

PROJET 1 – SIO1

DOCUMENTATION TECHNIQUE

SOMMAIRE

Présentation du projet	3
Contexte de la mission.....	3
Intitulé de la réalisation professionnelle	3
RESSOURCES FOURNIES.....	3
Schéma réseau.....	4
Mise en place d'un Serveur Windows	4
Installation du serveur	4
Configuration réseau du serveur.....	11
Installation du service ADDS DNS.....	13
Configuration du domaine.....	17
Création des Unités d'organisations et des utilisateurs	22
Mise en place d'un routeur PfSense	25
Installation de PfSense	25
Réglage de l'interface réseau	29
Paramétrage de l'interface Web	31
Configuration de l'interface de synchronisation	35
Configuration de l'Ip Virtuelle	40
Création du réseau EMPLOYES.....	42
Mise en place d'un serveur stockage TrueNAS.....	45
Installation de TrueNAS.....	45
Configuration de l'interface réseau.....	47
Accès à l'interface web	49
Création du pool de stockage	49
Ajout d'un dataset dans le pool	51
Configuration du protocole de partage de fichier.....	52
Configuration du partage de fichier.....	53
Paramétrage des comptes utilisateurs TrueNAS	54
Ajout de l'emplacement réseau sur les machines	56
Paramétrage du Windows Client	59
Paramétrage du réseau	59
Rentrer le pc client dans le domaine.....	61
Remerciement	64

Présentation du projet

Contexte de la mission

Ayant rejoint l'entreprise **TechSupp**, une entreprise en plein début d'une trentaine d'employés, spécialisée dans le support technique informatique pour les PME. Avec le recrutement de ses effectifs, TechSupp faisait face à des besoins urgent en matière d'organisation, de sécurité réseau et de communication interne. L'infrastructure réseau était à réaliser, les politiques de sécurité étaient à définir, et la communication entre les collaborateurs était dispersée.

Le projet visait à créer l'infrastructure, assurer une haute disponibilité des services et à consolider les communications dans l'équipe.

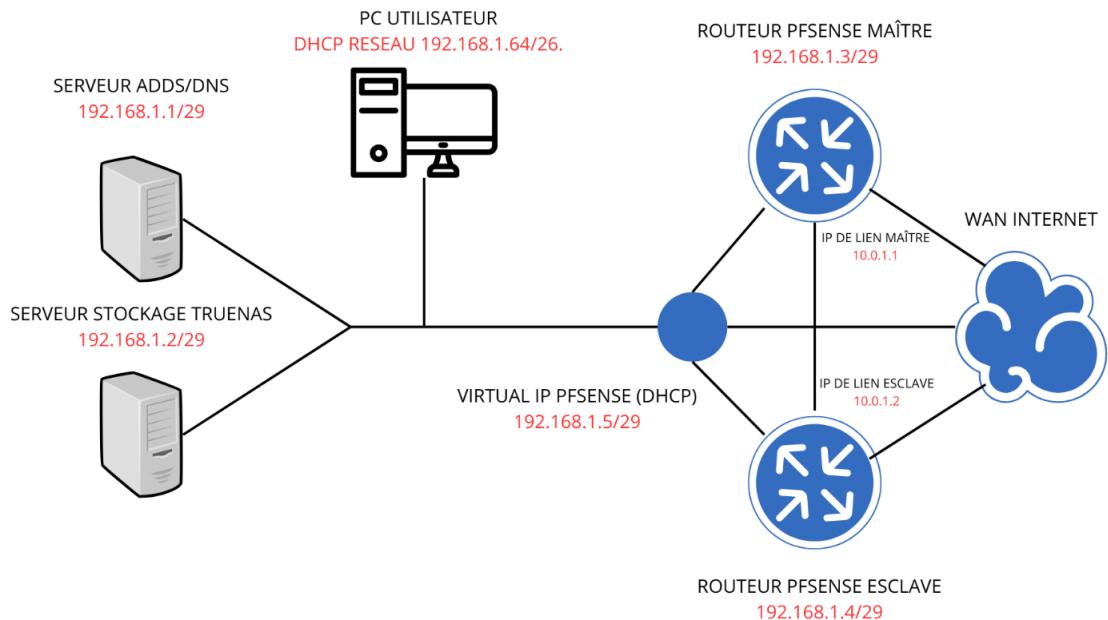
Intitulé de la réalisation professionnelle

- 1- Mise en place d'un Serveur Windows 2022 avec service ADDS/DNS
- 2- Mise en place d'un Serveur Stockage TrueNAS
- 3- Intégration de deux routeur PFSENSE en redondance grâce à une IP Virtuelle
- 4- Segmentation du réseau à l'aide de masque de sous-réseau.
- 5- Intégration d'un poste client en paramétré en DHCP sur réseau 192.168.1.64/26

RESSOURCES FOURNIES

- Contexte et problématique TechSupp
- Schéma réseau
- Matériel : Ordinateur sous Windows 11 Professionnel
- Virtualisation: VM Windows Server 2022, VM XIVO Serveur, VM Windows 10, 2 VM PFSENSE

Schéma réseau



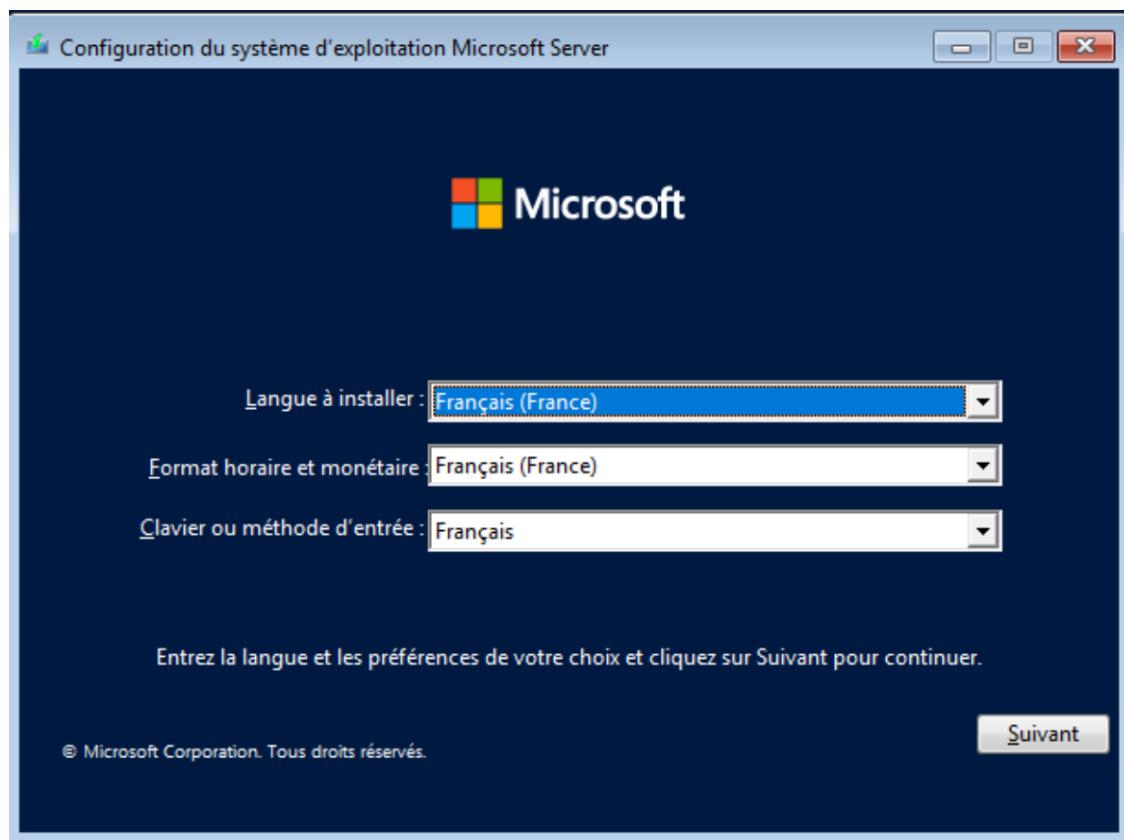
Mise en place d'un Serveur Windows

Installation du serveur

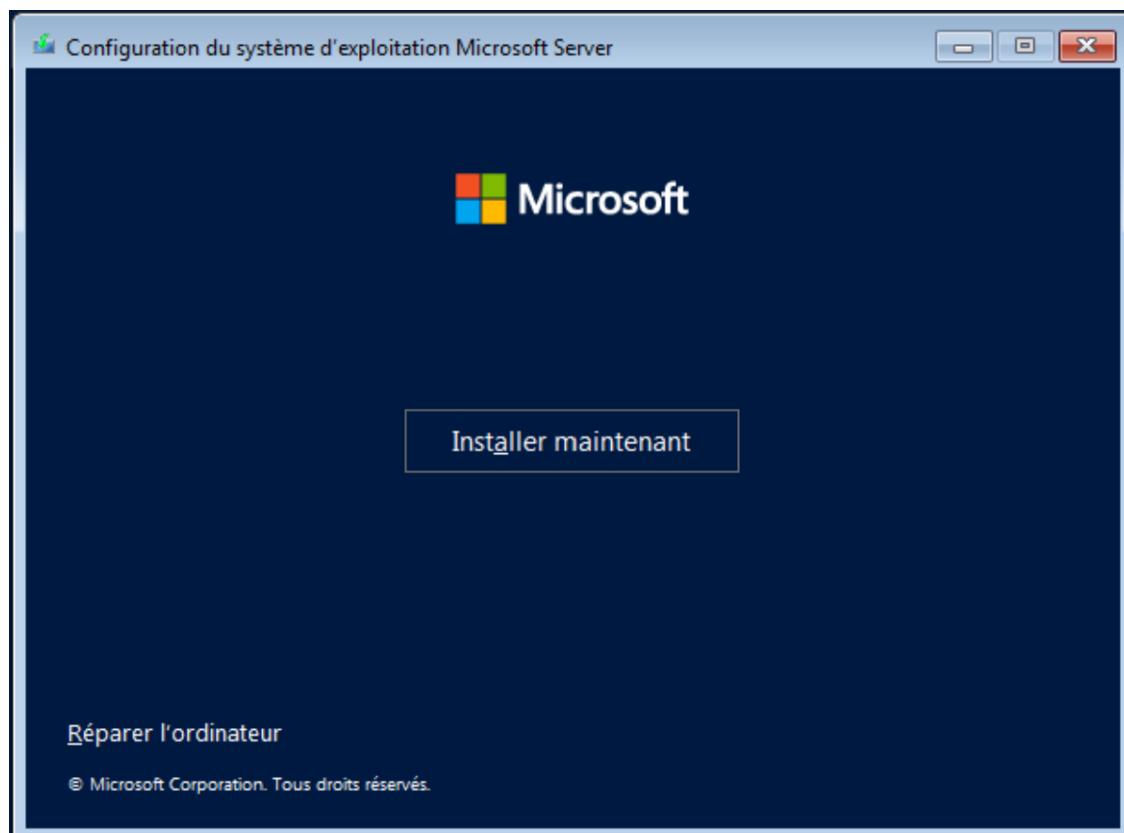
Configuration du serveur

Device	Summary
Memory	4 GB
Processors	4
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file C:\Users\Antoine\Des...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

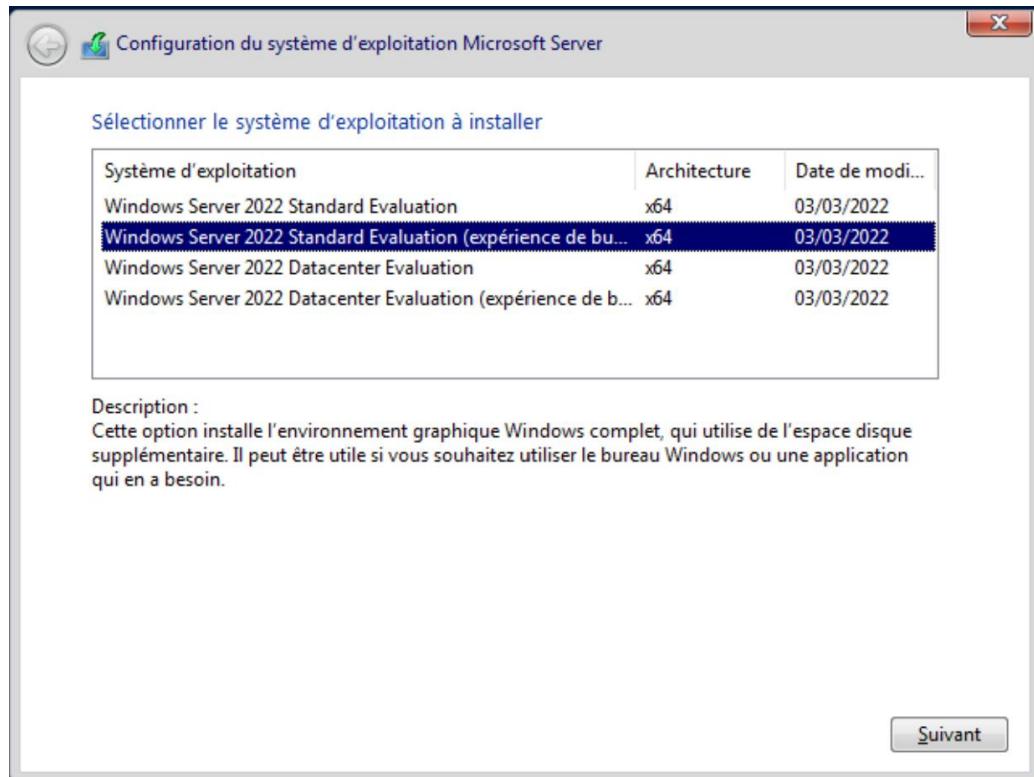
Dans un premier temps nous allons lancer le serveur, un fois lancé il nous sera demander quelle langue nous utilisons sur le serveur, nous choisirons le français.



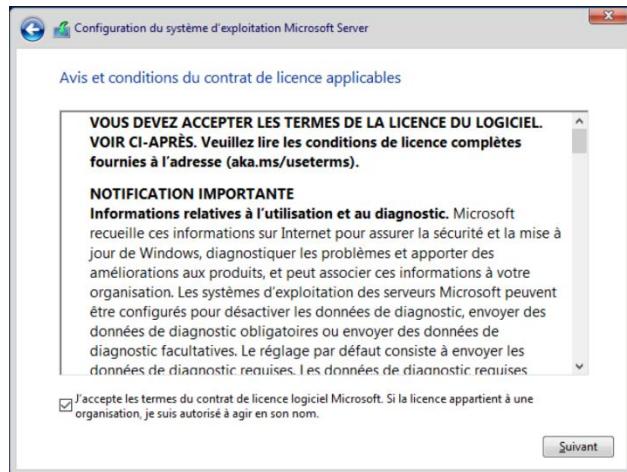
Suite à ce choix nous devrons en suite installer le système d'exploitation du serveur, ici Windows Server 2022.



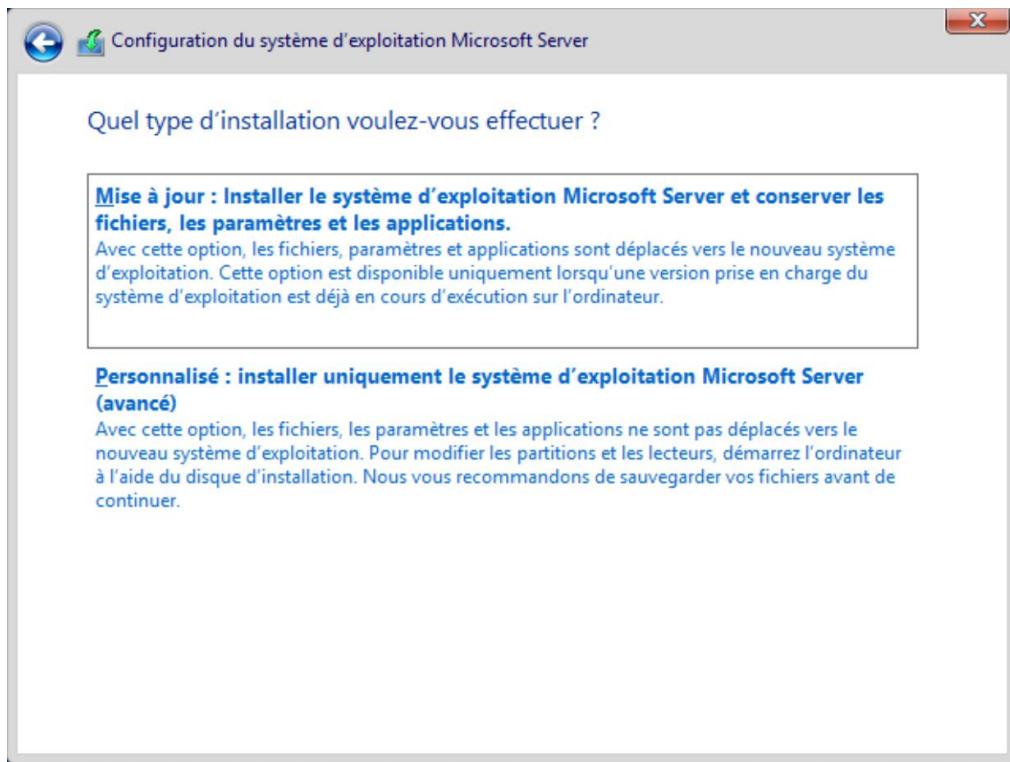
On nous propose ensuite de choisir la version de serveur, nous choisirons le Windows Server 2022 Standard en version expérience de bureau afin d'avoir l'interface graphique.



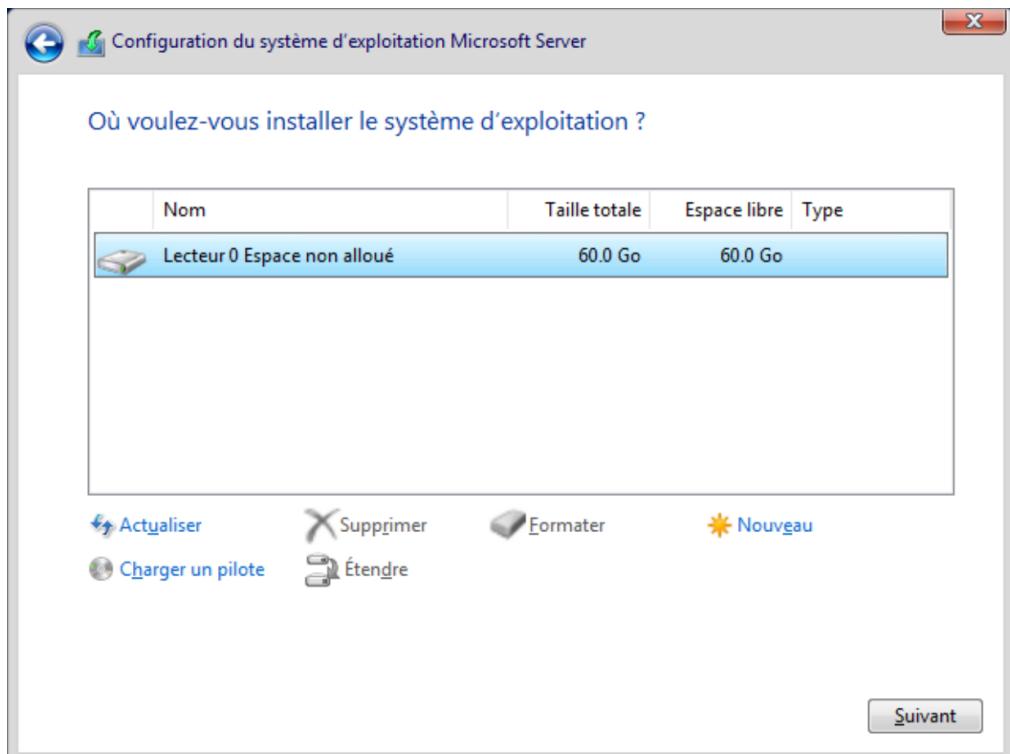
On doit ensuite accepter les conditions générales de Windows.



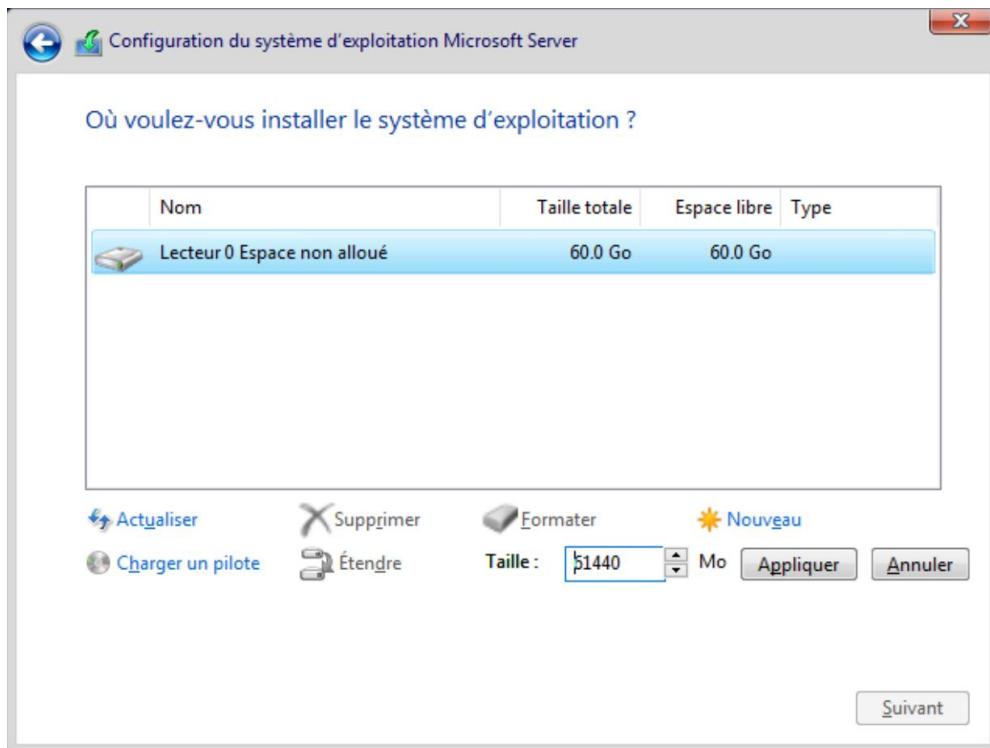
Suite à ça on choisit de faire l'installation personnalisé de Windows Server.



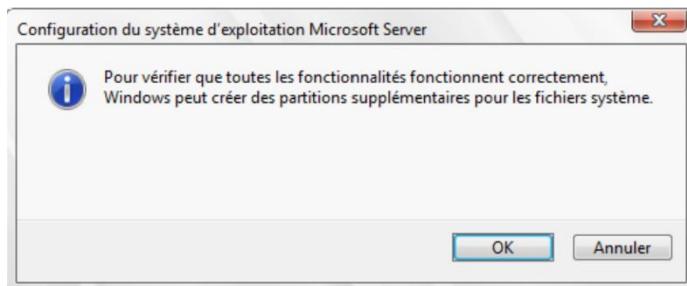
On arrive ensuite sur le programme d'allocation de l'espace disque, nous allons appuyer sur nouveau afin d'allouer l'espace disque non utilisé.



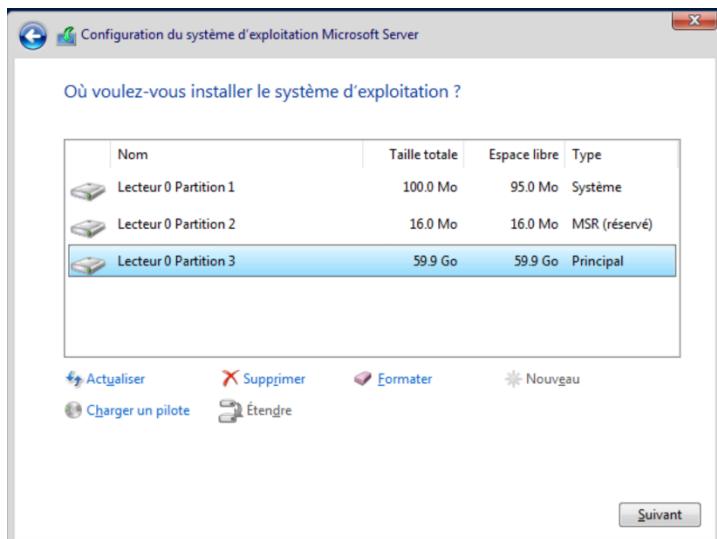
On clique en suite sur appliquer en ayant tout l'espace disque sélectionné afin d'utiliser entièrement l'espace disque.



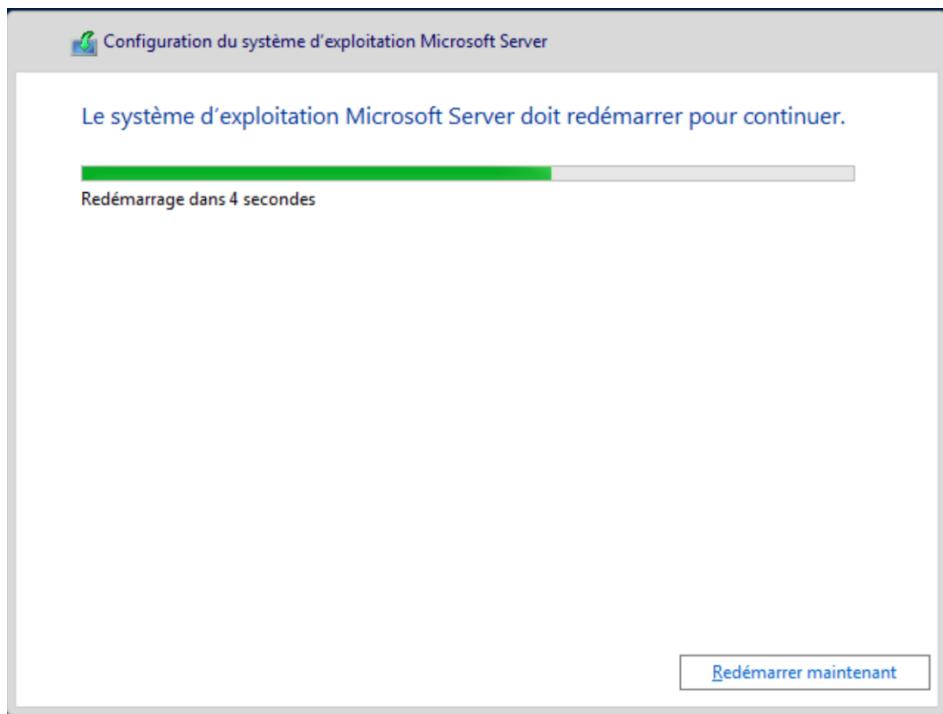
On clique ensuite sur ok pour le message qui s'affiche nous indiquant que Windows va créer des partitions supplémentaires pour garantir un fonctionnement correct.



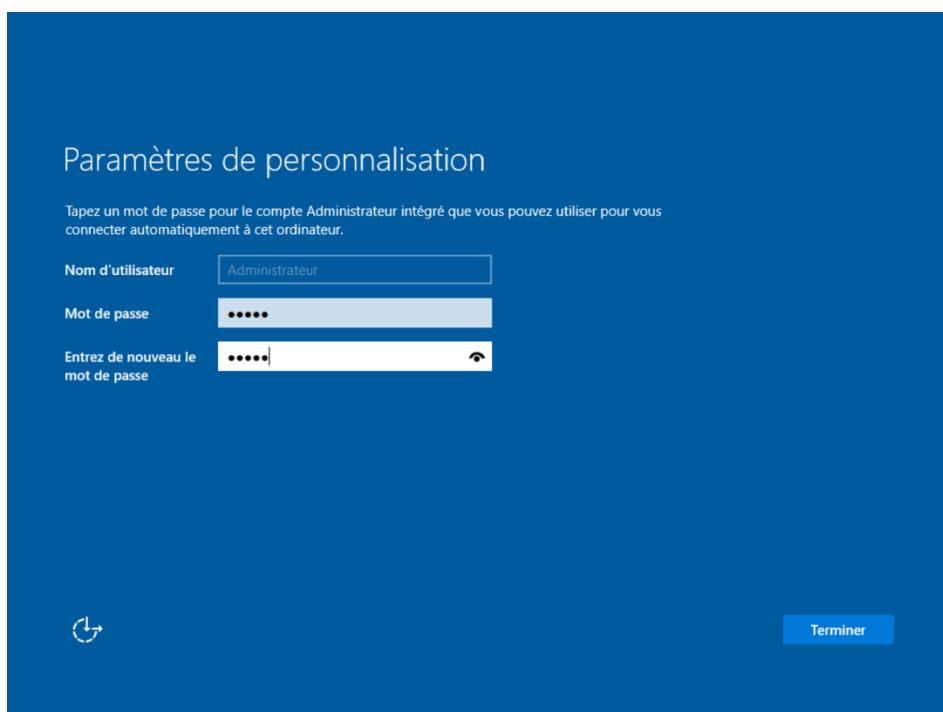
Une fois ces étapes réalisé, les partitions sont créés et nous pouvons cliquer sur suivant.



Suite à ces étapes le serveur va ensuite redémarrer.



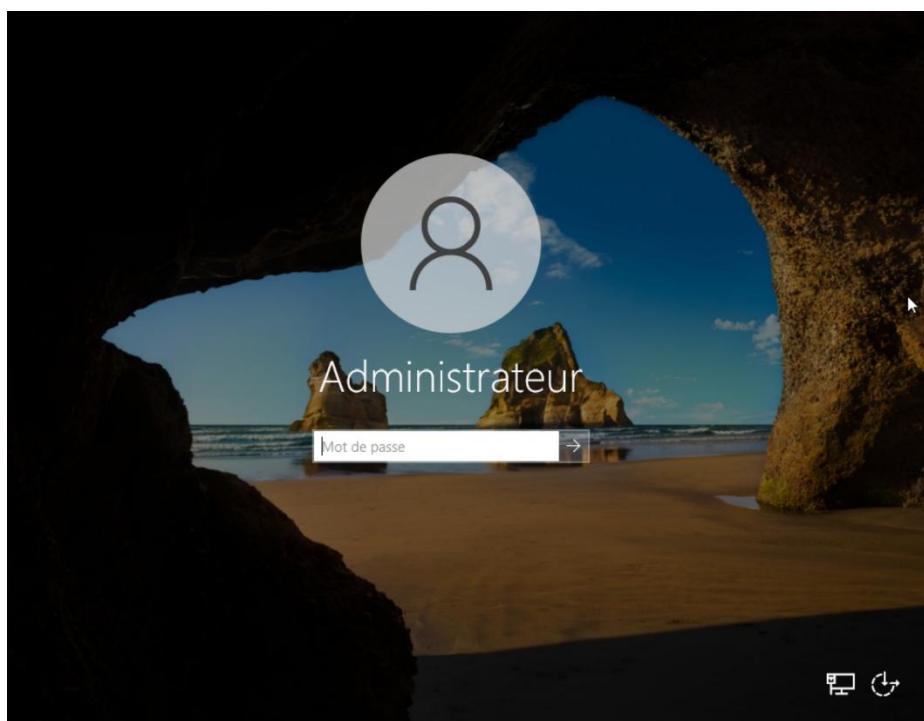
Après le redémarrage du serveur nous devrons configurer le mot de passe de l'administrateur du serveur.



Après avoir choisi le mot de passe administrateur nous arriverons ensuite sur l'écran de verrouillage du serveur.



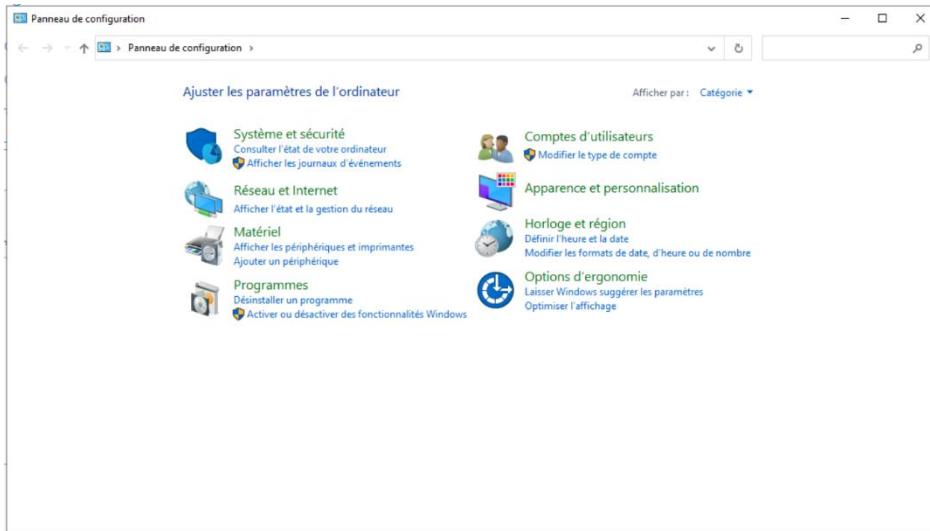
Nous pouvons ensuite nous connecter au serveur en utilisant les codes administrateur précédemment mis en place.



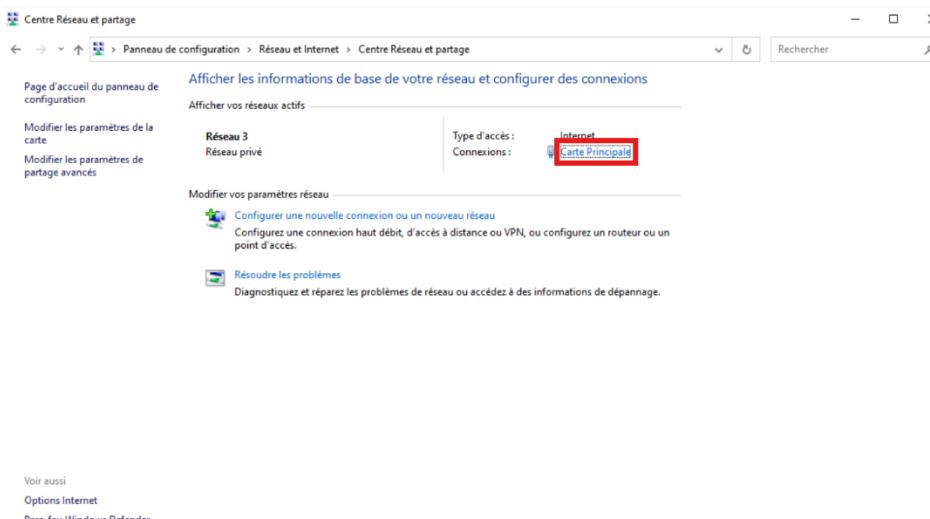
L'installation de base du serveur est réalisé il nous reste à installer les différents services sur le serveur.

Configuration réseau du serveur

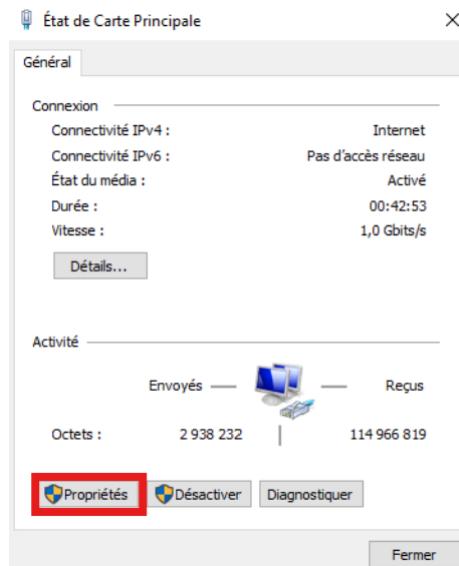
Pour configurer l'interface réseau de notre serveur nous irons tout d'abord dans le panneau de configuration.



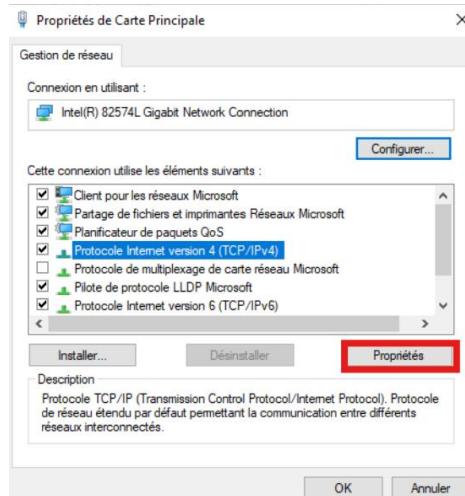
On cliquera ensuite sur afficher l'état gestion réseau, puis on cliquera sur la carte réseau principale.



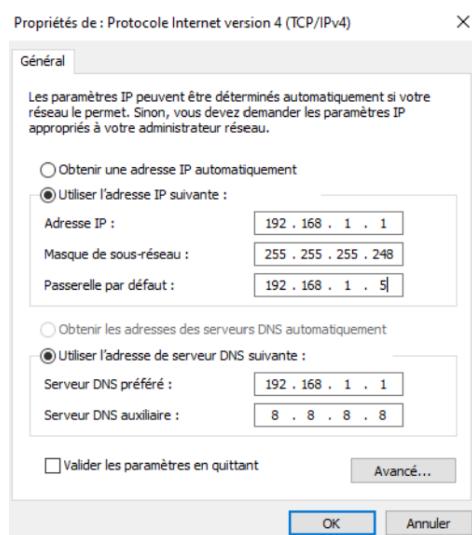
On cliquera ensuite sur propriété une fois arrivé sur l'interface réseau.



On cliquera ensuite de nouveau sur propriétés.

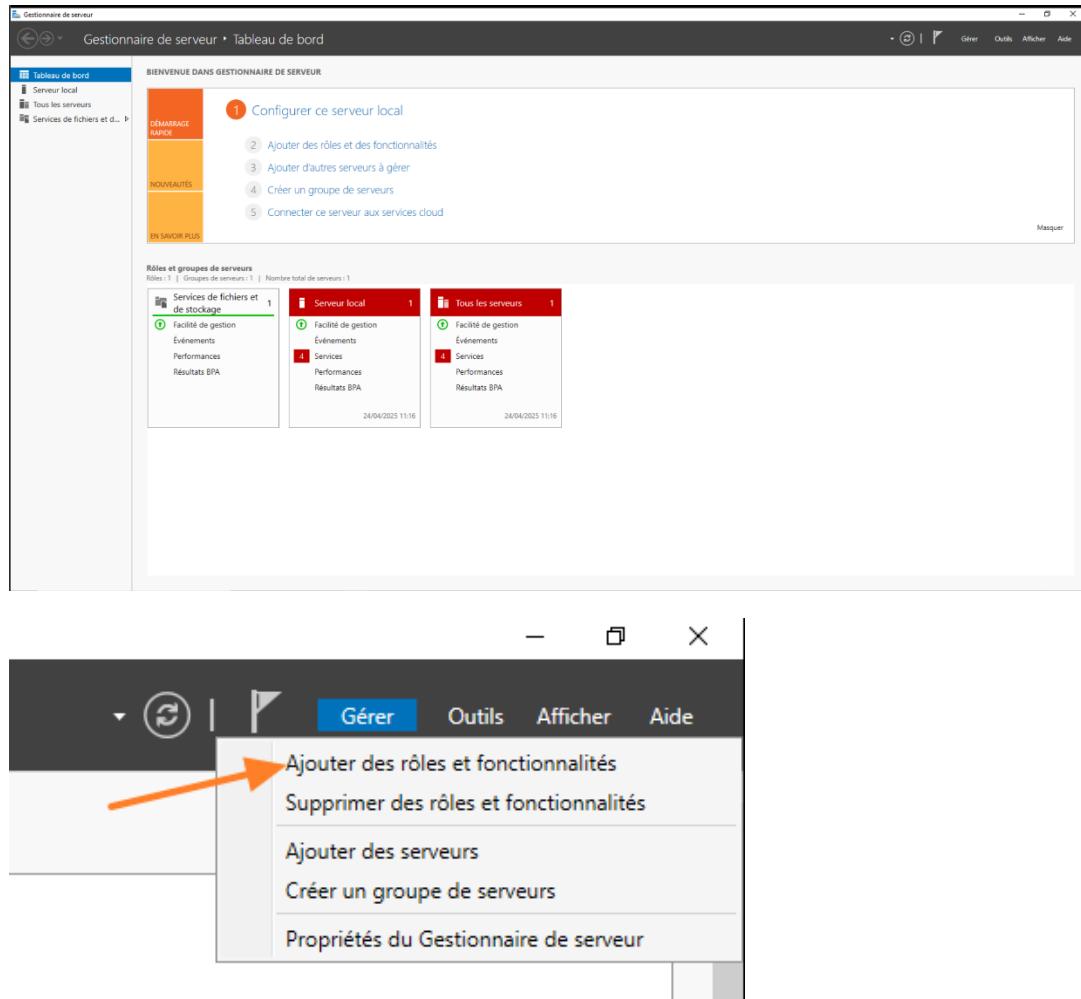


On pourra ensuite mettre la configuration réseau voulu.

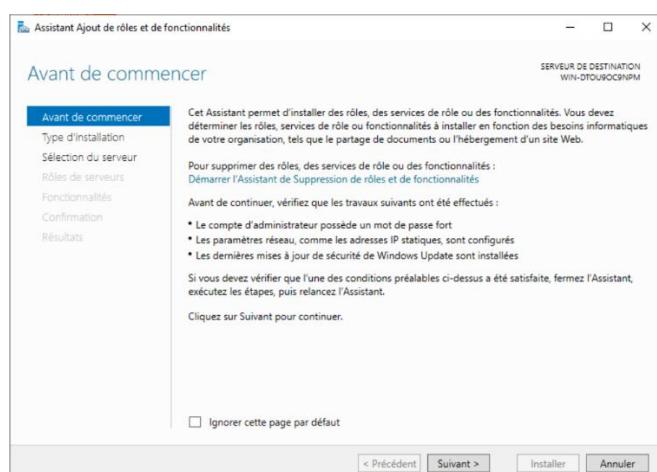


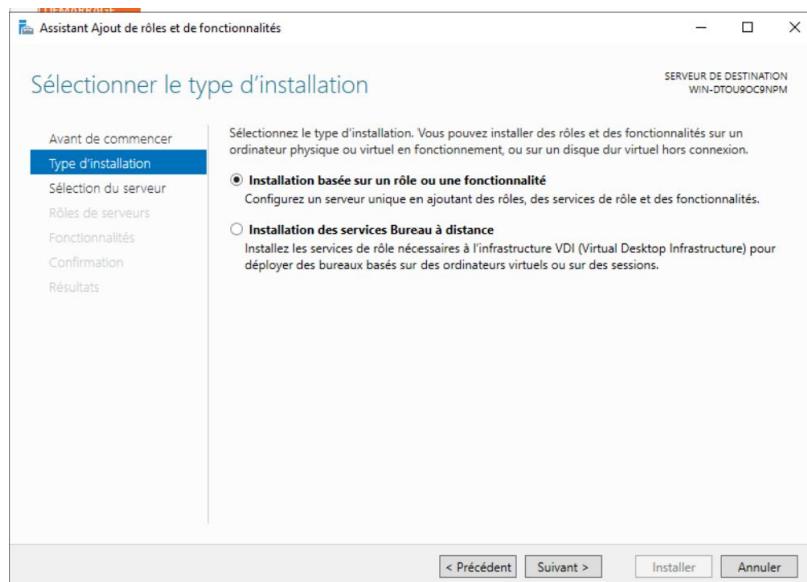
Installation du service ADDS DNS

Pour l'ajout du rôle ADDS DNS, nous irons tout d'abord dans le gestionnaire de serveur et on cliquera sur « Gérer » en haut à droite, puis « Ajouter des rôles et fonctionnalités ».

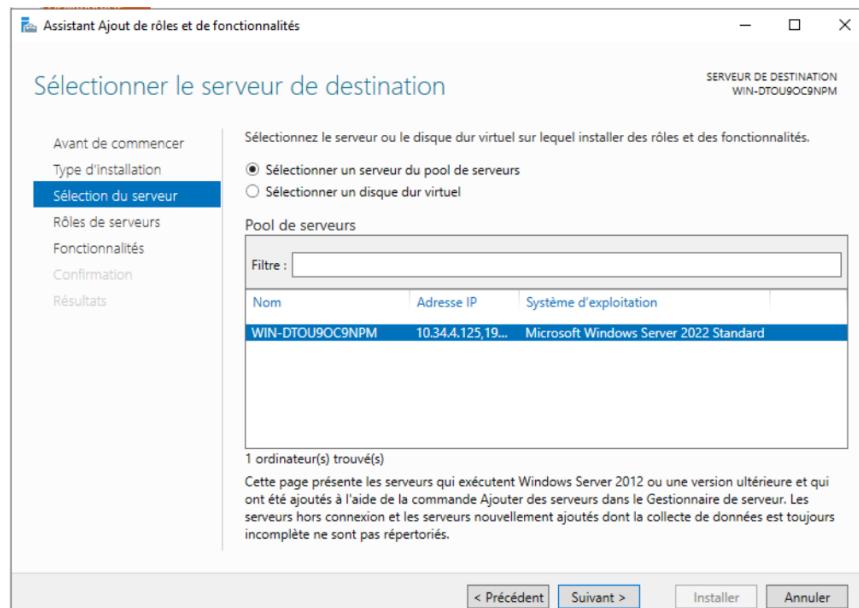


Passez l'étape "Avant de commencer" et poursuivez ensuite en laissant le type d'installation sur le choix "Installation basée sur un rôle ou une fonctionnalité".

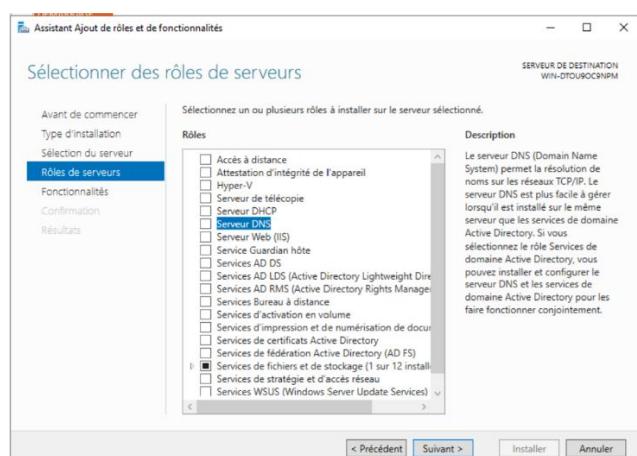




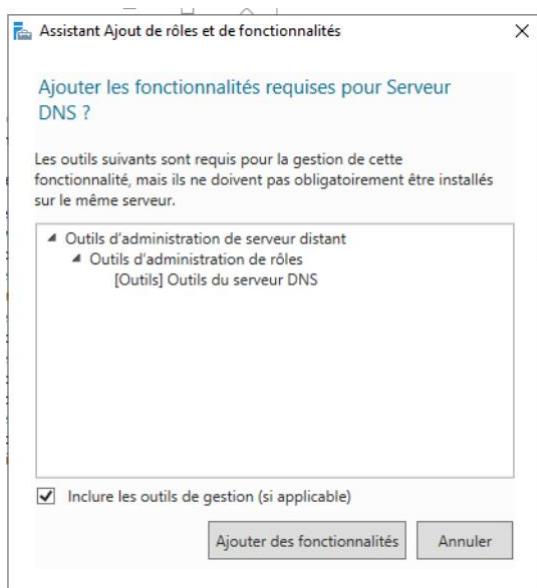
On sélectionne ensuite notre serveur.



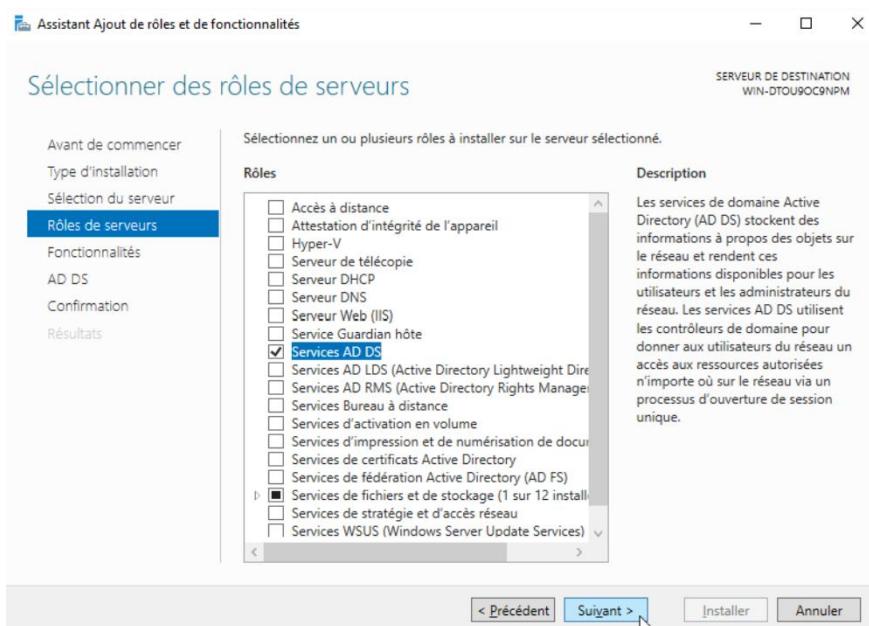
On sélectionne ensuite le rôle « DNS » et « ADDS ».



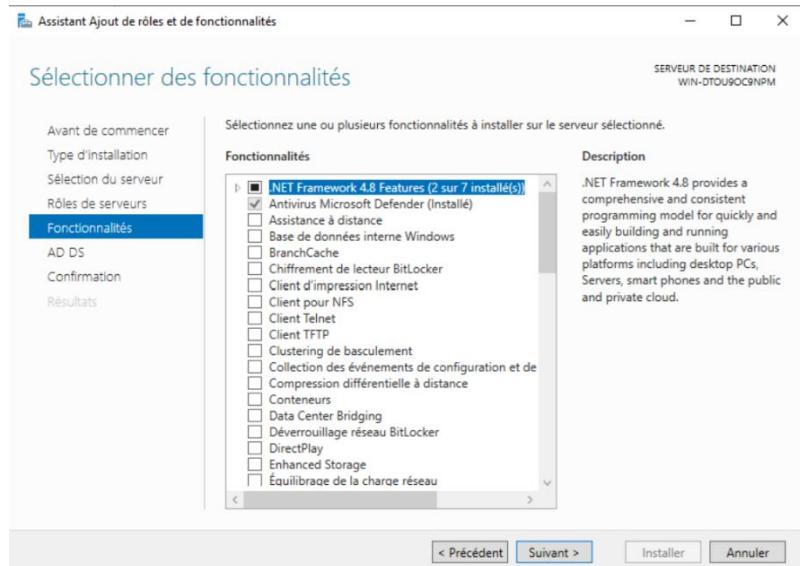
On valide ensuite l'ajout du rôle sur la prochaine fenêtre qui apparaîtra.



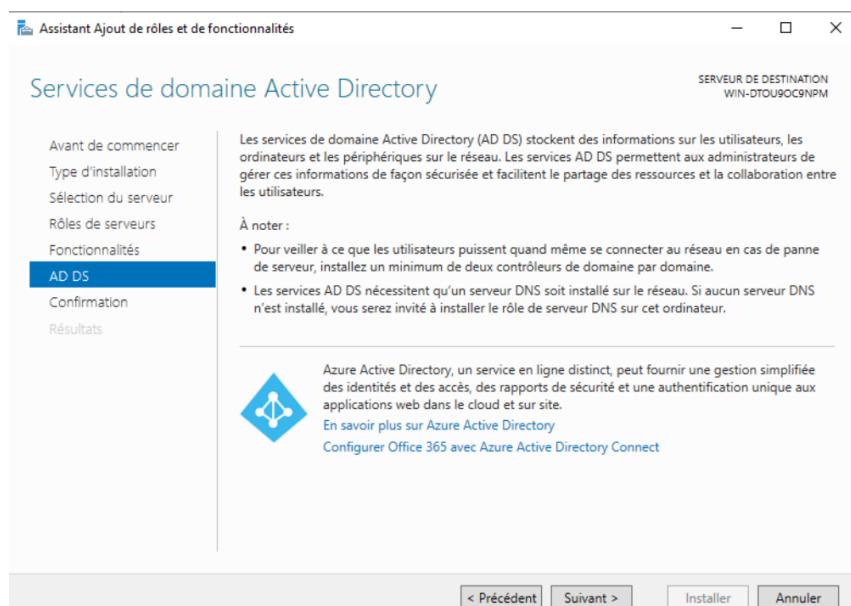
On appuie ensuite sur « Suivant ».



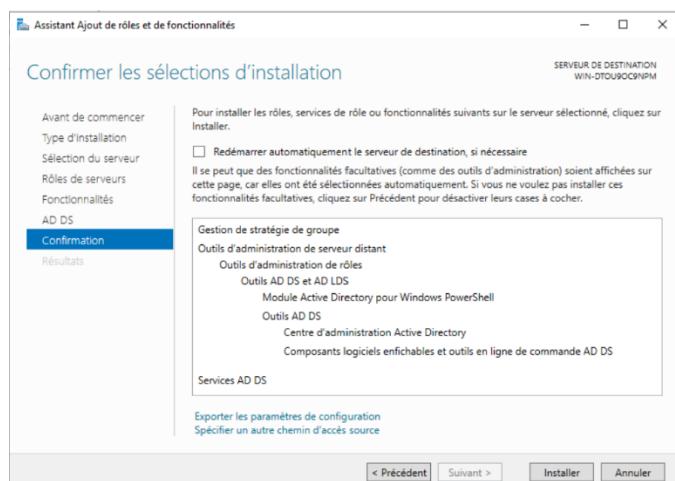
On ne rajoutera pas de fonctionnalités de serveur en plus donc on cliquera simplement sur suivant.



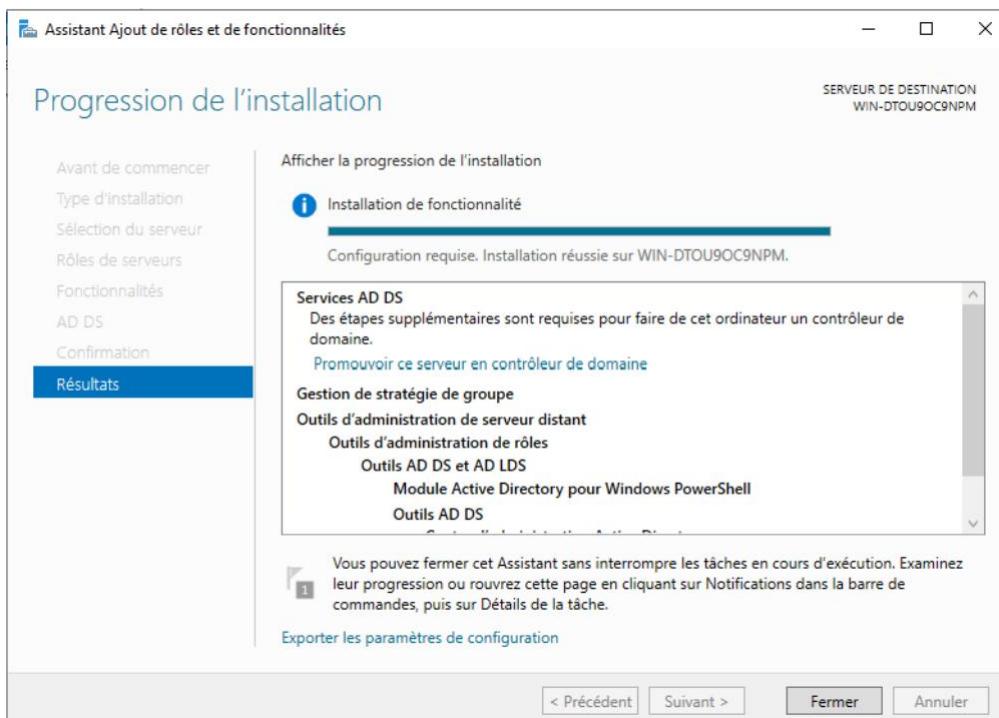
Cliquer suivant sur l'écran suivant 2 fois afin de confirmer le choix.



Cliquez sur "Installer" pour démarrer l'installation, qui peut prendre quelques minutes.

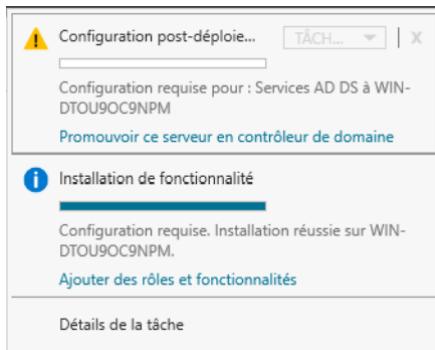


Cliquer sur fermer une fois l'installation terminé.

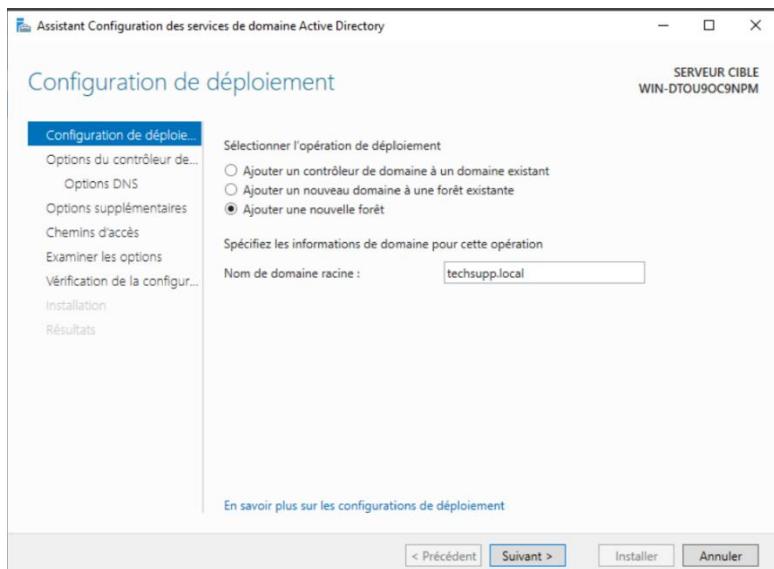


Configuration du domaine

Cliquer sur le bouton « Promouvoir ce serveur en contrôleur de domaine en haut à droite.

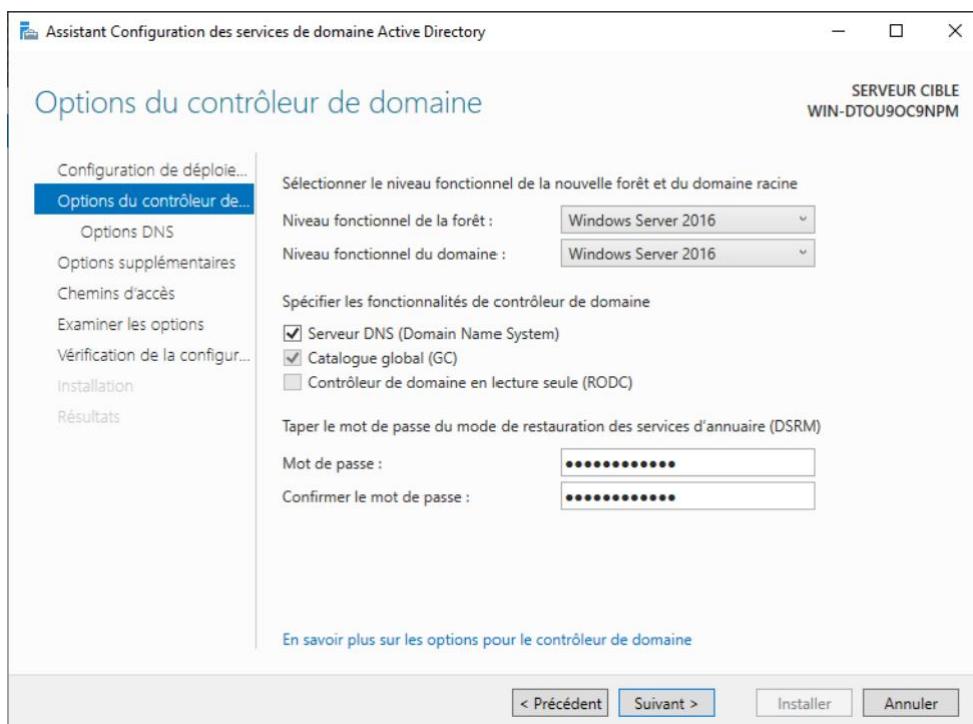


Comme il s'agit d'un nouveau domaine dans une nouvelle forêt, choisissez "Ajouter une nouvelle forêt" et indiquez le nom de domaine.

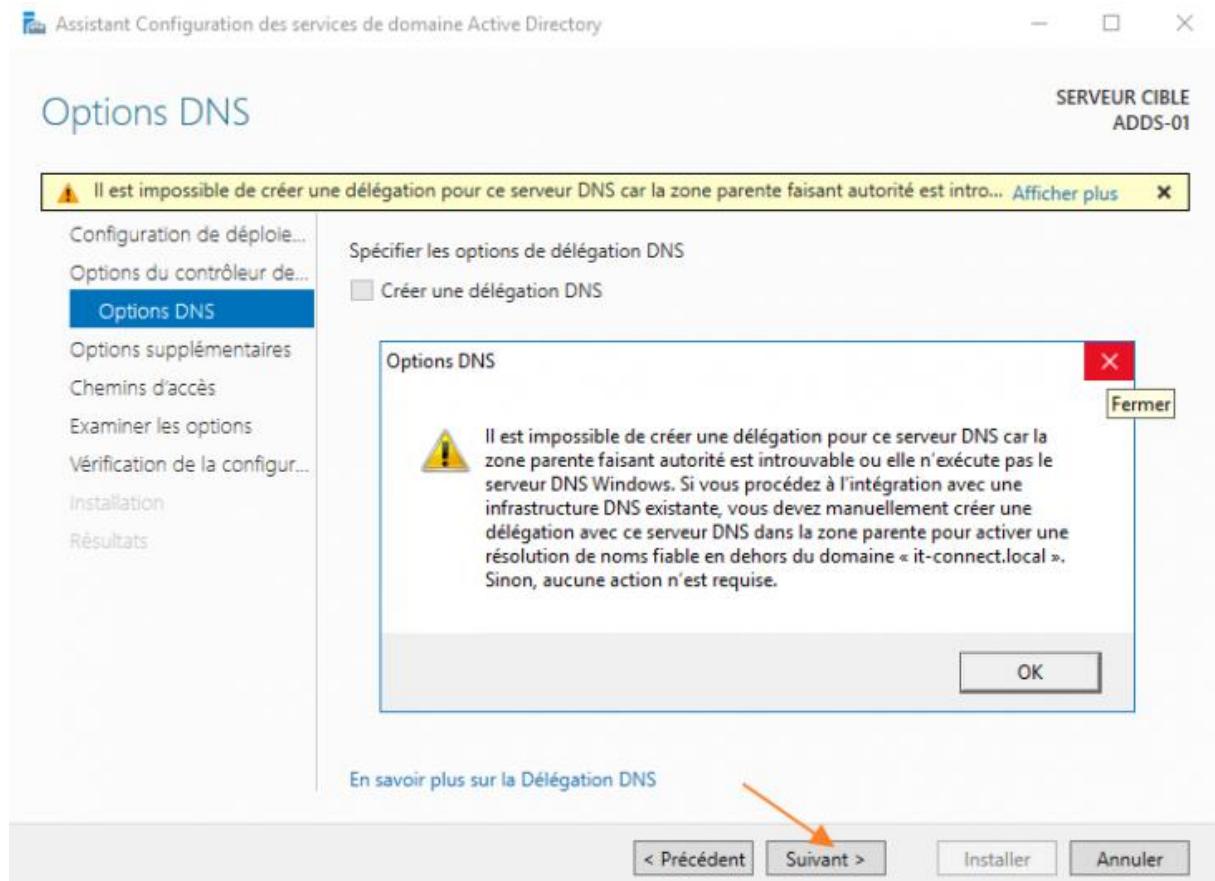


Pour le niveau fonctionnel de la forêt et du domaine, on indique "Windows Server 2022".

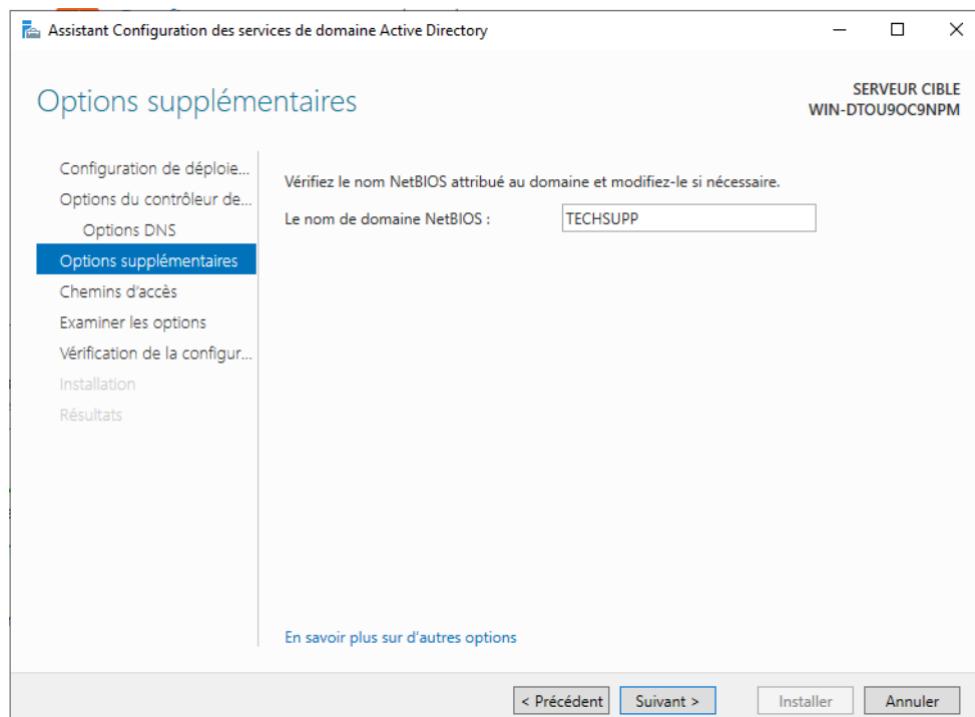
Enfin, on indique un mot de passe pour les services de restauration de l'annuaire.



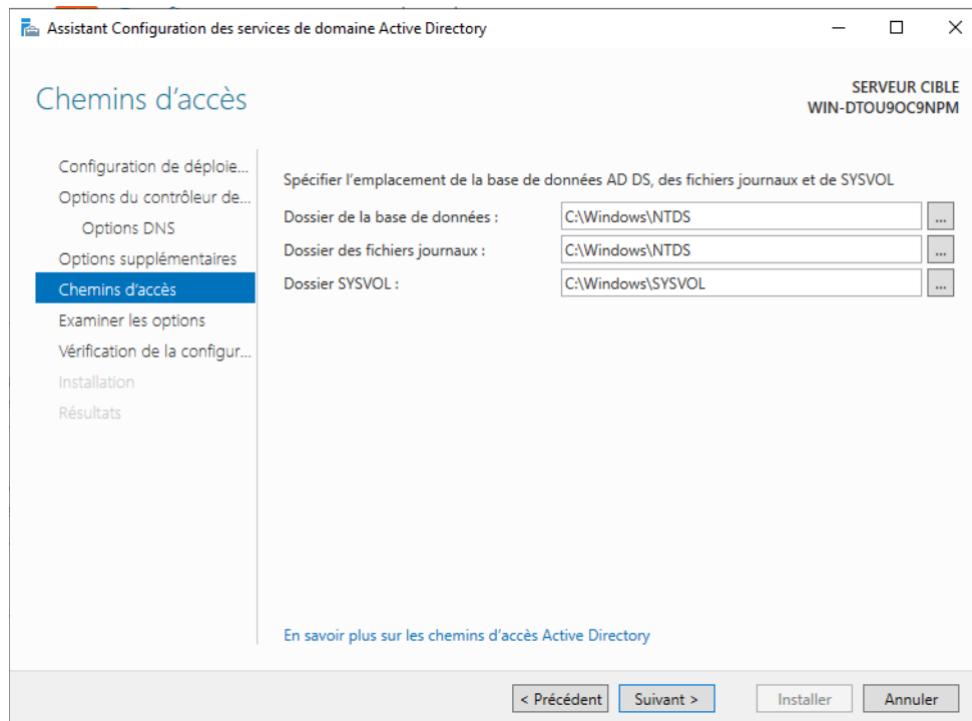
Comme il s'agit d'un nouveau serveur DNS pour une nouvelle zone ce message est normal.



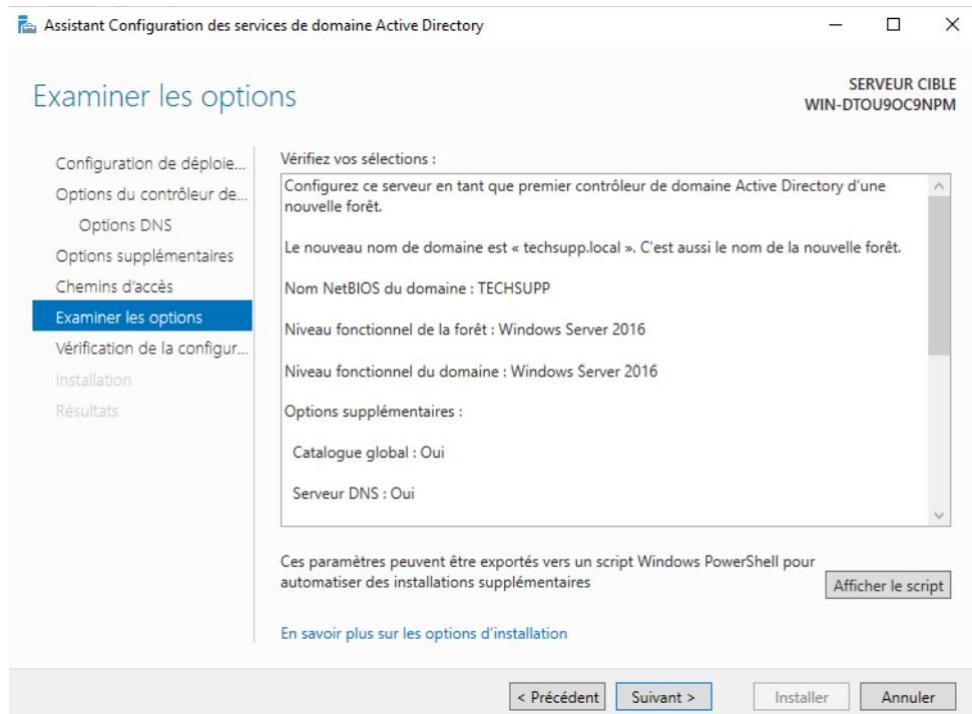
On indique un nom NETBIOS pour le domaine, à savoir un nom court et qui ne s'appuie pas sur DNS pour être résolu.



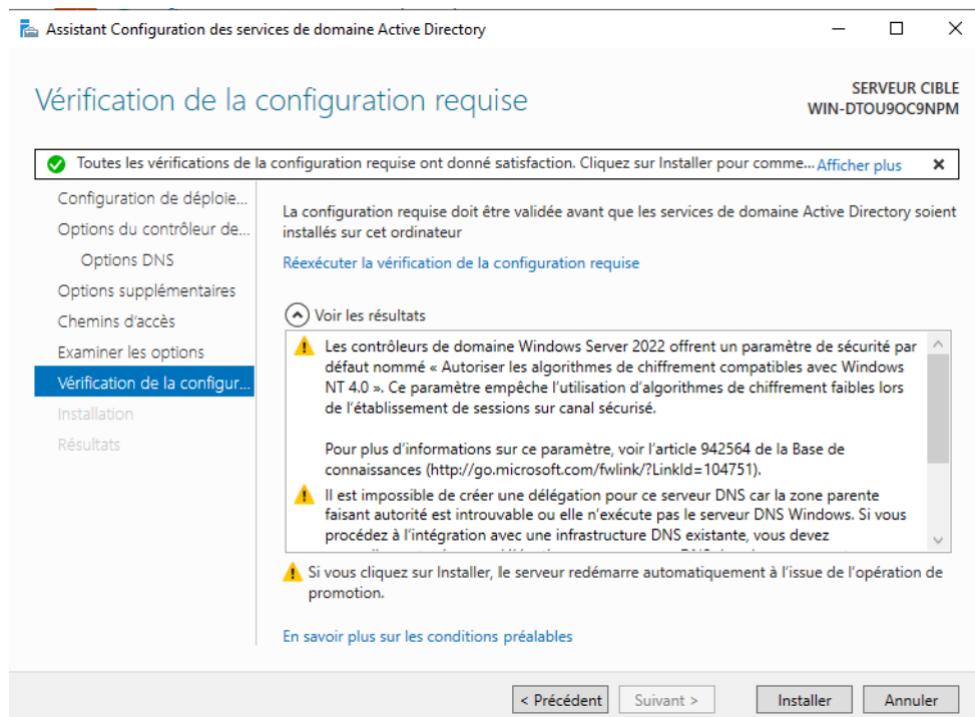
On laisse les chemins par défaut et on continue.



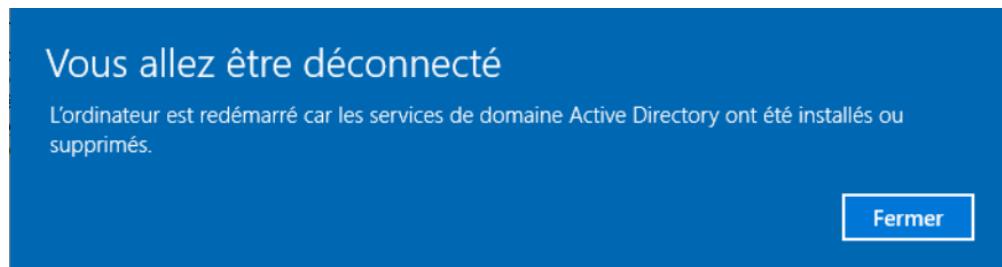
On clique sur suivant ensuite.



On clique pour finir sur installer pour démarrer la création du domaine et la configuration du DC.

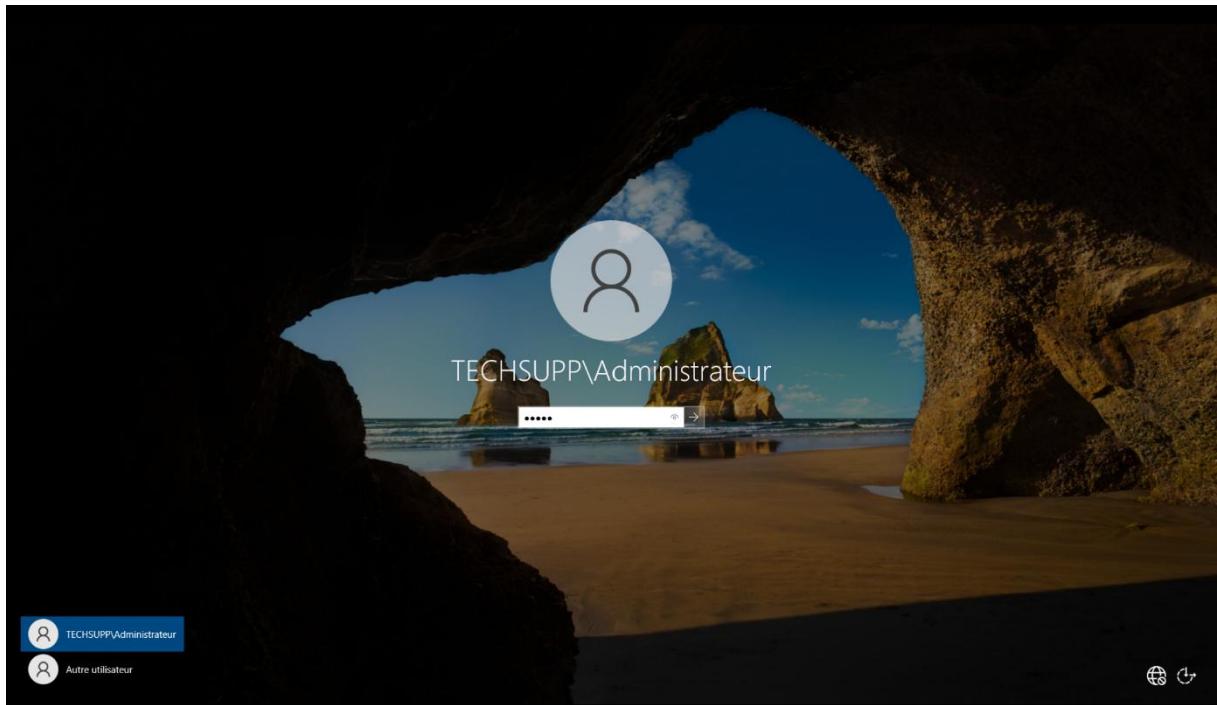


Quand ce sera terminé, le serveur va obligatoirement redémarrer, de façon automatique.



Après le redémarrage nous pourrons nous connecter avec le compte administrateur.

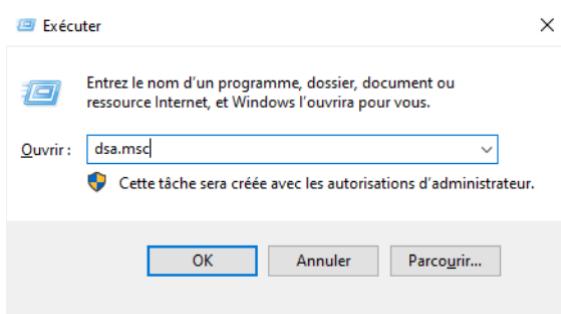




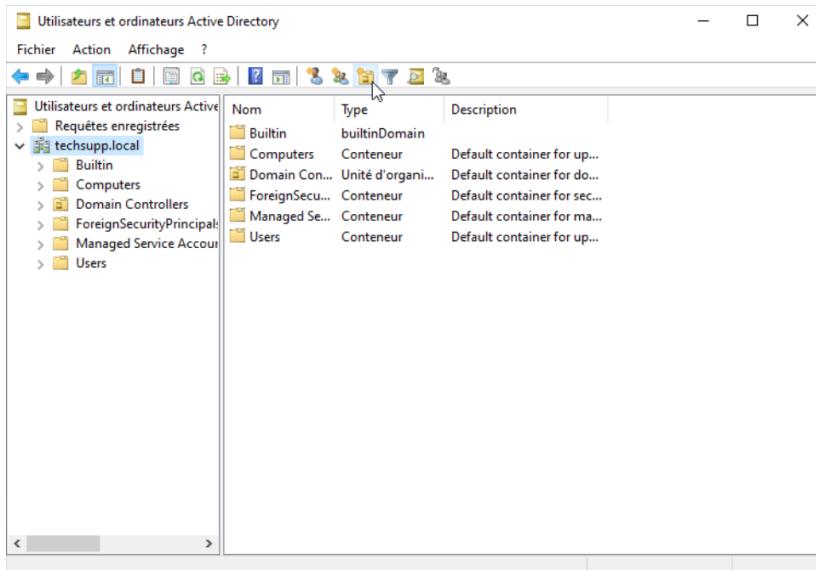
Création des Unités d'organisations et des utilisateurs

Après avoir créer le domaine nous allons pouvoir créer les utilisateurs sur le domaine.

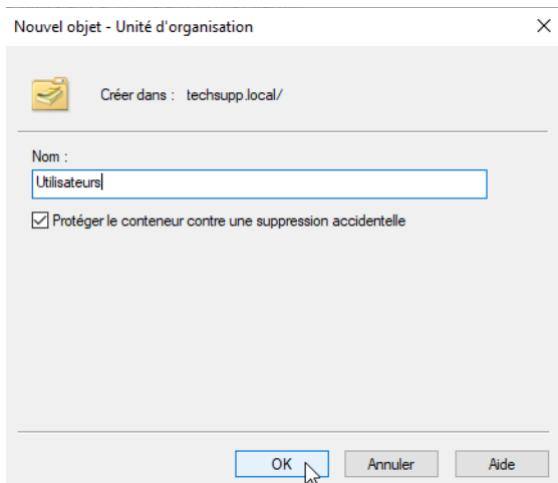
Pour cela nous allons faire une commande afin d'ouvrir le panneau de configuration des utilisateurs de l'Active Directory.



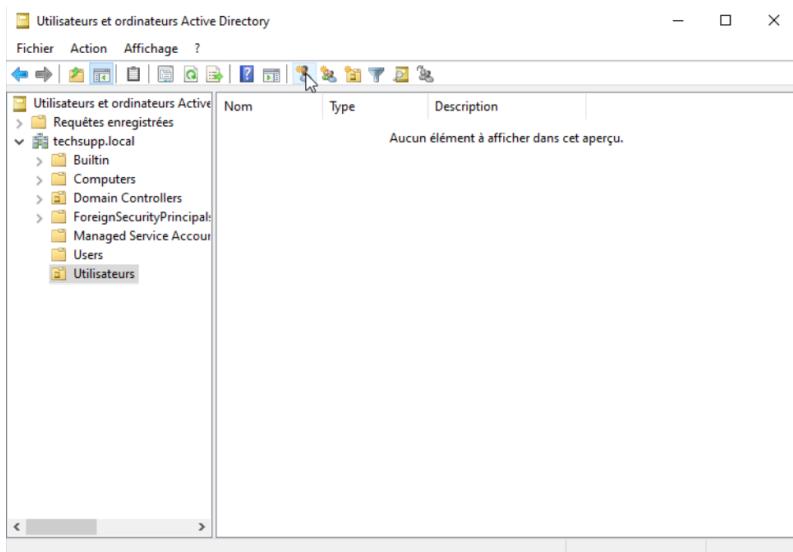
Nous allons ensuite créer une unité d'organisation dans le domaine créer précédemment.



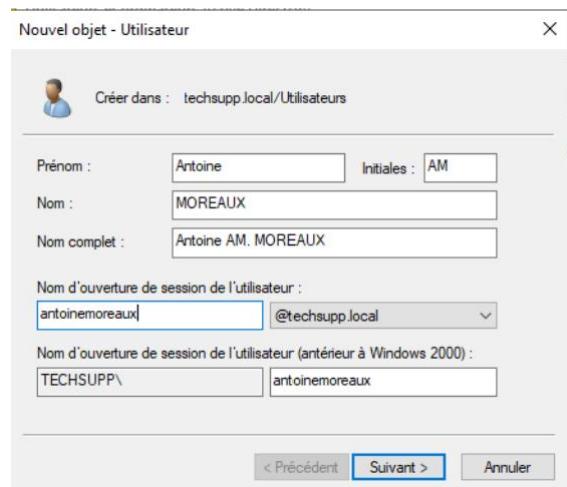
Nous nommons l'unité d'organisation, puis on continue.



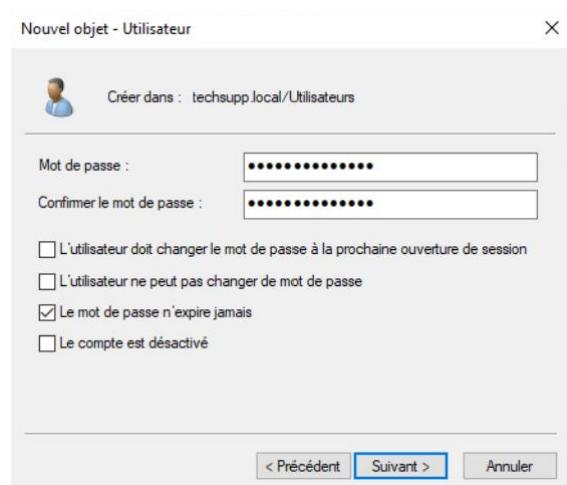
On va ensuite créer un utilisateur dans l'unité d'organisation créé précédemment.



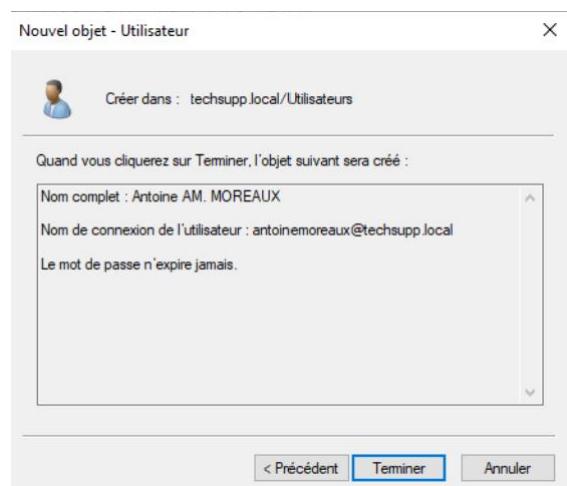
On nomme l'utilisateur, puis on continue.



On configure ensuite le mot de passe utilisateur.



Après ça nous avons terminé de créer l'utilisateur.

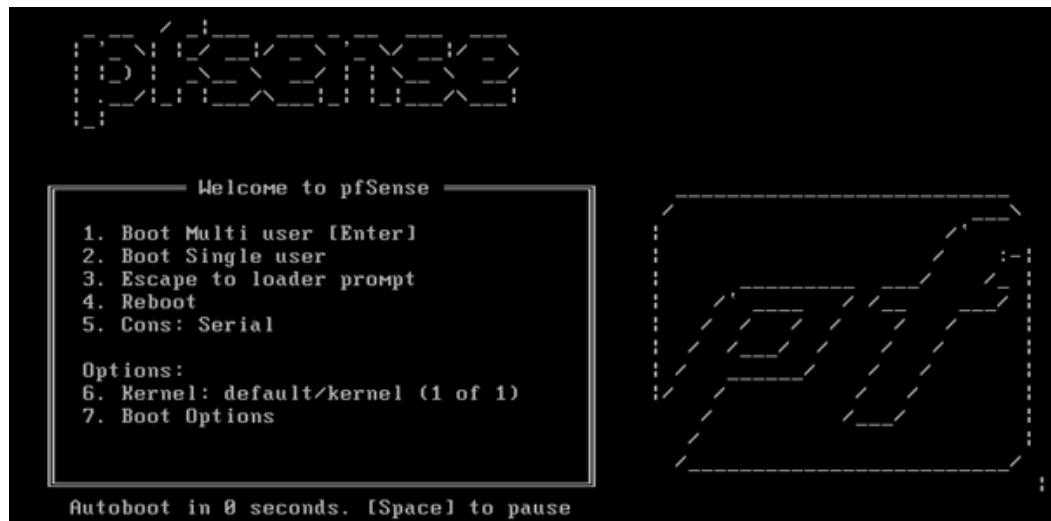


Mise en place d'un routeur PfSense

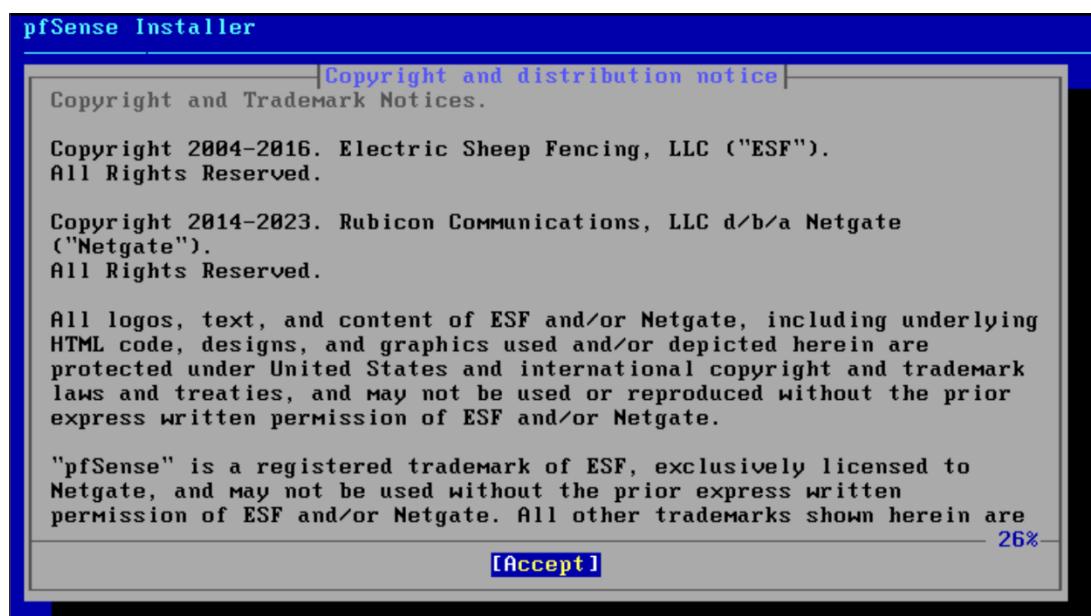
Installation de PfSense

Nous allons maintenant mettre en place un PfSense qui servira de routeur/pare-feu dans notre infrastructure.

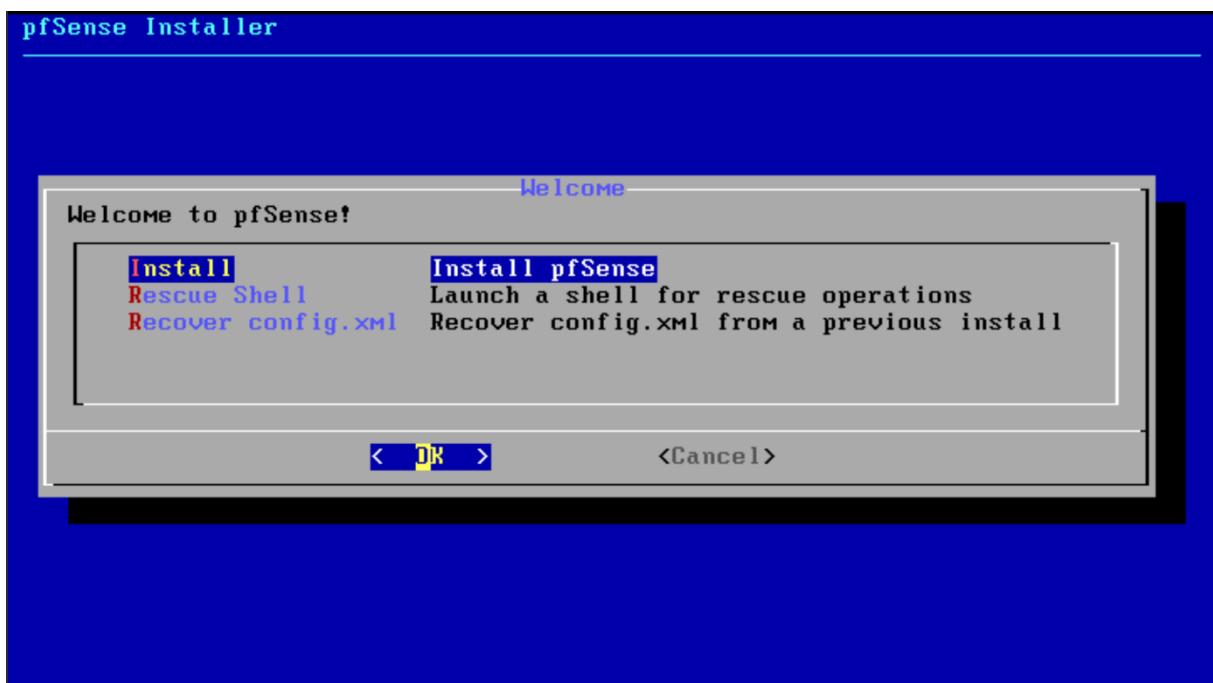
Tout d'abord nous allons démarrer le PfSense, il démarrera automatiquement au bout de 10 secondes.



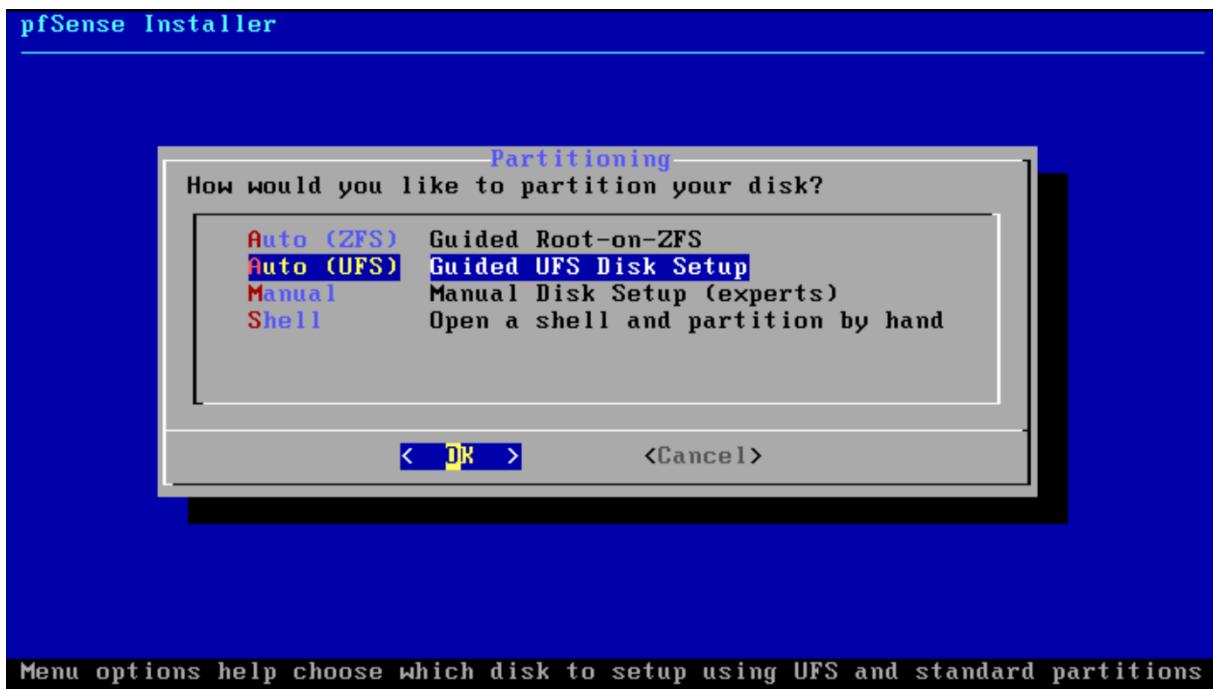
Après le démarrage on accepte les conditions générale puis on continue.



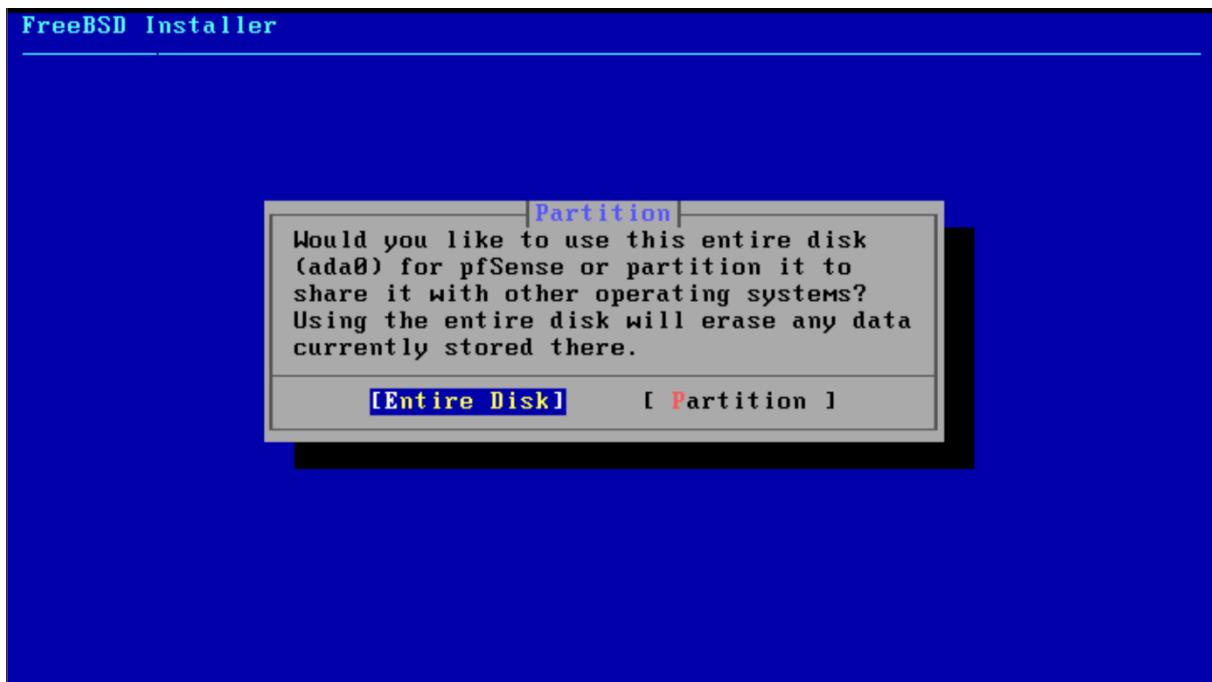
Après ça on sélectionne la première option pour installer pfSense.



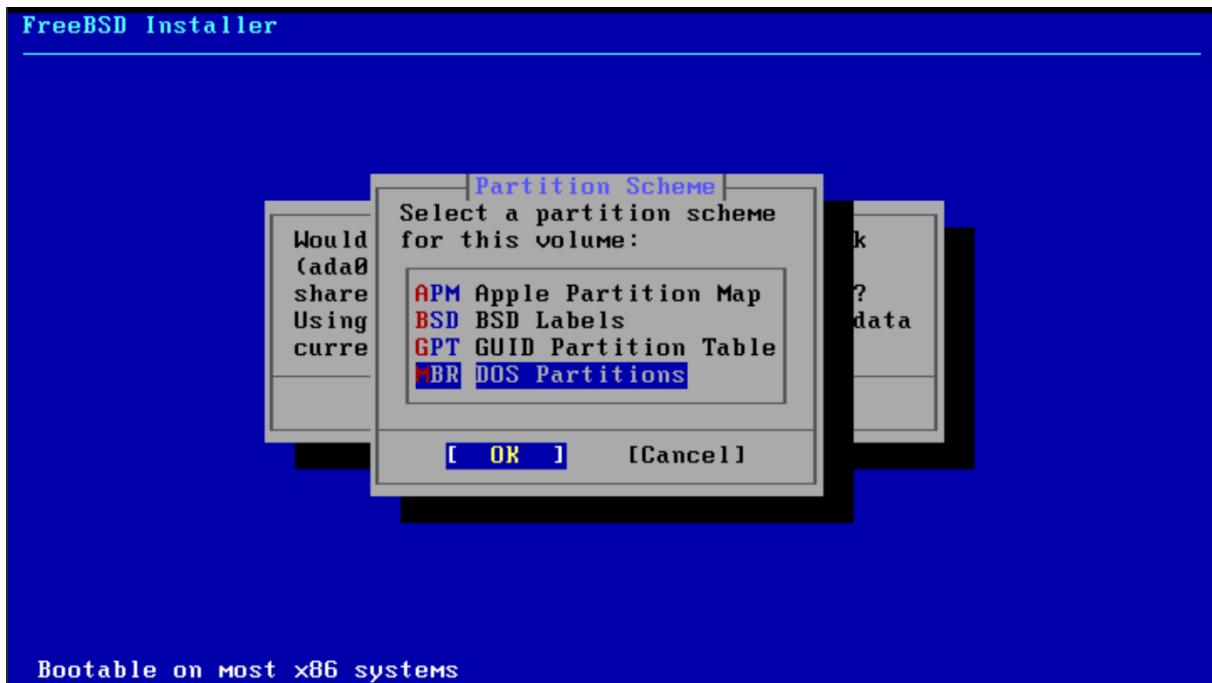
On doit ensuite choisir le type de partitionnement de disque, on choisit en UFS.



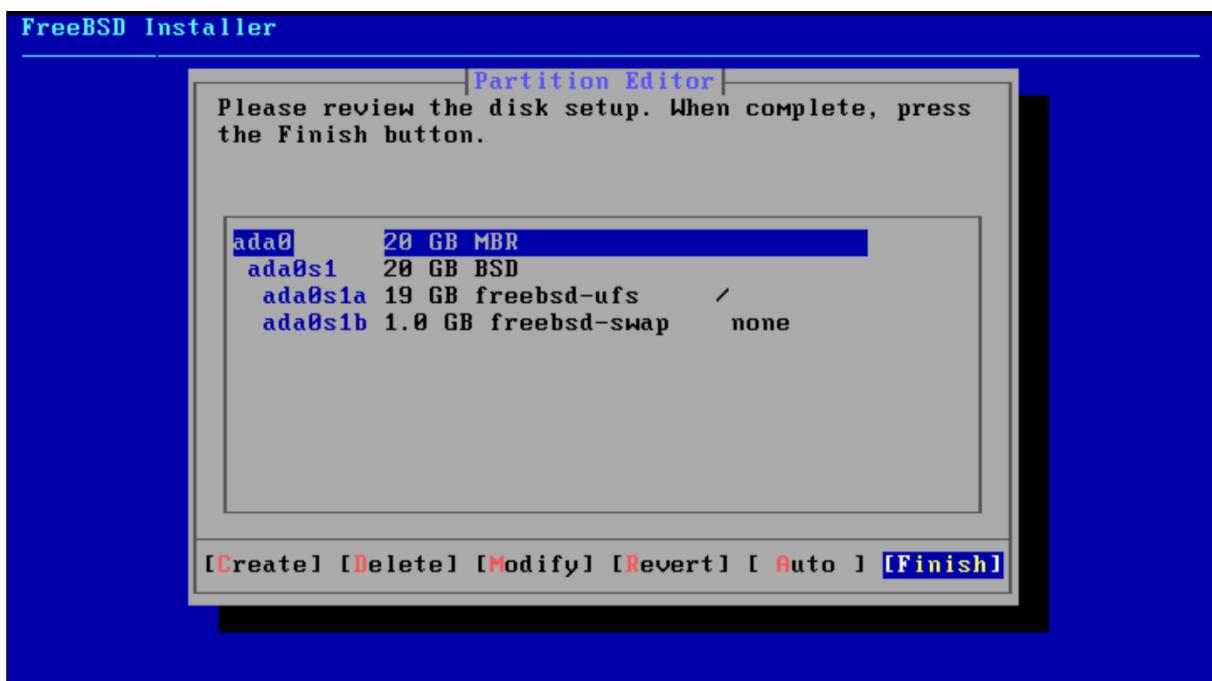
On choisit ensuite d'utiliser le disque entier attribué au pfsense.



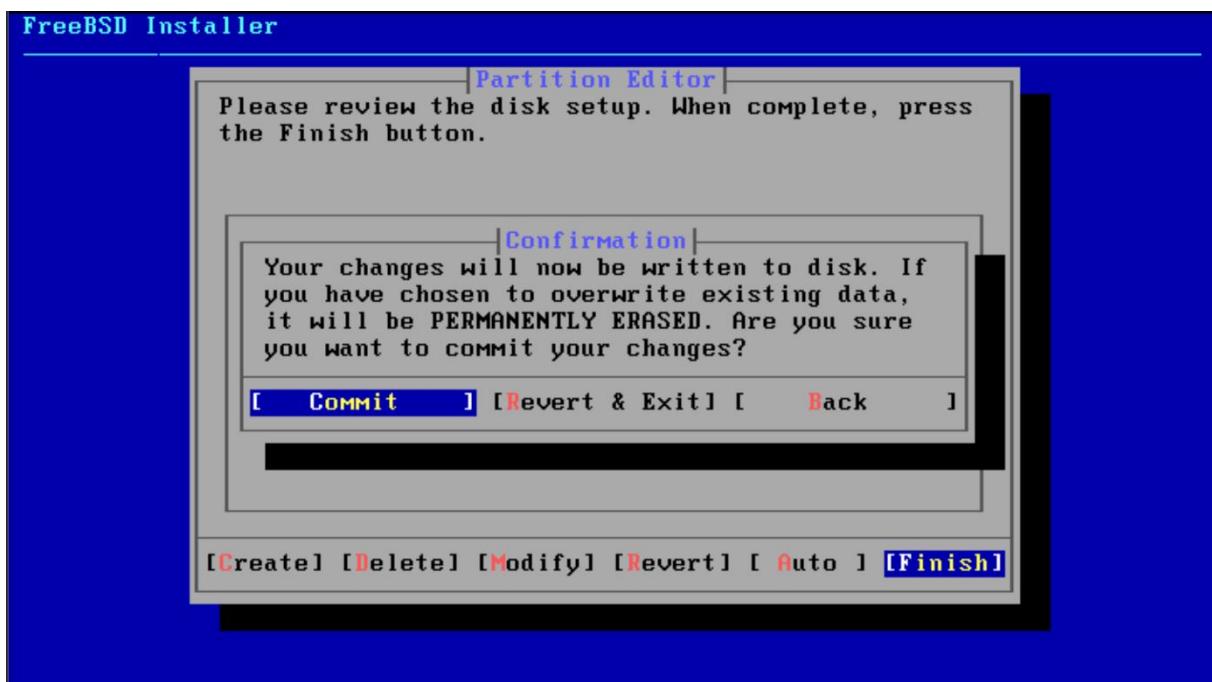
On choisit comme type de partitionnement le partitionnement en DOS.



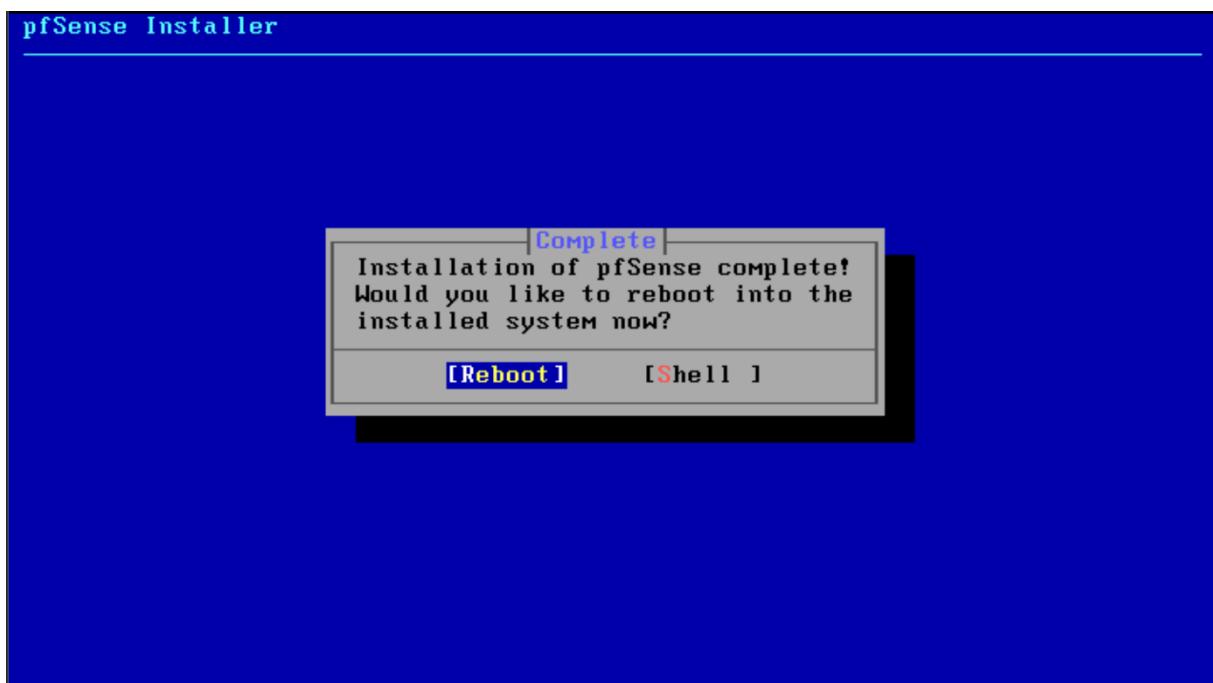
Le partitionnement de disque se fait automatiquement, on appuie sur « Finish ».



On doit ensuite valider le choix.



Après la création de partition, le PfSense va redémarrer.



Réglage de l'interface réseau

On va ensuite régler l'interface réseau, pour cela on sélectionne l'option 2 sur l'interface du pfSense.



On choisit ensuite l'interface à modifier, dans notre cas on sélectionne l'interface 2.

```
Available interfaces:  
1 - WAN (em0 - dhcp, dhcp6)  
2 - LAN (em1 - static)  
Enter the number of the interface you wish to configure: 2
```

On choisit de ne pas configurer l'interface via le DHCP.

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

On remplit ensuite l'interface réseau, dans notre cas on met l'interface du pfsense en 192.168.1.3.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.1.3
```

On remplit ensuite le masque de sous réseau de l'interface.

```
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 29
```

Comme nous configurons l'interface LAN on laisse cette option vide.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
> 
```

Comme nous n'utilisons pas l'ipv6 on ne le configure pas.

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
Enter the new LAN IPv6 address. Press <ENTER> for none:  
> 
```

Pour l'instant on active pas le DHCP, on l'activera plus tard sur l'interface Web du pfsense.

```
Do you want to enable the DHCP server on LAN? (y/n) n
```

On laisse l'interface du pfsense en https.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Notre interface est désormais configurée.

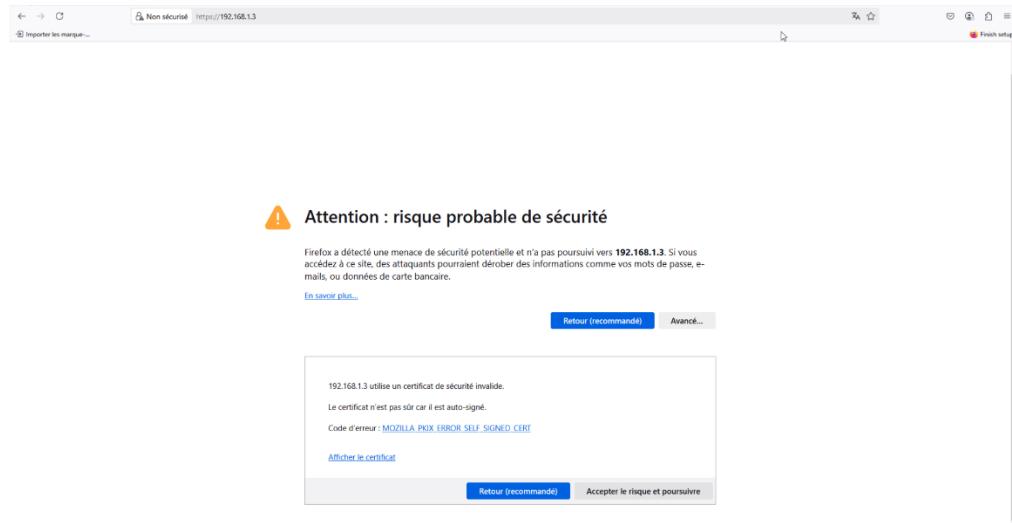
```
The IPv4 LAN address has been set to 192.168.1.3/29
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.1.3/
Press <ENTER> to continue. █
```

On paramètre également un deuxième pfsense qui nous servira plus tard afin de mettre en place un fail over.

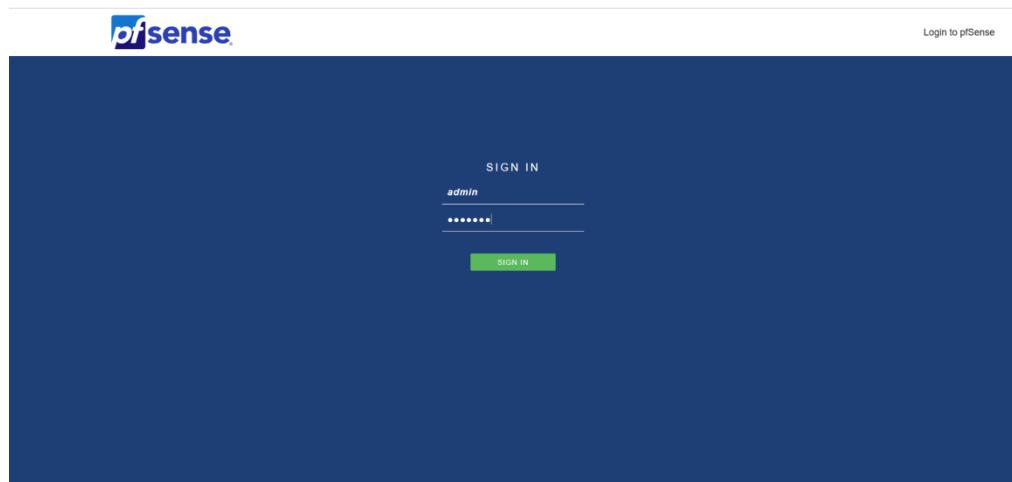
```
WAN (wan)          -> em0          -> v4/DHCP4: 10.34.4.150/24
LAN (lan)          -> em1          -> v4: 192.168.1.4/29
```

Paramétrage de l'interface Web

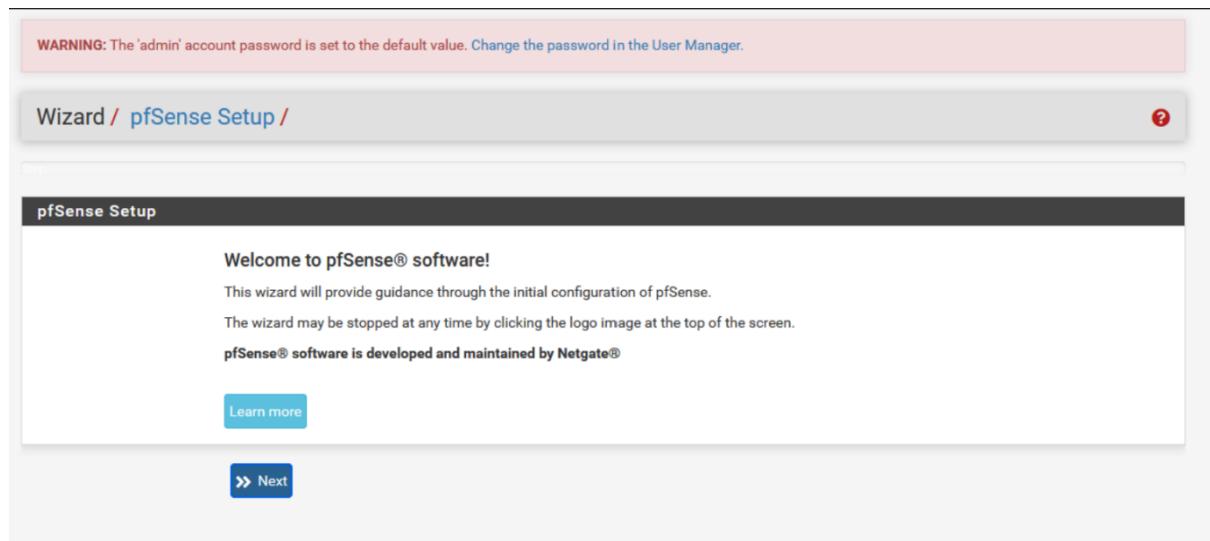
On se connecte désormais à l'interface web du pfsense via son adresse ip à partir d'un navigateur.



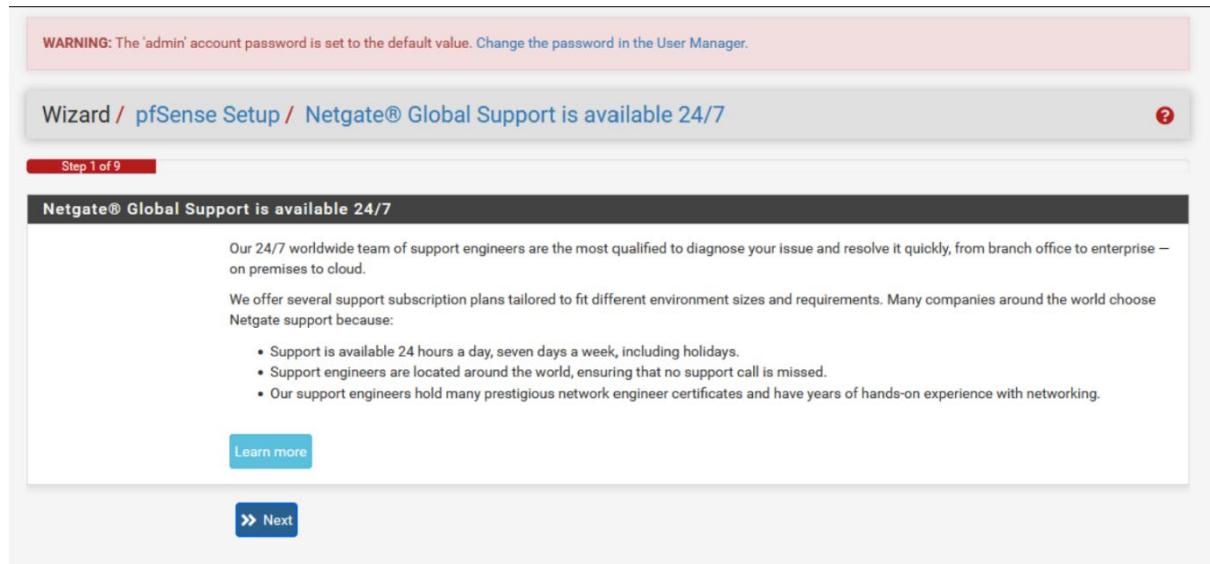
On se connecte à l'interface web à l'aide des identifiant de pfsense par défaut.



Après s'être connecté, un message d'accueil s'affiche, appuie sur « Next ».



On appuie de nouveau sur le bouton continuer après ça.



On remplit ensuite nom d'hôte du routeur et le domaine du routeur.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain techsupp
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

On remplit ensuite le serveur temps du routeur.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone Europe/Paris

>> Next

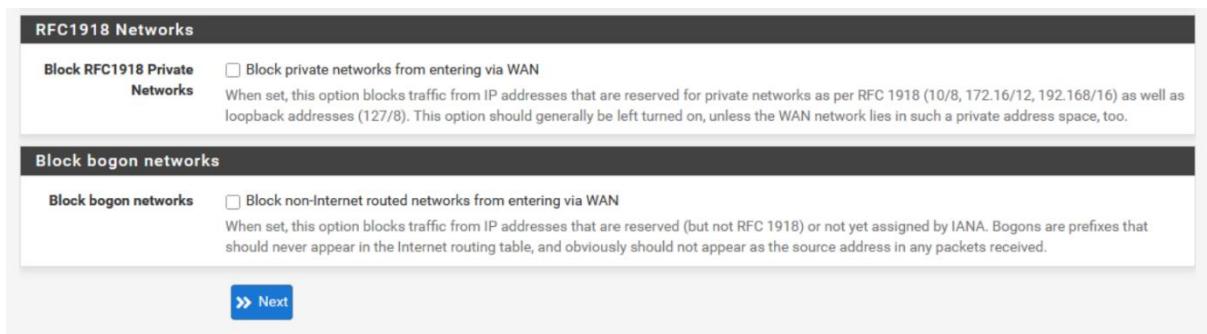
On configure l'interface WAN en DHCP.

Configure WAN Interface

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

SelectedType

Comme nous sommes en virtualisation nous devons décocher ces deux paramètres.



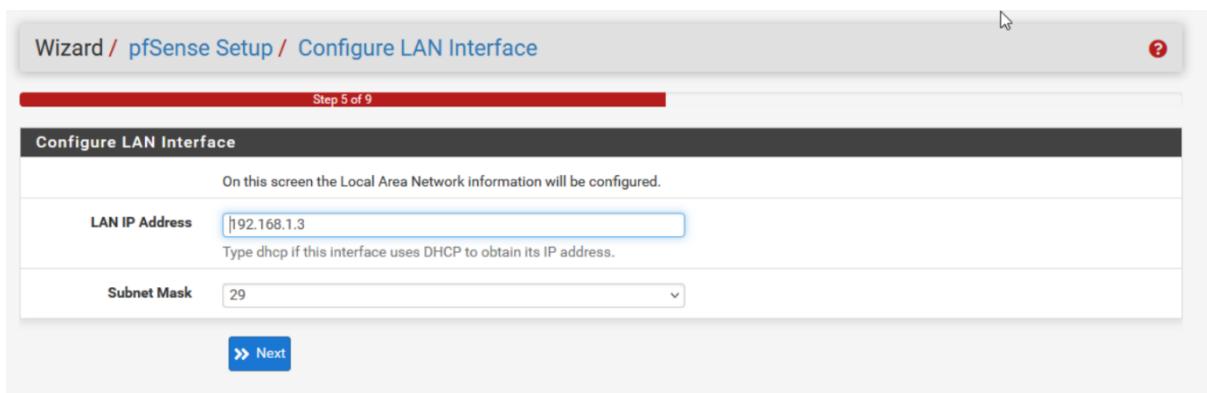
RFC1918 Networks

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

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

>> Next

L'interface LAN a déjà été paramétré depuis l'interface du pfSense donc nous pouvons juste cliquer sur le bouton continuer.



Wizard / pfSense Setup / Configure LAN Interface

Configure LAN Interface

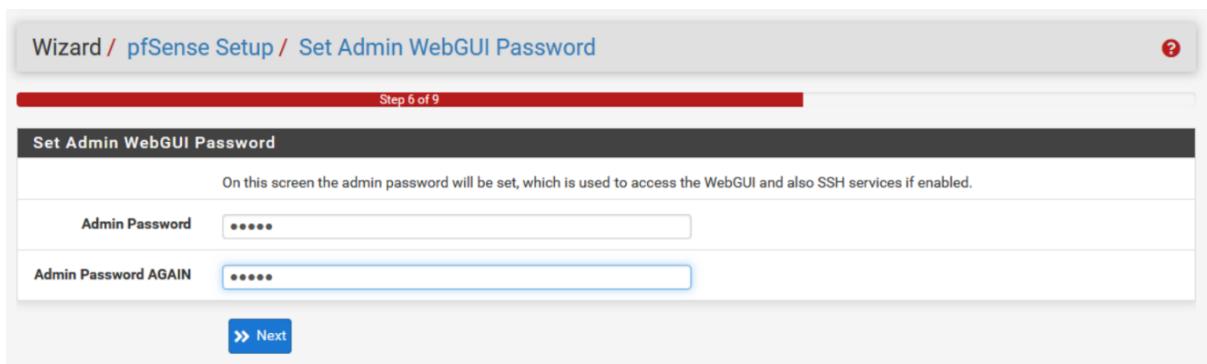
On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.1.3
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 29
Type subnetmask if this interface uses a static subnet mask.

>> Next

On change le mot de passe du compte admin par mesure de sécurité.



Wizard / pfSense Setup / Set Admin WebGUI Password

Set Admin WebGUI Password

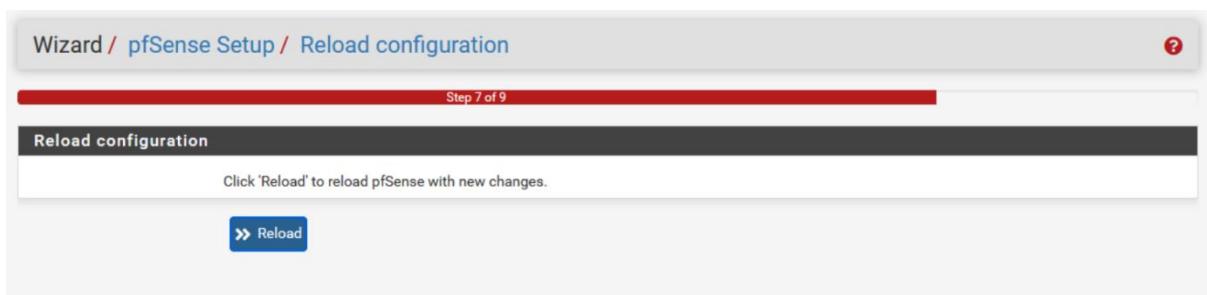
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: *****

Admin Password AGAIN: *****

>> Next

On doit ensuite recharger la page pfSense.



Wizard / pfSense Setup / Reload configuration

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Nous avons terminé de configurer l'interface web du pfSense.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. [Visit our forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Configuration de l'interface de synchronisation

On va maintenant créer l'interface de synchronisation sur les deux pfSense. Cette interface permettra de synchroniser les deux pfSense afin que lorsque on fait des modifications sur le pfSense maître, le pfSense esclave prennent aussi les modifications.

Pour cela, on va tout d'abord aller dans « Interfaces » puis « Assignments ».

System Information

- Name: pfSense.techsupp
- User: admin@192.168.1.1 (Local Database)
- System: VMware Virtual Machine
Netgate Device ID: 055655494e5ac7406dd4
- BIOS: Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
- Version: 2.7.2-RELEASE (amd64)
built on Wed Dec 6 21:10:00 CET 2023
FreeBSD 14.0-CURRENT
- CPU Type: Intel(R) Core(TM) Ultra 9 185H
2 CPUs: 2 package(s) x 1 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
- Hardware crypto: Inactive
- Kernel PTI: Enabled
- MDS Mitigation: Inactive
- Uptime: 01 Hour 19 Minutes 46 Seconds
- Current date/time: Thu Apr 24 15:00:01 CEST 2025
- DNS server(s): 127.0.1, 1.1.1.3, 193.110.81.0
- Last config change: Thu Apr 24 14:56:53 CEST 2025
- State table size: 10,000,000

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

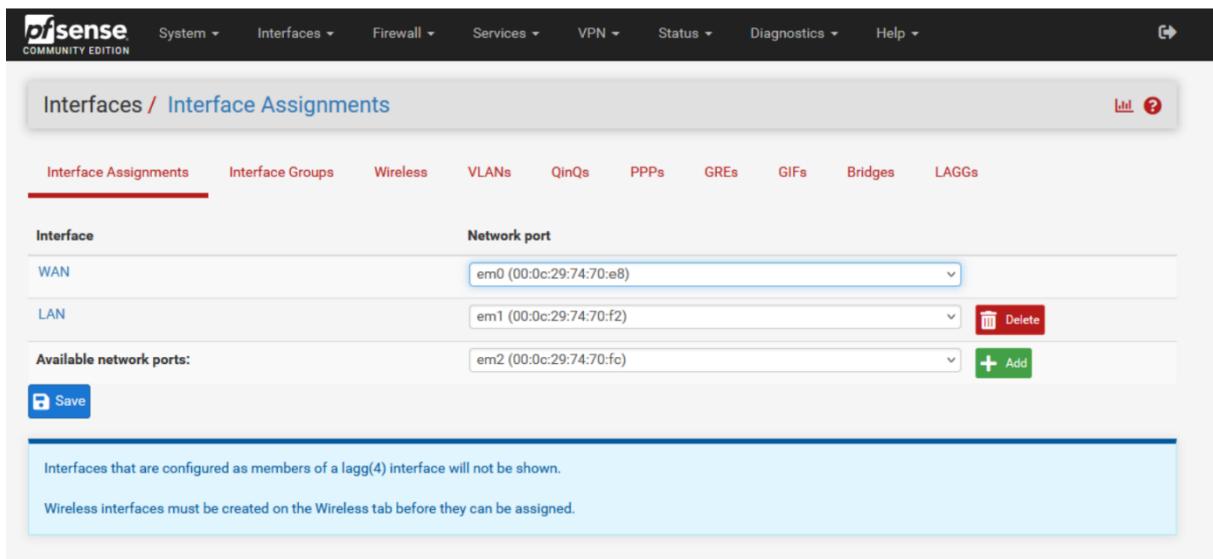
- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

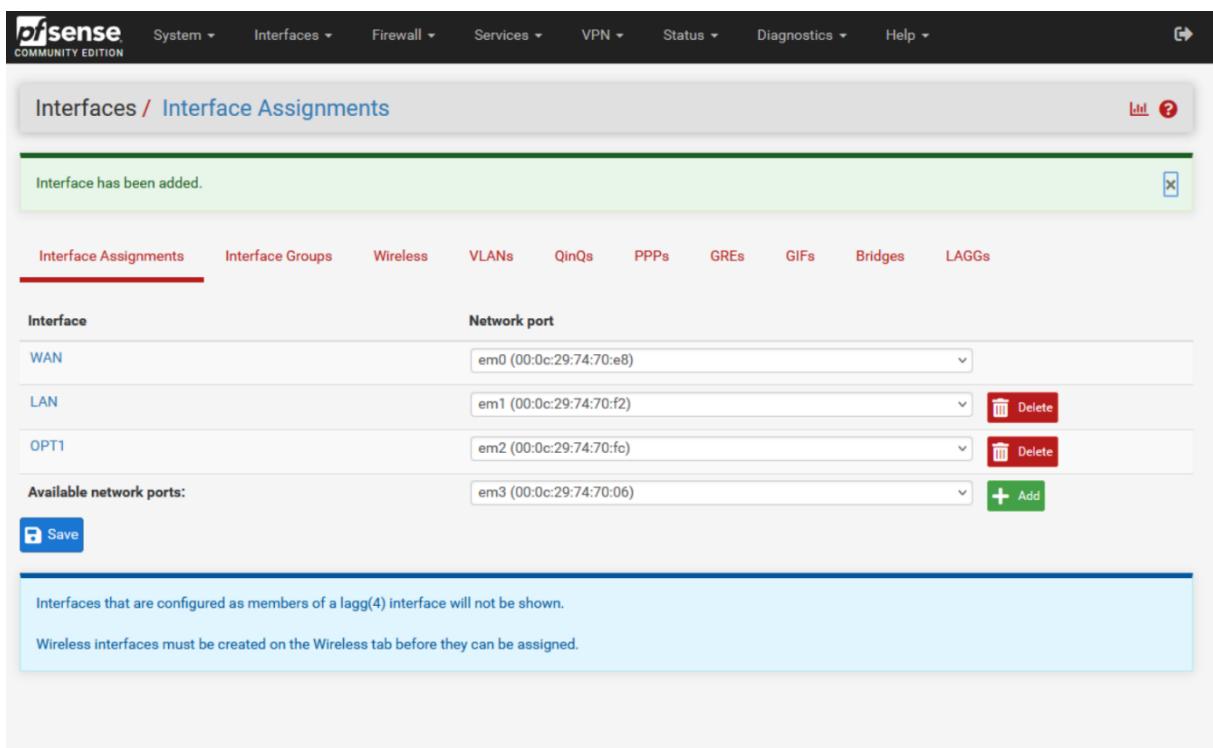
Interface	Speed	Link Status
WAN	1000baseT <full-duplex>	10.34.4.122
LAN	1000baseT <full-duplex>	192.168.1.3

Ensuite, on appuie sur le bouton « Add » afin de rajouter une interface.



The screenshot shows the pfSense interface assignments page. The 'WAN' interface is assigned to 'em0'. The 'LAN' interface is assigned to 'em1', with a 'Delete' button next to it. The 'Available network ports' section shows 'em2' assigned. A 'Save' button is at the bottom left. A note at the bottom states: 'Interfaces that are configured as members of a lagg(4) interface will not be shown. Wireless interfaces must be created on the Wireless tab before they can be assigned.'

Une fois l'interface créé, on clique dessus pour la configurer.



The screenshot shows the pfSense interface assignments page after adding a new interface. The 'WAN' interface is assigned to 'em0'. The 'LAN' interface is assigned to 'em1'. The 'OPT1' interface is assigned to 'em2', with a 'Delete' button next to it. The 'Available network ports' section shows 'em3' assigned. A 'Save' button is at the bottom left. A note at the bottom states: 'Interfaces that are configured as members of a lagg(4) interface will not be shown. Wireless interfaces must be created on the Wireless tab before they can be assigned.'

On paramètre ensuite l'interface suivant les paramètres ci-dessous.

The screenshot shows the configuration for interface OPT1 (em2). The 'General Configuration' section includes fields for Enable (checked), Description (PFSync), IPv4 Configuration Type (Static IPv4), IPv6 Configuration Type (None), MAC Address (xx:xx:xx:xx:xx:xx), MTU (1500), MSS (30), Speed and Duplex (Default), and a Static IPv4 Configuration section with IPv4 Address (10.0.1.1) and IPv4 Upstream gateway (None). The 'Static IPv4 Configuration' section also includes a 'Add a new gateway' button.

On configure également une interface similaire sur le pfSense esclave.

The screenshot shows the configuration for interface OPT1 (em2) on the slave pfSense device. The 'General Configuration' section includes fields for Enable (checked), Description (PFSync-ESCLAVE), IPv4 Configuration Type (Static IPv4), IPv6 Configuration Type (None), MAC Address (xx:xx:xx:xx:xx:xx), MTU (1500), MSS (30), Speed and Duplex (Default), and a Static IPv4 Configuration section with IPv4 Address (10.0.1.2) and IPv4 Upstream gateway (None). The 'Static IPv4 Configuration' section also includes a 'Add a new gateway' button.

Nous devons ensuite aller dans « System » puis « High Availability ».

On configure ensuite le protocole pfsync qui permet la synchronisation.

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer
IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

On met en place les paramètres ci-dessous sur le maître et l'esclave pour le protocole. Le « Synchronize config to IP » n'est à configurer que sur le pfSense maître, tout comme le mot de passe ainsi que le username du pfSense de l'esclave afin que le pfSense maître puisse se connecter à celui-ci.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password Confirm
Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

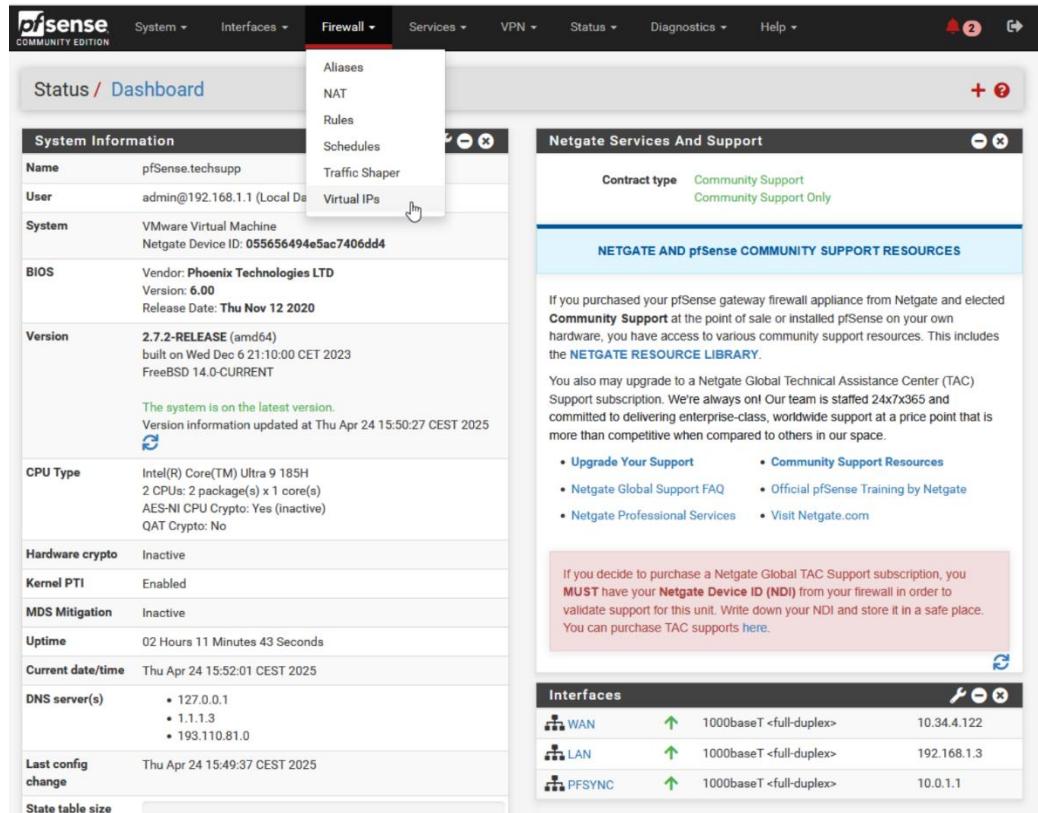
Select options to sync

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WOL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations

Configuration de l'Ip Virtuelle

Après avoir mis en place la synchronisation nous allons mettre en place une ip virtuelle, celle-ci permet de basculer d'un routeur à l'autre si l'un d'entre eux est en défaut.

Pour cela, nous irons tout d'abord dans « Firewall » puis dans « Virtual IPs ».



The screenshot shows the pfSense 2.7.2-RELEASE dashboard. The top navigation bar has 'Firewall' selected. A dropdown menu is open under 'Firewall' with 'Virtual IPs' highlighted. The main content area shows 'System Information' and 'Netgate Services And Support' sections. The 'Virtual IPs' section is not yet visible in the main content area.

Une fois sur le menu nous cliquerons sur le bouton « Add » afin d'ajouter une ip virtuelle.



The screenshot shows the 'Virtual IP Address' table. The 'Actions' column for the first row (WAN) has a green 'Add' button highlighted.

Virtual IP address	Interface	Type	Description	Actions
10.34.4.122	WAN	1000baseT <full-duplex>		
192.168.1.3	LAN	1000baseT <full-duplex>		
10.0.1.1	PFSYNC	1000baseT <full-duplex>		

Nous mettons en place le protocole CARP pour l'ip virtuelle, on lui indique l'adresse ip qu'elle va prendre, ainsi qu'un mot de passe pour se connecter sur la même virtual ip.

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface LAN

Address type Single address

Address(es) 192.168.1.5 / 29

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password Confirm

Enter the VHID group password.

VHID Group 1

Enter the VHID group that the machines will share.

Advertising frequency 1 (Base) 0 (Skew)

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description

A description may be entered here for administrative reference (not parsed).

Save

On va ensuite dans le menu « Firewall » puis « Rules ».

Status / Dashboard

System Information

- Name**: pfSense.techsupp
- User**: admin@192.168.1.1 (Local Data)
- System**: VMware Virtual Machine
Netgate Device ID: 055656494e5ac7406dd4
- BIOS**: Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
- Version**: 2.7.2-RELEASE (amd64)
built on Wed Dec 6 21:10:00 CET 2023
FreeBSD 14.0-CURRENT
- CPU Type**: Intel(R) Core(TM) Ultra 9 185H
2 CPUs: 2 package(s) x 1 core(s)
AES-NI CPU Crypto: Yes (Inactive)
QAT Crypto: No
- Hardware crypto**: Inactive
- Kernel PTI**: Enabled
- MDS Mitigation**: Inactive
- Uptime**: 02 Hours 18 Minutes 23 Seconds
- Current date/time**: Thu Apr 24 15:58:40 CEST 2025
- DNS server(s)**: 127.0.0.1, 1.1.1.3, 193.110.81.0
- Last config change**: Thu Apr 24 15:57:23 CEST 2025

Firewall **Aliases** **NAT** **Rules** **Schedules** **Traffic Shaper** **Virtual IPs**

Netgate Services And Support

- Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

Interface	Link Status	Speed & Duplex	IP Address
WAN	Up	1000baseT <full-duplex>	10.34.4.122
LAN	Up	1000baseT <full-duplex>	192.168.1.3
PFSYNC	Up	1000baseT <full-duplex>	10.0.1.1

On ajoute une règle sur l'interface afin que tout puisse passer car l'interface étant déjà isoler en étant sur son propre réseau, nous n'avons pas besoin de mettre de règle stricte.

Notre ip virtuelle est désormais active.

Création du réseau EMPLOYES

Nous allons maintenant créer le réseau sur lequel les employés de l'entreprise vont pouvoir se connecter tout en pouvant communiquer avec les serveurs.

Pour cela nous irons dans « Interfaces » puis dans « Assignments ».

Nous cliquerons ensuite sur « Add » pour rajouter l'interface LAN_EMPLOYES.

Interface Assignments

Interface

Network port

WAN em0 (00:0c:29:74:70:e8)

LAN em1 (00:0c:29:74:70:f2) Delete

PFSync em2 (00:0c:29:74:70:fc) Delete

Available network ports: em3 (00:0c:29:74:70:06) Add

Save

Après ça on clique sur l'interface pour la configurer.

OPT2 em3 (00:0c:29:74:70:06) Delete

On effectue les paramètres ci-dessous pour l'interface.

General Configuration

Enable Enable interface

Description LAN_EMPLOYES

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address 00:0c:29:74:70:06

MTU

MSS

Speed and Duplex Default (no preference, typically autoselect)

Static IPv4 Configuration

IPv4 Address 192.168.1.126 / 26

IPv4 Upstream gateway None Add a new gateway

On va ensuite paramétrer le DHCP sur l'interface.

Pour cela nous allons aller dans « Services » puis dans « DHCP Server ».



On met ensuite les réglages ci-dessous pour le DHCP.

General DHCP Options

DHCP Backend: ISC DHCP

Enable: Enable DHCP server on LAN_EMPLOYES interface

BOOTP: Ignore BOOTP queries

Deny Unknown Clients: Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Denied Clients: Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore Client Identifiers: Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet: 192.168.1.64/26

Subnet Range: 192.168.1.65 - 192.168.1.126

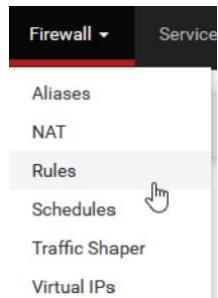
Address Pool Range: From 192.168.1.65 To 192.168.1.125

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

On va ensuite rajouter une règle sur l'interface pour que le LAN_EMPLOYES puisse communiquer avec le réseau des serveurs.



On appuie sur le bouton « Add » pour ajouter une règle.

A screenshot of the 'Firewall / Rules / LAN_EMPLOYES' interface. The 'LAN_EMPLOYES' tab is selected. The main area shows a table header with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. Below the table, a message says: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.' At the bottom right, there is a toolbar with buttons for Add (highlighted with a cursor), Delete, Toggle, Copy, Save, and Separator.

On fait en sorte que tout puisse passer entre les deux réseaux.

A screenshot of the 'Edit Firewall Rule' dialog. The 'Action' dropdown is set to 'Pass'. The 'Disabled' section has a checkbox 'Disable this rule' which is unchecked. The 'Interface' dropdown is set to 'LAN_EMPLOYES'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'TCP'. The 'Source' section includes a 'Source' dropdown, an 'Invert match' checkbox, a 'LAN address' dropdown, and a 'Source Address' input field. A 'Display Advanced' button is available. The 'Destination' section includes a 'Destination' dropdown, an 'Invert match' checkbox, a 'Any' dropdown, a 'Destination Address' input field, and a 'Destination Port Range' section with 'From' and 'To' fields both set to 'Custom'. A note at the bottom says: 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.'

On ajoute la même règle sur l'interface des serveurs afin qu'ils puissent répondre.

Mise en place d'un serveur stockage TrueNAS

Installation de TrueNAS

Nous allons maintenant installer le serveur de stockage TrueNAS.

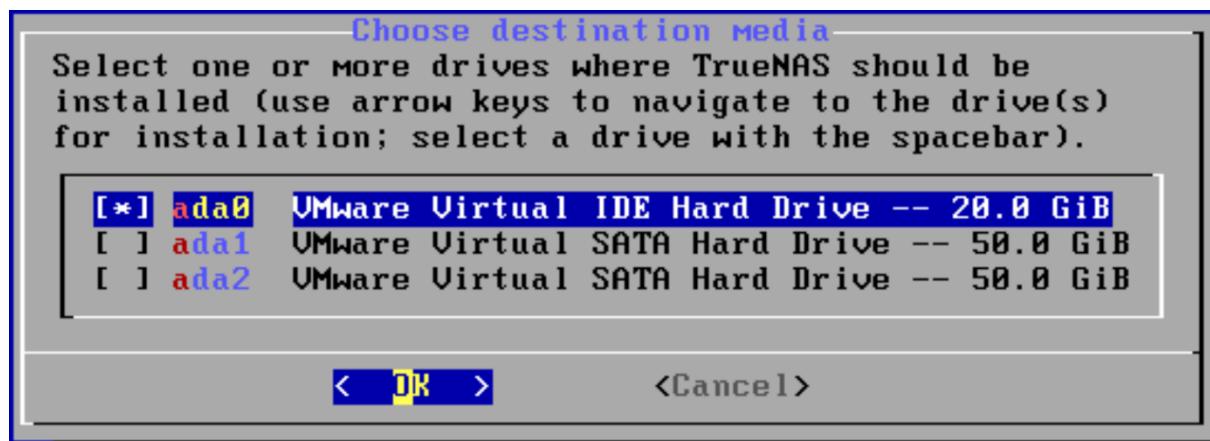
Lorsque on démarre sur l'image ISO de Truenas on arrive sur ce menu. Pour une installation normale et complète, on saisi 1.



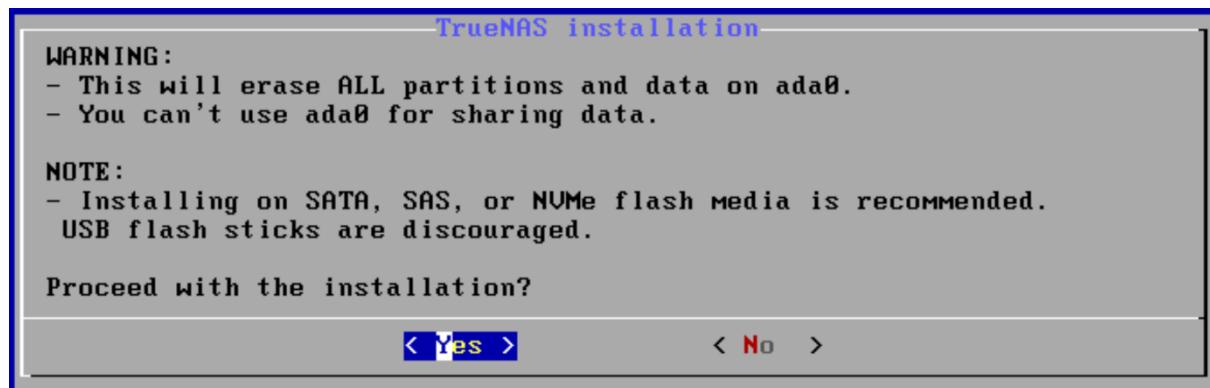
On se met sur l'option 1 et on appuie sur entrer. Cela permet soit d'installer le système TrueNAS, soit de le mettre à jour dans le cas où une version est déjà installée.



On sélectionne le volume sur lequel on souhaite installer TrueNAS. Il est à noter que le volume utilisé pour l'installation de TrueNAS ne pourra pas être utilisé pour la mise en place d'un système RAID.



On confirme qu'on souhaite bien installer TrueNAS.



L'installation est terminée, le serveur redémarre.



Une fois que le serveur est redémarré. On saisis 1 pour accéder aux paramètres réseau.

Console setup

- 1) Configure Network Interfaces
- 2) Configure Link Aggregation
- 3) Configure VLAN Interface
- 4) Configure Default Route
- 5) Configure Static Routes
- 6) Configure DNS
- 7) Reset Root Password
- 8) Reset Configuration to Defaults
- 9) Shell
- 10) Reboot
- 11) Shut Down

The web user interface is at:

<http://192.168.1.73>
<https://192.168.1.73>

Enter an option from 1-11: 1

Configuration de l'interface réseau

On va désormais configurer l'interface réseau du serveur.

Choisir l'interface à configurer.

1) em0
Select an interface (q to quit): 1

On choisit de ne pas déconnecter l'interface.

Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n

On va configurer l'interface manuellement donc on dit non pour la configuration via le dhcp.

Configure interface for DHCP? (y/n) n

On configure l'ipv4.

```
Configure IPv4? (y/n) y█
```

On configure le nom de l'interface.

```
Interface name:em0█
```

Puis on met les paramètres ci-dessous pour la configuration réseau.

```
Several input formats are supported
Example 1 CIDR Notation:
    192.168.1.1/24
Example 2 IP and Netmask separate:
    IP: 192.168.1.1
    Netmask: 255.255.255.0, /24 or 24
IPv4 Address:192.168.1.2/29█
```

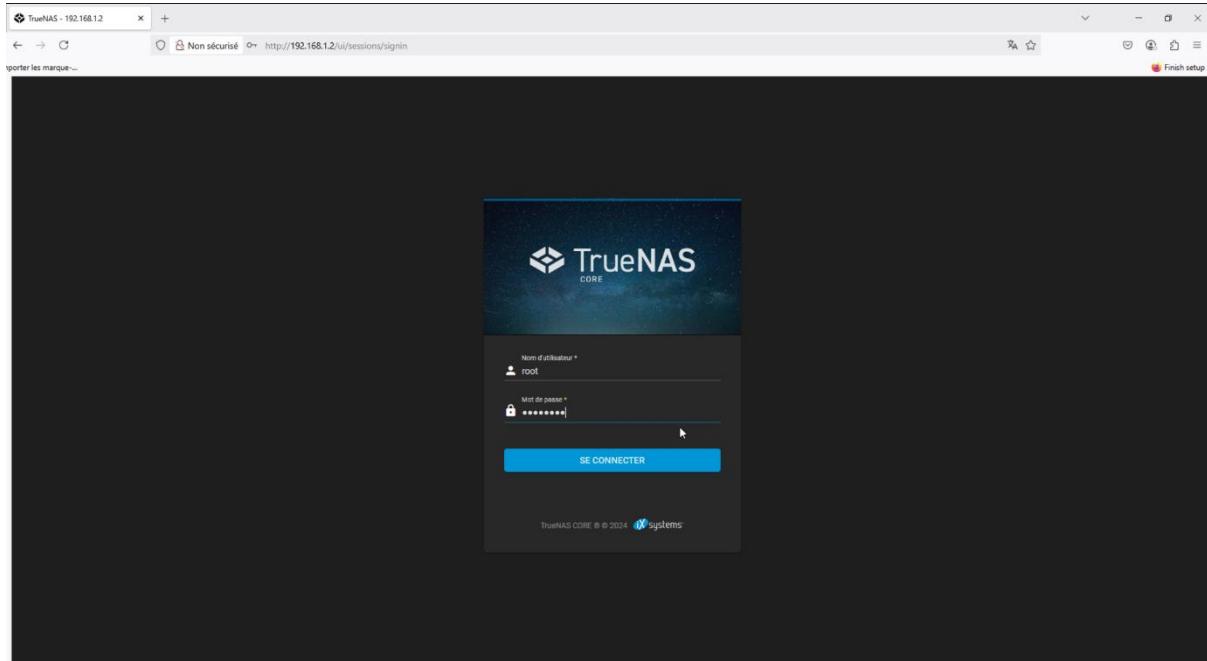
Après ça on ne configure pas l'ipv6 car on ne l'utilisera pas et on peut voir sur l'interface du TrueNAS que l'ip de la machine a bien été modifié.

```
The web user interface is at:
http://192.168.1.2
https://192.168.1.2
```

Accès à l'interface web

A l'aide de votre navigateur internet vous pouvez accéder à l'interface web de TrueNAS en indiquant l'adresse IP de votre serveur dans la barre d'adresse.

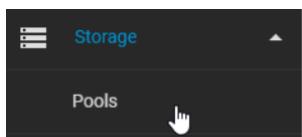
On se connecte donc ensuite depuis l'interface réseau.



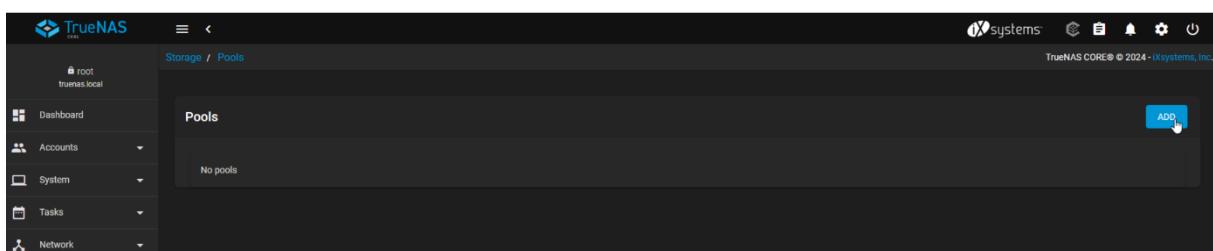
Création du pool de stockage

On va maintenant créer le pool sur lequel seront créer les répertoires partagés du serveur.

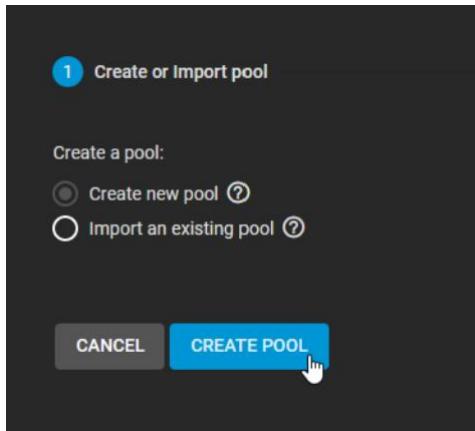
On clique donc sur « Storage » puis sur « Pools ».



On appuie ensuite sur le bouton « add » pour ajouter le pool.

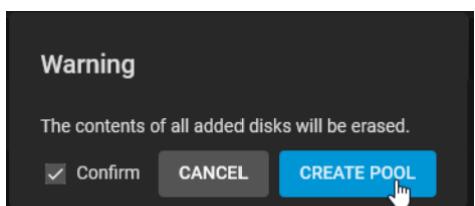


On clique sur le bouton « Create Pool » ensuite.



On met les configurations ci-dessous pour le pool créé. On lui attribue les deux disque que nous avons mis dans le TrueNAS.

On confirme ensuite l'ajout du pool.



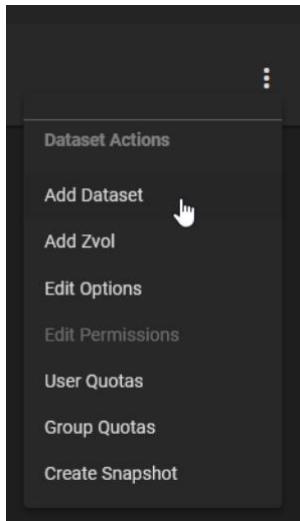
Le pool est maintenant créé.

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments	⋮
STOCKAGE	FILESYSTEM	7.77 MiB	46.02 GiB	lz4	18.21	false	OFF		

Ajout d'un dataset dans le pool

Nous allons maintenant pouvoir paramétrer le dataset dans le pool créé, ce sera le dossier auquel auront accès les utilisateurs.

On appuie sur les trois petits points à droite du pool, puis on clique sur « Add Dataset ».



On paramètre le dataset selon la configuration ci-dessous.

Name and Options

Name * PARTAGE_EMPLOYES

Comments

Sync: Inherit (standard)

Compression level: Inherit (lz4)

Enable Atime: Inherit (off)

Encryption Options

Inherit (non-encrypted) [?](#)

Other Options

ZFS Deduplication: Inherit (off)

Case Sensitivity: Insensitive

Share Type: SMB

Buttons

SUBMIT CANCEL ADVANCED OPTIONS

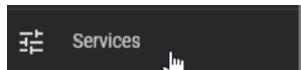
Le dataset est maintenant créé.

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments	⋮
STOCKAGE	FILESYSTEM	7.94 MiB	46.02 GiB	lz4	18.00	false	OFF		⋮
PARTAGE_EMPLOYES	FILESYSTEM	96 KiB	46.02 GiB	Inherits (lz4)	1.00	false	OFF		⋮

Configuration du protocole de partage de fichier

Nous allons maintenant activer le protocole du partage de fichier qui sera disponible sur le serveur.

On clique donc sur « Services ».



On appuie ensuite sur le petit stylo à droite de l'option SMB, on utilise ce protocole car nous n'avons que des machines clientes Windows.

Name	Running	Start Automatically	Actions
LLDP	●	<input type="checkbox"/>	<input type="button" value="edit"/>
NFS	●	<input type="checkbox"/>	<input type="button" value="edit"/>
OpenVPN Client	●	<input type="checkbox"/>	<input type="button" value="edit"/>
OpenVPN Server	●	<input type="checkbox"/>	<input type="button" value="edit"/>
Rsync	●	<input type="checkbox"/>	<input type="button" value="edit"/>
S.M.A.R.T.	●	<input checked="" type="checkbox"/>	<input type="button" value="edit"/>
S3	●	<input type="checkbox"/>	<input type="button" value="edit"/>
SMB	●	<input type="checkbox"/>	<input type="button" value="edit"/> <input type="button" value="Configure"/>
SNMP	●	<input type="checkbox"/>	<input type="button" value="edit"/>
SSH	●	<input type="checkbox"/>	<input type="button" value="edit"/>
TFTP	●	<input type="checkbox"/>	<input type="button" value="edit"/>
UPS	●	<input type="checkbox"/>	<input type="button" value="edit"/>

On paramètre le protocole comme ci-dessous.

NetBIOS

NetBIOS Name *
truenas ?

NetBIOS Alias

Workgroup *
techsupp.local ?

Description
TrueNAS Server ?

Enable SMB1 support ?

NTLMv1 Auth ?

SAVE **CANCEL** **ADVANCED OPTIONS**

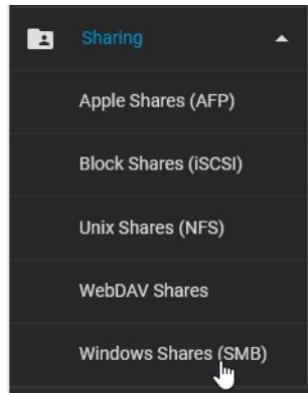
On active ensuite le service.



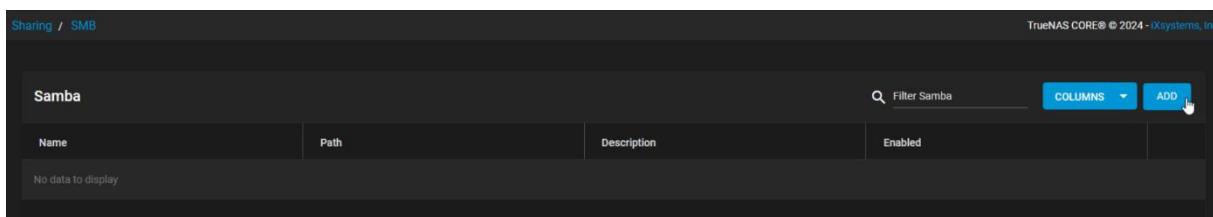
Configuration du partage de fichier

Nous allons maintenant configurer le partage de fichier.

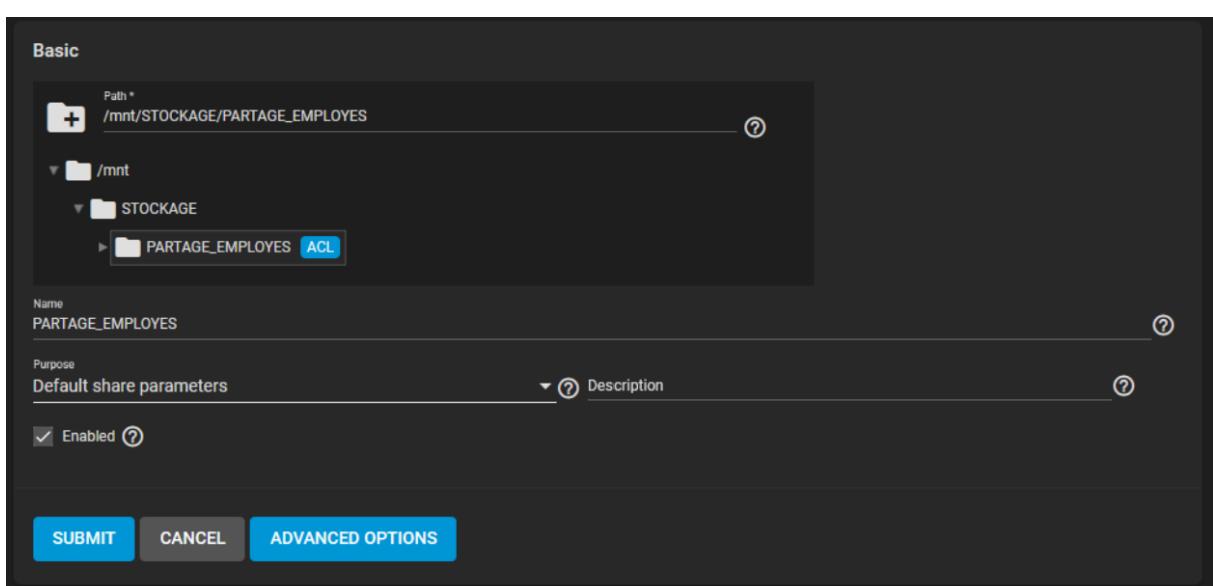
Pour cela nous allons cliquer sur « Sharing » puis « Windows Shares ».



On appuie ensuite sur « Add ».



Puis on met les paramètres ci-dessous pour le partage.



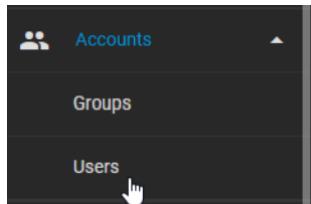
Le partage est désormais créé.

Name	Path	Description	Enabled	⋮
PARTAGE_EMPLOYES	/mnt/STOCKAGE/PARTAGE_EMPLOYES		yes	⋮

Paramétrage des comptes utilisateurs TrueNAS

Nous allons maintenant créer les utilisateurs sur TrueNAS.

Pour cela nous devons aller dans « Accounts » puis dans « Users ».



On clique sur le bouton « Add » pour ajouter l'utilisateur.

Users				Filter Users	ADD	⋮
Username	UID	Builtin	Full Name			
root	0	yes	root			
1 - 1 of 1						

On créer le compte avec ses informations dans notre cas.

Identification

Full Name *
Antoine MOREAUX

Username *
amoreaux

Email

Password *

Confirm Password *

User ID and Groups

User ID *
1000

New Primary Group

Primary Group

Auxiliary Groups

On lui donne les permissions sur le partage que l'on viens de créer.

Directories and Permissions

Home Directory: /mnt/STOCKAGE/PARTAGE_EMPLOYES

Home Directory Permissions

	Read	Write	Execute
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Authentication

SSH Public Key

Disable Password: No

Shell: sh

Lock User

Permit Sudo

Microsoft Account

Samba Authentication

Le compte est désormais créé.

Users

Username	UID	Builtin	Full Name
amoreaux	1000	no	Antoine MOREAUX
root	0	yes	root

1 - 2 of 2

On crée aussi un compte admin qui aura plus de droit sur le partage.

Users

Username	UID	Builtin	Full Name
admintechsupp	1001	no	Admin Techsupp
amoreaux	1000	no	Antoine MOREAUX
root	0	yes	root

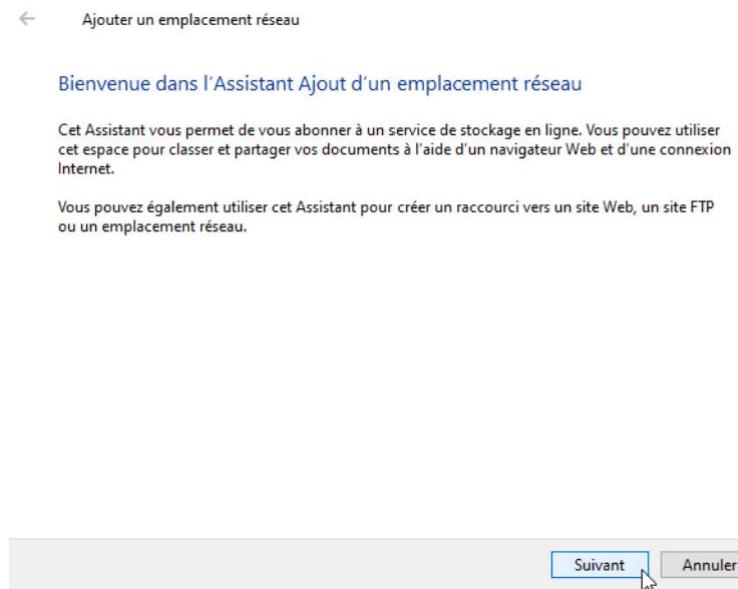
1 - 3 of 3

Ajout de l'emplacement réseau sur les machines

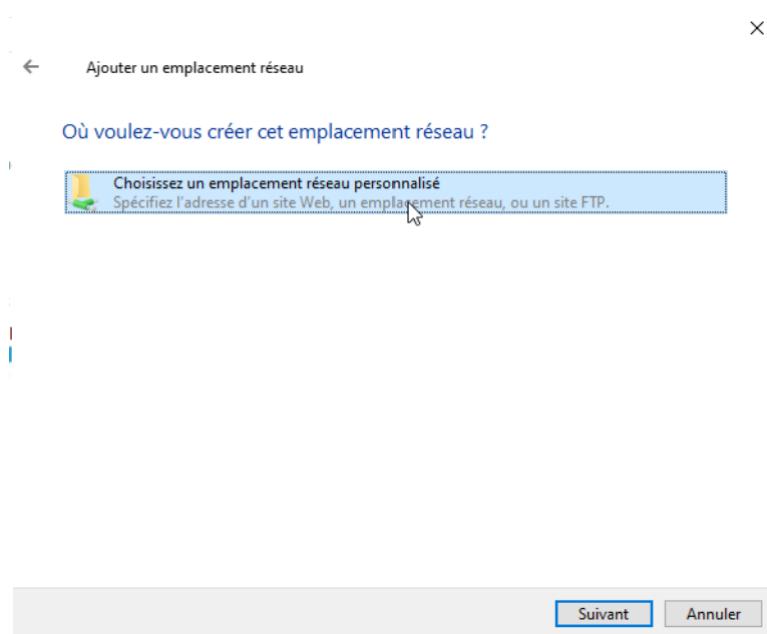
Nous allons maintenant passer du côté du Windows Server afin de rajouter la partage réseau dessus en tant que raccourci.

Pour cela, on ira sur l'Explorateur de fichier, puis on fait clique droit et « Ajout de lecteur réseau »

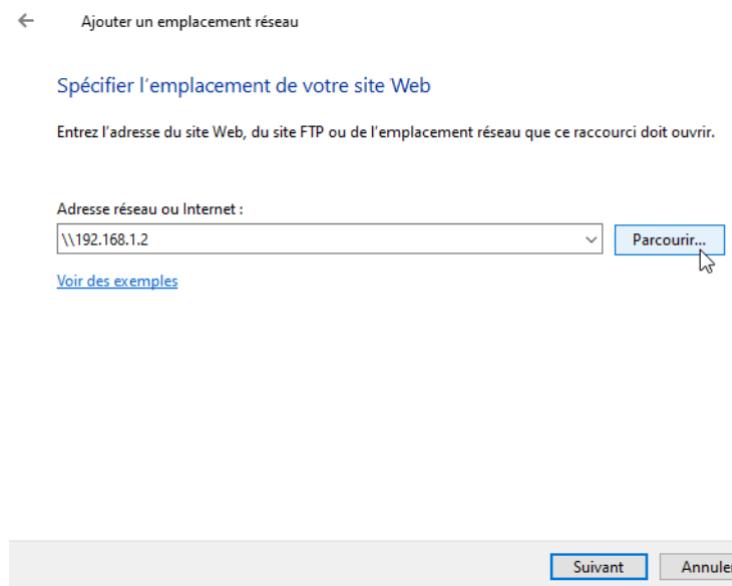
On arrive ensuite sur l'Assistant d'ajout d'emplacement réseau. On clique sur « Suivant » une fois arrivé dessus.



On ajoute un emplacement réseau personnalisé.



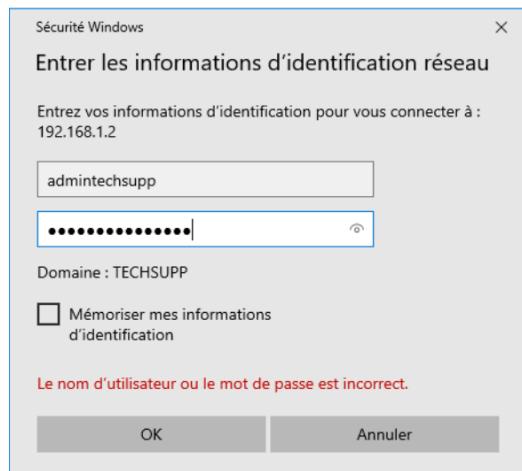
On met l'ip de notre serveur stockage puis on clique sur parcourir.



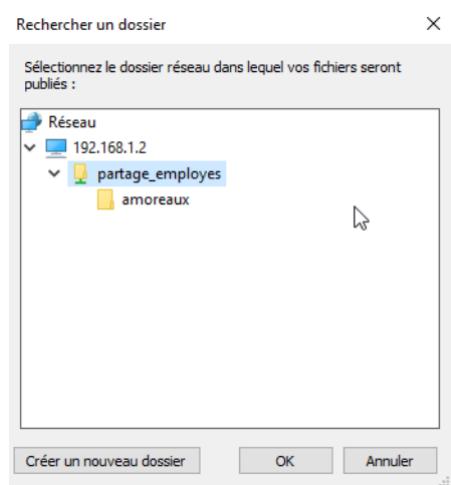
On voit qu'on trouve le serveur, on double clique dessus.



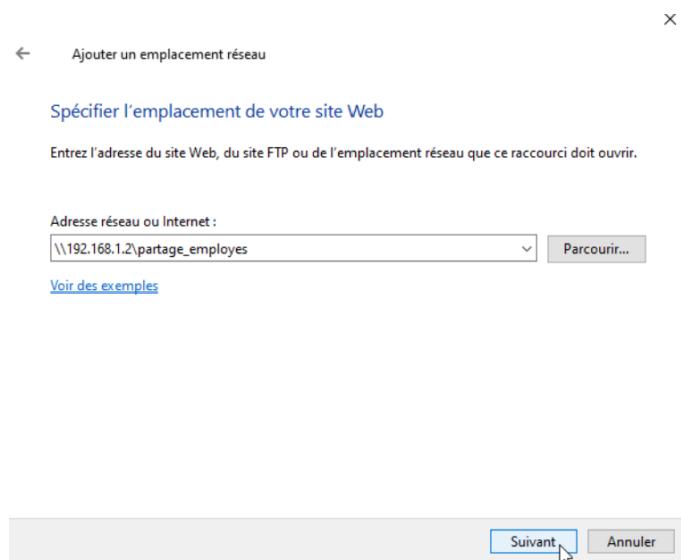
On rentre ensuite nos informations d'utilisateur créé précédemment.



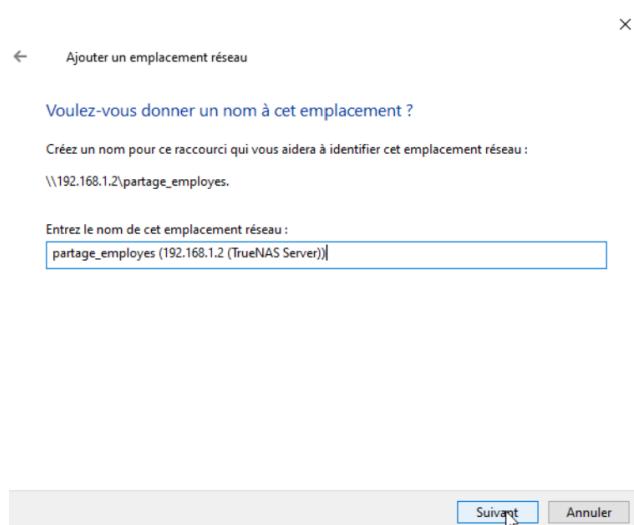
On choisit ensuite le dossier que l'on veut rajouter comme raccourci.



On vérifie que le chemin soit correct puis on clique sur suivant.



On définit ensuite le nom du partage puis on clique sur suivant et terminer.



Le partage réseau est désormais rajouté sur le Windows Server.

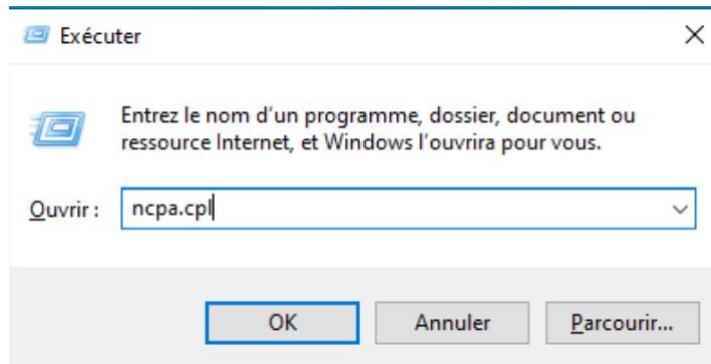
Paramétrage du Windows Client

Nous allons maintenant paramétré le client qui servira pour les employés de l'entreprise.

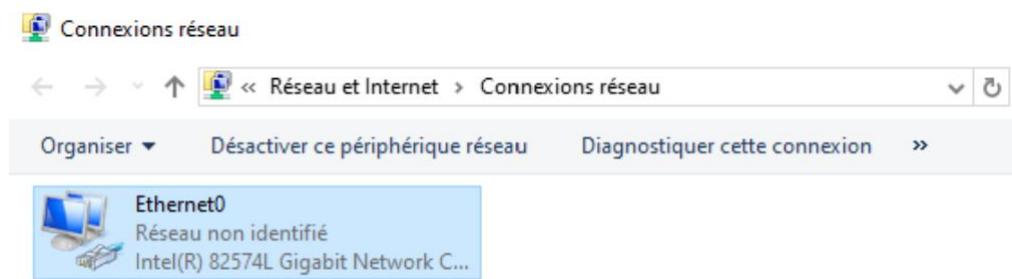
Paramétrage du réseau

Nous allons tout d'abord configurer l'interface réseau du client.

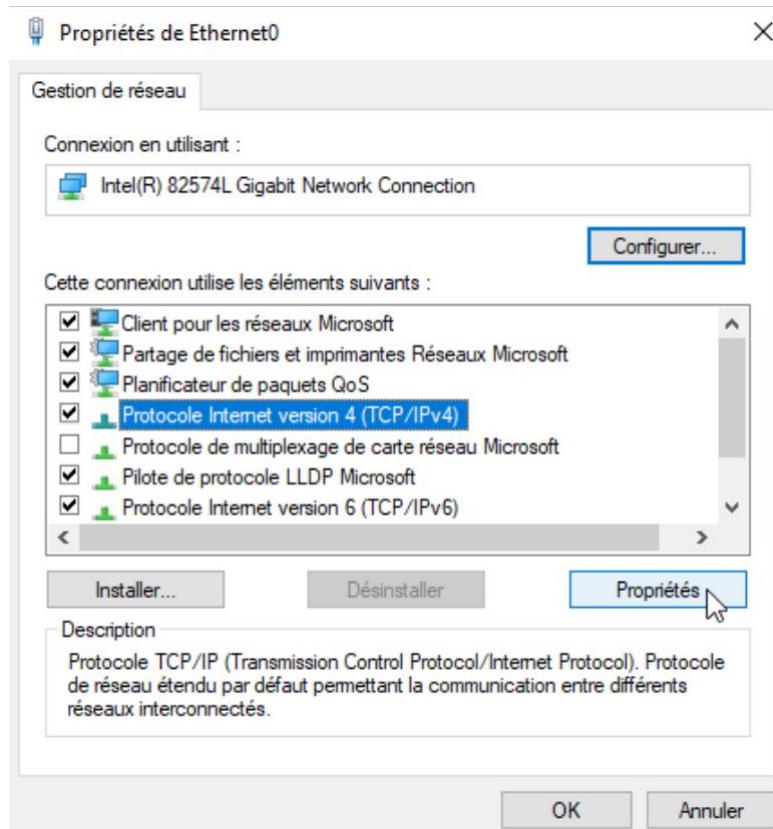
Pour cela on ouvrira le panneau des paramètres réseau et internet.



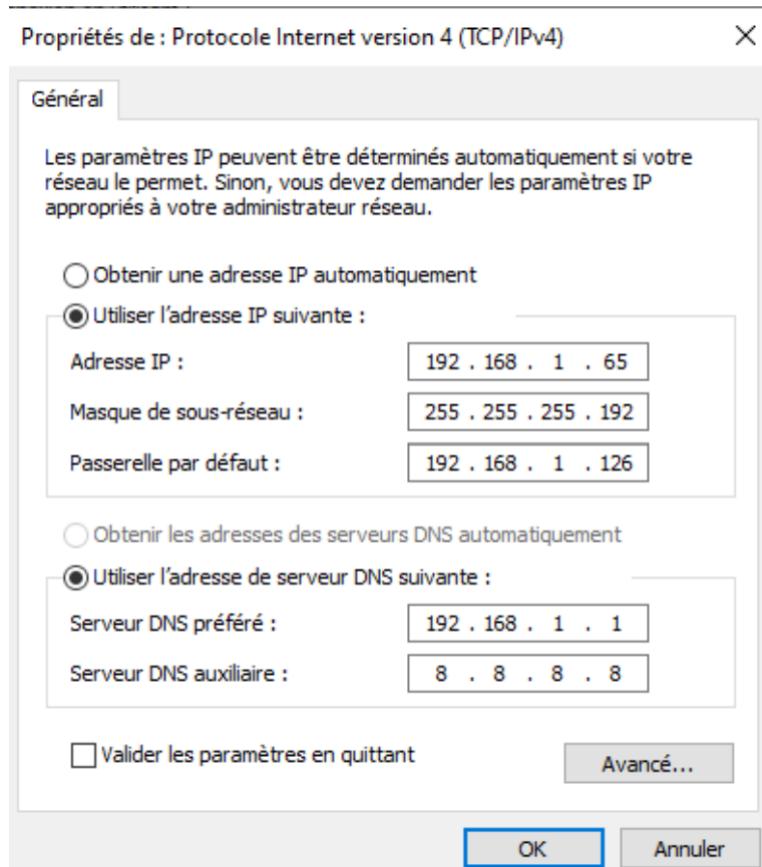
On fait ensuite clique droit sur l'interface réseau puis interface.



Après ça on clique sur « Propriétés ».



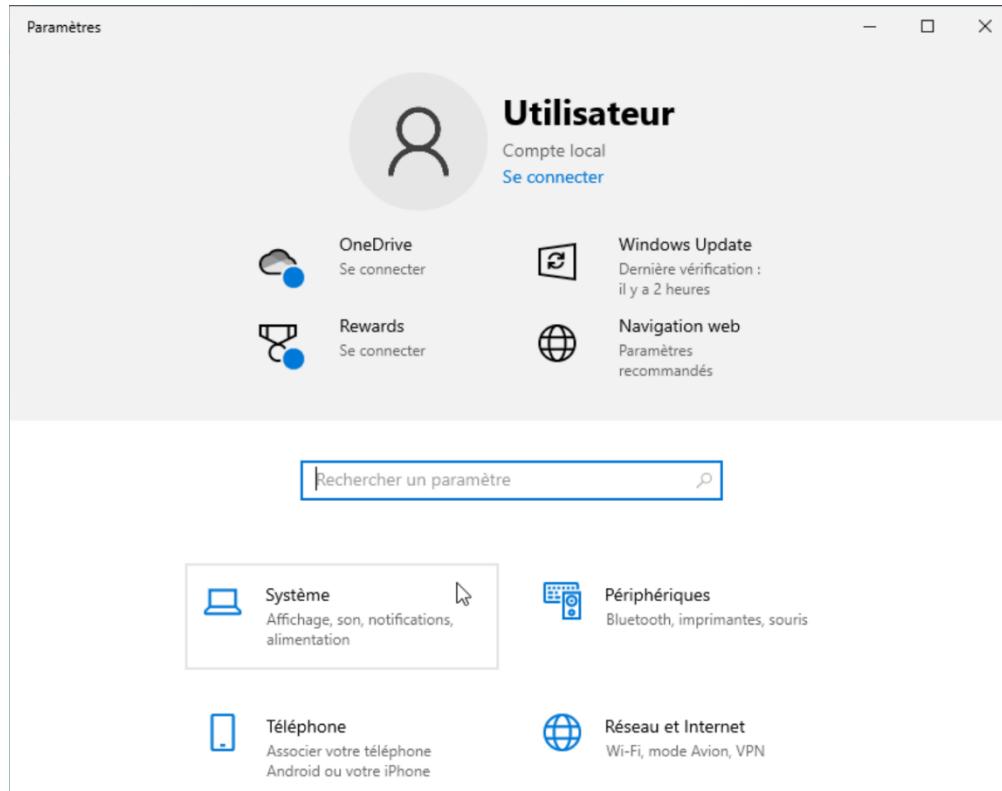
On met ces paramètres réseau pour l'instant.



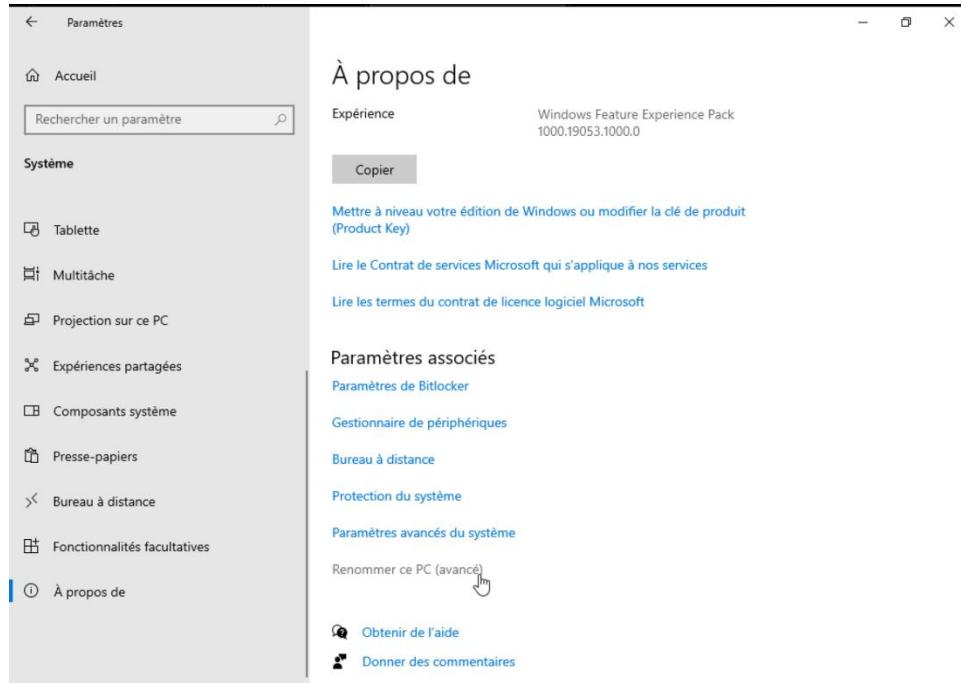
Rentrer le pc client dans le domaine

Nous allons maintenant faire rentrer le pc client dans le domaine précédemment créé.

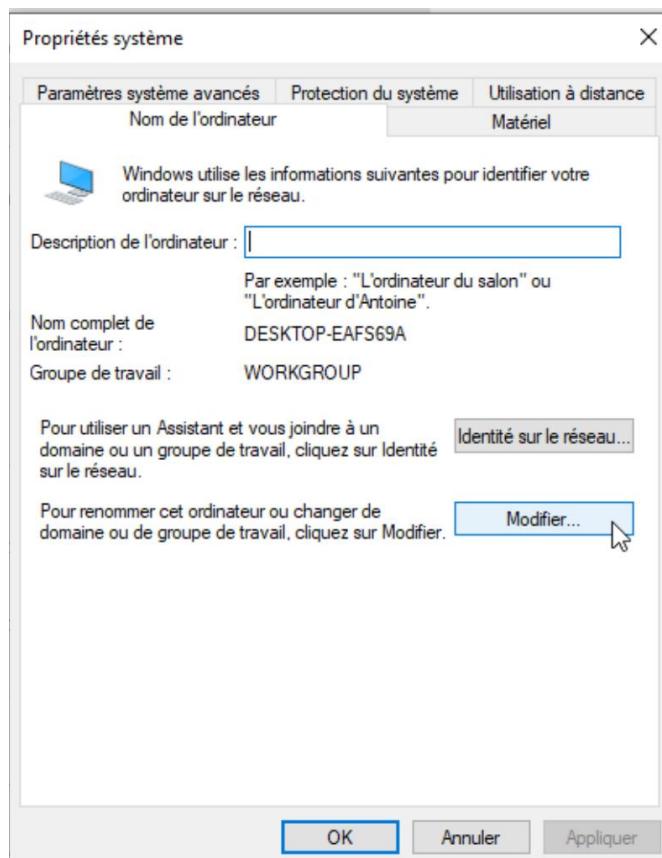
On va tout d'abord dans les paramètres puis on clique sur « Système ».



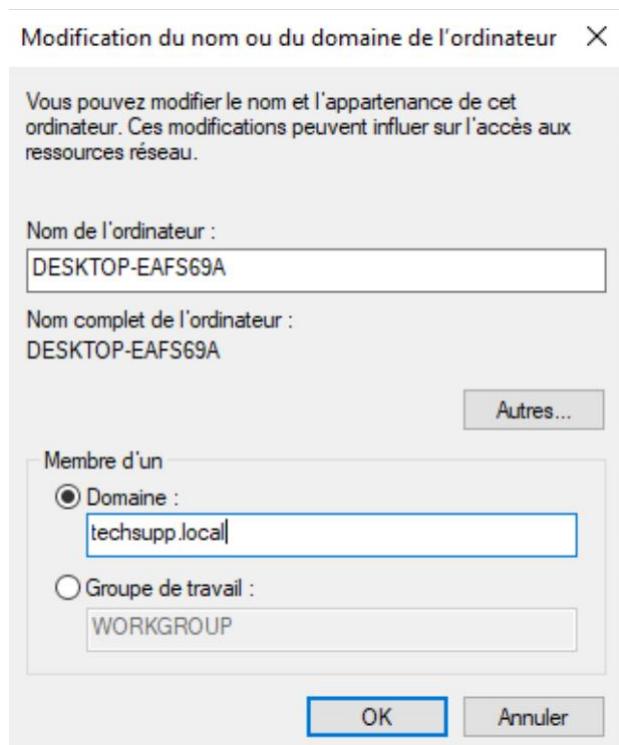
On va ensuite dans « A propos de » puis sur « Renommer ce pc(avancé) ».



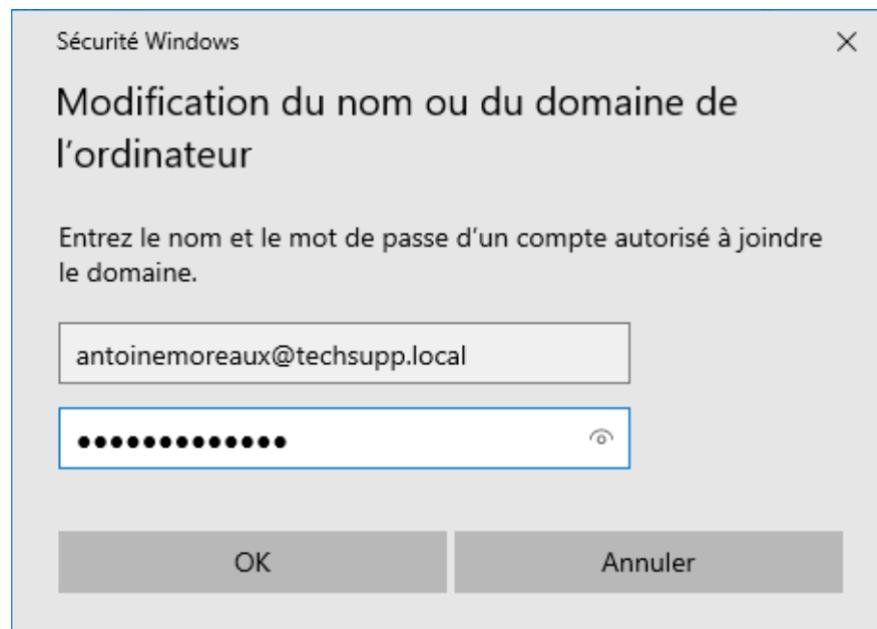
On clique ensuite sur « Modifier ».



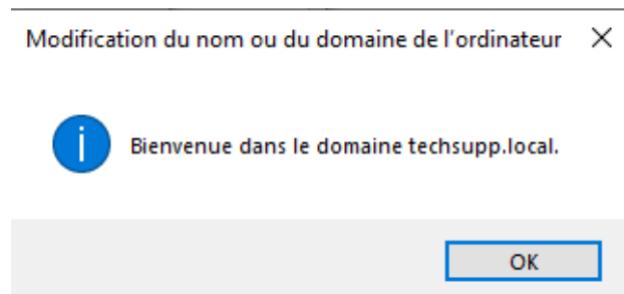
On rentre maintenant qu'on souhaite rejoindre.



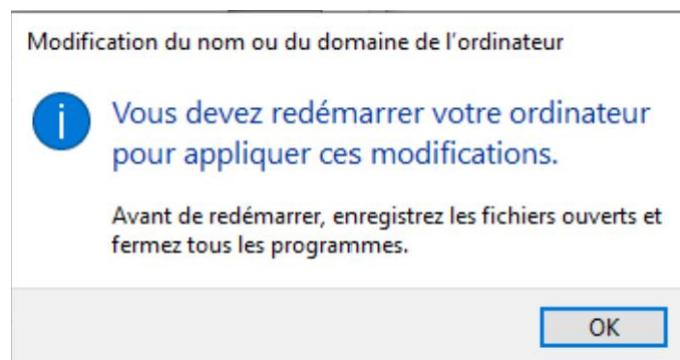
On doit ensuite rentrer les codes de l'utilisateur avec lequel on souhaite rejoindre le domaine.



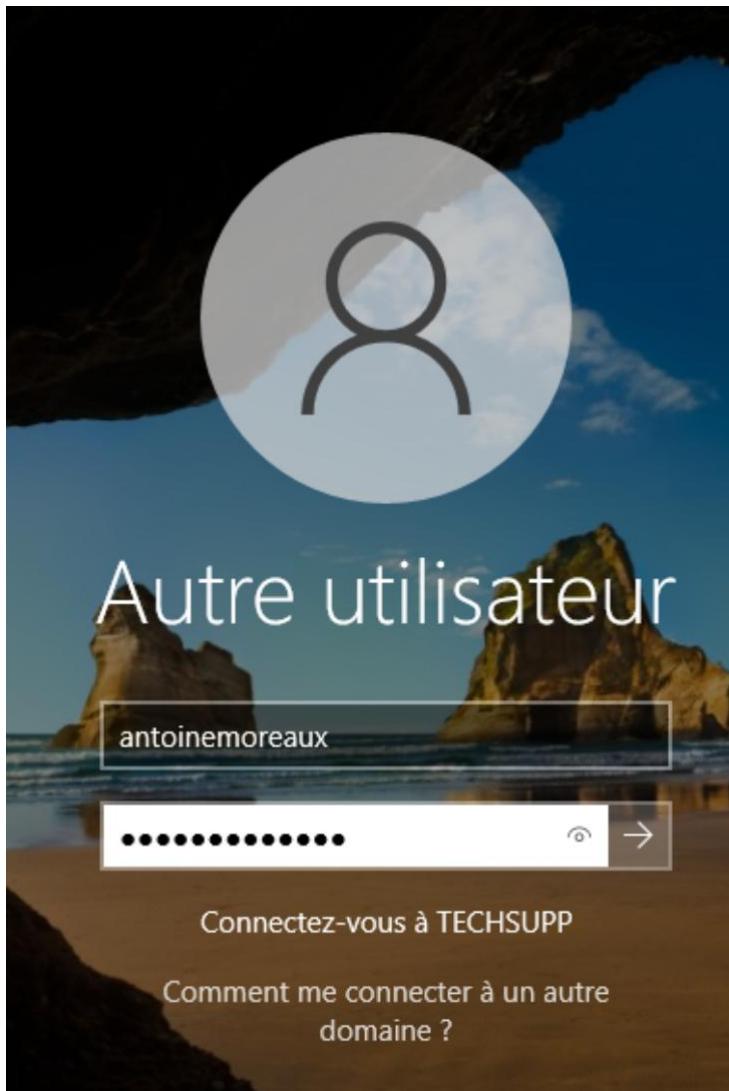
Nous sommes maintenant connectés au domaine à partir du PC client.



Le PC va juste devoir redémarrer.



Après un redémarrage, nous allons désormais pouvoir nous connecter avec un compte du domaine.



Remerciement

Je tiens à exprimer ma sincère gratitude à toutes les personnes qui m'ont accompagné et soutenu tout au long de ma période de stage chez Perfectys Telecom.

Je remercie particulièrement toute l'équipe de Perfectys Telecom pour leur accueil chaleureux, leur disponibilité, ainsi que pour l'encadrement et la confiance qu'ils m'ont accordés durant cette expérience professionnelle enrichissante. Leur expertise et leurs conseils m'ont permis d'approfondir mes compétences dans le domaine de l'informatique et de mieux comprendre les réalités du monde professionnel.

Je souhaite également remercier Monsieur NACERI, mon professeur d'informatique, pour son suivi, ses conseils avisés, et son soutien tout au long de la formation. Son accompagnement pédagogique a été précieux dans la réalisation de ce projet et dans l'élaboration de ce dossier technique.

Enfin, je remercie l'ensemble des enseignants et du personnel de l'établissement pour leur implication et leur disponibilité tout au long de ces deux années de BTS SIO.