# Documentation d’exploitation

*Réalisé par :*

*Blondel Lucas*

*Caparros Maxime*

# Table des matières

# Introduction

Le projet consiste en la mise en place d'un intranet pour la gestion simplifiée de l'ensemble des services IT d'une entreprise, comprenant notamment un annuaire, une gestion de mails, une prise de notes, un agenda et une gestion de fichiers.

Le projet doit également proposer des applications internes telles qu'un serveur mail, un serveur web et une gestion d'agenda, ainsi qu'une gestion d'utilisateurs et de groupes via un annuaire, un portail captif, un VPN, etc. Le système doit mettre en œuvre un SSO fonctionnel, une interface "access management" pour les liens vers les applications internes et un accès distant (VPN).

## 1. Schéma d'infrastructure

## 2. Les différentes technologies utilisées

### 1. Choix d'un Firewall

Pour le choix du firewall nous en avons choisi 3 puis nous avons effectué un tableau de pondération :

| | OS Linux | Routage | Filtrage IDS - IPS | Facilité d'utilisation | Open-source | Reverse proxy | Proxy | DNS | DHCP | Total /45 |
|---|---|---|---|---|---|---|---|---|---|---|
| Pondération | 3 | 3 | 5 | 4 | 5 | 5 | 2 | 2 | 2 | |
| Pfsense | 4 | 4 | 5 | 4 | 5 | 3 | 4 | 3 | 3 | 35 |
| OPNSense | 4 | 3 | 5 | 4 | 5 | 3 | 4 | 3 | 3 | 34 |
| IP Fire | 0 | | | | | | | | | 0 |
| Pour faire le choix de notre pare feu nous appuierons notre relfexion sur les travaux de l'ANSSI → | | | | | | Guide ANSSI pour choisir des pare feux | | | | |
| Solution mono-éditeur ou multi-éditeurs ? | Une solution mono éditeur est plus simple d'administration, une seule tecnologie en présence à connaitre et maitriser et est moins couteuse (entretien, formation, temps), mais plus faillible. | | | | | | | | | |
| | Une solution multi éditeurs est complexe à administrer car elle nécessité la connaissance et le savoir faire de deux technologie différente et est plus couteuse (entretien, formation, temps)mais est bien moins faillible | | | | | | | | | |

Selon nos critères nous avons donc choisi pfsense.

### 2. Choix de la solution pour l'intranet

Ensuite nous avons choisi notre solution pour héberger notre intranet avec un annuaire, une gestion de mail, des prises de notes, un agenda et une gestion de fichiers. Pour cela nous avons choisi plusieurs critères :

| | Fonctionnalités de partage de fichiers | Fonctionnalités de collaboration (édition de documents en temps réel) | Fonctionnalités de gestion de tâches | Fonctionnalités de calendrier et d'agenda | Fonctionnalités de gestion de contacts | Interface utilisateur | Sécurité (chiffrement des données, protection contre les attaques) | Facilité d'installation et de configuration | Support technique | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| Pondération | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | |
| Nextcloud | 5 | 4 | 3 | 4 | 4 | 4 | 5 | 4 | 4 | 37 |
| Zimbra | 3 | 3 | 4 | 5 | 5 | 3 | 4 | 3 | 4 | 34 |

Pour le serveur Active Directory nous avons pris serveur Windows 2019.

Pour tout mettre en place nous avons utilisé Proxmox.

## 3. Proxmox

Nous avons un serveur Proxmox avec les caractéristiques suivantes :

32GB de ram

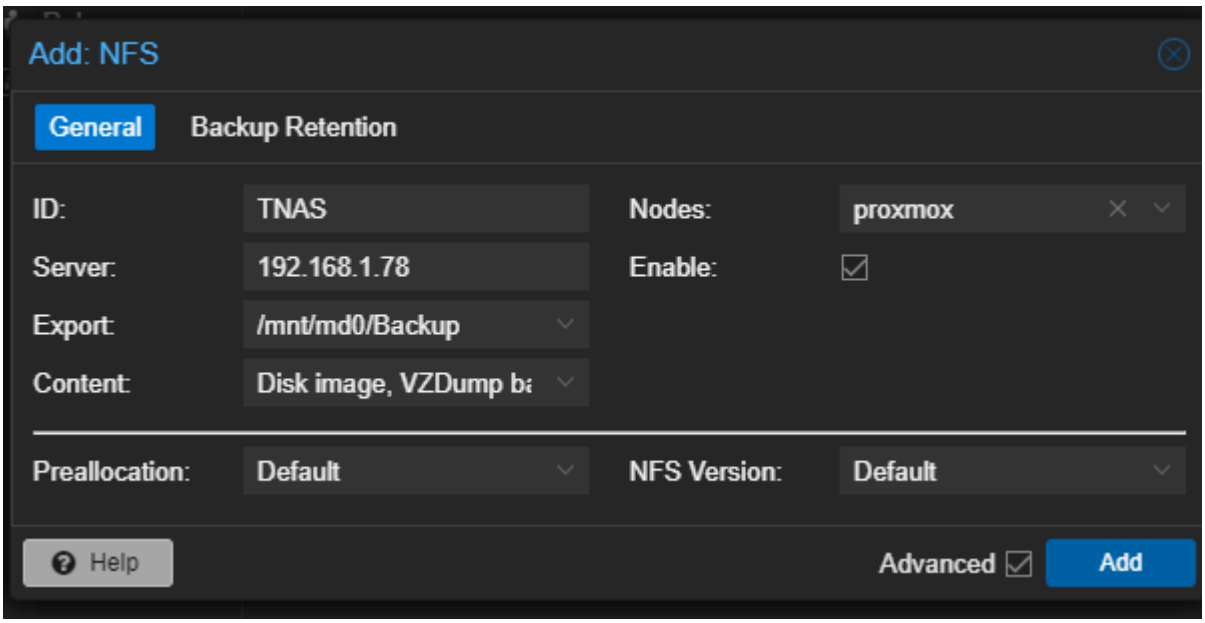
8 cœurs 16 processeurs logiques

1TB SSD m.2

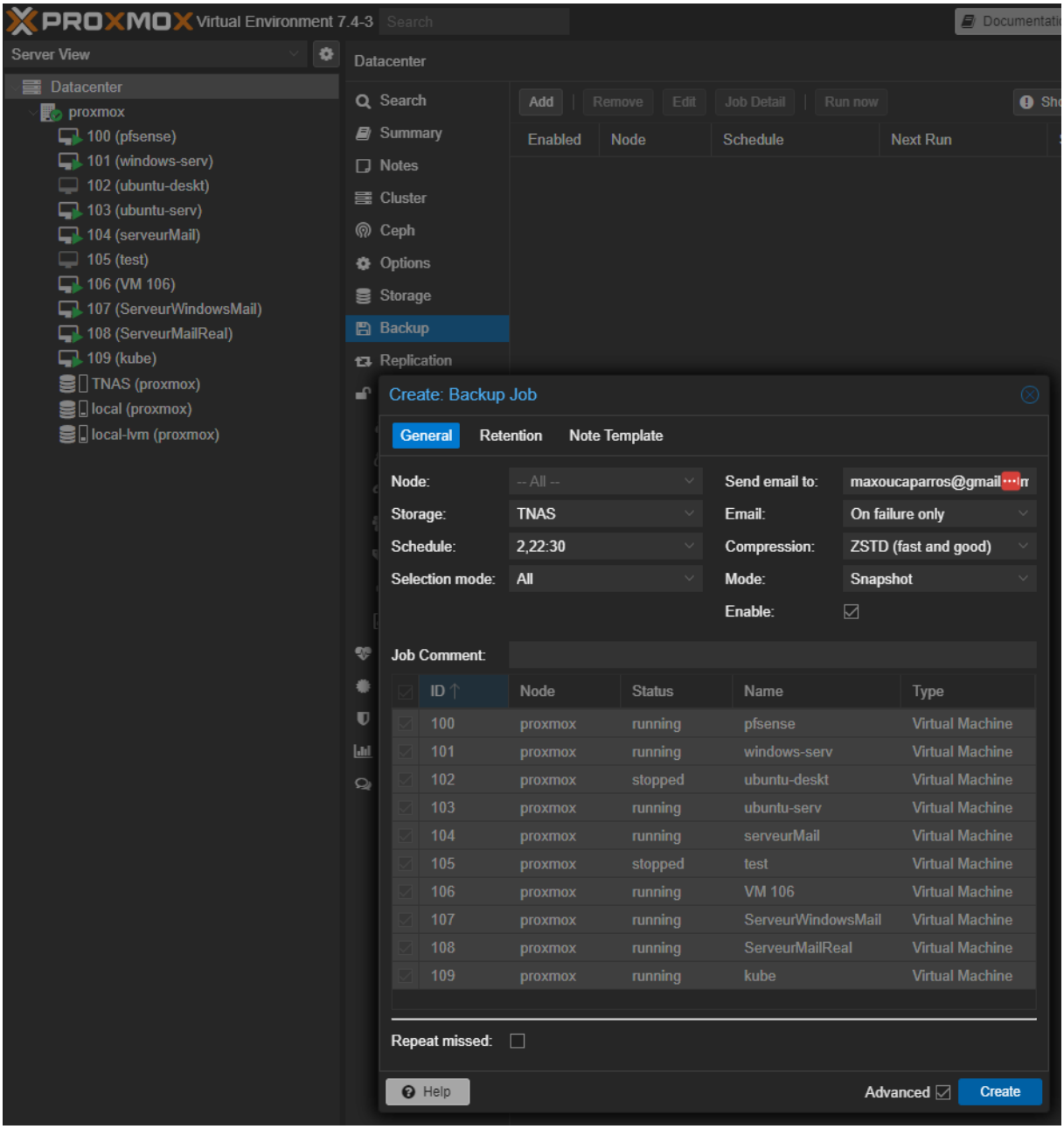
### 1. Backup

Nous avons mis en place un backup de toutes les VMs dans un NAS.

D'abord nous avons créé un dossier partagé avec le NAS.



On crée ensuite un backup de toutes les VM proxmox




Création d'une sauvegarde tous les jours à 2h30 et à 22h30 !

## 4. Mise en place du firewall

Pour mettre en place notre firewall nous avons choisi PFsense qui va nous servir de serveur VPN, de routeur et bien évidement de firewall.

### 1. Objectifs

Voici une liste des objectifs de notre politique de sécurité :

1. Bloquer les connexions entrantes non autorisées
2. Bloquer les connexions sortantes non autorisées
3. Contrôler les protocoles autorisés
4. Contrôler les adresses IP autorisées
5. Gérer les connexions VPN
6. Surveiller et analyser les logs

Le firewall doit être configurée pour mettre en place une politique de sécurité efficace et contrôler les flux de trafic réseau pour protéger les ressources internes de l'entreprise contre les attaques extérieures.

## 2. Configuration matérielle

Pour notre firewall nous l'avons mis en place sur Proxmox avec la configuration matérielle suivant :

1. 1 Processeur,
2. 1 cœur par processeur
3. 512 mb de ram
4. 4 cartes réseau
5. 5GB de disque virtuel en SCSI

## 3. Configuration logicielle

Configuration logicielle : Décrivez la version de pfSense utilisée et comment elle a été installée sur le matériel. Précisez également les packages additionnels installés.

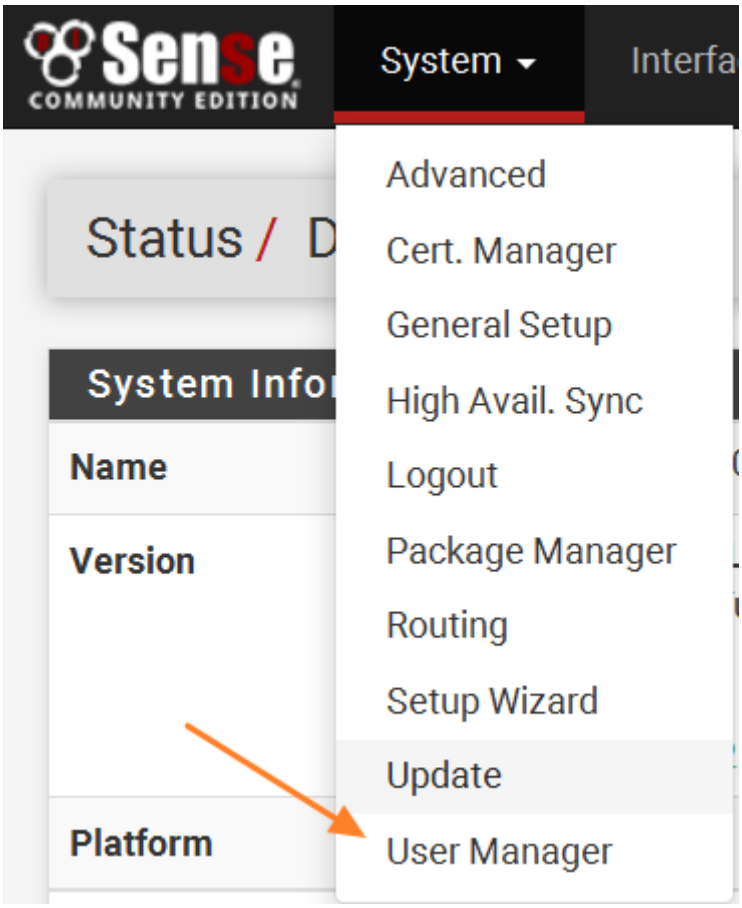
La mise en place du serveur pfsense s'est effectué via une image ISO de pfsense sur l'outil de virtualisation Proxmox.

### 1. Configuration du LDAP

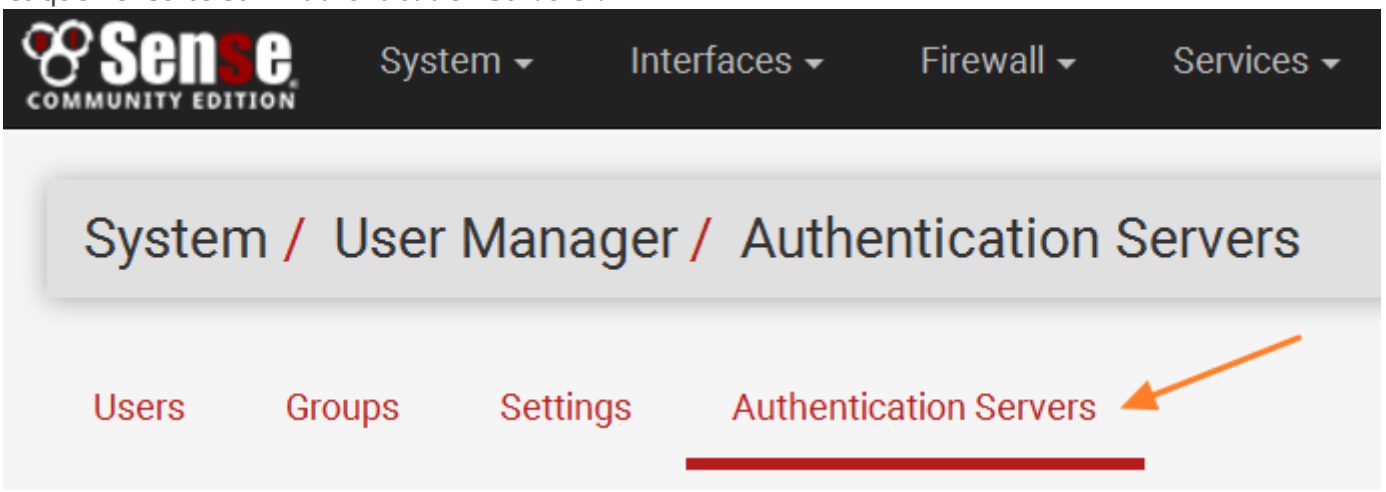
#### *1.1 Déclarer l'annuaire Active Directory sur pfSense*

Se connecter au WebGUI du pfSense avec un compte administrateur.

Cliquez sur le bouton "System" puis "User Manager" qui permet de gérer les utilisateurs et les groupes pfSense, ainsi que de configurer un serveur d'authentification.



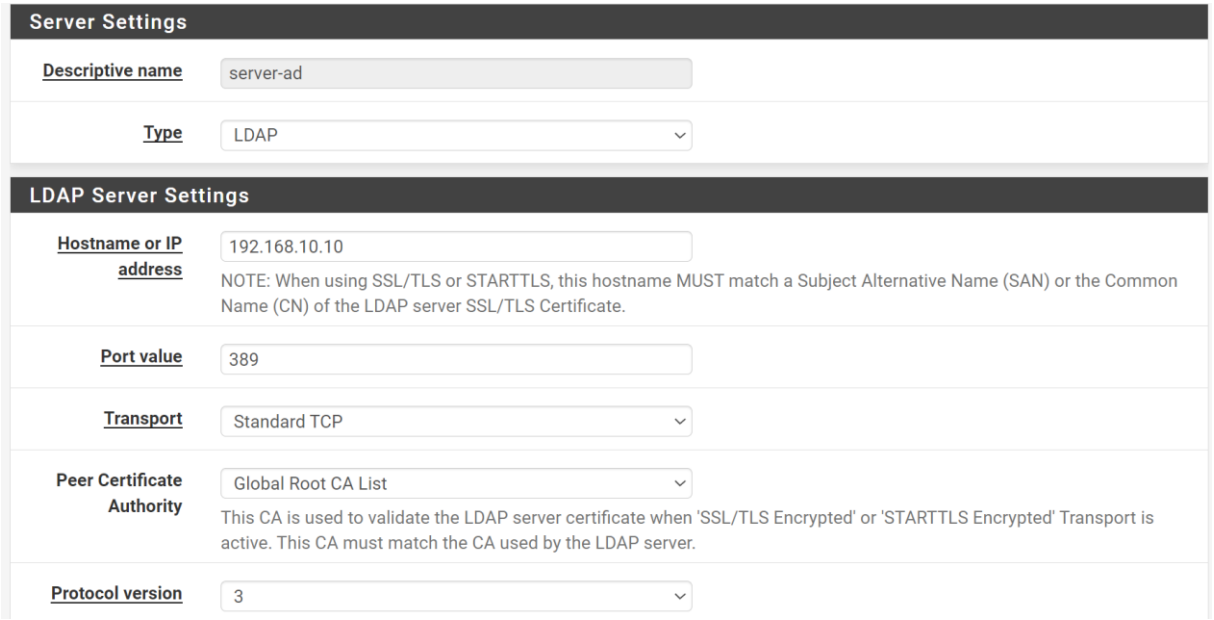

Cliquez ensuite sur "*Authentication Servers*".




Les trois copies d'écran qui suivent font partie de la même page de configuration. Tous les paramètres n'ont pas besoin d'être modifiés.

- **Descriptive name** : Indiquez un nom pour ce serveur.
- **Type** : Indiquez "LDAP" qui est le choix par défaut de pfSense.
- **Hostname or IP address** : Indiquez l'IP

C'est tout pour cette première partie.



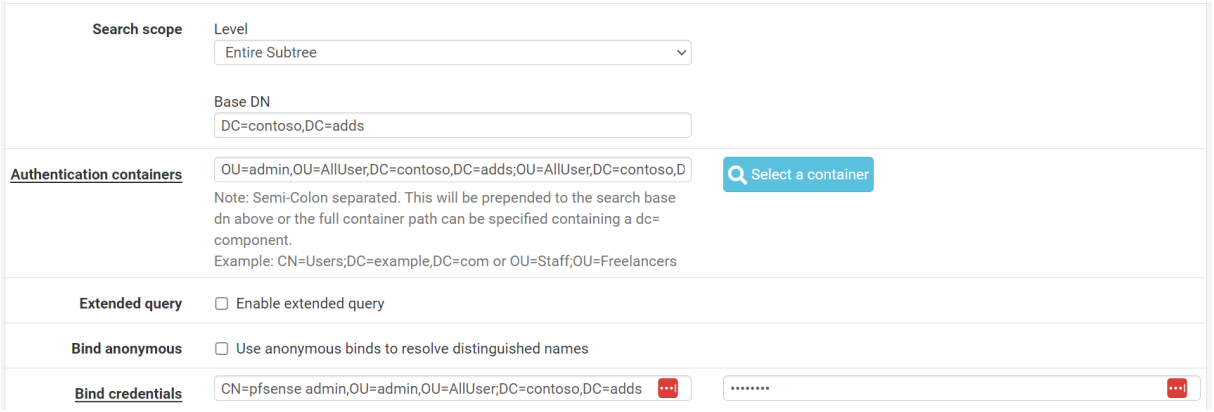

Voici la suite du paramétrage :

- **Search Scope** : Laissez "*Entire Subtree*" pour le scope de recherche, puis pour la "Base DN" indiquez la racine de votre AD.
- **Authentication containers** : Indiquez une ou plusieurs OU dans lesquelles pfSense peut regarder pour trouver les utilisateurs qui tentent de se connecter.

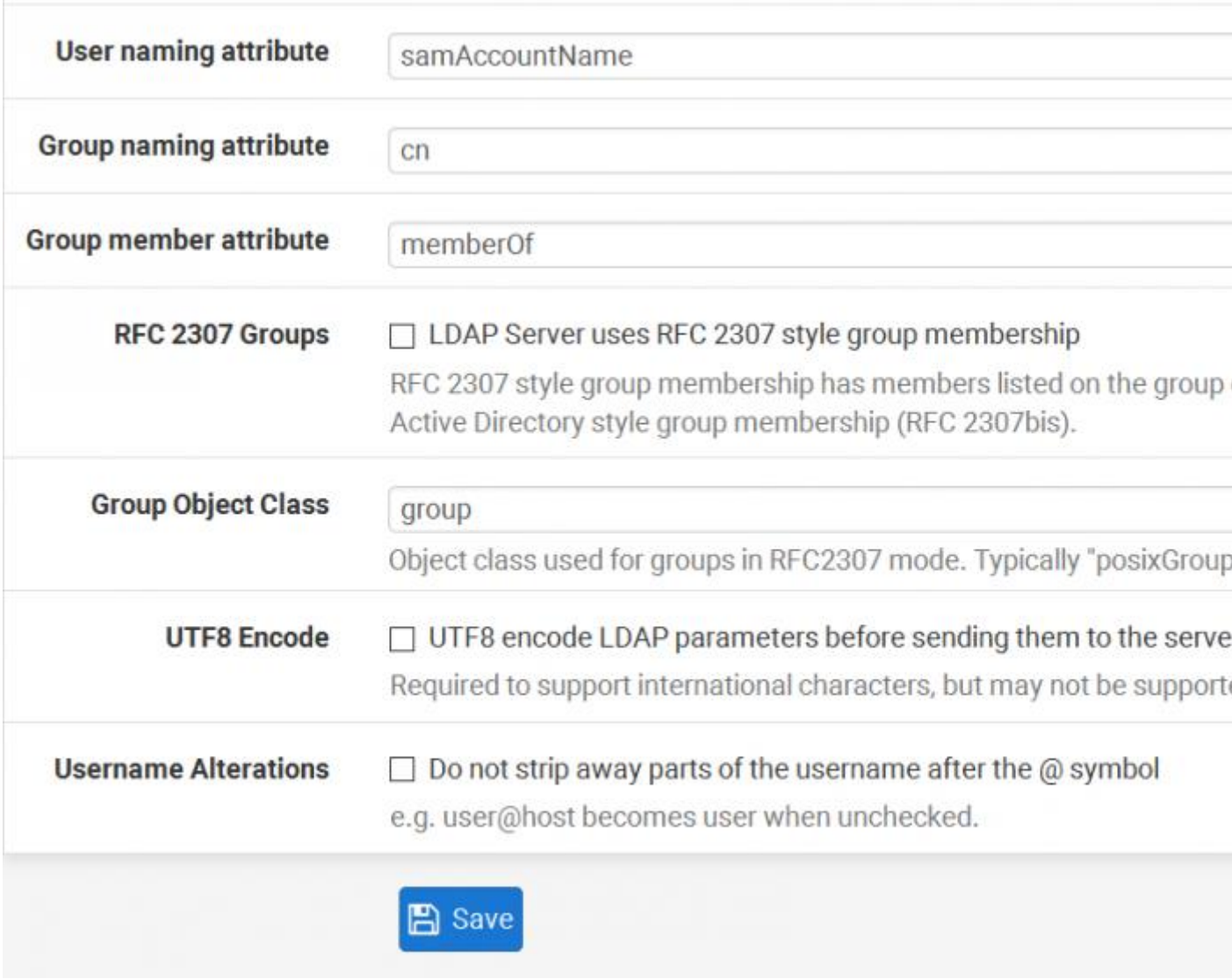
Ensuite décochez l'option de "*Bind anonymous*" on va plutôt s'authentifier pour requête l'AD. Au préalable, nous avons créé un compte pfsenseadmin pour pouvoir s'identifier avec.
Pour récupérer le DN de l'utilisateur on tape la commande suivante en powershell sur notre serveur AD :

```
(get-aduser -filter 'samaccountname -eq "pfsense.connect"').DistinguishedName
```

Copiez ensuite la valeur retournée dans le champ "*Bind credentials*" de la conf pfSense, puis sur le champ juste à droite indiquez le mot de passe associé à ce compte.



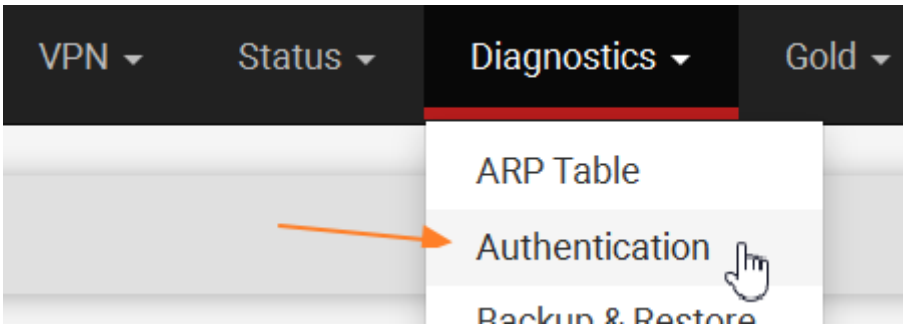
Vous pouvez seulement indiquer "*group*" à la place de "*posixGroup*", et veillez à ne pas cocher l'option "*LDAP Server uses RFC 2307 style group membership*" sinon pfSense ne pourra pas récupérer le nom du groupe auquel appartient votre utilisateur.



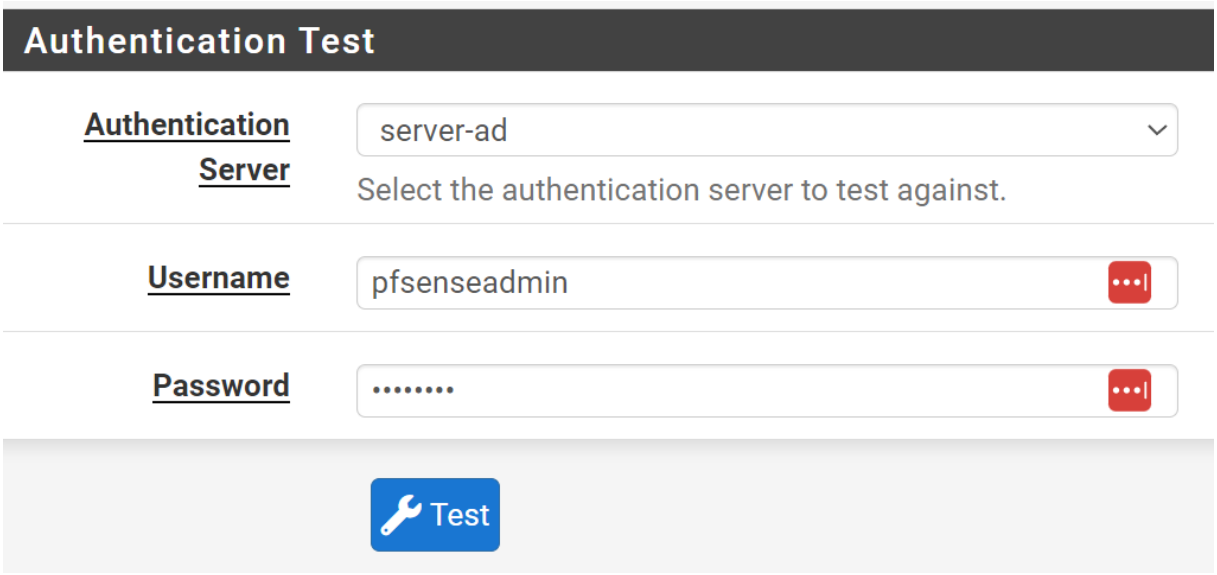

Sauvegardez la configuration avec le bouton "Save".

### *1.2 Tester l'authentification AD*

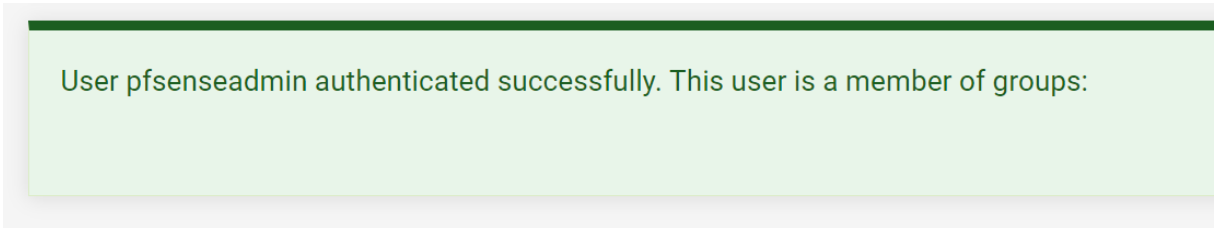
Dans le menu "*Diagnostics*", cliquez sur "*Authentication*".




Choisissez votre AD comme serveur d'authentification puis tester un login et un mot de passe qui est censé fonctionner.




Cliquez sur "Test", si tout est OK vous devriez obtenir ce message :




### *1.3 Déclarer le groupe local dans pfSense*

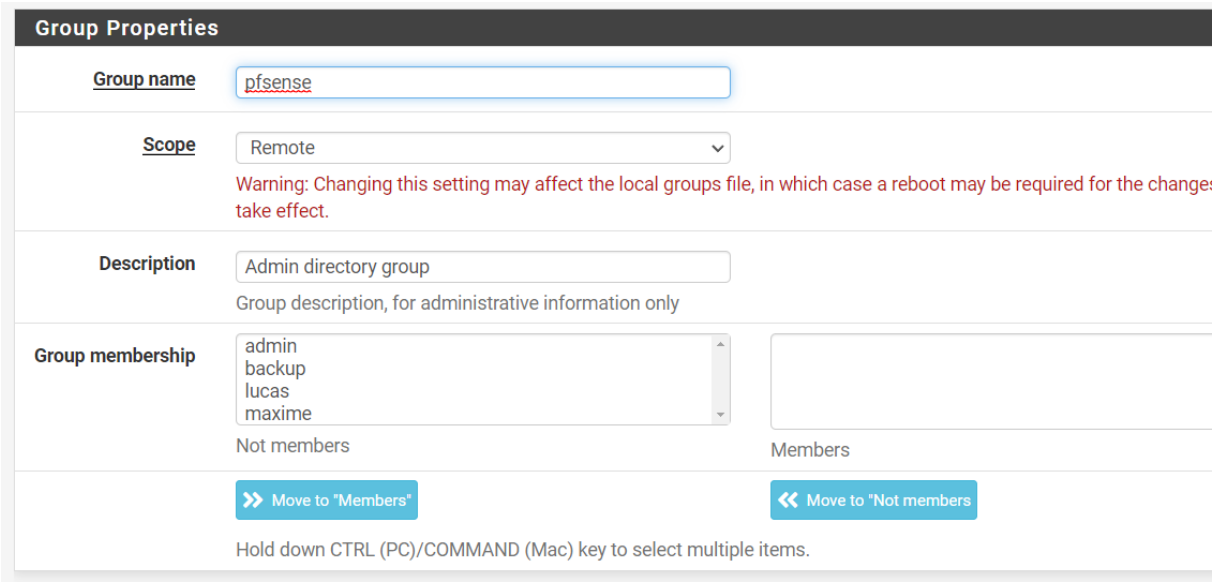
Il faut créer un groupe local qui aura le même nom que le groupe Active directory

Dans System, User Manager, accédez à l'onglet "Groups" et cliquez sur "Add".


Nommez le groupe comme celui de l'AD, donc dans notre cas on note pfsense.

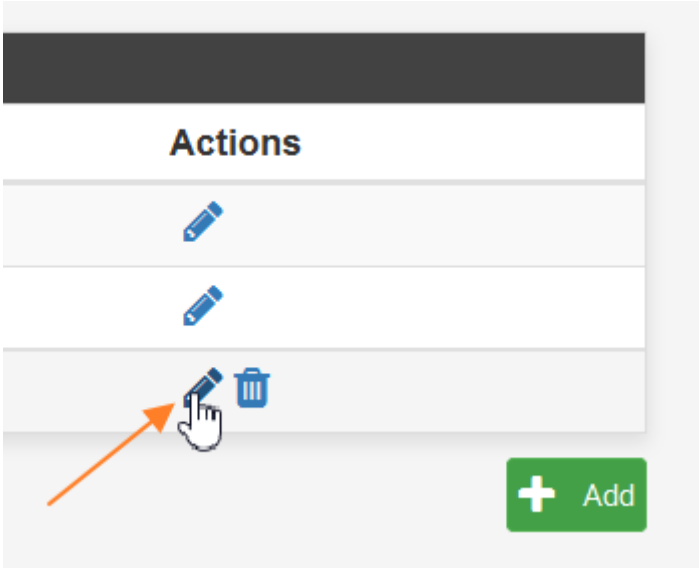
Pour le scope on choisit Remote.

Et on sauvegarde



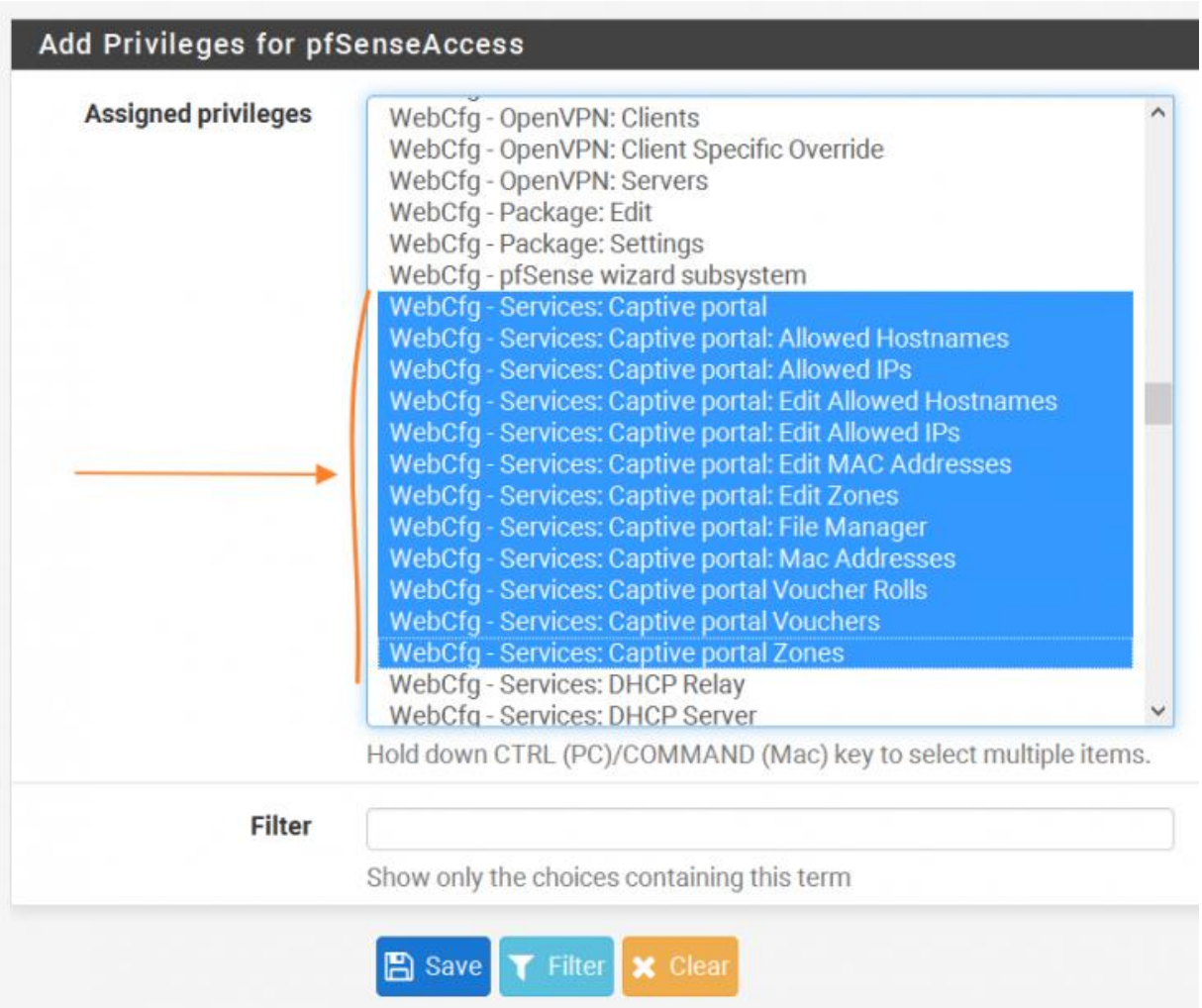

*1.4 Attribution des droits au groupe local*

Toujours dans la gestion des groupes, cliquez sur l'icône en forme de crayon pour éditer le groupe fraîchement créé.




Descendez au niveau de la section "Assigned Privileges" et cliquez sur "Add".

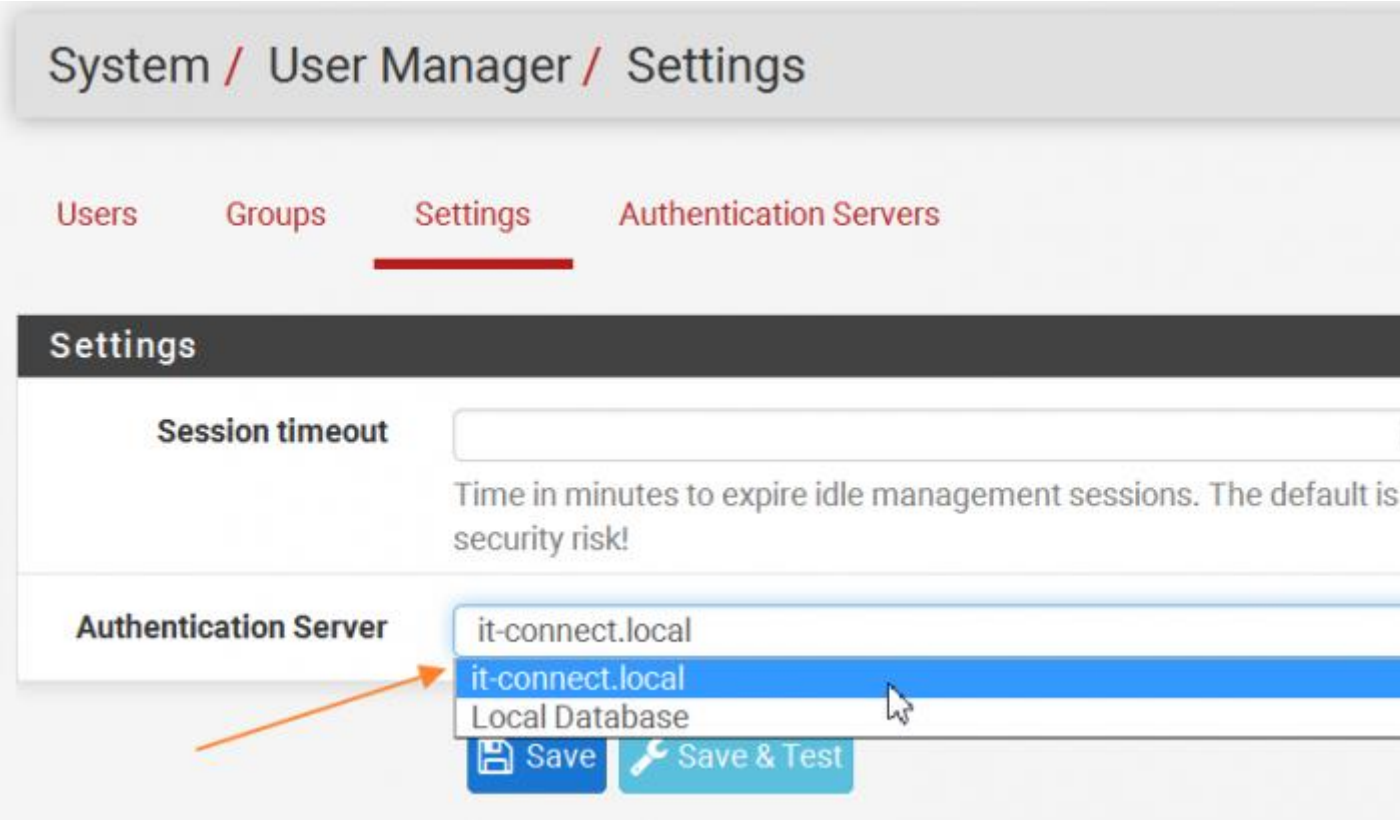

Ensuite, toute la liste des privilèges apparaît, voici ce qu'il faut sélectionner :




On aurait pu ajouter d'autres privilèges pour accéder à la partie log du portail captif. Cliquez sur "Save" dès lors que votre sélection est effectuée.

### *1.5 Définir notre serveur AD pour l'authentification*

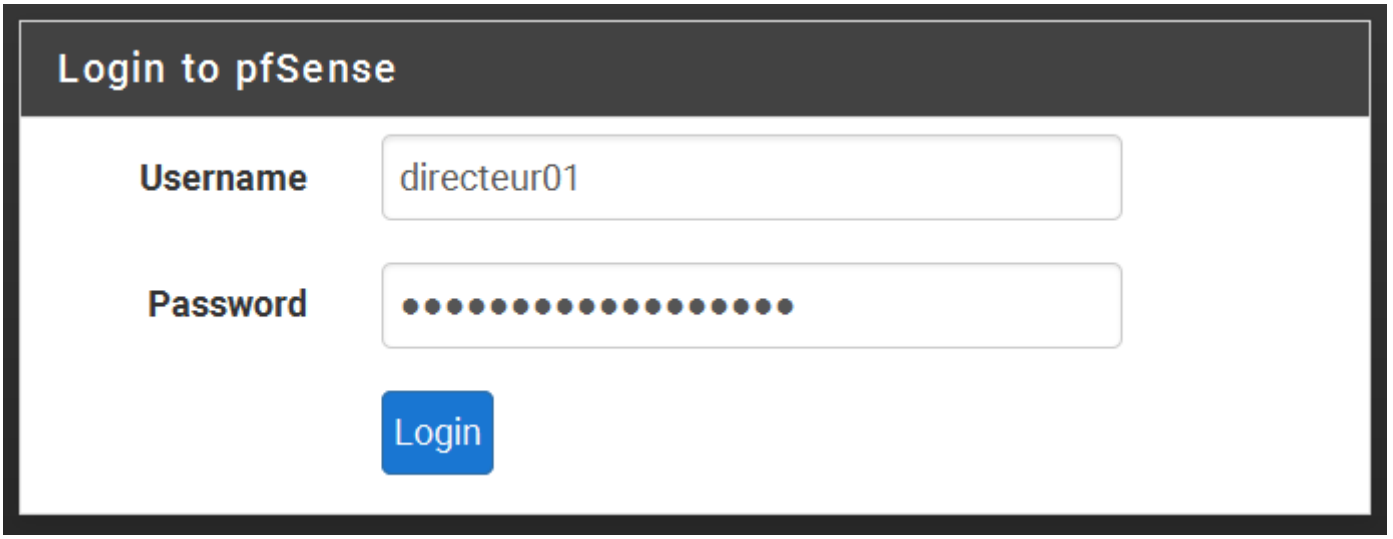
Cette étape de la configuration est indispensable sinon la connexion à pfSense s'appuiera sur la base locale et non sur l'AD. Toujours dans System / User Manager / Settings, définissez l'AD. Puis, sauvegardez.




Cette étape est déjà terminée, maintenant il va falloir tester cette config.

### *1.6 Tester la connexion à la WebGUI pfSense avec un compte AD*

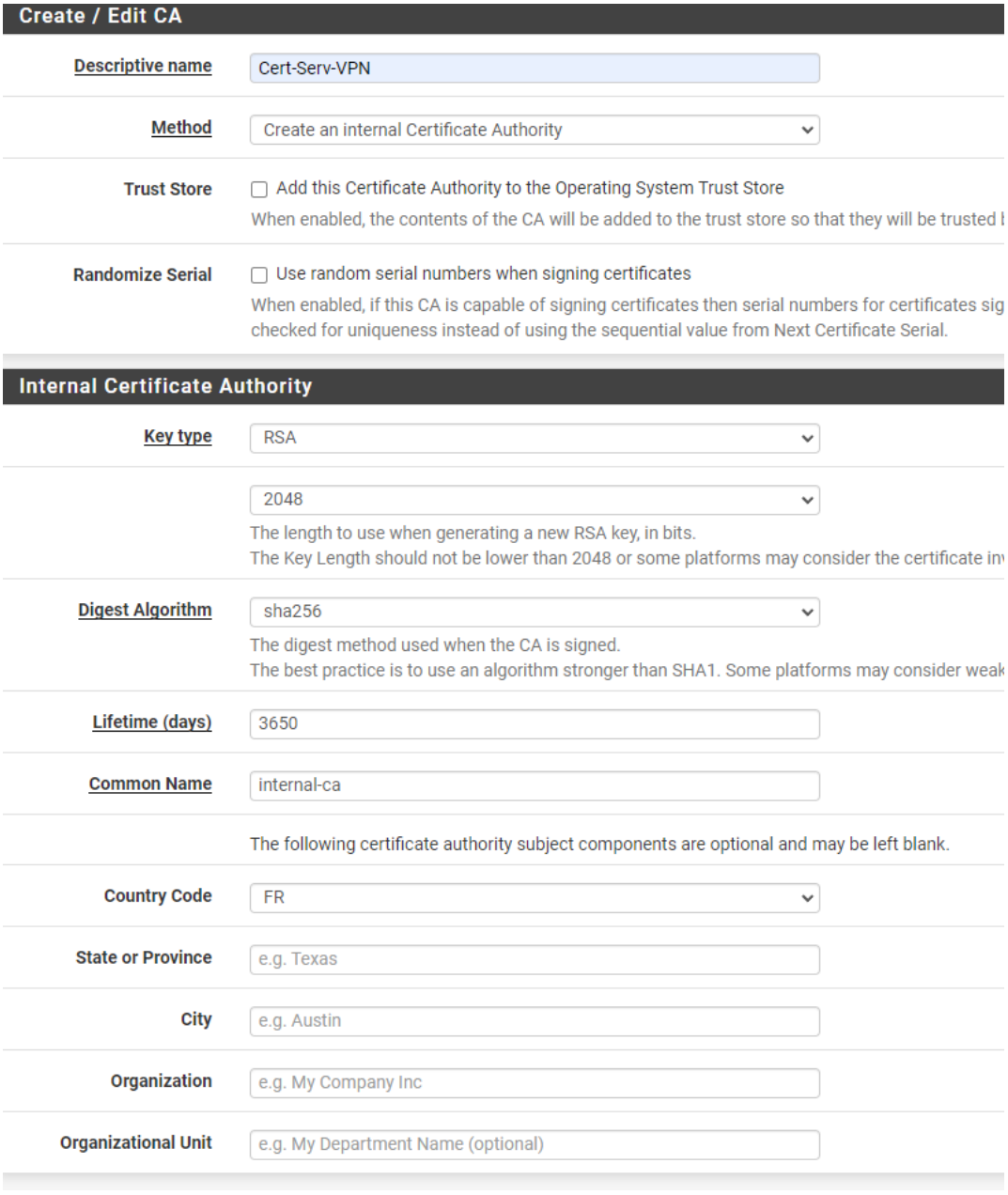
Ouvrez un navigateur et accédez à la page de connexion de pfSense. Ensuite, tentez de vous connecter avec un compte AD :



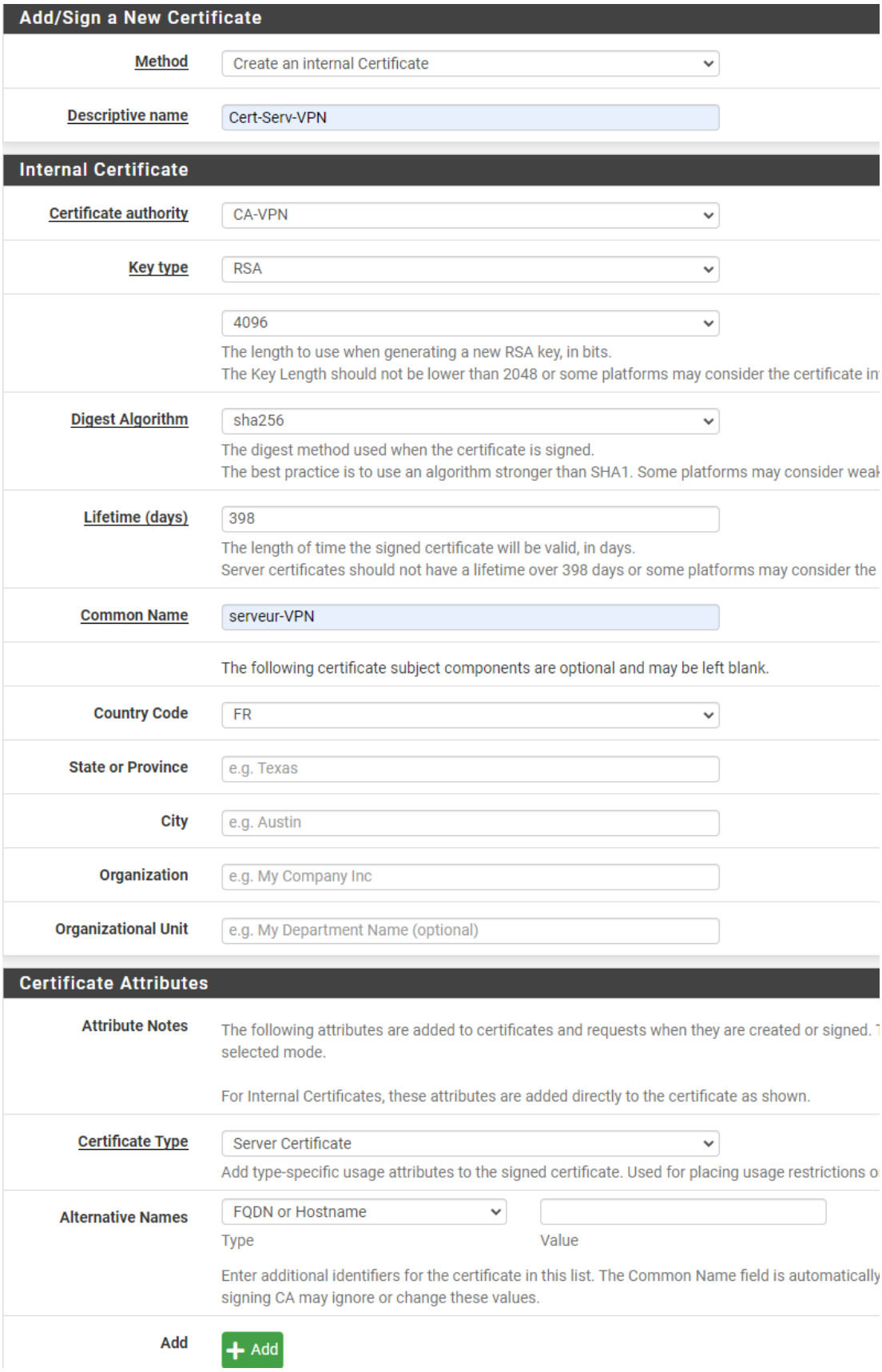
## 2. OpenVPN

### *2.1 Certificat d'autorité*

On crée un certificat d'autorité pour créer nos certificats de serveurs et d'utilisateurs.

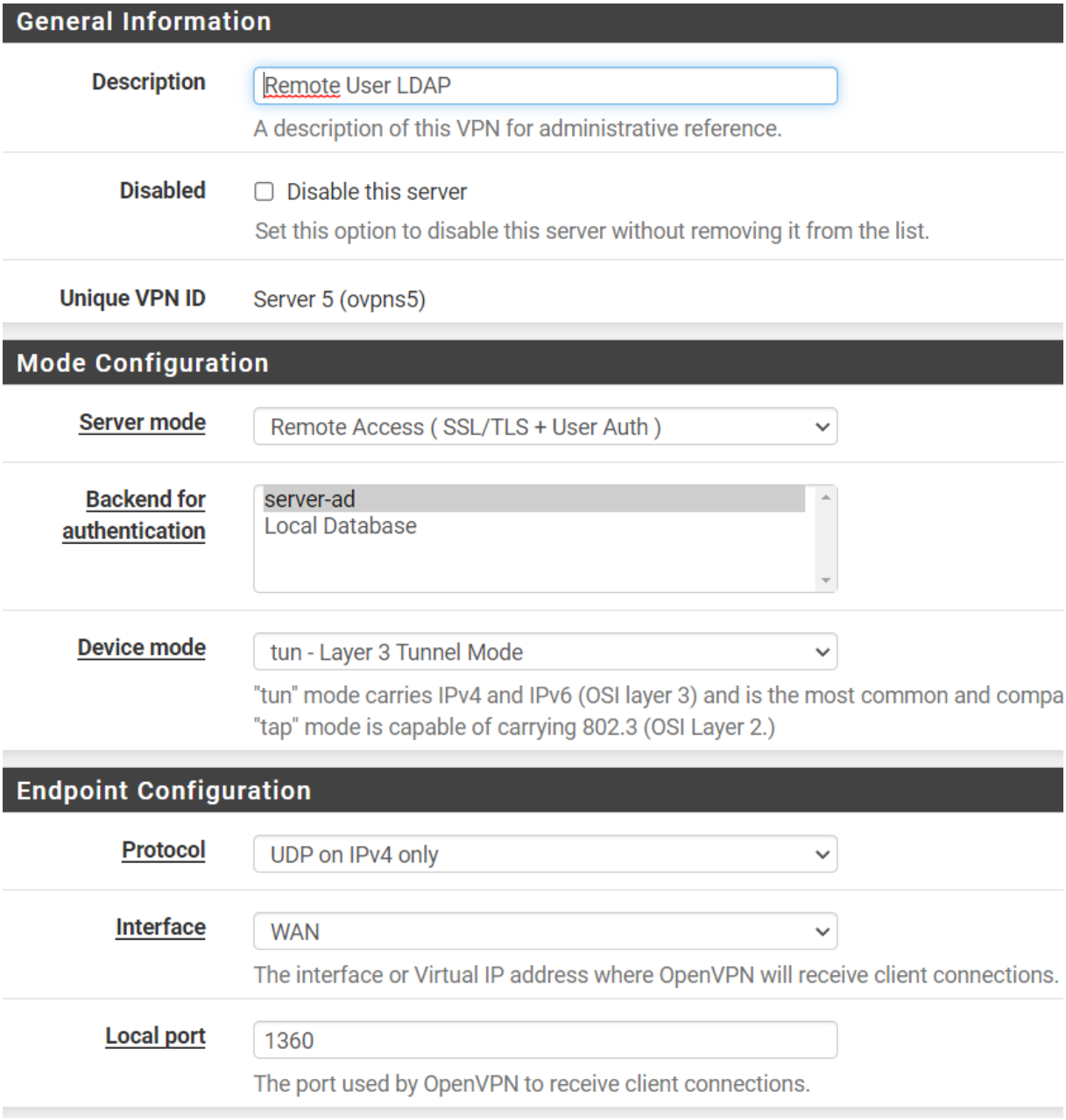



### *2.2 Certificat de serveur*




*2.3 Serveur VPN*

Le serveur VPN va utiliser la base de données server-AD qui est notre base de données AD. On utilise donc l'authentification par User Auth. On utilise aussi le port local 1360 pour faire passer les requêtes



**Server certificate**
Cert-Serv-User-VPN (Server: Yes, CA: CA-VPN)

**DH Parameter Length**
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.

**ECDH Curve**
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

**Data Encryption Negotiation**
Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

**Data Encryption Algorithms**

| Available | Allowed |
|---|---|
| AES-128-CBC (128 bit key, 128 bit block)<br>AES-128-CFB (128 bit key, 128 bit block)<br>AES-128-CFB1 (128 bit key, 128 bit block)<br>AES-128-CFB8 (128 bit key, 128 bit block)<br>AES-128-GCM (128 bit key, 128 bit block)<br>AES-128-OFB (128 bit key, 128 bit block)<br>AES-192-CBC (192 bit key, 128 bit block)<br>AES-192-CFB (192 bit key, 128 bit block)<br>AES-192-CFB1 (192 bit key, 128 bit block)<br>AES-192-CFB8 (192 bit key, 128 bit block) | AES-256-GCM<br>AES-128-GCM<br>CHACHA20-POLY1305 |

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

**Fallback Data Encryption Algorithm**
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

**Auth digest algorithm**
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

**Hardware Crypto**
No Hardware Crypto Acceleration

**Certificate Depth**
One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

**Strict User-CN Matching**
Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

**Client Certificate Key Usage Validation**
Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

## Tunnel Settings

**IPv4 Tunnel Network**
10.0.8.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

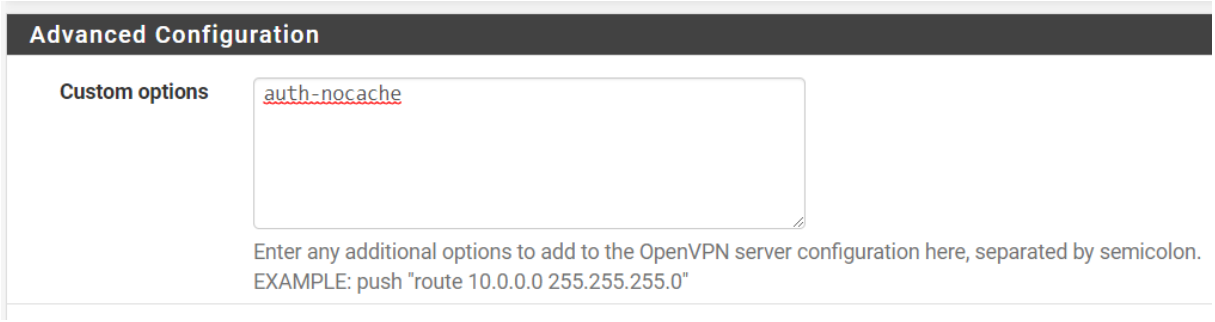
| | |
|---|---|
| **IPv4 Local network(s)** | 192.168.99.0/24<br>IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list type aliases. This may be left blank if not adding a route to the local network through this tunnel on the LAN network. |
| **IPv6 Local network(s)** | IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list aliases. This may be left blank if not adding a route to the local network through this tunnel on the rem network. |
| **Concurrent connections** | Specify the maximum number of clients allowed to concurrently connect to this server. |
| **Allow Compression** | Refuse any non-stub compression (Most secure)<br>Allow compression to be used with this VPN instance.<br>Compression can potentially increase throughput but may allow an attacker to extract secrets if they c VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME the use case for this specific VPN is vulnerable to attack.<br><br>Asymmetric compression allows an easier transition when connecting with older peers. |
| **Push Compression** | ☐ Push the selected Compression setting to connecting clients. |
| **Type-of-Service** | ☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value. |
| **Inter-client communication** | ☐ Allow communication between clients connected to this server |
| **Duplicate Connection** | ☐ Allow multiple concurrent connections from the same user<br>When set, the same user may connect multiple times. When unset, a new connection from a user will<br><br>Users are identified by their username or certificate properties, depending on the VPN configuration. T may be necessary in some environments. |

## Client Settings

| | |
|---|---|
| **Dynamic IP** | ☐ Allow connected clients to retain their connections if their IP address changes. |
| **Topology** | net30 -- Isolated /30 network per client<br>Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on I Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Androi clients such as Yealink phones may require "net30". |

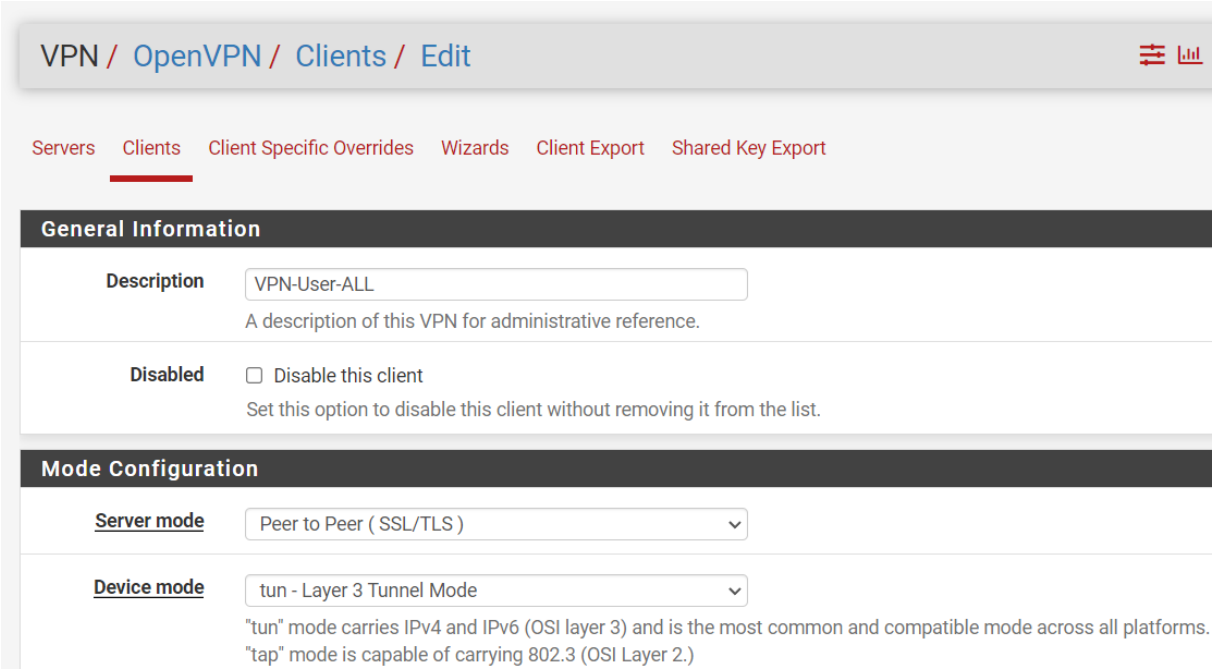
## Ping settings

| | |
|---|---|
| **Inactive** | 300<br>Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet.<br>A value of 0 disables this feature.<br>This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunn not restart. |




### *2.4 Création du VPN Client*

Nous allons créer un VPN client pour tous nos users.



## Endpoint Configuration

**Protocol**: UDP on IPv4 only

**Interface**: WAN

The interface used by the firewall to originate this OpenVPN client connection

**Local port**:

Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic por

**Server host or address**: pfsense.maxcaptab.com

The IP address or hostname of the OpenVPN server.

**Server port**: 1360

The port used by the server to receive client connections.

**Proxy host or address**:

The address for an HTTP Proxy this client can use to connect to a remote server.
TCP must be used for the client and server protocol.

**Proxy port**:

**Proxy Authentication**: none

The type of authentication used by the proxy server.

## Cryptographic Settings

**TLS Configuration**: ☑ Use a TLS Key

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

☑ Automatically generate a TLS Key.

**TLS keydir direction**: Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

**Peer Certificate Authority**: CA-VPN

**Peer Certificate Revocation list**: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation

**Client Certificate**: Cert-Serv-User-VPN (Server: Yes, CA: CA-VPN)

**Data Encryption Negotiation**: ☑ Enable Data Encryption Negotiation

This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

**Data Encryption Algorithms**

| Available Data Encryption Algorithms | Allowed Data Encryption Algorithms |
| --- | --- |
| AES-128-CBC (128 bit key, 128 bit block)<br>AES-128-CFB (128 bit key, 128 bit block)<br>AES-128-CFB1 (128 bit key, 128 bit block)<br>AES-128-CFB8 (128 bit key, 128 bit block)<br>AES-128-GCM (128 bit key, 128 bit block)<br>AES-128-OFB (128 bit key, 128 bit block)<br>AES-192-CBC (192 bit key, 128 bit block)<br>AES-192-CFB (192 bit key, 128 bit block)<br>AES-192-CFB1 (192 bit key, 128 bit block)<br>AES-192-CFB8 (192 bit key, 128 bit block) | AES-256-GCM<br>AES-128-GCM<br>CHACHA20-POLY1305 |
| Click to add or remove an algorithm from the list | Click an algorithm name to remove it from the list |

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

**Fallback Data Encryption Algorithm**

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

**Auth digest algorithm**

SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

**Hardware Crypto**

No Hardware Crypto Acceleration

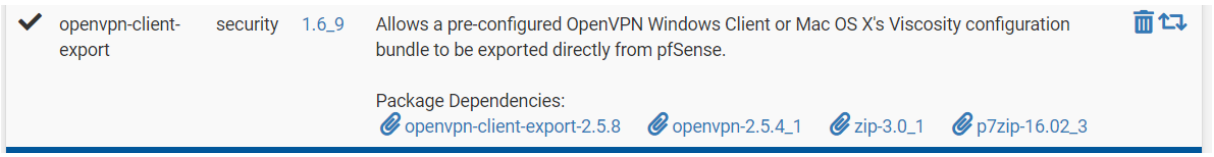
**Server Certificate Key Usage Validation**

☑ Enforce key usage

Verify that remote host uses a server certificate (EKU: "TLS Web Server Authentication").

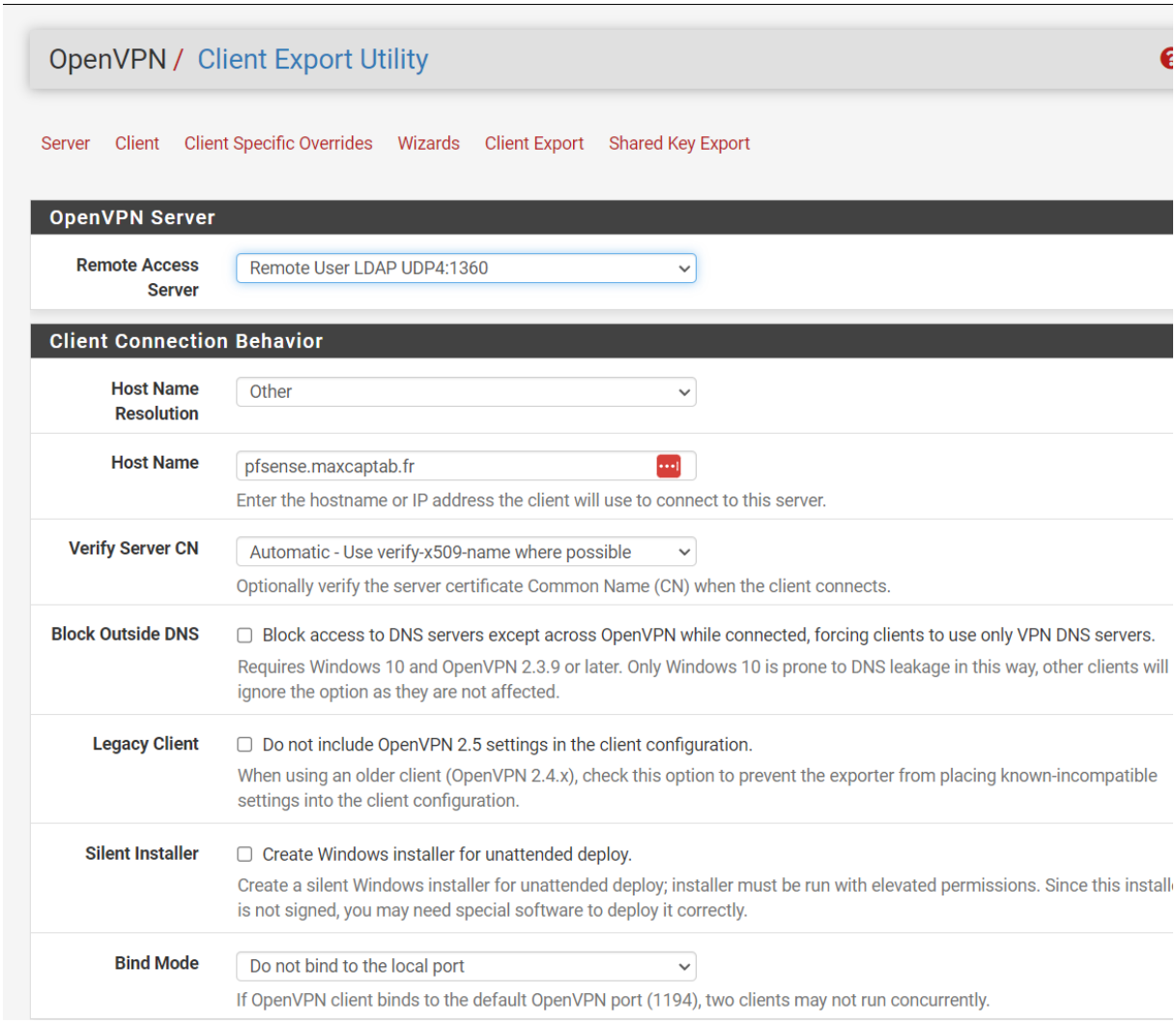

## *2.5 Exporter notre configuration vpn*

Il faut d'abord installer le package suivant :

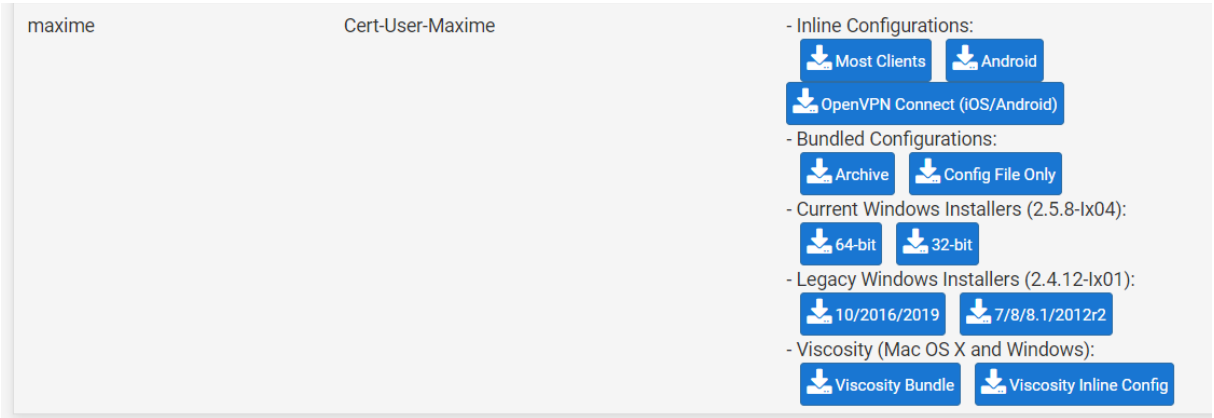


Ce package va nous permettre d'exporter notre configuration pour le VPN.

Ensuite nous allons dans OpenVPN puis dans Client Export.




Puis on export le certificat

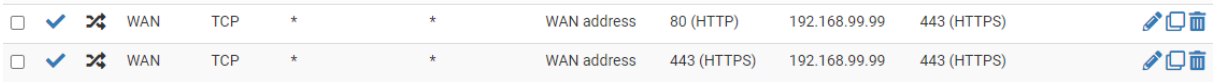


# 4. Politique de sécurité

## 1. Configuration des règles

### *1.1 Règle NAT*

Pour nos règles on va rediriger les requêtes http et https du port Wan vers notre serveur web avec des règles NAT :

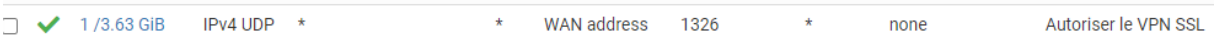


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| WAN | TCP | * | * | WAN address | 80 (HTTP) | 192.168.99.99 | 443 (HTTPS) | |
| WAN | TCP | * | * | WAN address | 443 (HTTPS) | 192.168.99.99 | 443 (HTTPS) | |

On fait cela pour recevoir les certificats SSL pour notre serveur web.

### *1.2 Règle WAN*

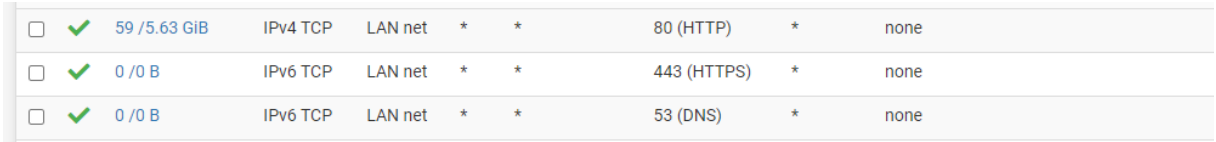
Ensuite nous avons fait une règle pour autoriser le VPN SSL du coté de notre Wan :



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 /3.63 GiB | IPv4 UDP | * | * | WAN address | 1326 | * | none | Autoriser le VPN SSL |

### *1.3 Règle LAN*

Pour les règles LAN on autorise les requêtes http, https et dns pour internet.



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 59 /5.63 GiB | IPv4 TCP | LAN net | * | * | 80 (HTTP) | * | none | |
| 0 /0 B | IPv6 TCP | LAN net | * | * | 443 (HTTPS) | * | none | |
| 0 /0 B | IPv6 TCP | LAN net | * | * | 53 (DNS) | * | none | |

### *1.4 Règle Lan-DMZ*

Pour les règles Lan-DMZ on fait passer les requêtes pour le serveur mail et aussi les requêtes pour Internet.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0 /38 KiB | IPv4 TCP | 192.168.99.99 | * | * | 587 (SUBMISSION) | * | none | | |
| | 0 /0 B | IPv4 TCP | * | * | 192.168.10.100 | 25 (SMTP) | * | none | | SMPT |
| | 0 /0 B | IPv4 TCP | * | * | 192.168.10.100 | 995 (POP3/S) | * | none | | POP3 TLS |
| | 0 /0 B | IPv4 TCP | * | * | 192.168.99.100 | 993 (IMAP/S) | * | none | | IMAP TLS |
| | 0 /0 B | IPv4 TCP | * | * | 192.168.99.100 | 143 (IMAP) | * | none | | IMAP |
| | 0 /40.90 MiB | IPv4 TCP | LANDMZ net | * | 192.168.10.10 | 389 (LDAP) | * | none | | |
| | 0 /1012.75 MiB | IPv4 TCP/UDP | LANDMZ net | * | * | 443 (HTTPS) | * | none | | |
| | 0 /776.60 MiB | IPv4 TCP/UDP | LANDMZ net | * | * | 80 (HTTP) | * | none | | |
| | 0 /2.98 MiB | IPv4 TCP/UDP | LANDMZ net | * | * | 53 (DNS) | * | none | | |

### *1.5 Règle VPN*

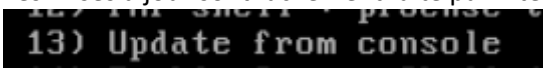
On autorise le réseau 10.0.1.0/24 à accéder aux autres pcs en ssh ou en rdp. Il aura aussi accès à l'interface web de pfsense. Le reste ne pourra seulement avoir accès aux services web de notre serveur web.

**Rules (Drag to Change Order)**

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2 /605 KiB | IPv4 TCP | 10.0.1.0/24 | * | LAN address | 443 (HTTPS) | * | none | | | |
| | 6 /44.24 MiB | IPv4 TCP | * | * | 192.168.99.99 | 9443 | * | none | | | |
| | 2 /193.39 MiB | IPv4 TCP | * | * | 192.168.99.99 | 443 (HTTPS) | * | none | | | |
| | 2 /7.80 MiB | IPv4 TCP | 10.0.1.0/24 | * | 192.168.99.99 | 22 (SSH) | * | none | | | |
| | 0 /0 B | IPv4 TCP | 10.0.1.0/24 | * | 192.168.99.110 | 22 (SSH) | * | none | | | |
| | 0 /0 B | IPv4 TCP | 10.0.1.0/24 | * | 192.168.99.120 | 22 (SSH) | * | none | | | |
| | 0 /2.17 MiB | IPv4 TCP | 10.0.1.0/24 | * | 192.168.99.120 | 9000 | * | none | | | |
| | 0 /0 B | IPv4 TCP | 10.0.1.0/24 | * | LAN net | 3389 (MS RDP) | * | none | | | |

## 5. Gestion des mises à jour

Les mises à jour sont facilement faite par interface web ou alors par ssh :




## 6. Gestion des accès

Nous utilisons des mots de passes forts pour les comptes administratifs de pfsense.
Seuls les utilisateurs créés en local et les utilisateurs admin de l'AD avec le groupe pfsense ont accès à l'interfaces web.

# 5. Mise en place d'un serveur intranet

Pour la mise en place du serveur intranet nous avons choisi de mettre en place Nextcloud avec Authelia et Traefik.

## 1. Objectifs

Pour notre intranet nous avons besoins de plusieurs fonctionnalités :

- Stockage et partage de fichiers
- Collaboration en temps réel
- Accessibilité
- Sécurité :
- Gestion des tâches et des calendriers :
- Applications tierces

## 2. Configuration matérielle

Pour notre firewall nous l'avons mis en place sur Proxmox avec la configuration matérielle suivant :

2 Processeur,

1 cœur par processeur

4GB de ram

100GB de disque virtuel en SCSI

## 3. Configuration logicielle

Configuration logicielle : Décrivez la version de pfSense utilisée et comment elle a été installée sur le matériel. Précisez également les packages additionnels installés.

La mise en place du serveur pfsense s'est effectué via une image ISO de pfsense sur l'outil de virtualisation Proxmox.

### 1. Docker compose de traefik, authelia et nextcloud

*1.1 Docker compose*

Le docker compose se trouve dans /home/appdata

```
version: "3.8"

volumes:
  nextcloud:
  db:

secrets:
  JWT_SECRET:
    file: authelia/secrets/JWT_SECRET
  SESSION_SECRET:
    file: authelia/secrets/SESSION_SECRET
  STORAGE_PASSWORD:
    file: authelia/secrets/STORAGE_PASSWORD
  STORAGE_ENCRYPTION_KEY:
    file: authelia/secrets/STORAGE_ENCRYPTION_KEY
  PASSWORD:
    file: authelia/secrets/PASSWORD

networks:
  net:
    external: true
    name: nextcloud

services:
   db:
    image: mariadb:10.6
    restart: always
    command: --transaction-isolation=READ-COMMITTED --log-bin=binlog --binlog-
format=ROW
    networks:
      net: {}
    volumes:
      - db:/var/lib/mysql
    environment:
      - MYSQL_ROOT_PASSWORD=***
      - MYSQL_PASSWORD=***
      - MYSQL_DATABASE=nextcloud
      - MYSQL_DATABASE=authelia
      - MYSQL_USER=nextcloud

  app:
    image: nextcloud
    restart: always
    links:
      - db
```

```
    networks:
      net: {}
    volumes:
      - nextcloud:/var/www/html/
    environment:
      - MYSQL_PASSWORD=***
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud
      - MYSQL_HOST=db
      - NEXTCLOUD_URL=nextcloud.maxcaptab.fr
    labels:
      - 'traefik.enable=true'
      #- 'traefik.http.routers.test-
redirectscheme.redirectscheme.scheme=https'
      #- 'traefik.http.routers.test-
redirectscheme.redirectscheme.permanent=true'
      - 'traefik.http.routers.nextcloud.rule=Host(`nextcloud.maxcaptab.fr`)'
      - 'traefik.http.routers.nextcloud.entryPoints=https'
      - 'traefik.http.routers.nextcloud.tls=true'
      - 'traefik.http.routers.nextcloud.middlewares=authelia@docker'
      #- "traefik.http.routers.nextcloud.tls.certresolver=myresolver"

  authelia:
    container_name: authelia
    image: docker.io/authelia/authelia:latest
    restart: unless-stopped
    networks:
      net:
        aliases:
          - "auth.maxcaptab.fr"
    expose:
      - 9091
    secrets: [JWT_SECRET, SESSION_SECRET, STORAGE_PASSWORD,
STORAGE_ENCRYPTION_KEY]
    environment:
      AUTHELIA_JWT_SECRET_FILE: /run/secrets/JWT_SECRET
      AUTHELIA_SESSION_SECRET_FILE: /run/secrets/SESSION_SECRET
      AUTHELIA_STORAGE_ENCRYPTION_KEY_FILE:
/run/secrets/STORAGE_ENCRYPTION_KEY
    volumes:
      - ./authelia/config:/config
    labels:
      - 'traefik.enable=true'

      - 'traefik.http.routers.authelia.rule=Host(`auth.maxcaptab.fr`)'
      - 'traefik.http.routers.authelia.entryPoints=https'
      - 'traefik.http.routers.authelia.tls=true'
      #- traefik.http.routers.authelia-insecure.entrypoints=web
      #- traefik.http.routers.authelia-insecure.rule=Host(`auth.maxcaptab.fr`)
```

```
      #- traefik.http.routers.authelia-insecure.middlewares=force-secure
      -
'traefik.http.middlewares.authelia.forwardAuth.address=http://authelia:9091/ap
i/verify?rd=https%3A%2F%2Fauth.maxcaptab.fr%2F'
      -
'traefik.http.middlewares.authelia.forwardAuth.trustForwardHeader=true'
      -
'traefik.http.middlewares.authelia.forwardAuth.authResponseHeaders=Remote-
User,Remote-Groups,Remote-Name,Remote-Email'
      - 'traefik.http.middlewares.authelia-
basic.forwardAuth.address=http://authelia:9091/api/verify?auth=basic'
      - 'traefik.http.middlewares.authelia-
basic.forwardAuth.trustForwardHeader=true'
      - 'traefik.http.middlewares.authelia-
basic.forwardAuth.authResponseHeaders=Remote-User,Remote-Groups,Remote-
Name,Remote-Email'
      #- "traefik.http.routers.authelia.tls.certresolver=myresolver"
  traefik:
    container_name: traefik
    image: traefik:v2.9
    restart: unless-stopped
    command:
      - '--api=true'
      - '--api.dashboard=true'
      - '--api.insecure=false'
      - '--pilot.dashboard=false'
      - '--global.sendAnonymousUsage=false'
      - '--global.checkNewVersion=false'
      - '--log=true'
      - '--log.level=DEBUG'
      - '--log.filepath=/config/traefik.log'
      - '--providers.docker=true'
      - '--providers.docker.exposedByDefault=false'
      - '--entryPoints.http=true'
      - '--entryPoints.http.http.redirections.entryPoint.to=https'
      - '--entryPoints.http.http.redirections.entryPoint.scheme=https'
      #- '--entrypoints.web.address=:80'
      #- '--entrypoints.web.http.redirections.entryPoint.to=websecure'
      #- '--entrypoints.web.http.redirections.entryPoint.scheme=https'
      #- '--entrypoints.web.http.redirections.entrypoint.permanent=true'
      #- '--entrypoints.websecure.address=:443'
      - '--entryPoints.http.address=:80/tcp'
      ## Please see the Forwarded Header Trust section of the Authelia Traefik
Integration documentation.
      - '--entryPoints.http.forwardedHeaders.trustedIPs=10.0.1.0/24,
10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'
      - '--entryPoints.http.proxyProtocol.trustedIPs=10.0.1.0/24,
10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'
      - '--entryPoints.http.forwardedHeaders.insecure=false'
```

```
      - '--entryPoints.http.proxyProtocol.insecure=false'
      - '--entryPoints.https=true'
      - '--entryPoints.https.address=:443/tcp'
      ### Please see the Forwarded Header Trust section of the Authelia
Traefik Integration documentation.
      - '--entryPoints.https.forwardedHeaders.trustedIPs=10.0.1.0/24,
10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'
      - '--entryPoints.https.proxyProtocol.trustedIPs=10.0.1.0/24,
10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'
      - '--entryPoints.https.forwardedHeaders.insecure=false'
      - '--entryPoints.https.proxyProtocol.insecure=false'
      - "--
certificatesresolvers.letsencrypt.acme.email=maxoucaparros@gmail.com"
      - "--certificatesresolvers.letsencrypt.acme.storage=/config/acme.json"
      - "--certificatesresolvers.letsencrypt.acme.caserver=https://acme-
v02.api.letsencrypt.org/directory"
      - "--certificatesresolvers.letsencrypt.acme.keytype=RSA4096"
      - "--certificatesresolvers.letsencrypt.acme.dnschallenge=true"
      - "--
certificatesresolvers.letsencrypt.acme.dnschallenge.provider=cloudflare"
      - "--
certificatesresolvers.letsencrypt.acme.dnschallenge.delaybeforecheck=0"
      - "--
certificatesresolvers.letsencrypt.acme.dnschallenge.resolvers=1.1.1.1:53,8.8.8
.8:53"
    networks:
          net: {}
    ports:
      - "80:80"
      - "443:443"
      - "8443:443"
      - "8080:80"
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - ./traefik/data/traefik:/config
      #- "./cert/:/certs/"
      #- ./letsencrypt:/letsencrypt
      #- ./acme.json:/acme.json
      #- ./traefik.yml:/etc/traefik/traefik.yml
    labels:
      - 'traefik.enable=true'
      # middleware redirect
      - traefik.http.middlewares.force-secure.redirectscheme.scheme=https
      - traefik.http.middlewares.force-secure.redirectscheme.permanent=true
      #- 'traefik.http.routers.reverse-proxy.rule=Host(`maxcaptab.fr`)'
      - 'traefik.http.routers.api.rule=Host(`traefik.maxcaptab.fr`)'
      - 'traefik.http.routers.api.entryPoints=https'
      - 'traefik.http.routers.api.tls=true'
```

```
      - 'traefik.http.routers.api.service=api@internal'
      - 'traefik.http.routers.api.middlewares=authelia@docker'
      #- "traefik.http.routers.api.tls.certresolver=myresolver"
    depends_on:
      - authelia
```

### *1.2 Traefik*

Pour traefik voici la configuration qu'on a mis en place :

- Redirection http -> https
- Port 80 pour http et 443 pour https
- Trusted IP 10.0.1.0/24 pour le VPN admin et 10.0.8.0/24 pour le VPN User. Ensuite les IPs local
- Nous avons aussi essayé de récupérer un certificat avec letsencrypt pour notre nom de domaine : maxcaptab.fr
- Nous avons configuré le middleware authelia@docker pour utiliser le SSO d'authelia
- Nous stockons les logs dans /home/appdata/traefik/traefik/data/traefik
- Nous avons utilisé depends_on : authelia, pour pouvoir lancer traefik après authelia.

### *1.3 Authelia*

Nous avons tout d'abord créé des clés secrètes pour encrypter Authelia.

Les secrets se trouvent dans /home/appdata/authelia/secrets

Ensuite nous avons créé un alias pour que les autres containers puissent utiliser l'alias afin de communiquer avec authelia.

Nous avons configuré le middleware pour qu'il fonctionne.

Pour la configuration d'authelia nous avons utilisé les configurations suivantes :

```
default_redirection_url: "https://nextcloud.maxcaptab.fr"
```

```
authentication_backend:
 ldap:
 implementation: activedirectory
 url: ldap://192.168.10.10:389
 start_tls: false
 tls:
  server_name: server-AD
  base_dn: dc=contoso,dc=adds
  username_attribute: sAMAccountName
```

```
  users_filter:
(&({username_attribute}={input})(objectCategory=person)(objectClass=user))
  groups_filter:
(&(member:1.2.840.113556.1.4.1941:={dn})(objectClass=group)(objectCategory=gro
up))
  group_name_attribute: cn
  mail_attribute: mail
  display_name_attribute: displayName
  permit_referrals: false
  user: CN=pfsense admin,OU=admin,OU=AllUser;DC=contoso,DC=adds
  password: ***
```

rules :

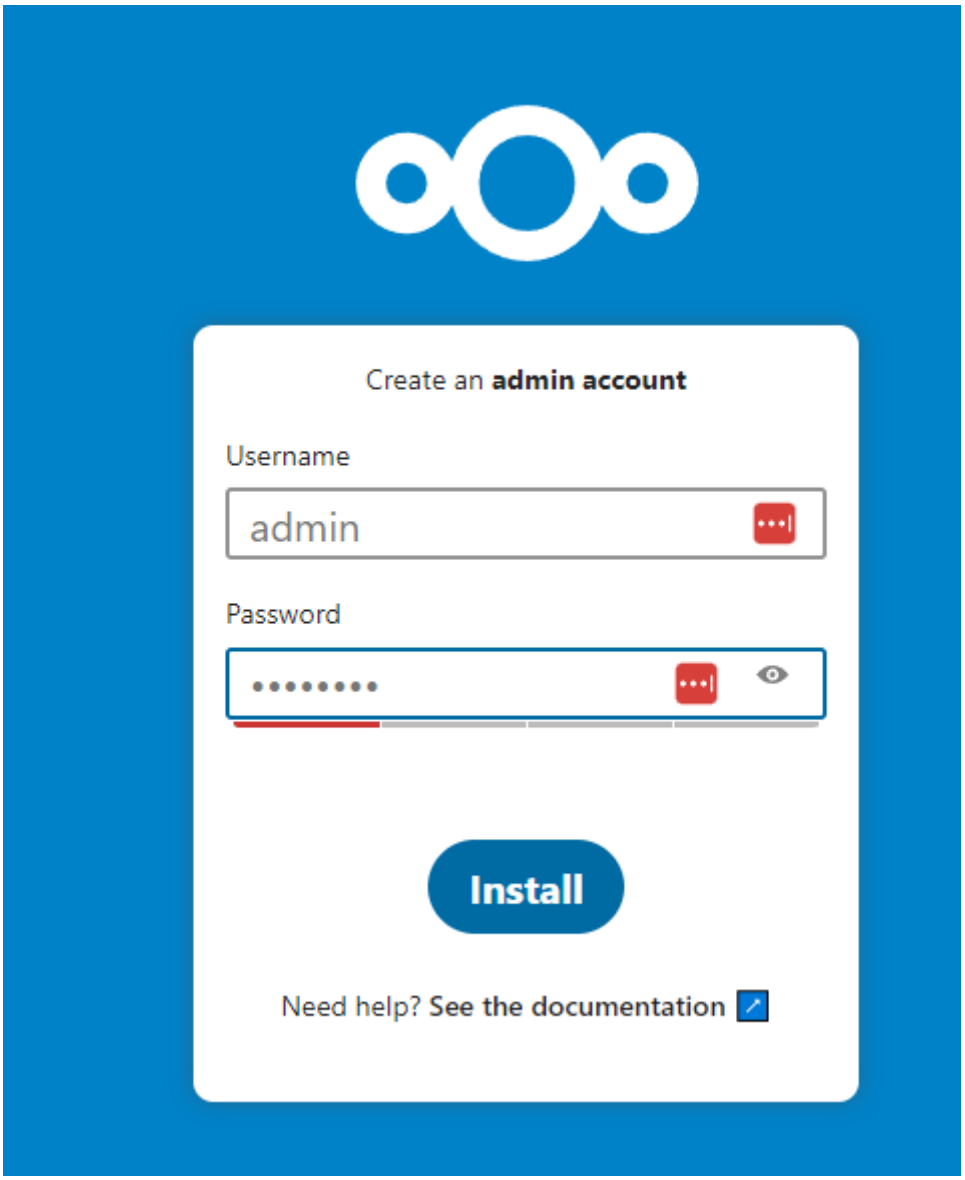
```
access_control:
  default_policy: one_factor

  networks:
    - name: internal
      networks:
        - 192.168.99.0/24
        - 192.168.20.0/24
        - 192.168.10.0/24
    - name: VPN
      networks: 10.0.1.0/24

  rules:
    ## Rules applied to everyone
    - domain: '*.maxcaptab.fr'
      policy: one_factor
      networks:
        - internal
        - VPN
    - domain: '*'
      policy: one_factor
```

```
identity_providers:
  oidc:
    hmac_secret: Slj^2tvRREiA86Rgaw%G^1E1%mC8H*o#rq#jWU0vkwFHCa*
  issuer_private_key: | ****
 clients:
      -
        id: nextcloudID

        description: Nextcloud
```

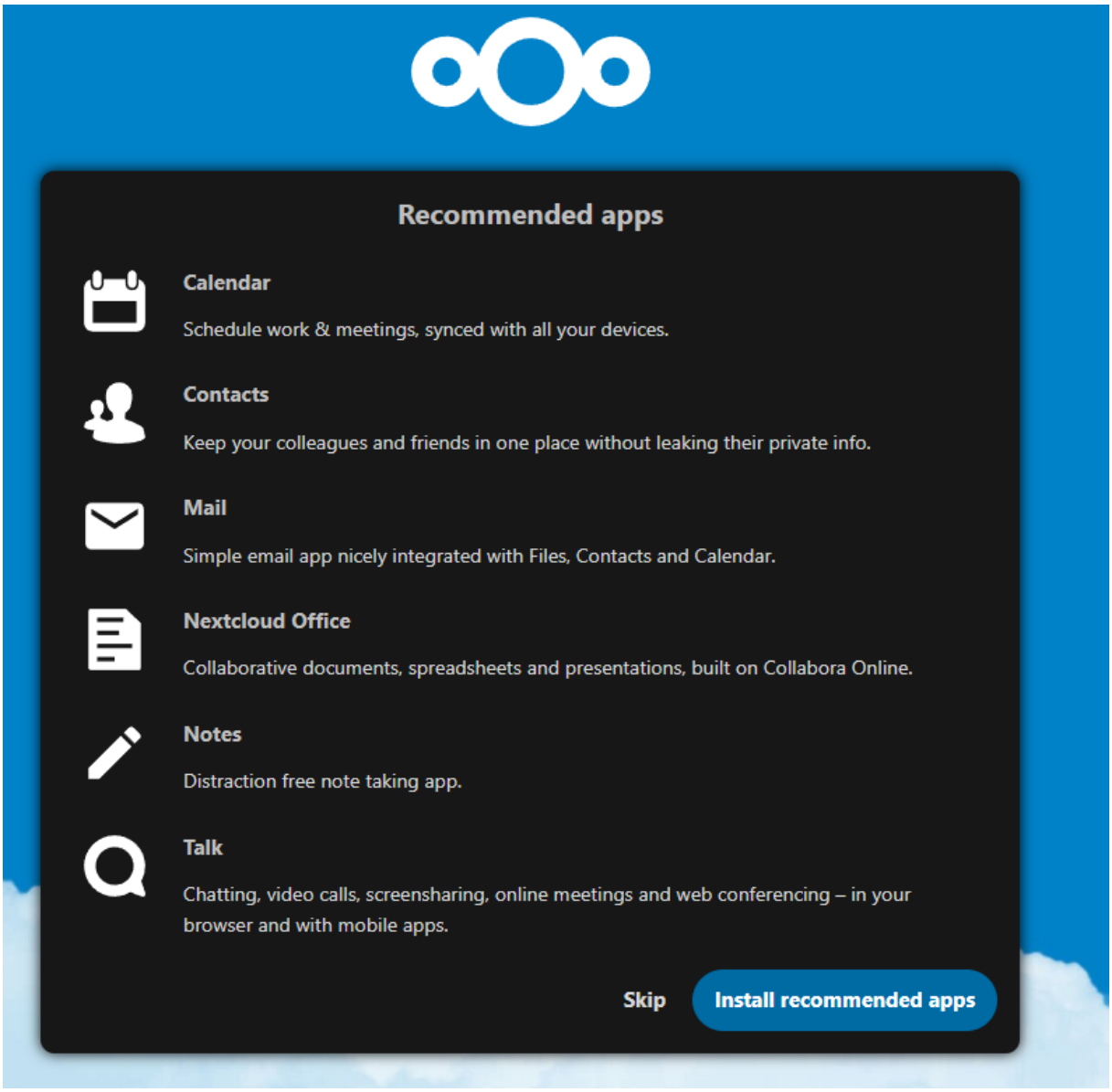
```
        secret:
'!HydLZ2RcQwvOzwwlgqr2epM0S*!XrmaMG@rcc5*ebFc3z4$UciBOV5zl7BCHZJklu@7IsOQd4IhI
'
        public: false

        authorization_policy: one_factor

        consent_mode: auto

        pre_configured_consent_duration: 1w
        audience: []

        scopes:
          - openid
          - groups
          - email
          - profile

        redirect_uris:
        - https://nextcloud.maxcaptab.fr/apps/oidc_login/oidc
```

*1.4 Nextcloud*

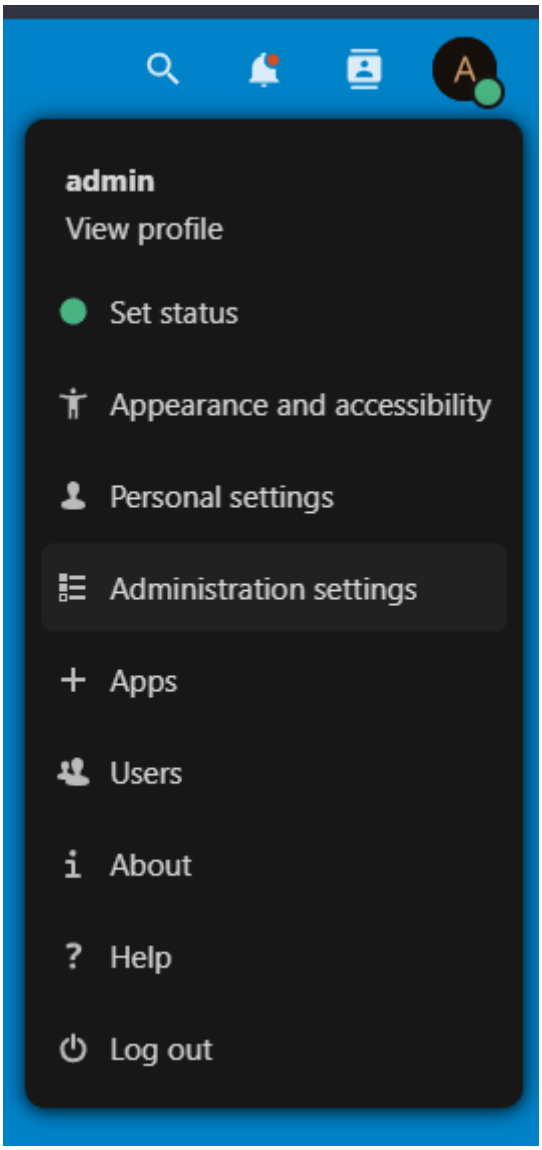
Configuration de nextcloud




On installe ensuite les applications recommandées :

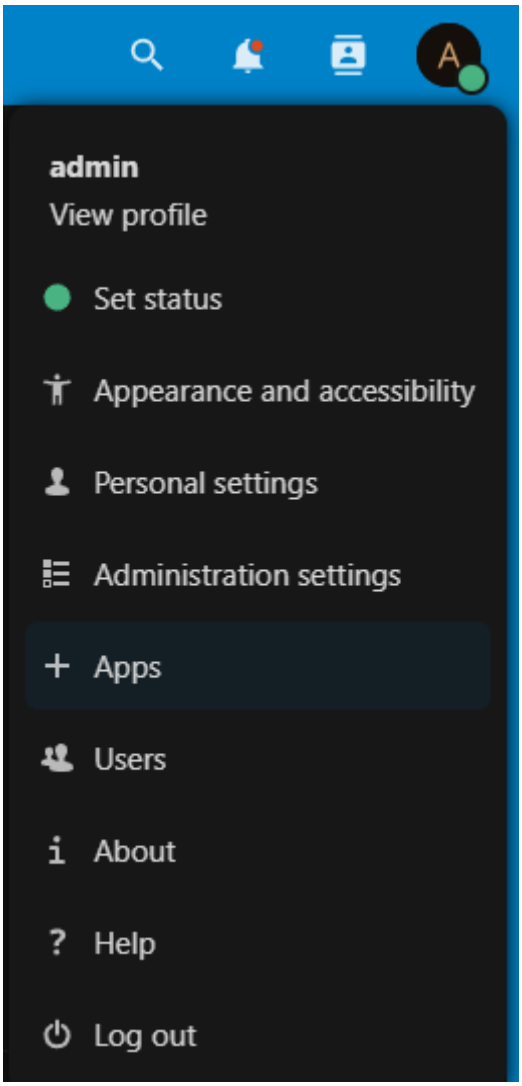


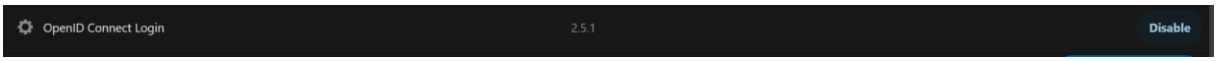

Puis on se dirige dans l’es options d’administrations




## Application SSO

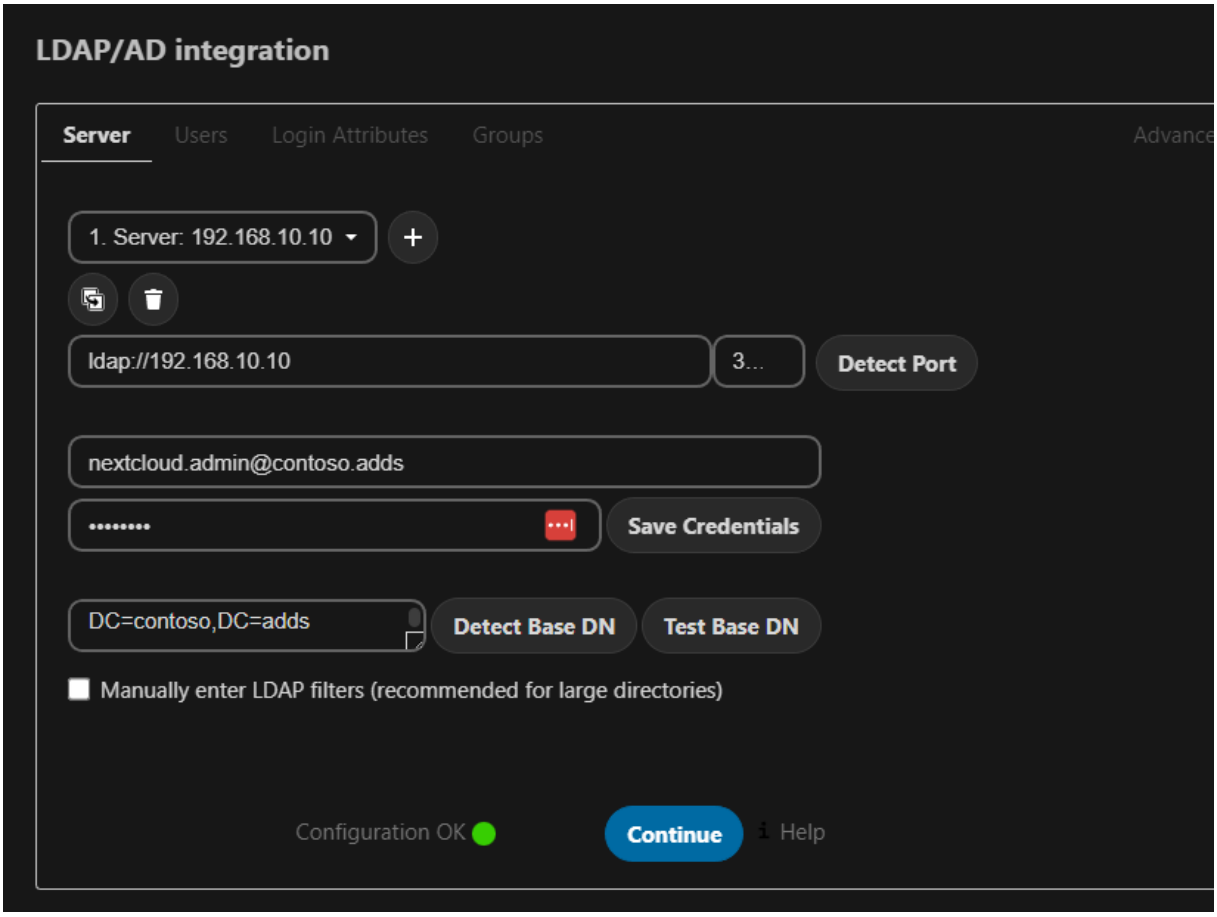
Pour l’application SSO nous utiliserons OpenId connect login qui va nous permettre de lier les logins Authelia avec nextcloud.




## Intégration avec l'AD

Nextcloud permet une intégration dans l'AD très facile il suffit de faire la conf suivante :




## Intégration avec Authelia

Il faut changer le fichier config.php d'Authelia et rentrer la config suivante :

```
$CONFIG = array (
    'allow_user_to_change_display_name' => false,
    'lost_password_link' => 'disabled',
    'oidc_login_provider_url' => 'https://auth.maxcaptab.fr,
    'oidc_login_client_id' => 'nextcloud',
    'oidc_login_client_secret' => 'insecure_secret',
    'oidc_login_auto_redirect' => false,
    'oidc_login_end_session_redirect' => false,
    'oidc_login_button_text' => 'Log in with Authelia',
    'oidc_login_hide_password_form' => false,
    'oidc_login_use_id_token' => true,
    'oidc_login_attributes' => array (
        'id' => 'preferred_username',
        'name' => 'name',
        'mail' => 'email',
        'groups' => 'groups',
    ),
    'oidc_login_default_group' => 'oidc',
    'oidc_login_use_external_storage' => false,
    'oidc_login_scope' => 'openid profile email groups',
    'oidc_login_proxy_ldap' => false,
    'oidc_login_disable_registration' => true,
    'oidc_login_redir_fallback' => false,
    'oidc_login_alt_login_page' => 'assets/login.php',
    'oidc_login_tls_verify' => true,
    'oidc_create_groups' => false,
    'oidc_login_webdav_enabled' => false,
    'oidc_login_password_authentication' => false,
    'oidc_login_public_key_caching_time' => 86400,
    'oidc_login_min_time_between_jwks_requests' => 10,
    'oidc_login_well_known_caching_time' => 86400,
    'oidc_login_update_avatar' => false,
                            );
```

Avec cette configuration nous allons pouvoir nous connecter à Nextcloud avec les logins d'Authelia.

## 4. Politique de sécurité

Nous autorisont seulement les réseaux suivants à accéder à nos pages web :

- 10.0.1.0/24
- 10.0.8.0/24
- 172.0.0.0/8
- 127.0.0.0/8

## 5. Gestion des mises à jour

Les mises à jour sont gérées par l'interface web de Nextcloud ou alors avec le fichier docker compose.

### 6. Gestion des logs

Les logs sont affichés sur Portainer.

### 7. Gestion des accès

L'accès administratifs de Nextcloud est géré par le compte nextcloud.admin qui est créé sur l'AD.

## 6. Serveur mail

Pour la mise en place du serveur mail nous avons choisi de mettre en place hmailserv.

### 1. Objectifs

Pour notre serveur mail nous avons besoins de plusieurs fonctionnalités :

- Avoir un serveur mail connecté à l'AD

### 2. Configuration matérielle

Pour notre firewall nous l'avons mis en place sur Proxmox avec la configuration matérielle suivant :

2 Processeur,

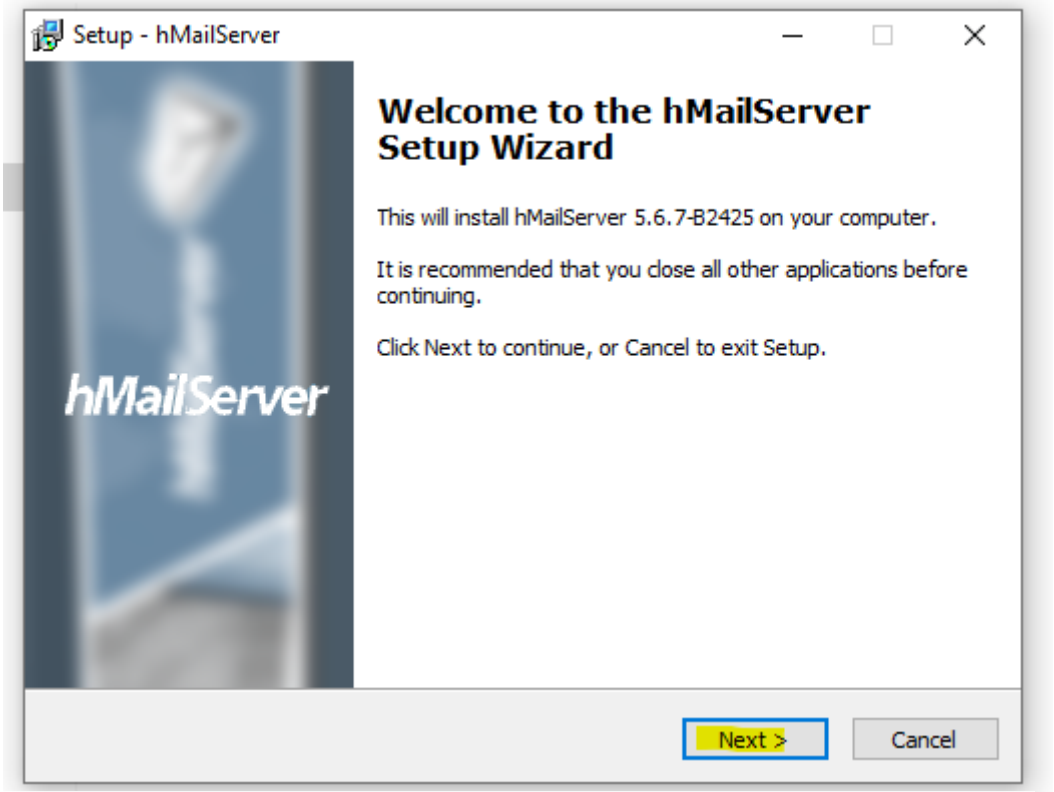
1 cœur par processeur

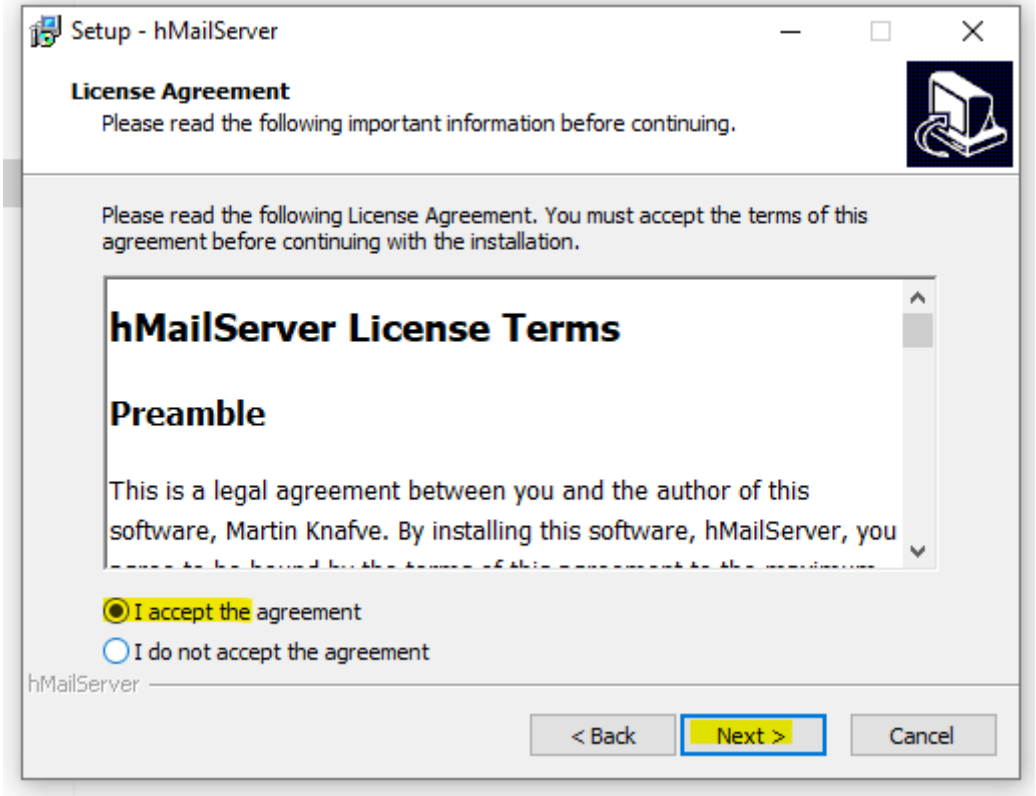
4GB de ram

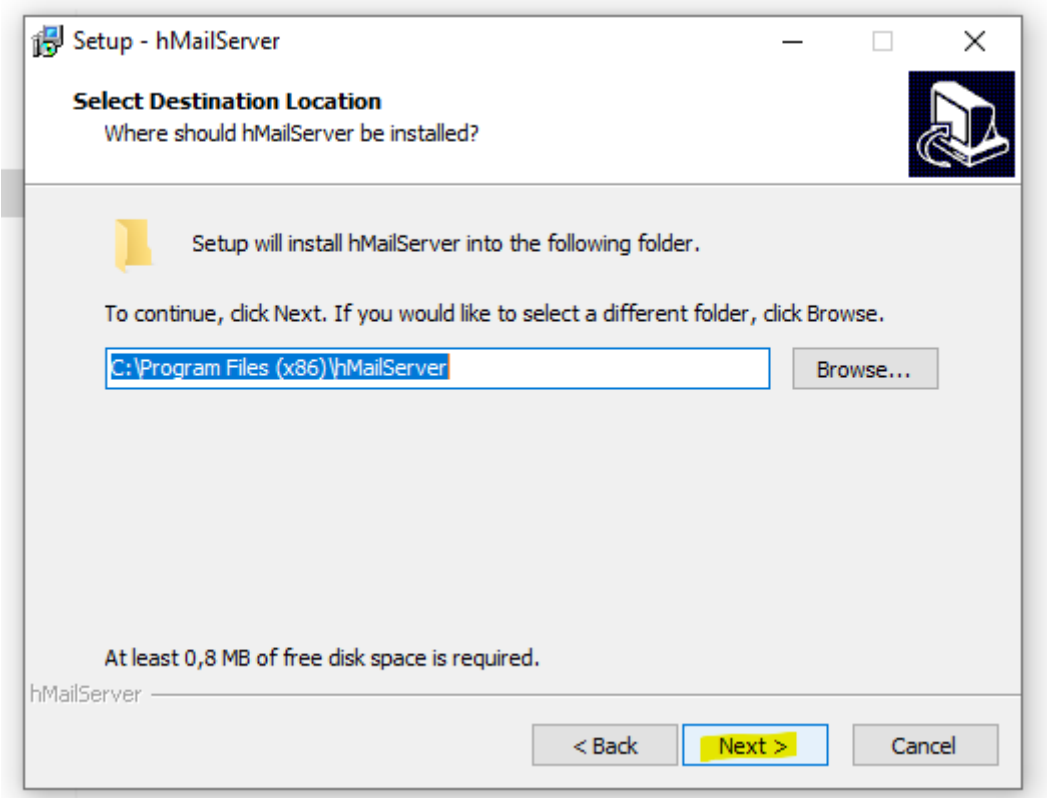
60GB de disque virtuel en SCSI

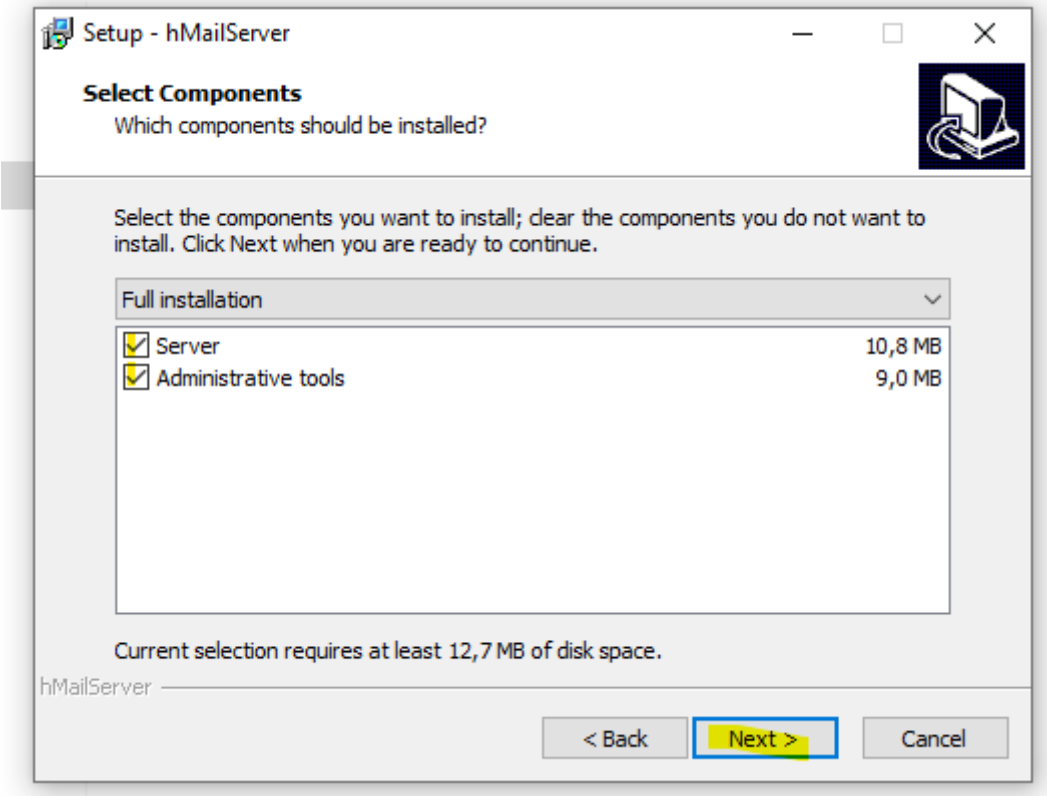
### 3. Configuration logicielle

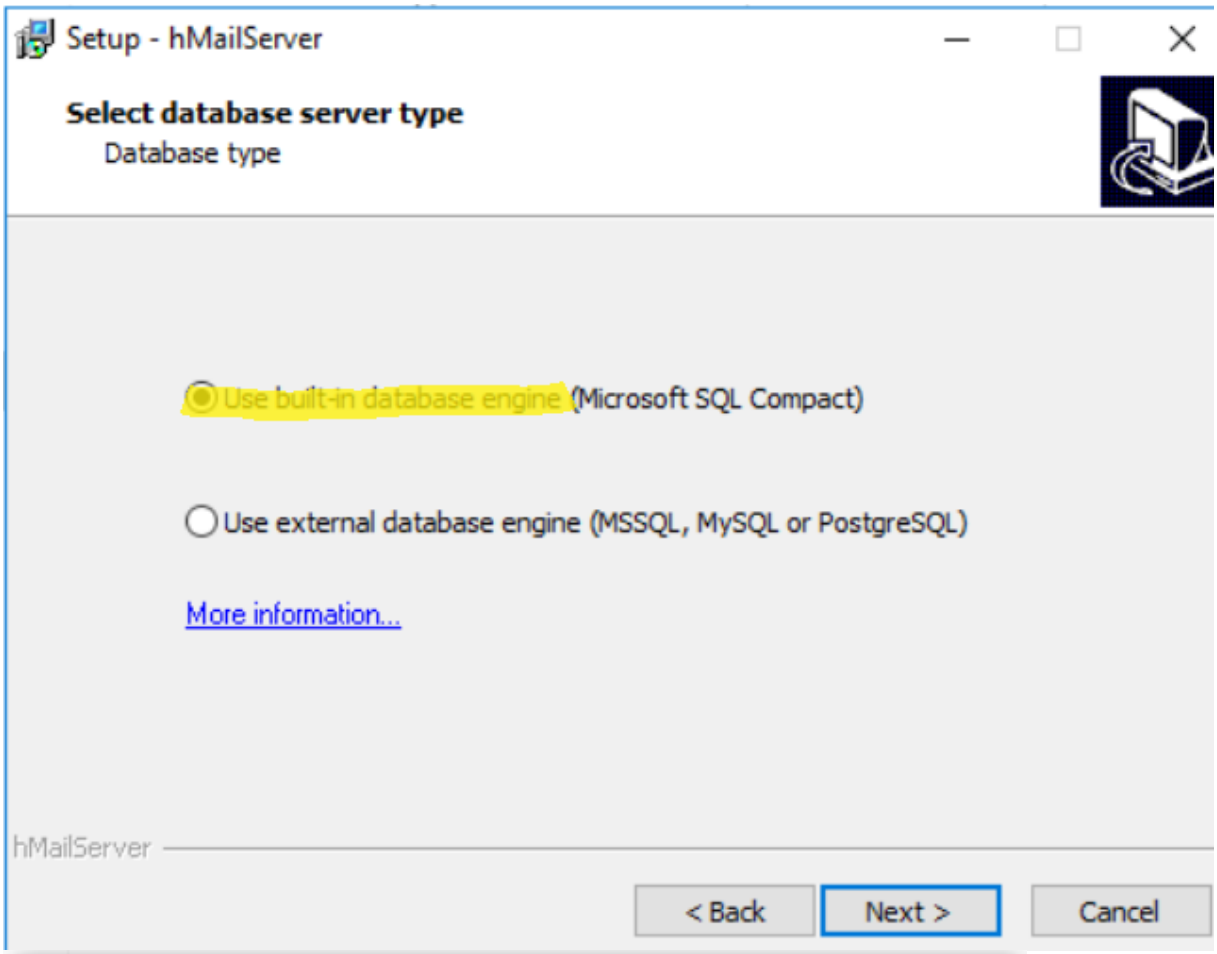
#### 1. Setup de l'application hmailserv

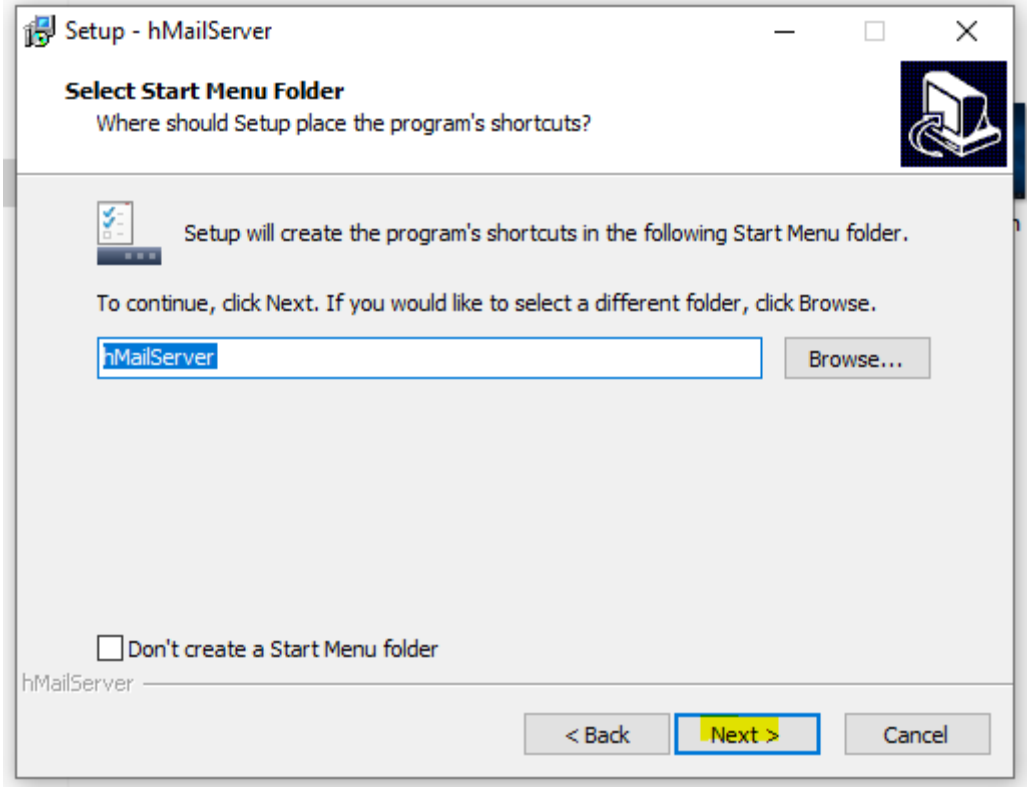

Setup - hMailServer
hMailServer
Welcome to the hMailServer Setup Wizard
This will install hMailServer 5.6.7-B2425 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

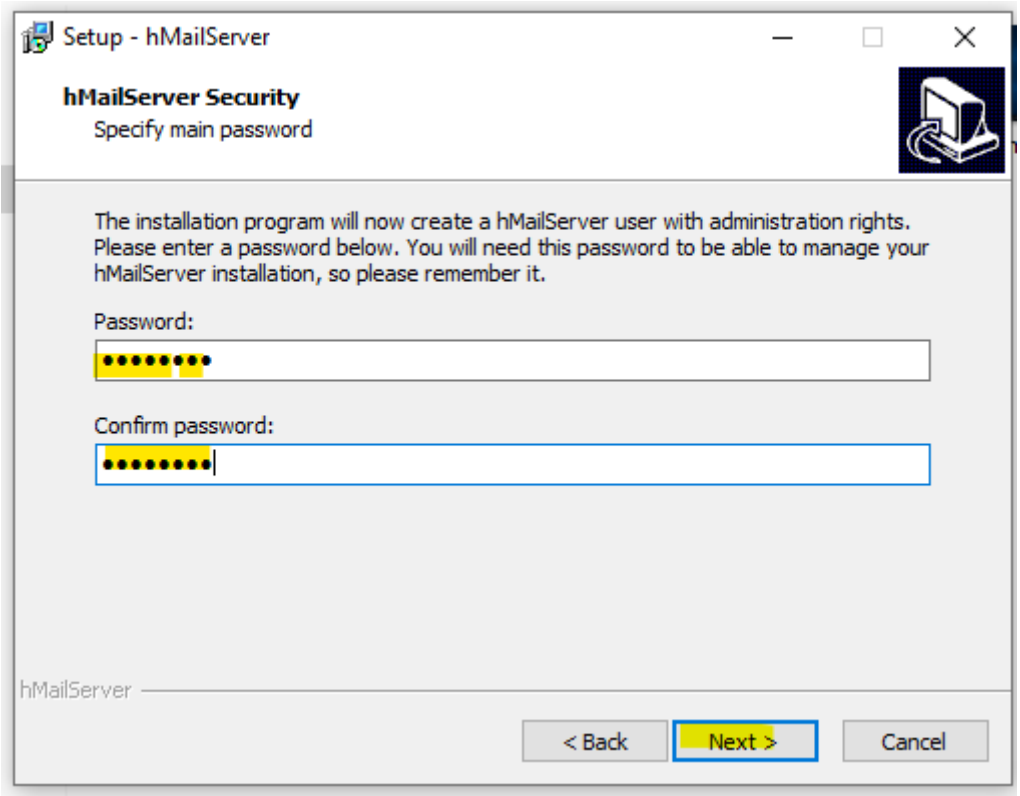

Setup - hMailServer
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
hMailServer License Terms
Preamble
This is a legal agreement between you and the author of this software, Martin Knafve. By installing this software, hMailServer, you
I accept the agreement
I do not accept the agreement
hMailServer
< Back
Next >
Cancel


Setup - hMailServer
Select Destination Location
Where should hMailServer be installed?
Setup will install hMailServer into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\hMailServer
Browse...
At least 0,8 MB of free disk space is required.
hMailServer
< Back
Next >
Cancel

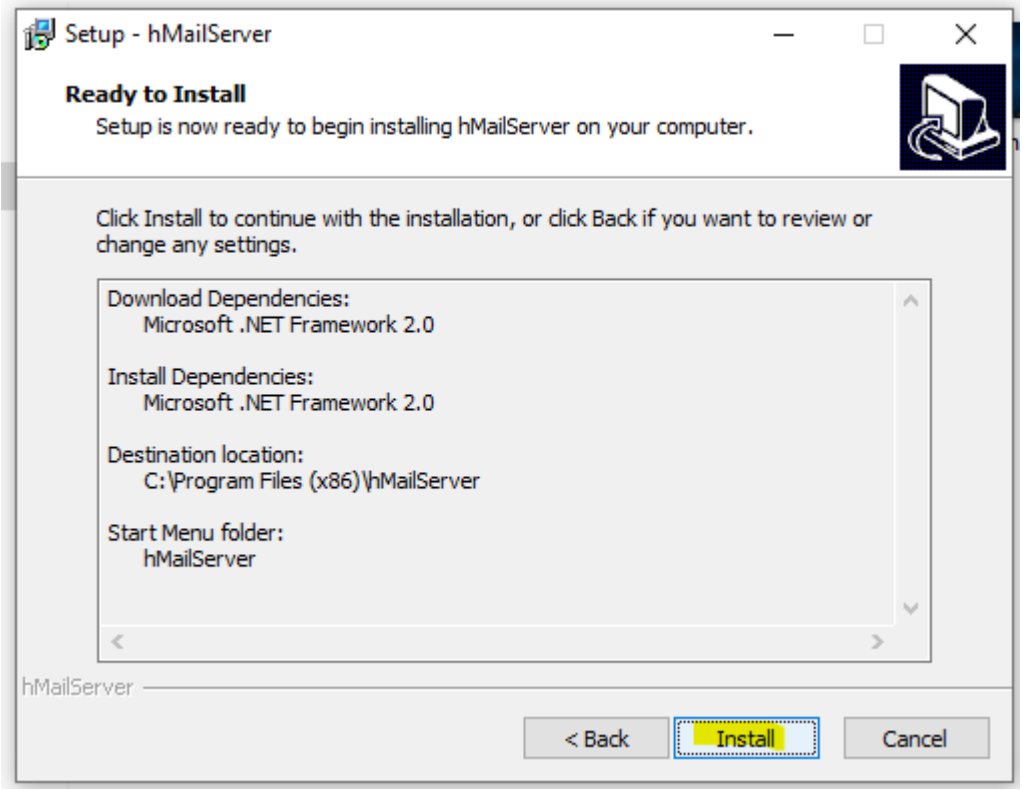

Setup - hMailServer
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
Server
10,8 MB
Administrative tools
9,0 MB
Current selection requires at least 12,7 MB of disk space.
hMailServer
< Back
Next >
Cancel

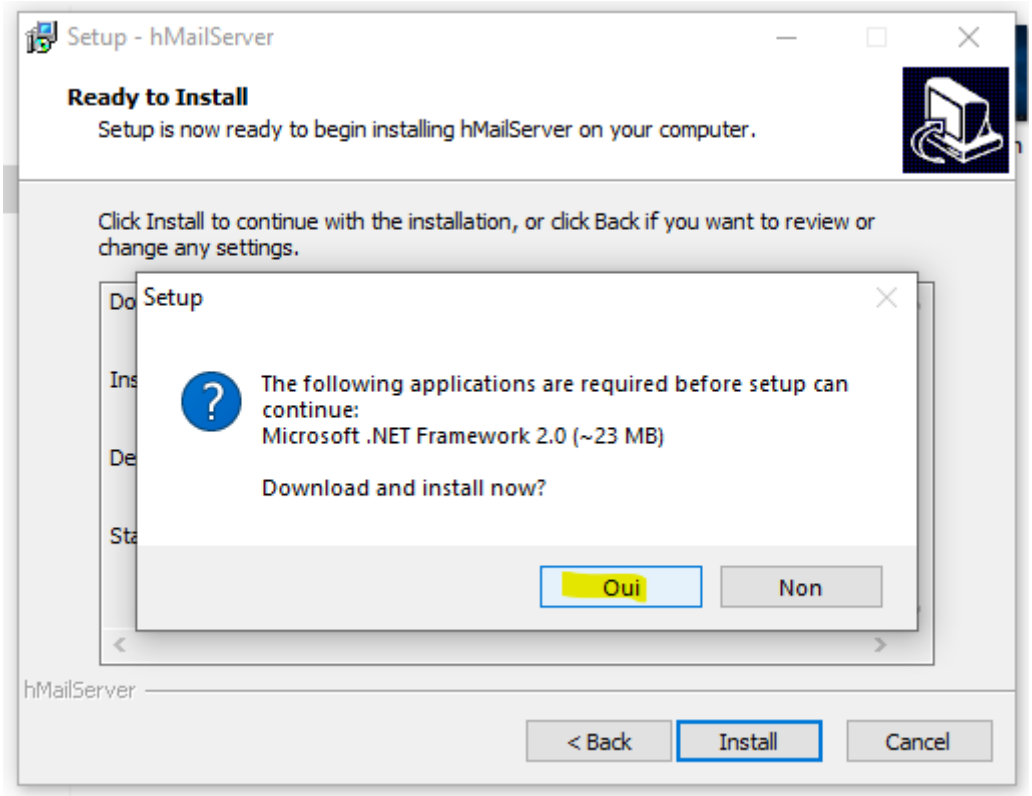

Setup - hMailServer
Select database server type
Database type
Use built-in database engine (Microsoft SQL Compact)
Use external database engine (MSSQL, MySQL or PostgreSQL)
More information...
hMailServer
< Back
Next >
Cancel

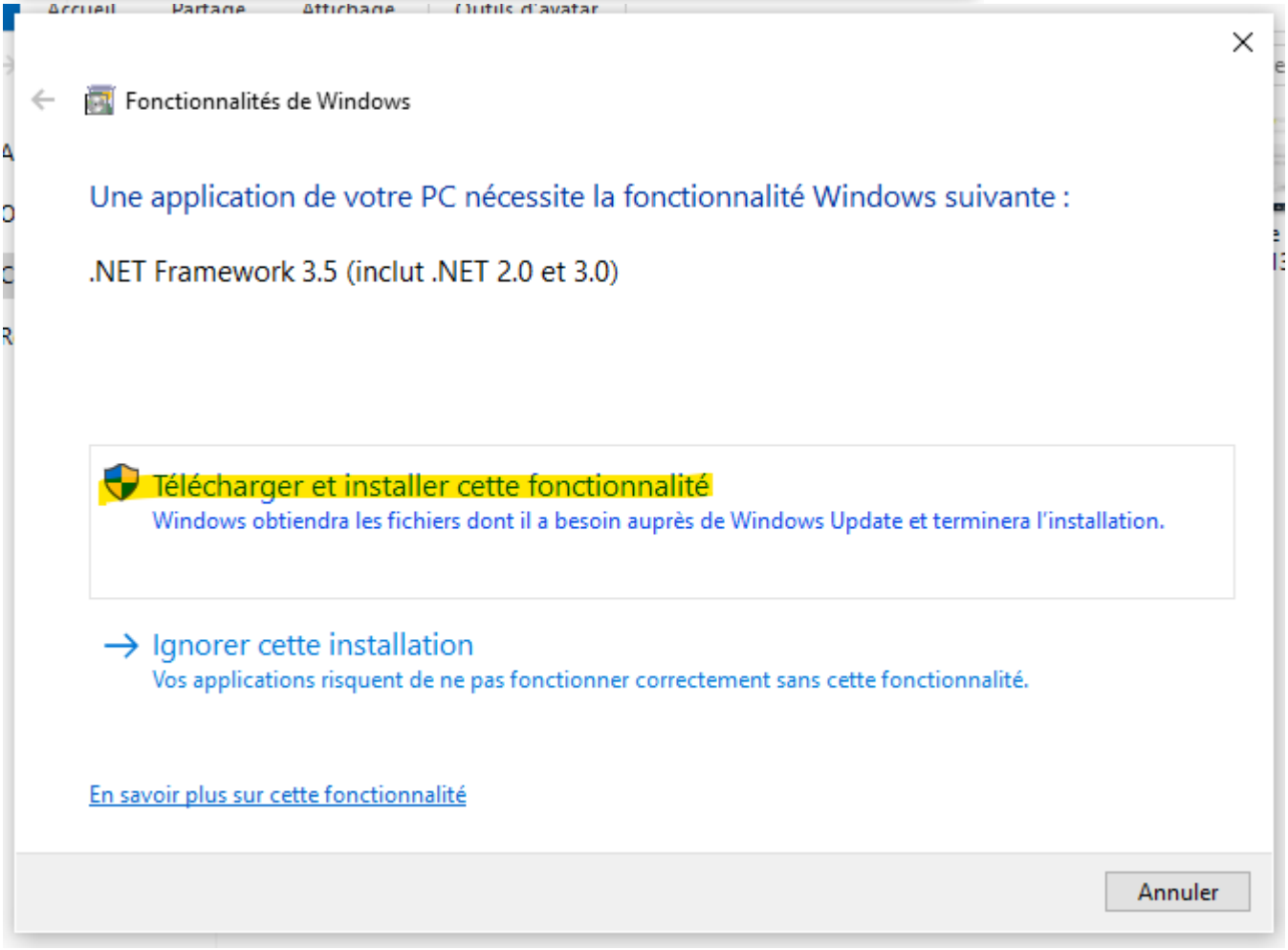

Setup - hMailServer
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
hMailServer
Browse...
Don't create a Start Menu folder
hMailServer
< Back
Next >
Cancel

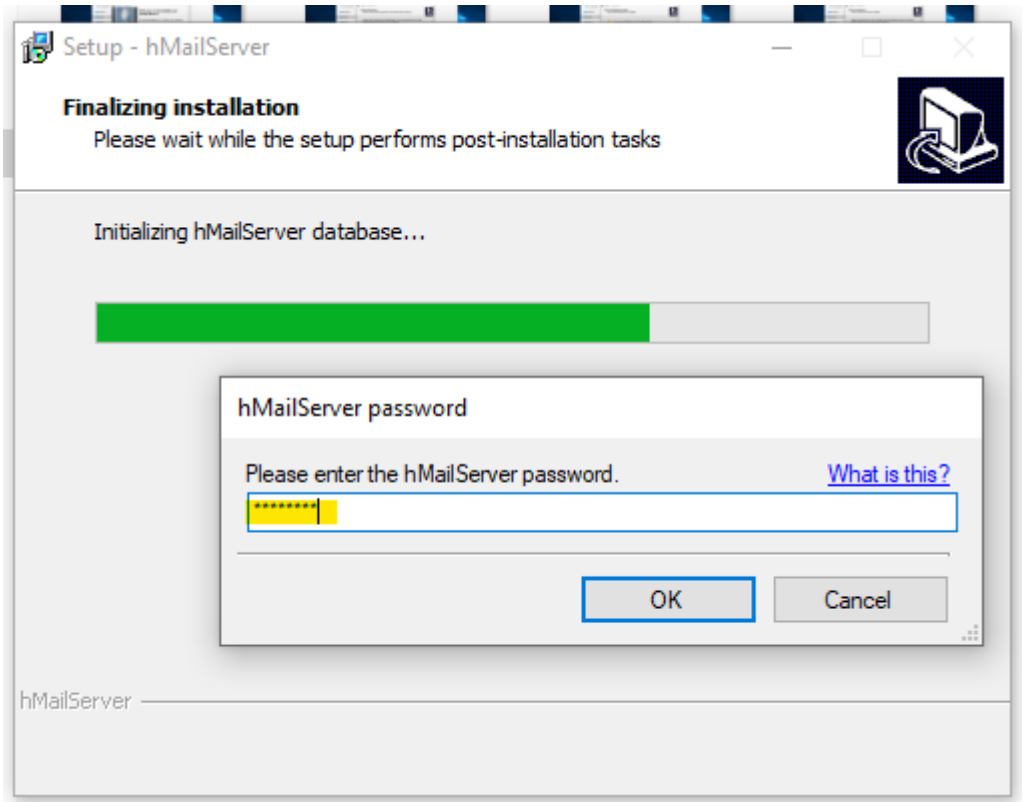


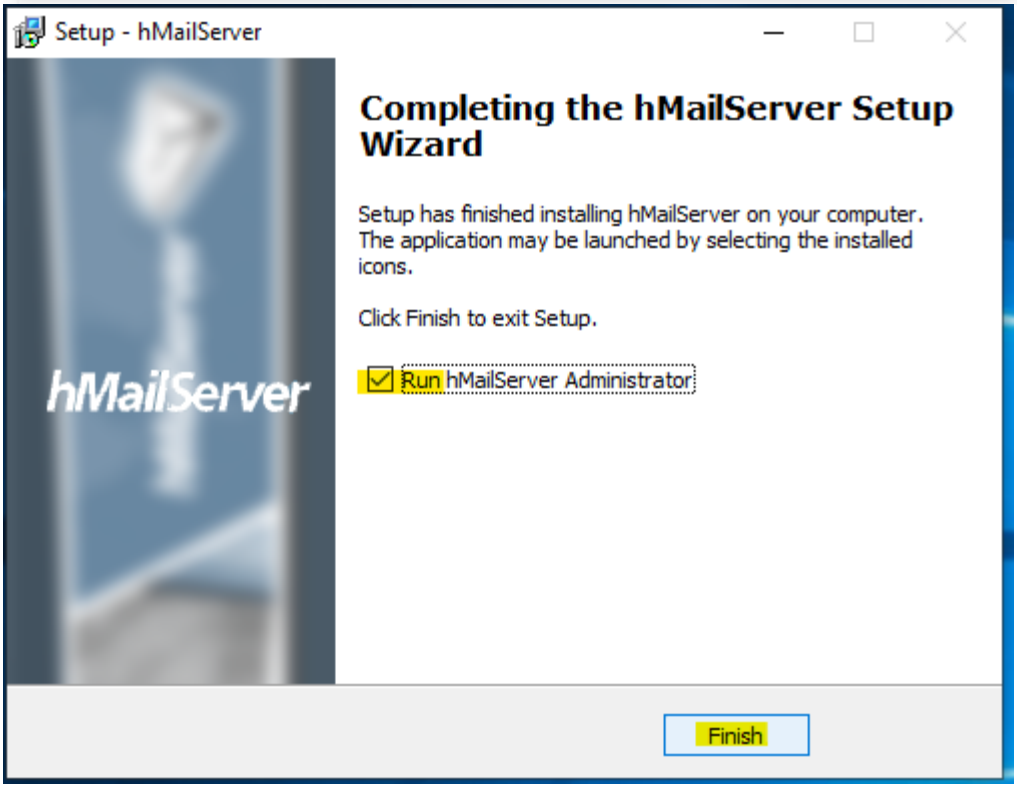

*** Mot de passe pour l'administration de l'application. Il sera demandé pour accéder à l'interface.**




Setup - hMailServer
Ready to Install
Setup is now ready to begin installing hMailServer on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Setup
The following applications are required before setup can continue:
Microsoft .NET Framework 2.0 (~23 MB)
Download and install now?
Oui
Non
hMailServer
< Back
Install
Cancel

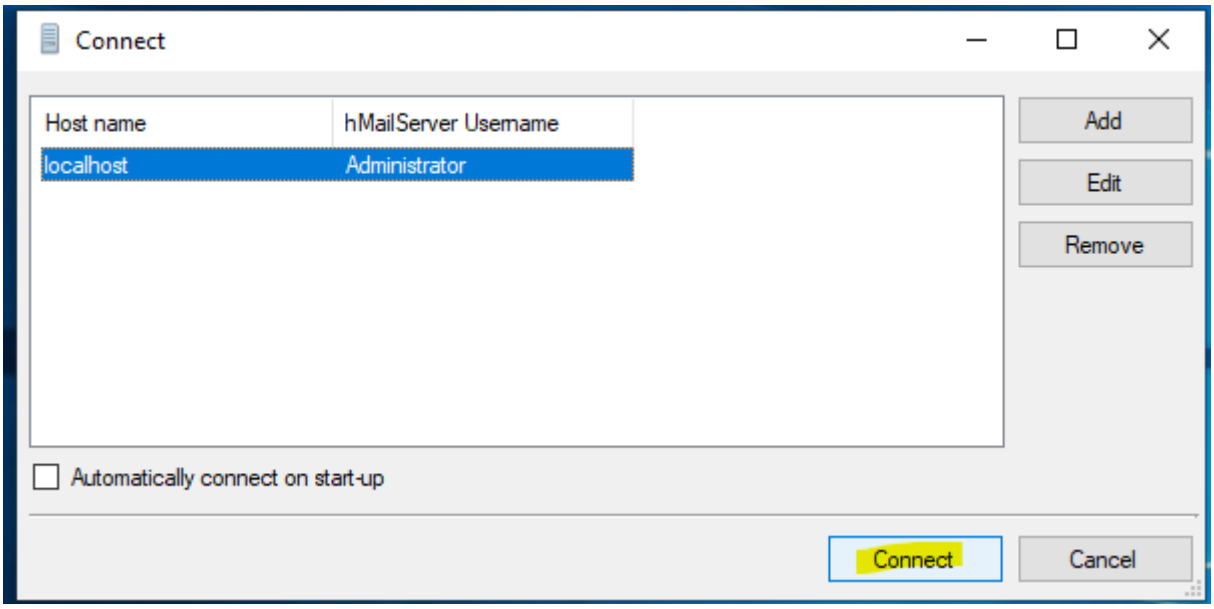

Fonctionnalités de Windows
Une application de votre PC nécessite la fonctionnalité Windows suivante :
.NET Framework 3.5 (inclut .NET 2.0 et 3.0)
Télécharger et installer cette fonctionnalité
Windows obtiendra les fichiers dont il a besoin auprès de Windows Update et terminera l'installation.
Ignorer cette installation
Vos applications risquent de ne pas fonctionner correctement sans cette fonctionnalité.
En savoir plus sur cette fonctionnalité
Annuler

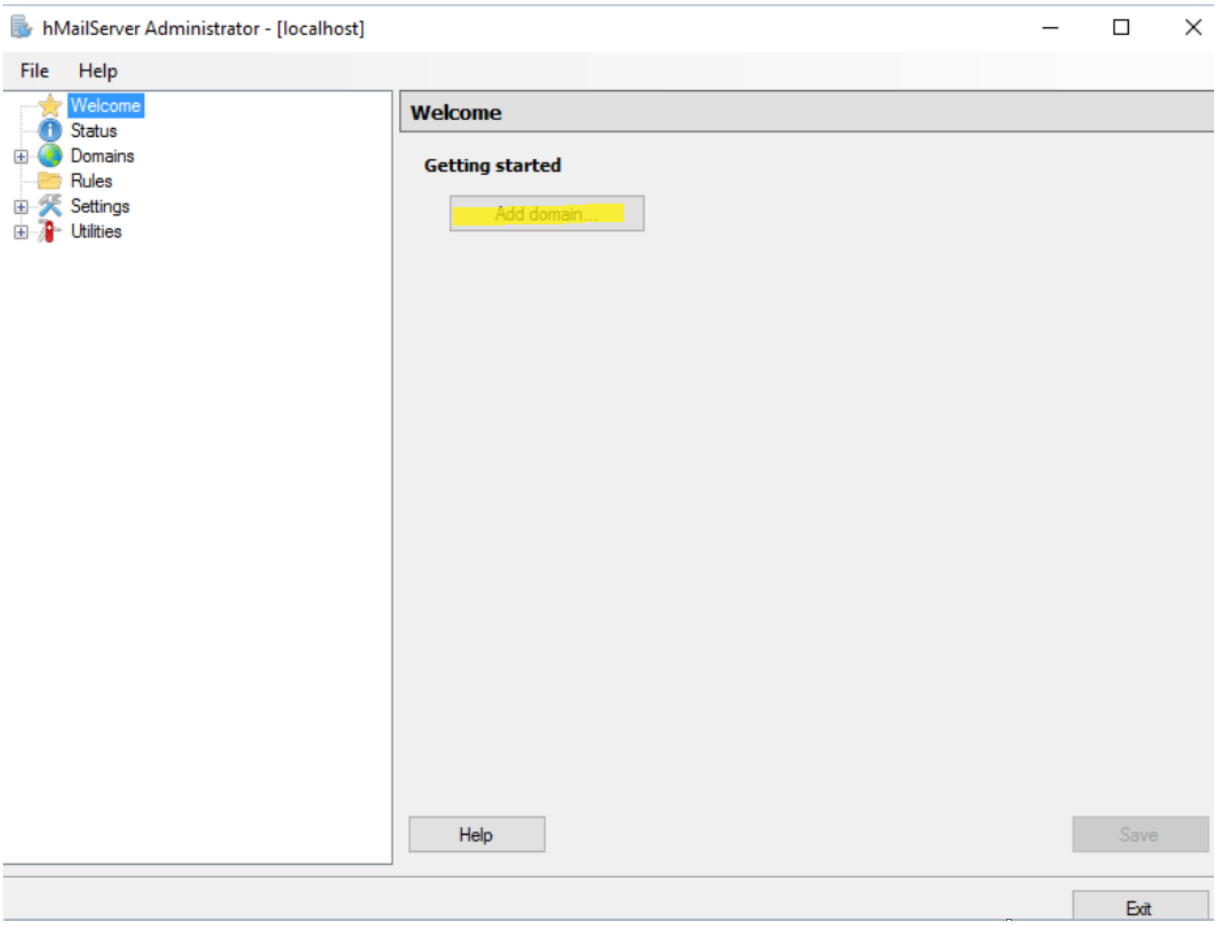


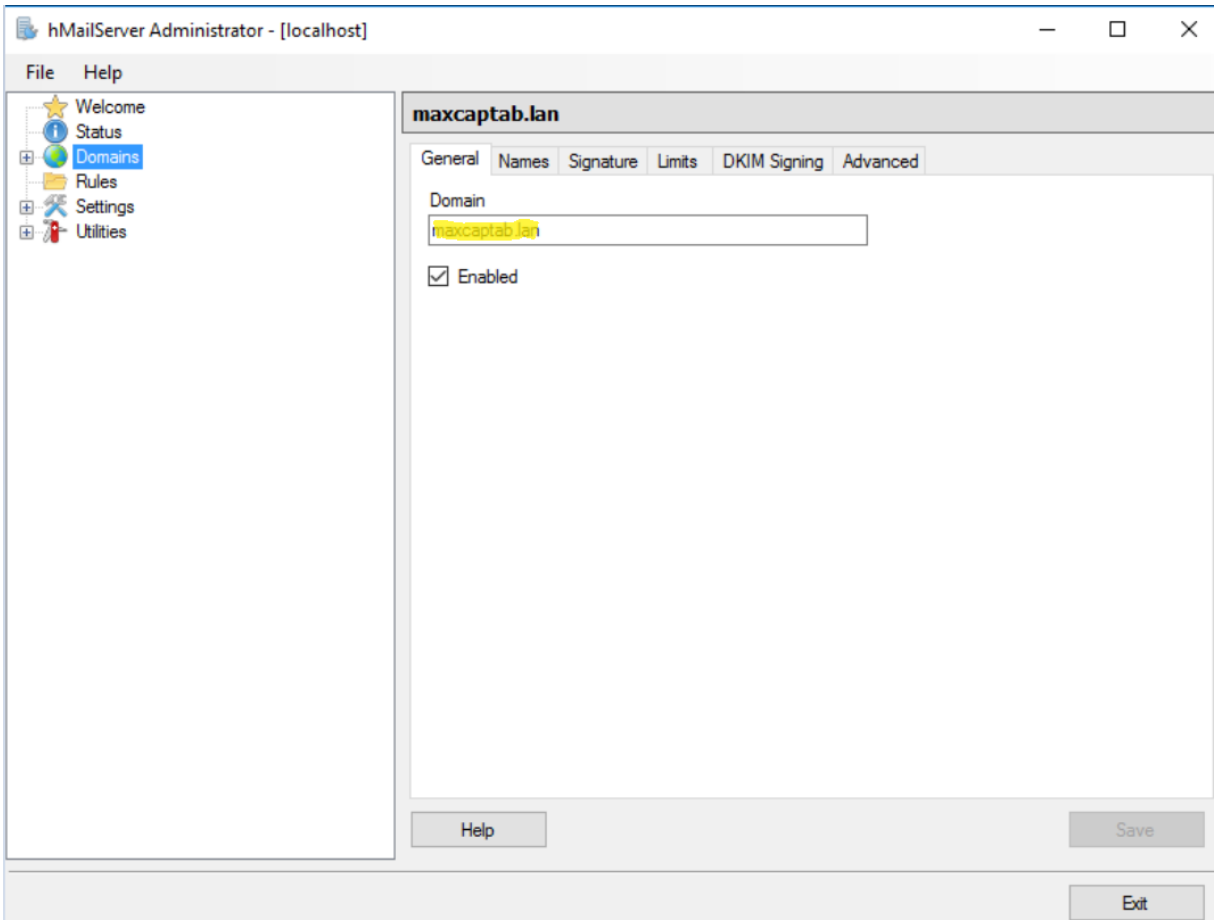




- L'application hMailServer est installée !!!

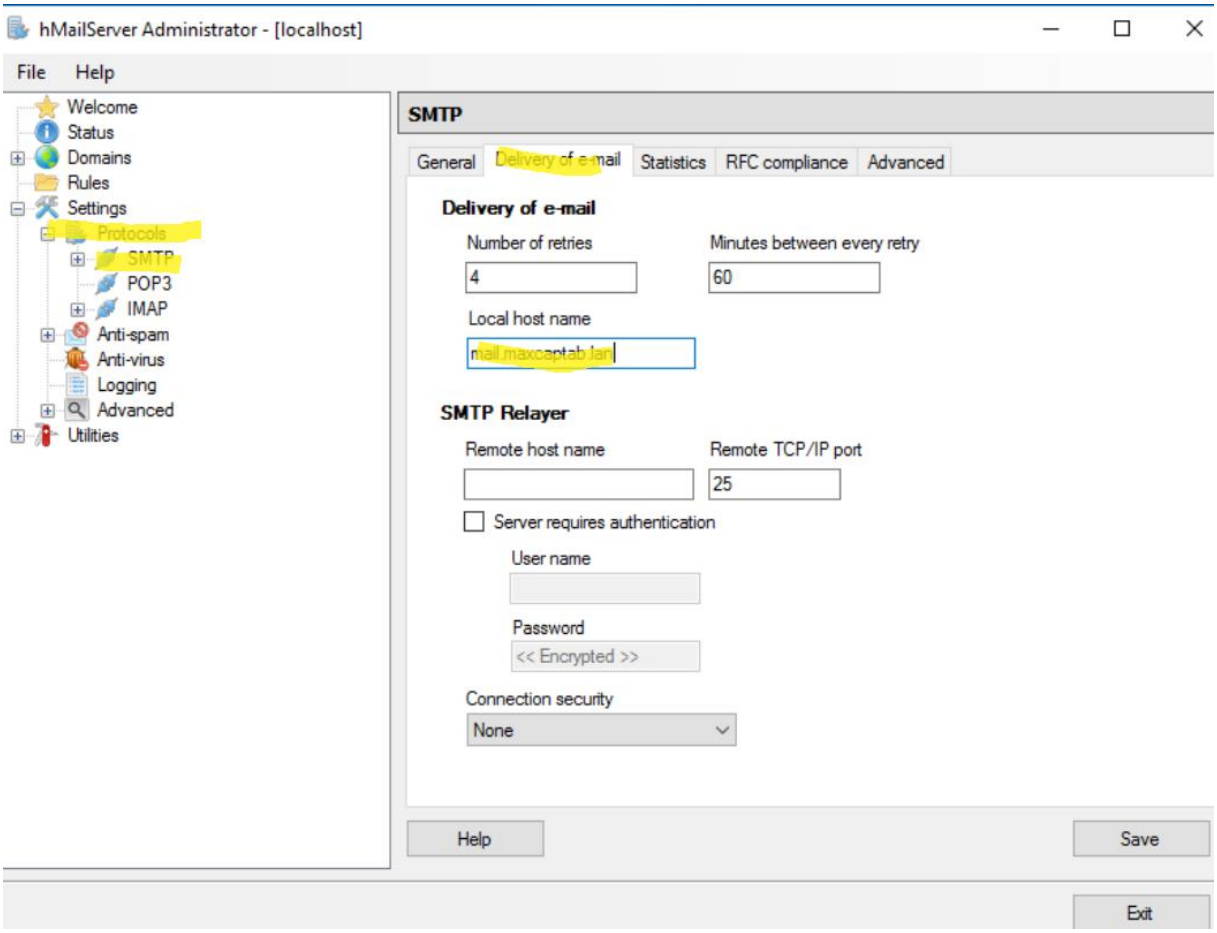
**- Configuration**


Connect
Host name
hMailServer Username
localhost
Administrator
Add
Edit
Remove
Automatically connect on start-up
Connect
Cancel


hMailServer Administrator - [localhost]
File
Help
Welcome
Status
Domains
Rules
Settings
Utilities
Welcome
Getting started
Add domain...
Help
Save
Exit

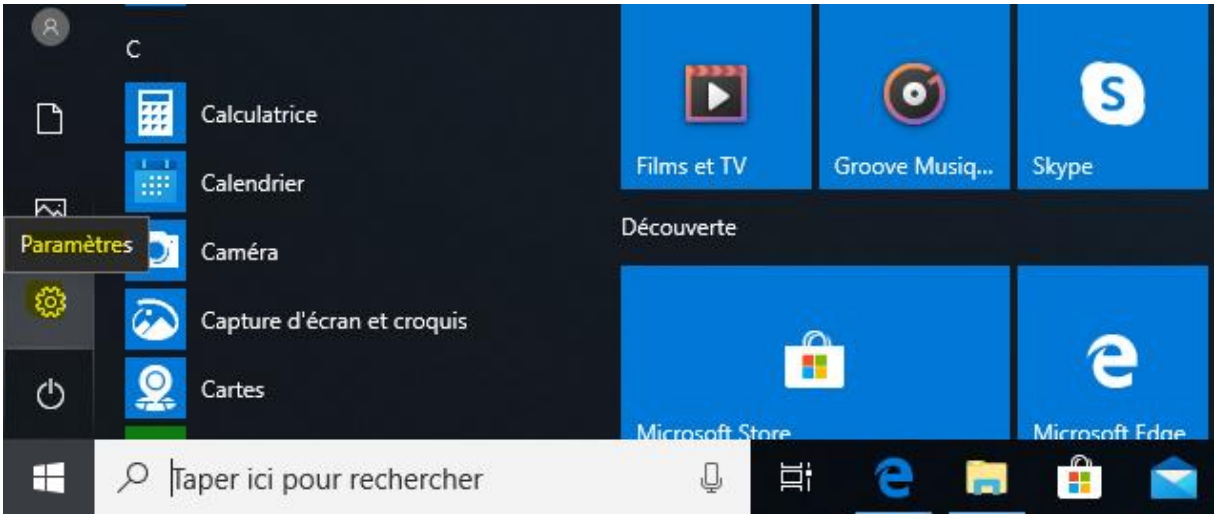


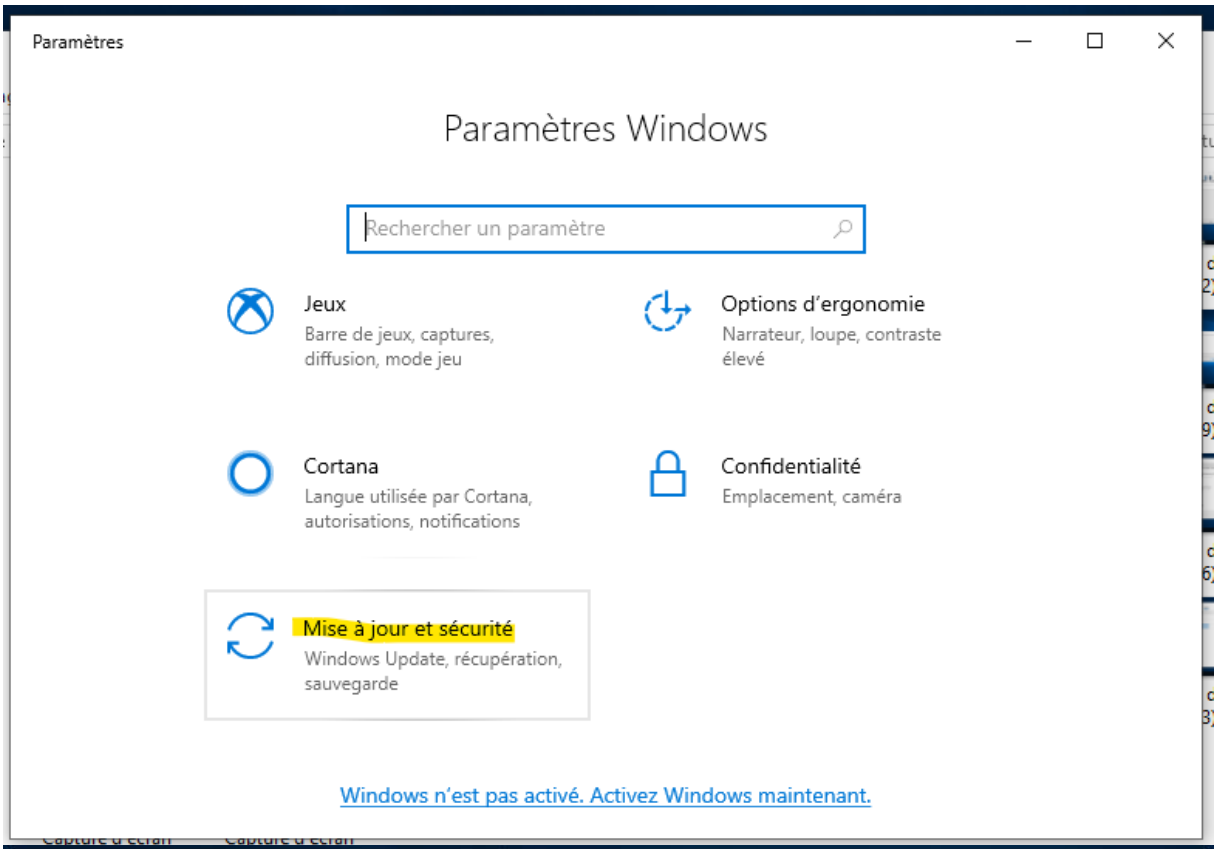

**Il faut saisir un nom de domaine. L'extension de ce nom domaine doit être obligatoirement : .lan / .loc / .dom / .hom / .bur / .ent**

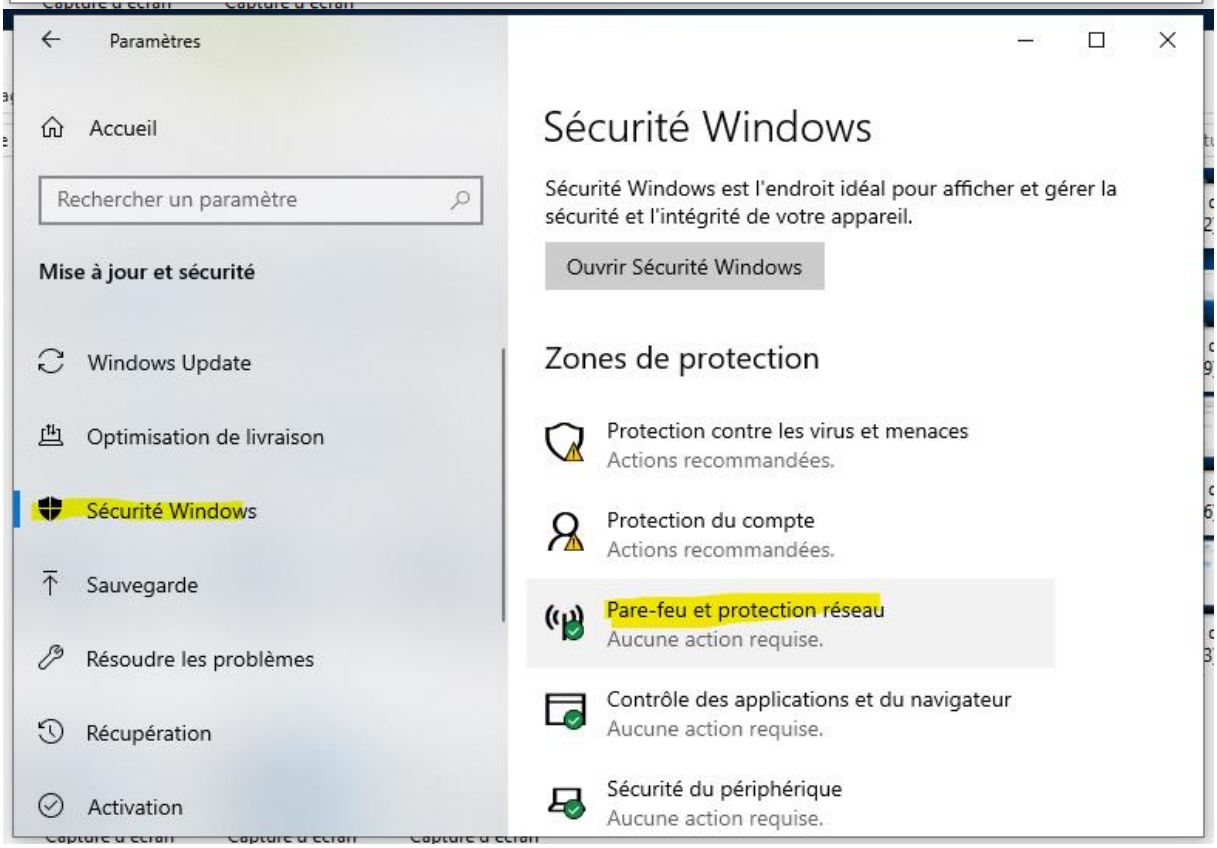


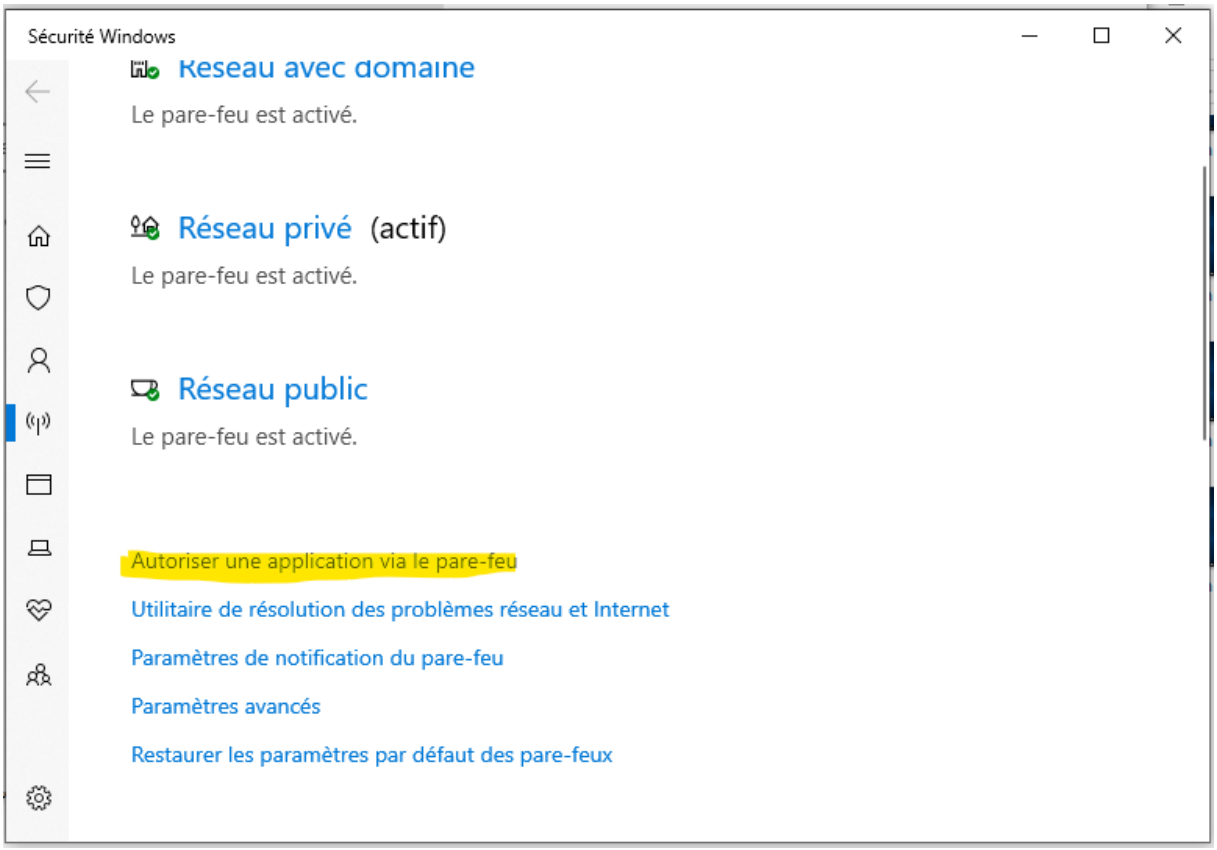

## 4. Gestion de la sécurité

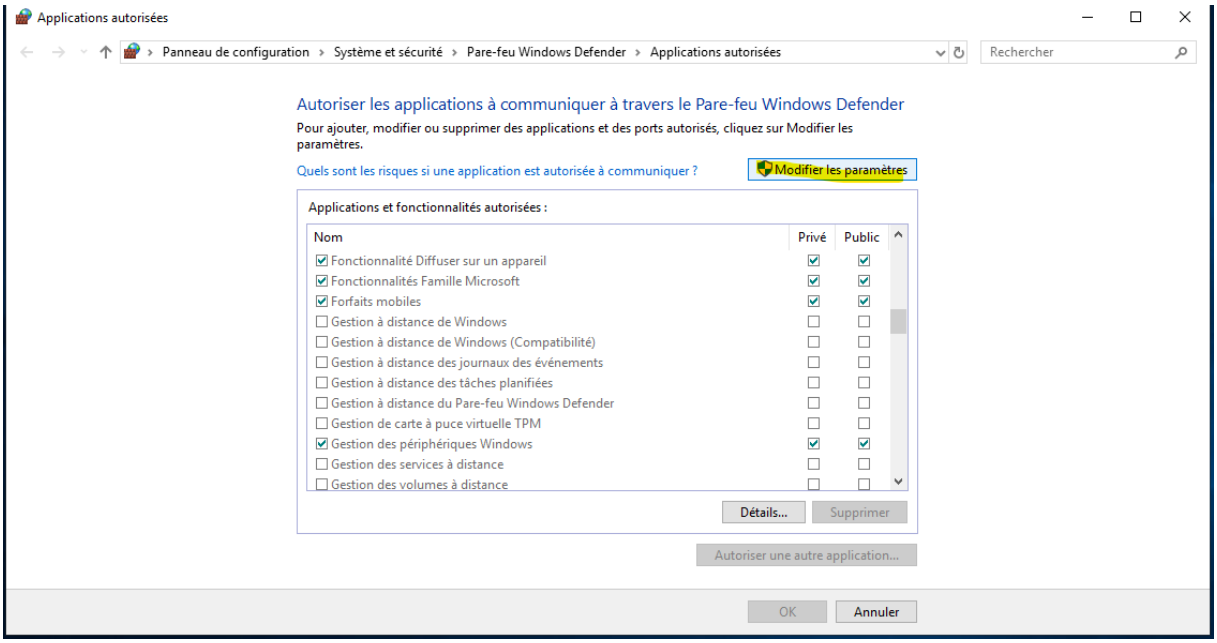
Afin de pouvoir interroger le service depuis une autre machine, il faut autoriser la connexion à hMailServer au niveau du pare-feu (Firewall)

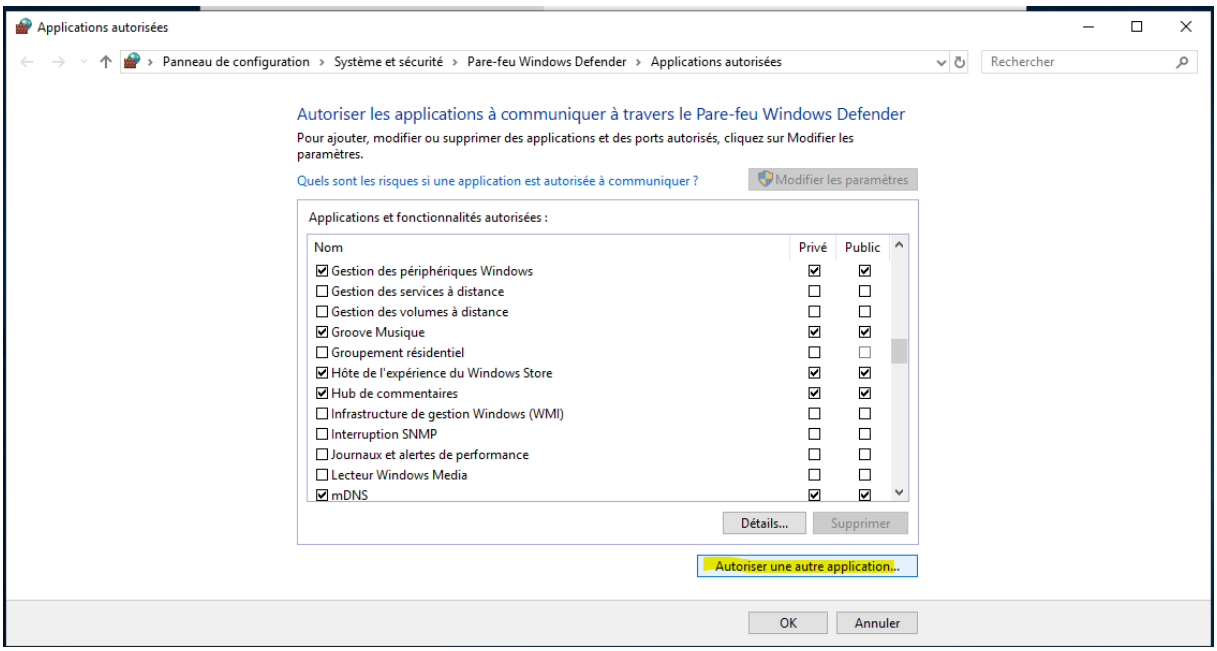


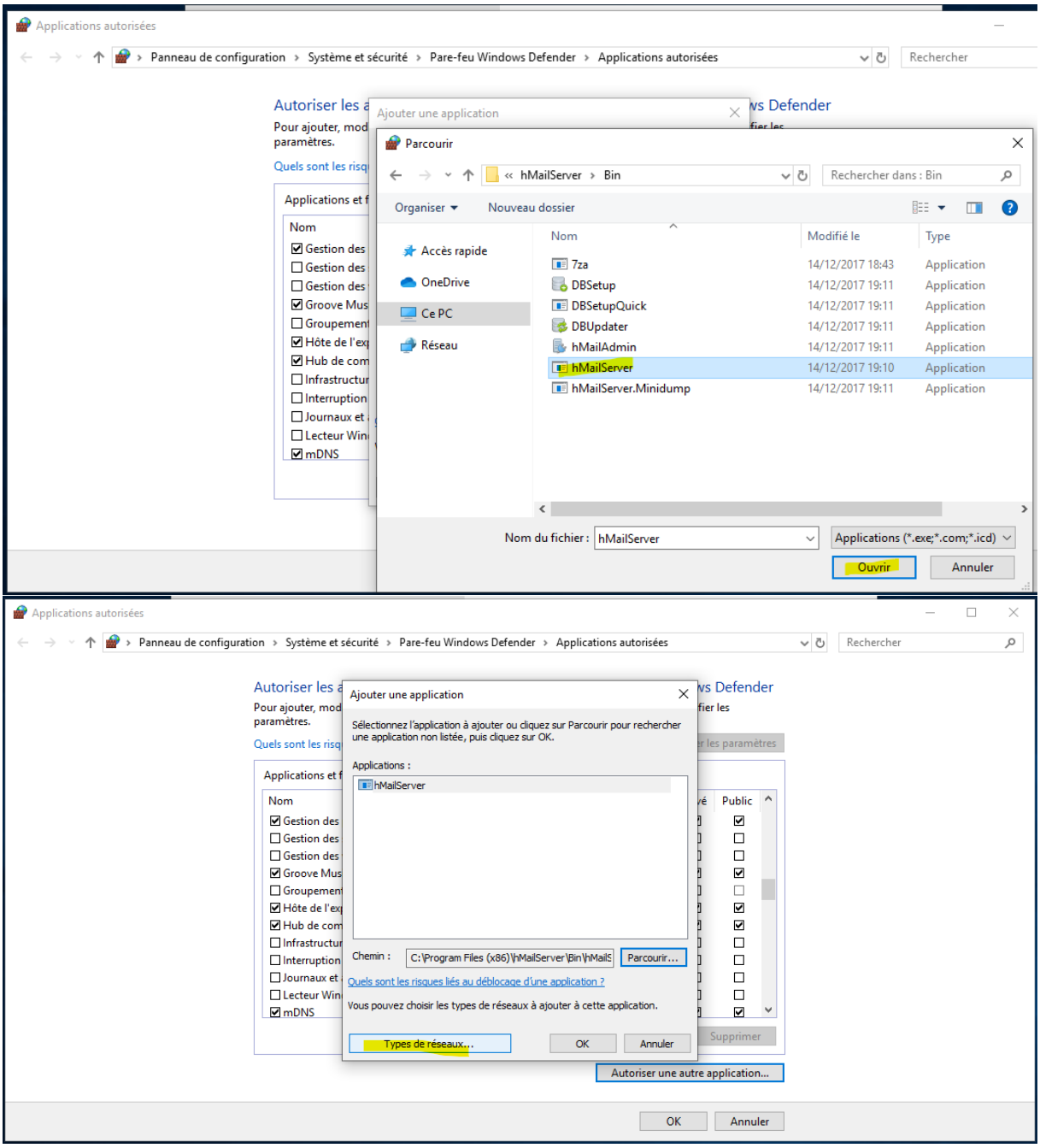

Paramètres
Paramètres Windows
Rechercher un paramètre
Jeux
Barre de jeux, captures, diffusion, mode jeu
Options d'ergonomie
Narrateur, loupe, contraste élevé
Cortana
Langue utilisée par Cortana, autorisations, notifications
Confidentialité
Emplacement, caméra
Mise à jour et sécurité
Windows Update, récupération, sauvegarde
Windows n'est pas activé. Activez Windows maintenant.

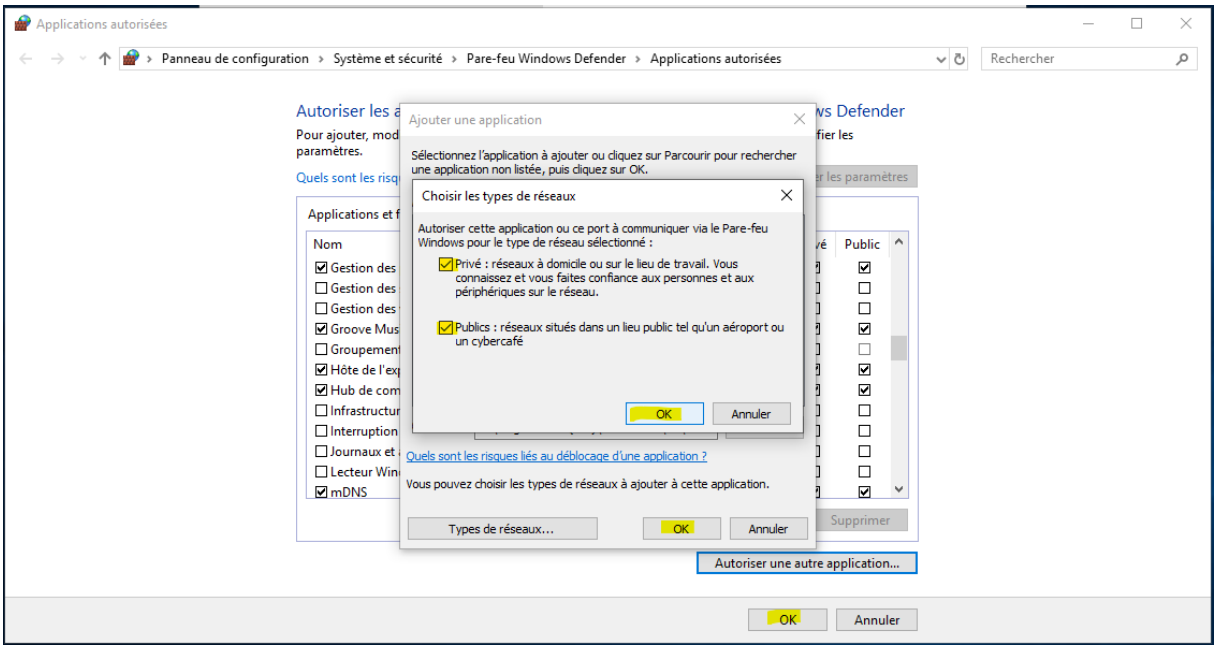

Paramètres
Accueil
Rechercher un paramètre
Mise à jour et sécurité
Windows Update
Optimisation de livraison
Sécurité Windows
Sauvegarde
Résoudre les problèmes
Récupération
Activation
Sécurité Windows
Sécurité Windows est l'endroit idéal pour afficher et gérer la sécurité et l'intégrité de votre appareil.
Ouvrir Sécurité Windows
Zones de protection
Protection contre les virus et menaces
Actions recommandées.
Protection du compte
Actions recommandées.
Pare-feu et protection réseau
Aucune action requise.
Contrôle des applications et du navigateur
Aucune action requise.
Sécurité du périphérique
Aucune action requise.


Sécurité Windows
Réseau avec domaine
Le pare-feu est activé.
Réseau privé (actif)
Le pare-feu est activé.
Réseau public
Le pare-feu est activé.
Autoriser une application via le pare-feu
Utilitaire de résolution des problèmes réseau et Internet
Paramètres de notification du pare-feu
Paramètres avancés
Restaurer les paramètres par défaut des pare-feux

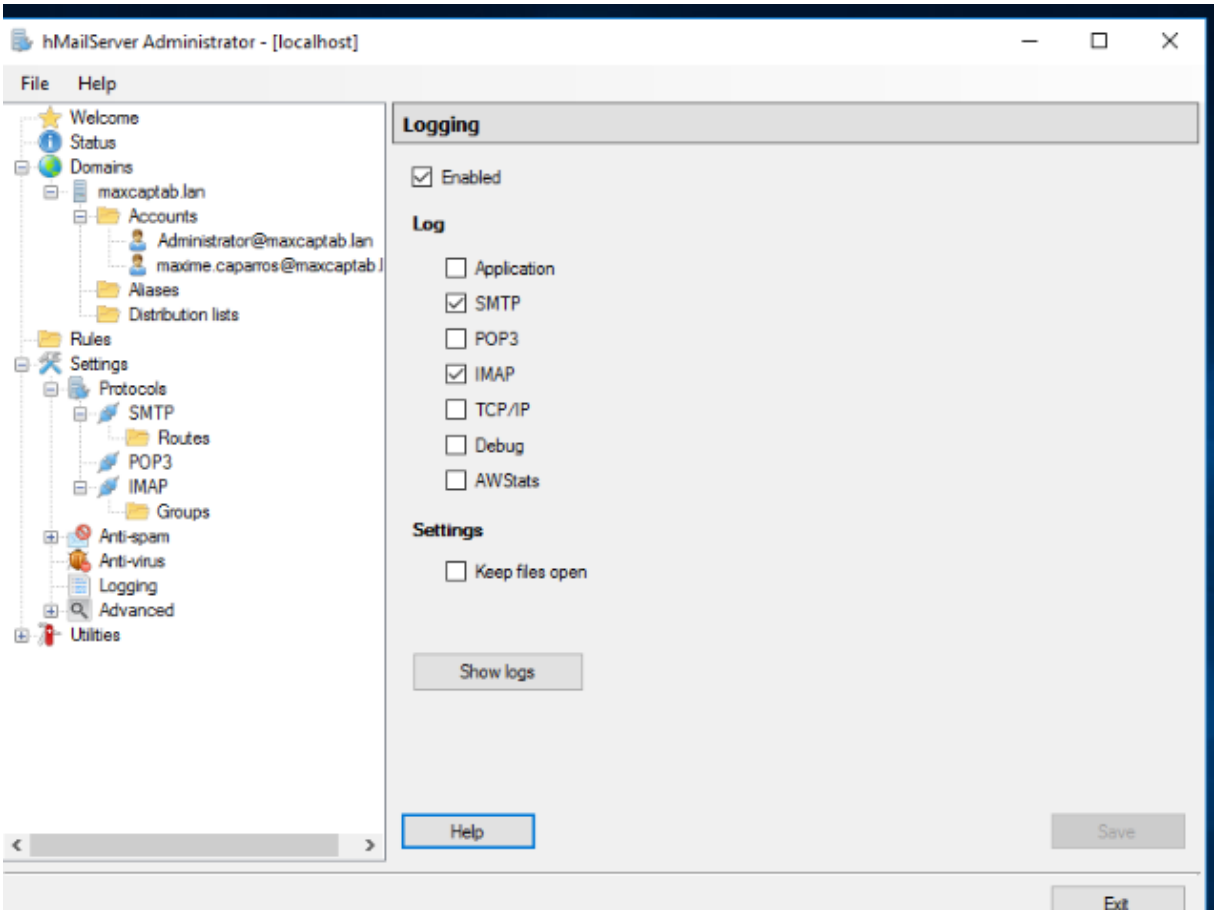

Applications autorisées
Panneau de configuration › Système et sécurité › Pare-feu Windows Defender › Applications autorisées
Rechercher
Autoriser les applications à communiquer à travers le Pare-feu Windows Defender
Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.
Quels sont les risques si une application est autorisée à communiquer ?
Modifier les paramètres
Applications et fonctionnalités autorisées :
Nom
Privé
Public
Fonctionnalité Diffuser sur un appareil
Fonctionnalités Famille Microsoft
Forfaits mobiles
Gestion à distance de Windows
Gestion à distance de Windows (Compatibilité)
Gestion à distance des journaux des événements
Gestion à distance des tâches planifiées
Gestion à distance du Pare-feu Windows Defender
Gestion de carte à puce virtuelle TPM
Gestion des périphériques Windows
Gestion des services à distance
Gestion des volumes à distance
Détails...
Supprimer
Autoriser une autre application...
OK
Annuler


Applications autorisées
Panneau de configuration › Système et sécurité › Pare-feu Windows Defender › Applications autorisées
Rechercher
Autoriser les applications à communiquer à travers le Pare-feu Windows Defender
Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.
Quels sont les risques si une application est autorisée à communiquer ?
Modifier les paramètres
Applications et fonctionnalités autorisées :
Nom
Privé
Public
Gestion des périphériques Windows
Gestion des services à distance
Gestion des volumes à distance
Groove Musique
Groupement résidentiel
Hôte de l'expérience du Windows Store
Hub de commentaires
Infrastructure de gestion Windows (WMI)
Interruption SNMP
Journaux et alertes de performance
Lecteur Windows Media
mDNS
Détails...
Supprimer
Autoriser une autre application...
OK
Annuler


Applications autorisées
Panneau de configuration › Système et sécurité › Pare-feu Windows Defender › Applications autorisées
Rechercher
Autoriser les a
Pour ajouter, mod
paramètres.
Quels sont les risq
Applications et f
Nom
Gestion des
Gestion des
Gestion des
Groove Mus
Groupement
Hôte de l'ex
Hub de com
Infrastructur
Interruption
Journaux et
Lecteur Win
mDNS
Ajouter une application
Parcourir
« hMailServer › Bin
Rechercher dans : Bin
Organiser
Nouveau dossier
Accès rapide
OneDrive
Ce PC
Réseau
Nom
Modifié le
Type
7za
14/12/2017 18:43
Application
DBSetup
14/12/2017 19:11
Application
DBSetupQuick
14/12/2017 19:11
Application
DBUpdater
14/12/2017 19:11
Application
hMailAdmin
14/12/2017 19:11
Application
hMailServer
14/12/2017 19:10
Application
hMailServer.Minidump
14/12/2017 19:11
Application
Nom du fichier : hMailServer
Applications (*.exe;*.com;*.icd)
Ouvrir
Annuler
Applications autorisées
Panneau de configuration › Système et sécurité › Pare-feu Windows Defender › Applications autorisées
Rechercher
Autoriser les a
Pour ajouter, mod
paramètres.
Quels sont les risq
Applications et f
Nom
Public
Gestion des
Gestion des
Gestion des
Groove Mus
Groupement
Hôte de l'ex
Hub de com
Infrastructur
Interruption
Journaux et
Lecteur Win
mDNS
Supprimer
Autoriser une autre application...
OK
Annuler
Ajouter une application
Sélectionnez l'application à ajouter ou cliquez sur Parcourir pour rechercher une application non listée, puis cliquez sur OK.
Applications :
hMailServer
Chemin :
C:\Program Files (x86)\hMailServer\Bin\hMailS
Parcourir...
Quels sont les risques liés au déblocage d'une application ?
Vous pouvez choisir les types de réseaux à ajouter à cette application.
Types de réseaux...
OK
Annuler

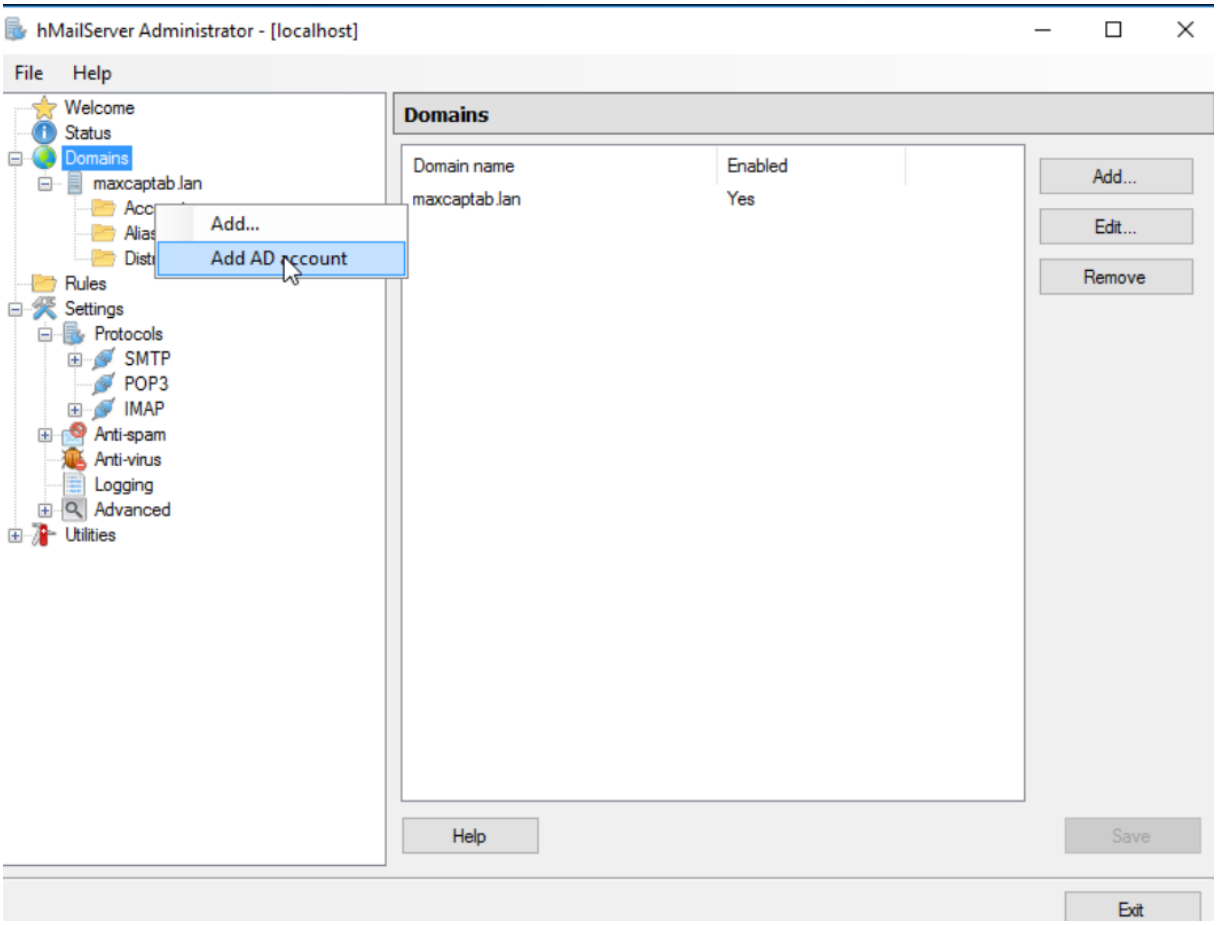


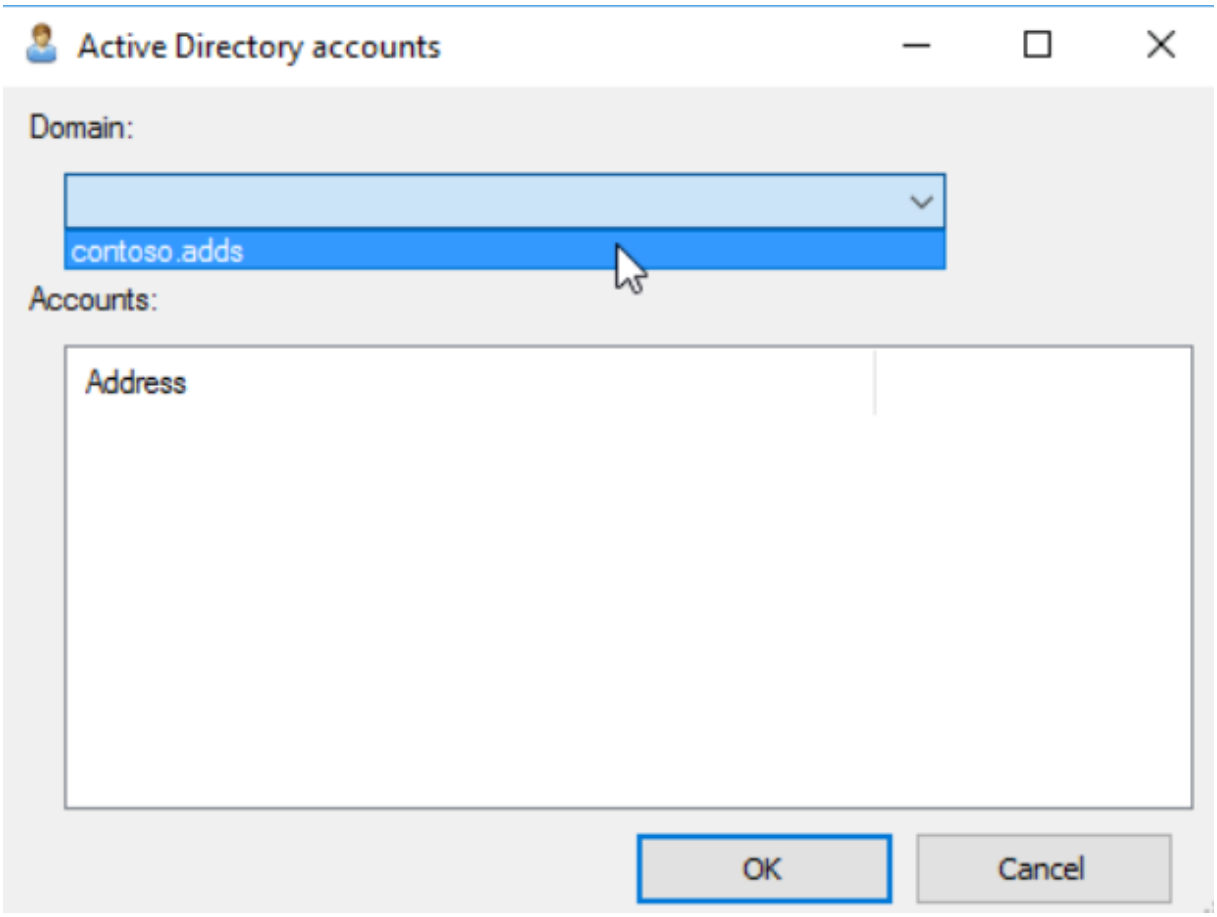

## 5. Gestion des logs

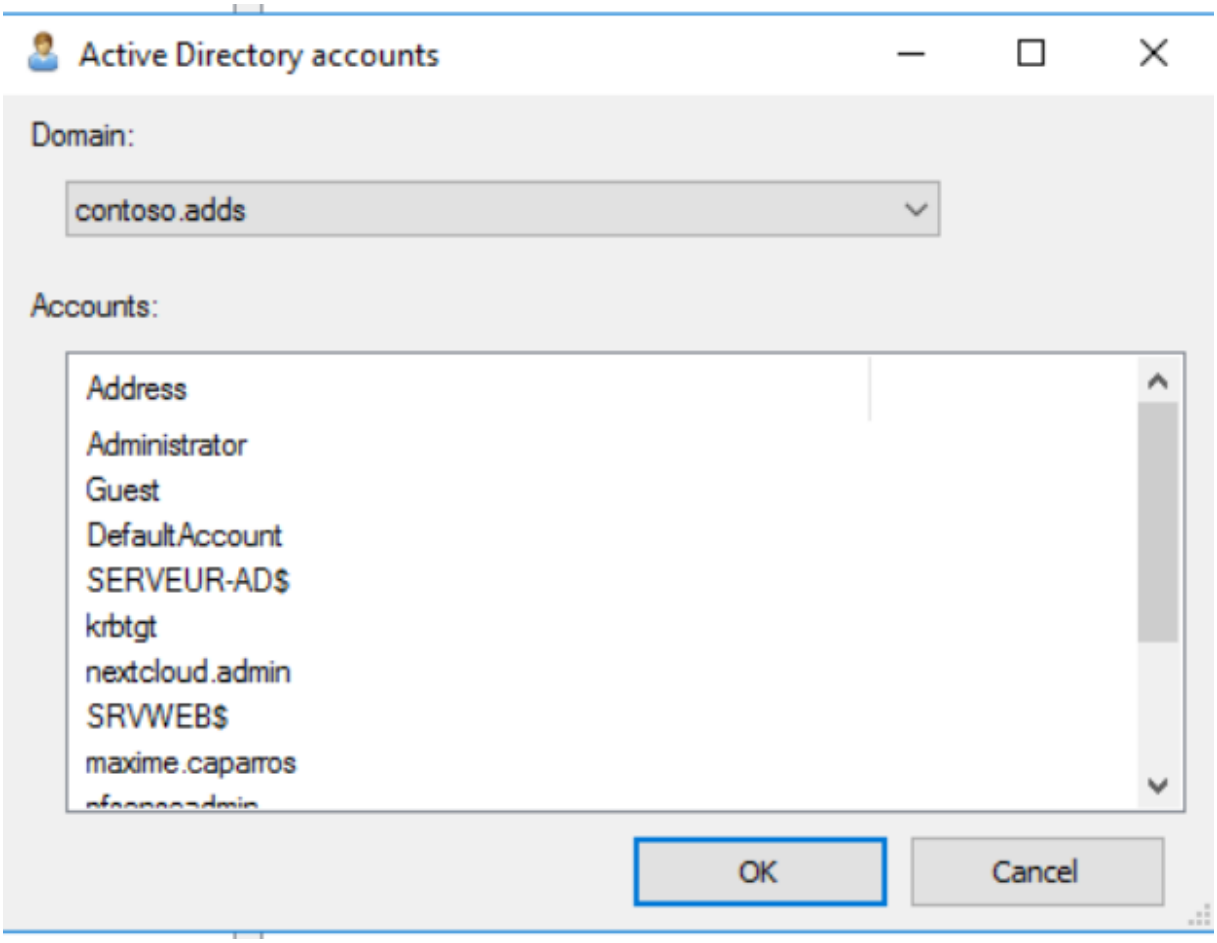



On active les logs qu'on souhaite.

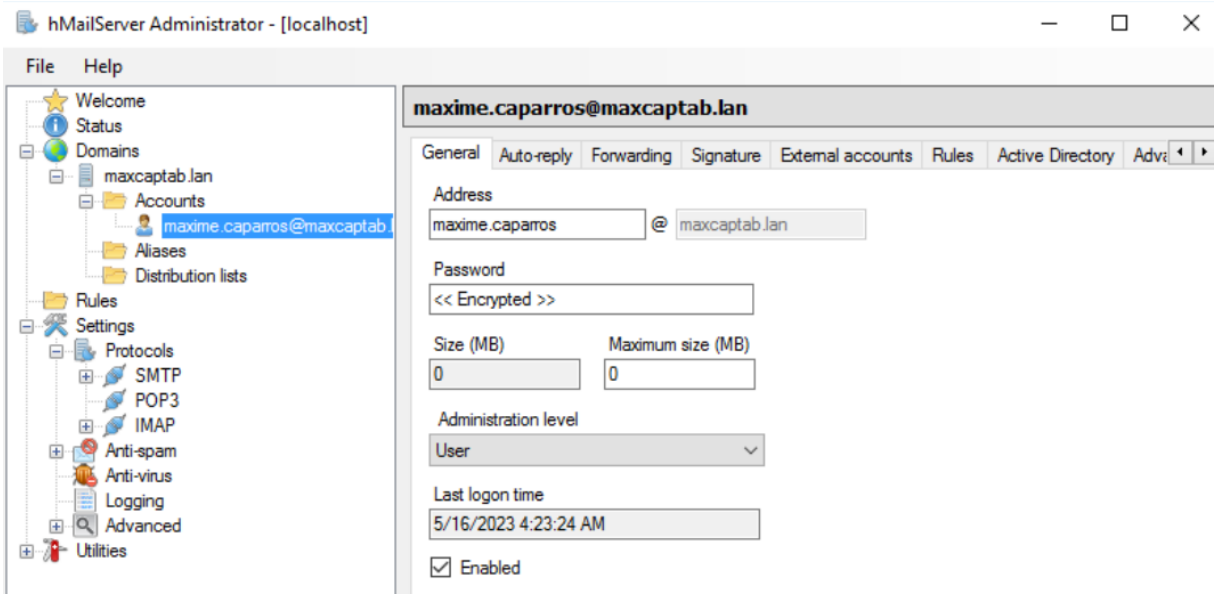
## 6. Ajout d'un utilisateur de l'AD




Active Directory accounts
Domain:
contoso.adds
Accounts:
Address
OK
Cancel


Active Directory accounts
Domain:
contoso.adds
Accounts:
Address
Administrator
Guest
DefaultAccount
SERVEUR-AD$
krbtgt
nextcloud.admin
SRVWEB$
maxime.caparros
OK
Cancel

Choisir un compte puis sélectionnez OK.




Et tout est bon le compte a été créé

# 7. Serveur AD

Pour mettre en place notre serveur AD nous avons créé un serveur windows dans notre réseau lan.

## 1. Objectifs

Voici l'objectif clés de notre serveur AD :

LDAP

## 2. Configuration matérielle

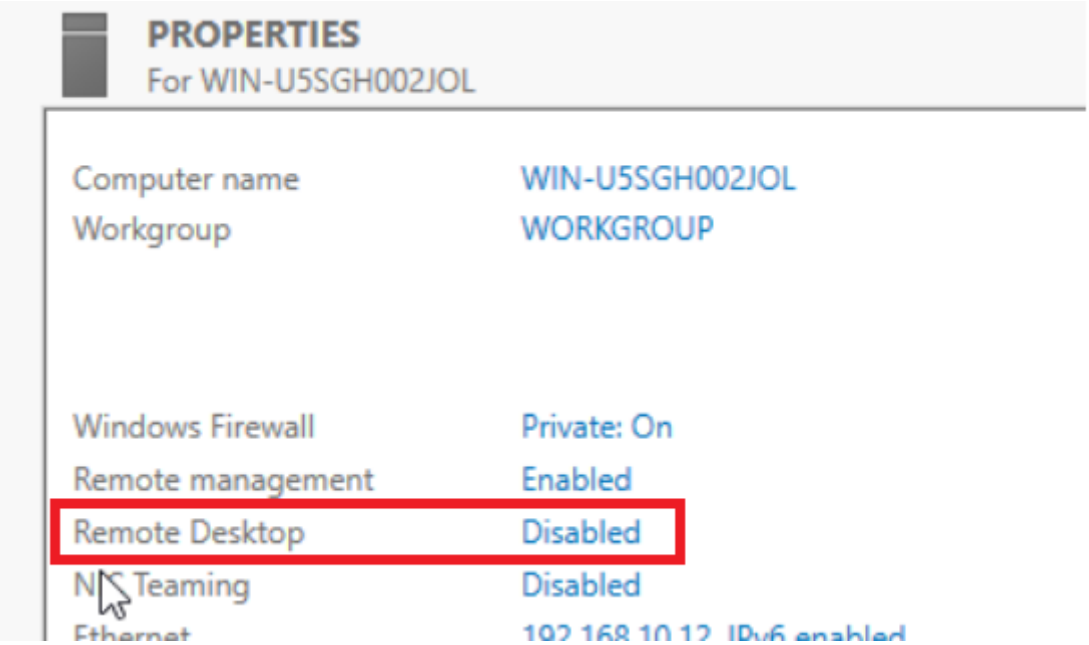
Pour notre serveur AD nous l'avons mis en place sur Proxmox avec la configuration matérielle suivant :

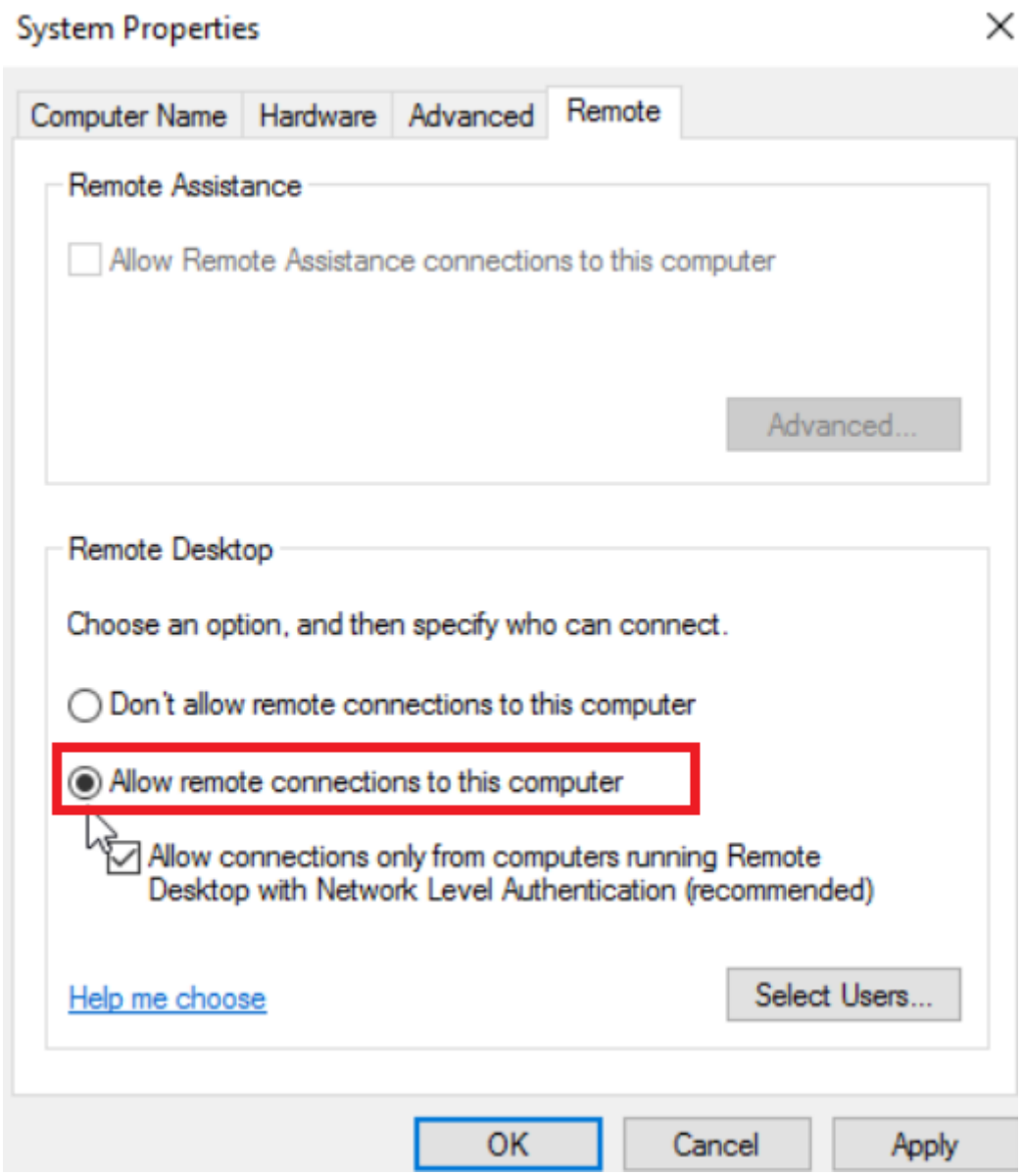
6. 2 Processeur,
7. 1 cœur par processeur
8. 4GB de ram
9. 1 carte réseau
10. 100GB de disque virtuel en SCSI

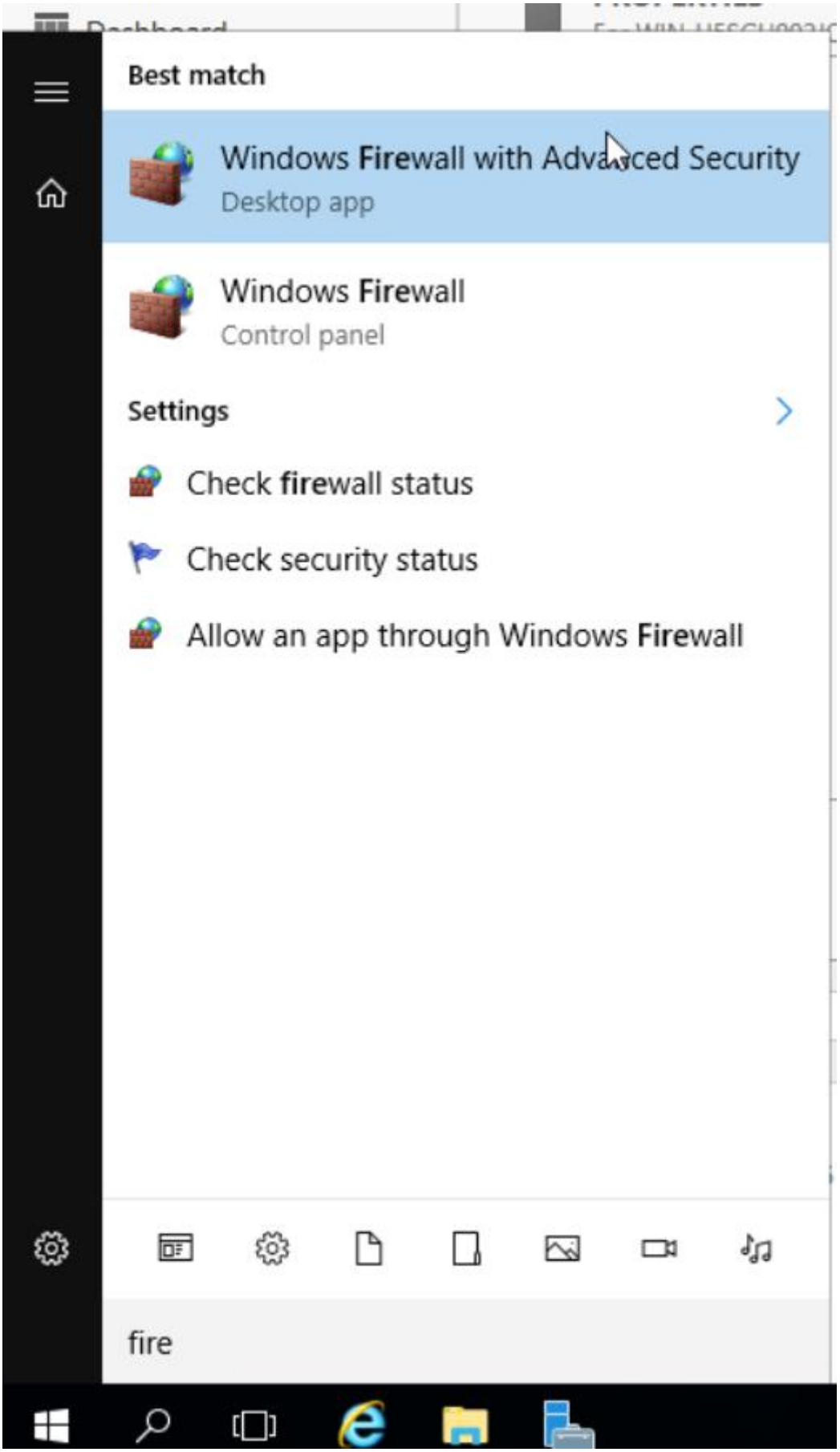
## 3. Configuration logicielle

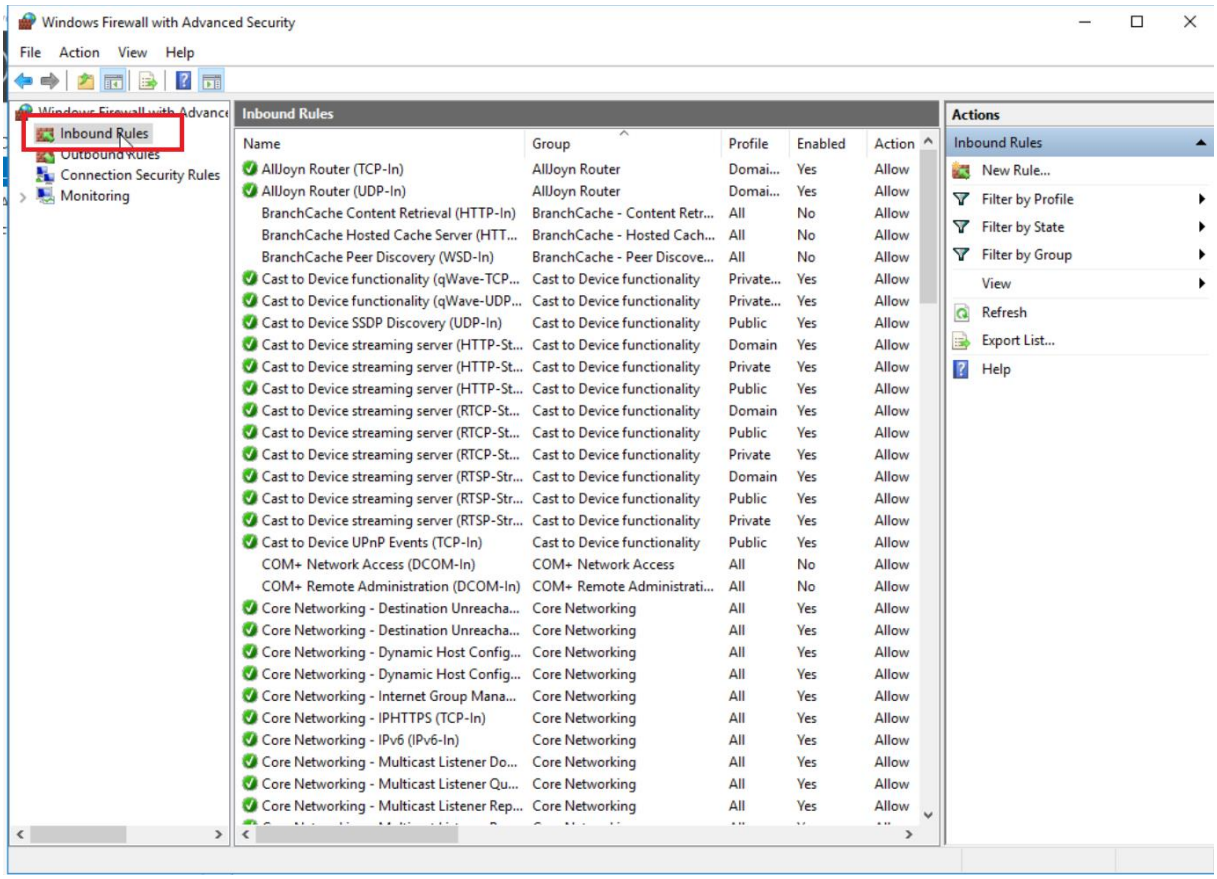
### 1. Remote desktop

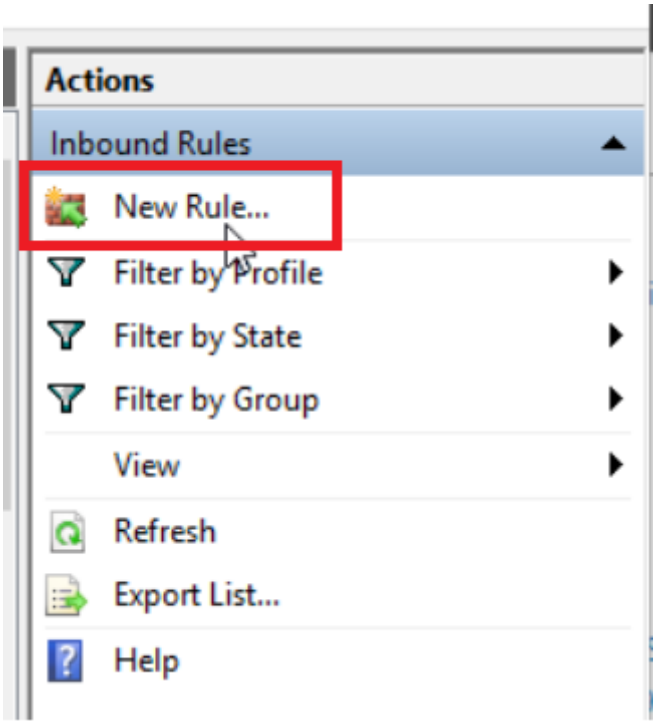
Voici comment activer le RDP sur un serveur windows :

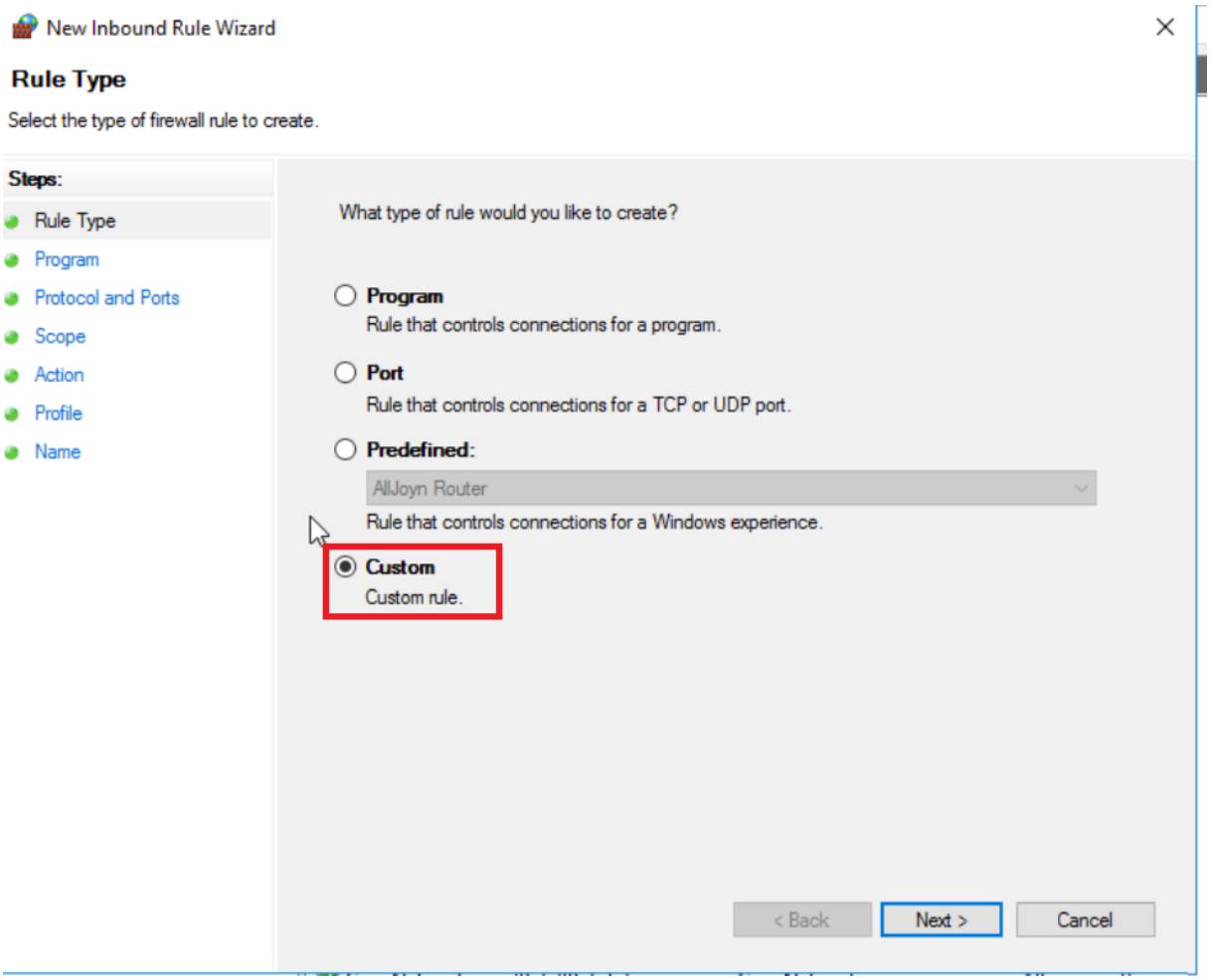


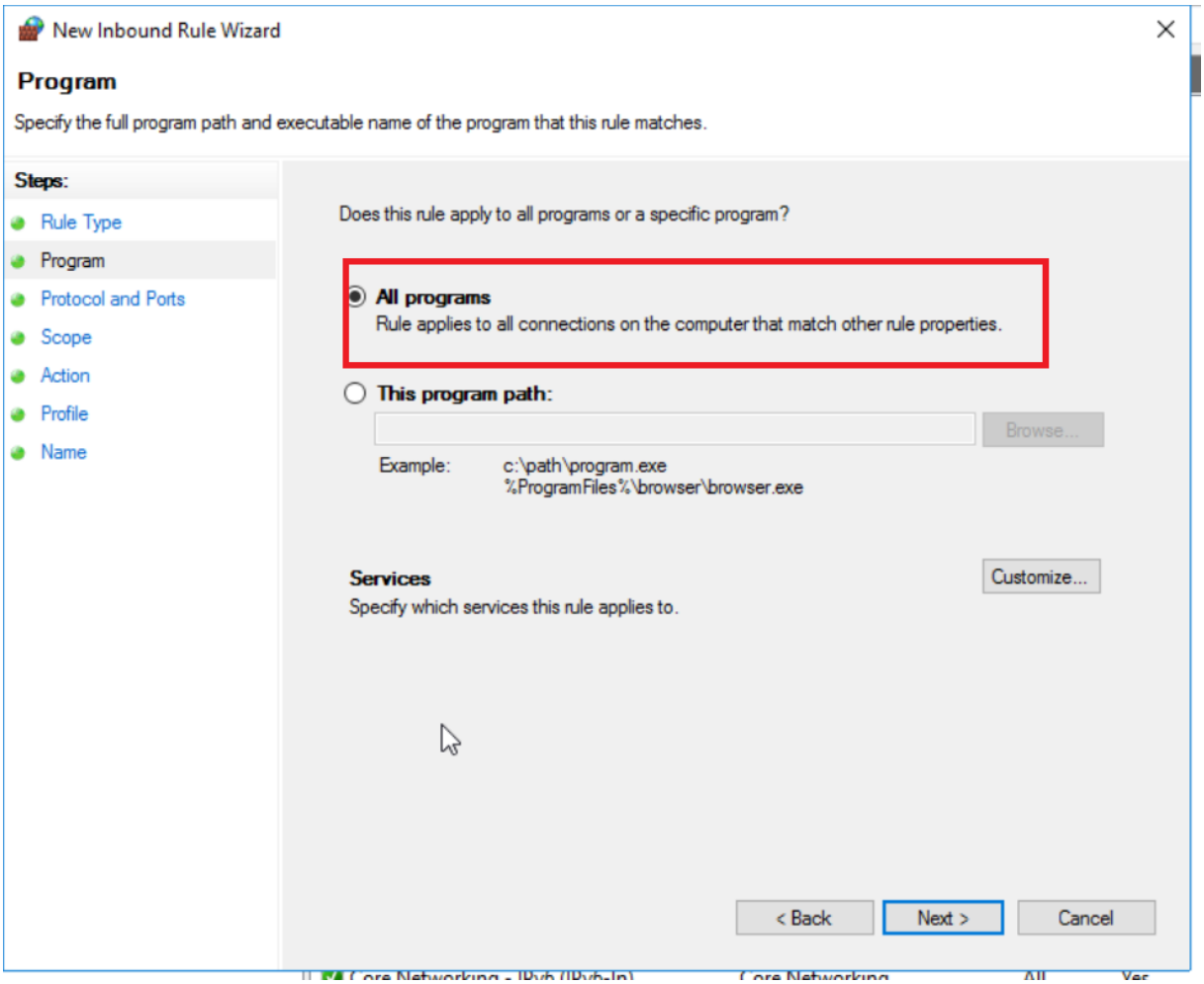

System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply

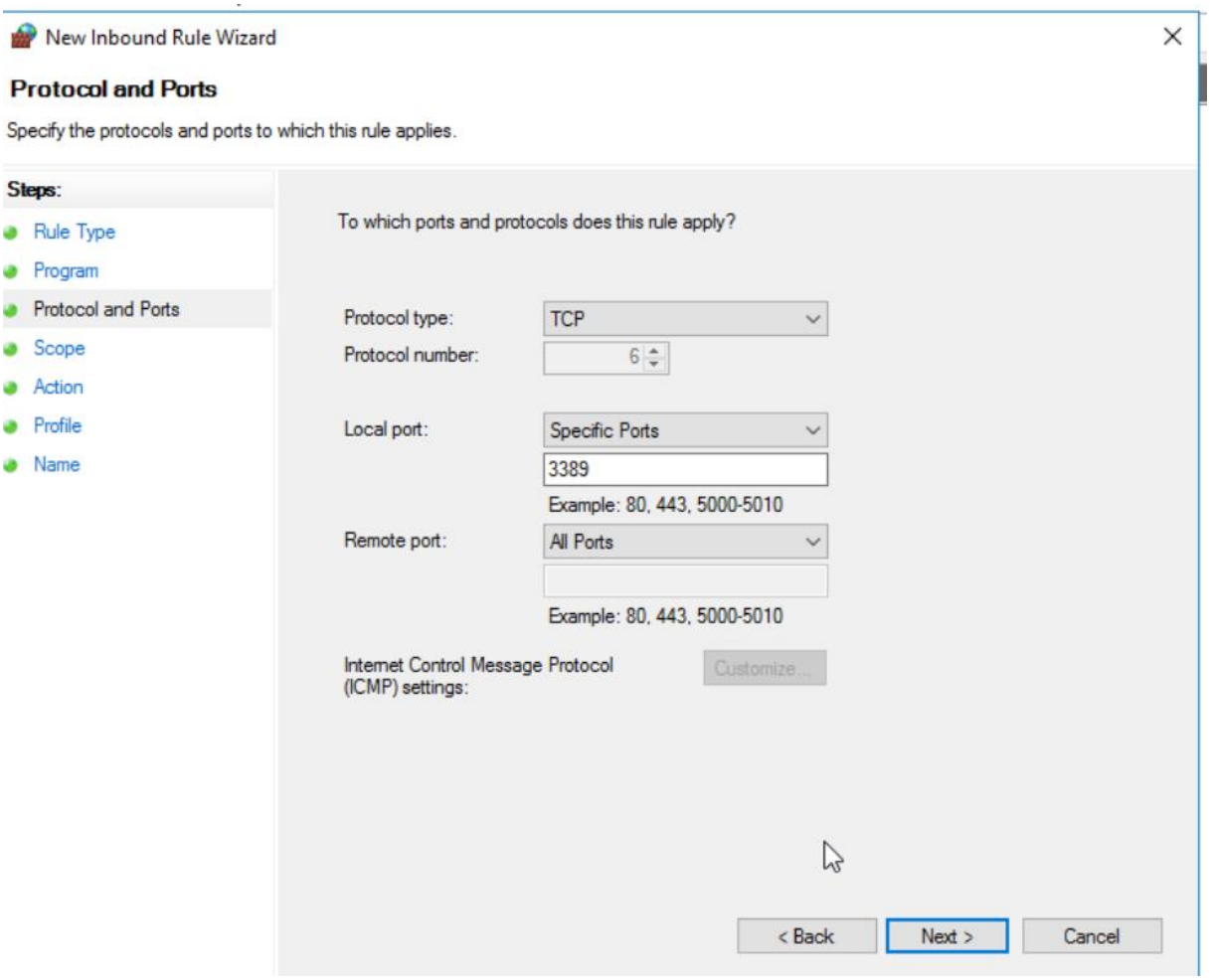

Best match
Windows Firewall with Advanced Security
Desktop app
Windows Firewall
Control panel
Settings
Check firewall status
Check security status
Allow an app through Windows Firewall
fire

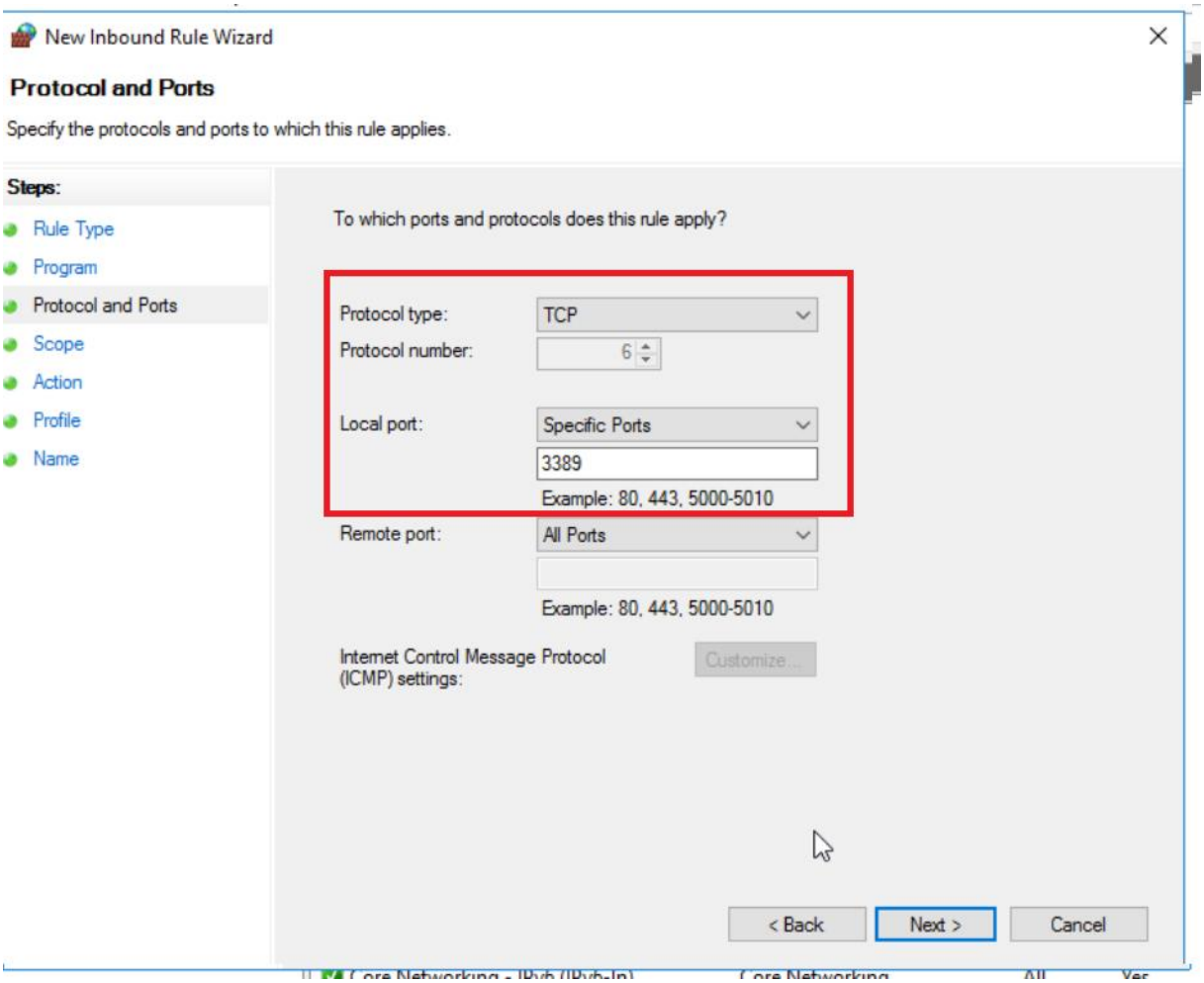

Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes Allow
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes Allow
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No Allow
BranchCache Hosted Cache Server (HTT... BranchCache - Hosted Cach... All No Allow
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No Allow
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes Allow
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes Allow
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Public Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Private Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Public Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Private Yes Allow
Cast to Device UPnP Events (TCP-In) Cast to Device functionality Public Yes Allow
COM+ Network Access (DCOM-In) COM+ Network Access All No Allow
COM+ Remote Administration (DCOM-In) COM+ Remote Administrati... All No Allow
Core Networking - Destination Unreacha... Core Networking All Yes Allow
Core Networking - Destination Unreacha... Core Networking All Yes Allow
Core Networking - Dynamic Host Config... Core Networking All Yes Allow
Core Networking - Dynamic Host Config... Core Networking All Yes Allow
Core Networking - Internet Group Mana... Core Networking All Yes Allow
Core Networking - IPHTTPS (TCP-In) Core Networking All Yes Allow
Core Networking - IPv6 (IPv6-In) Core Networking All Yes Allow
Core Networking - Multicast Listener Do... Core Networking All Yes Allow
Core Networking - Multicast Listener Qu... Core Networking All Yes Allow
Core Networking - Multicast Listener Rep... Core Networking All Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

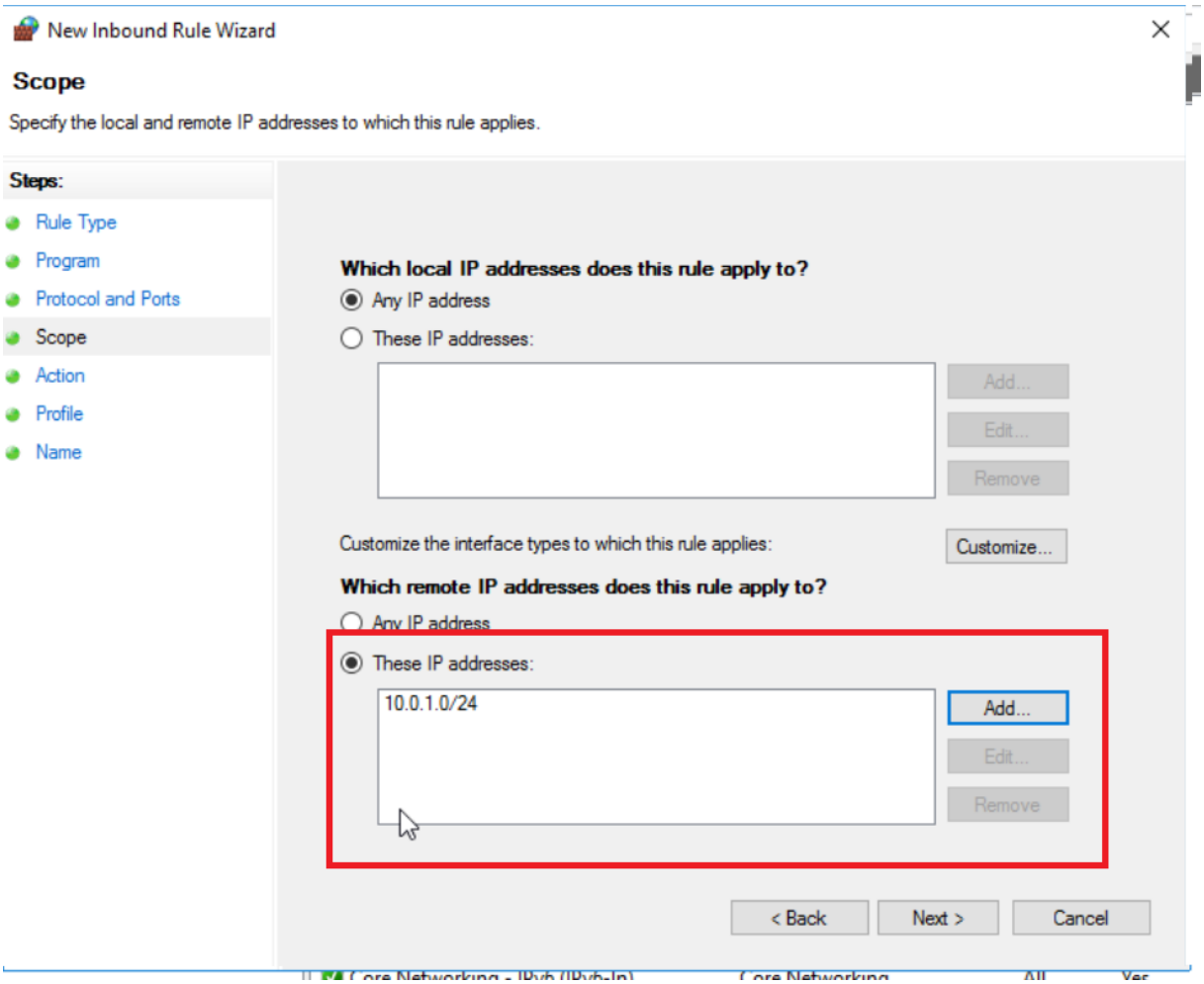

Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

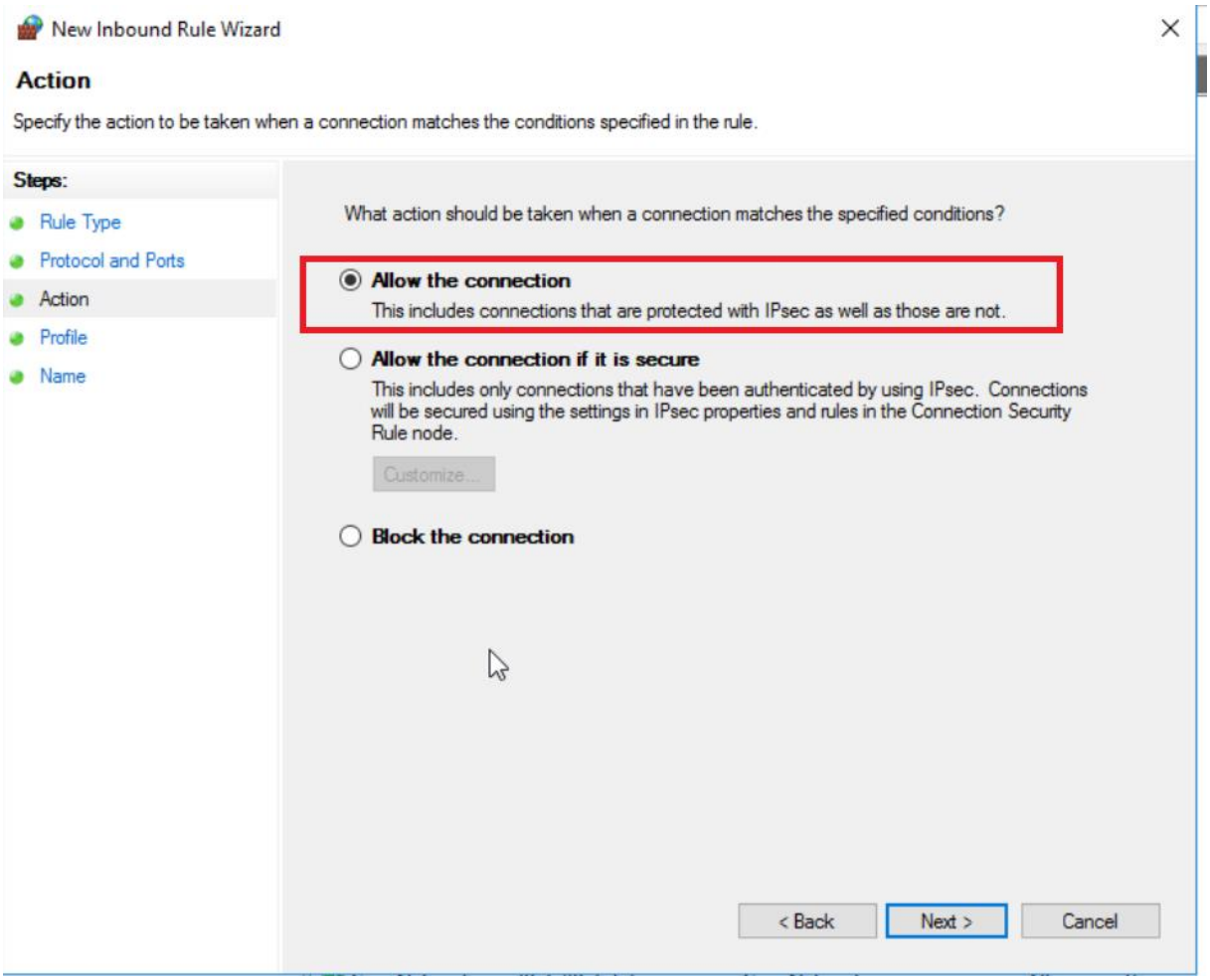

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

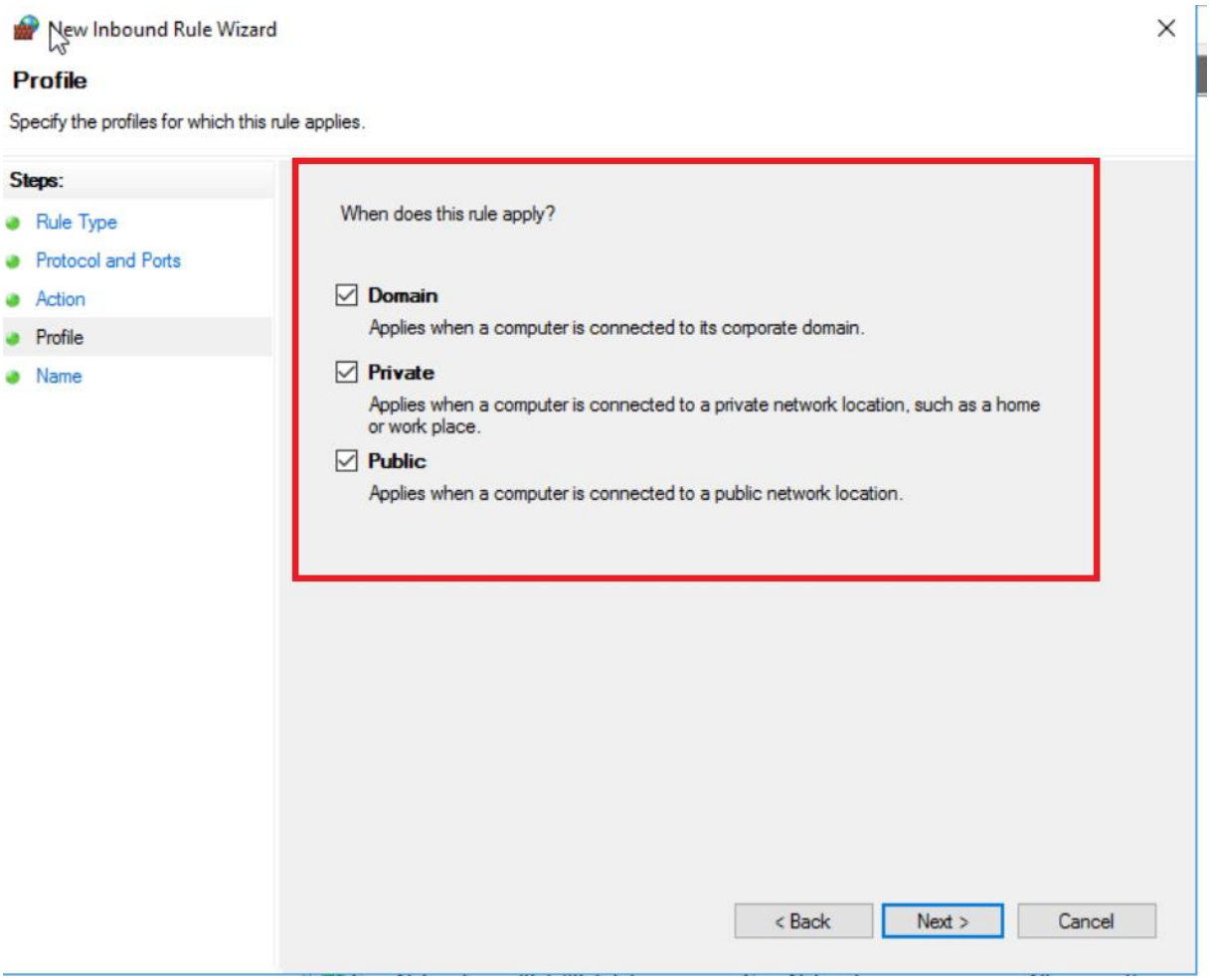

New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel

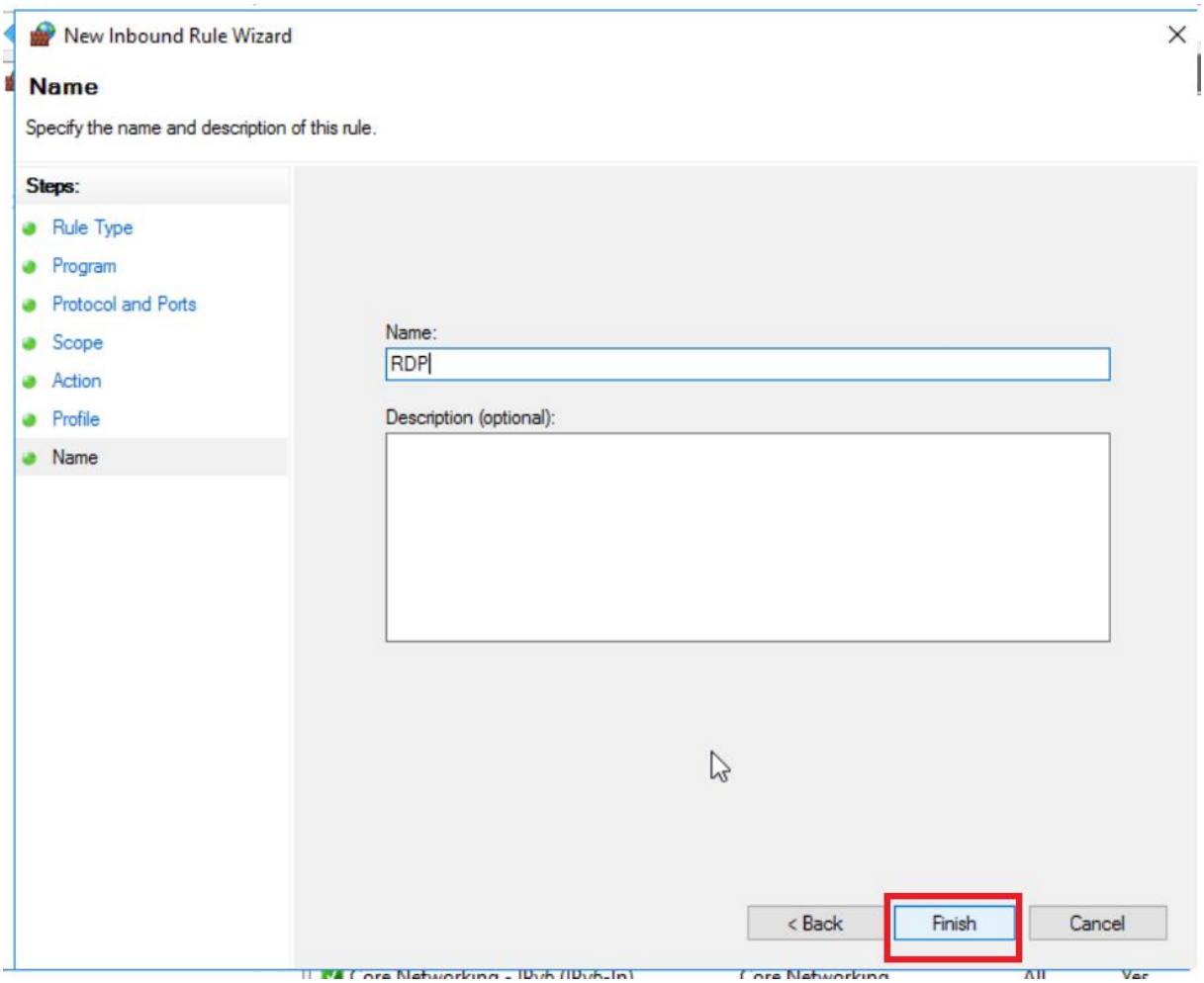

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
TCP
Protocol number:
6
Local port:
Specific Ports
3389
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
TCP
Protocol number:
6
Local port:
Specific Ports
3389
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
10.0.1.0/24
Add...
Edit...
Remove
< Back
Next >
Cancel

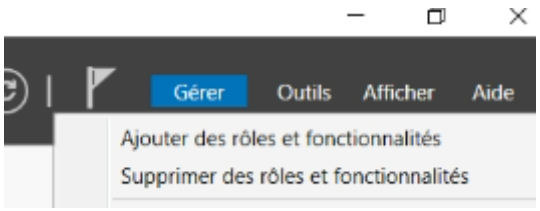

New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel

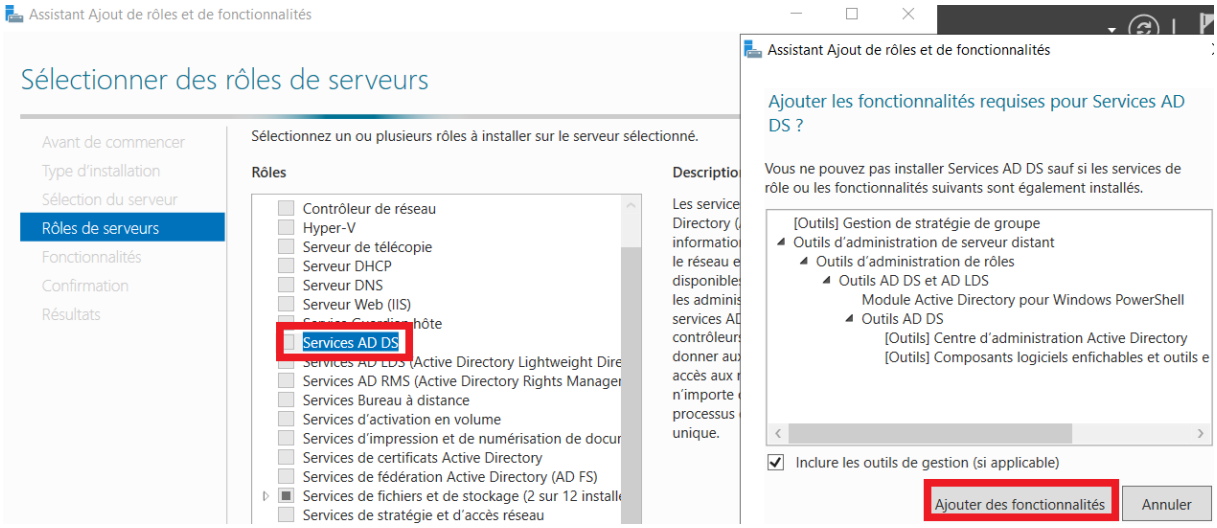



## 2. Installer l'active Directory sur son serveur

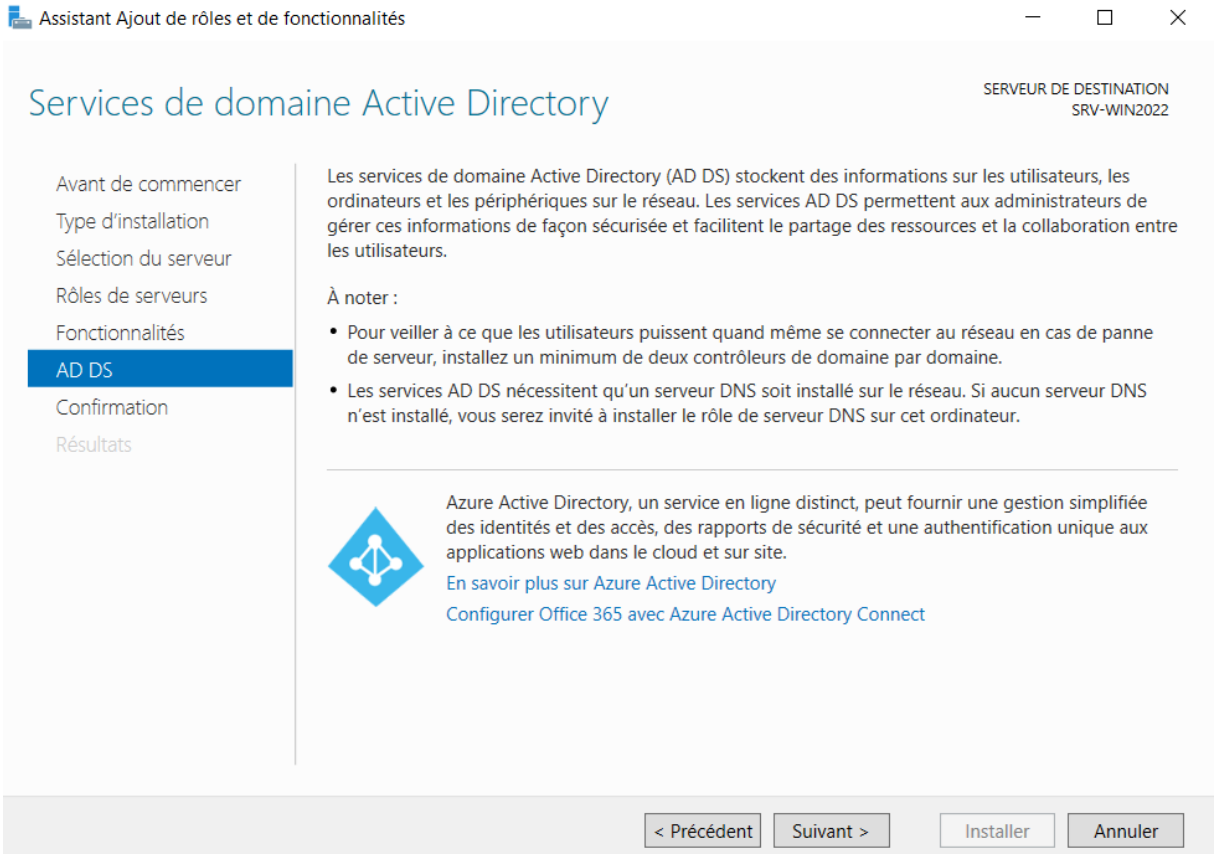
Pour installer l'AD sur son serveur, nous allons installer des rôles et fonctionnalités.



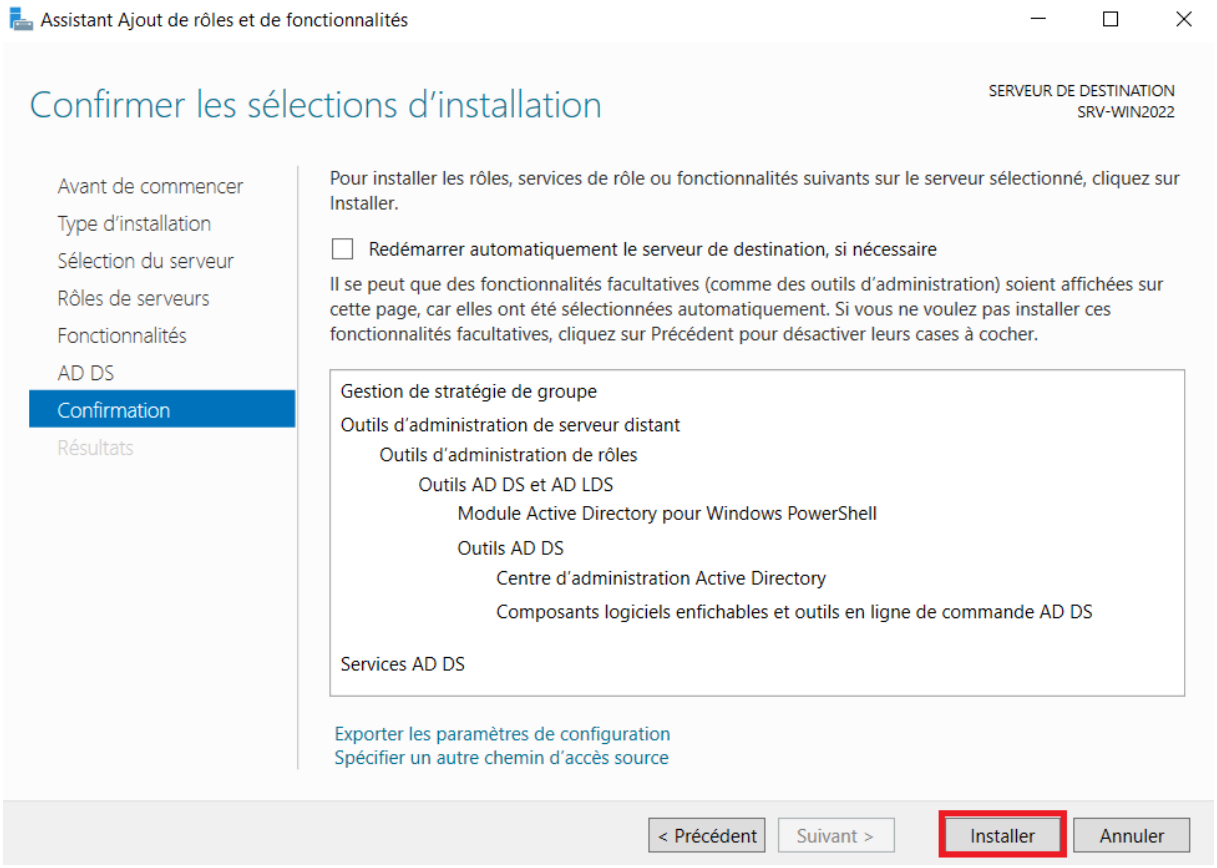

Passer sur suivant jusqu'à arriver à la page rôle de serveurs.
Nous sélectionnons **Services AD DS** puis **Ajouter des fonctionnalités.**
Puis nous passons à la suite.



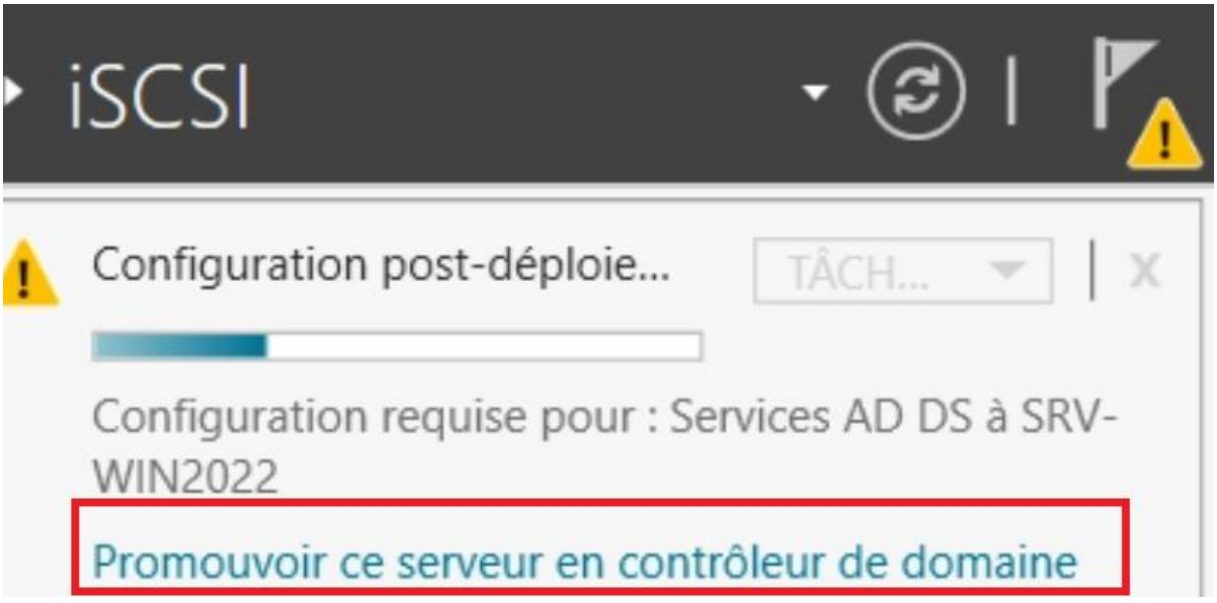

Cette page nous donne des informations sur le service que nous allons installer.



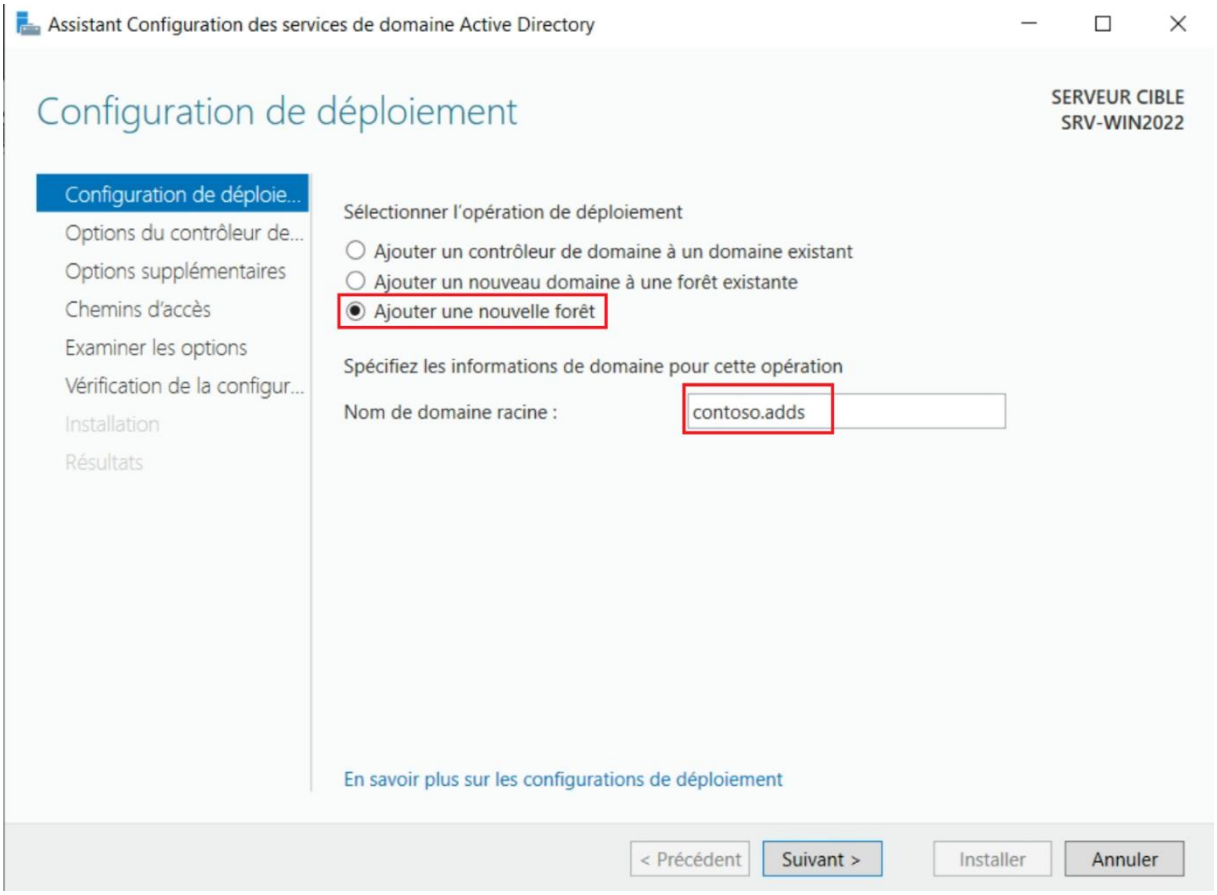

Nous cliquons sur installer.



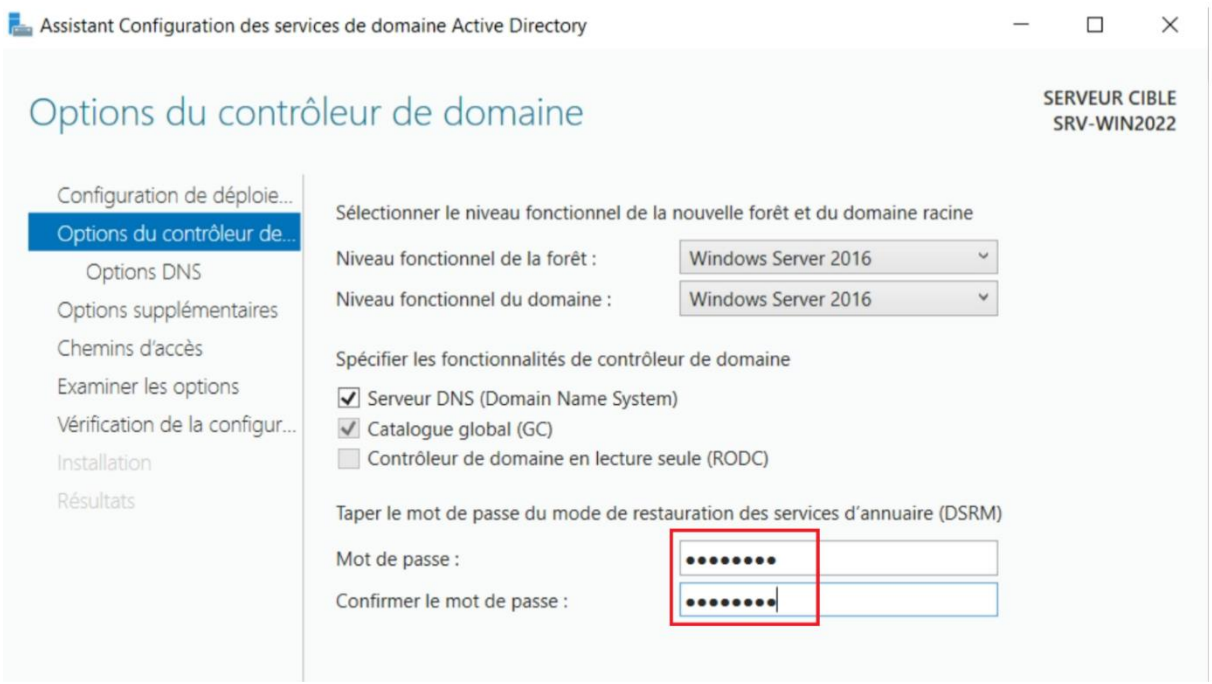

Après l'installation, accédez à l'icône d'avertissement jaune et cliquez sur "Promouvoir ce serveur en contrôleur de domaine" pour démarrer la configuration du contrôleur de domaine.



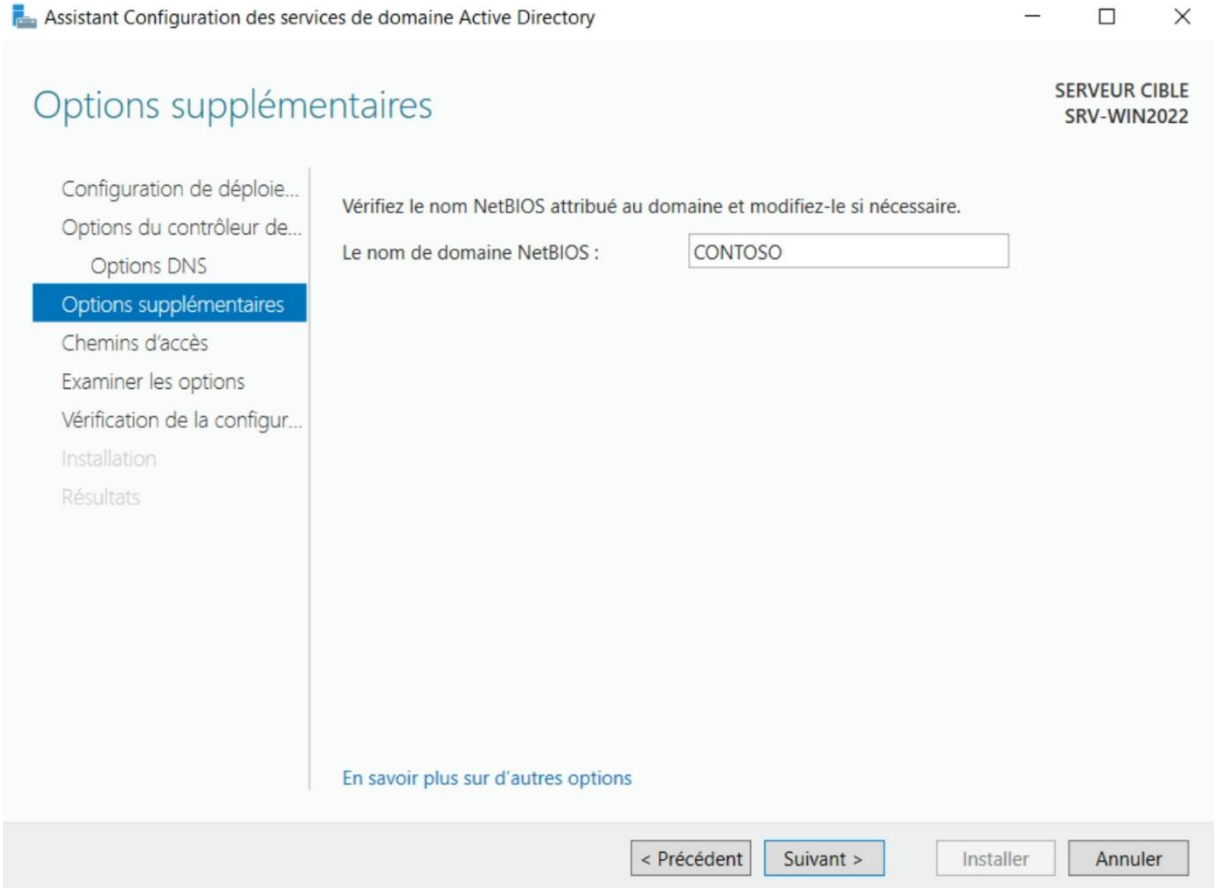
Dans le menu suivant, configurez une nouvelle forêt avec le nom "contoso.adds".



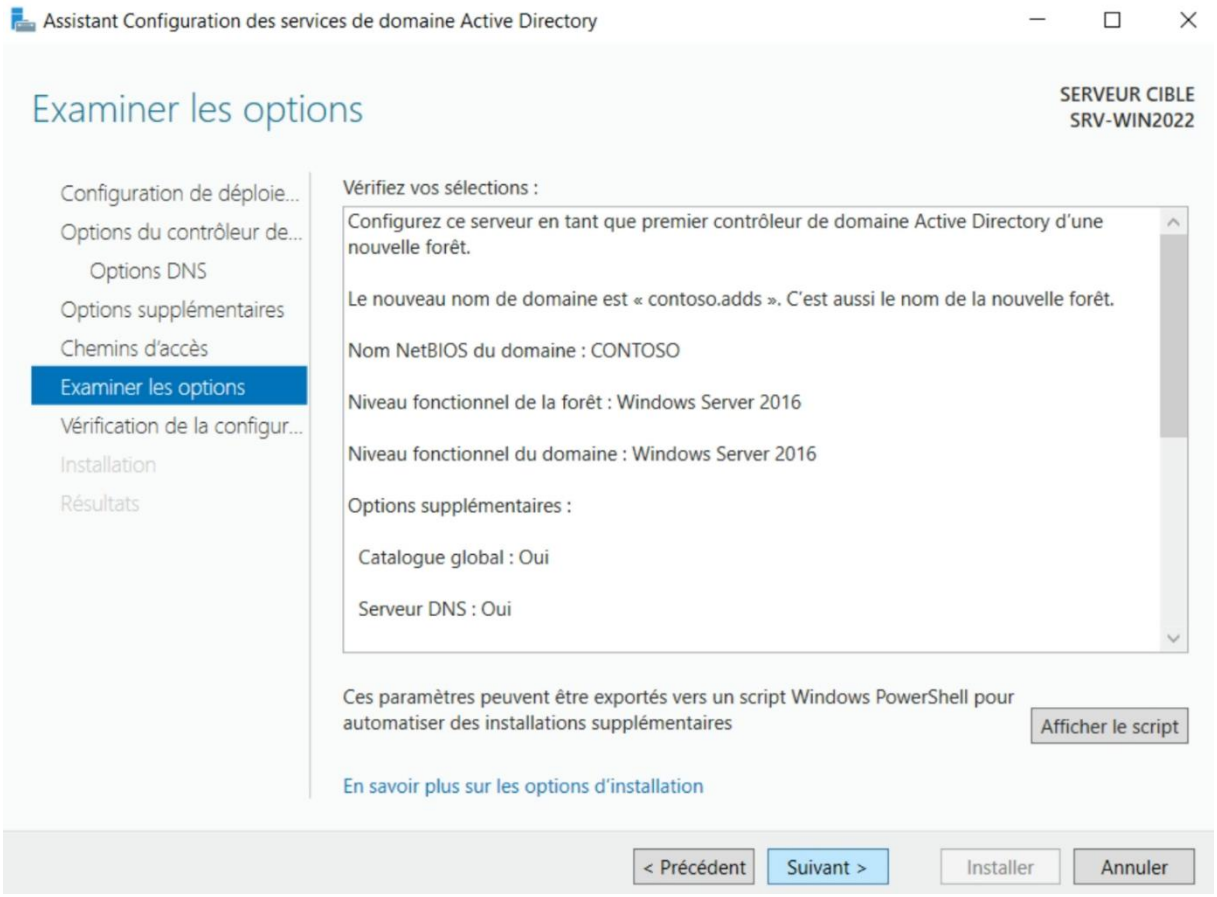

Nous mettons ensuite un mot de passe.



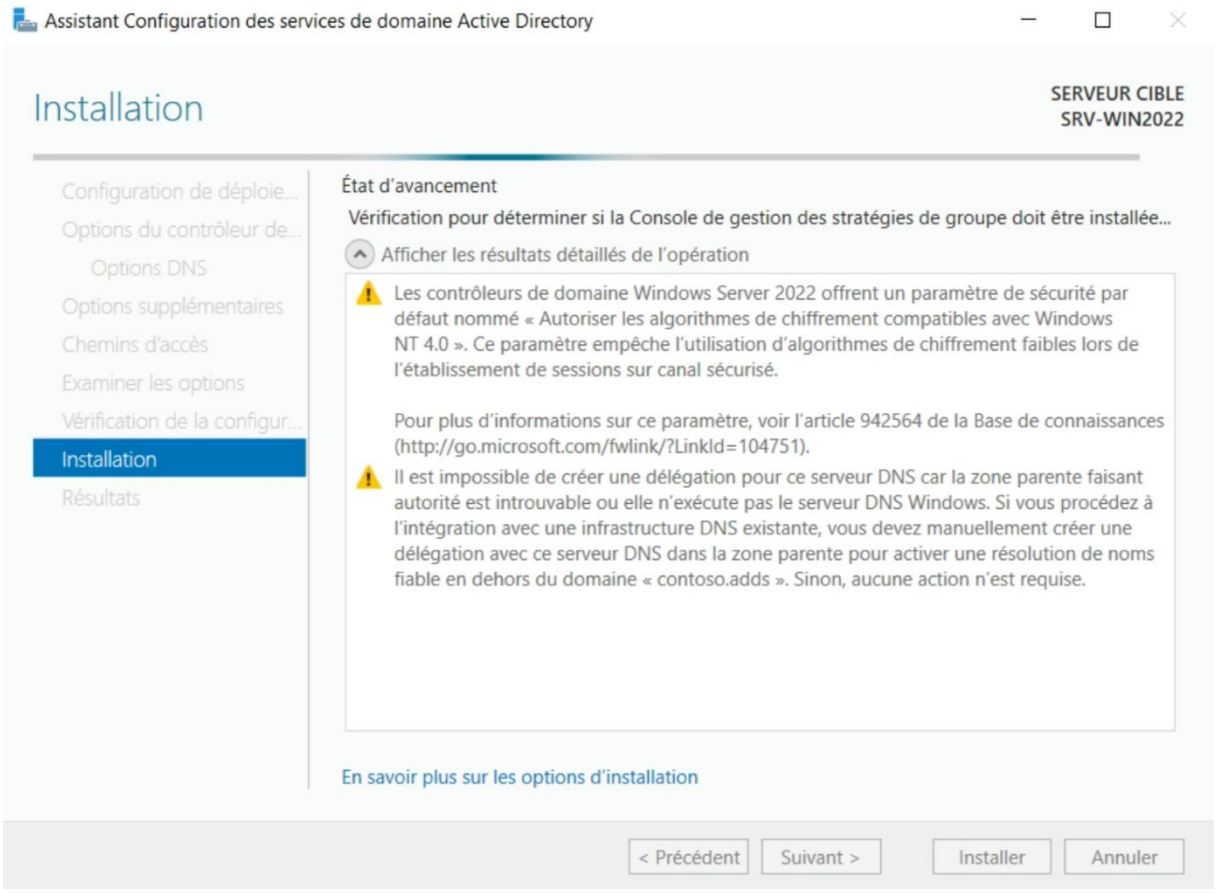

Ici nous mettons CONTOSO.



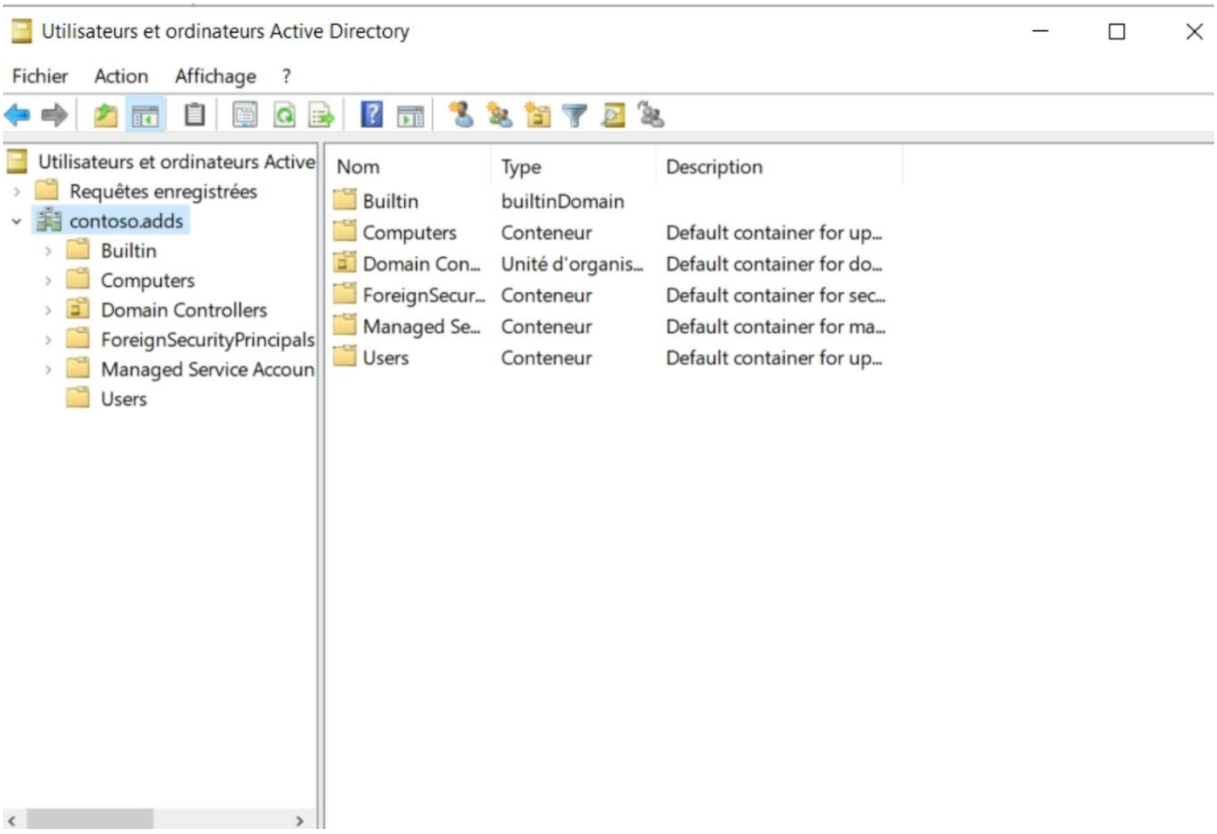
Pour continuer la configuration, cliquez sur "Suivant".




Pour ensuite cliquer sur “Installer”




Une fois l'installation terminée, vous pouvez commencer à utiliser le domaine Active Directory en utilisant la console "Utilisateurs et ordinateurs Active Directory". Cette console vous permet de gérer les objets dans l'annuaire.




# 8. Sauvegarde/Backup

## 7.1 Objectifs

## 7.2 Choix materiel

Pour effectuer nos backups nous utiliserons un NAS (Network Attached Storage)  Terra Master F4-210.
Nous ferons en sorte d'y stocker les backups de nos serveurs PFsense, Windows serveur et Ubuntu.

### Choix technologie

Pour la technologie utilisée pour effectuer nos backups, nous avons choisi entre deux :
 Windows Backup et VEEAM
Nous avons fait notre choix selon le tableau de pondération suivant

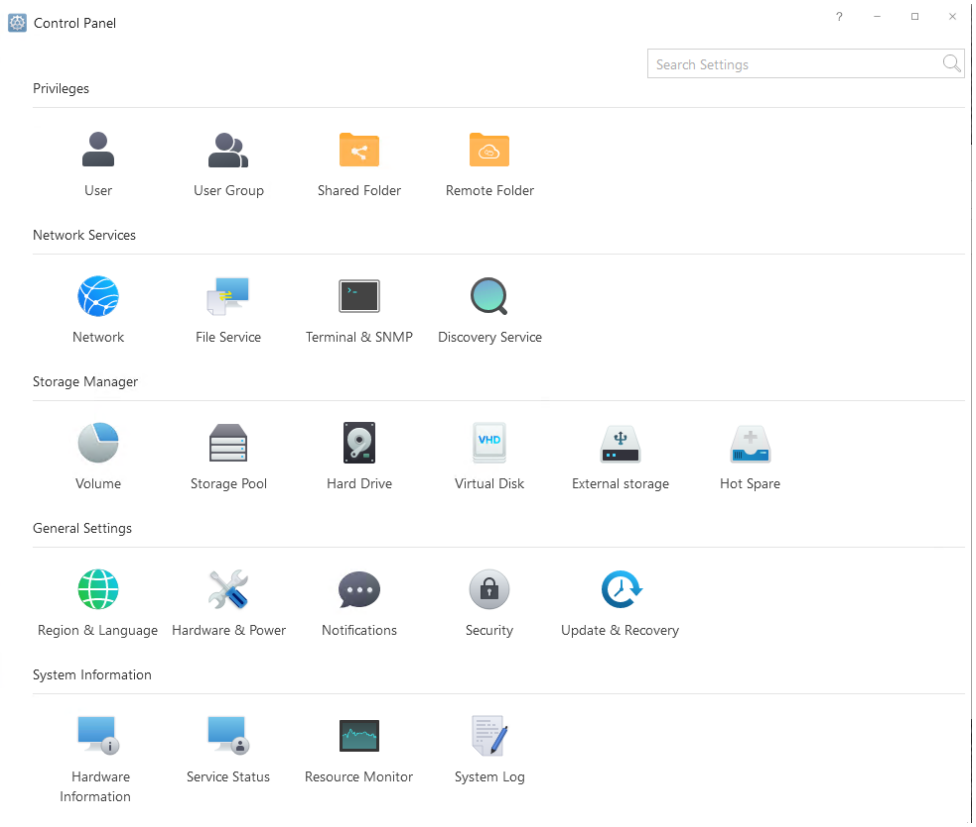
| | Capacité de stockage | Performances | Facilité d'utilisation | Coût | Total /20 |
|---|---|---|---|---|---|
| Pondération | 4 | 3 | 5 | 4 | |
| Windows backup | 4 | 3 | 3 | 3 | 13 |
| VEEAM Agent Windows | 4 | 4 | 5 | 5 | 18 |

Il en ressort donc que notre choix se tourneras vers VEEAM.

## 7.3 Mise en place de la solution

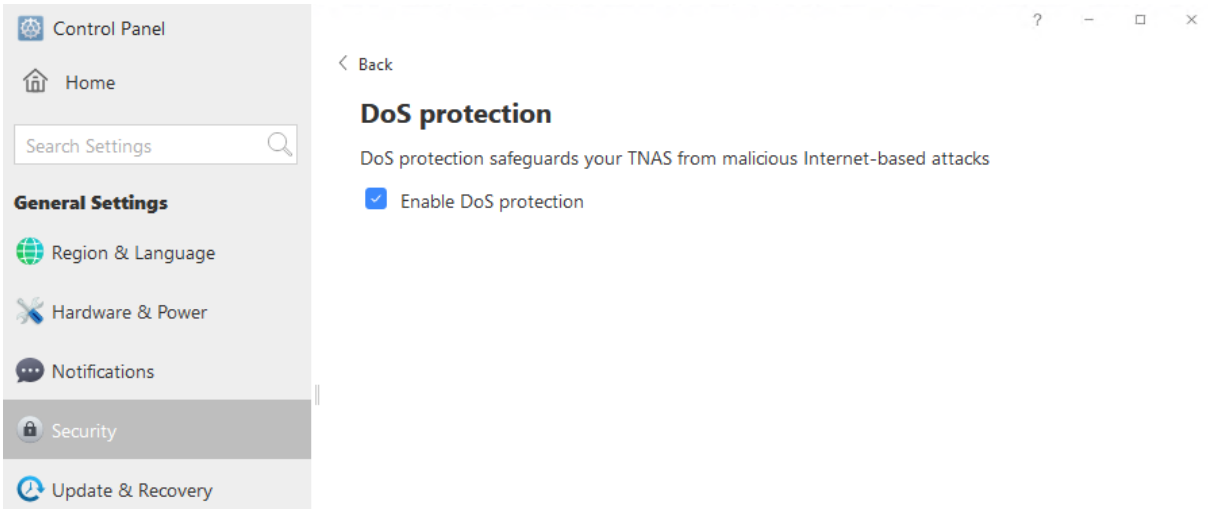
### Le NAS

Nous avons commencé par paramétrer notre NAS via les options du panneau de contrôle

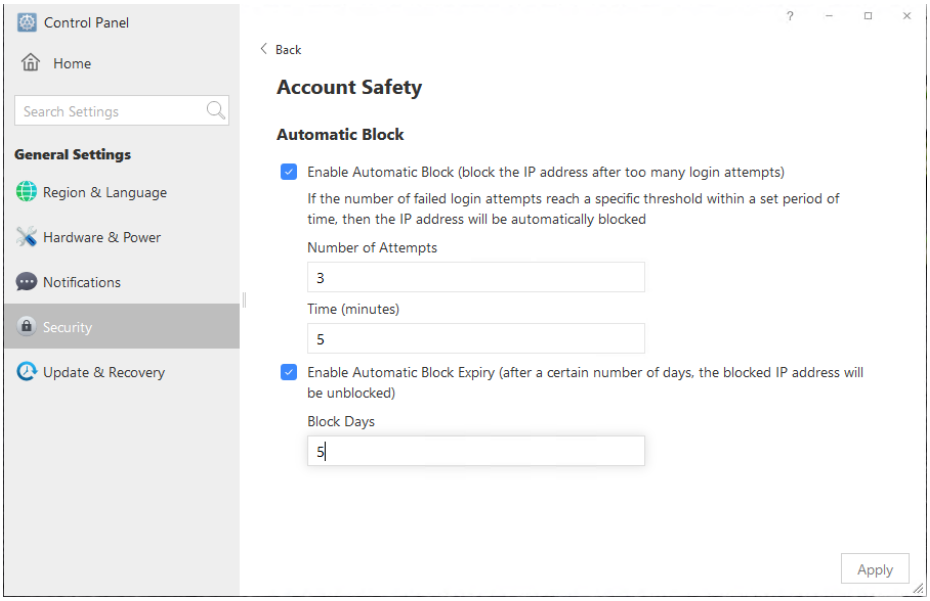



- La sécurité

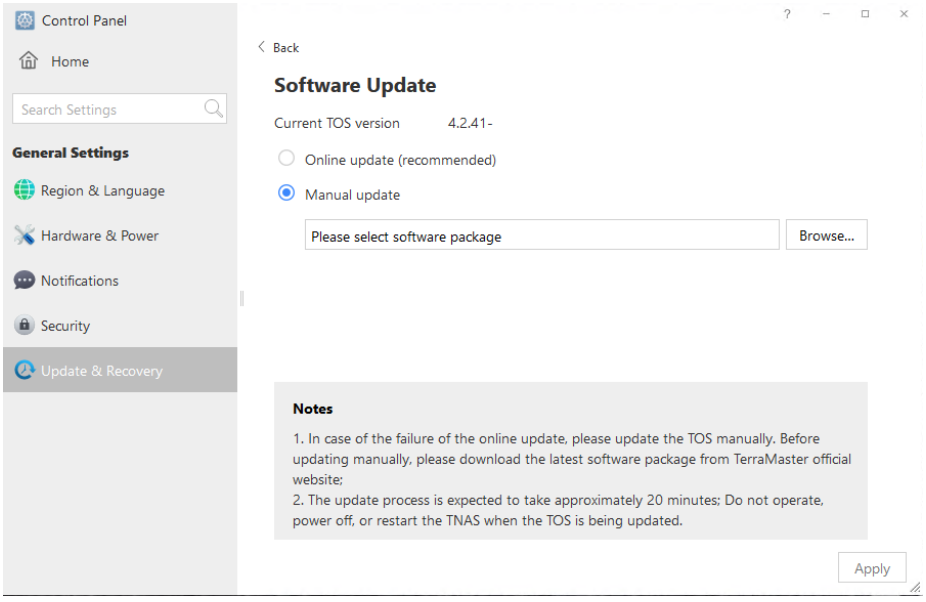
Dans le panneau de contrôle du Terra Master nous sommes venus trouver les paramètres de sécurité. Nous avons activé la protection du NAS contre les attaques DOS (Deny Of Service) qui permet de se prémunir en cas d'une attaque consistant à submerger notre service avec un nombre de requête outre passant les capacités de traitement de notre NAS et le rendant hors d'usage.



Nous avons aussi activé la sécurité de compte, qui se fait par du blocage d'adresses en cas de tentatives de connexions infructueuses trop répétées



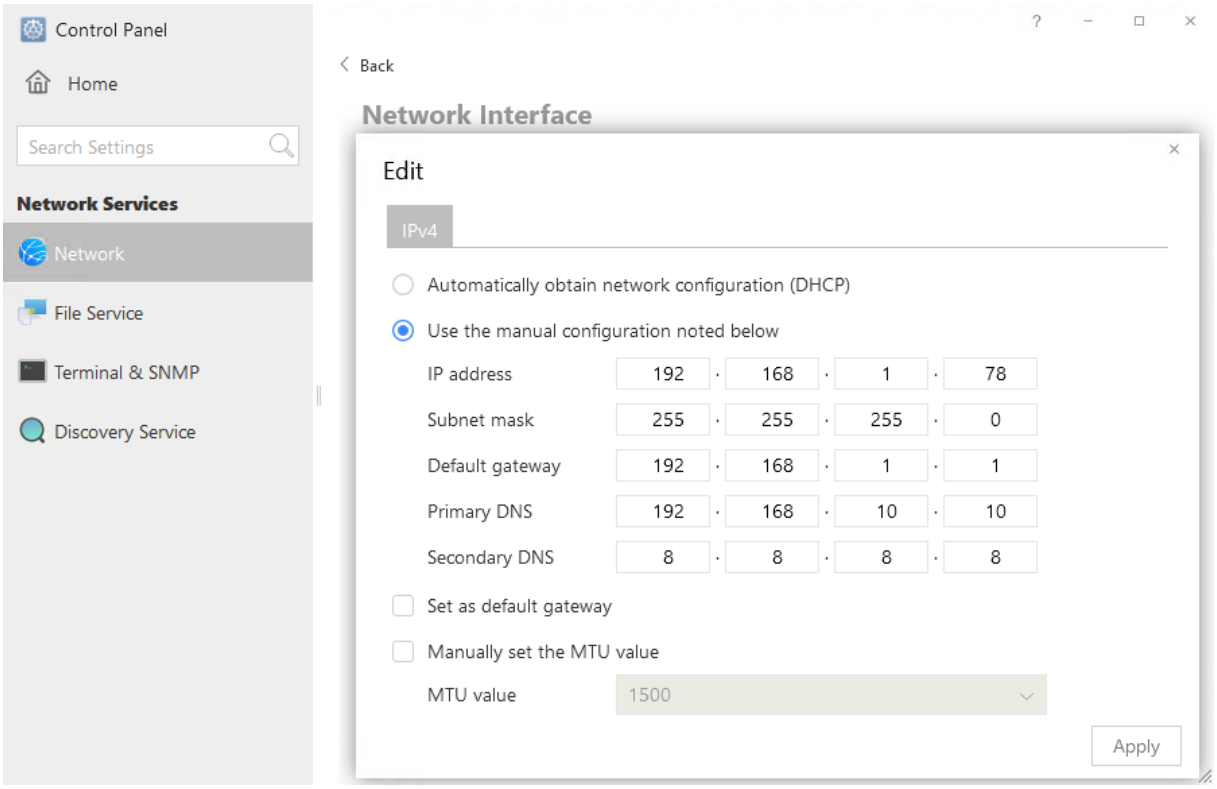

D'un point de vue « moins » sécurité à proprement parlé mais dans le but de gardé notre service efficient au maximum, nous avons réglé les mises à jour du NAS en manuelle. De cette façon nous pouvons maitriser les mises à jour et faire en sorte de ne pas être impacté en cas de mises à jour qui pourraient potentiellement entrainer une mal fonction ou des interruptions de notre service

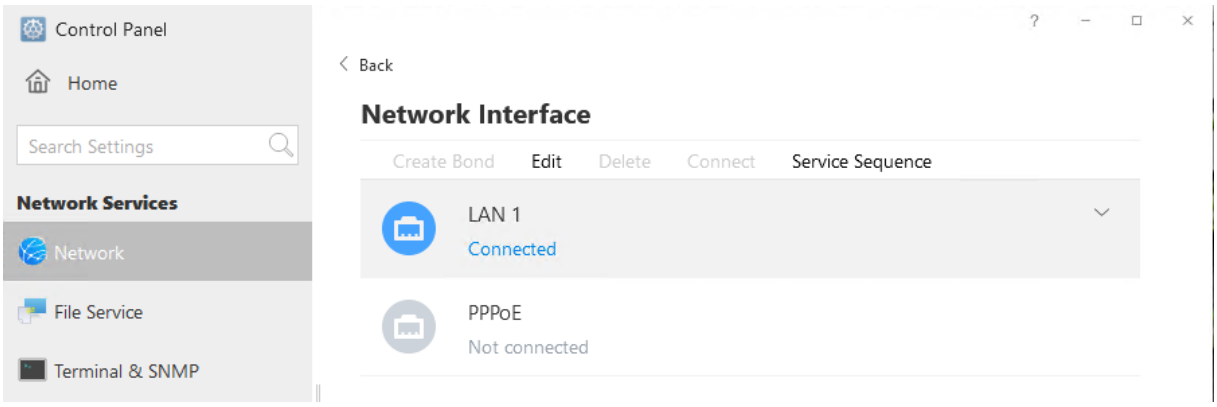


Par la suite nous avons paramétré les services réseau de notre NAS

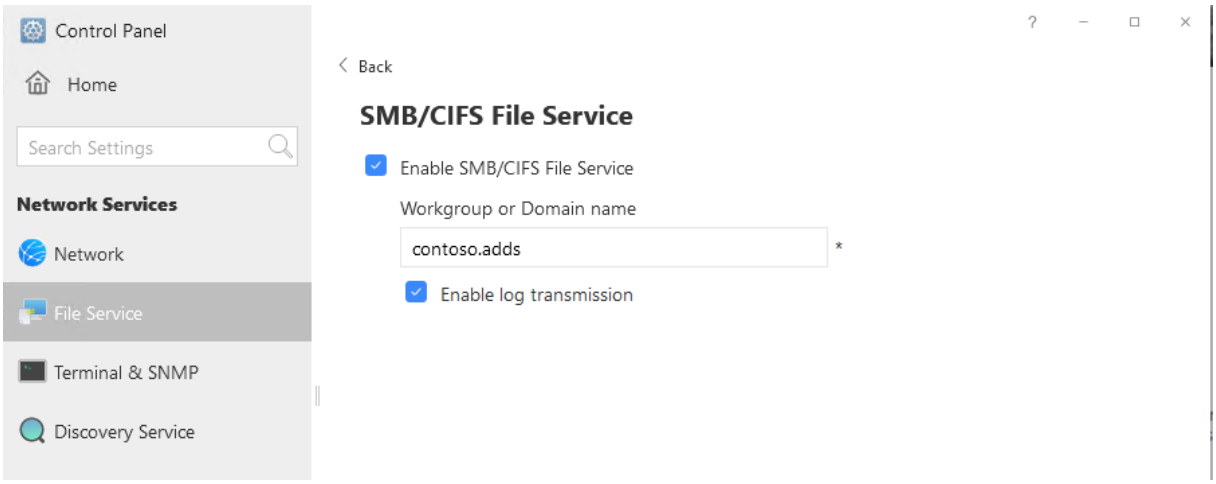
- Service réseau

Nous avons commencé par attribuer une adresse IP fixe à notre NAS dans ses paramétrage réseaux.

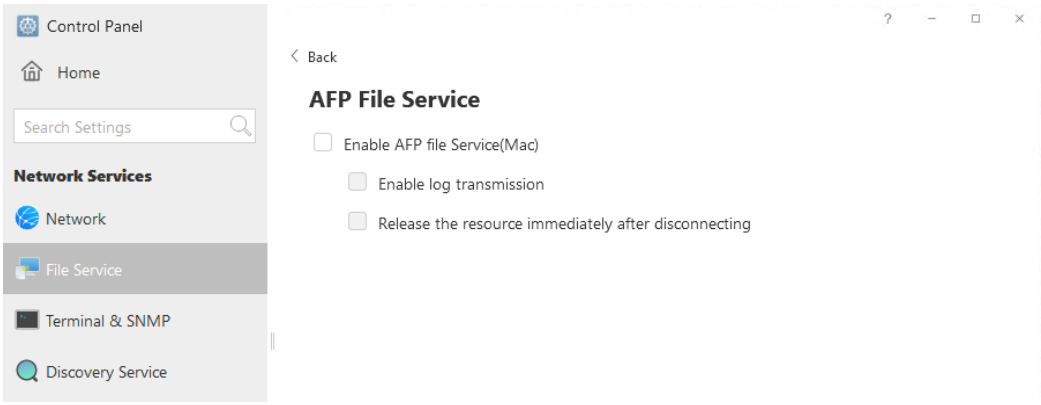


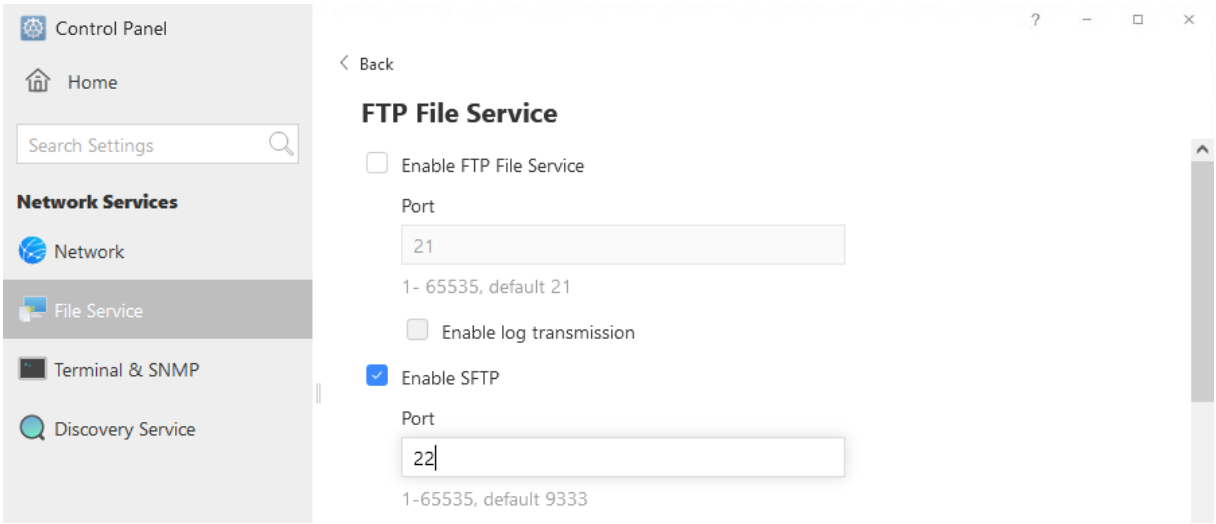

Pour nous permettre un partage de fichiers sur notre environnement Windows nous viendrons activer les options suivantes en renseignant le nom de domaine de notre serveur



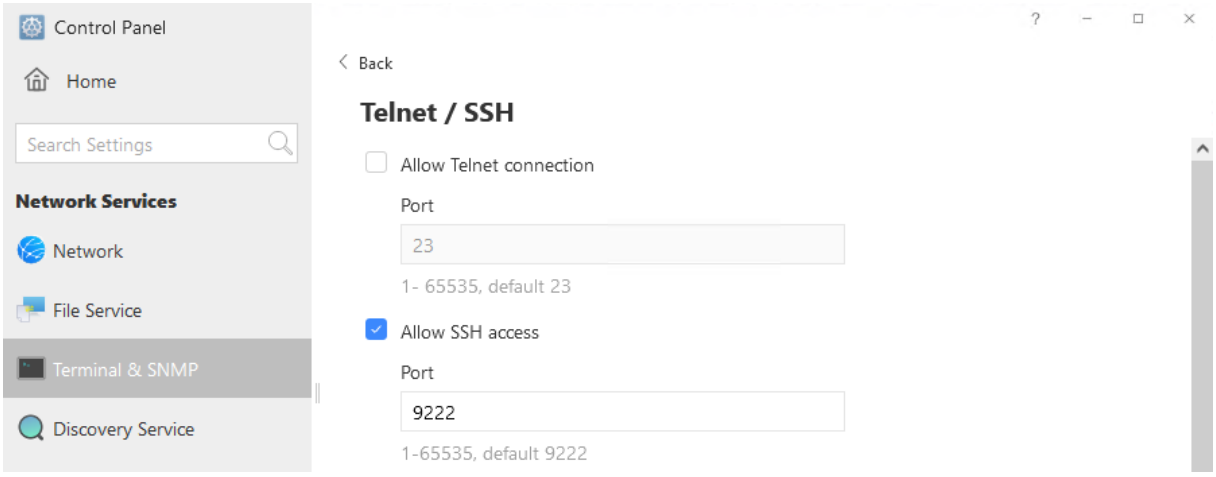

Nous avons par la suite, dans la partie Service de fichier, désactiver le service de fichier AFP



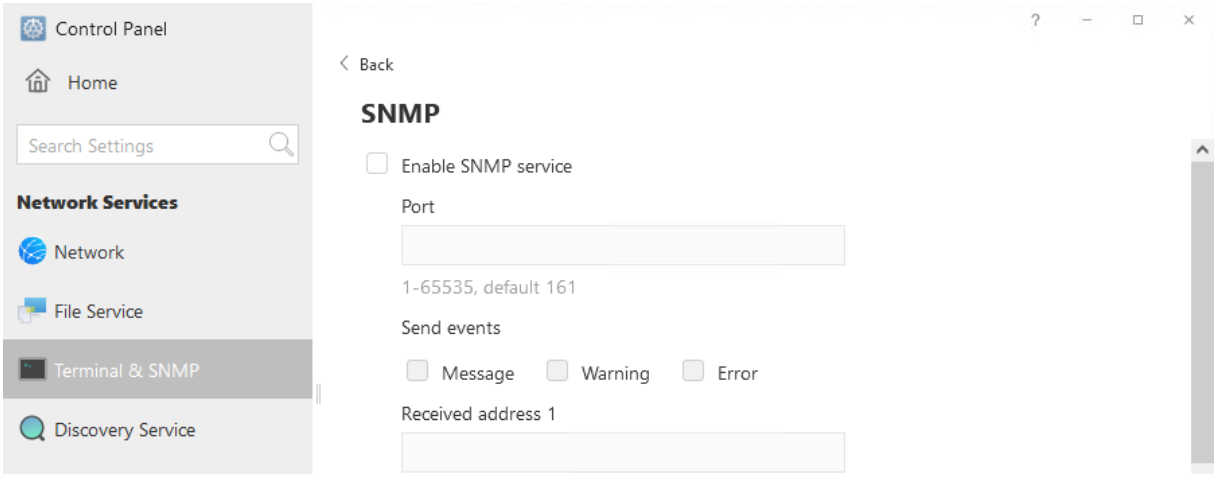

Nous avons désactivé le service FTP et activé, à la place, le service SFTP qui permettra un partage de fichier sécurisé au besoin.



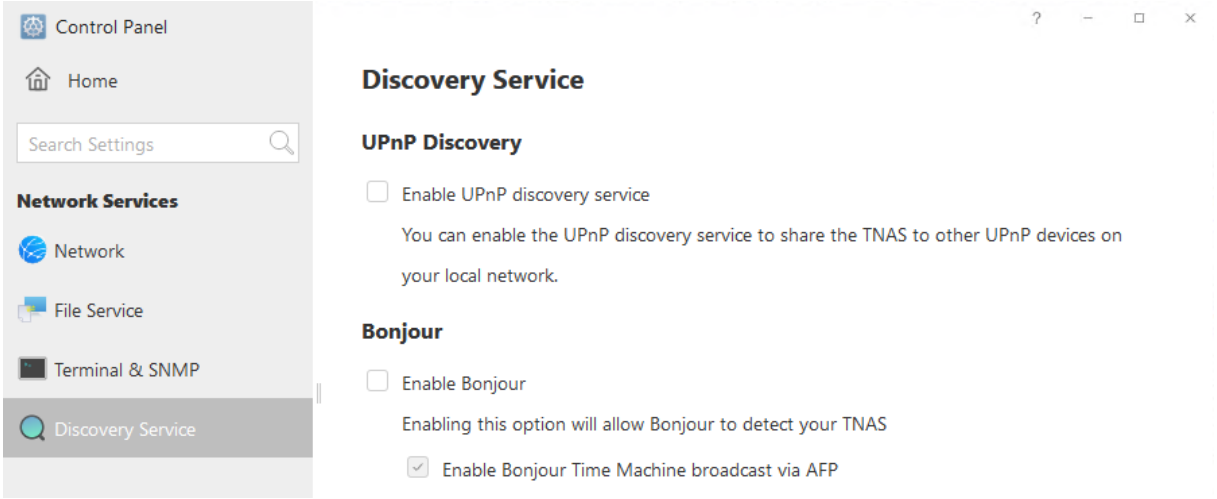

Nous avons également activé dans la partie Terminal et SNMP (Simple Network Management Protocol) l'accès sécurisé SSH et désactivé les connexions via Telnet qui n'est pas sécurisées.




Nous avons noté la présence de la fonction SNMP qui pourra nous servir à monitorer le NAS via un outil tels que Zabbix qui permet de recenser les alertes sur l'état du matériel, ses performances...



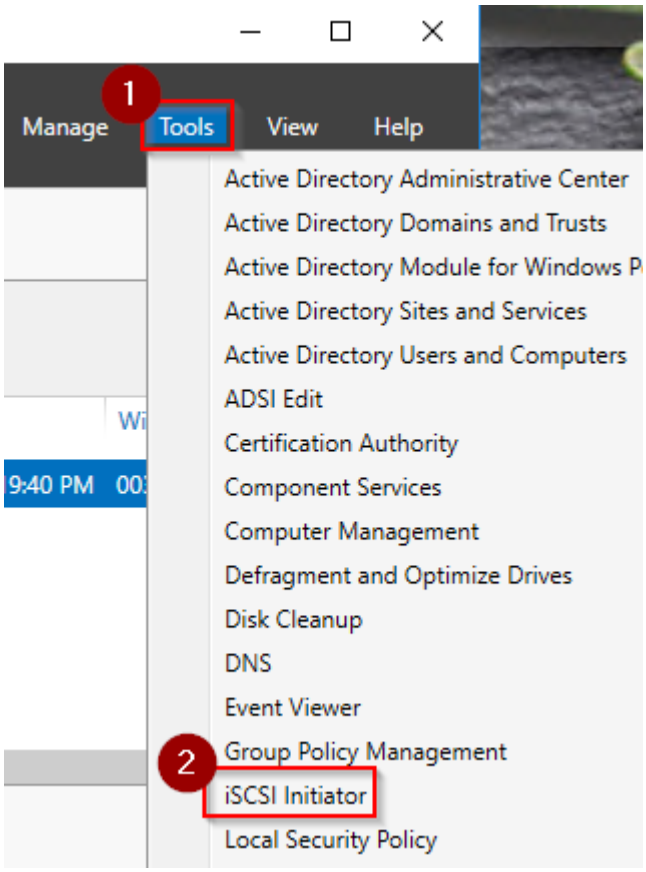

Et enfin nous avons désactivé les options de découverte, comme l'option « Bonjour »

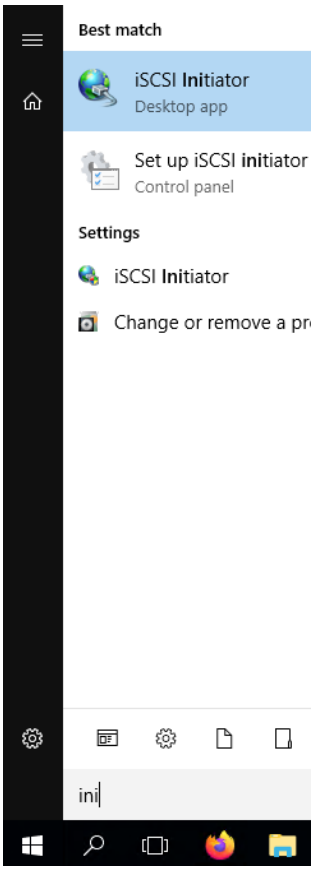


Par la suite nous verrons la configuration de(s) notre/nos ISCSI (Internet Small Computer System Interface) qui nous permettra de transférer des données souhaitées comme nos backups de nos machines hôtes vers notre NAS.

### ISCSI sur notre Windows Server

Il nous faudra dans un premier temps activer la fonction ISCSI initiator sur notre Windows Server



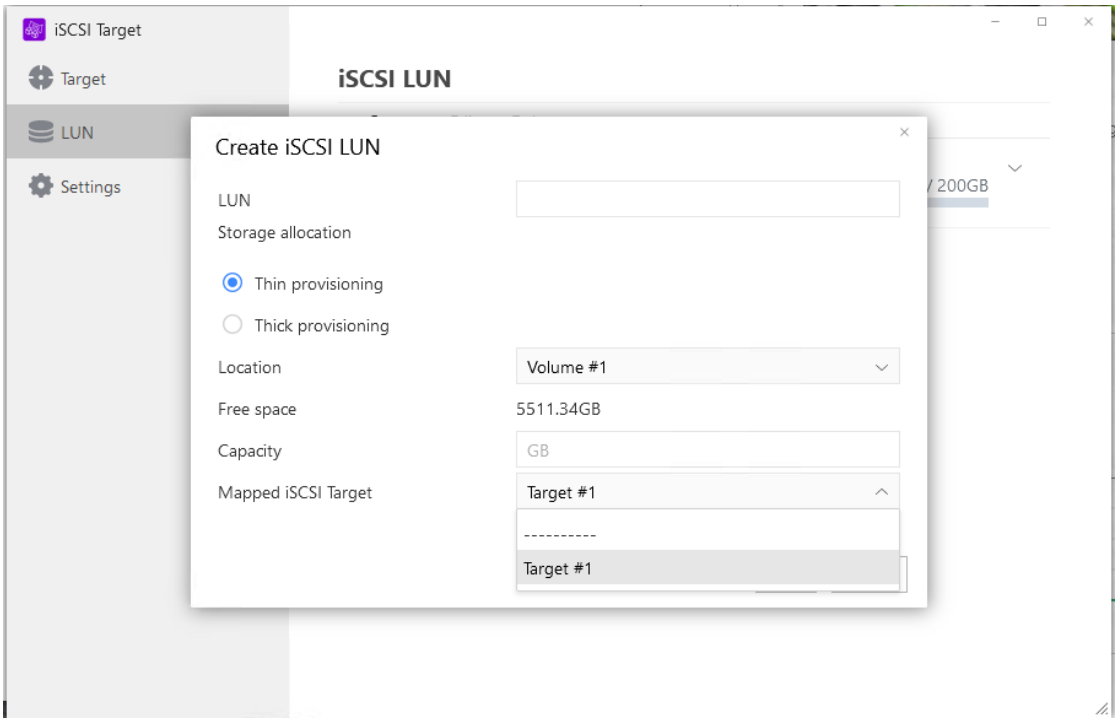

Une fois notre initiateur ISCSI activé nous revenons sur le NAS pour configurer notre « ISCSI target » qui sera, à juste titre, notre cible de stockage à atteindre.

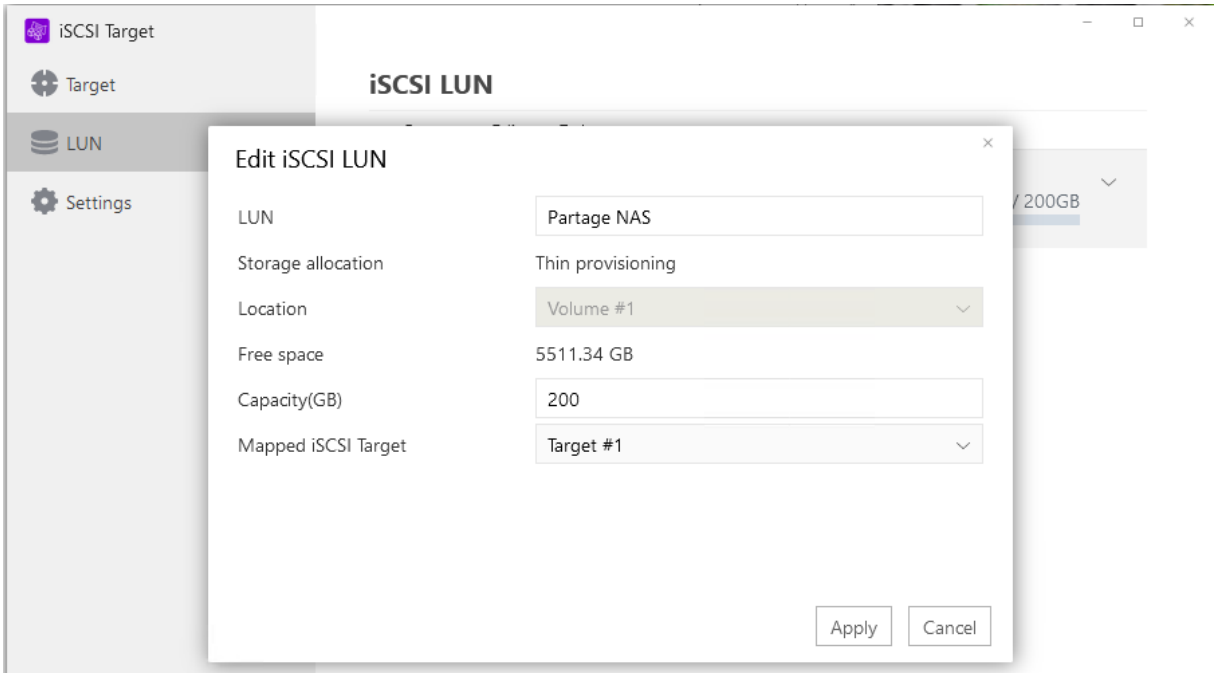
Avant toute chose il nous faut configurer notre espace de stockage qui servira de cible, un LUN.

On lui donne un nom, le type d'allocation de stockage entre THIN et THICK proviosionning.

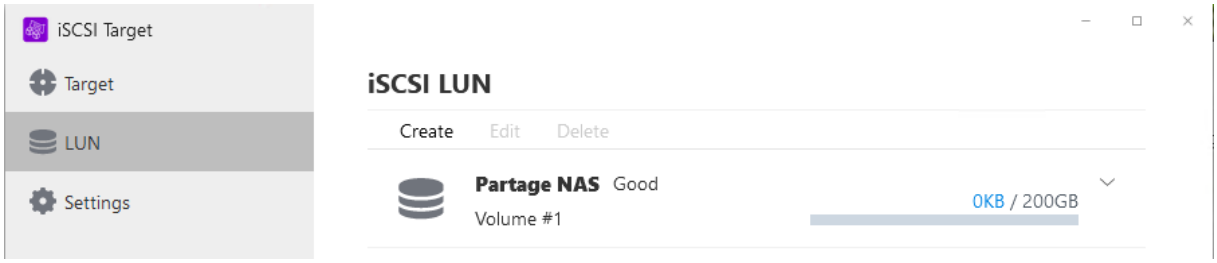
Nous choisirons le THIN car cela permet d'établir un quantité de stockage sans pour autant mobiliser cette dernière à la création. Elle se remplira au fil de ce que l'on stockera sur cet espace. A l'inverse le THICK qui mobilise, à la création, la quantité donnée souhaitée.

Cet espace sera mappé comme étant la cible 1 (TARGET #1)



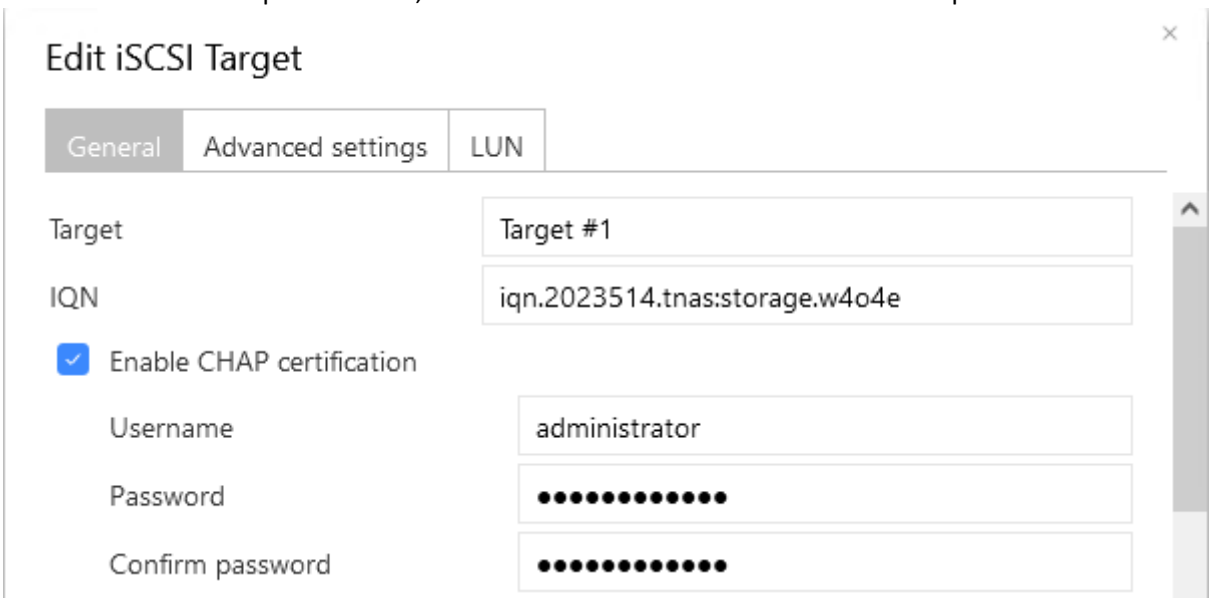




Nous avons donc bien notre LUN créé qui sera notre cible ISCSI

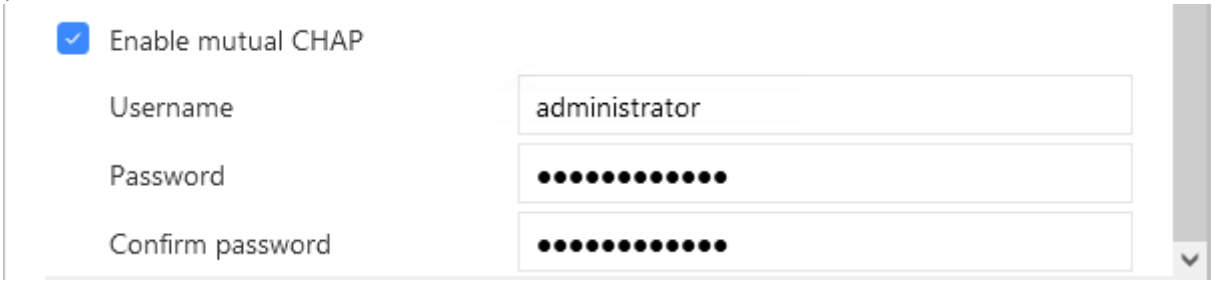



Nous allons aussi sécurisé notre cible ISCSI en activant la certification CHAP et CHAPmutuel
Il nous faut sélectionner notre cible et l'éditer pour atteindre un affichage semblable (cf ci-dessous)

Nous cochons la case pour l'activer, entrons un username souhaité et le mot de passe



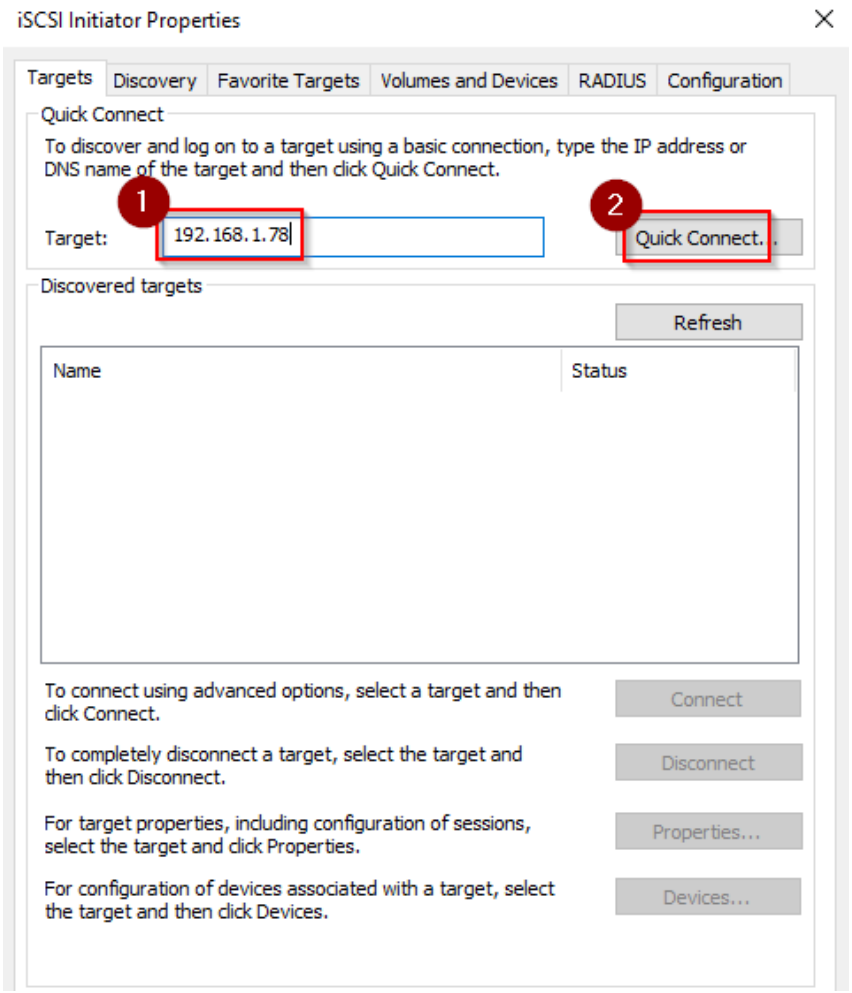

Pour affiner la sécurité, à la suite de notre certification CHAP, nous paramètrerons également le CHAP mutuel
Comme précédmeent il faudra cocher la case pour l'activer et entrer un username ainsi qu'un mot de passe



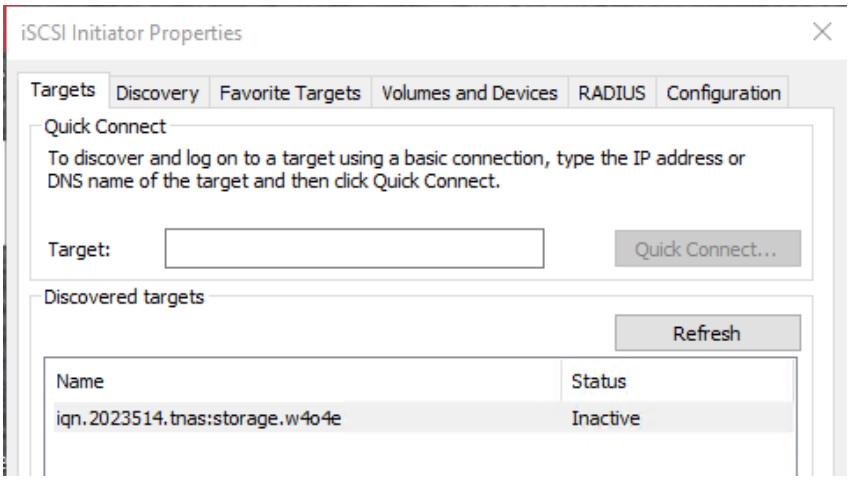

Après avoir créé notre LUN/cible ISCSI sur notre NAS nous revenons sur notre Windows sever pour connecté nos cible ISCSI

Nous venons trouver notre initiateur ISCSI et l'exécutons

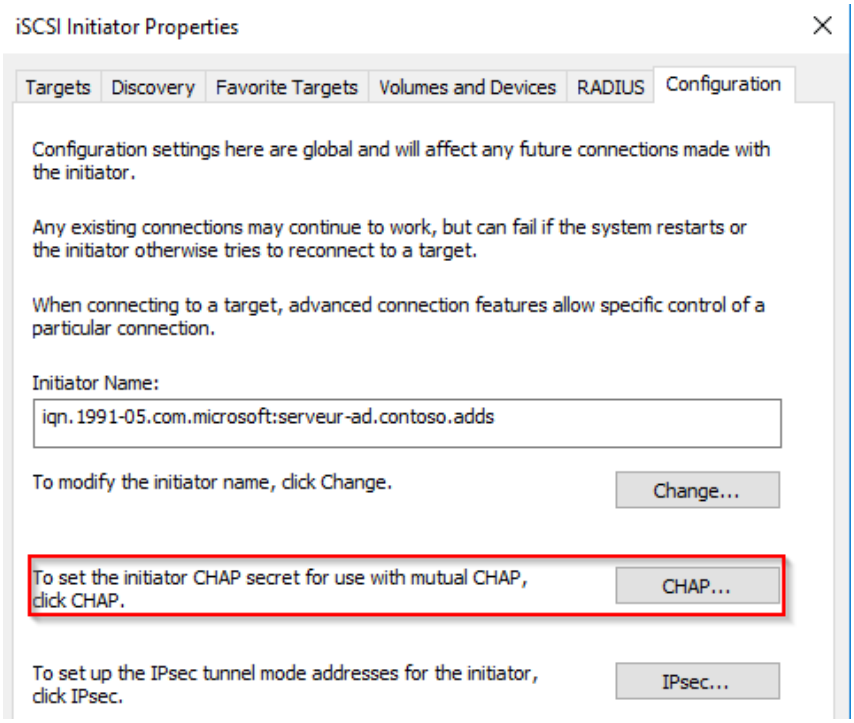

Sur l'interface qui apparait nous venons saisir l'adresse de notre NAS pour établir une connexion avec une potentielle cible ISCSI, si existante.



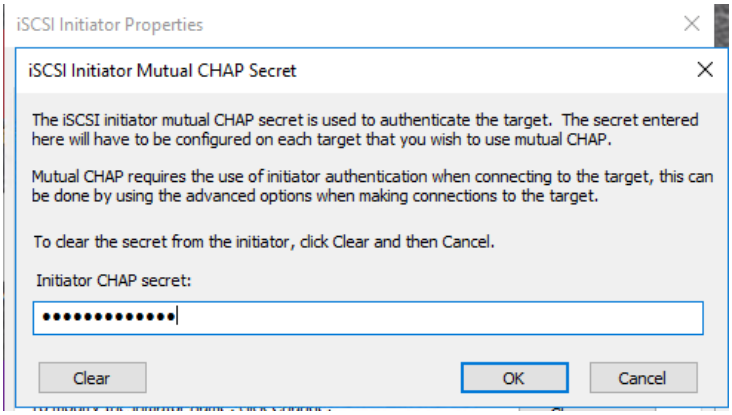

Après validation, on retrouve bien notre cible ISCSI



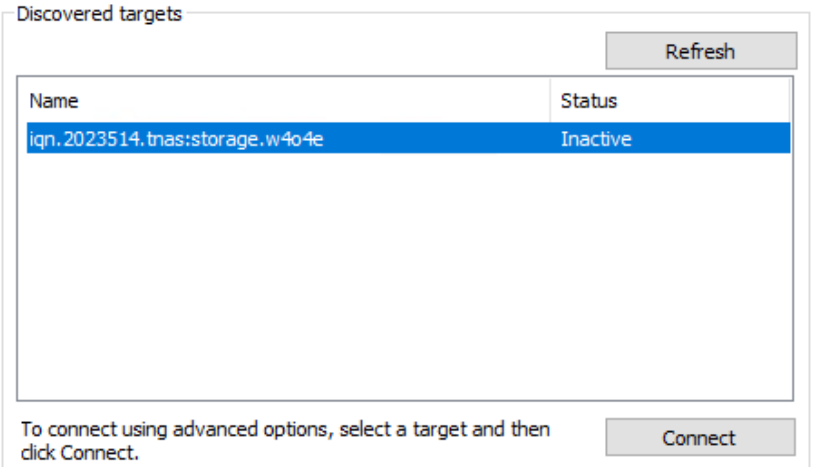
Avant de l'activer, nous allons nous rendre dans l'onglet configuration pour rentrer l'identifiant du chap mutuel pour permettre la connexxion du serveur à la cible



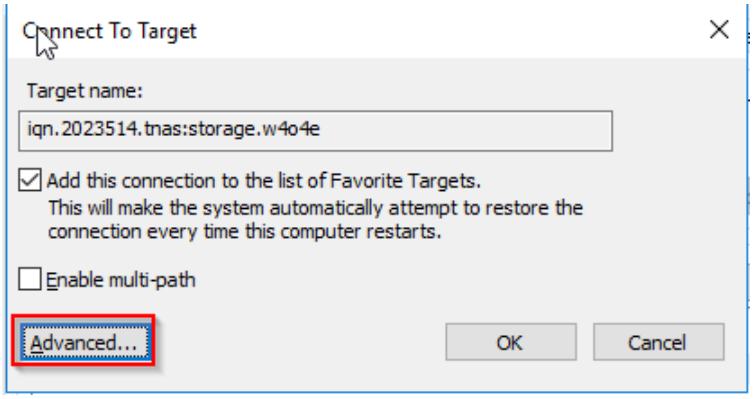

Nous viendrons saisir le mot de passe de notre chap mutuel

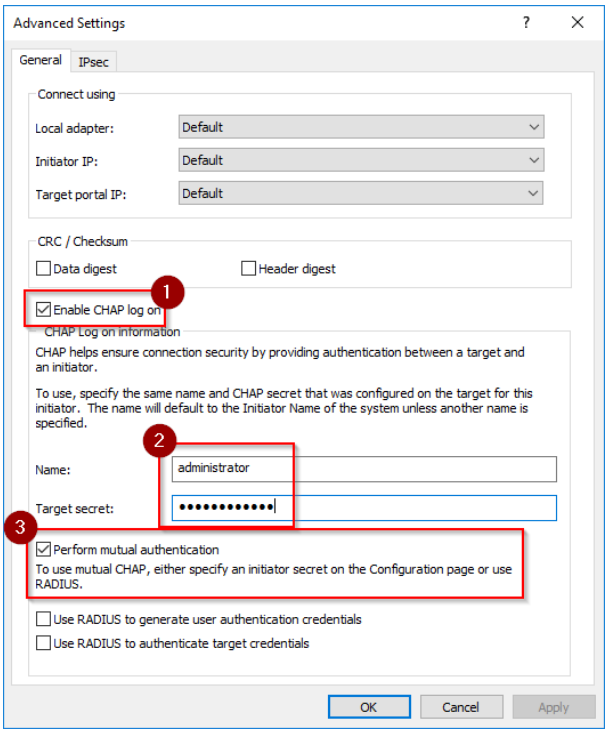



Nous reviendorns sur l'interface avec notre cible et la connecterons.



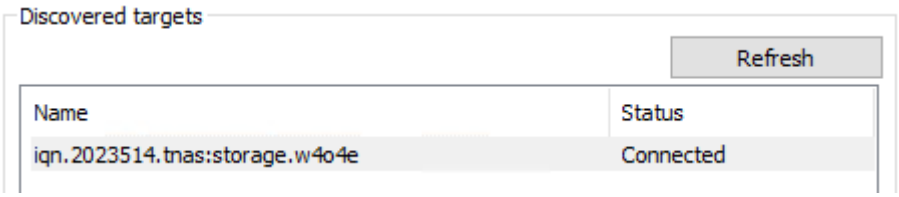
Au moment de la connexion il nous faudra aller dans les options avancées pour configurer la certification chap et activer l'execution du chap mutuel entre le nas et notre serveur



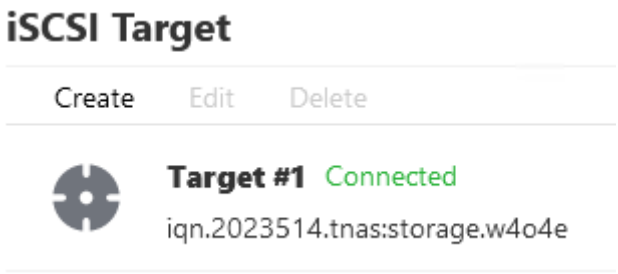




Si nos noms d'utilisateurs et mots de passe correspondent notre cible devrait être connectée de part et d'autre

Serveur



NAS

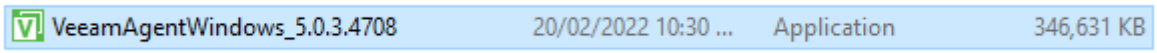


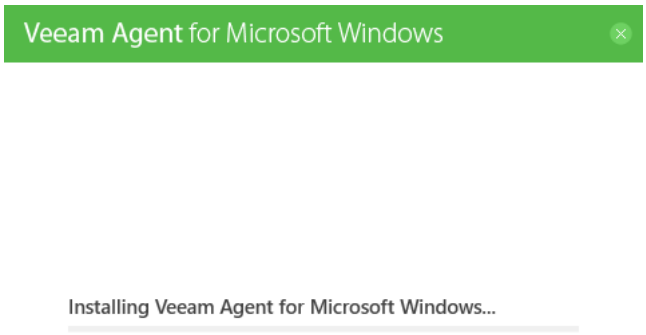

## Configuration de VEEAM agent et de(s) sauvegarde(s)

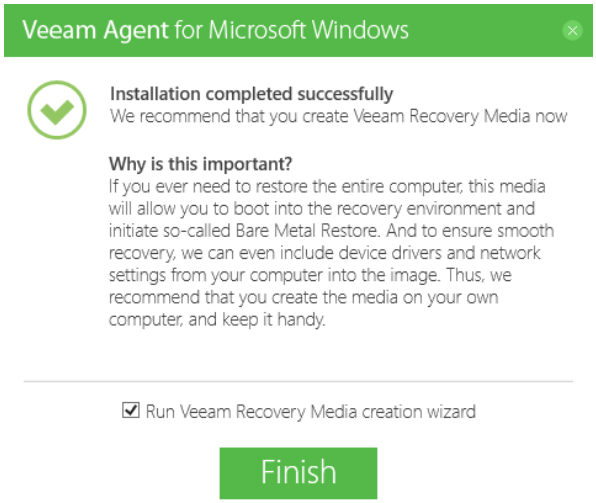
Veeam Agent for Windows est une solution de sauvegarde et de récupération pour les ordinateurs et serveurs exécutant le système d'exploitation Windows. Il permet de protéger les données et les systèmes en effectuant des sauvegardes régulières et en offrant des options de restauration flexibles. Permet des sauvegarde complète d'un système, propose des options de planification et de rétention des sauvegarde....

Il nous faudra d'abord l'installer sur notre serveur Windows comme suit

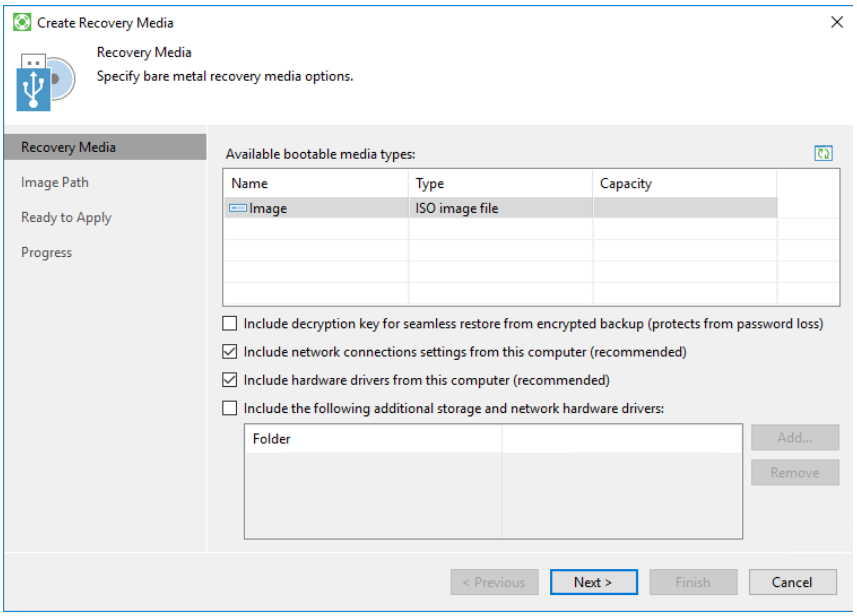
Executer le programme après son téléchargment et après installation

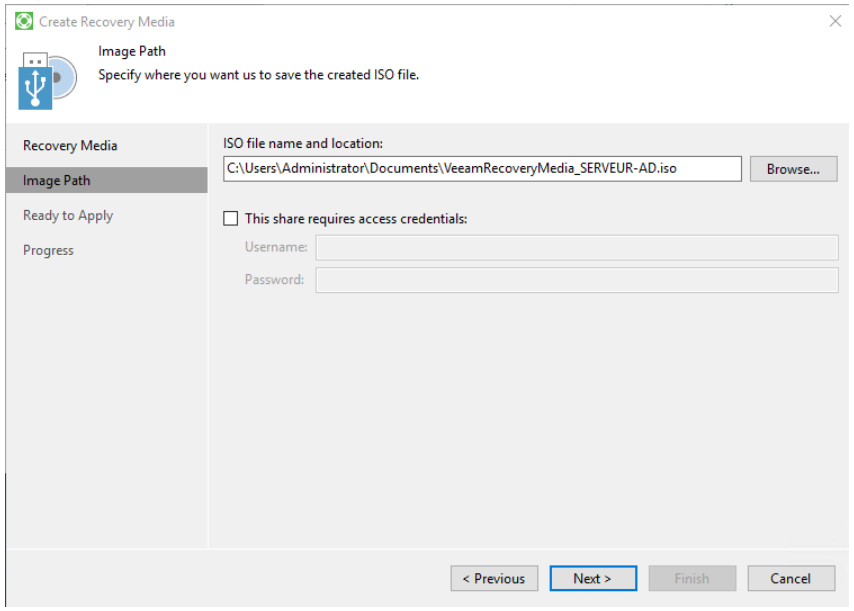


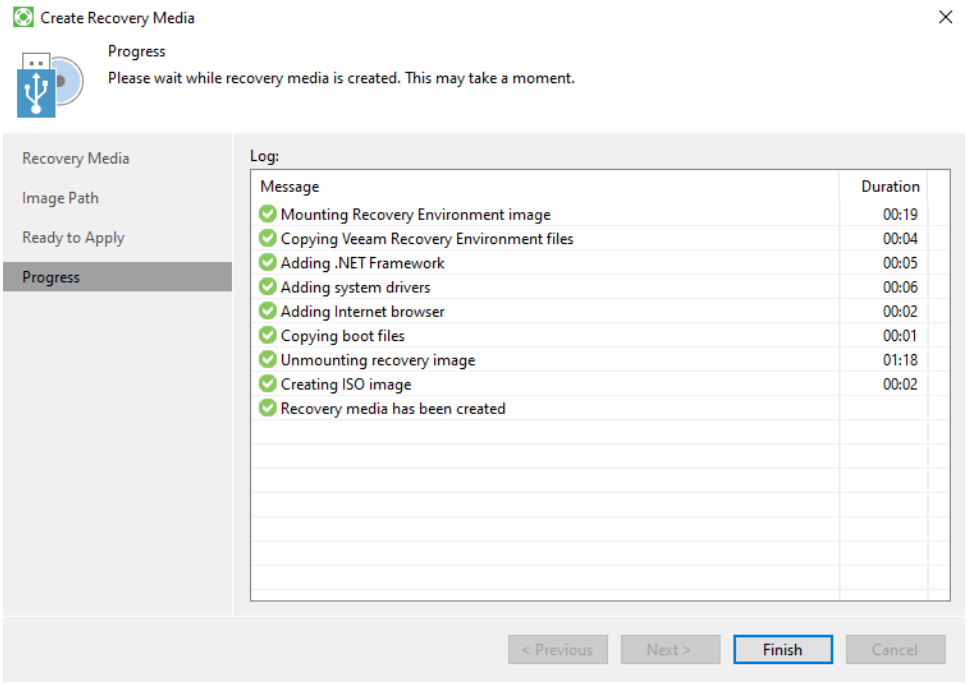




Suivre les étapes suivantes


Create Recovery Media
Recovery Media
Specify bare metal recovery media options.
Recovery Media
Image Path
Ready to Apply
Progress
Available bootable media types:
Name
Type
Capacity
Image
ISO image file
Include decryption key for seamless restore from encrypted backup (protects from password loss)
Include network connections settings from this computer (recommended)
Include hardware drivers from this computer (recommended)
Include the following additional storage and network hardware drivers:
Folder
Add...
Remove
< Previous
Next >
Finish
Cancel

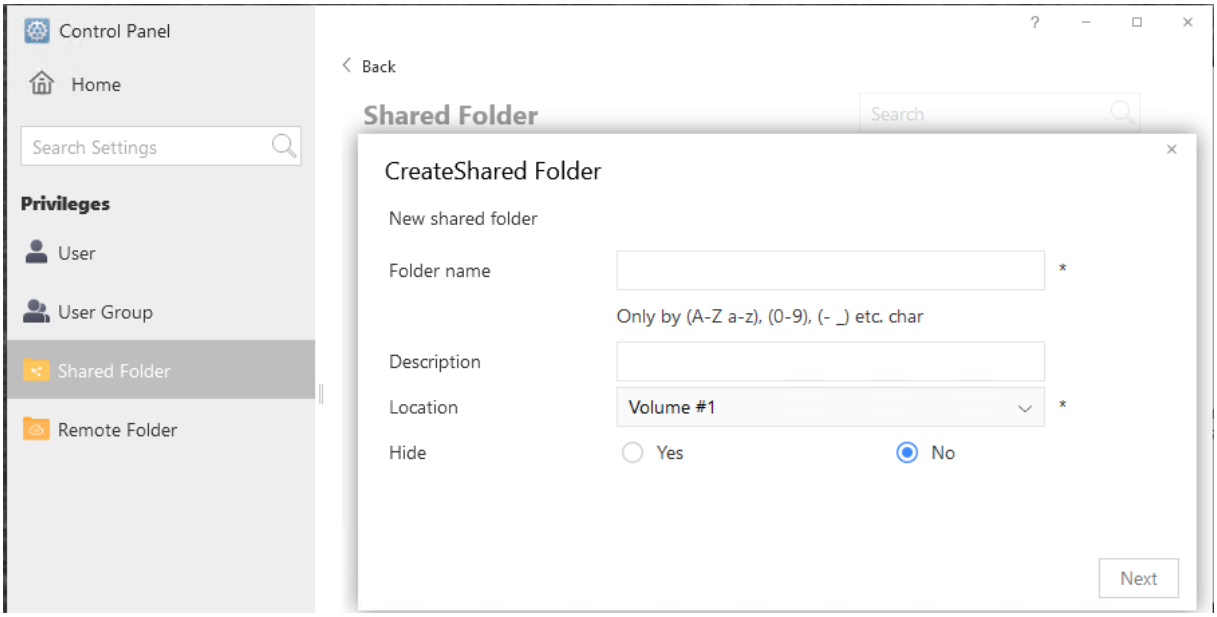

Create Recovery Media
Image Path
Specify where you want us to save the created ISO file.
Recovery Media
Image Path
Ready to Apply
Progress
ISO file name and location:
C:\Users\Administrator\Documents\VeeamRecoveryMedia_SERVEUR-AD.iso
Browse...
This share requires access credentials:
Username:
Password:
< Previous
Next >
Finish
Cancel

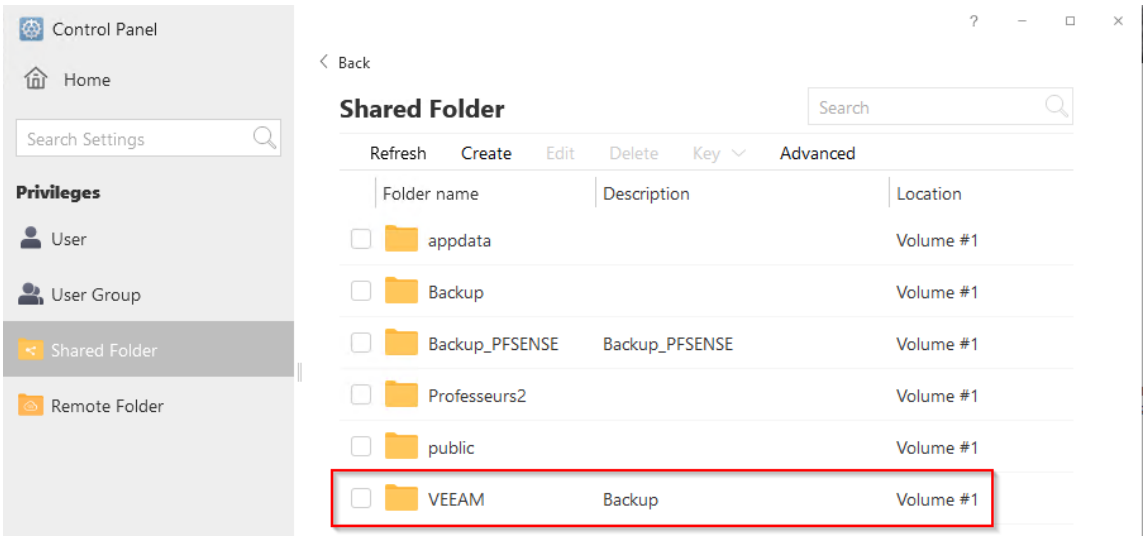
Une fois cette étape terminer notre outil de récupération est créé, nous pouvons continuer



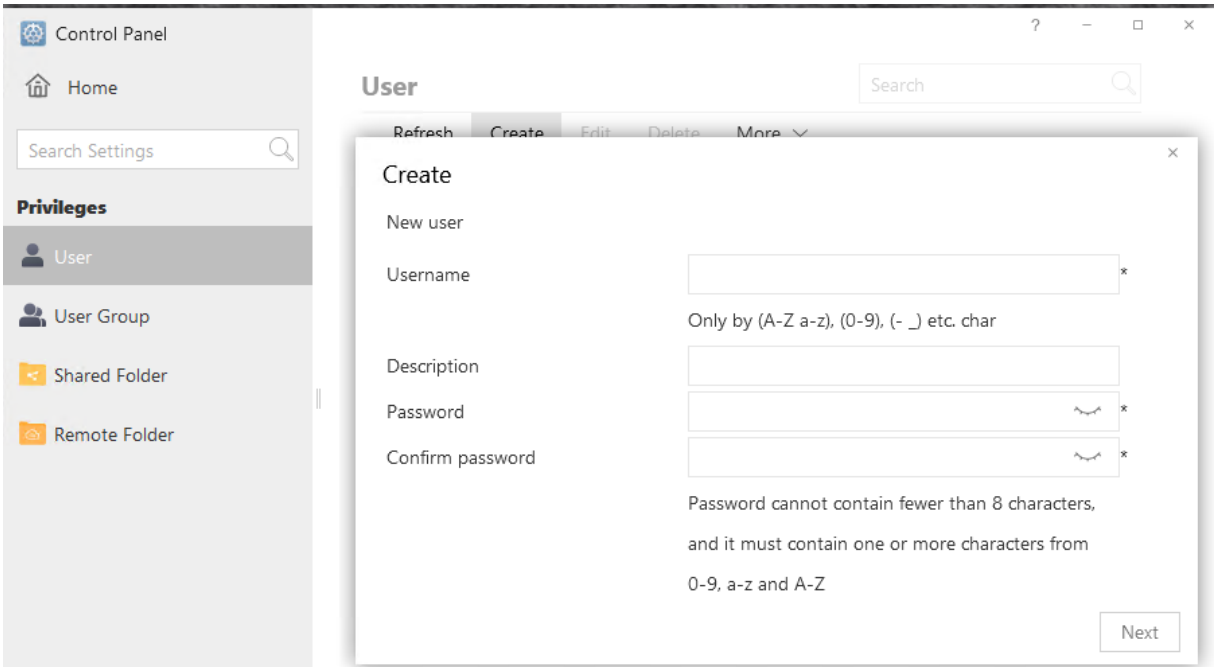

Nous reviendrons ensuite sur le NAS pour créeer un fichier partager qui servira par la suite de destination pour notre backup

Il nous faudra aller sur le panneau de contrôle puis shared folder, sélectionner l'onglet shared folder et venir créer un nouveau shared folder






Nous créerons également un utilisateur qui sera administrateur de ce fichier partagé de backup

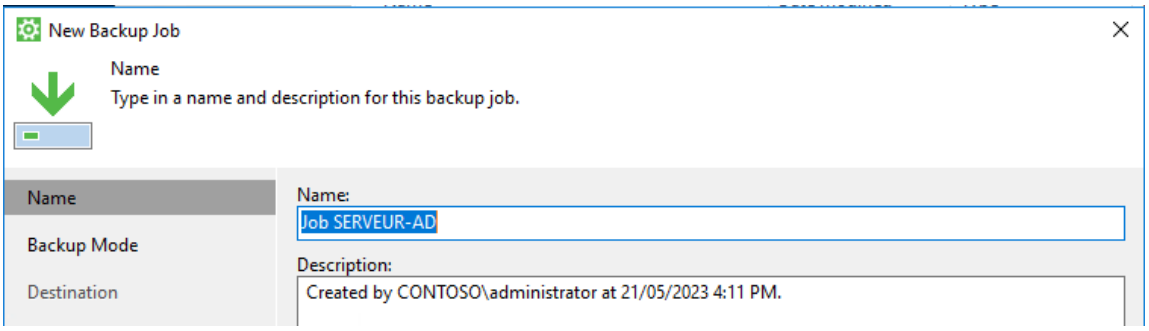



En terme d'autorisation nous mettons tout les droits à cet utilisateurs en particulier

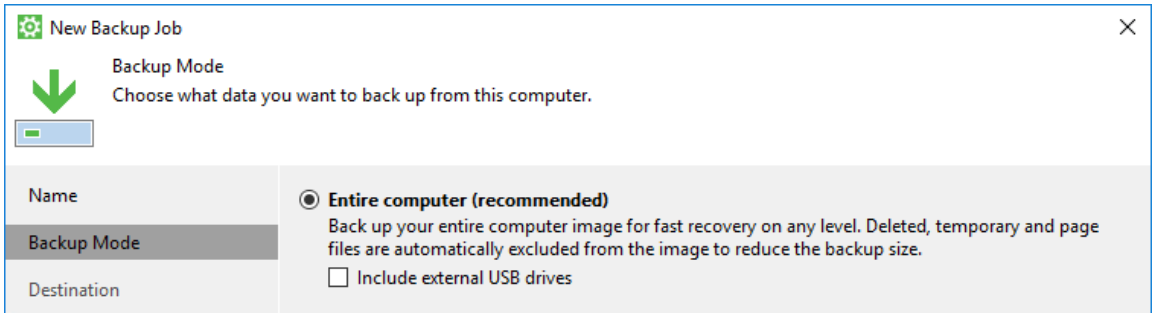
| Username | Permission | Deny | Read/Write | Read only |
|---|---|---|---|---|
| backupadm | Read/Write | ☐ | ☑ | ☐ |
| CGORIE | Deny | ☑ | ☐ | ☐ |
| guest | Deny | ☑ | ☐ | ☐ |

Nous viendrons ensuite paramétrer nos backup comme suit

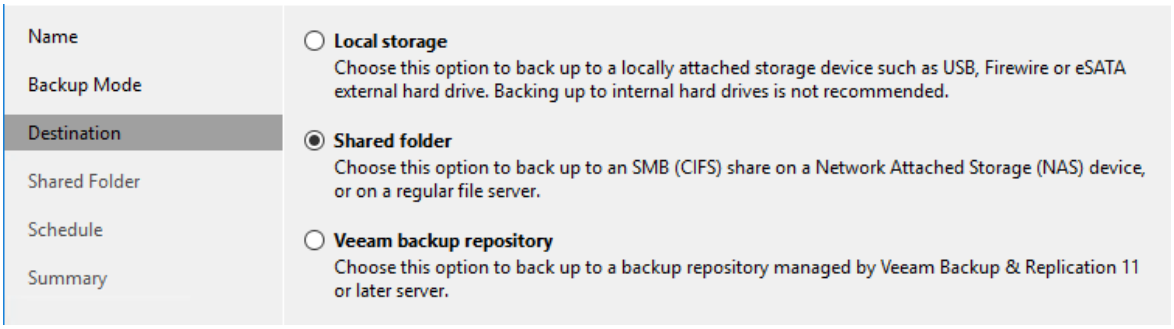
Ouvrir l'outil New Backup Job, auquel nous donnerons un nom



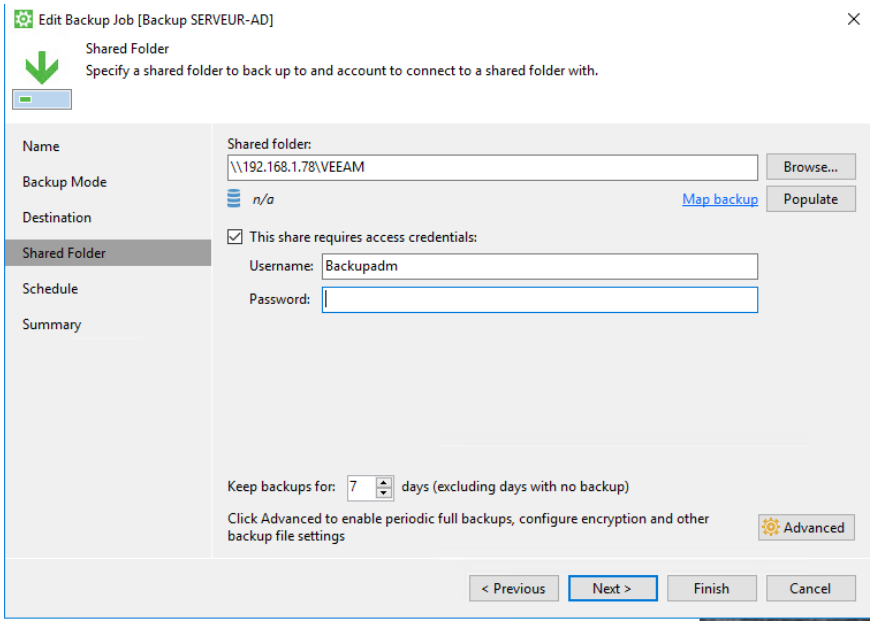

Nous viendorns par la suite séléctionner l'option « Entire computer » pour notre mode de Backup



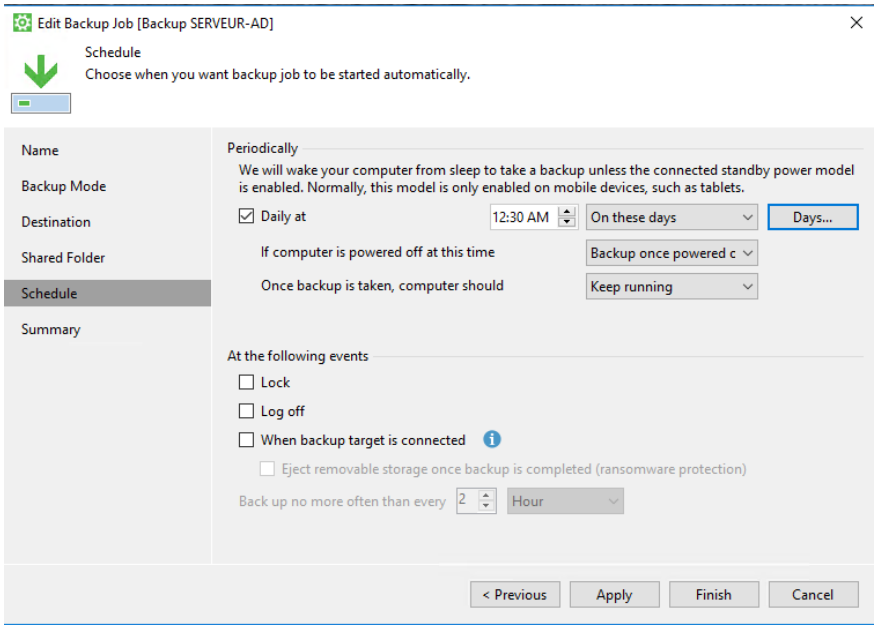

Comme destination de stockage nous viendrons selectionner shared folder pour le stocker sur notr NAS.



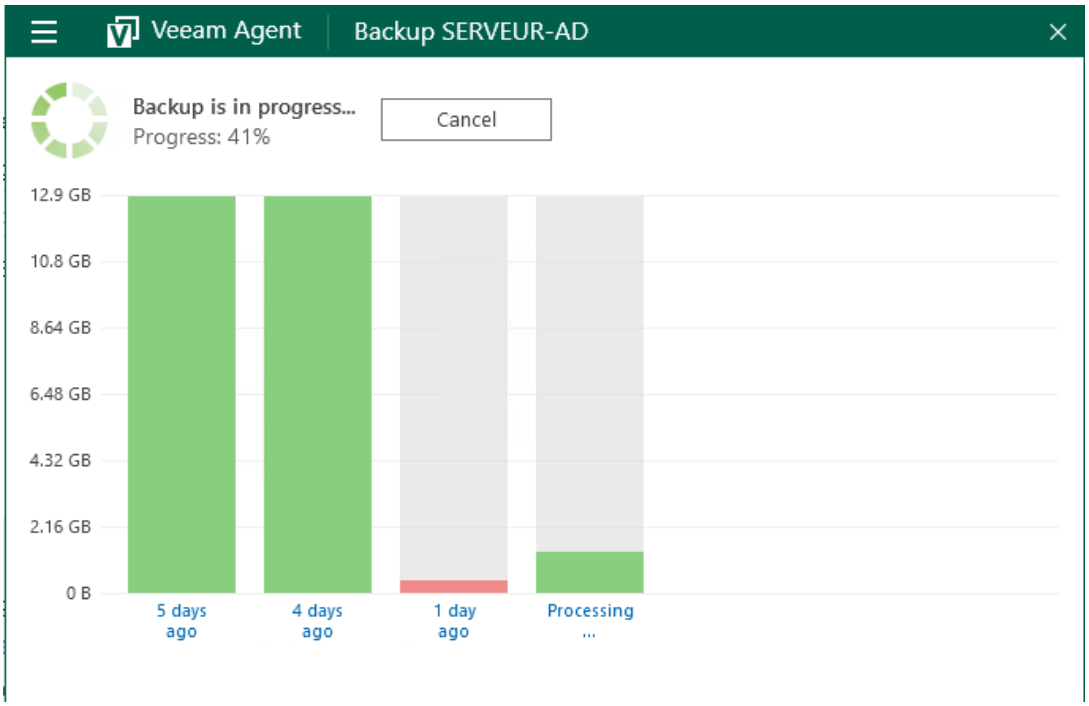
Rentrer le chemin vers le fichier partagé que nous avons créé plus haut avec les identifiants si besoin est. Dans notre cas oui car nous avons créé un utilisateur propriétaire du fichier pârtagé de backup sur notre NAS.




Paramétrer la periodicité de l'exécution des backup du system puis terminer et appliquer

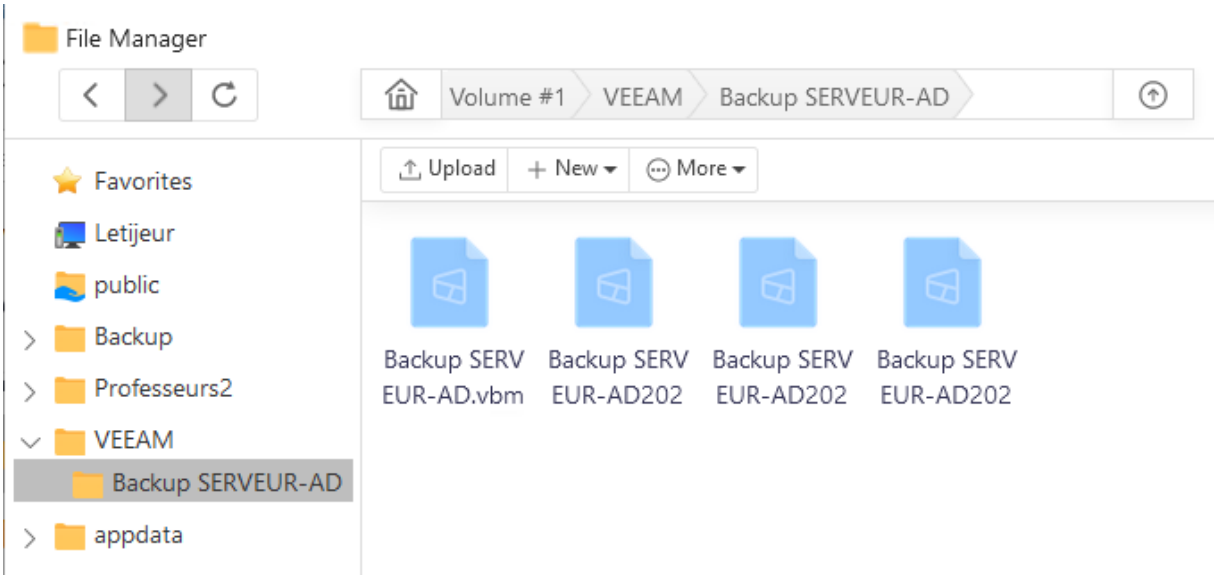



Et lancer une première backup manuellement




Sur notre NAS, en allant dans les fichier partagés on retrouve bien nos backups

Ls



Sur notre serveur Ubuntu il nous faudra télécharger le paquet VEEAM sur le site https://www.veeam.com/linux-backup-download.html avec la comande

sudo wget https://www.veeam.com/download_add_packs/backup-agent-linux/deb-64

```
srvweb@srvweb:~$ cd /home/
srvweb@srvweb:/home$ ls
appdata  nextcloud.admin@contoso.adds  srvweb  veeam
srvweb@srvweb:/home$ cd veeam/
srvweb@srvweb:/home/veeam$ sudo wget https://www.veeam.com/download_add_packs/backup-a
gent-linux/deb-64
[sudo] password for srvweb:
--2023-05-21 14:59:52--  https://www.veeam.com/download_add_packs/backup-agent-linux/d
eb-64
Resolving www.veeam.com (www.veeam.com)... 107.22.239.89, 34.200.193.251, 54.164.47.25
3, ...
Connecting to www.veeam.com (www.veeam.com)|107.22.239.89|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://login.veeam.com/auth/realms/veeamsso/protocol/openid-connect/auth?cl
ient_id=veeam-com&response_type=code&redirect_uri=https%3A%2F%2Fwww.veeam.com%2Foauth&
scope=profile&state=5863e61179589fd8a94ca30a0cd61aaa [following]
--2023-05-21 14:59:53--  https://login.veeam.com/auth/realms/veeamsso/protocol/openid-
connect/auth?client_id=veeam-com&response_type=code&redirect_uri=https%3A%2F%2Fwww.vee
am.com%2Foauth&scope=profile&state=5863e61179589fd8a94ca30a0cd61aaa
Resolving login.veeam.com (login.veeam.com)... 184.73.38.238, 54.160.73.185, 54.243.45
.85, ...
Connecting to login.veeam.com (login.veeam.com)|184.73.38.238|:443... connected.
HTTP request sent, awaiting response... 307 Temporary Redirect
Location: https://login.veeam.com/auth/realms/veeamsso/protocol/openid-connect/auth?sc
ope=profile&response_type=code&redirect_uri=https%3A%2F%2Fwww.veeam.com%2Foauth&state=
5863e61179589fd8a94ca30a0cd61aaa&client_id=veeam-com&restarted=true [following]
--2023-05-21 14:59:53--  https://login.veeam.com/auth/realms/veeamsso/protocol/openid-
connect/auth?scope=profile&response_type=code&redirect_uri=https%3A%2F%2Fwww.veeam.com
%2Foauth&state=5863e61179589fd8a94ca30a0cd61aaa&client_id=veeam-com&restarted=true
Reusing existing connection to login.veeam.com:443.
HTTP request sent, awaiting response... 200 OK
Length: 15481 (15K) [text/html]
Saving to: 'deb-64.1'

deb-64.1             100%[=====================>]  15,12K  --.-KB/s    in 0s

2023-05-21 14:59:53 (206 MB/s) - 'deb-64.1' saved [15481/15481]
```