, Agence Nationale de la Sécurité des Systèmes d'Information, 2019.

[2] ISO/IEC 27001, 2013, Information technology, Security techniques, Information security management systems, Requirements.

[3] ISO/IEC 27002 : 2022, Code of practice for information security controls.

[4] NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, National Institute of Standards and Technology, 2009.

[5] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, 2020.

[6] RFC 2196, Site Security Handbook, Internet Engineering Task Force (IETF), 1997.

[7] Richard Bejtlich, The Practice of Network Security Monitoring : Understanding Incident Detection and Response, No Starch Press, 2013.

[8] William Stallings, Network Security Essentials: Applications and Standards, Pearson, 2017.

[9] Brian W. Kernighan & Rob Pike, The Unix Programming Environment, Prentice Hall, 1984.

[10] Chris McNab, Network Security Assessment: Know Your Network, O'Reilly Media, 2016.

[11] Mark Ciampa, Security+ Guide to Network Security Fundamentals, Cengage Learning, 2020.

[12] Apache HTTP Server Documentation, Apache Software Foundation, consulté en 2025.

[13] Microsoft TechNet, Group Policy Settings Reference for Windows and Active Directory, Microsoft Corporation, consulté en 2025.

[14] Gabriel Popovici, Bibliographie centrée sur les usages des TIC et numériques, MSH Paris Nord, Université Paris 8 et Université Paris 13, Les Cahiers du numérique, 2013/2 (Vol. 9), pp. 137-161.

[15] Olivier Palluault, La vieille histoire d'une science moderne, De l'Antiquité à la révolution industrielle, 2010.

[16] Pierre Mounier-Kuhn, La vieille histoire d'une science moderne, De l'Antiquité à la révolution industrielle, 2012.

[17] Cloud Computing ou informatique dans les nuages, Revue Le Monde Informatique, 2015.

[18] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley, 2015.

[19] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2020.

[20] Eric Cole, Advanced Persistent Threats: Understanding the Danger and How to Protect Your Organization, Syngress, 2013.

[21] SANS Institute, Critical Security Controls for Effective Cyber Defense, 2021.

[22] ENISA, European Union Agency for Cybersecurity, Good Practices for Security of IoT, 2020.

[23] CNIL, Guide RGPD et sécurité des données personnelles, Commission Nationale de l'Informatique et des Libertés, 2021.

[24] ISO/IEC 27005:2018, Information security risk management.

[25] RFC 4301, Security Architecture for the Internet Protocol (IPsec), IETF, 2005.

[26] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, IETF, 2008.

[27] RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, IETF, 2018.

[28] Patrick Engebretson, The Basics of Hacking and Penetration Testing, Syngress, 2013.

[29] Kevin Mitnick, The Art of Invisibility, Little, Brown and Company, 2017.

[30] Jean-Philippe Rennard, Introduction à la cybersécurité, Dunod, 2021.

[31] Guillaume Poupard, Cybersécurité : enjeux et perspectives, ANSSI, 2020.

[32] Open Web Application Security Project (OWASP), Top 10 Web Application Security Risks, 2021.

[33] Cisco Systems, Cisco SAFE Security Reference Architecture, 2019.

[34] VMware, Zero Trust Security Model, Livre blanc, 2020.

[35] Palo Alto Networks, Next-Generation Firewall Best Practices, 2021.

[36] Check Point Software Technologies, Cyber Security Report, 2022.

[37] Fortinet, FortiGate Firewall Administration Guide, 2023.

[38] Red Hat, SELinux User Guide, 2022.

[39] Debian Project, Debian Security Manual, 2023.

[40] Ubuntu Documentation, Hardening Ubuntu Servers, Canonical, 2024.

WEBOGRAPHIE

[1] Visite de www.anssi.fr

- Lien : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
- Objectif : consultation du guide d'hygiène informatique de l'ANSSI pour les bonnes pratiques de sécurité.
- Date et heure : Mercredi, 5 Novembre 2025 à 09h00
- Durée de la visite : 30 minutes

[2] Visite de www.iso.org

- Lien : https://www.iso.org/isoiec-27001-information-security.html/
- Objectif : étude des normes ISO/IEC 27001 relatives au management de la sécurité de l'information.
- Date et heure : Mercredi, 5 Novembre 2025 à 09h45
- Durée de la visite : 25 minutes

[3] Visite de www.nist.gov

- Lien : https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final/
- Objectif : analyse des contrôles de sécurité et de confidentialité pour les systèmes d'information.
- Date et heure : Mercredi, 5 Novembre 2025 à 10h15
- Durée de la visite : 20 minutes

[4] Visite de httpd.apache.org

Lien : https://httpd.apache.org/docs/2.4/

Objectif : durcissement et configuration sécurisée du serveur Apache.

Date et heure : Mercredi, 5 Novembre 2025 à 11h00

Durée de la visite : 20 minutes

[5] Visite de learn.microsoft.com

- Lien : https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/
- Objectif : documentation sur Active Directory et les stratégies de groupe (GPO). Date et heure : Mercredi, 5 Novembre 2025 à 11h30
- Durée de la visite : 25 minutes

[6] Visite de www.owasp.org

- Lien : https://owasp.org/www-project-top-ten

- Objectif : étude des dix principales vulnérabilités des applications web selon OWASP.
- Date et heure : Mercredi, 5 Novembre 2025 à 12h00
- Durée de la visite : 20 minutes

[7] Vidéo OpenClassrooms, Introduction à la cybersécurité

- Lien : https://www.youtube.com/watch?v=YHkZqERWEB4/
- Objectif : comprendre les fondamentaux de la cybersécurité et les enjeux pour les entreprises. Date et heure : Mercredi, 5 Novembre 2025 à 14h00
- Durée de la visite : 30 minutes

[8] Vidéo OpenClassrooms, Plongez au cœur d'une cyberattaque

Lien : https://www.youtube.com/watch?v=SNlObWfVQGo/

- Objectif : étude de cas pratique sur la gestion d'incidents et la réponse aux attaques.
- Date et heure : Mercredi, 5 Novembre 2025 à 14h45
- Durée de la visite : 25 minutes

[9] Vidéo OpenClassrooms, Créer et gérer une GPO dans Active Directory

Lien : https://www.youtube.com/watch?v=TxMXsFN-25g

- Objectif : tutoriel sur la création et la configuration d'une première stratégie de groupe Active Directory.
- Date et heure : Mercredi, 5 Novembre 2025 à 16h15
- Durée de la visite : 20 minutes

[10] Visite de www.cisco.com

- Lien : https://www.cisco.com/c/en/us/solutions/security/index.html
- Objectif : consultation des architectures de sécurité réseau Cisco SAFE.
- Date et heure : Jeudi, 6 Novembre 2025 à 09h00
- Durée de la visite : 30 minutes

[11] Visite de www.vmware.com

- Lien : https://www.vmware.com/security/zero-trust.html/
- Objectif : recherche sur le modèle de sécurité Zero Trust.
- Date et heure : Jeudi, 6 Novembre 2025 à 09h45
- Durée de la visite : 25 minutes

[12] Vidéo OpenClassrooms, Comprendre Active Directory et Group Policy

- Lien : https://www.youtube.com/watch?v=Q4I2lKHboDw/
- Objectif : approfondissement sur le fonctionnement d'Active Directory et des GPO. Date et heure : Jeudi, 6 Novembre 2025 à 11h00
- Durée de la visite : 30 minutes

[13] Vidéo OpenClassrooms, Formation complète sur Active Directory et GPO

- Lien : https://www.youtube.com/watch?v=Lyu-vVt-Jg8/
- Objectif : cours complet sur Active Directory et GPO avec des scénarios réels.
- Date et heure : Jeudi, 6 Novembre 2025 à 14h00
- Durée de la visite : 45 minutes

[14] Visite de www.cnil.fr

- Lien : https://www.cnil.fr/fr/rgpd-de-a-a-z/
- Objectif : conformité réglementaire RGPD et protection des données personnelles.
- Date et heure : Vendredi, 7 Novembre 2025 à 09h00
- Durée de la visite : 30 minutes

[15] Visite de www.enisa.europa.eu

- Lien : https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/
- Objectif : bonnes pratiques de sécurité pour l'Internet des Objets (IoT).
- Date et heure : Vendredi, 7 Novembre 2025 à 09h45
- Durée de la visite : 25 minutes

[16] Vidéo OpenClassrooms, Sécuriser un système Linux avec iptables

- Lien : https://www.youtube.com/watch?v=SD9HtdYOmMs/
- Objectif : formation pratique sur la configuration d'un pare-feu iptables.
- Date et heure : Vendredi, 7 Novembre 2025 à 11h00
- Durée de la visite : 40 minutes

[17] Vidéo OpenClassrooms, Sécurisation avancée des serveurs Ubuntu

- Lien : https://www.youtube.com/watch?v=rEhTzP-ScBo/
- Objectif : durcissement des serveurs Ubuntu et bonnes pratiques de sécurité.
- Date et heure : Vendredi, 7 Novembre 2025 à 14h00
- Durée de la visite : 35 minutes