Projet Sécurité 184



**Rapport de projet**

Amir, Anthony, Francesco – CIN2B

ETML, Vennes – A22

24 Périodes

Maître : M. Schaffter

Table des matières

[1 Description du projet dans son ensemble 4](#_Toc187410451)

[1.1 Titre 4](#_Toc187410452)

[1.2 Sujet 4](#_Toc187410453)

[2 Raisonnement 4](#_Toc187410454)

[3 Tâches et journal de travail 4](#_Toc187410455)

[4 Rapport 5](#_Toc187410456)

[5 Inventaire 5](#_Toc187410457)

[6 Attribution des Adresses IP 5](#_Toc187410458)

[7 Installations des serveurs 6](#_Toc187410459)

[7.1 Serveur 1 6](#_Toc187410460)

[7.2 Serveur 2 (Amir) 7](#_Toc187410461)

[7.2.1 Boot de la clé USB 7](#_Toc187410462)

[7.2.2 Installation du serveur 8](#_Toc187410463)

[7.2.3 Mise en place du bureau à distance 8](#_Toc187410464)

[8 Services 8](#_Toc187410465)

[8.1 Dynamic Host Configuration Protocol (DHCP) 8](#_Toc187410466)

[8.1.1 Utilisation du service dans le projet 8](#_Toc187410467)

[8.2 Active Directory (AD) 8](#_Toc187410468)

[8.2.1 Utilisation du service dans le projet 9](#_Toc187410469)

[8.3 pfSense 9](#_Toc187410470)

[8.3.1 Utilisation du service dans le projet 9](#_Toc187410471)

[8.4 Open VPN 9](#_Toc187410472)

[8.4.1 Utilisation du service dans le projet 9](#_Toc187410473)

[8.5 Bureau à distance (RDP) 10](#_Toc187410474)

[8.5.1 Utilisation du service dans le projet 10](#_Toc187410475)

[9 Schémas 10](#_Toc187410476)

[9.1 Schéma physique du serveur 1 10](#_Toc187410477)

[9.2 Schéma châssis 11](#_Toc187410478)

[9.3 Schéma physique de la mise en place du réseau 12](#_Toc187410479)

[9.4 Schéma VPN 12](#_Toc187410480)

[10 installation vm 13](#_Toc187410481)

[11 Installation Hyper-v 13](#_Toc187410482)

[12 Installation PfSense 17](#_Toc187410483)

[13 Installation dhcp 23](#_Toc187410484)

[14 Installation dns 23](#_Toc187410485)

[15 Installation ad ds 23](#_Toc187410486)

[16 Problèmes rencontrés 23](#_Toc187410487)

[16.1 Boot de la clé USB 23](#_Toc187410488)

[17 Conclusion 23](#_Toc187410489)

[17.1 Personnelle 23](#_Toc187410490)

[17.1.1 Francesco 23](#_Toc187410491)

[17.1.2 Amir 23](#_Toc187410492)

[17.1.3 Anthony 23](#_Toc187410493)

# Description du projet dans son ensemble

## Titre

Mise en place d’un accès distant à une petite infrastructure

## Sujet

Configuration de deux serveurs puissants (34 cœurs, 256 Go de RAM, 1 To SSD chacun), avec choix entre Linux ou Windows.

Mise en place des services essentiels :

Active Directory (AD) pour la gestion des utilisateurs.

Serveur DNS pour la résolution des noms.

Serveur DHCP pour l’attribution automatique des adresses IP.

Implémentation d’une solution VPN sécurisée

Utilisation de pfSense et configuration d’OpenVPN pour permettre aux employés distants un accès sécurisé aux ressources de l’entreprise.

Gestion des certificats et création de règles pour rediriger les ports nécessaires.

Notre objectif est de fournir un réseau performant et protégé contre les menaces.

# Raisonnement

Nous avons établi une certaine "manière de faire" pour la réalisation de ce projet. La communication entre les trois personnes chargées du travail est primordiale.

Pour bien débuter ce projet, nous avons commencé par établir une liste des tâches pas forcément très précise et créer un journal de travail expliqué juste ci-dessous. Dans le même temps, nous avons créé un rapport de travail listant tous les points pour la réalisation du projet, le rapport est expliqué ci-dessous également.

Après la création de tout ce qui est "administratif", nous allons débuter avec la réalisation concrète du projet dans son ensemble.

Pour cela, nous allons attribuer des adresses IP à chaque personne du groupe, mais surtout aux serveurs.

Ensuite, nous allons mettre en place les deux serveurs dans le châssis qui leur est destiné

# Tâches et journal de travail

Dans le cadre de ce projet, nous avons commencé par dresser une liste des tâches qu’on devrait faire durant le projet. Pour ce faire, nous avons plusieurs tâches qu’on a mis en commun dans le même fichier où se trouve le journal. Dans ce fichier Excel, nous inscrivons toutes les 15 minutes notre travail effectué, tout cela en commun, en spécifiant la personne qui a effectué le travail. Les tâches et le journal de travail ont été fait par les trois personnes du groupe.

# Rapport

Le rapport est rempli après chaque travail effectué afin simplifier l’explication de nos procédures. Des captures d’écran seront présentes avec des explications, nous allons également expliquer les différents problèmes que l’on a rencontrés durant la réalisation du projet. Le rapport est rempli par les trois personnes du groupe.

# Inventaire

Pour l’inventaire nous avons pris tous les objets nécessaires pour faire la connexion du serveur à notre PC. Nous n’avons pas pris la partie reliée au DHCP. Pour se faire on a dû aller dans la salle des serveurs et suivre tout le chemin pour arriver jusqu’à nos postes fixes. Nous avons pris chaque nom de chaque composants et câbles. On a compté chaque objet et mis une description pour savoir leurs utilités. L’infrastructure est représentée par un schéma et se trouve dans un fichier externe.

# Attribution des Adresses IP

Pour ce projet, une table d’adresses IP a été conçue :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Serveur 1 | Serveur 2 | Francesco | Amir | Anthony |
| 192.168.22.7 | 192.168.22.8 | 192.168.22.17 | 192.168.22.27 | 192.168.22.37 |

# Installations des serveurs

## Serveur 1

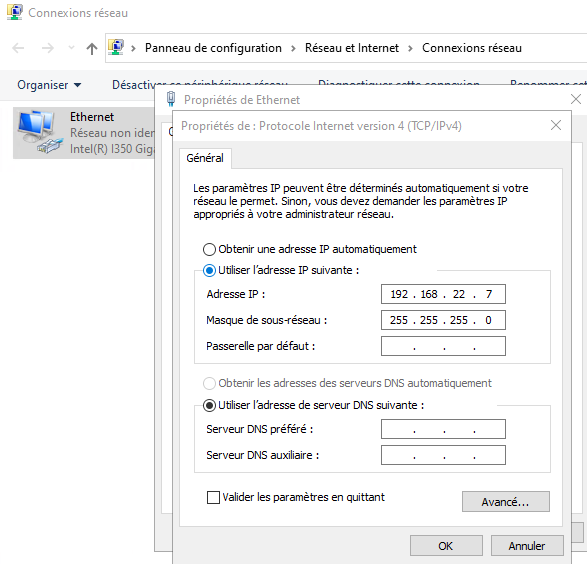
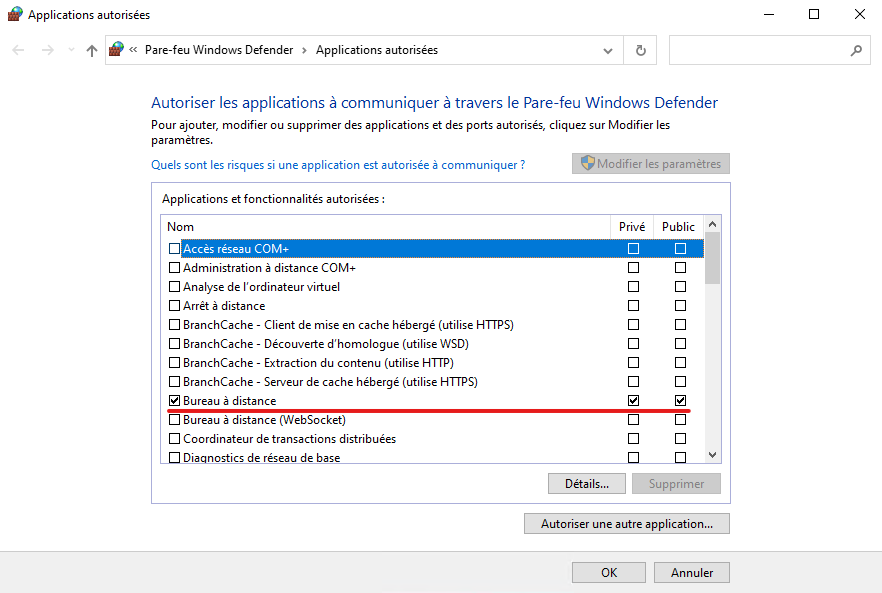
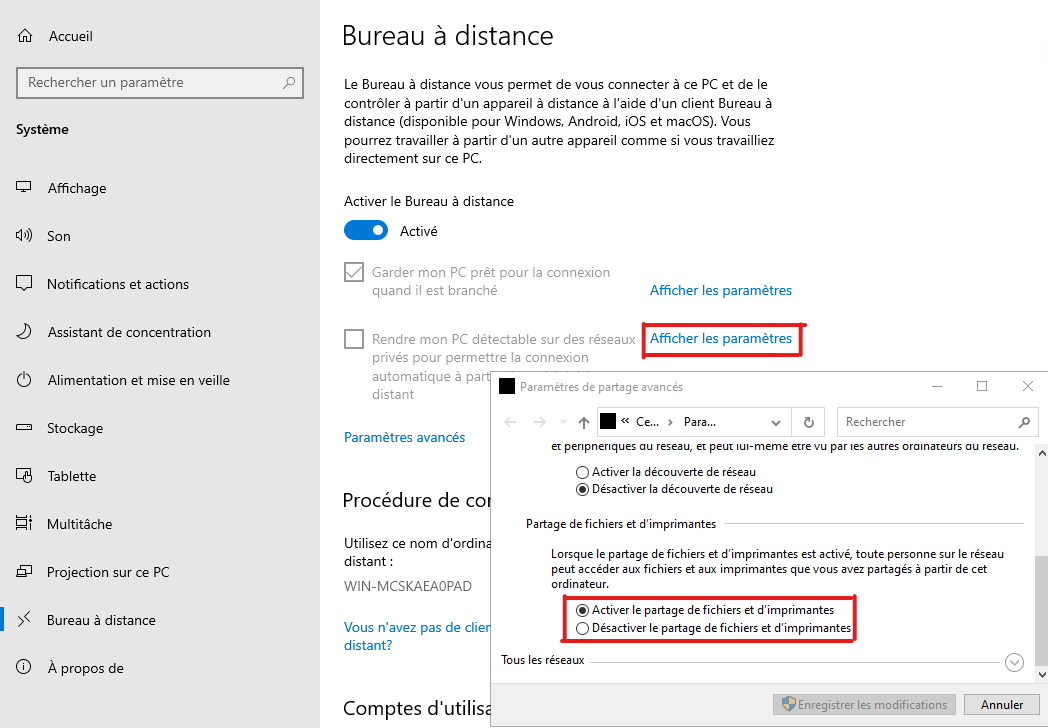


Figure 1 : Attribution réseau Serveur 1

Autoriser une application via le Pare-feu Windows





## Serveur 2 (Amir)

Je vais installer et configurer le deuxième serveur. L’installation sera la même que le premier serveur, on pourra s’y connecter à distance avec « Connexion Bureau à distance (RDP) ».

Pour commencer, je vais booter une clé USB avec l’installation de Windows Server 2022.

### Boot de la clé USB

J’ai commencé par installer Rufus, un logiciel pour booter des disques.

Voici les paramètres à choisir pour mon type d’installation :

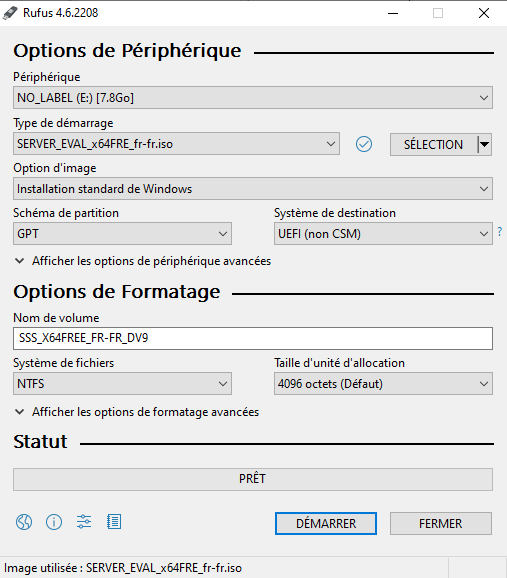
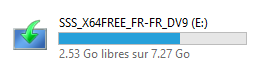


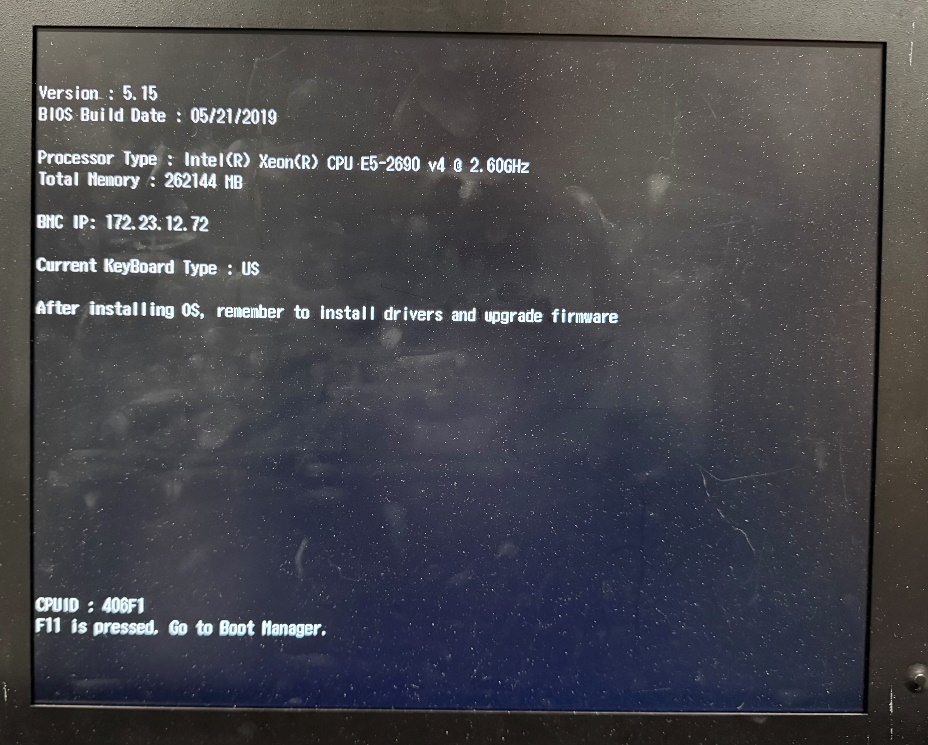
Figure 2 : Sélection des paramètres (boot)

Voici la clé bootée :

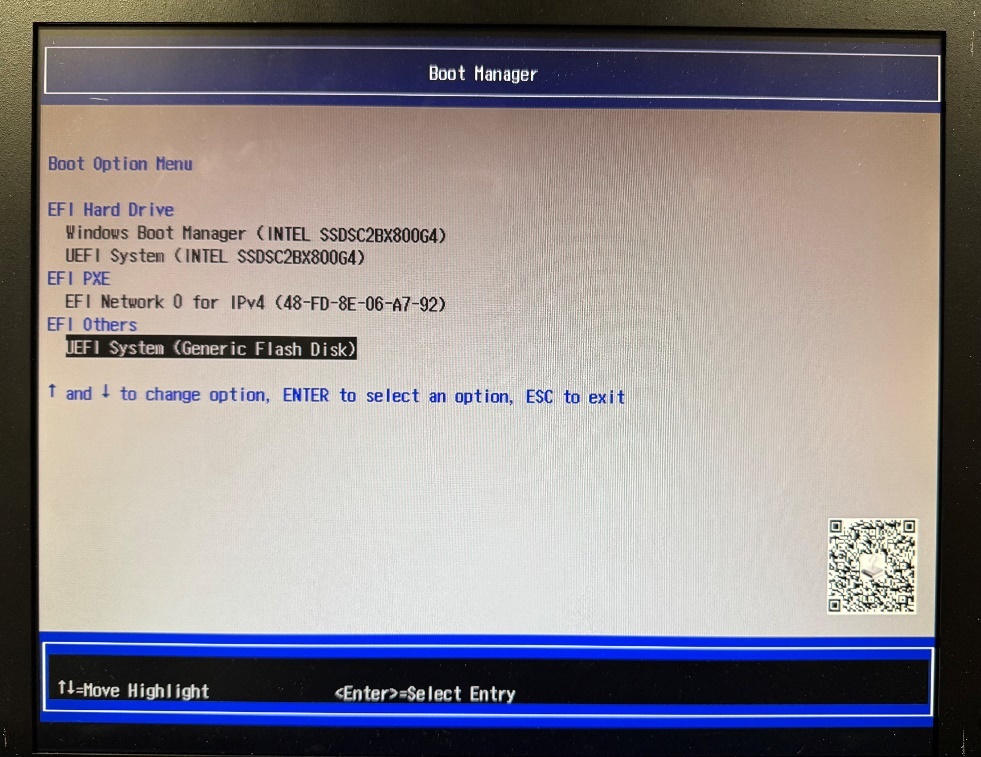


### Installation du serveur

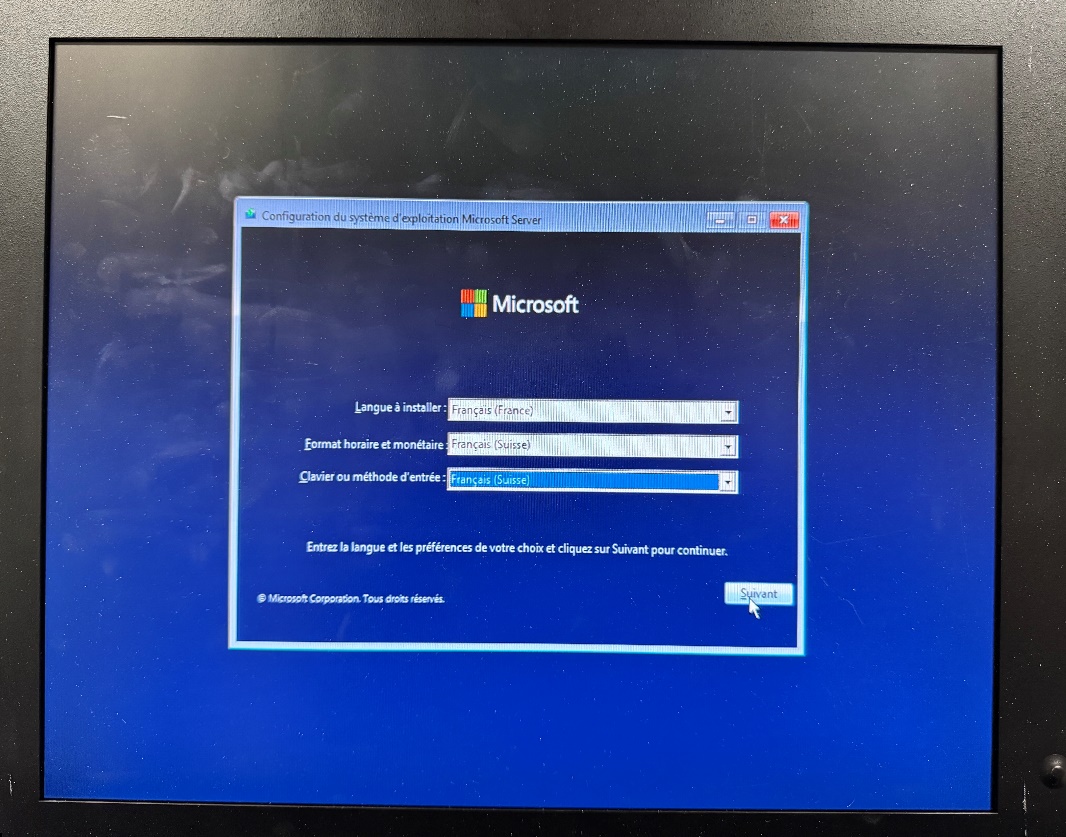
Au moment de l’allumage du serveur, ces lignes-sous s’affichent. Je dois accéder au Boot Manager, et pour ceci, j’appuie sur F11.



Une fois dans le Boot Manager, je sélectionne ma clé USB bootée auparavant, comme ceci.



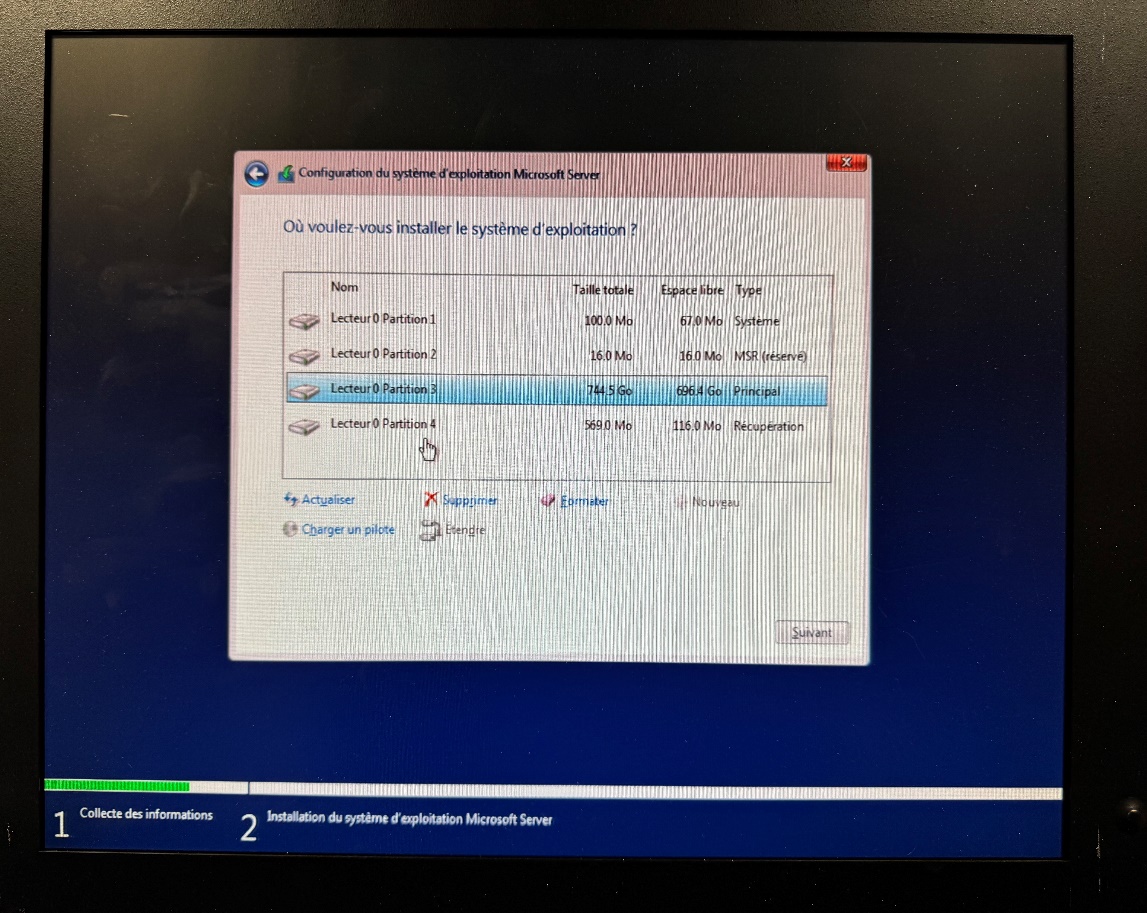
Je sélectionne la langue française avec la région Suisse.



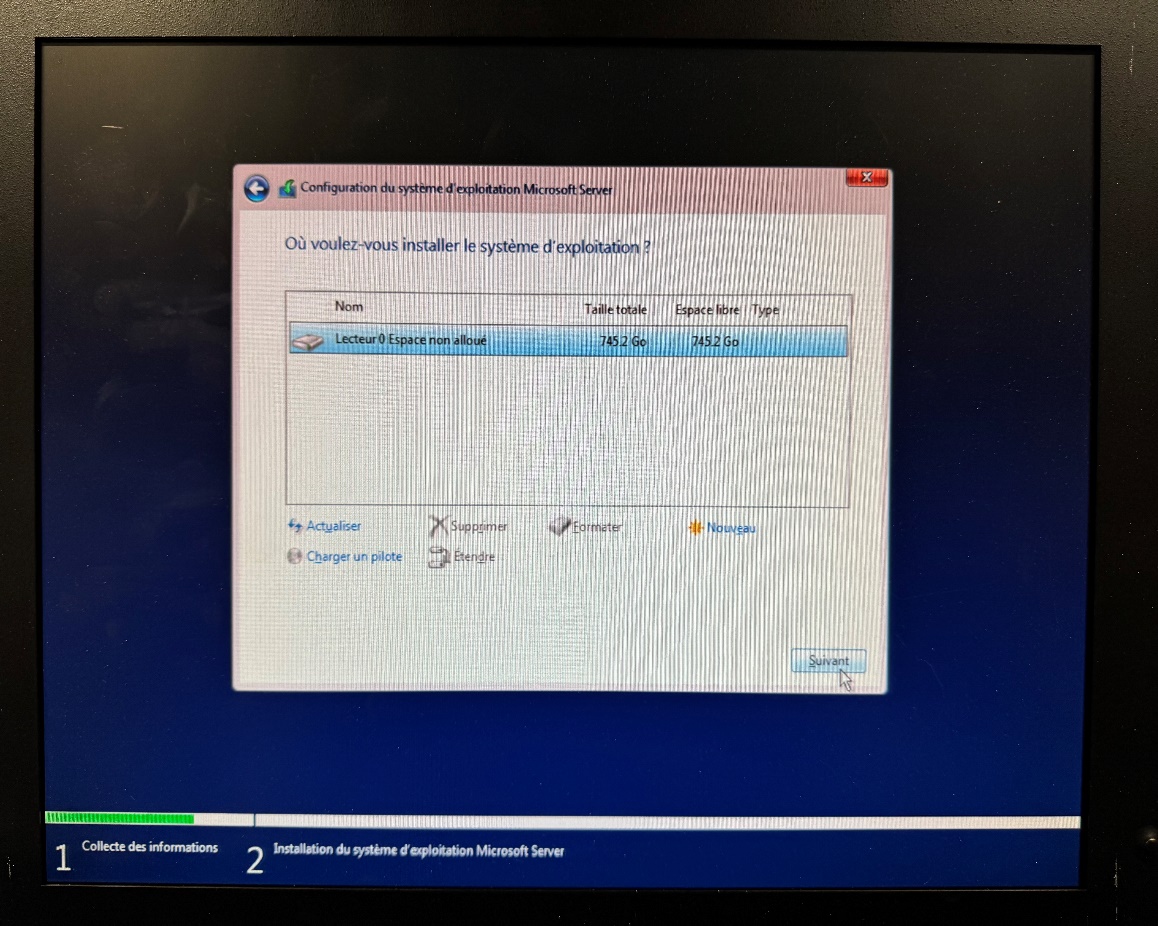
Dans la sélection du système d’exploitation, je choisis la version standard, mais surtout la version graphique et non en lignes de commandes.



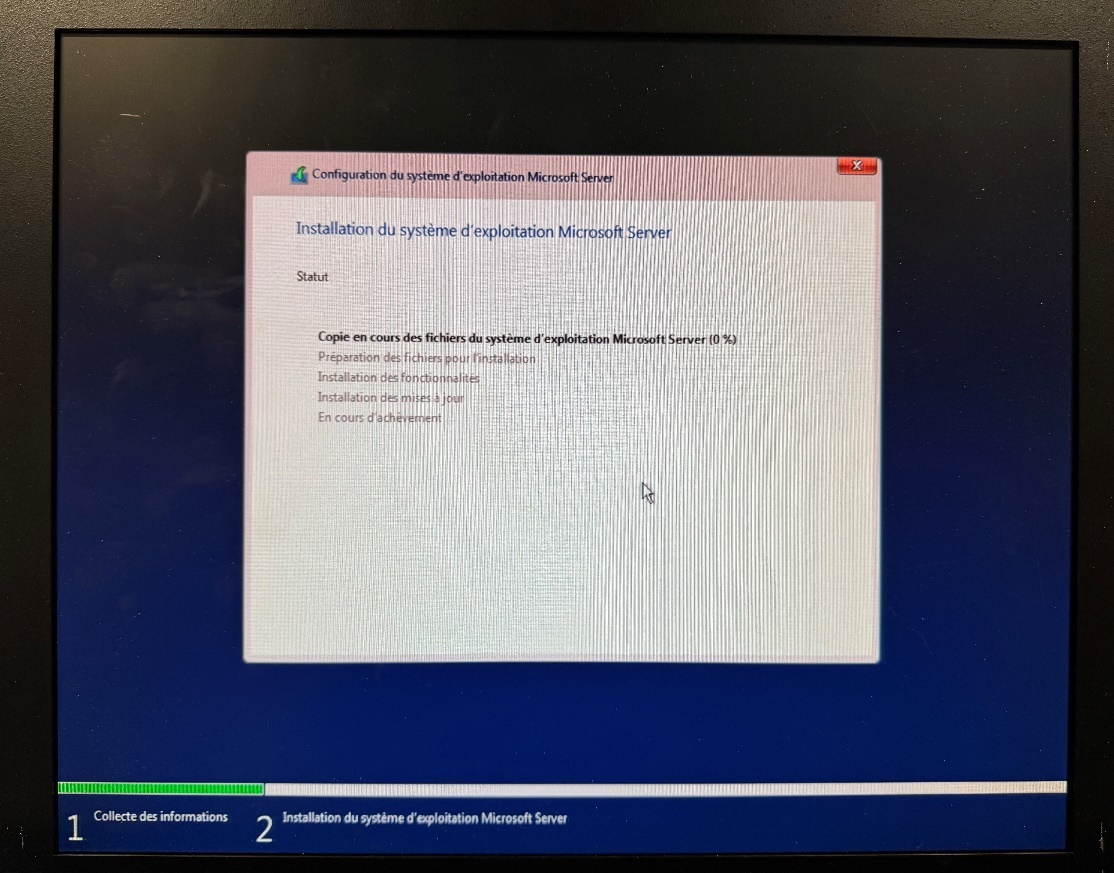
Je choisis de personnaliser l’installation, pour ensuite supprimer toutes les partitions.



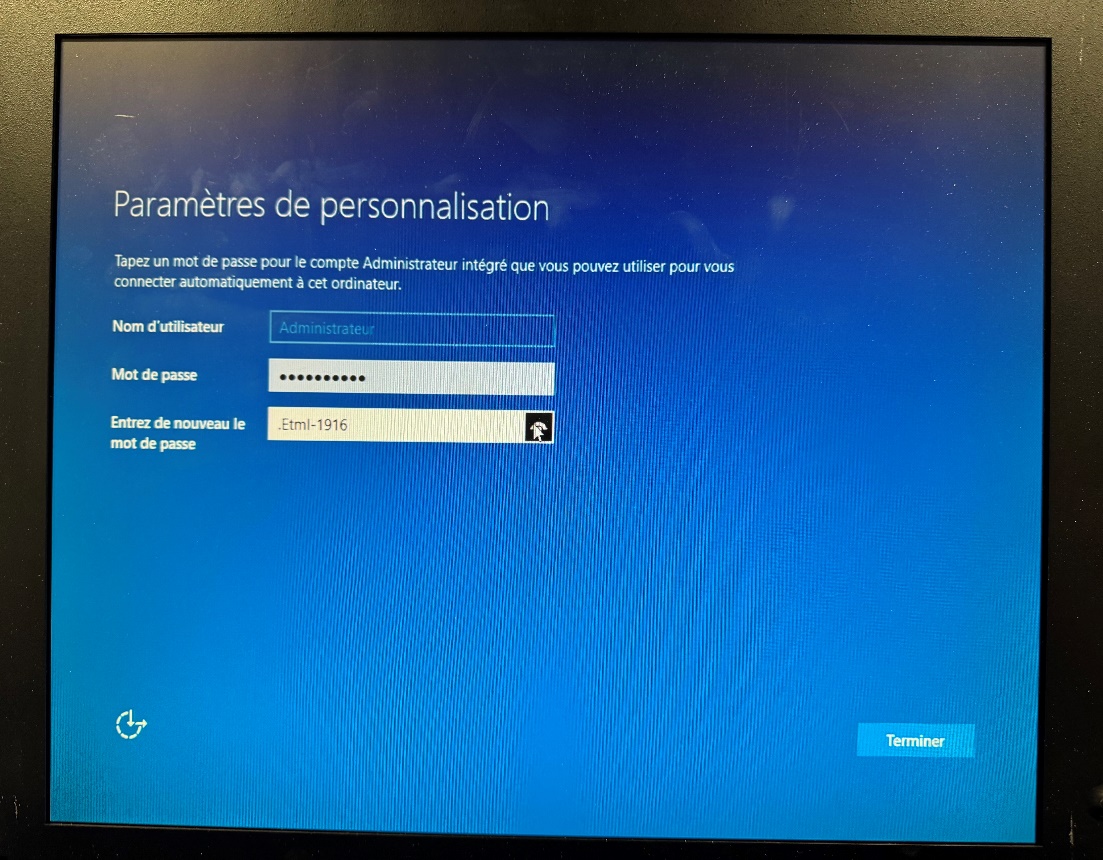
Le résultat doit être ainsi, suffit juste de cliquer sur Suivant pour lancer l’installation.



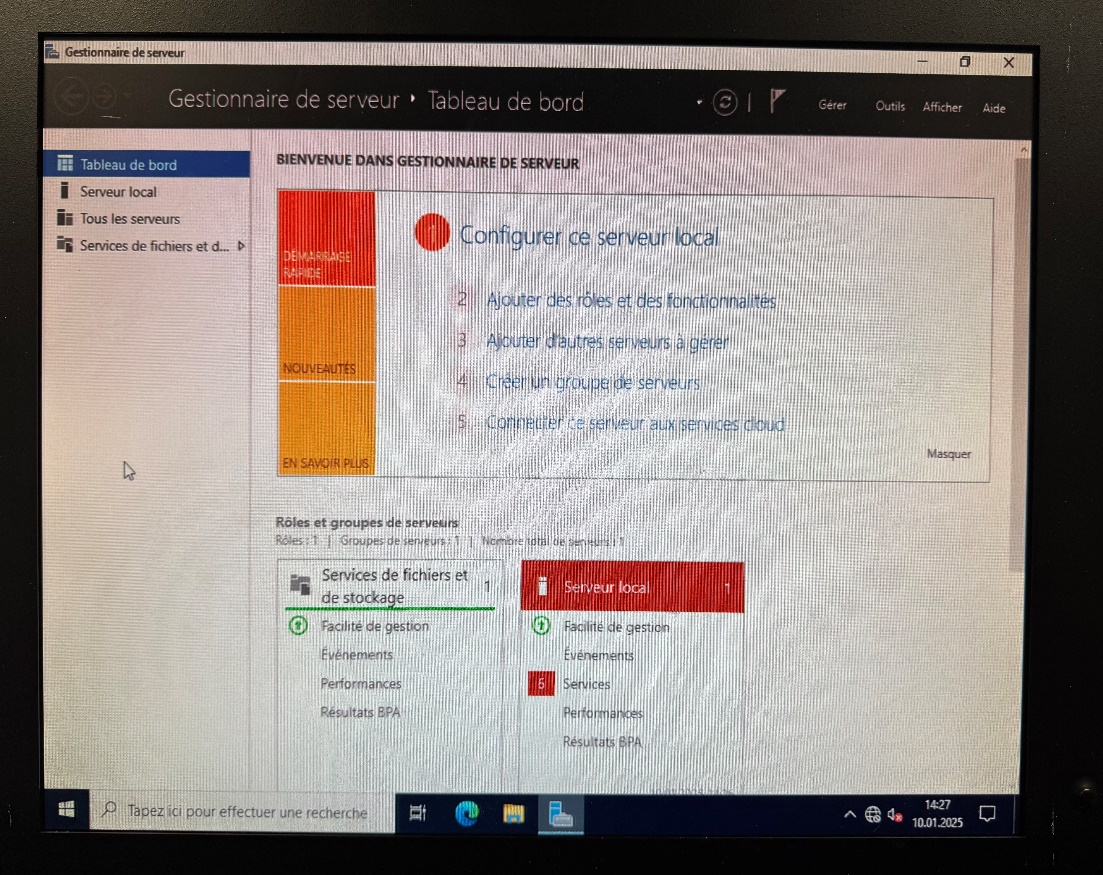
Voici l’installation en cours.



À l’étape du mot de passe, j’ai inscrit .Etml-1916.

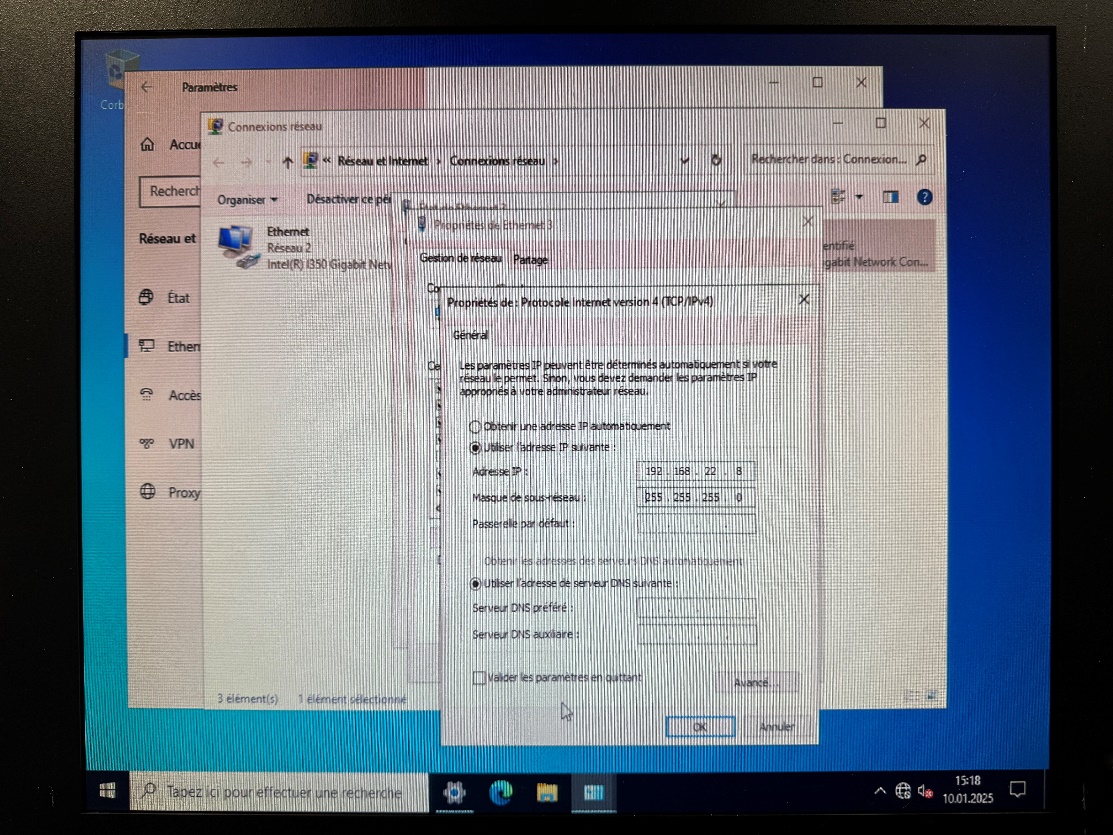


L’installation est finie. Me voici sur le serveur windows.

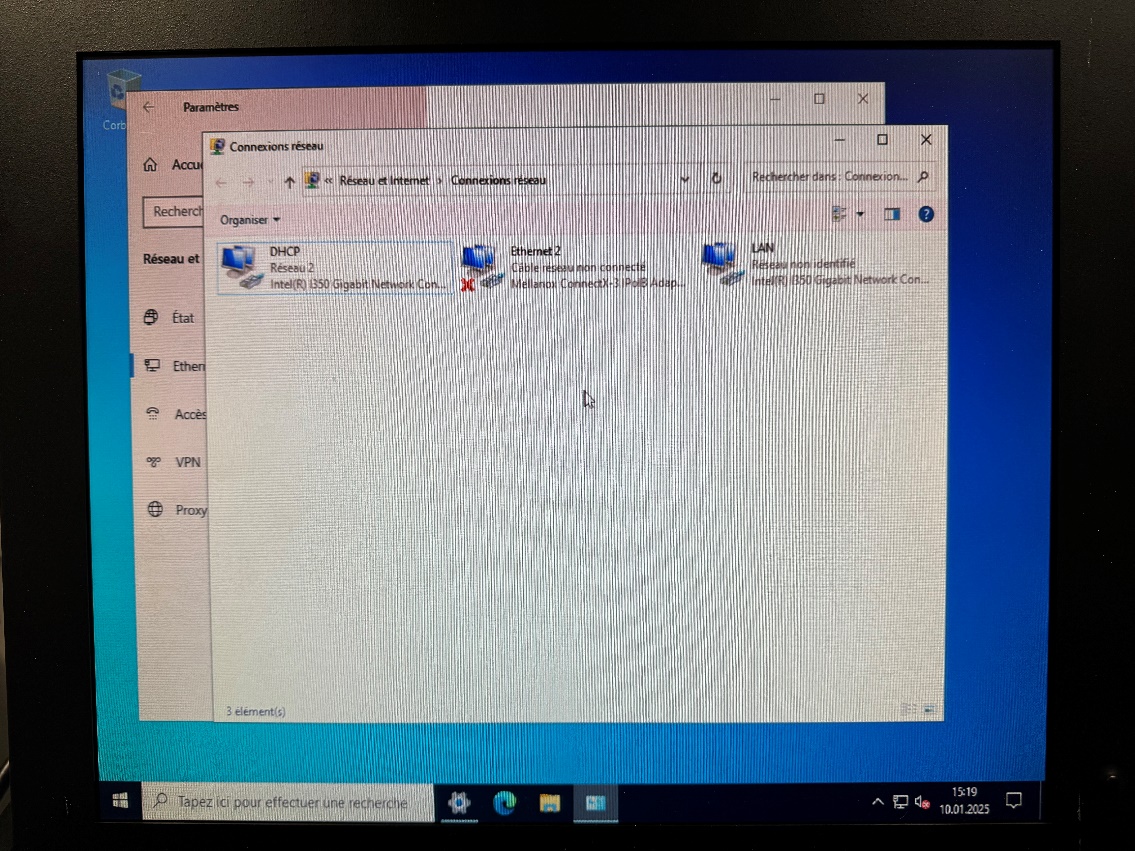


### Configuration réseau du serveur

Sur le deuxième port RJ45 du serveur, j’attribue une adresse IP statique avec le masque de sous-réseaux convenu.

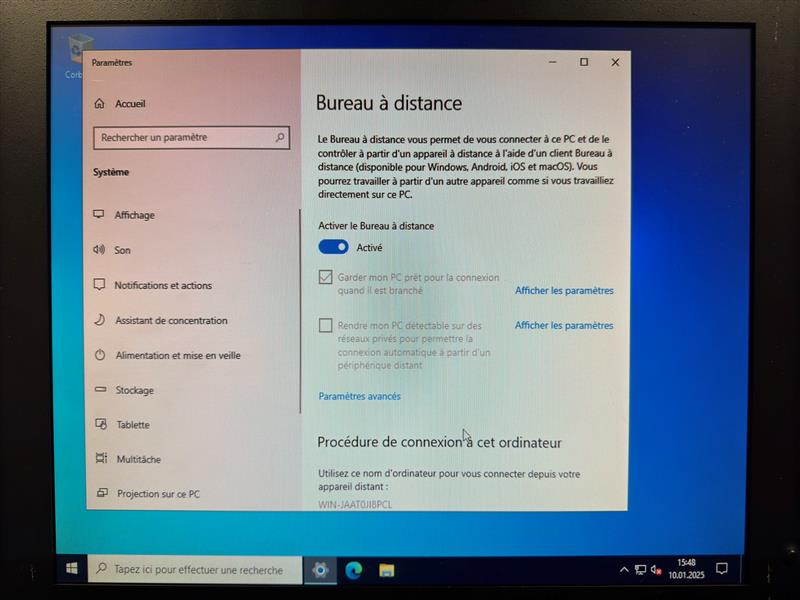


Le premier port RJ45, je laisse le DHCP activé. Pour finir la configuration réseau, je renomme les réseaux en DHCP et LAN.

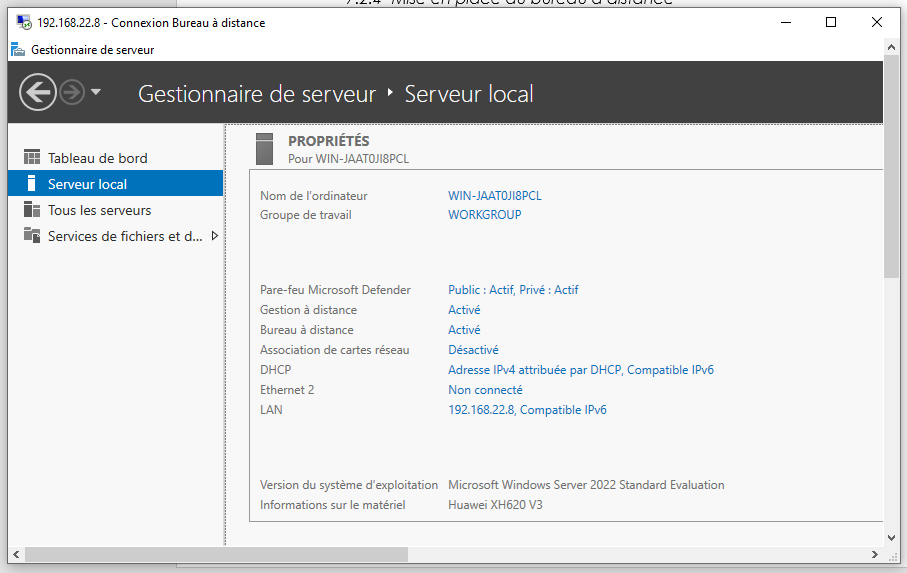


### Mise en place du bureau à distance

Pour activer la connexion de bureau à distance il suffit simplement, depuis le serveur, de se rendre dans les paramètres du bureau à distance, et d’activer le bureau à distance.



Je suis maintenant, depuis mon poste, connecté à distance au serveur.



# Services

## Dynamic Host Configuration Protocol (DHCP)

Le DHCP est un protocole réseau permettant l’attribution automatique des adresses IP aux appareils connectés.

**Rôle principal** : Simplifier la gestion des adresses IP en évitant leur configuration manuelle.

**Fonctionnement** : Lorsqu’un appareil se connecte au réseau, il envoie une requête au serveur DHCP. Ce dernier assigne une adresse IP disponible, ainsi que des informations comme la passerelle par défaut et le DNS.

**Avantages** : Gestion centralisée, réduction des erreurs de configuration et amélioration de l’efficacité administrative.

### Utilisation du service dans le projet

Notre premier serveur possède le DHCP activé et fonctionnel.

## Active Directory (AD)

Active Directory est une solution de gestion des utilisateurs et des ressources réseau développée par Microsoft.

**Rôle principal** : Centraliser l’administration des comptes utilisateurs, groupes, appareils et politiques de sécurité.

**Fonctionnalités clés** :

* Authentification et autorisation des utilisateurs.
* Gestion des droits d’accès aux fichiers, applications et services réseau.
* Application de politiques de groupe (GPO) pour renforcer la sécurité et automatiser les configurations.

**Avantages** : Sécurité renforcée, gestion simplifiée des ressources et évolutivité.

### Utilisation du service dans le projet

Notre premier serveur possède l’Active Directory activé et fonctionnel.

## Domain Name System (DNS)

Le DNS (Domain Name System) est un système essentiel au fonctionnement d'Internet, permettant la résolution des noms de domaine en adresses IP.

Son rôle principal est de traduire des noms de domaine lisibles par l’humain (ex. : www.example.com) en adresses IP compréhensibles par les machines (ex. : 192.168.1.1), facilitant ainsi la navigation sur le réseau.

**Fonctionnement :** Lorsqu’un utilisateur saisit un nom de domaine dans un navigateur, une requête est envoyée au serveur DNS. Ce dernier recherche l’adresse IP correspondante dans sa base de données ou interroge d’autres serveurs DNS pour obtenir la réponse, qu’il transmet ensuite au client.

Avantages :

* Simplifie la navigation réseau grâce à des noms de domaine intuitifs.
* Réduit la complexité de la gestion des adresses IP.
* Optimise la redondance et la rapidité grâce à un système distribué.

### Utilisation du service dans le projet

Notre premier serveur possède le DNS activé et fonctionnel.

## pfSense

pfSense est une solution de pare-feu et de routeur open-source basée sur FreeBSD.

**Rôle principal** : Protéger le réseau contre les intrusions et assurer le routage efficace du trafic réseau.

**Fonctionnalités clés** :

* Gestion avancée des pares-feux pour filtrer le trafic entrant et sortant.
* Support des VPN, comme OpenVPN, pour des connexions sécurisées.
* Surveillance et journalisation des activités réseau pour le diagnostic et la sécurité.

**Avantages** : Fiabilité, flexibilité et coût réduit comparé aux solutions commerciales.

## Open VPN

OpenVPN est une solution de réseau privé virtuel (VPN) open-source qui assure une connexion sécurisée entre un utilisateur distant et le réseau de l’entreprise.

**Rôle principal** : Chiffrer les données échangées entre les employés distants et les ressources internes.

**Fonctionnement** :

* Les employés se connectent via un client OpenVPN qui établit un tunnel sécurisé avec le serveur VPN.
* Le trafic est alors protégé contre les interceptions et attaques.

**Avantages** : Haute sécurité grâce au chiffrement, compatibilité multiplateforme et configuration personnalisable.

### Utilisation du service dans le projet

Ce service n’a pas été implémenté dans ce projet, pour cause du manque de temps. (24 périodes)

## Bureau à distance (RDP)

Le Bureau à distance, ou Remote Desktop Protocol (RDP), permet aux utilisateurs d’accéder à un ordinateur ou un serveur à distance comme s’ils étaient physiquement devant.

**Rôle principal** : Offrir un accès distant aux systèmes pour les administrateurs et les employés.

**Fonctionnement** :

* L’utilisateur lance une session RDP depuis un appareil client.
* Une connexion sécurisée est établie avec le système distant, offrant une interface complète.

**Applications pratiques** : Administration à distance, accès aux ressources de bureau ou dépannage

**Avantages** : Haute sécurité grâce au chiffrement, compatibilité multiplateforme et configuration personnalisable.

### Utilisation du service dans le projet

Nos deux serveurs ont la connexion bureau à distance activées et fonctionnelles.

# Schémas

## Schéma physique du serveur 1

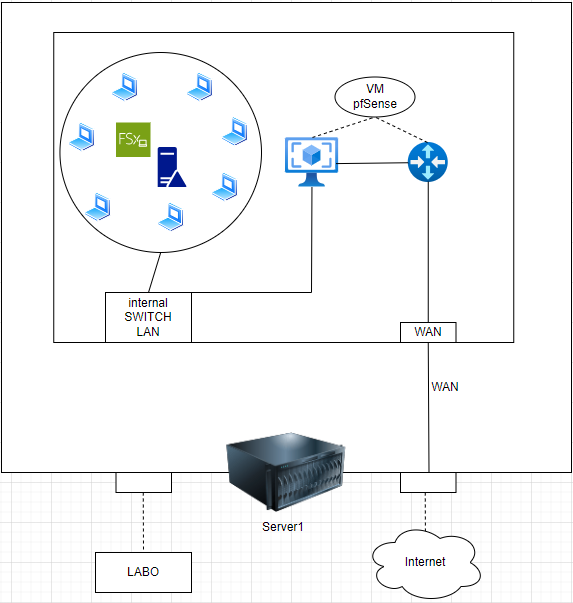


Figure 3 : Schéma physique serveur 1

Le serveur contient 4 ou 5 machines virtuelles suivant le nombre de machine virtuelle pour nos PC client, qui sont-elles créées sur nos PC grâce à l’application Oracle VM VirtualBox.

L’une sert de communication entre l’internal switch LAN et de la sortie WAN, elle est représentée pas un routeur et elle est installée avec pfSense.

Dans le serveur on peut voir un cercle avec pleins de pc clients et au centre un Domain Controller avec un File Server. Ceux-ci ne sortent pas mais peuvent communiquer entre eux.

La sortie WAN depuis la machine virtuelle représentée par un routeur, sort directement sur internet.

Si nous voulons accéder depuis le LABO nous devons nous connecter directement au serveur.

Par la suite, si le temp nous le permet, nous pourrons surement faire une entrée directement sur le LABO.

## Schéma châssis

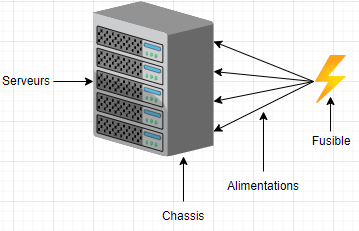


Figure 4 : Schéma châssis

Voici le schéma représentant le fonctionnement en gros d’un Châssis.

Le châssis comporte normalement des serveurs, suivant les châssis nous pouvons avoir un nombre restreint de serveur. Dans notre environnement de ce projet, les châssis ont la capacité d’avoir 8 serveurs. Notre groupe travail que sur les 2 derniers (7-8).

Sur notre châssis il y a 4 alimentations qui sont, elles branchées sur 1 fusible.

Cette installation n’est pas très optimisée contre une éventuelle panne(défaillance) sur le fusible. De base, dans une infrastructure plus grande de plus grosse entreprise, la redondance est un élément très important. Ce qui veut dire que l’on aurait branché 2 alimentations sur 1 fusible est les deux autres sur un deuxième fusible.

Nous devons avoir constamment nos serveurs en marches, c’est pour cela que notre châssis contient 4 alimentations, ce qui permet d’être sûr que lorsqu’une alimentation lâche les autres peuvent toujours garder en marche le châssis.

## Schéma physique de la mise en place du réseau

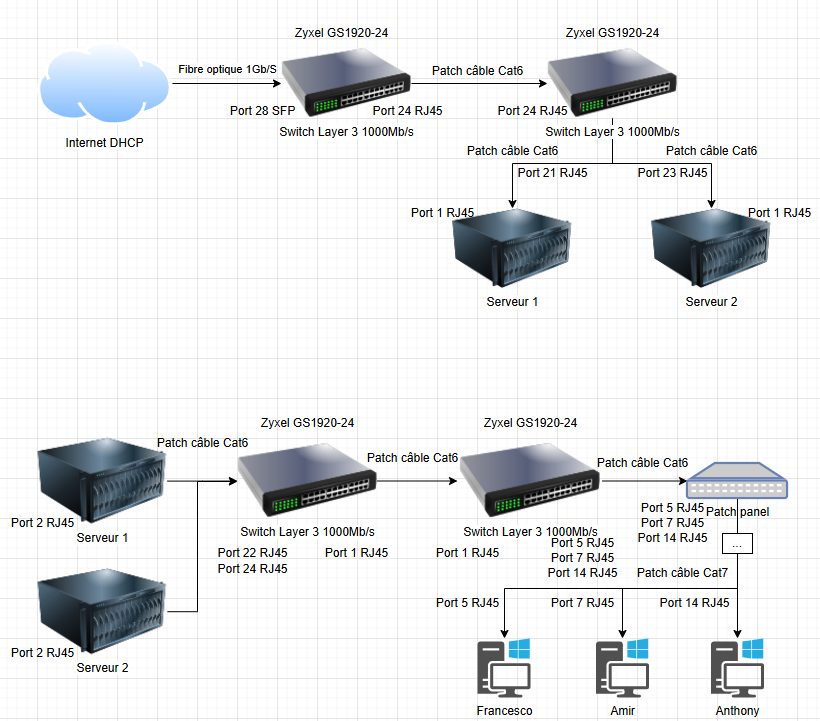


Figure 5 : Schéma physique mise en place réseau

## Schéma VPN

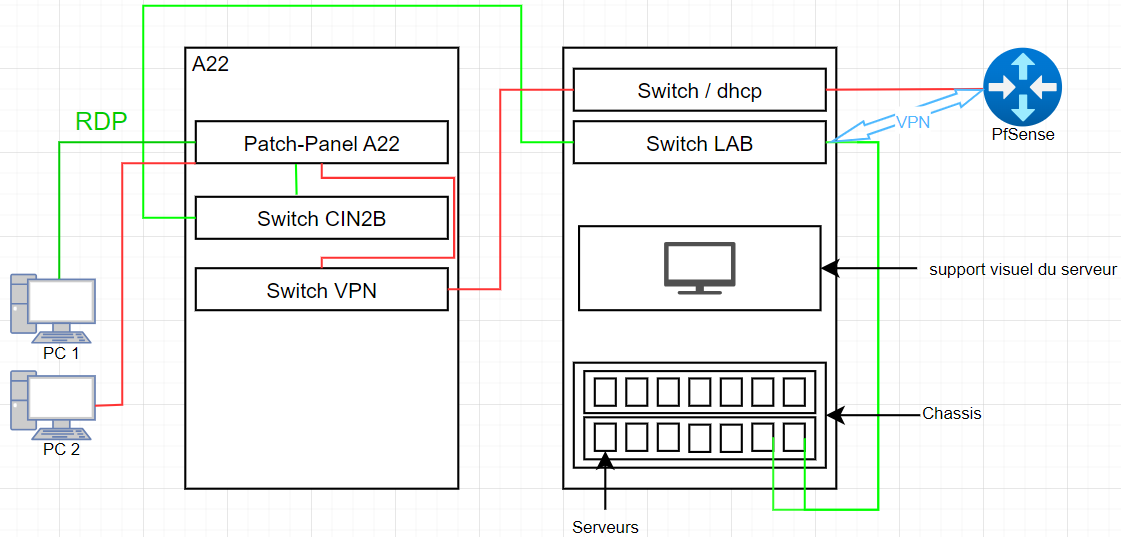


Figure 6 : Schéma VPN

Voici le schéma pour la mise en œuvre de l’installation et de la mise en marche du VPN.

On peut aussi voir la connexion en RDP d’un PC au serveur représenté par la ligne verte.

En rouge on peut voir que la mise en place du VPN se fera par une connexion avec un 2ème PC.

Celui-ci passera par le Patch-Panel de la salle A22 puis par un nouveau switch réservé au VPN qui lui ira directement au switch internet DHCP.

Depuis cet endroit nous allons faire la machine virtuelle qui servira de routeur avec PfSense avec inclus le VPN.

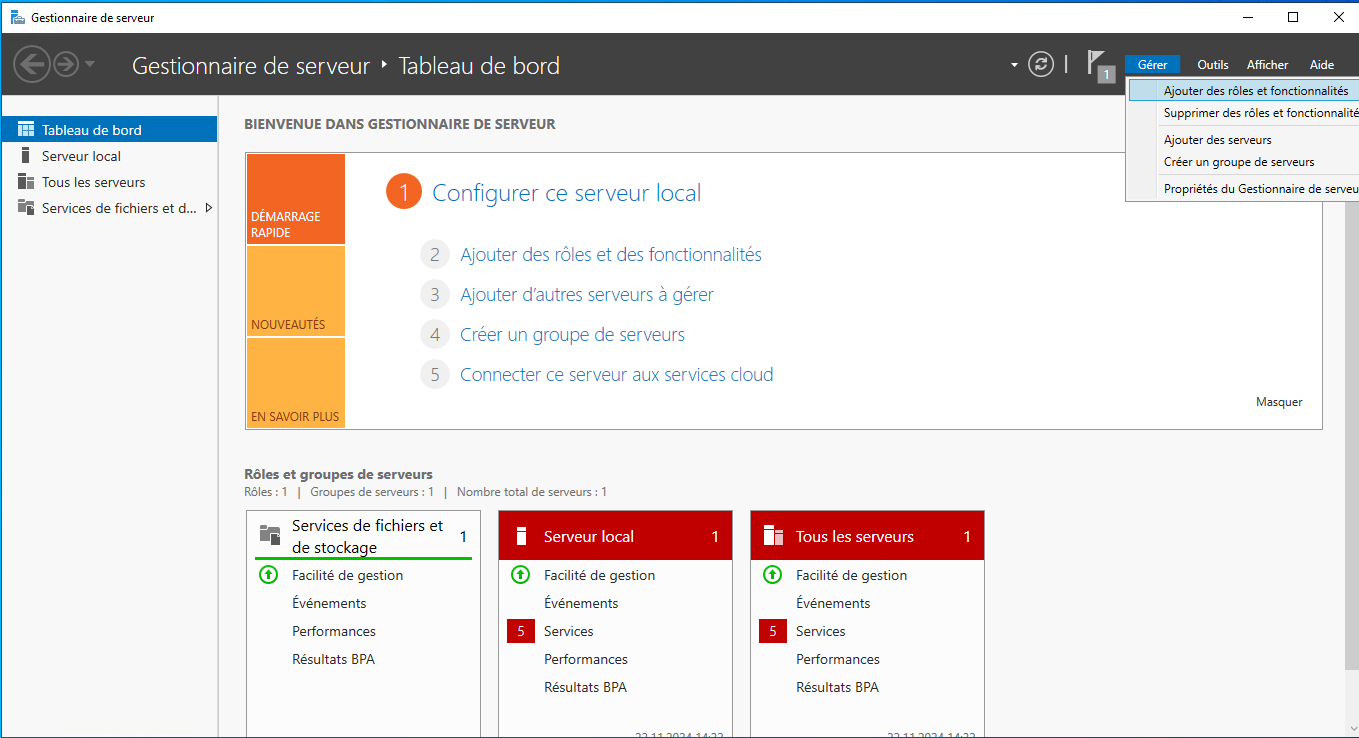
# installation vm

Pour ce projet nous avons dû créer 4 machines virtuelles :

1. pfSense (routeur)
2. Contrôleur domaine : DHCP, DNS, AD DS
3. File serveur
4. PC client

# Installation Hyper-v

Pour commencer nous avons dû ouvrir le **Gestionnaire de serveur** sur notre futur hyperviseur, puis on est allé sur le bouton « **Gérer** », puis « **Ajouter des rôles et fonctionnalités**».



On a passé l'étape « **Avant de commencer** » il n’y rien besoin de toucher.

On a ensuite conservé le choix "Installation basée sur un rôle ou une fonctionnalité" à l'étape "Type d'installation". On a aussi passé l'étape "Sélection du serveur".

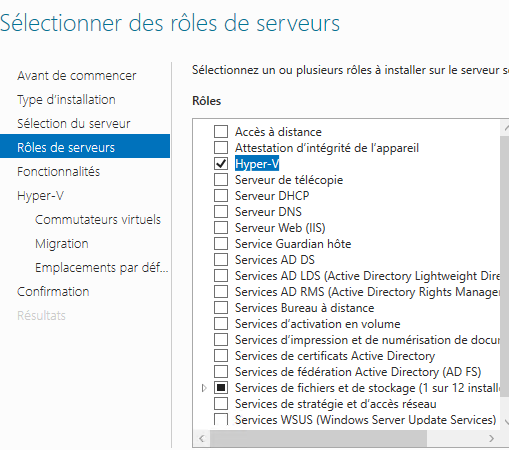
À l'étape « Rôles de serveur », on a coché l’onglet "Hyper-V" dans la liste. Puis, on a validé l'installation des fonctionnalités correspondantes aux outils d'Hyper-V. Ceci va permettre d'ajouter la console "Gestionnaire Hyper-V" ainsi que le module PowerShell pour Hyper-V (ceci ajoute au système, des commandes PowerShell propre à la configuration d'Hyper-V et des VMs).

Figure 7 : Sélection des rôles de serveurs

Par la suite si nous continuons nous allons arriver sur une étape de configuration nommée Hyper-V, où nous allons effectuer la configuration de base de notre hyperviseur.

L’onglet commutateur virtuel (switch virutel en anglais) va nous permettre d’assurer la connectivité réseau des machines virtuelles. Sans switch les machines virtuelles ne peuvent pas être connectées au réseau.

L'assistant d'installation nous propose de créer un premier switch virtuel dès maintenant, en sélectionnant la carte réseau détectée sur la machine. Nous devons donc décocher toutes les cases, et cliquez sur "Suivant". Nous verrons par la suite comment configurer le réseau virtuel.

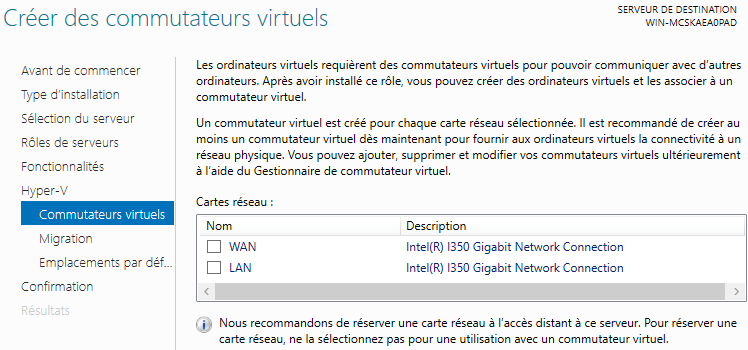


Figure 8 : Création des commutateurs virtuels

Ensuite, un onglet nommée Migration se présente à l'écran. Ceci fait référence à la fonctionnalité d'Hyper-V permettant de migrer des ordinateurs virtuels d'un hyperviseur vers un autre (envoyer ou recevoir).

Pour utiliser cette fonctionnalité, nous devons disposer d'au moins deux hyperviseurs Hyper-V, ce qui ne sera pas le cas pour le moment, donc on a décoché l'option « Autoriser ce serveur à envoyer et recevoir des migrations dynamiques d'ordinateurs virtuels ». Elle peut être activée, désactivée et configurée à tout moment par la suite. Poursuivez quand c'est fait.

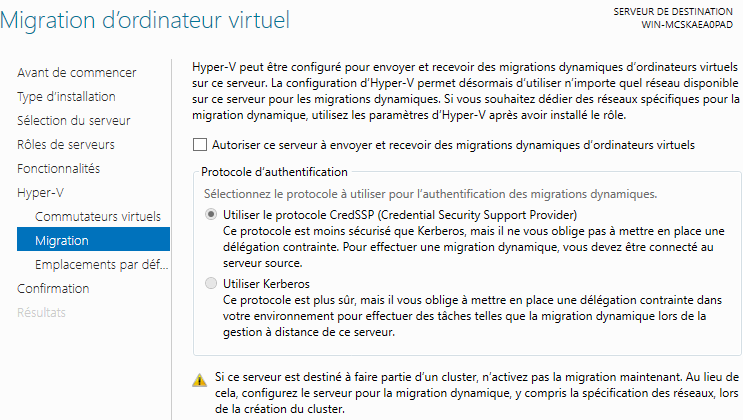


Figure 9 : Migration d'ordinateurs virtuel

Puis pour finir la dernière étape nommée « Emplacements par défaut » s'affiche à l'écran. Il est recommandé de stocker les fichiers relatifs aux machines virtuelles sur un volume dédié et différent de celui du système. Selon les configurations, il peut s'agir d'un volume local ou d'un volume associé à une cible distante (via iSCSI, par exemple).

Le répertoire « Virtual Hard Disks » sera utilisé par Hyper-V pour stocker tous les disques virtuels associés aux machines virtuelles d'Hyper-V. Nous verrons par la suite que tout cela est personnalisable.

Voici un exemple de configuration où nous utilisons le volume « C: » du serveur pour stocker les données correspondantes à nos machines virtuelles :

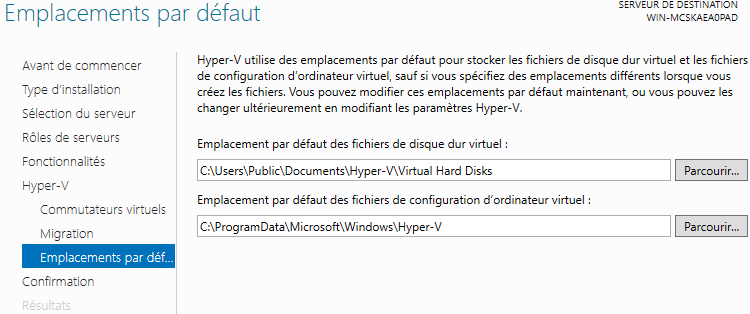


Figure 10 : Emplacements des disques virtuels

Lorsque l'installation est terminée, nous avons dû redémarrer le serveur pour finaliser l'installation du rôle Hyper-V.

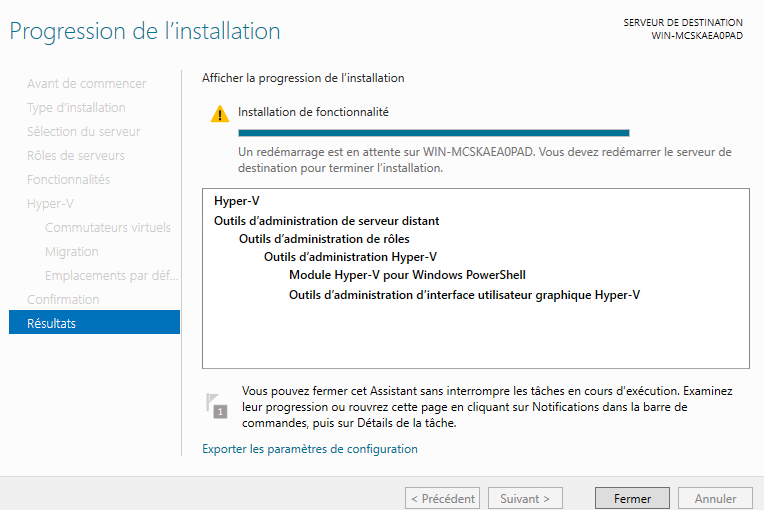
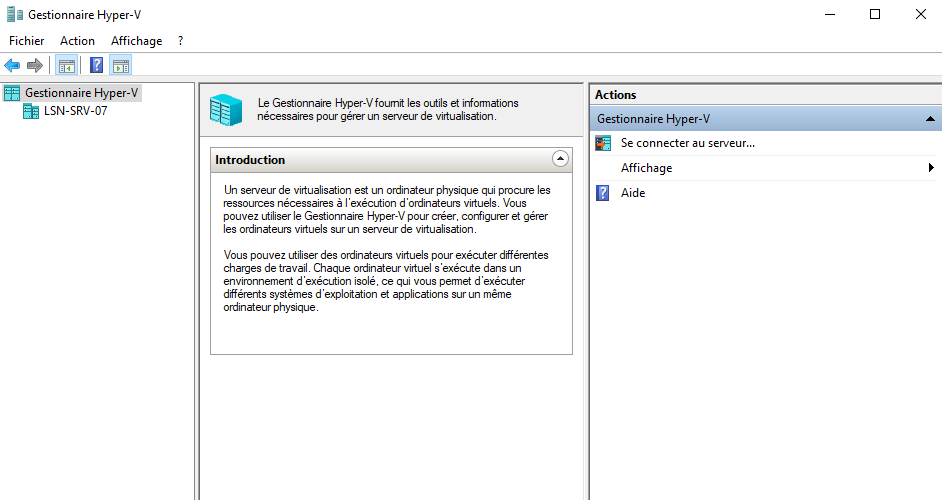


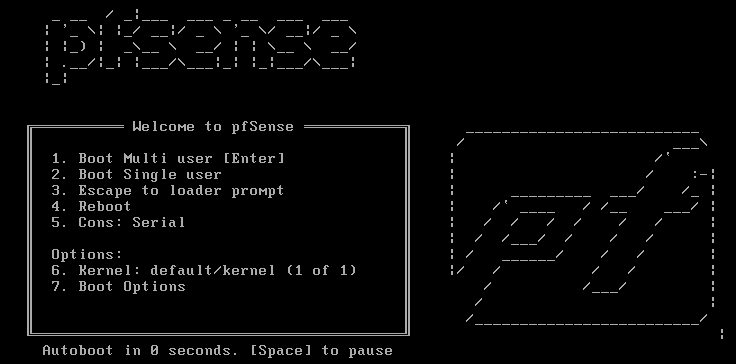
Figure 11 : Progression de l'installation Hyper-V

A partir de maintenant Hyper-V est installer et nous pouvons le vérifier en cherchant dans la barre des tâches « Gestionnaire Hyper-V »

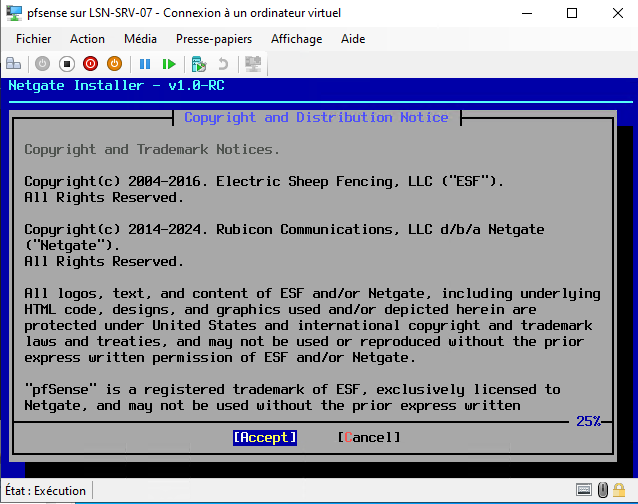


# Installation PfSense

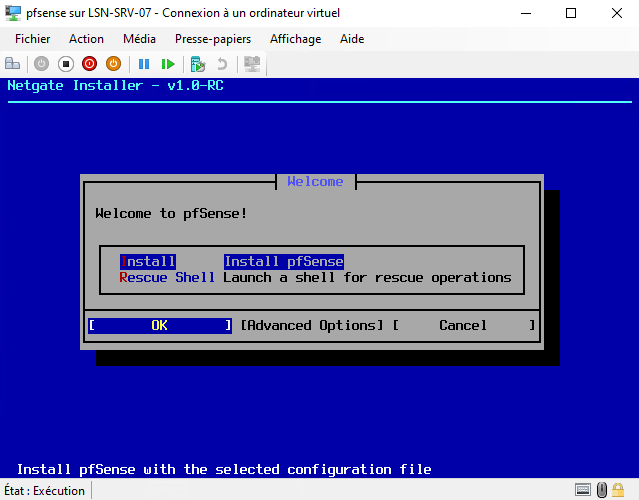
Commençons tout de suite par installer pfsense. Après avoir insérer l’ISO de pfsense dans la VM, la machine peut être démarrer et le setup va démarrer automatiquement après quelques secondes.

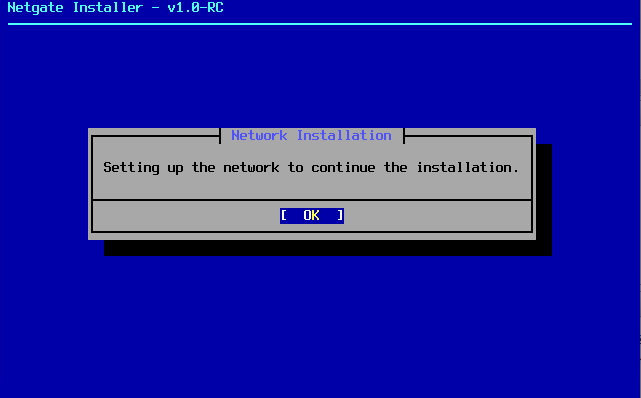


L’installation commence par l’acceptation des Copyright, qu’il faut Accepter.

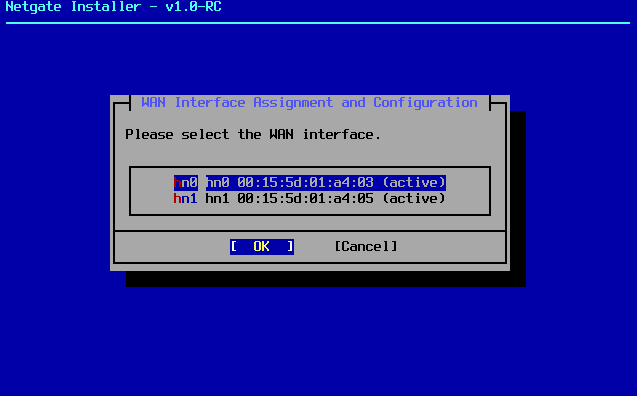


Il faut ensuite vérifier d’être bien sur « Install » et appuyer sur OK pour commencer l’installation.

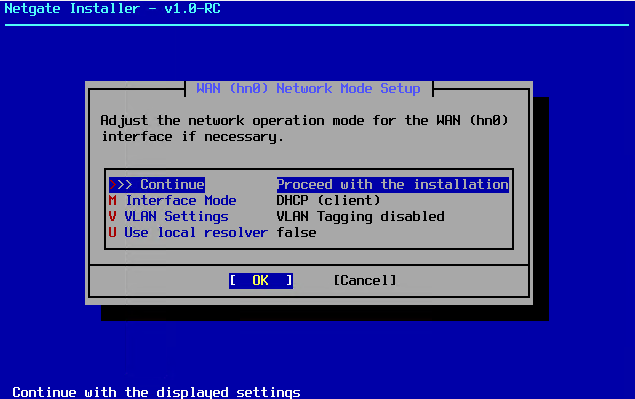




Ici il est demandé de sélectionner l’interface pour la carte réseau virtuel WAN. Cette configuration peut aussi être faite après l’installation de pfsense.



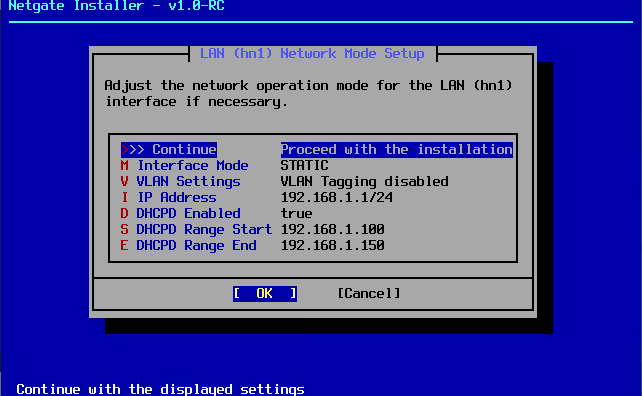
Cette page est la Mode Setup pour l’interface WAN, qui permet de modifier des informations si ont été mises fausses et rajouter des options supplémentaires s’il faut.



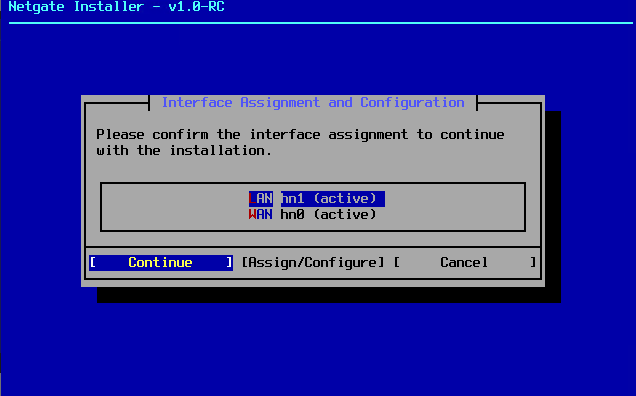
Ensuite comme pour l’interface WAN, il est demandé de sélectionner l’interface pour la carte réseau virtuel LAN.



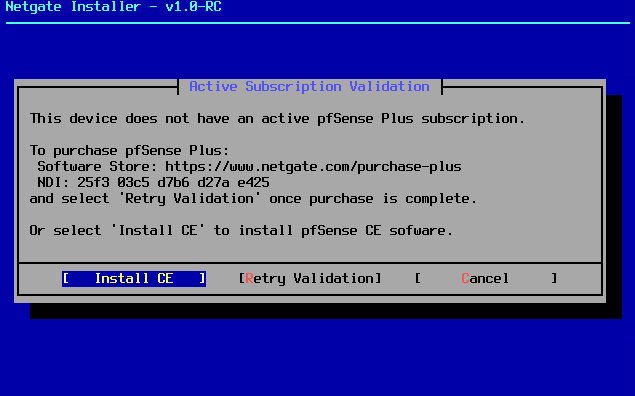
Mode Setup mais pour l’interface LAN



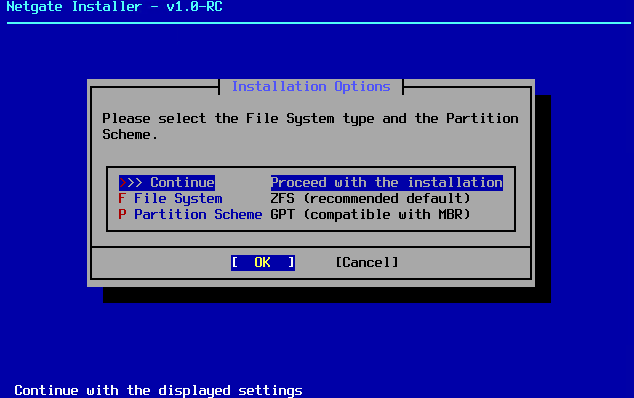
Ici il faut confirmer l’attribution des cartes réseaux aux interfaces pour continuer l’installation.



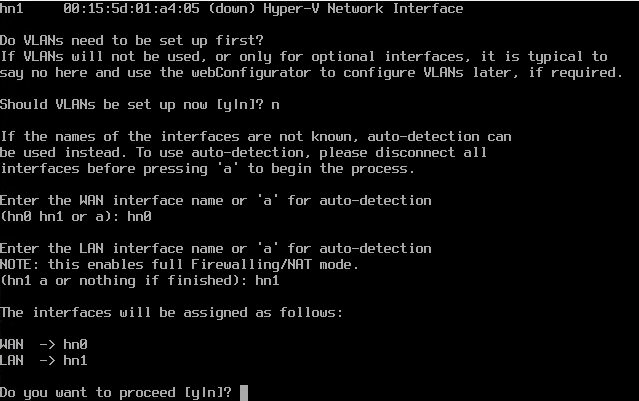
Il nous est ensuite demandé d’installer un certificat CE pour installer pfSense CE software, car la machine n’a pas de suscription actif pour pfSense.



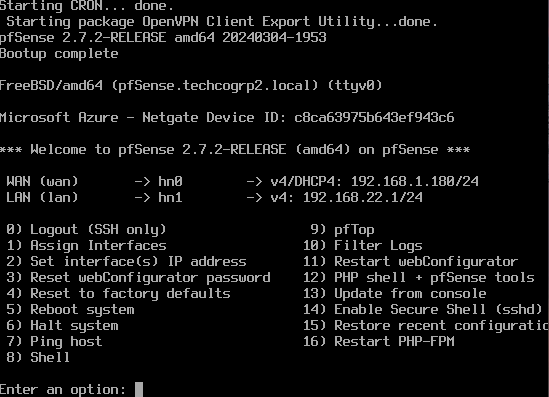
Ici il est demandé de choisir le type de partition pour continuer l’installation mais on sélectionne sur Continue qui est l’option par défaut qui se trouve en MBR Dos Partitions.



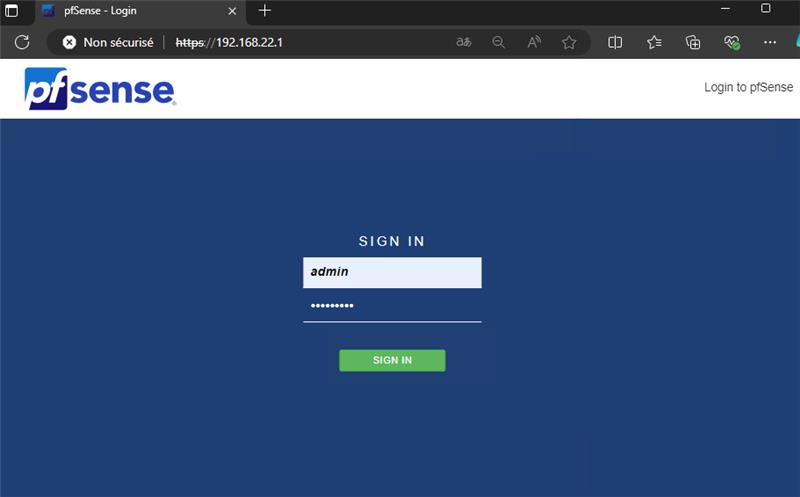
Vers la fin de l’installation il demande une dernière confirmation pour l’attribution des interfaces où il faut confirmer le choix pour compléter l’installation.



Une fois complété l’installation on se trouve avec cette interface qui montre le WAN avec une adresse IP automatique attribuée par le DHCP et le LAN en mode statique avec l’adresse IP 192.168.22.1.



Enfin il faut se rendre sur n’apporte quel navigateur sur une machine qui fait partie de la même infrastructure (ex IP : 192.168.22.2) avec le switch virtuel LAN qui se trouve en privé et insérer l’adresse IP de l’interface LAN (192.168.22.1) pour se retrouver sur cette page :

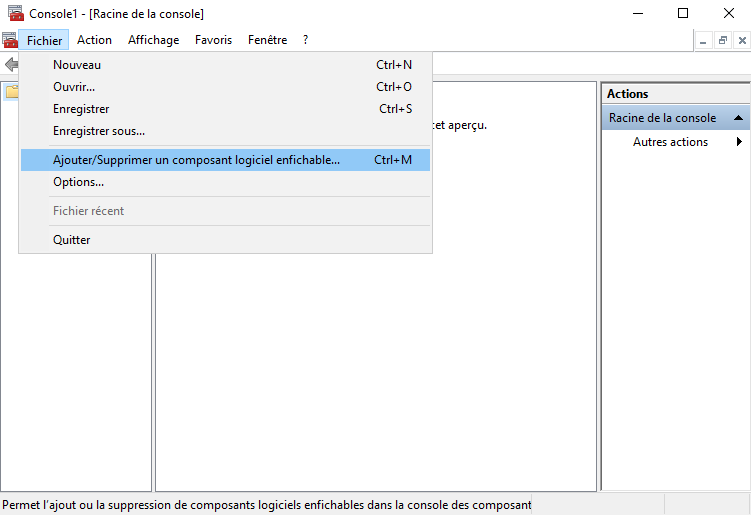


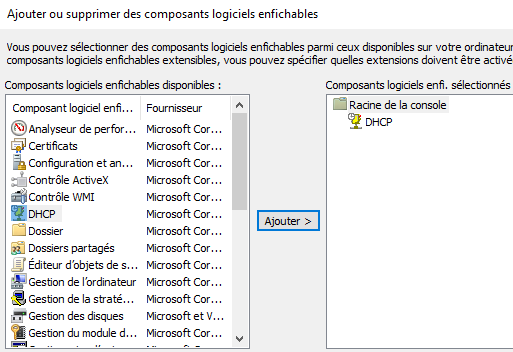
# Installation dhcp

1. Tout d’abord il faut se rendre dans le Gestionnaire de Serveur > "Gérer" et "Ajouter des rôles et fonctionnalités"
2. Arriver jusqu’à la liste des "Rôles de serveur" et cochez "Serveur DHCP" et ensuite l’installer.

## Configuration du service DHCP

1. Ensuite Ouvrir un "mmc" (Microsoft Management Console) et rajouter le DHCP





1. Créer une nouvelle étendue qu’on va appeler "zEtendue" avec les configurations suivantes :

Plage d’adresse IP : 192.168.22.50 à 192.168.22.100/24

Durée du bail : 6 jours (Le bail sert pour attribuer une adresse IP avec une durée, dans ce cas 6 jours)

Routeur : 192.168.22.1, option d’étendue 003

1. Activer l’étendue
2. Modifier l’adresse IP de la machine cliente en automatique pour qu’elle puisse avoir une adresse IP attribuer par le DHCP.
3. Faire ipconfig /release et ipconfig /release dans l’invite de commande sur la machine cliente pour que le DHCP puisse distribuer l’adresse IP (192.168.22.50)

# Installation dns

## Installation du service DNS

1. Comme il a été fait pour le DHCP il faudra aller dans le gestionnaire de serveur et rajouter le rôle "Serveur DNS " et ensuite l’installer.

## Configuration du service DNS

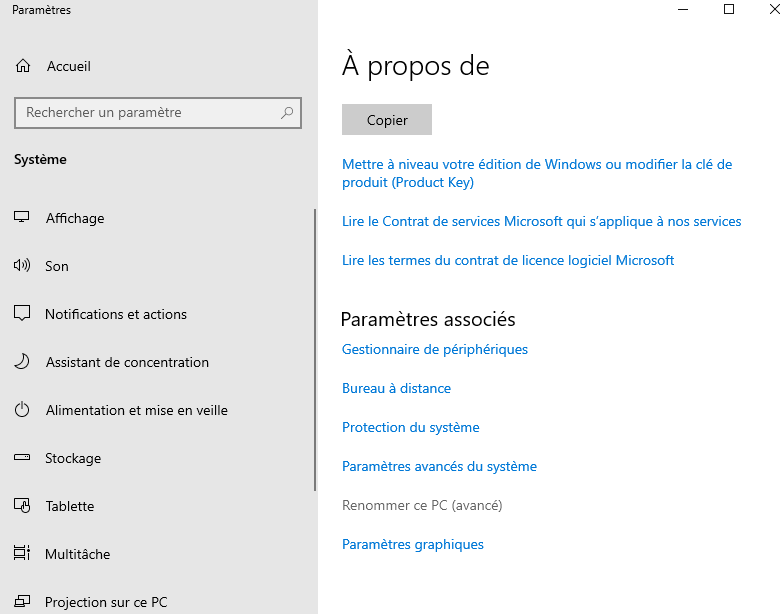
1. Aller dans le MMC et rajouter le DNS
2. Ensuite créer 1 nouvelle zone pour la zone de recherche directe et une pour celle inversée :

Configuration pour celle directe (Les zones de recherche directe sont principalement utilisées pour mapper les noms de domaine à leurs adresses IP correspondants):

1. Principal
2. Nom de la zone : techcogrp2.local
3. Autoriser les mises à jour dynamiques

Configuration pour celle inversée (Les zones de recherche inversée s’occupent de mapper les adresses IP aux noms de domaine) :

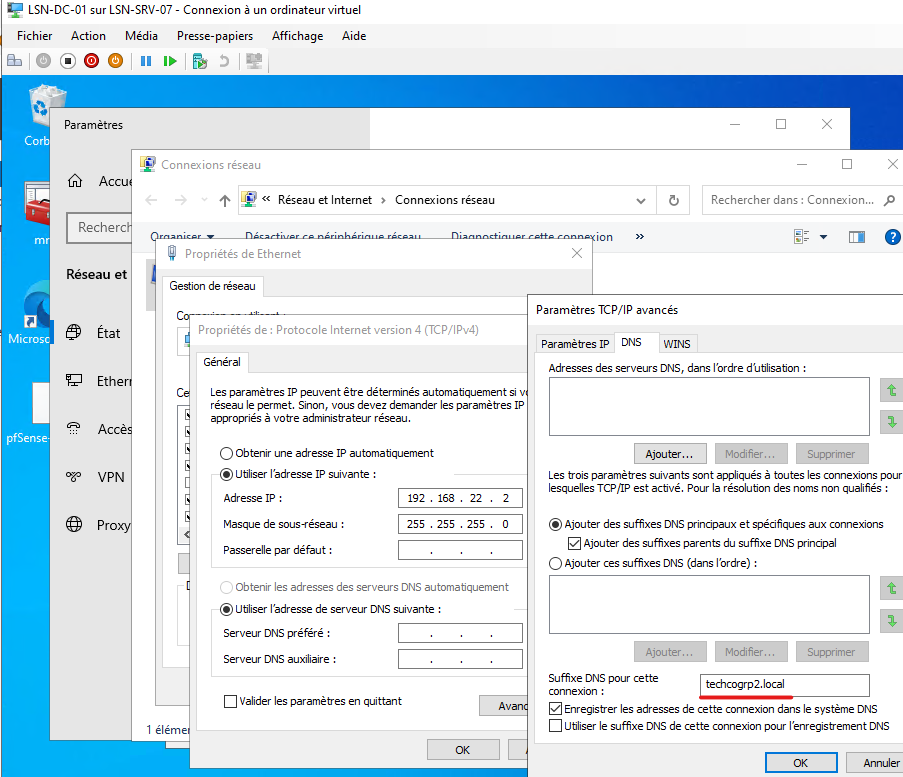
1. Principal
2. IPv4
3. ID réseau : 192.168.22
4. Autoriser les mises à jour dynamiques
5. Puis aller dans le paramètre pour modifier le nom du PC



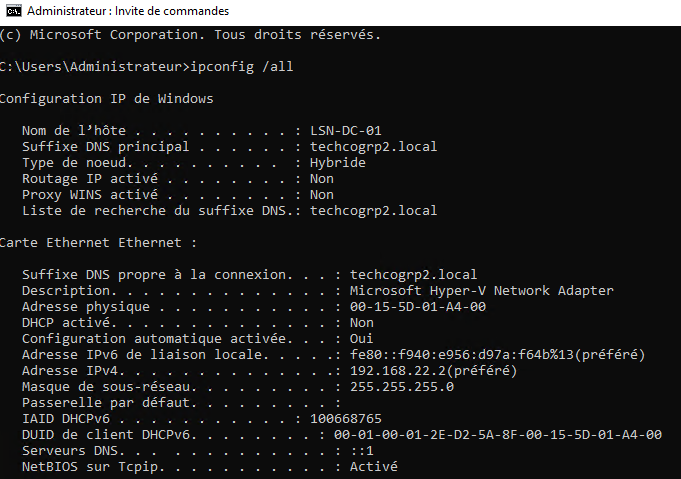
"Modifier" > Autres > et rajouter le suffixe DNS "techcogrp2.local"

Ça va demander de redémarrer le Serveur, mettre ultérieurement.

1. Modifier aussi le suffixe DNS via le protocole TCP/IP > Avancé > DNS > Suffixe DNS pour cette connexion : techcogrp2.local



Après avoir terminé cette configuration redémarrer le serveur et voir dans l’invite de commande avec la commande ipconfig /all si y a les 3 techcogrp2.local

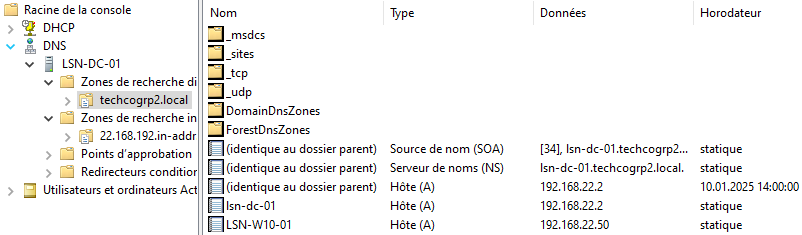


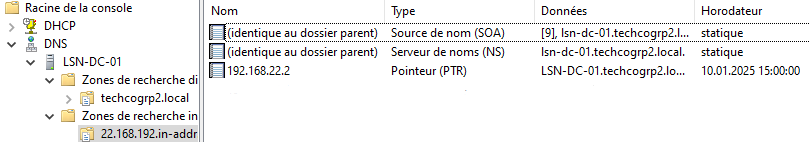
1. Répéter le même processus sur le PC client
2. Via le mmc rajouter dans le Options Serveur du DHCP les options 6 et 15

Pour l’option 6 : Insérer l’adresse IP du serveur (192.168.22.2)

Pour l’option 15 : techcogrp2.local

1. Enfin il faudra vérifier auprès du service DNS, que les ordinateurs possèdent les enregistrement DNS adéquats, comme les suivants :





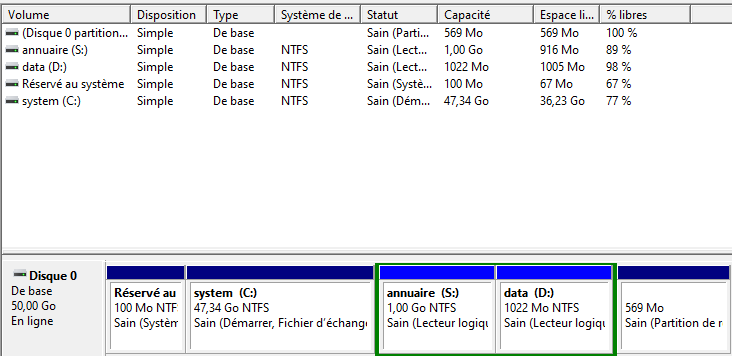
## Test du service DNS

1. Faire un Ping du nom du serveur à partir de la machine cliente pour voir si on voit l’adresse IP du serveur
2. Faire un Ping de l’adresse IP avec –a (Résout les adresse IP en noms d’hôtes, affichant le nom d’hôte associé à l’adresse IP) et vérifier si le nom du serveur est affiché.

# Installation ad ds

## Préparation pour l’installation de l’AD DS

1. Il faut créer une nouvelle partition qu’on va appeler annuaire, cette partition va être utilisé pour stocker les bases de données de l’AD DS :
2. Aller dans Gestion des disques et créer deux nouvelles partitions de 1GB :



## Installation du service AD DS

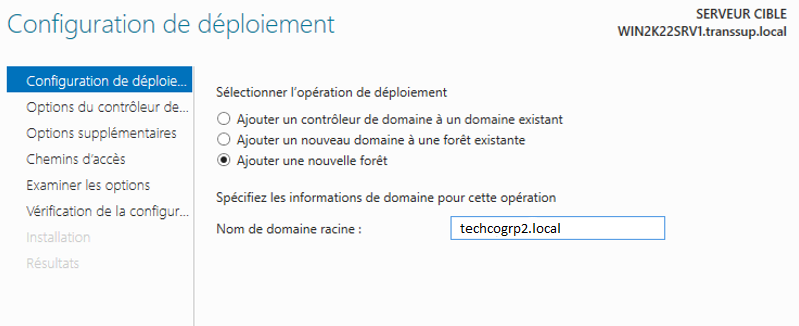
1. Comme il a été fait pour le DHCP et le DNS il faudra aller dans le gestionnaire de serveur et rajouter le rôle "Services AD DS " et ensuite l’installer.

## Configuration du déploiement

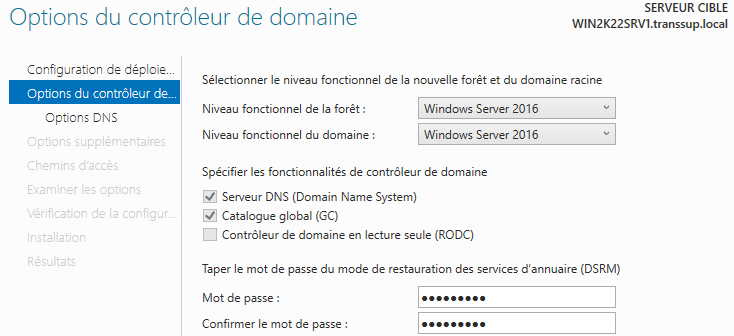
1. Après l’installation du rôle il faudra aller dans les notifications du gestionnaire de serveur et appuyer sur « Promouvoir ce serveur en contrôleur de domaine »



1. Ensuite il faudra créer une nouvelle forêt :



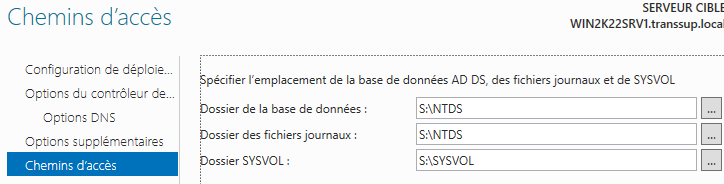
1. Rajouter un mot de passe qui verra utilisé pour intégrer les machines au domaine



1. Décocher cette option :

Cette option permet d’organiser efficacement l’espace de noms en plusieurs zones, facilitant ainsi la gestion et la réplication des informations de résolution de noms sur différents serveurs DNS.

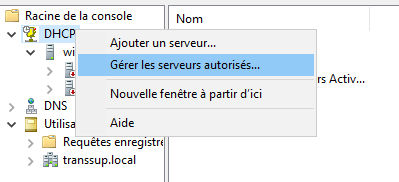
1. Laisser Le nom de domaine NetBIOS par défaut
2. Spécifier les emplacements de la DB AD DS et des fichiers journaux et de SYSVOL :



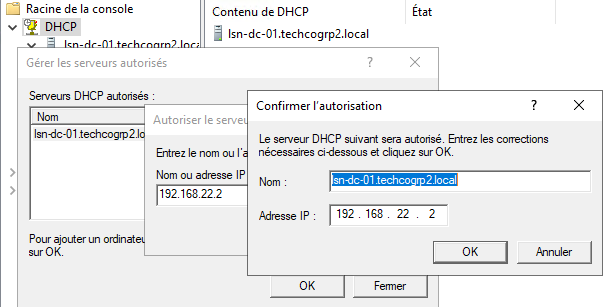
1. Après cette configuration il faut compléter l’installation et redémarrer le serveur

## Autorisation du DHCP

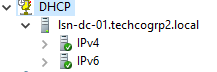
1. On peut constater que notre service DHCP ne plus fonctionnel, du coup il faudra l’autoriser :



1. Autoriser le serveur en rajoutant son adresse IP

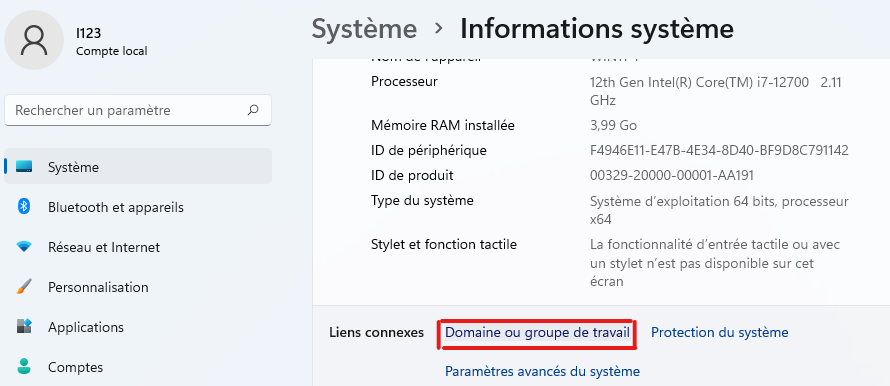


1. Actualiser pour voir si le serveur DHCP est fonctionnel



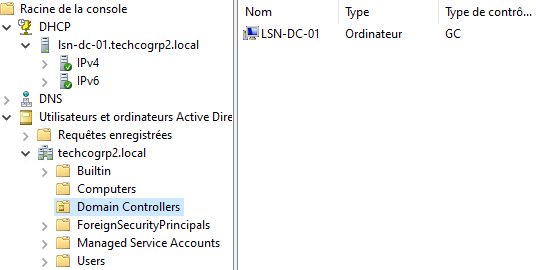
## Intégration au domaine

1. Intégrer les zones directe et indirecte de techcogrp2.local à l’annuaire d’entreprise
2. Aller sur la machine cliente et intégrer le pc au domaine :



Modifier > Sélectionner « Domaine » et rajouter le domaine « techcogrp2.local »

1. Vérifier si le serveur LSN-DC-01 est bien le Catalogue Global (GC)



# Problèmes rencontrés

## Boot de la clé USB

Dans l’installation des serveurs nous avons eu besoin d’une clé USB bootée avec l’ISO Windows Server 2022. C’est le professeur qui nous l’a fournie, mais il y a eu un problème avec cette clé.

# Conclusion

## Personnelle

### Francesco

Pour ce projet, je me suis chargé de la partie pratique, en créant l'infrastructure. J'ai mis en place un serveur DC (Domain Controller), un serveur de fichiers (non finalisé), un firewall pfSense avec une configuration partielle d'OpenVPN, ainsi qu'une machine cliente. Malheureusement, je n'ai pas pu avancer sur le serveur de fichiers, car, à cause d’une mauvaise organisation dans l’équipe, les autres membres n’ayant pas travaillé sur la partie pratique ont dû rattraper et poursuivre le projet différemment.

Cela dit, j’ai apprécié refaire ce projet, car il m’a permis de consolider mes connaissances et d’améliorer certains aspects de ma méthode de travail. De plus, ayant déjà réalisé ce projet l’année passée, j’ai pu aider mes coéquipiers dans leurs tâches, ce qui m’a également permis de développer davantage mes compétences.

### Amir

En passant par la petite frustration du manque de pratique et en finissant par l’installation du deuxième serveur. Je dois dire que j’ai réellement apprécié réaliser, étudier, analyser et planifier ce projet. La mise en place de serveurs et en plus général la mise en réseau, c’est quelque chose qui me passionne en informatique. Au début, c’était un peu flou pour moi, comme je ne connaissais pas pfSense, OpenVPN et certains termes spécifiques. Mais j’ai pu m’en sortir, grâce à la documentation sur internet mais aussi grâce à Francesco, qui lui, avait déjà fait ce projet l’année passée.

### Anthony

J’ai beaucoup apprécié ce projet, le fait de pouvoir travailler en groupe aussi a été une bonne idée, peut-être avec des groupes de 2 la départissions des tâches aurait été plus simple. Le fait de toucher aux matérielles étaient beaucoup plus intéressant que d’autre projet. Si je devrais refaire ce projet je le ferais.