

Documentation d'exploitation

Réalisé par :

Blondel Lucas

Caparros Maxime

Table des matières

Introduction.....	4
1. Schéma d'infrastructure	4
2. Les différentes technologies utilisées.....	4
1. Choix d'un Firewall	4
2. Choix de la solution pour l'intranet.....	4
3. Proxmox.....	5
1. Backup	5
4. Mise en place du firewall.....	6
1. Objectifs.....	6
2. Configuration matérielle.....	7
3. Configuration logicielle.....	7
1. Configuration du LDAP	7
2. OpenVPN	16
4. Politique de sécurité.....	26
1. Configuration des règles.....	26
5. Gestion des mises à jour.....	27
6. Gestion des accès	27
5. Mise en place d'un serveur intranet.....	28
1. Objectifs.....	28
2. Configuration matérielle.....	28
3. Configuration logicielle.....	28
1. Docker compose de traefik, authelia et nextcloud.....	28
4. Politique de sécurité.....	41
5. Gestion des mises à jour.....	41
6. Gestion des logs.....	42
7. Gestion des accès	42
6. Serveur mail.....	42
1. Objectifs.....	42
2. Configuration matérielle.....	42
3. Configuration logicielle.....	42
1. Setup de l'application hmailserv.....	42
4. Gestion de la sécurité	51
5. Gestion des logs.....	56
6. Ajout d'un utilisateur de l'AD.....	57

7.	Serveur AD.....	59
1.	Objectifs.....	59
2.	Configuration matérielle.....	59
3.	Configuration logicielle.....	60
1.	Remote desktop	60
2.	Installer l'active Directory sur son serveur	71
8.	Sauvegarde/Backup	78
7.1	Objectifs.....	78
7.2	Choix matériel.....	78
7.3	Mise en place de la solution	79

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 réflexion 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 technologie en présence à connaître et maîtriser et est moins coûteuse (entretien, formation, temps), mais plus faillible.
	Une solution multi éditeurs est complexe à administrer car elle nécessite la connaissance et le savoir-faire de deux technologies différentes et est plus coûteuse (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

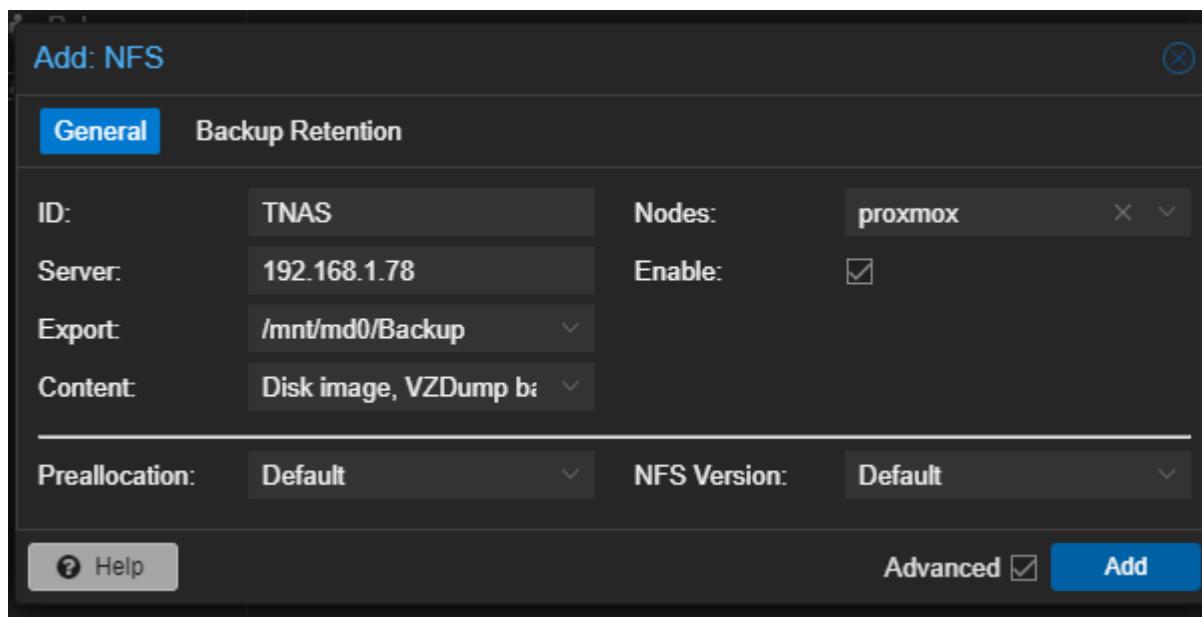
8 cœurs 16 processeurs logiques

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

The screenshot shows the Proxmox VE 7.4-3 interface. In the left sidebar under 'Datacenter', there is a tree view of nodes: 'proxmox' which contains VMs 100 through 109, and storage units TNAS, local (proxmox), and local-lvm (proxmox). The 'Backup' tab is selected in the main menu. A 'Create: Backup Job' dialog is open, showing the 'General' tab. The 'Node' dropdown is set to 'All'. The 'Storage' dropdown is set to 'TNAS'. The 'Schedule' dropdown shows two entries: '2,22:30' and '2,22:30'. The 'Selection mode' dropdown is set to 'All'. The 'Send email to:' field contains 'maxoucaparros@gmail.com'. The 'Email:' dropdown is set to 'On failure only'. The 'Compression:' dropdown is set to 'ZSTD (fast and good)'. The 'Mode:' dropdown is set to 'Snapshot'. The 'Enable:' checkbox is checked. Below the form is a table titled 'Job Comment:' with columns: ID ↑, Node, Status, Name, and Type. All 10 VMs listed in the sidebar are selected in the table. At the bottom of the dialog are 'Repeat missed:' and 'Advanced' checkboxes, and a 'Create' button.

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 évidemment 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.

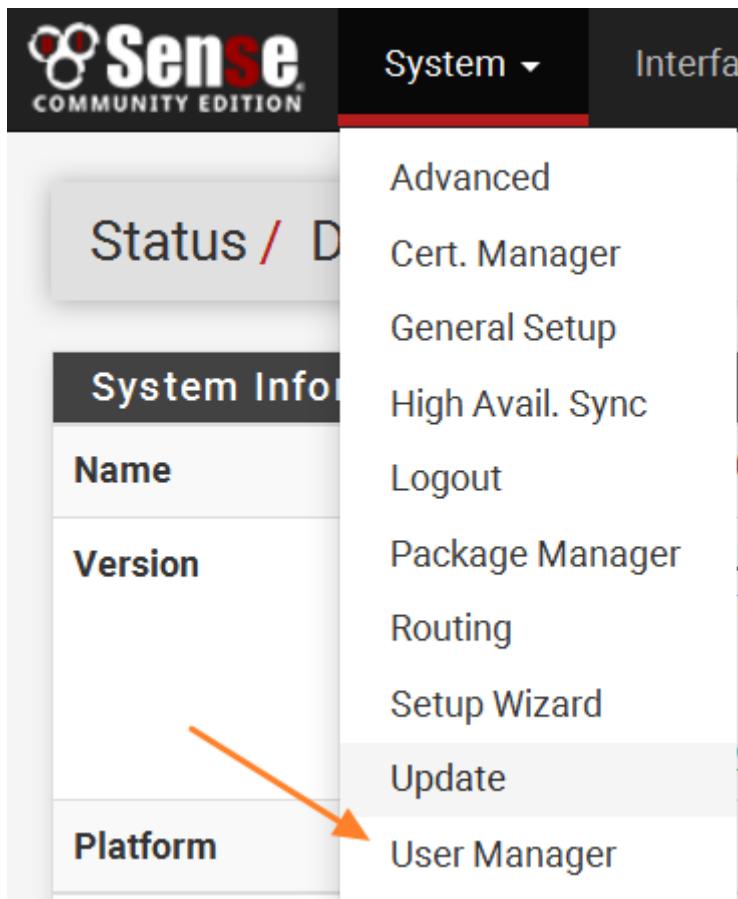
La mise en place du serveur pfSense s'est effectué via une image ISO de pfSense sur l'outil de virtualisation Proxmox.

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".

The screenshot shows the 'User Manager' section of the pfSense interface. The title bar says 'System / User Manager / Authentication Servers'. Below it, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers' (which is highlighted with a red arrow). The main content area is currently empty.

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.

Server Settings	
<u>Descriptive name</u>	server-ad
<u>Type</u>	LDAP

LDAP Server Settings	
<u>Hostname or IP address</u>	192.168.10.10
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.	
<u>Port value</u>	389
<u>Transport</u>	Standard TCP
<u>Peer Certificate Authority</u>	Global Root CA List
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.	
<u>Protocol version</u>	3

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.

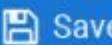
Pour récupérer le DN de l'utilisateur on tape la commande suivante en powershell sur notre serveur AD :

```
(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.

<u>Search scope</u>	Level Entire Subtree
<u>Base DN</u>	DC=contoso,DC=add
<u>Authentication containers</u>	OU=admin,OU=AllUser,DC=contoso,DC=add;OU=AllUser,DC=contoso,DC=add Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers
<u>Extended query</u>	<input type="checkbox"/> Enable extended query
<u>Bind anonymous</u>	<input type="checkbox"/> Use anonymous binds to resolve distinguished names
<u>Bind credentials</u>	CN=pfsense admin,OU=admin,OU=AllUser,DC=contoso,DC=add.....

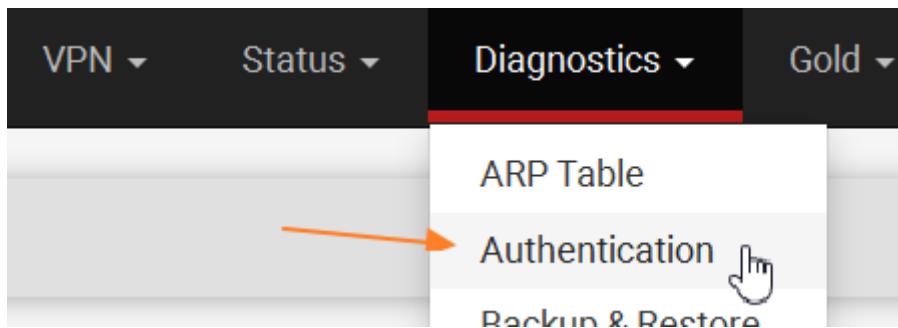
Vous pouvez seulement indiquer "group" à la place de "posixGroup", et veillez à ne pas cocher l'option "LDAP Server uses RFC 2307 style group membership" sinon pfSense ne pourra pas récupérer le nom du groupe auquel appartient votre utilisateur.

User naming attribute	samAccountName
Group naming attribute	cn
Group member attribute	memberOf
RFC 2307 Groups	<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership RFC 2307 style group membership has members listed on the group Active Directory style group membership (RFC 2307bis).
Group Object Class	group Object class used for groups in RFC2307 mode. Typically "posixGroup".
UTF8 Encode	<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server Required to support international characters, but may not be supported.
Username Alterations	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.
 Save	

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.

Authentication Test

Authentication ▼

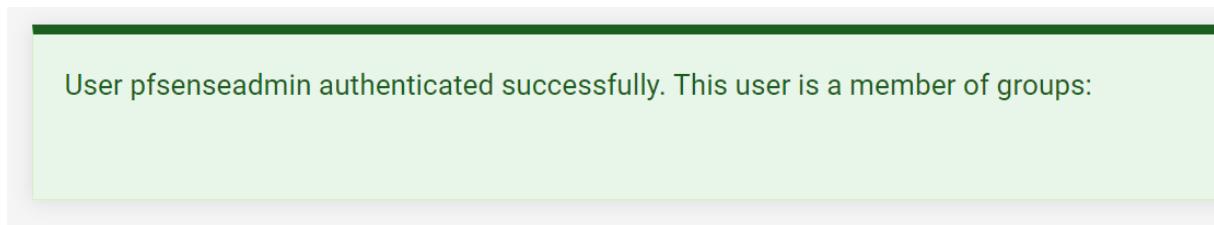
Server Select the authentication server to test against.

Username ...|

Password ...|

Test

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".

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	1	

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

Pour le scope on choisit Remote.

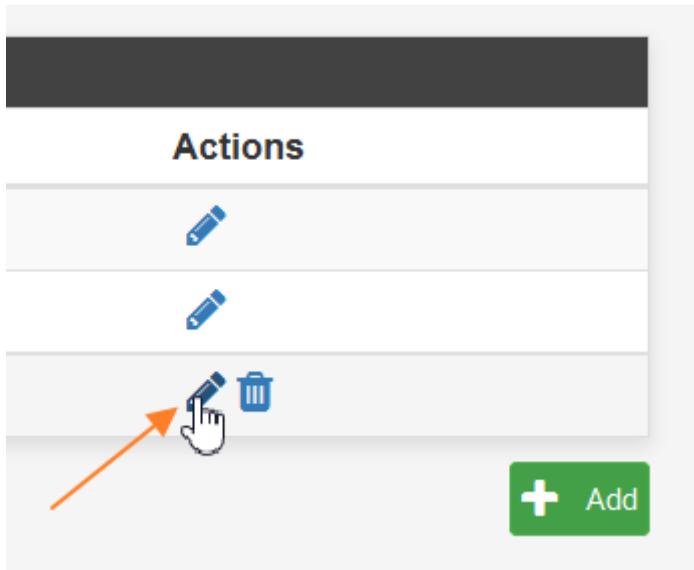
Et on sauvegarde

Group Properties

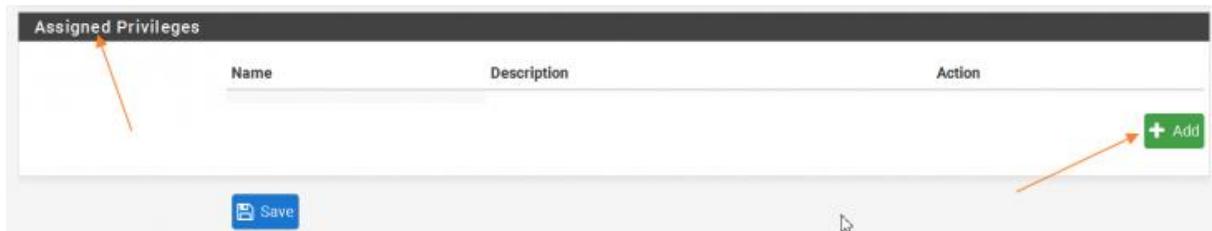
<u>Group name</u>	<input type="text" value="pfsense"/>	
<u>Scope</u>	Remote	
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.		
<u>Description</u>	<input type="text" value="Admin directory group"/> Group description, for administrative information only	
<u>Group membership</u>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> admin backup lucas maxime </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Not members </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Members </div>
<input members""="" type="button" value="» Move to "/> <input members""="" not="" type="button" value="« Move to "/>		
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.		

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 :

Add Privileges for pfSenseAccess

Assigned privileges

- WebCfg - OpenVPN: Clients
- WebCfg - OpenVPN: Client Specific Override
- WebCfg - OpenVPN: Servers
- WebCfg - Package: Edit
- WebCfg - Package: Settings
- WebCfg - pfSense wizard subsystem
- WebCfg - Services: Captive portal
- WebCfg - Services: Captive portal: Allowed Hostnames
- WebCfg - Services: Captive portal: Allowed IPs
- WebCfg - Services: Captive portal: Edit Allowed Hostnames
- WebCfg - Services: Captive portal: Edit Allowed IPs
- WebCfg - Services: Captive portal: Edit MAC Addresses
- WebCfg - Services: Captive portal: Edit Zones
- WebCfg - Services: Captive portal: File Manager
- WebCfg - Services: Captive portal: Mac Addresses
- WebCfg - Services: Captive portal Voucher Rolls
- WebCfg - Services: Captive portal Vouchers
- WebCfg - Services: Captive portal Zones
- WebCfg - Services: DHCP Relay
- WebCfq - Services: DHCP Server

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

 Save  Filter  Clear

On aurait pu ajouter d'autres priviléges 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.

System / User Manager / Settings

Users Groups **Settings** Authentication Servers

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is security risk!

Authentication Server

- it-connect.local
- it-connect.local**
- Local Database

 Save

 Save & Test

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 :

Login to pfSense

Username directeur01

Password 

Login

2. OpenVPN

2.1 Certificat d'autorité

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

Create / Edit CA

<u>Descriptive name</u>	Cert-Serv-VPN
<u>Method</u>	Create an internal Certificate Authority
<u>Trust Store</u>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted!
<u>Randomize Serial</u>	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed will be checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

<u>Key type</u>	RSA
	2048
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest Algorithm</u>	sha256
The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weak algorithms unsafe.	
<u>Lifetime (days)</u>	3650
<u>Common Name</u>	internal-ca
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	FR
<u>State or Province</u>	e.g. Texas
<u>City</u>	e.g. Austin
<u>Organization</u>	e.g. My Company Inc
<u>Organizational Unit</u>	e.g. My Department Name (optional)

2.2 Certificat de serveur

Add/Sign a New Certificate

<u>Method</u>	<input type="text" value="Create an internal Certificate"/>		
<u>Descriptive name</u>	<input type="text" value="Cert-Serv-VPN"/>		
Internal Certificate			
<u>Certificate authority</u>	<input type="text" value="CA-VPN"/>		
<u>Key type</u>	<input type="text" value="RSA"/>		
<input type="text" value="4096"/> <p>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</p>			
<u>Digest Algorithm</u>	<input type="text" value="sha256"/>		
<p>The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weak algorithms unsafe.</p>			
<u>Lifetime (days)</u>	<input type="text" value="398"/>		
<p>The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.</p>			
<u>Common Name</u>	<input type="text" value="serveur-VPN"/>		
<p>The following certificate subject components are optional and may be left blank.</p>			
<u>Country Code</u>	<input type="text" value="FR"/>		
<u>State or Province</u>	<input type="text" value="e.g. Texas"/>		
<u>City</u>	<input type="text" value="e.g. Austin"/>		
<u>Organization</u>	<input type="text" value="e.g. My Company Inc"/>		
<u>Organizational Unit</u>	<input type="text" value="e.g. My Department Name (optional)"/>		
Certificate Attributes			
<u>Attribute Notes</u>	<p>The following attributes are added to certificates and requests when they are created or signed. Learn more</p> <p>For Internal Certificates, these attributes are added directly to the certificate as shown.</p>		
<u>Certificate Type</u>	<input type="text" value="Server Certificate"/>		
<p>Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on the certificate.</p>			
<u>Alternative Names</u>	<input type="text" value="FQDN or Hostname"/> <table border="1"> <tr> <td>Type</td> <td>Value</td> </tr> </table>	Type	Value
Type	Value		
<p>Enter additional identifiers for the certificate in this list. The Common Name field is automatically populated with the certificate's common name. The signing CA may ignore or change these values.</p>			
Add	+ Add		

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

General Information

Description

A description of this VPN for administrative reference.

Disabled Disable this server

Set this option to disable this server without removing it from the list.

Unique VPN ID Server 5 (ovpns5)

Mode Configuration

Server mode

Backend for authentication
Local Database

Device mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

Interface

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

The port used by OpenVPN to receive client connections.

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. i	
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	<input checked="" type="checkbox"/> 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	<p>AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block)</p> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	<p>AES-256-GCM AES-128-GCM CHACHA20-POLY1305</p> <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p> <p>The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i</p>
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	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> 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)	<input type="text" value="192.168.99.0/24"/>	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)	<input type="text"/>	IPv6 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 rem network.
Concurrent connections	<input type="text"/>	Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>	Allow compression to be used with this VPN instance. 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.
		Asymmetric compression allows an easier transition when connecting with older peers.
Push Compression	<input type="checkbox"/>	Push the selected Compression setting to connecting clients.
Type-of-Service	<input type="checkbox"/>	Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input type="checkbox"/>	Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/>	Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will be rejected.
		Users are identified by their username or certificate properties, depending on the VPN configuration. This may be necessary in some environments.

Client Settings

Dynamic IP	<input type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="button" value="net30 – Isolated /30 network per client"/>	Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on Linux. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android) clients such as Yealink phones may require "net30".

Ping settings

Inactive	<input type="text" value="300"/>	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. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel not restart.
-----------------	----------------------------------	---

Advanced Configuration

Custom options `auth-nocache`

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

2.4 Création du VPN Client

Nous allons créer un VPN client pour tous nos users.

VPN / OpenVPN / Clients / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Description VPN-User-ALL
A description of this VPN for administrative reference.

Disabled Disable this client
Set this option to disable this client without removing it from the list.

Mode Configuration

Server mode Peer to Peer (SSL/TLS)

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

Endpoint Configuration

<u>Protocol</u>	UDP on IPv4 only
<u>Interface</u>	WAN
The interface used by the firewall to originate this OpenVPN client connection	
<u>Local port</u>	
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.	
<u>Server host or address</u>	pfsense.maxcaptab.com ...
The IP address or hostname of the OpenVPN server.	
<u>Server port</u>	1360
The port used by the server to receive client connections.	
<u>Proxy host or address</u>	
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.	
<u>Proxy port</u>	
<u>Proxy Authentication</u>	none
The type of authentication used by the proxy server.	

Cryptographic Settings

<u>TLS Configuration</u>	<input checked="" type="checkbox"/> 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.
	<input checked="" type="checkbox"/> Automatically generate a TLS Key.
<u>TLS keydir direction</u>	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.	
<u>Peer Certificate Authority</u>	CA-VPN
<u>Peer Certificate Revocation list</u>	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
<u>Client Certificate</u>	Cert-Serv-User-VPN (Server: Yes, CA: CA-VPN)
<u>Data Encryption Negotiation</u>	<input checked="" type="checkbox"/> 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

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

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

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

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.
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").

Tunnel Settings	
IPv4 Tunnel Network	<input type="text"/>
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.	
IPv6 Tunnel Network	<input type="text"/>
This is the IPv6 virtual network or network alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.	
IPv4 Remote network(s)	<input type="text" value="192.168.99.0/24"/>
IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.	
IPv6 Remote network(s)	<input type="text"/>
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.	
Limit outgoing bandwidth	<input type="text" value="Between 100 and 100,000,000 bytes/sec"/>
Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.	
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>
Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.	
Asymmetric compression allows an easier transition when connecting with older peers.	
Topology	<input type="button" value="net30 – Isolated /30 network per client"/>
Specifies the method used to configure a virtual adapter IP address.	
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Don't pull routes	<input type="checkbox"/> Bars the server from adding routes to the client's routing table This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.
Don't add/remove routes	<input type="checkbox"/> Don't add or remove routes automatically Do not execute operating system commands to install routes. Instead, pass routes to --route-up script using environmental variables.
Pull DNS	<input type="checkbox"/> Add server provided DNS If this option is set, pfSense will use DNS servers assigned by remote OpenVPN server for its own purposes (including the DNS Forwarder/DNS Resolver).

2.5 Exporter notre configuration vpn

Il faut d'abord installer le package suivant :

<input checked="" type="checkbox"/> openvpn-client-export	security	1.6.9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	
Package Dependencies:				
openvpn-client-export-2.5.8	openvpn-2.5.4_1	zip-3.0_1	p7zip-16.02_3	

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

Ensute nous allons dans OpenVPN puis dans Client Export.

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote Access Server

Client Connection Behavior

Host Name Resolution

Host Name Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client Do not include OpenVPN 2.5 settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this install is not signed, you may need special software to deploy it correctly.

Bind Mode If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Puis on export le certificat

maxime Cert-User-Maxime

- Inline Configurations:

[!\[\]\(1018cbaeb8126d17d20a2e98d8cdfd8d_img.jpg\) Most Clients](#) [!\[\]\(9f275a784d5961bd413806a3c0ffd217_img.jpg\) Android](#)

[!\[\]\(81a877a766e087aed60100a3a71e8a32_img.jpg\) OpenVPN Connect \(iOS/Android\)](#)

- Bundled Configurations:

[!\[\]\(af24d1a65839592fd91008e40516ab2d_img.jpg\) Archive](#) [!\[\]\(a8e6e45d6cdf4d2d4713ad25db8723b8_img.jpg\) Config File Only](#)

- Current Windows Installers (2.5.8-lx04):

[!\[\]\(f3cba4e51d91c28be6b6bae16f344082_img.jpg\) 64-bit](#) [!\[\]\(15ad35bd864d94590d3763a83978db4b_img.jpg\) 32-bit](#)

- Legacy Windows Installers (2.4.12-lx01):

[!\[\]\(e03df13717a2a892541a5a08341b946c_img.jpg\) 10/2016/2019](#) [!\[\]\(a330598aaeca4f4378454fb3b5cf3d0b_img.jpg\) 7/8/8.1/2012r2](#)

- Viscosity (Mac OS X and Windows):

[!\[\]\(c556be75167b5ddd16fd6fcb9c7888f5_img.jpg\) Viscosity Bundle](#) [!\[\]\(711ba964d161cf2bf5ce74d79ab8a167_img.jpg\) Viscosity Inline Config](#)

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 :

<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.99.99	443 (HTTPS)			
<input type="checkbox"/>	<input checked="" type="checkbox"/>		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 :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	59 /5.63 GiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 /0 B	IPv6 TCP	LAN net	*	*	443 (HTTPS)	*	none
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓ 0 /38 KiB	IPv4 TCP	192.168.99.99	*	*	587 (SUBMISSION)	*	none		
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	192.168.10.100	25 (SMTP)	*	none		SMPT
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	192.168.10.100	995 (POP3/S)	*	none		POP3 TLS
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	192.168.99.100	993 (IMAP/S)	*	none		IMAP TLS
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	192.168.99.100	143 (IMAP)	*	none		IMAP
<input type="checkbox"/>	✓ 0 /40.90 MiB	IPv4 TCP	LANDMZ net	*	192.168.10.10	389 (LDAP)	*	none		
<input type="checkbox"/>	✓ 0 /1012.75 MiB	IPv4 TCP/UDP	LANDMZ net	*	*	443 (HTTPS)	*	none		
<input type="checkbox"/>	✓ 0 /776.60 MiB	IPv4 TCP/UDP	LANDMZ net	*	*	80 (HTTP)	*	none		
<input type="checkbox"/>	✓ 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
<input type="checkbox"/>	✓ 2 /605 KiB	IPv4 TCP	10.0.1.0/24	*	LAN address	443 (HTTPS)	*	none			   
<input type="checkbox"/>	✓ 6 /44.24 MiB	IPv4 TCP	*	*	192.168.99.99	9443	*	none			   
<input type="checkbox"/>	✓ 2 /193.39 MiB	IPv4 TCP	*	*	192.168.99.99	443 (HTTPS)	*	none			   
<input type="checkbox"/>	✓ 2 /7.80 MiB	IPv4 TCP	10.0.1.0/24	*	192.168.99.99	22 (SSH)	*	none			   
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	10.0.1.0/24	*	192.168.99.110	22 (SSH)	*	none			   
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	10.0.1.0/24	*	192.168.99.120	22 (SSH)	*	none			   
<input type="checkbox"/>	✓ 0 /2.17 MiB	IPv4 TCP	10.0.1.0/24	*	192.168.99.120	9000	*	none			   
<input type="checkbox"/>	✓ 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 :

```
13) Update from console
```

6. Gestion des accès

Nous utilisons des mots de passe 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/api/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.redirects.entryPoint.to=https'
    - '--entryPoints.http.http.redirects.entryPoint.scheme=https'
    #- '--entrypoints.web.address=:80'
    #- '--entrypoints.web.http.redirects.entryPoint.to=websecure'
    #- '--entrypoints.web.http.redirects.entryPoint.scheme=https'
    #- '--entrypoints.web.http.redirects.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=group))
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: S1j^2tvRREiA86Rgaw%G^1E1%mC8H*o#rq#jWU0vkwFHCa*
    issuer_private_key: | ****
  clients:
    -
      id: nextcloudID
      description: Nextcloud

```

```
secret:  
' !HydLZ2RcQwvOzwlgqr2epM0S*!XrmaMG@rcc5*ebFc3z4$UciBOV5z17BCHZJklu@7Is0Qd4IhI  
'  
  
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



Create an **admin account**

Username

A text input field containing the text "admin". To the right of the input field is a small red rectangular button with three white dots.

Password

A password input field showing five asterisks ("*****"). To the right of the input field is a small red rectangular button with three white dots, and next to it is a small eye icon.

Install

Need help? See the documentation

On installe ensuite les applications recommandées :



Recommended apps



Calendar

Schedule work & meetings, synced with all your devices.



Contacts

Keep your colleagues and friends in one place without leaking their private info.



Mail

Simple email app nicely integrated with Files, Contacts and Calendar.



Nextcloud Office

Collaborative documents, spreadsheets and presentations, built on Collabora Online.



Notes

Distraction free note taking app.



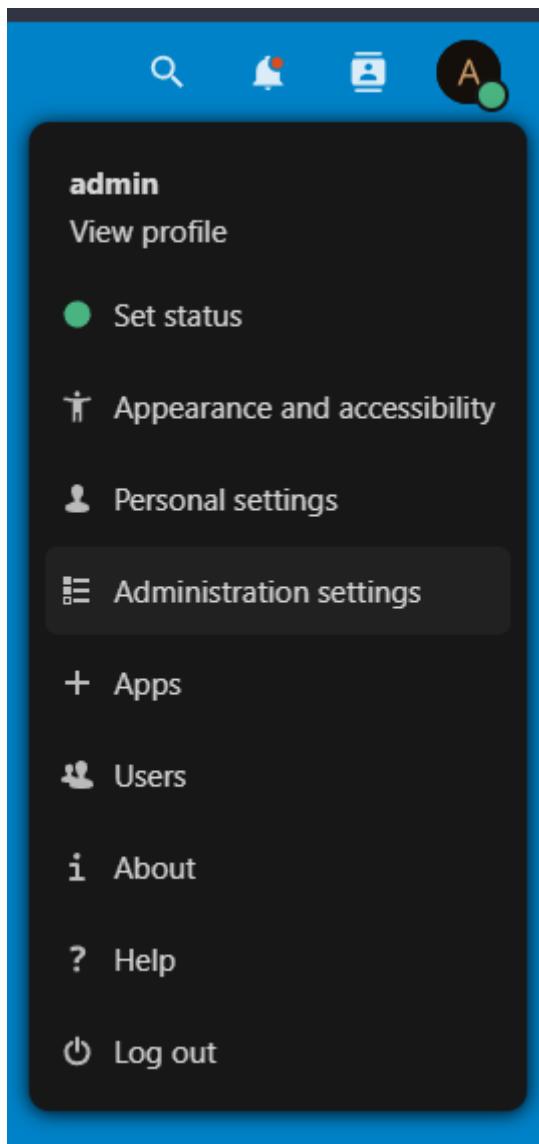
Talk

Chatting, video calls, screensharing, online meetings and web conferencing – in your browser and with mobile apps.

Skip

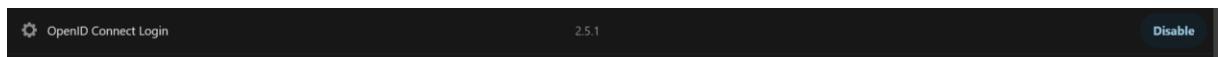
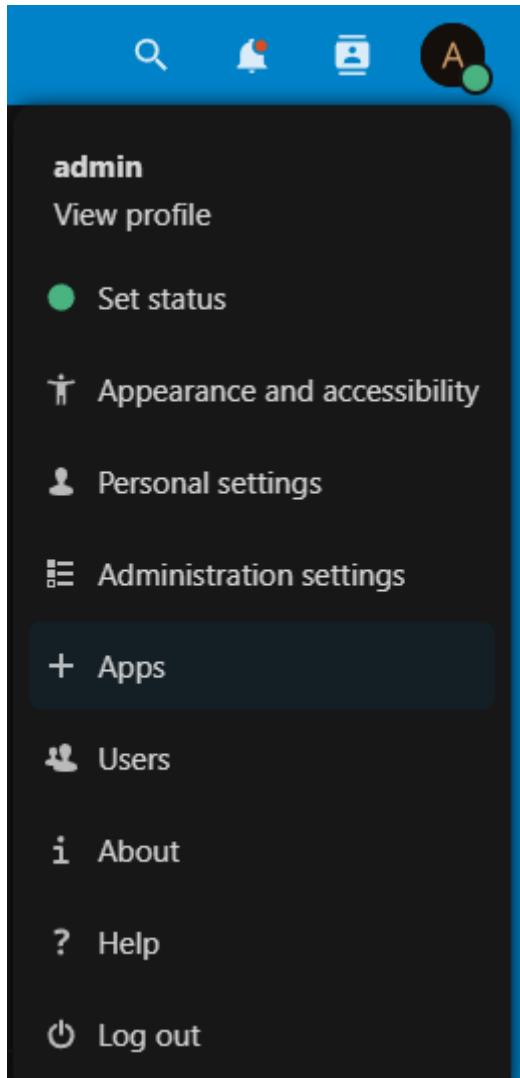
Install recommended apps

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



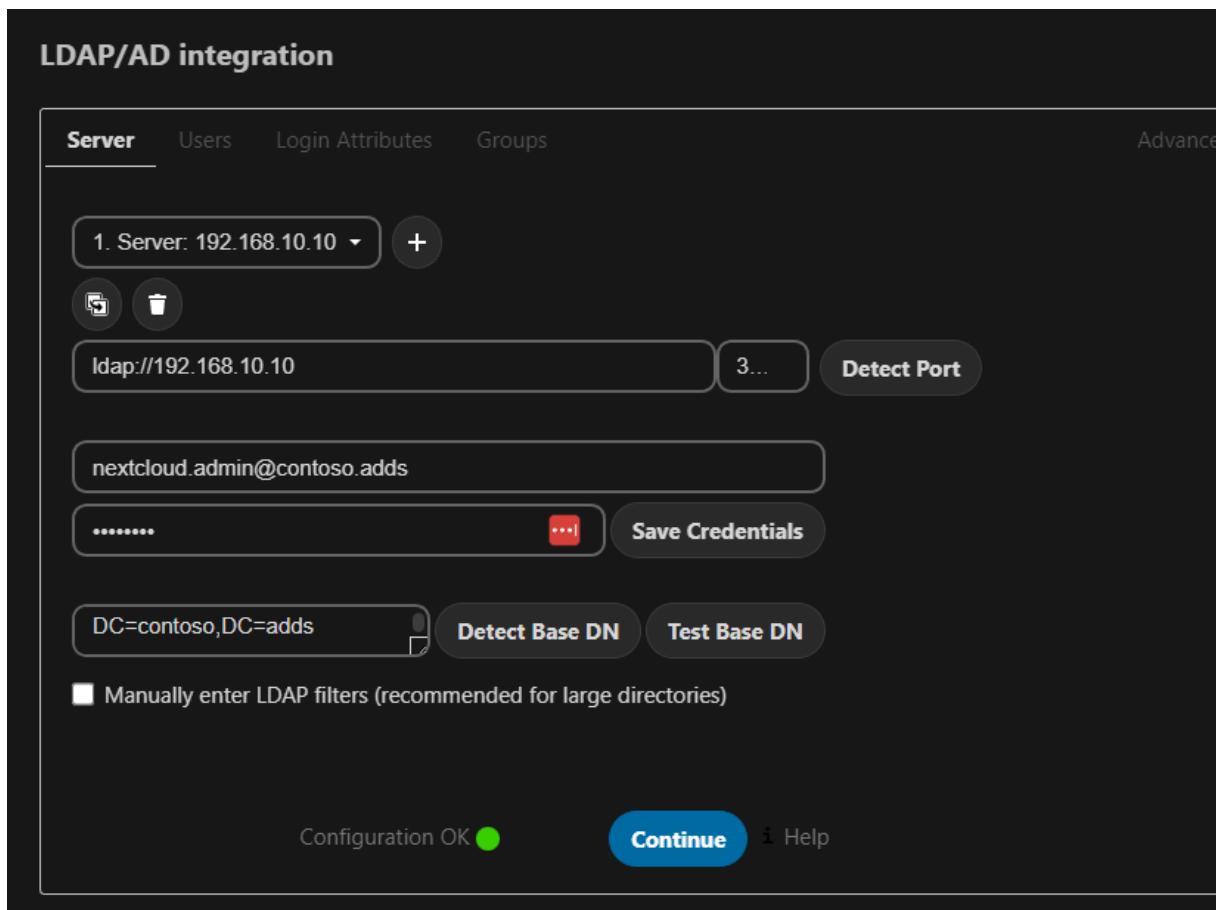
Application SSO

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 autorisons 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 administratif 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 besoin 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,

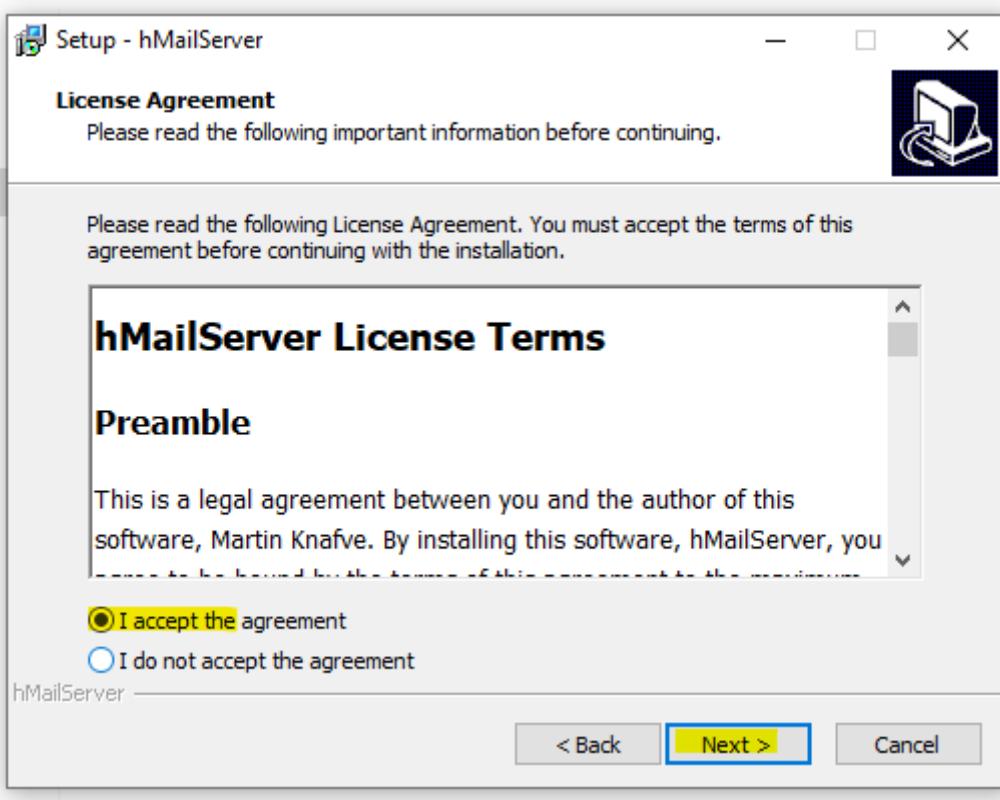
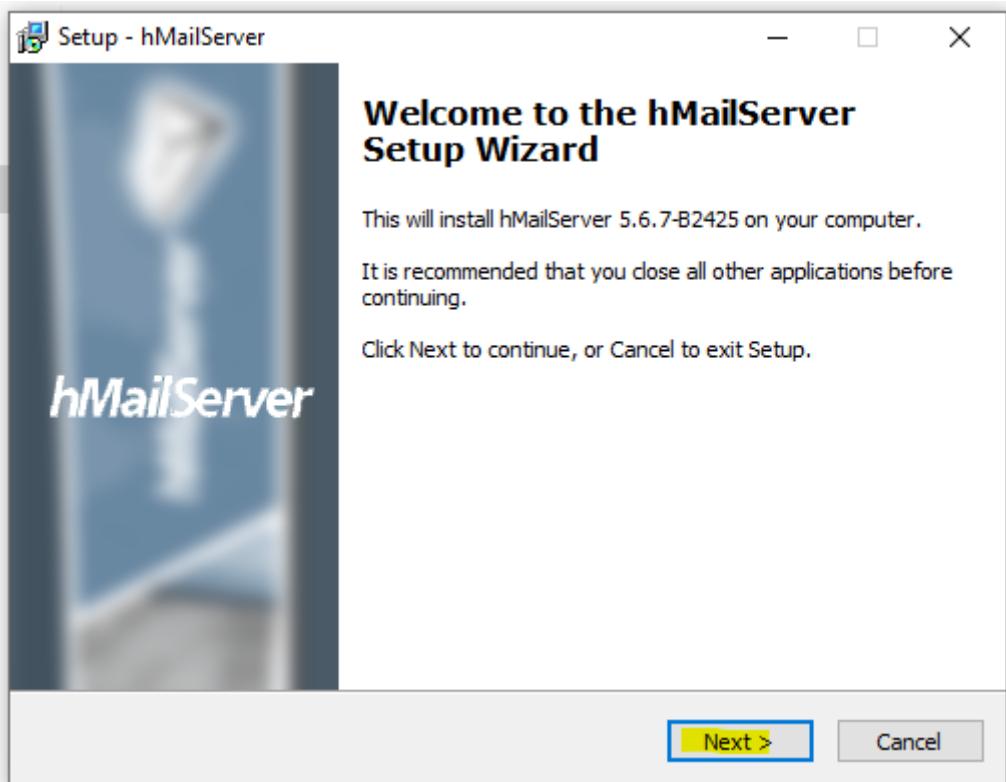
1 cœur par processeur

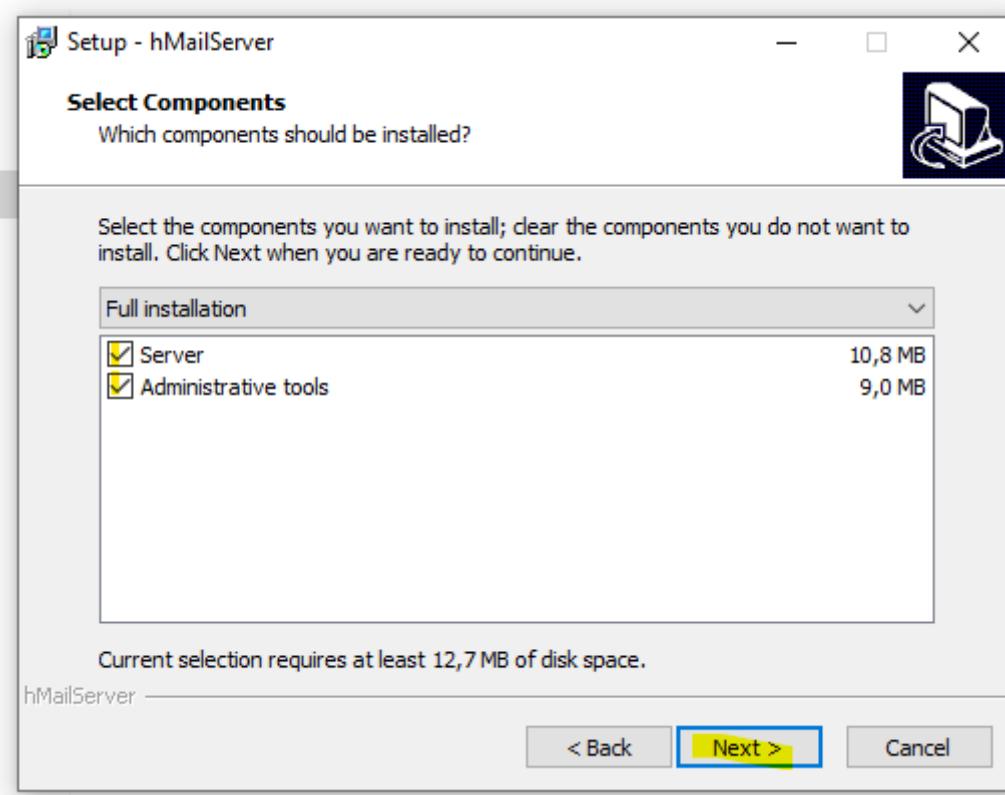
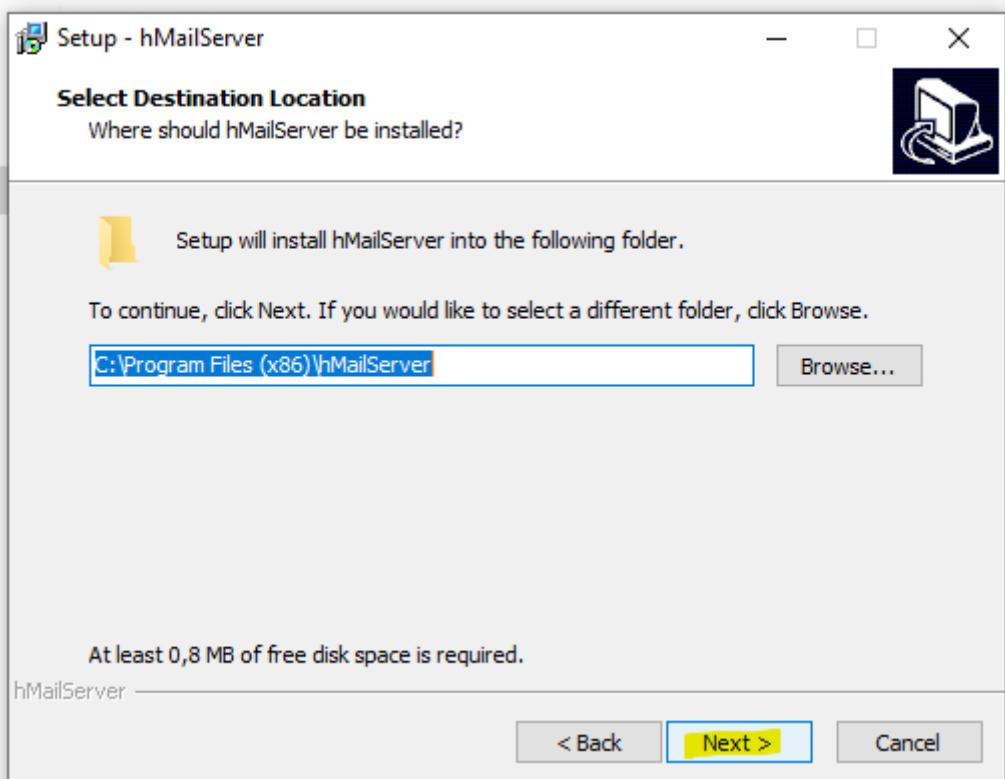
4GB de ram

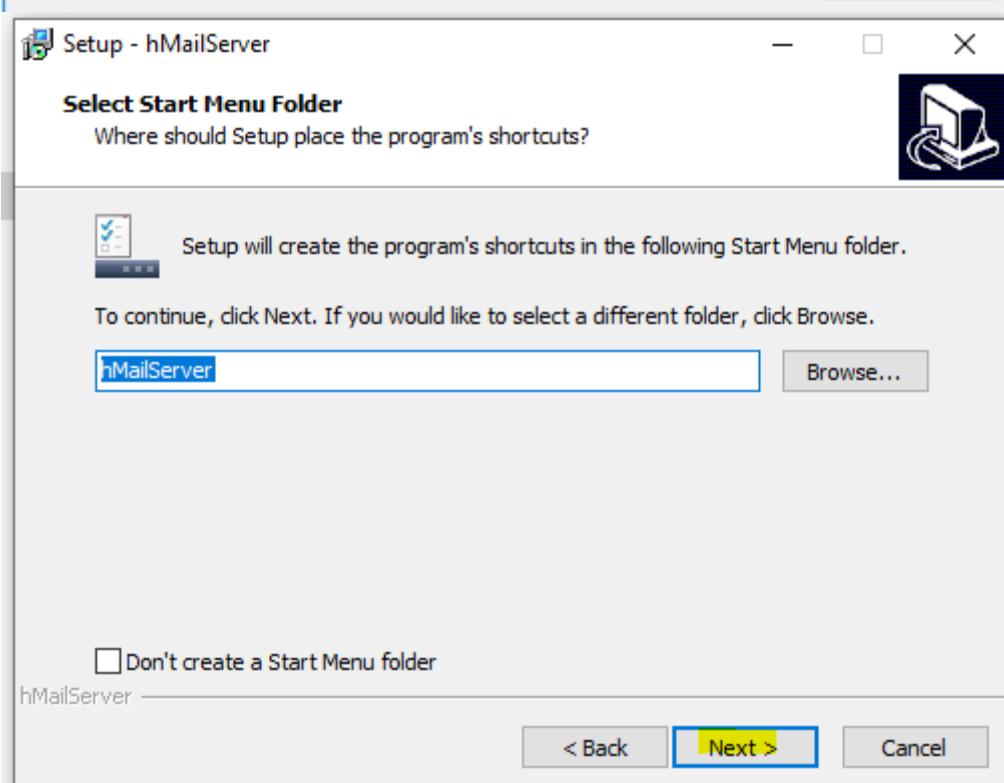
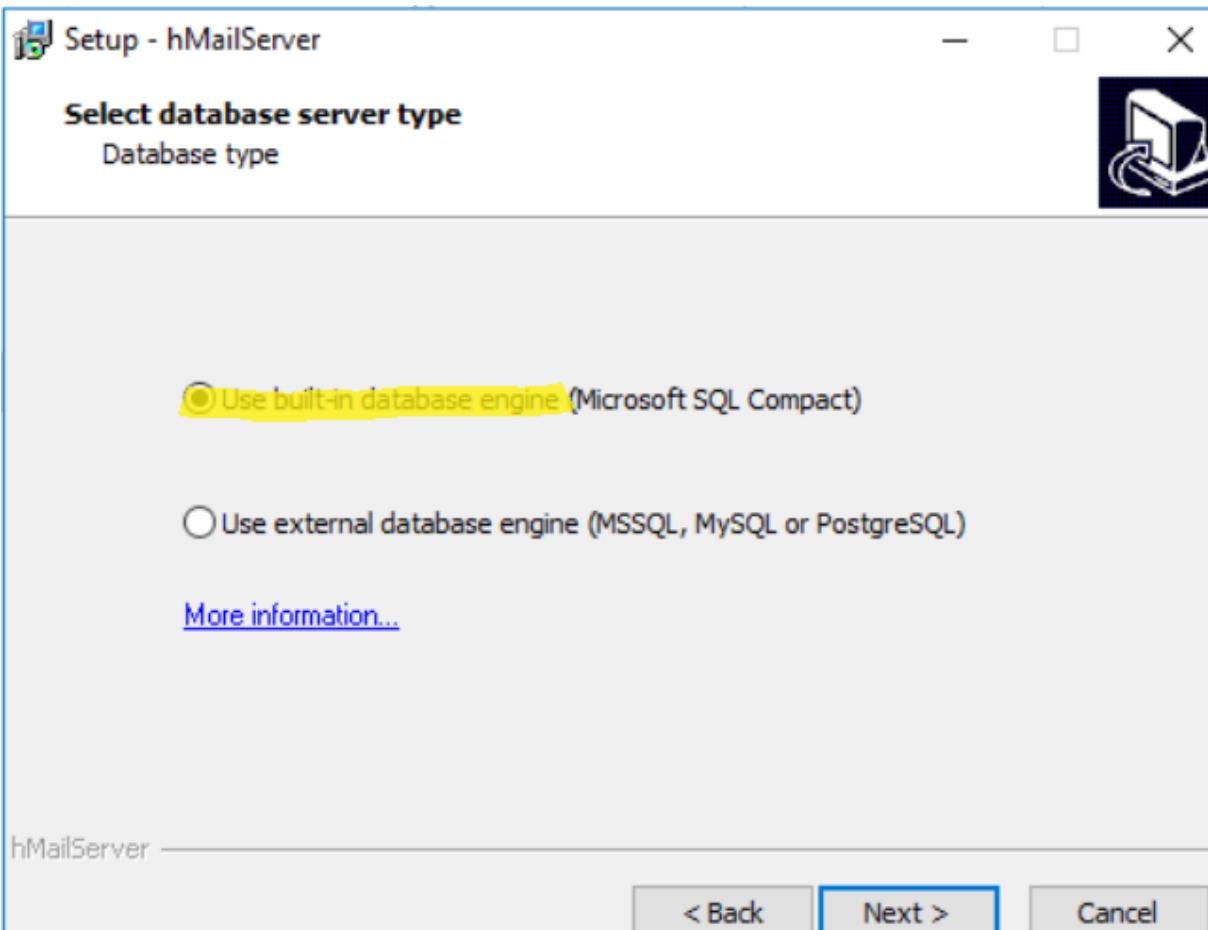
60GB de disque virtuel en SCSI

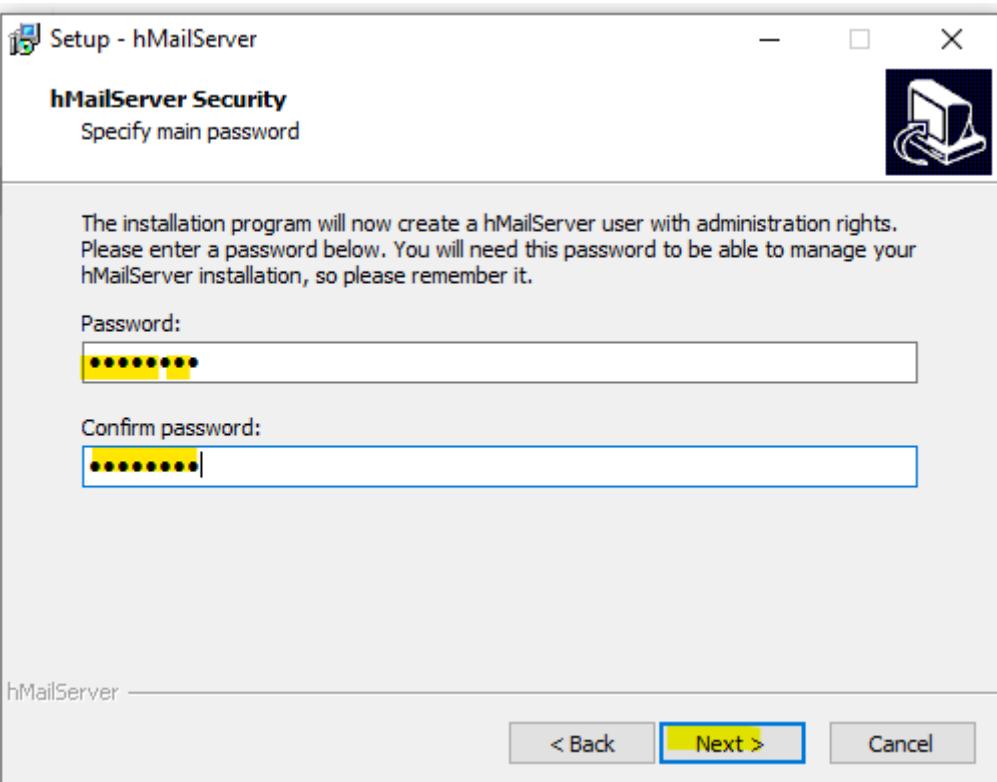
3. Configuration logicielle

1. Setup de l'application hmailserv

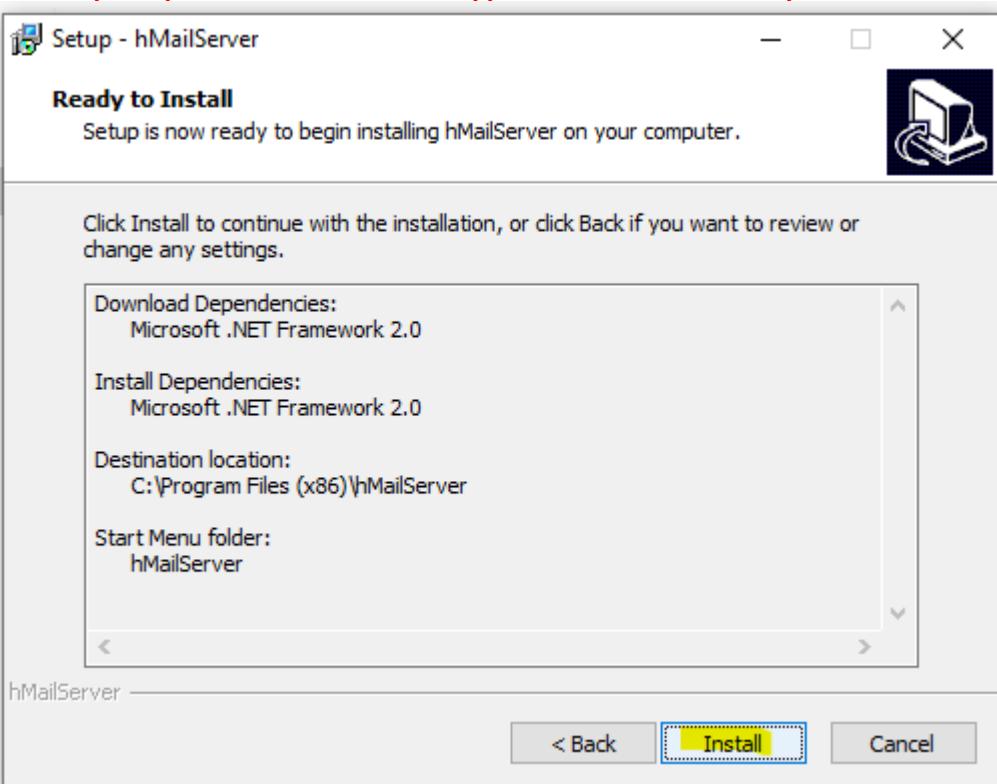


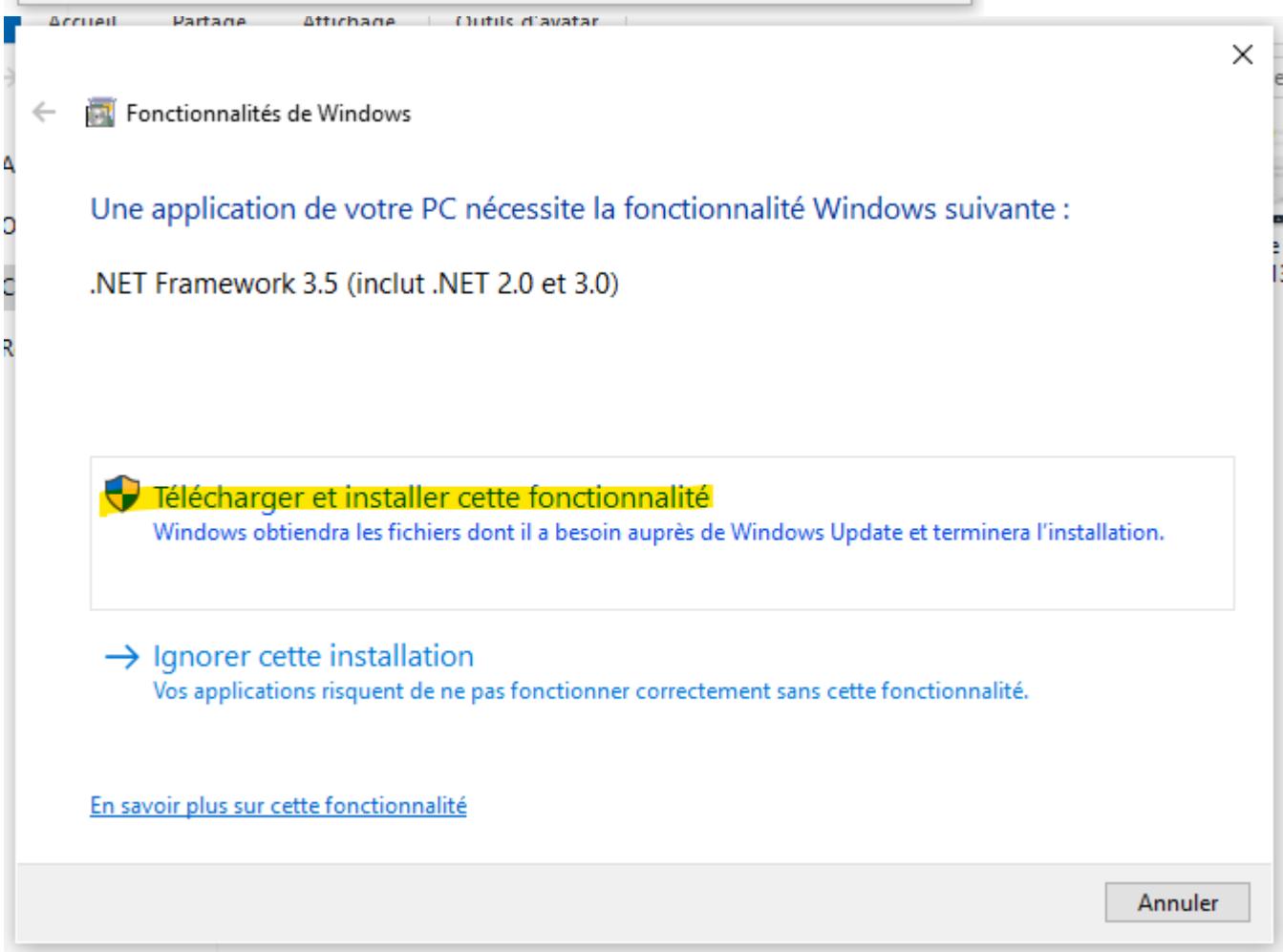
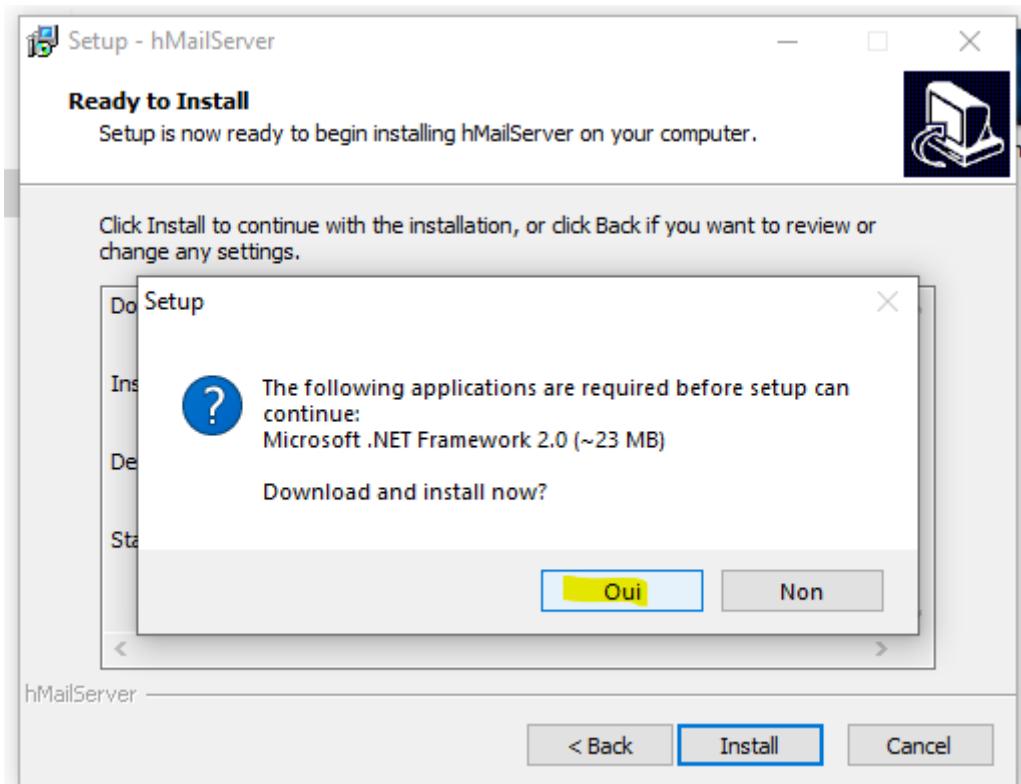


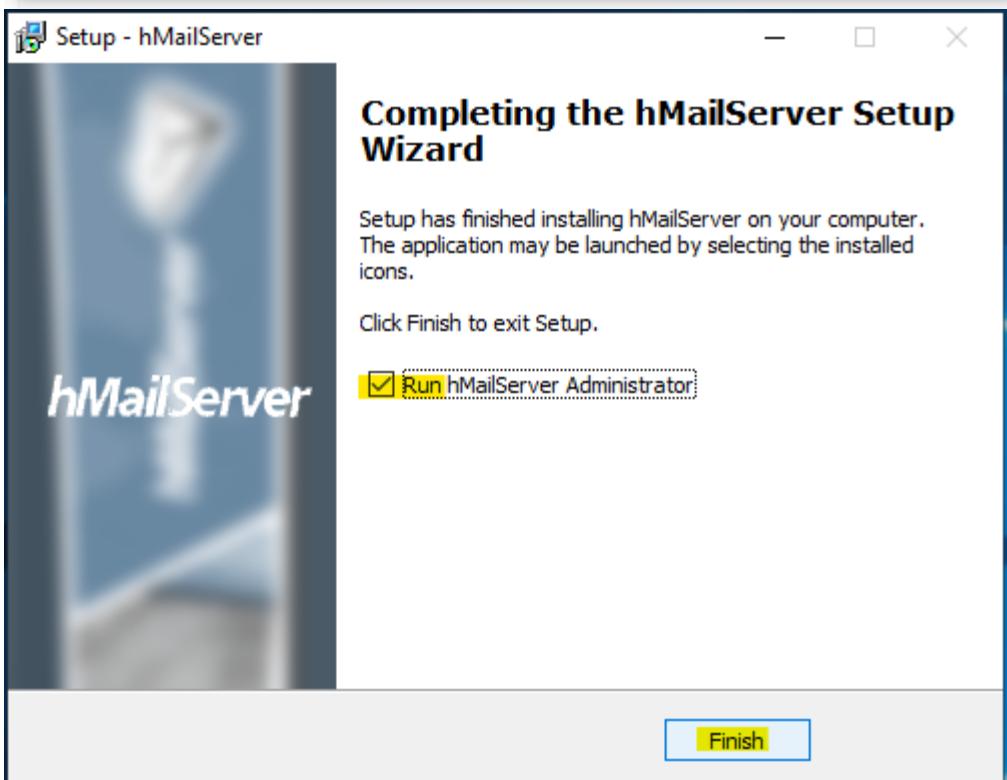
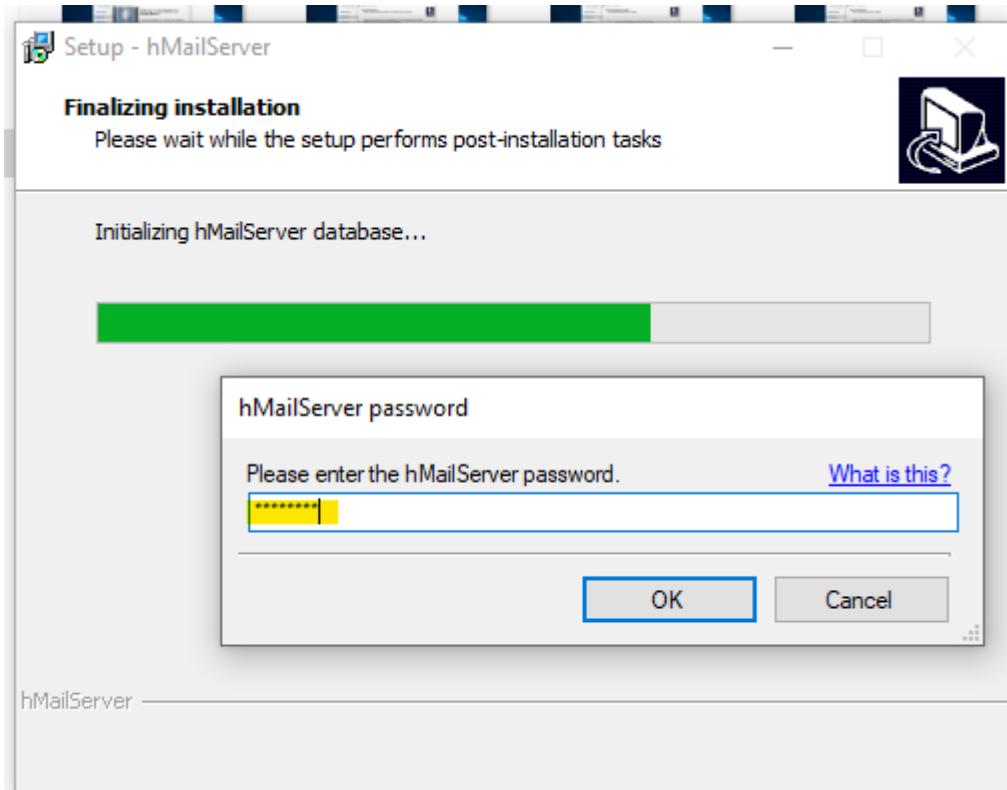




* Mot de passe pour l'administration de l'application. Il sera demandé pour accéder à l'interface.

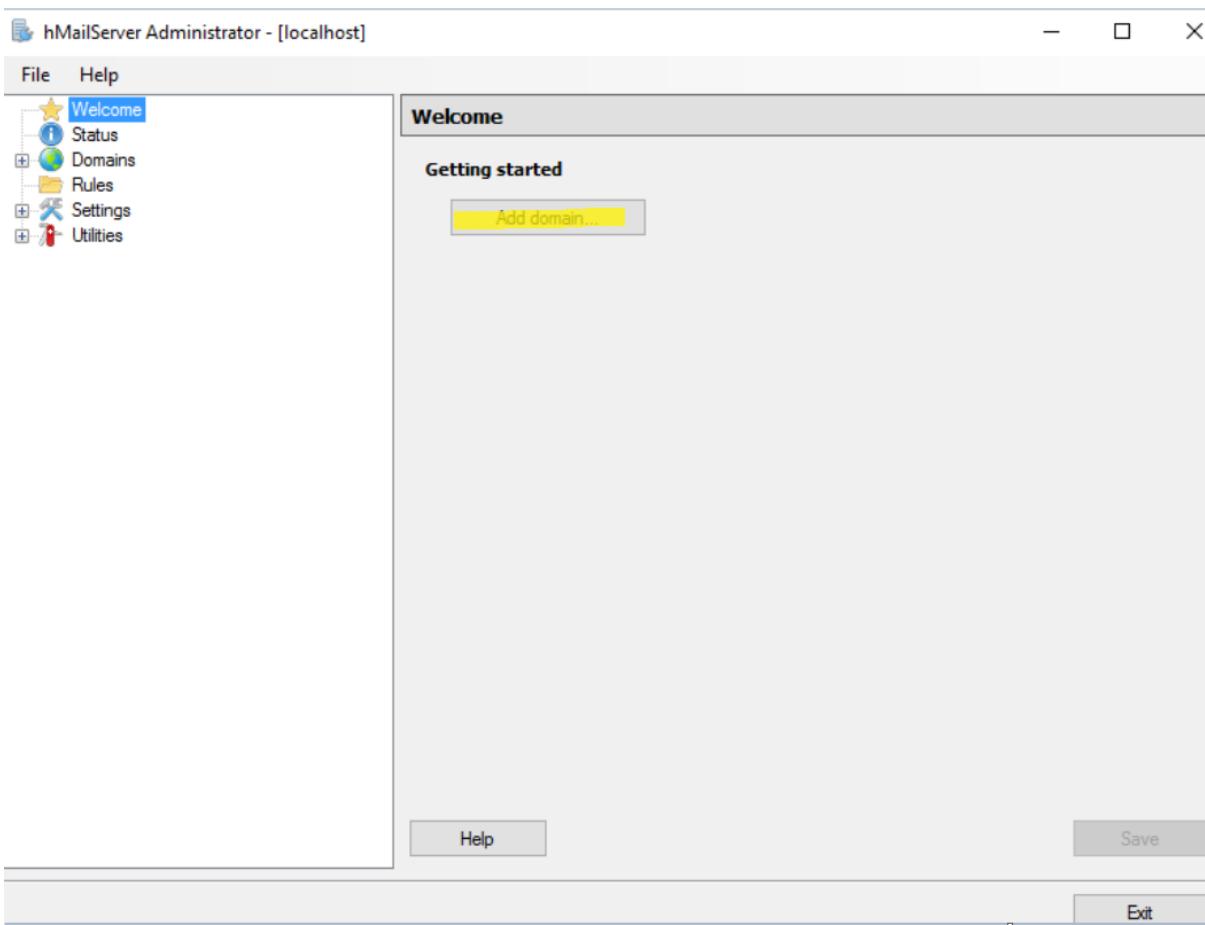
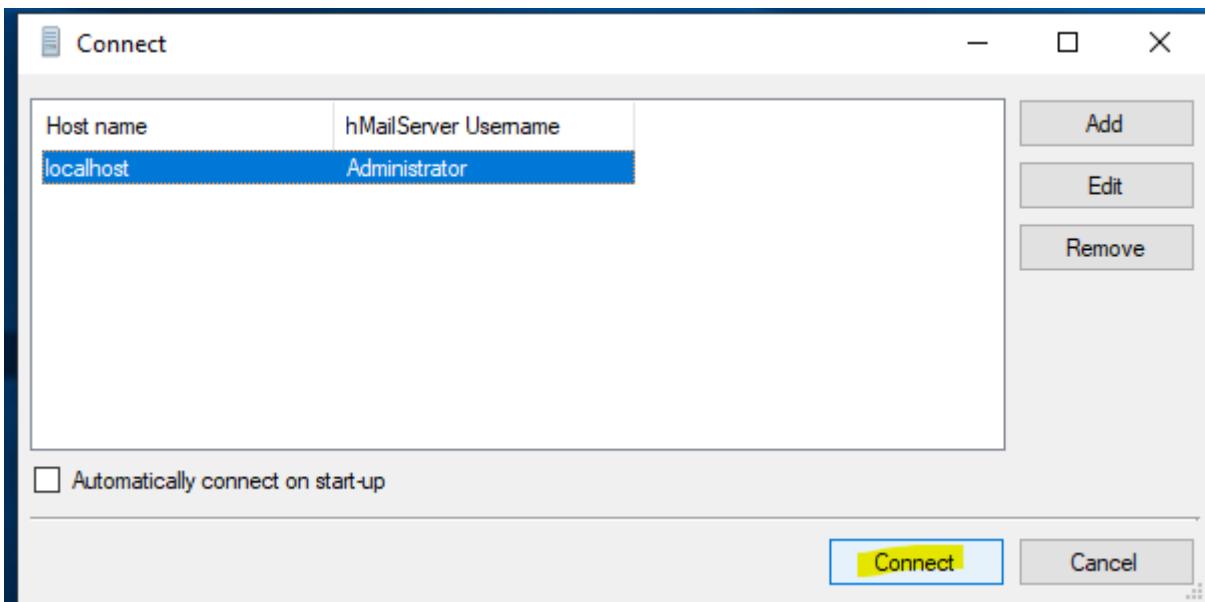


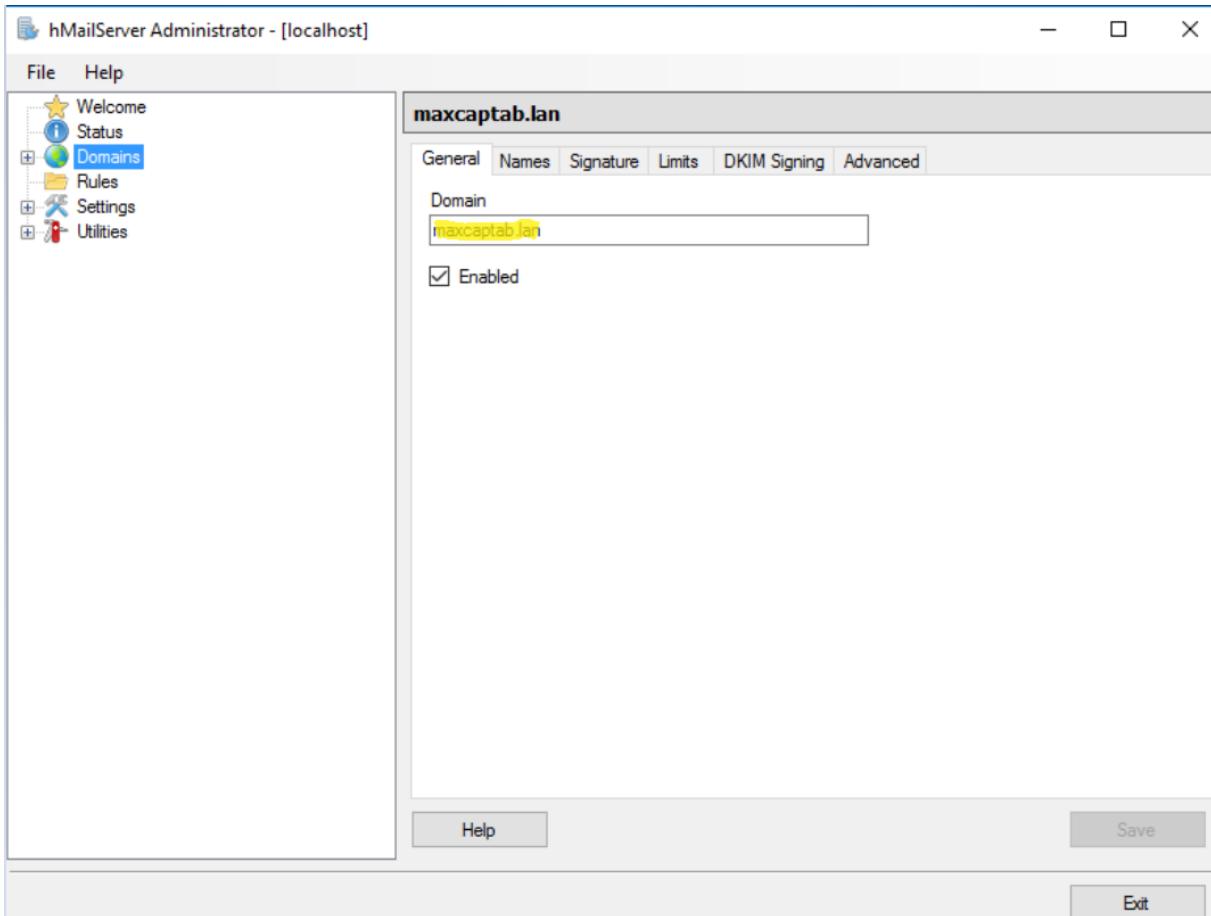




- L'application hMailServer est installée !!!

- Configuration





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

hMailServer Administrator - [localhost]

File Help

Welcome Status Domains Rules Settings Protocols SMTP POP3 IMAP Anti-spam Anti-virus Logging Advanced Utilities

SMTP

General Delivery of e-mail Statistics RFC compliance Advanced

Delivery of e-mail

Number of retries: 4 Minutes between every retry: 60

Local host name: mail/maxcaptab.fr

SMTP Relayer

Remote host name: Remote TCP/IP port: 25

Server requires authentication

User name:

Password: << Encrypted >>

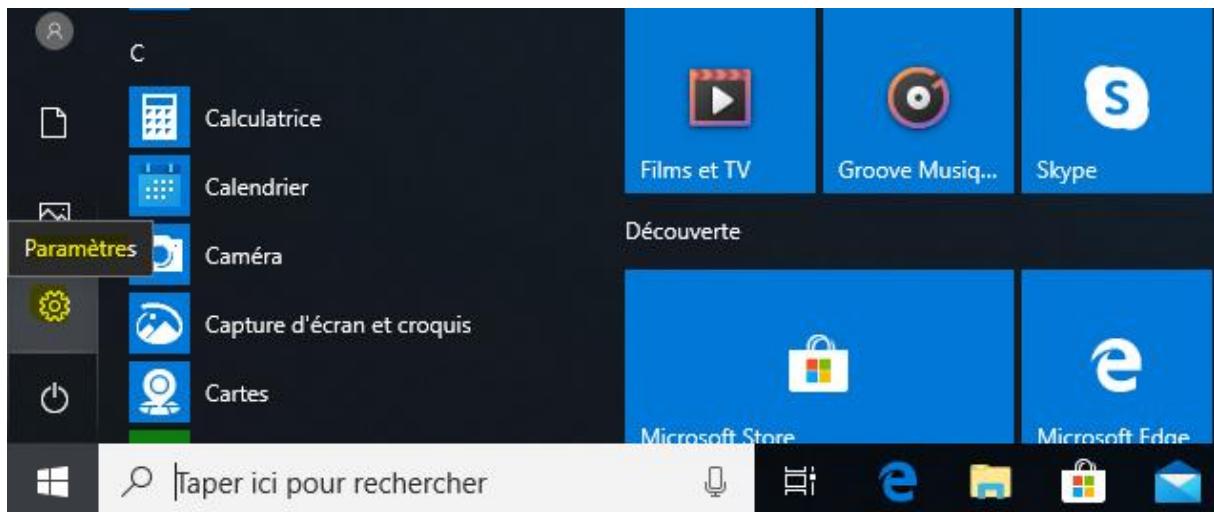
Connection security: None

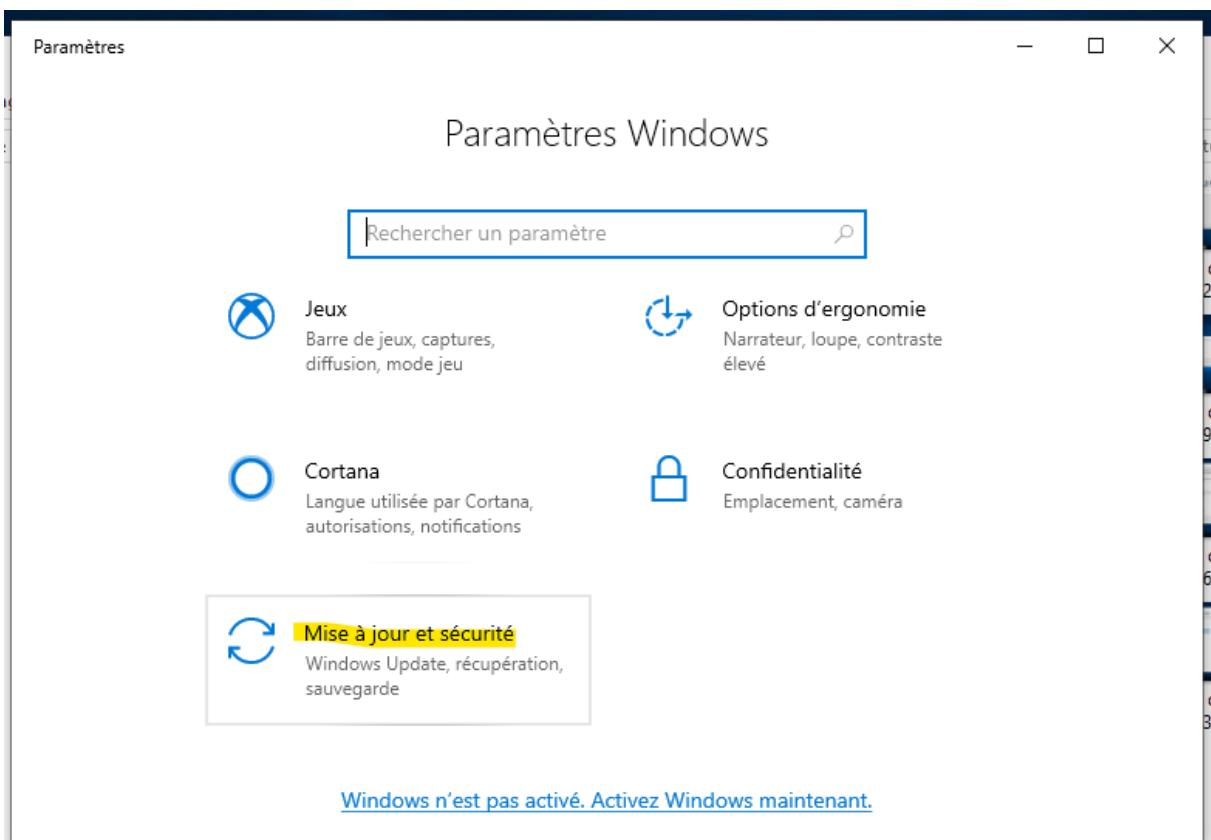
Help Save Exit

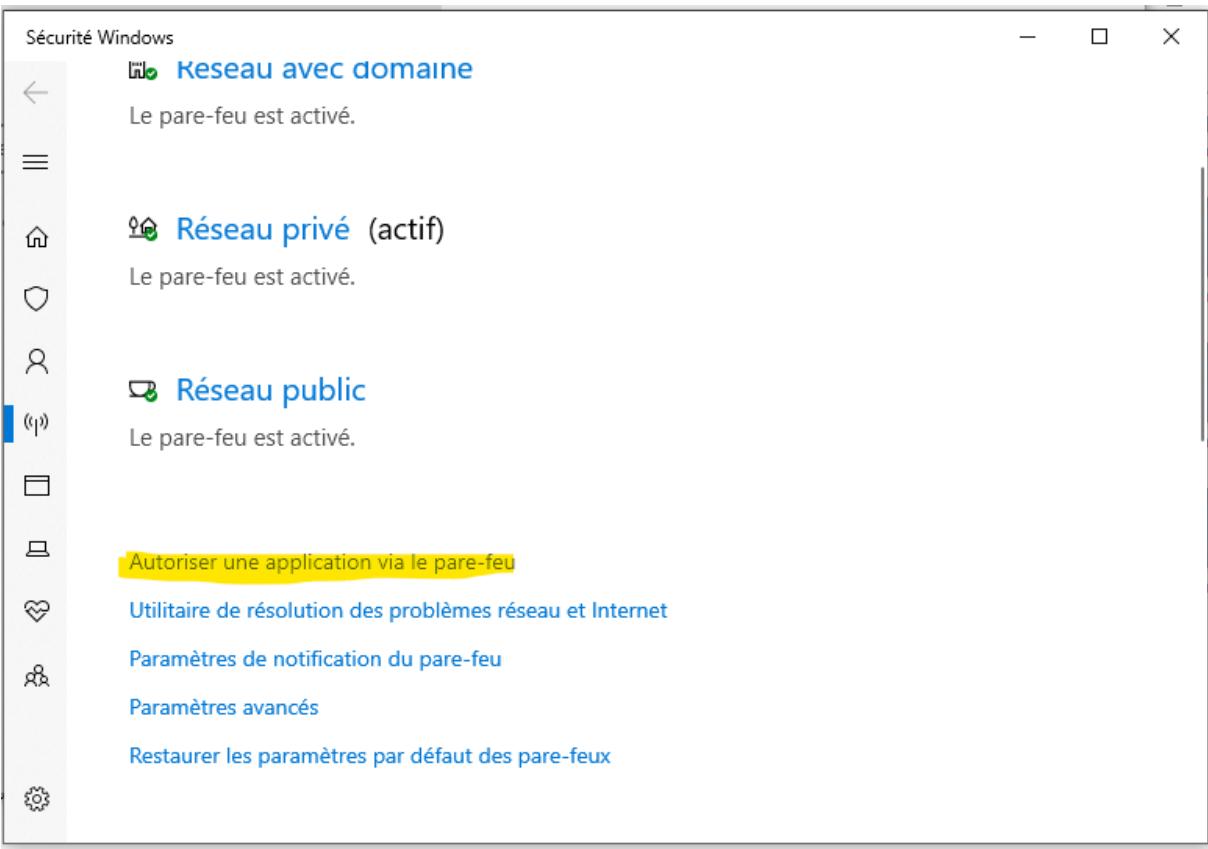
The screenshot shows the hMailServer Administrator interface. On the left is a navigation tree with items like Welcome, Status, Domains, Rules, Settings, Protocols (with SMTP selected), POP3, IMAP, Anti-spam, Anti-virus, Logging, Advanced, and Utilities. The main right pane is titled 'SMTP' and has tabs for General, Delivery of e-mail (which is selected and highlighted in yellow), Statistics, RFC compliance, and Advanced. Under 'Delivery of e-mail', there are fields for 'Number of retries' (set to 4) and 'Minutes between every retry' (set to 60). The 'Local host name' field contains 'mail/maxcaptab.fr'. Below this is the 'SMTP Relayer' section with fields for 'Remote host name' and 'Remote TCP/IP port' (set to 25), and a checkbox for 'Server requires authentication'. There are also fields for 'User name' and 'Password' with an 'Encrypted' button, and a dropdown for 'Connection security' set to 'None'. At the bottom are buttons for 'Help', 'Save', and 'Exit'.

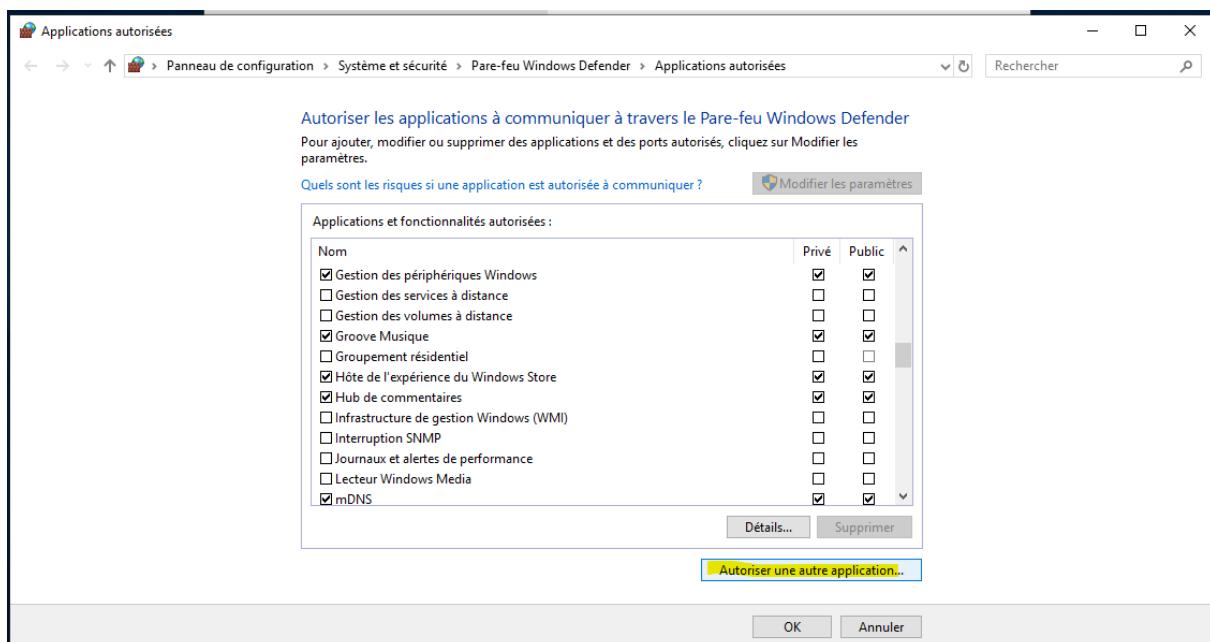
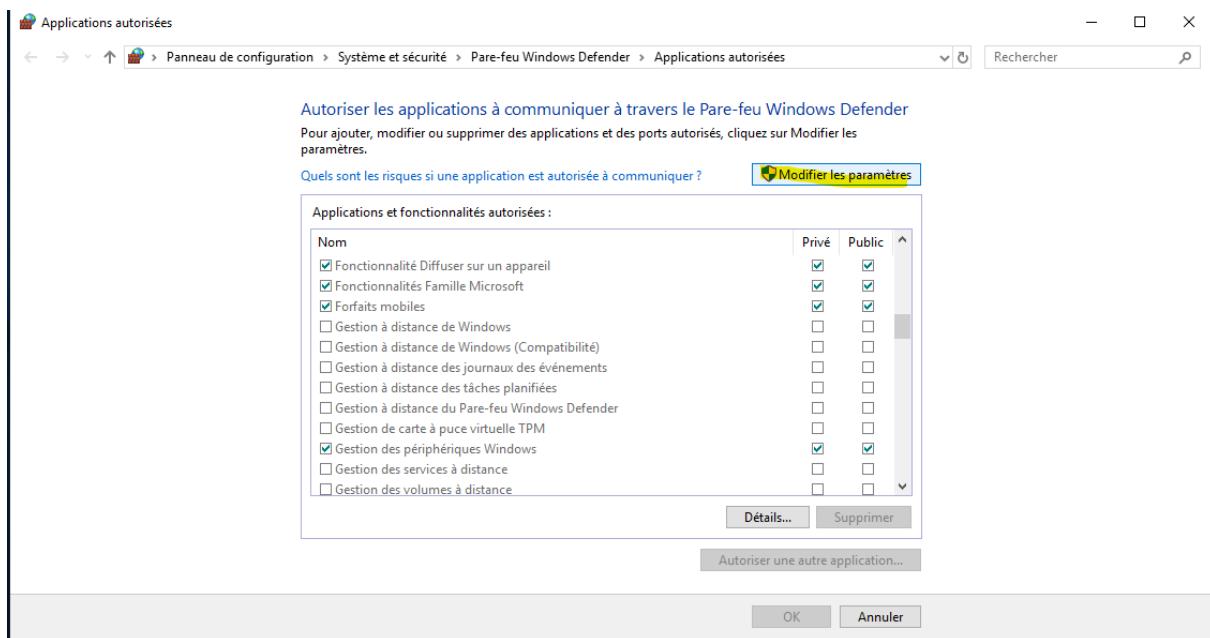
4. Gestion de la sécurité

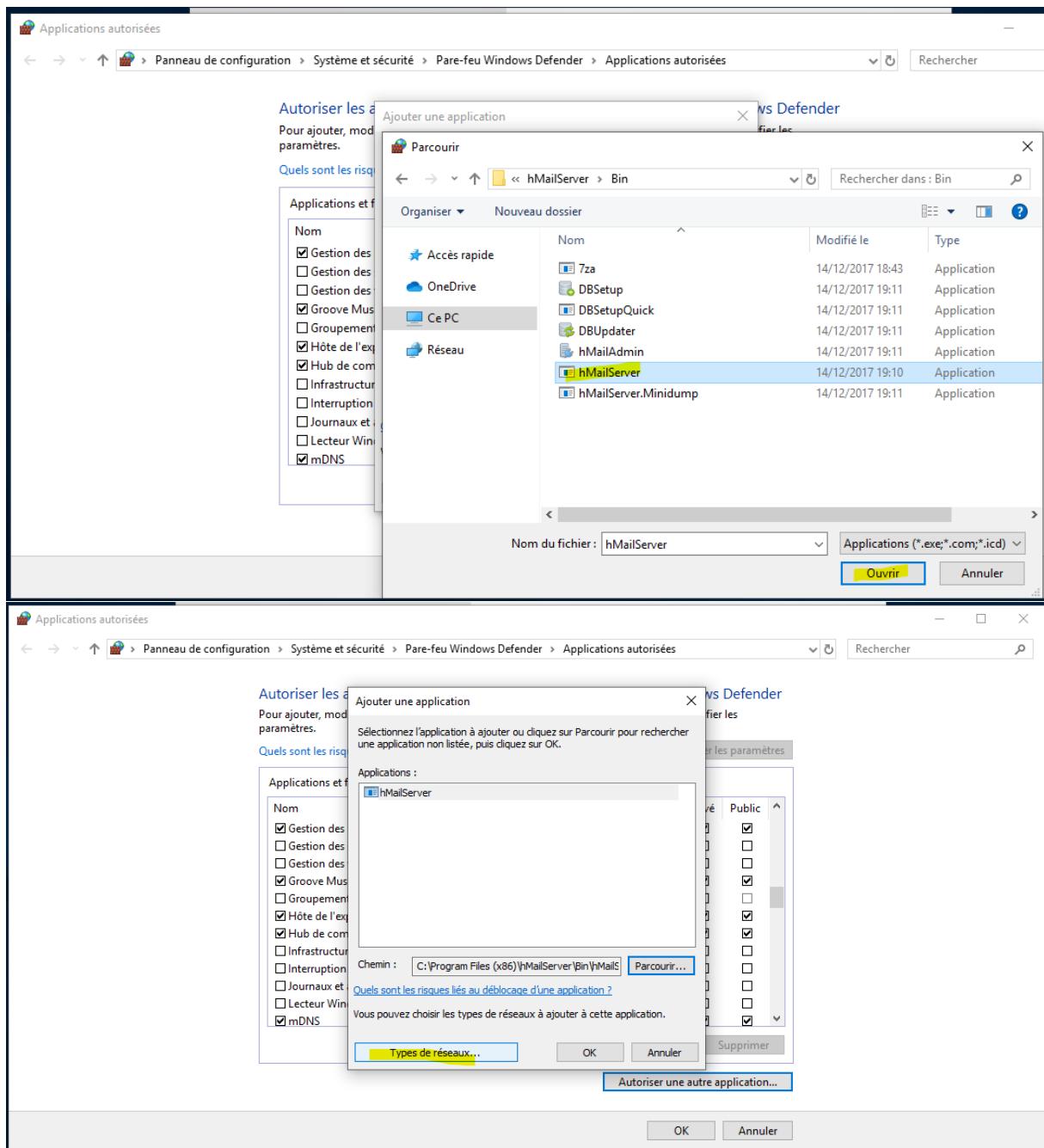
Afin de pouvoir interroger le service depuis une autre machine, il faut autoriser la connexion à hMailServer au niveau du pare-feu (Firewall)

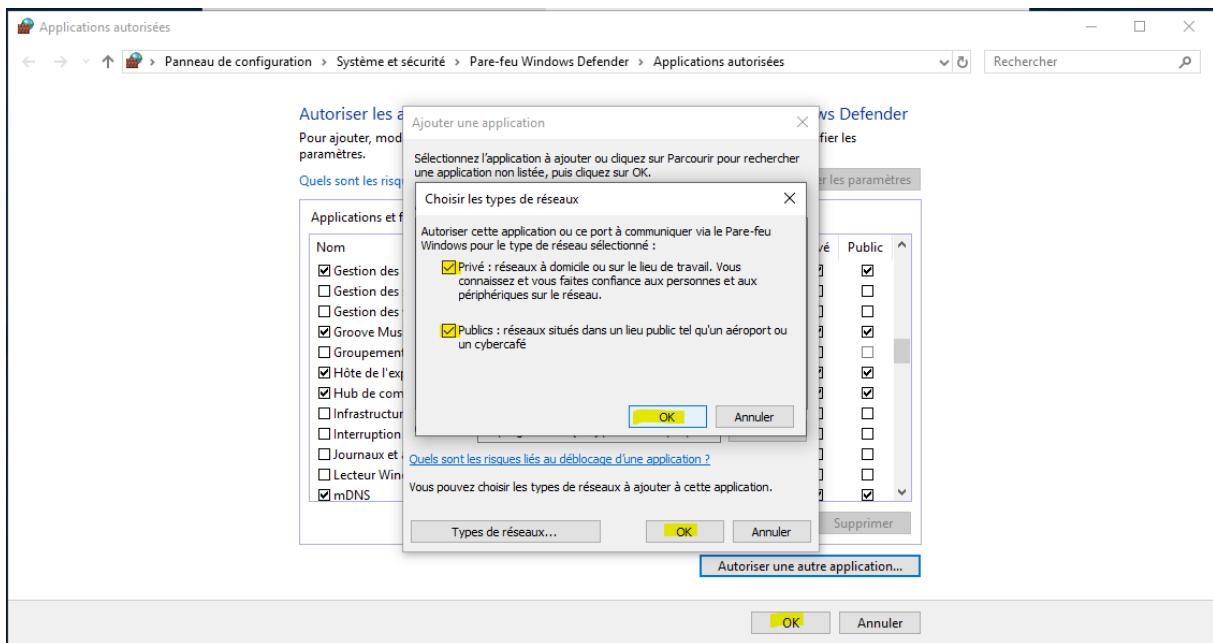












5. Gestion des logs

The screenshot shows the hMailServer Administrator interface. The left sidebar contains a navigation tree with sections like Welcome, Status, Domains, Accounts, Aliases, Distribution lists, Rules, Settings (Protocols: SMTP, POP3, IMAP, Groups; Anti-spam, Anti-virus, Logging, Advanced), Utilities, and Help.

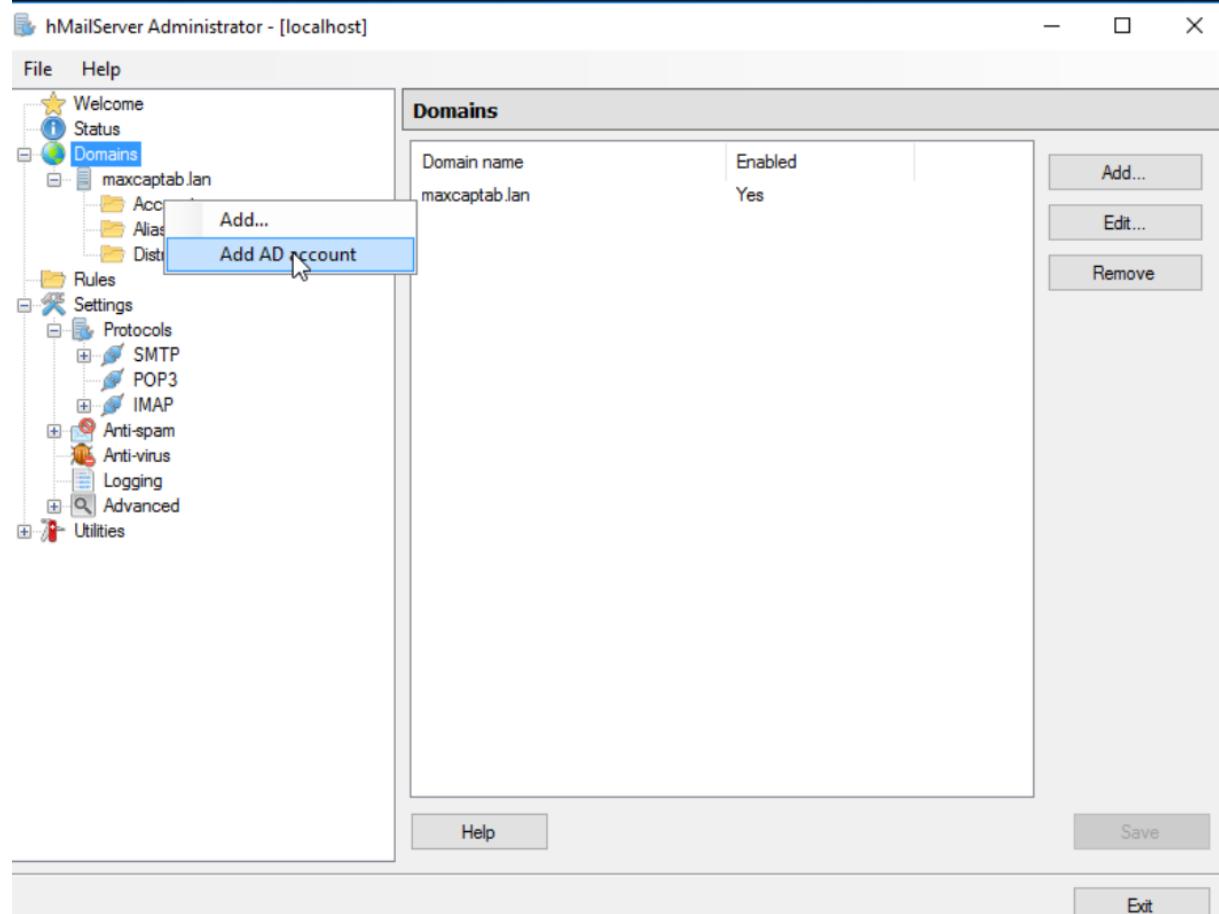
The main pane is titled "Logging". It has three sections:

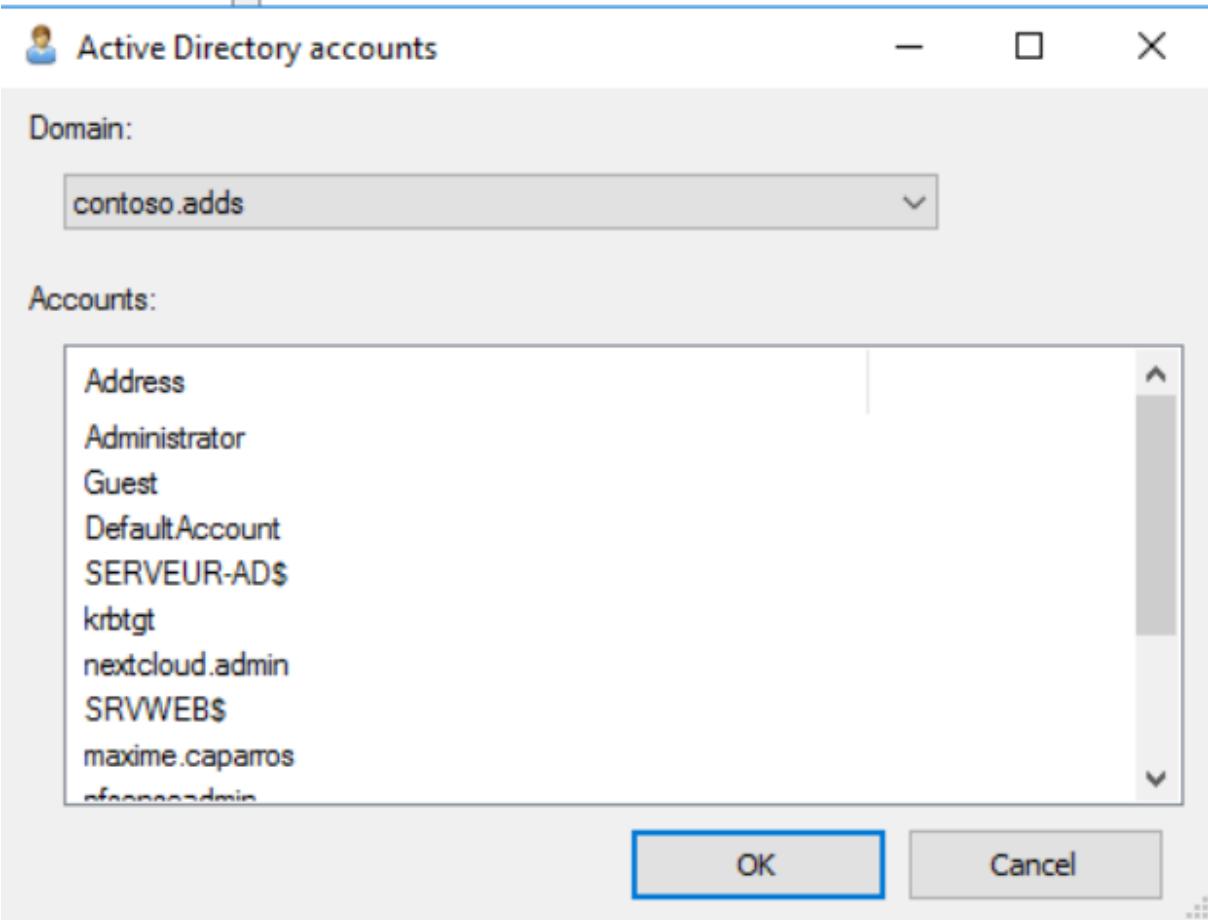
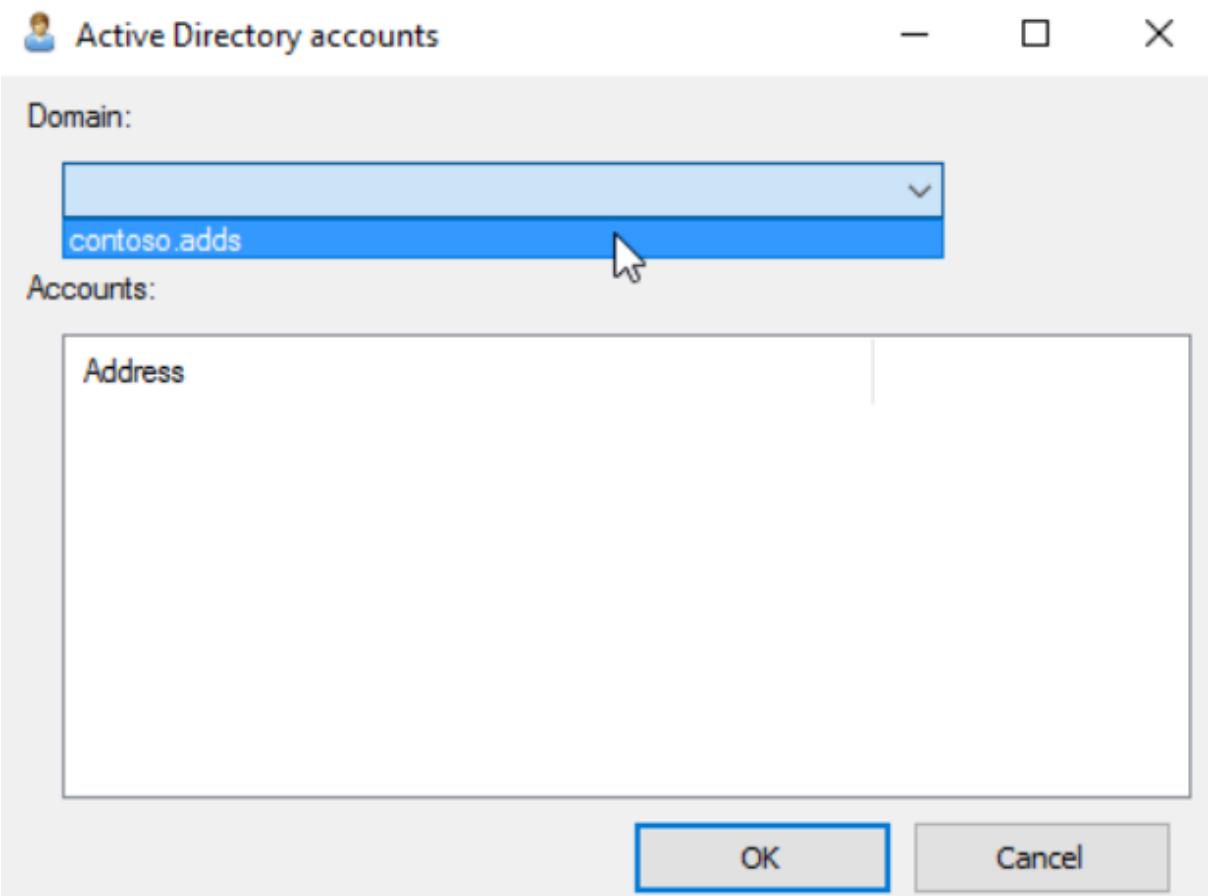
- Enabled:** A checkbox that is checked.
- Log:** A list of protocols with checkboxes:
 - Application
 - SMTP
 - POP3
 - IMAP
 - TCP/IP
 - Debug
 - AWStats
- Settings:** A checkbox for "Keep files open" which is unchecked.

At the bottom of the main pane are buttons for "Show logs", "Help", "Save", and "Exit".

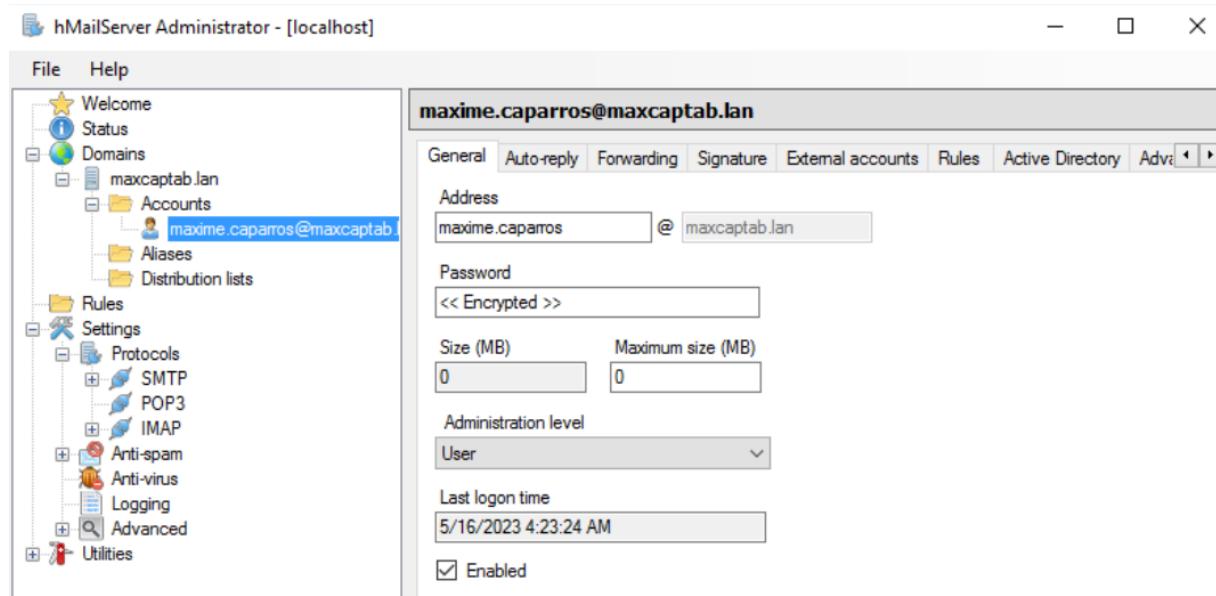
On active les logs qu'on souhaite.

6. Ajout d'un utilisateur de l'AD





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

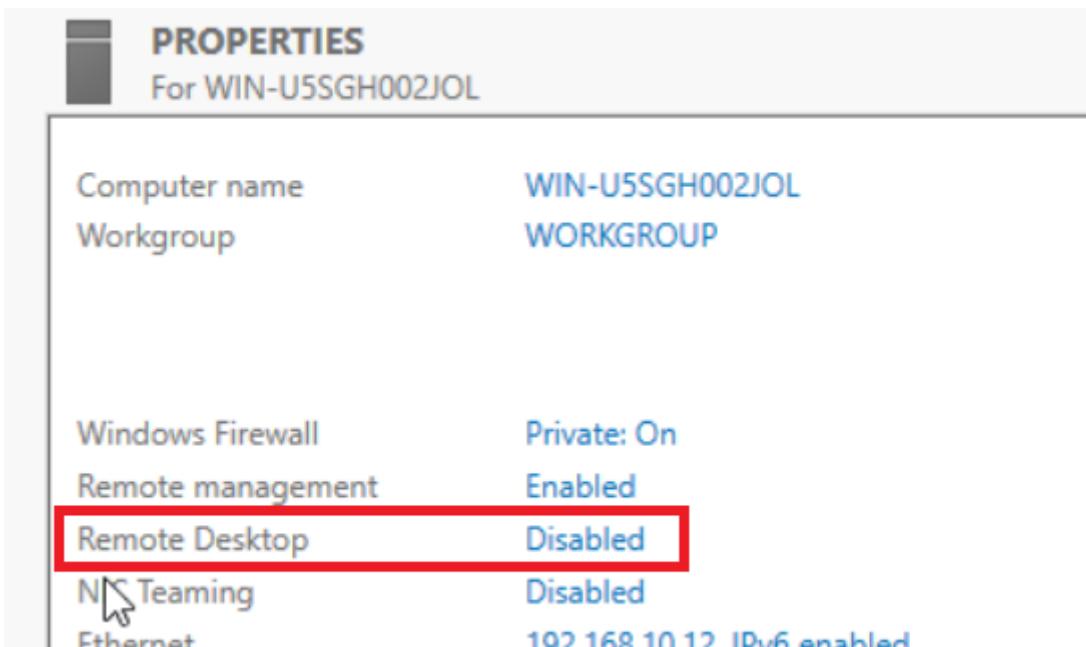
Pour notre serveur AD nous l'avons mis en place sur Proxmox avec la configuration matérielle suivant :

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

X

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)

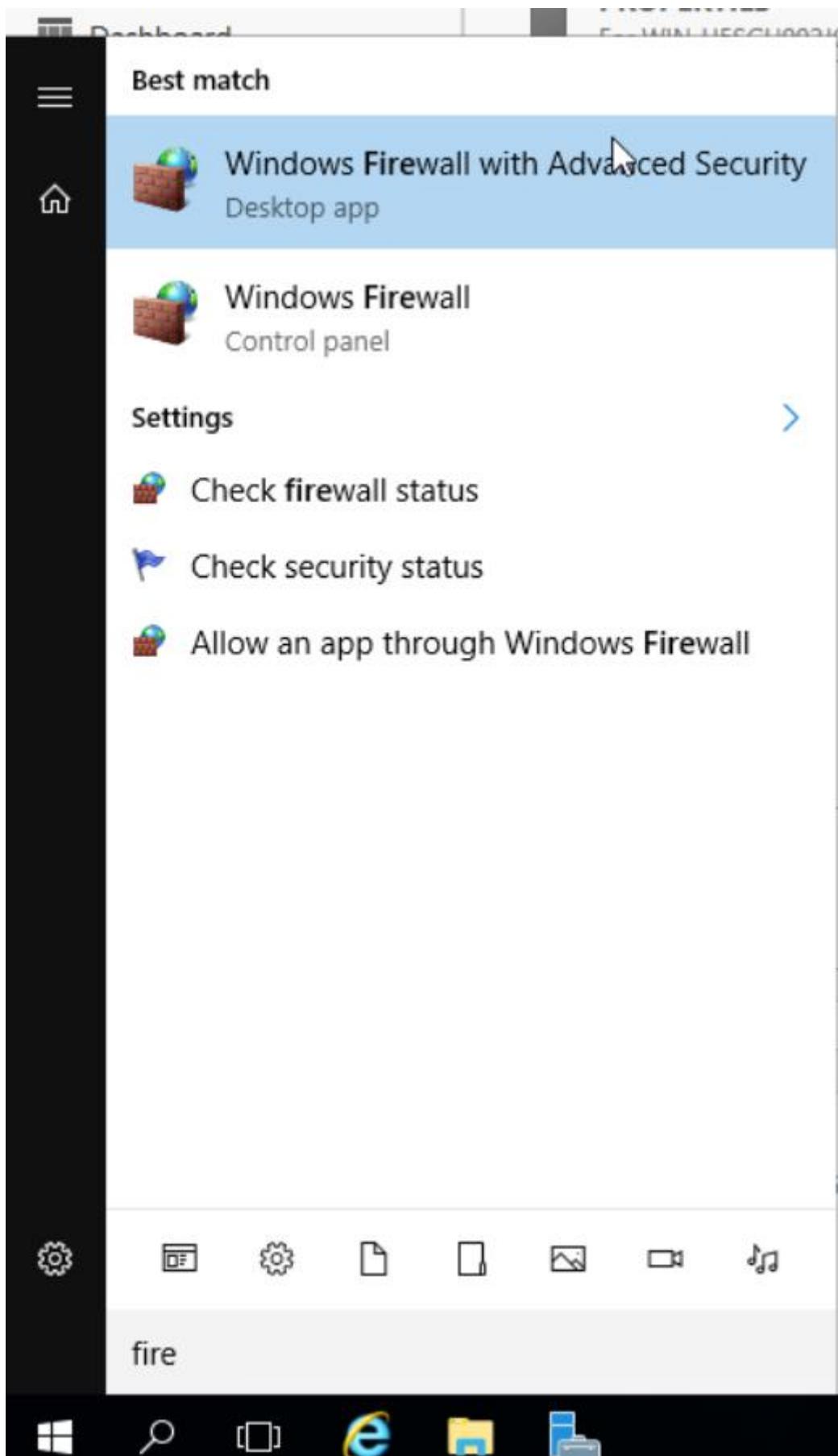
[Help me choose](#)

[Select Users...](#)

[OK](#)

[Cancel](#)

[Apply](#)



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	Domain	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	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 (RTSP-St...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTSP-St...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTSP-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
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow

Actions

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

X

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.

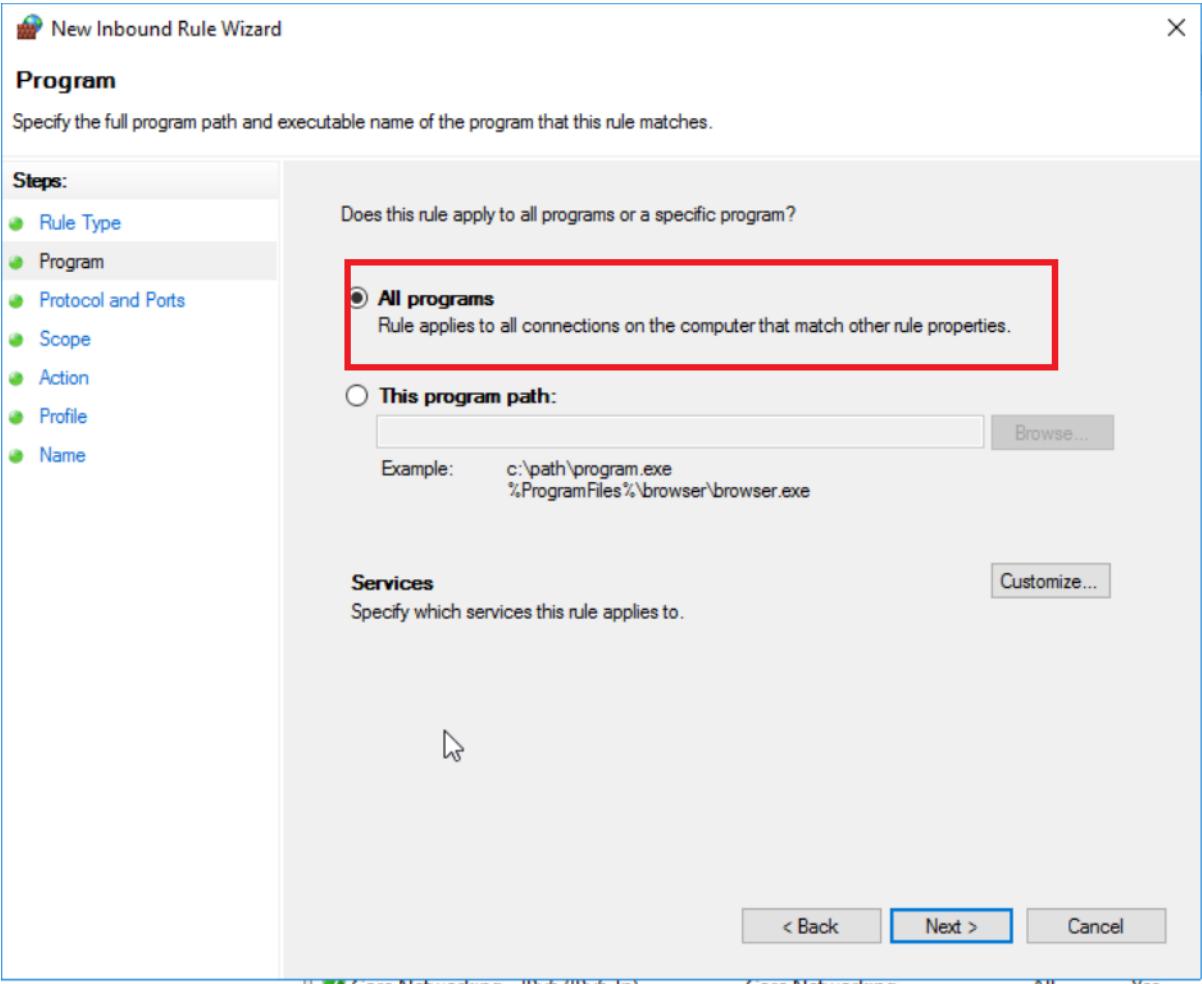
Custom

Custom rule.

< Back

Next >

Cancel



New Inbound Rule Wizard

X

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:

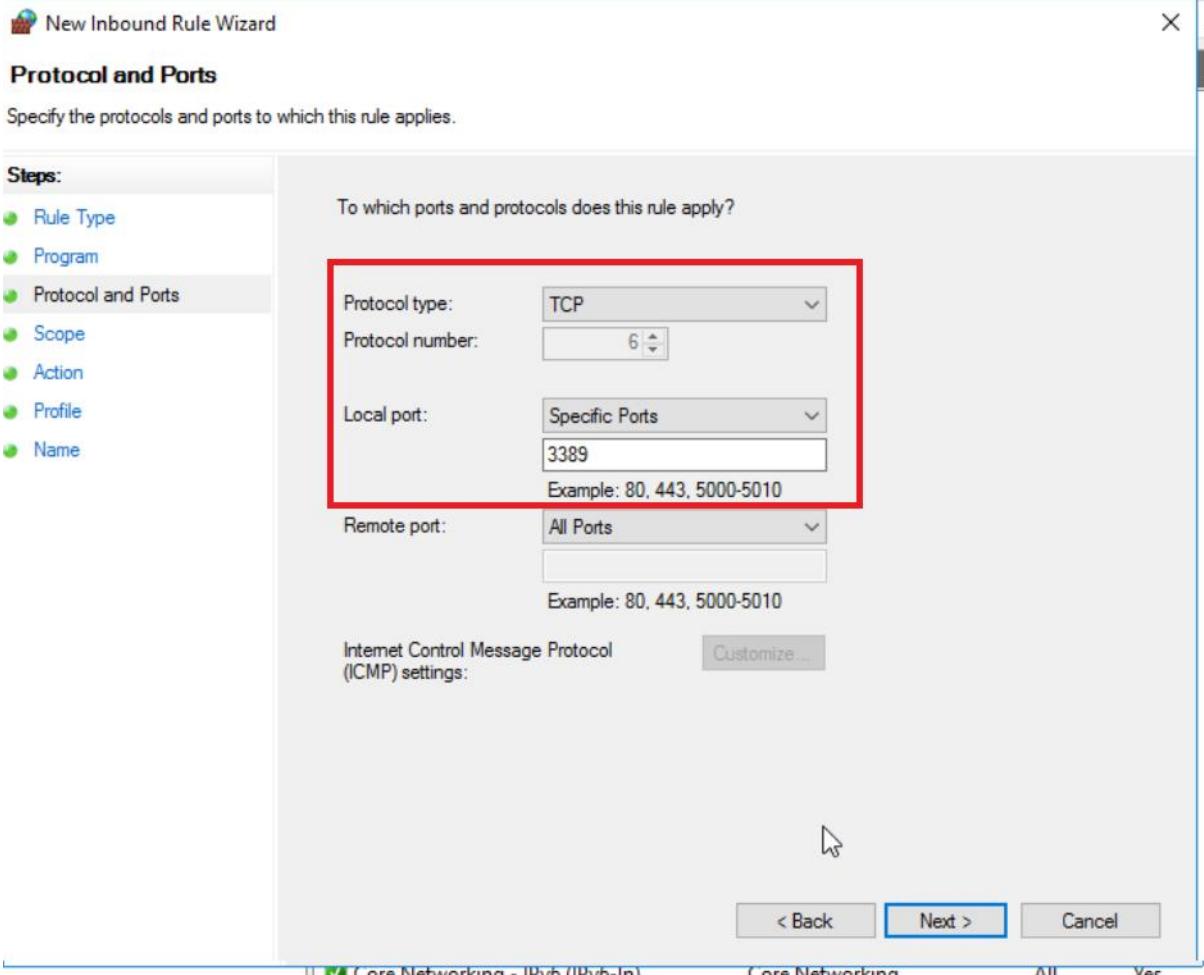
Customize...



< 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:

Add...

Edit...

Remove

< Back

Next >

Cancel

II Core Networking - IDiv6 (IDiv6-1)

Core Networking

All

Var



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



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.

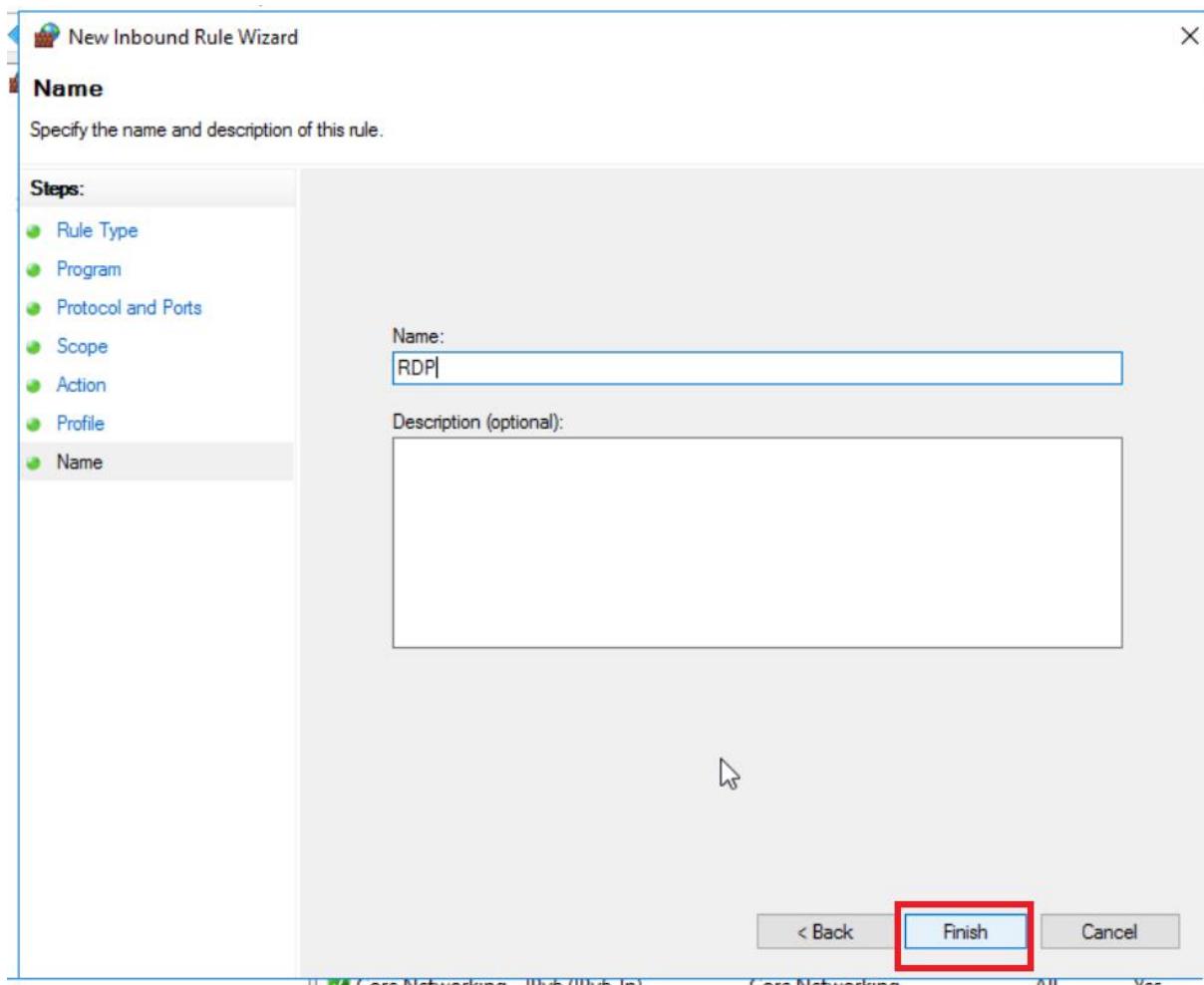
Public

Applies when a computer is connected to a public network location.

< Back

Next >

Cancel

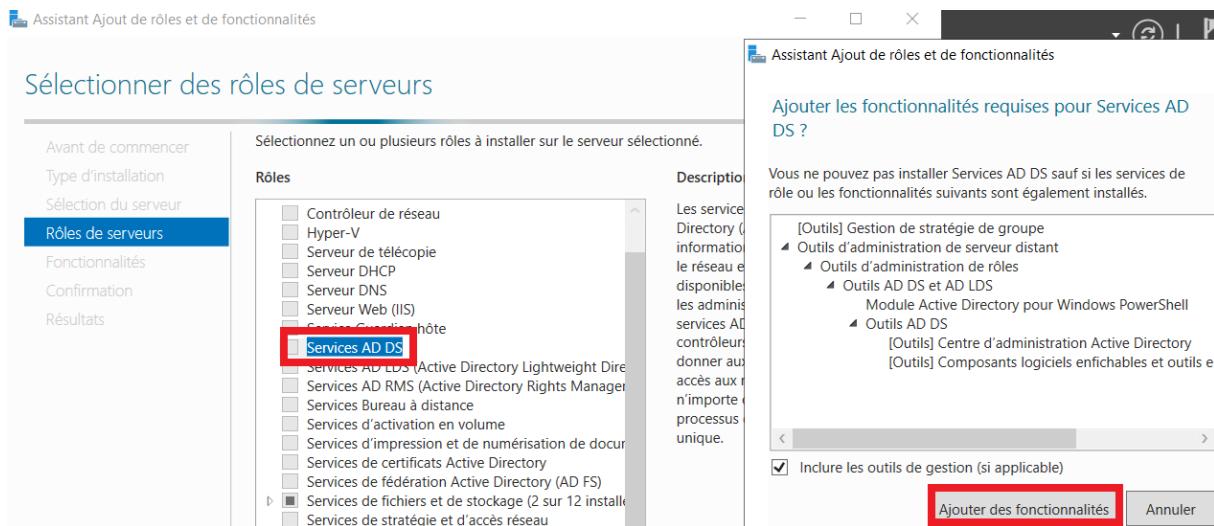


2. Installer l'active Directory sur son serveur

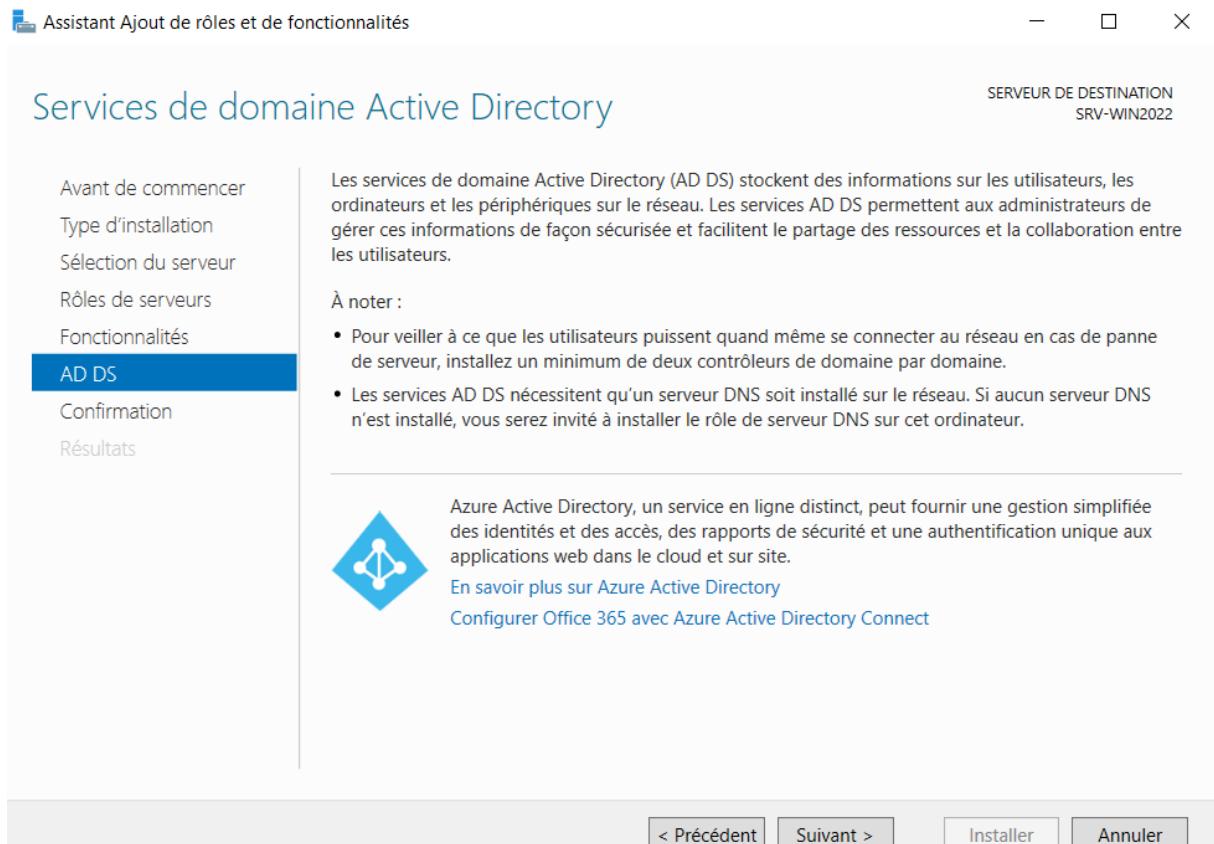
Pour installer l'AD sur son serveur, nous allons installer des rôles et fonctionnalités.



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.

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
SRV-WIN2022

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Gestion de stratégie de groupe

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS

Centre d'administration Active Directory

Composants logiciels enfichables et outils en ligne de commande AD DS

Services AD DS

Exporter les paramètres de configuration

Spécifier un autre chemin d'accès source

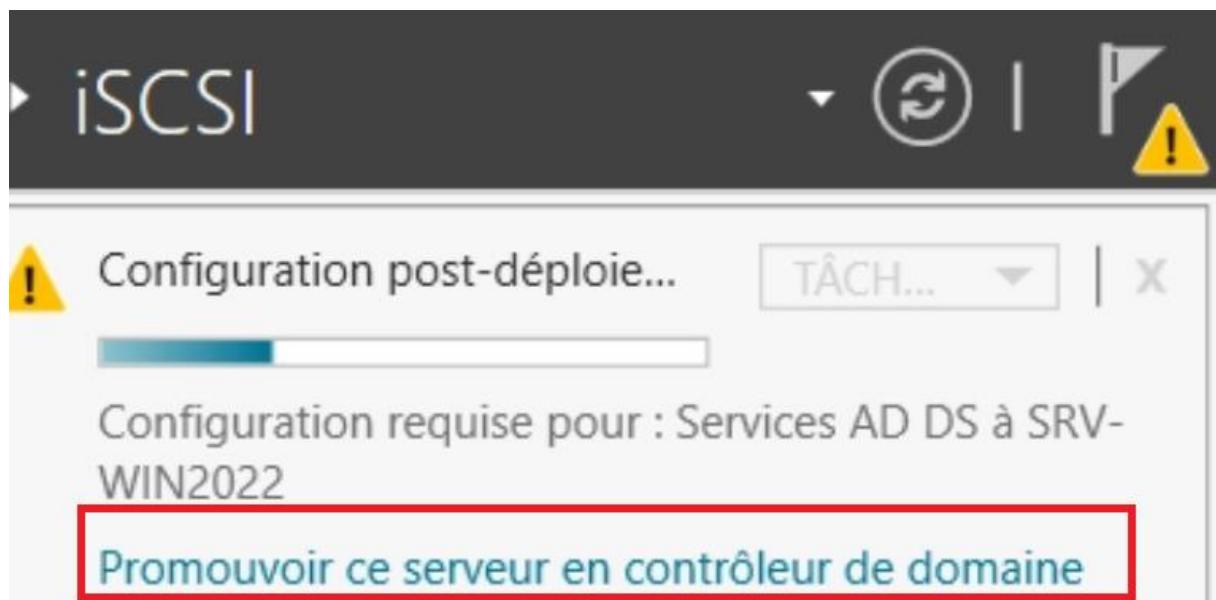
< Précédent

Suivant >

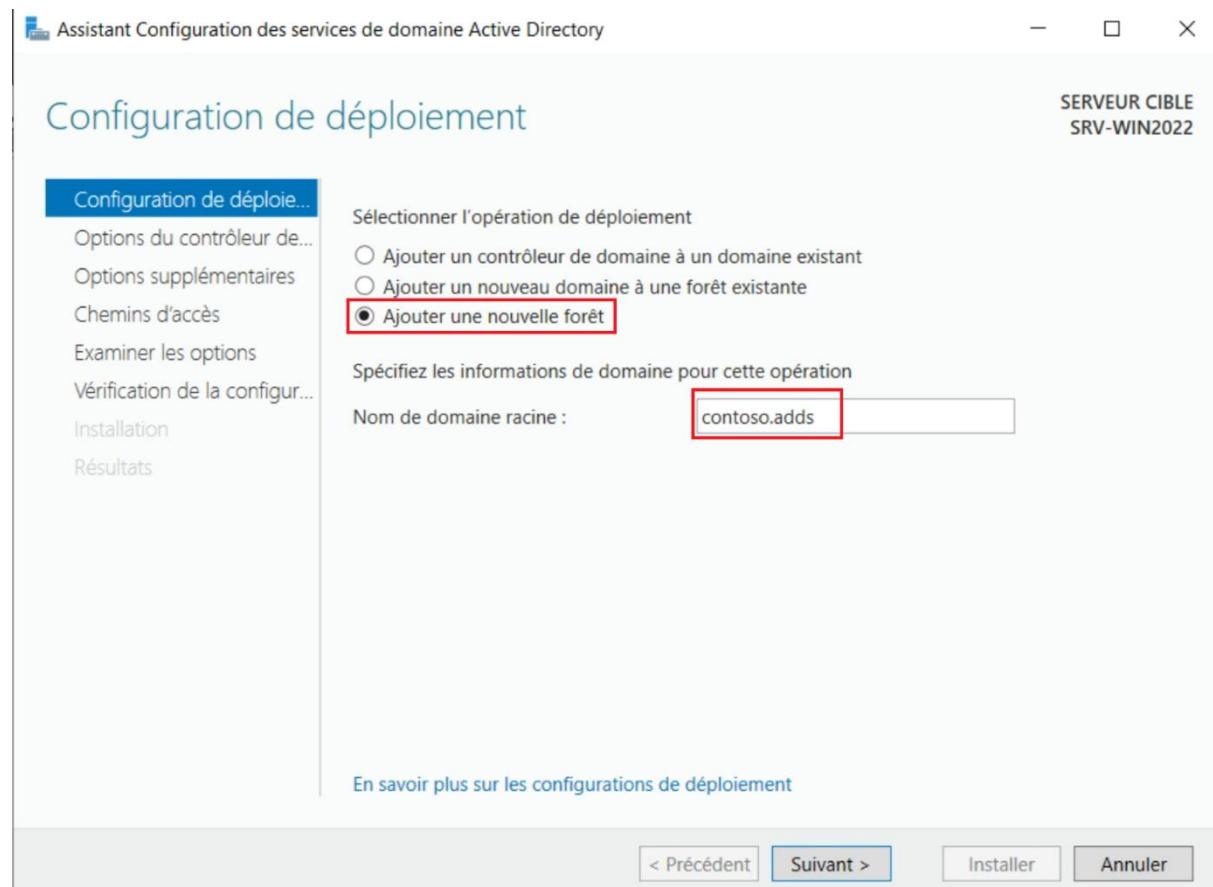
Installer

Annuler

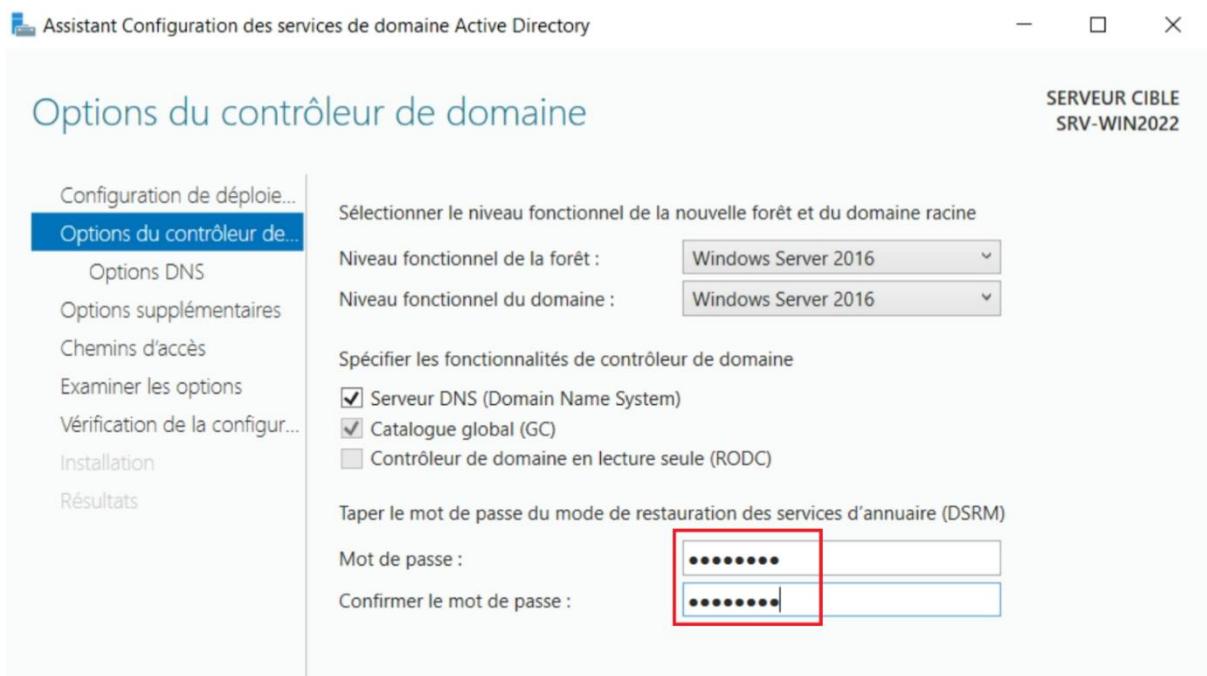
Après l'installation, accédez à l'icône d'avertissement jaune et cliquez sur "Promouvoir ce serveur en contrôleur de domaine" pour démarrer la configuration du contrôleur de domaine.



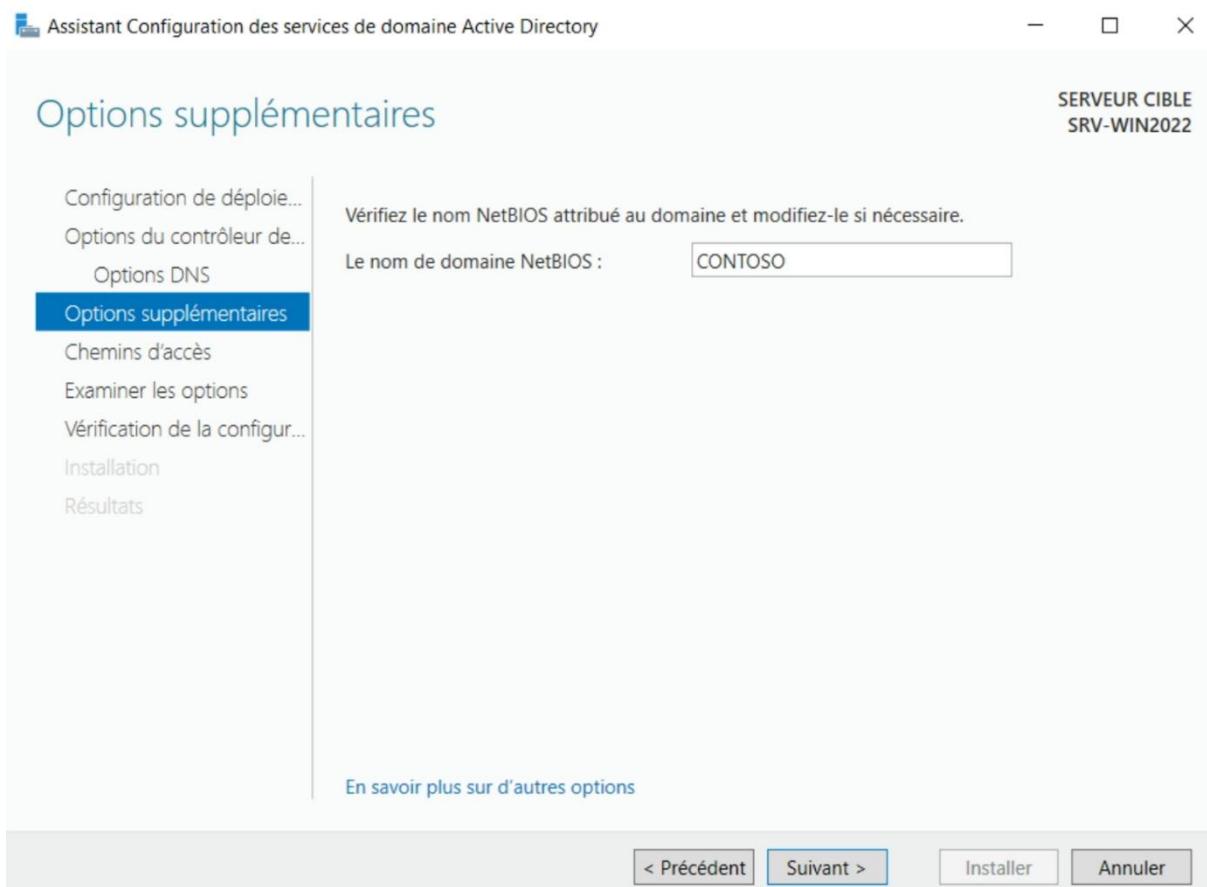
Dans le menu suivant, configurez une nouvelle forêt avec le nom "contoso.adds".



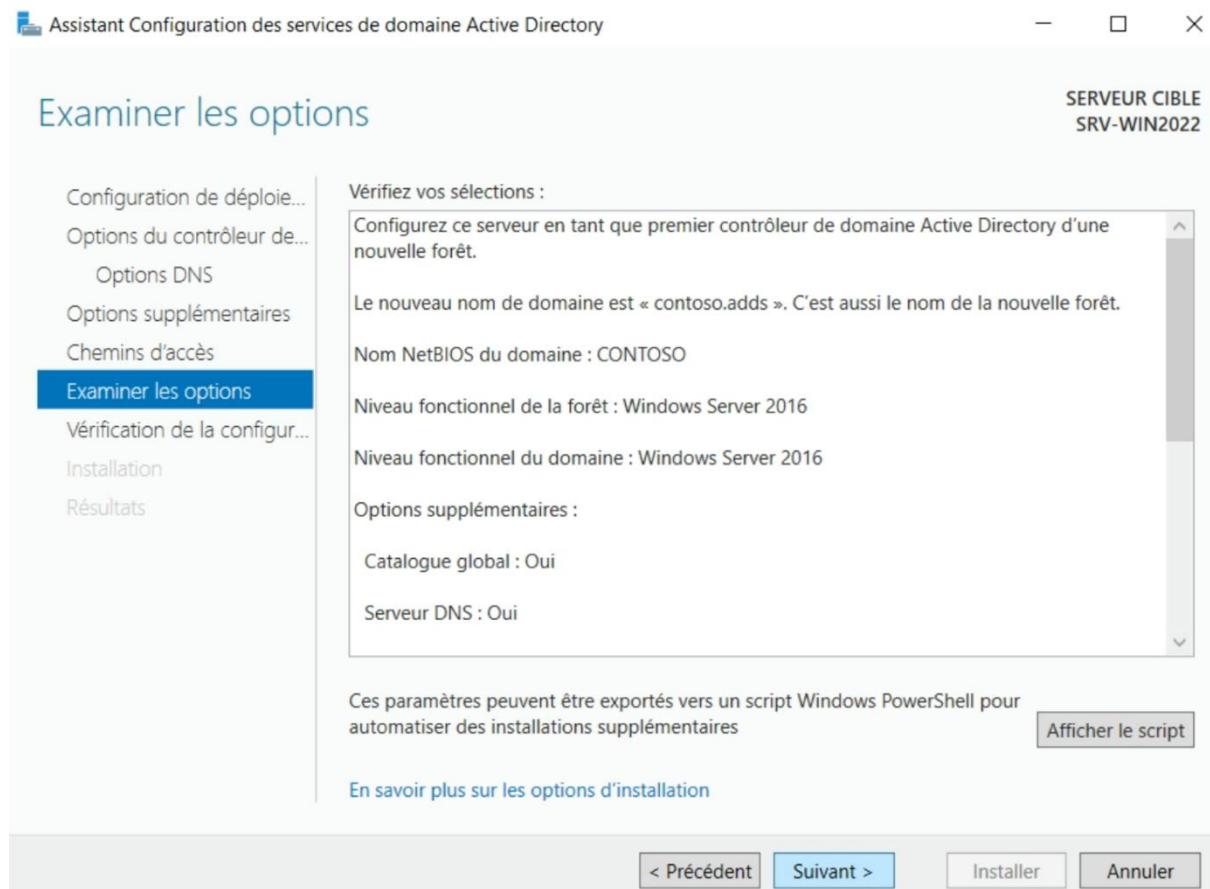
Nous mettons ensuite un mot de passe.



Ici nous mettons CONTOSO.



Pour continuer la configuration, cliquez sur "Suivant".



Pour ensuite cliquer sur “Installer”



Installation

SERVEUR CIBLE
SRV-WIN2022

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

État d'avancement

Vérification pour déterminer si la Console de gestion des stratégies de groupe doit être installée...

 Afficher les résultats détaillés de l'opération

⚠ Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « contoso.adds ». Sinon, aucune action n'est requise.

[En savoir plus sur les options d'installation](#)

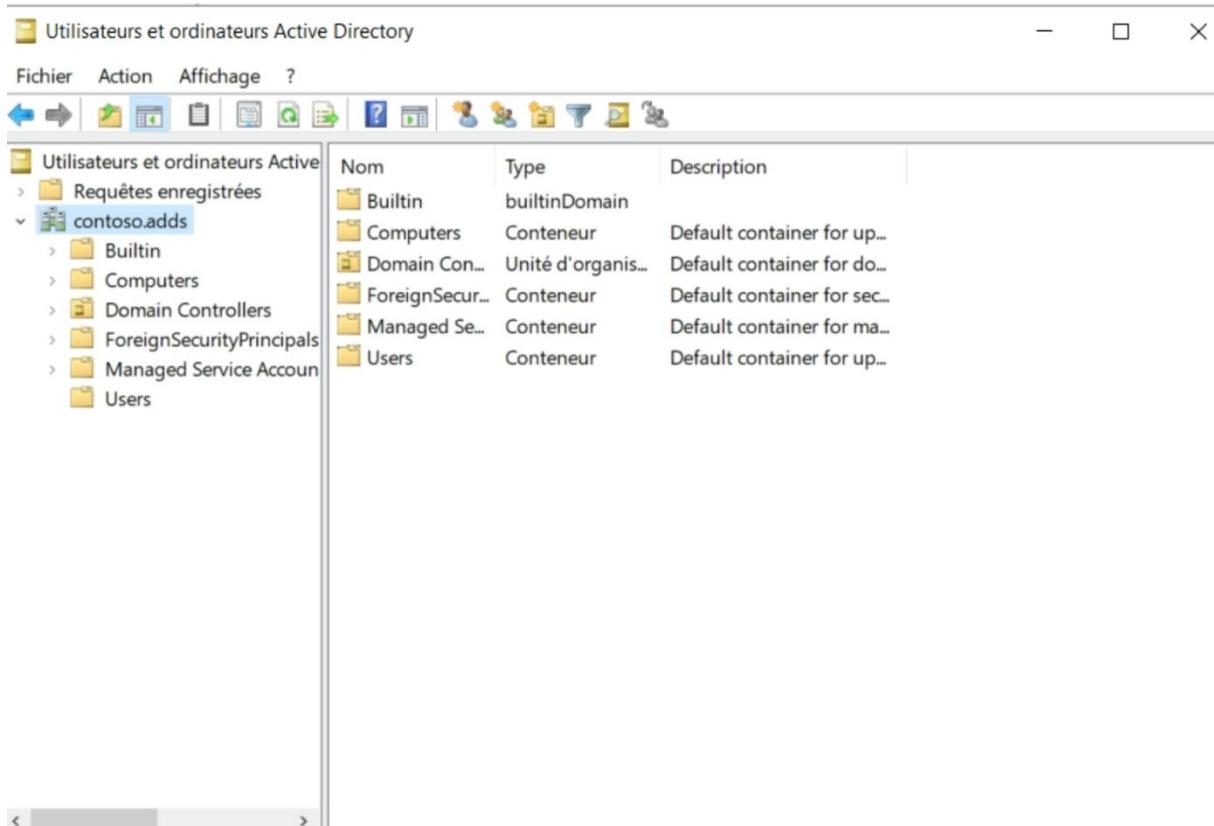
< Précédent

Suivant >

Installer

Annuler

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 matériel

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

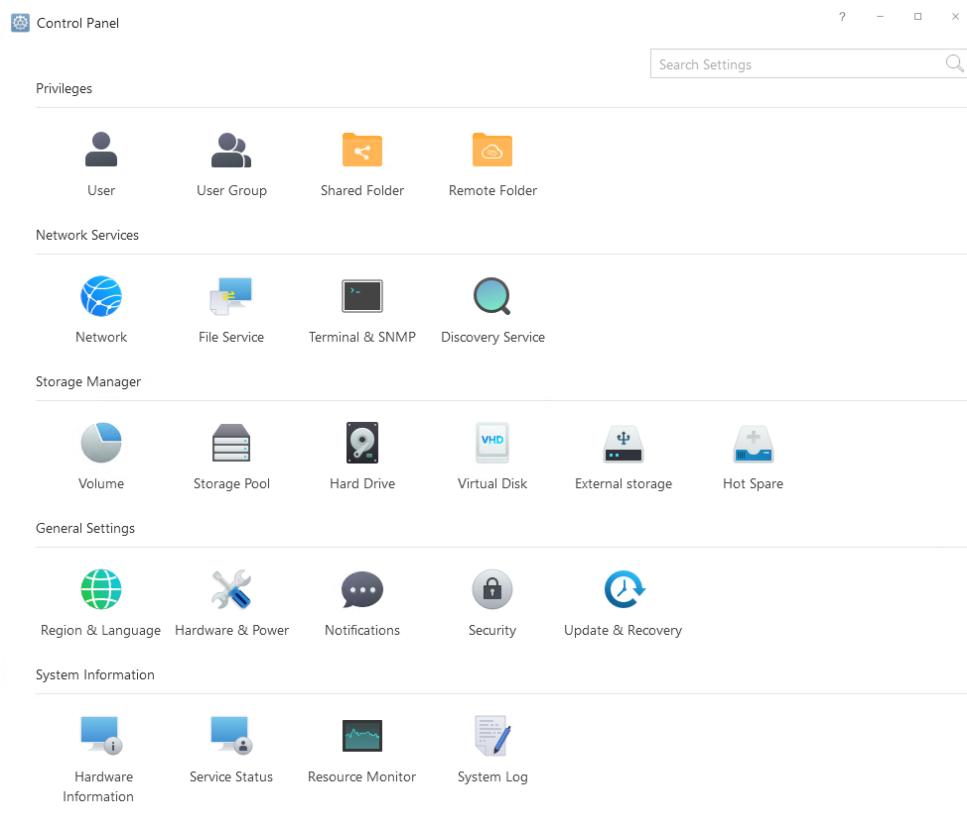
	Capacité de stockage	Performances	Facilité d'utilisation	Coût	Total /20
Pondération	4	3	5	4	
Windows backup	4	3	3	3	13
VEEAM Agent Windows	4	4	5	5	18

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

7.3 Mise en place de la solution

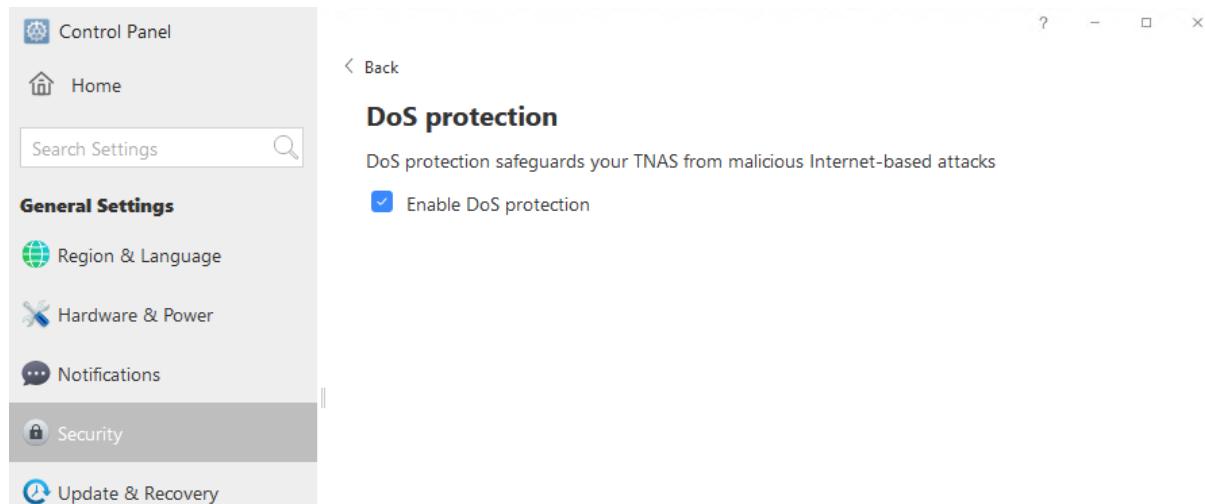
Le NAS

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

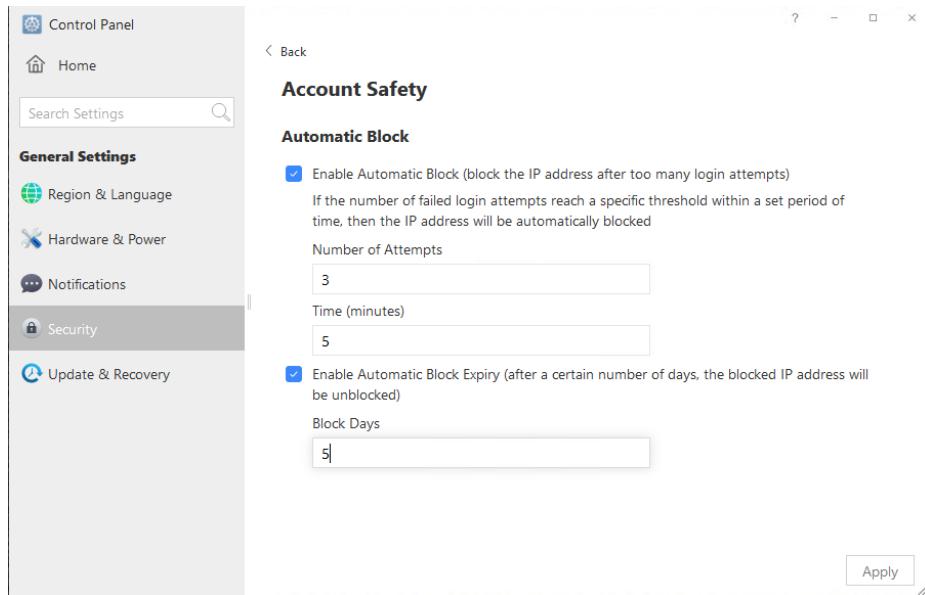


- La sécurité

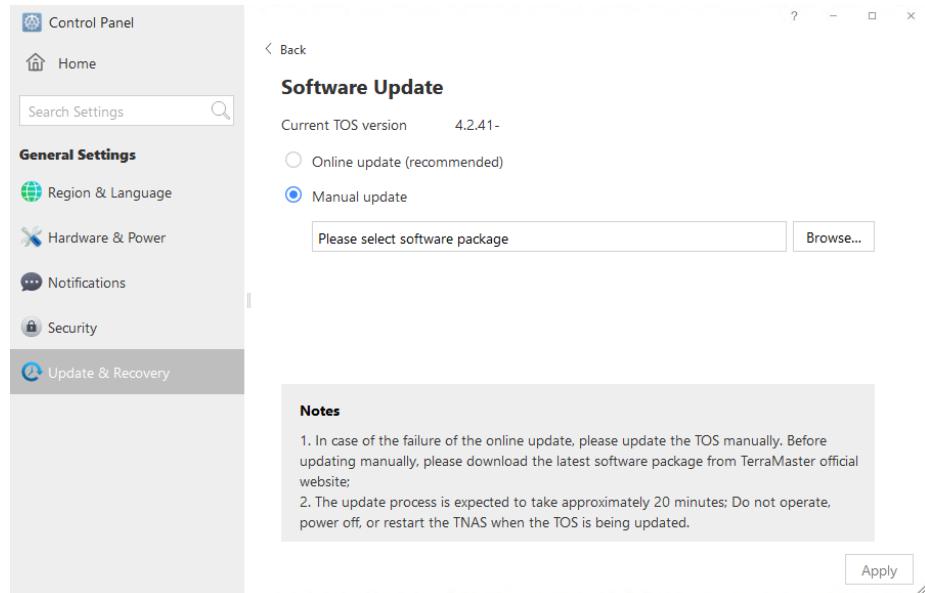
Dans le panneau de contrôle du Terra Master nous sommes venus trouver les paramètres de sécurité. Nous avons activé la protection du NAS contre les attaques DOS (Deny Of Service) qui permet de se prémunir en cas d'une attaque consistant à submerger notre service avec un nombre de requête autre passant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



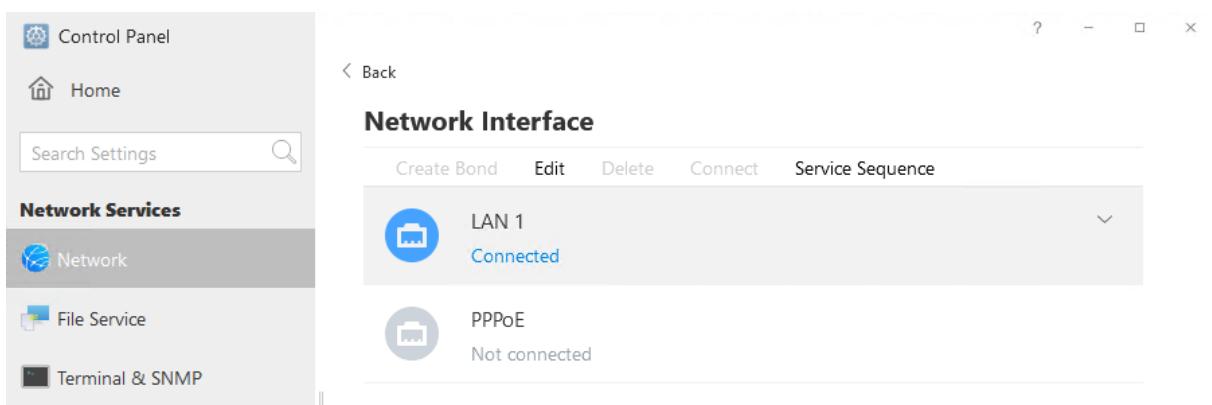
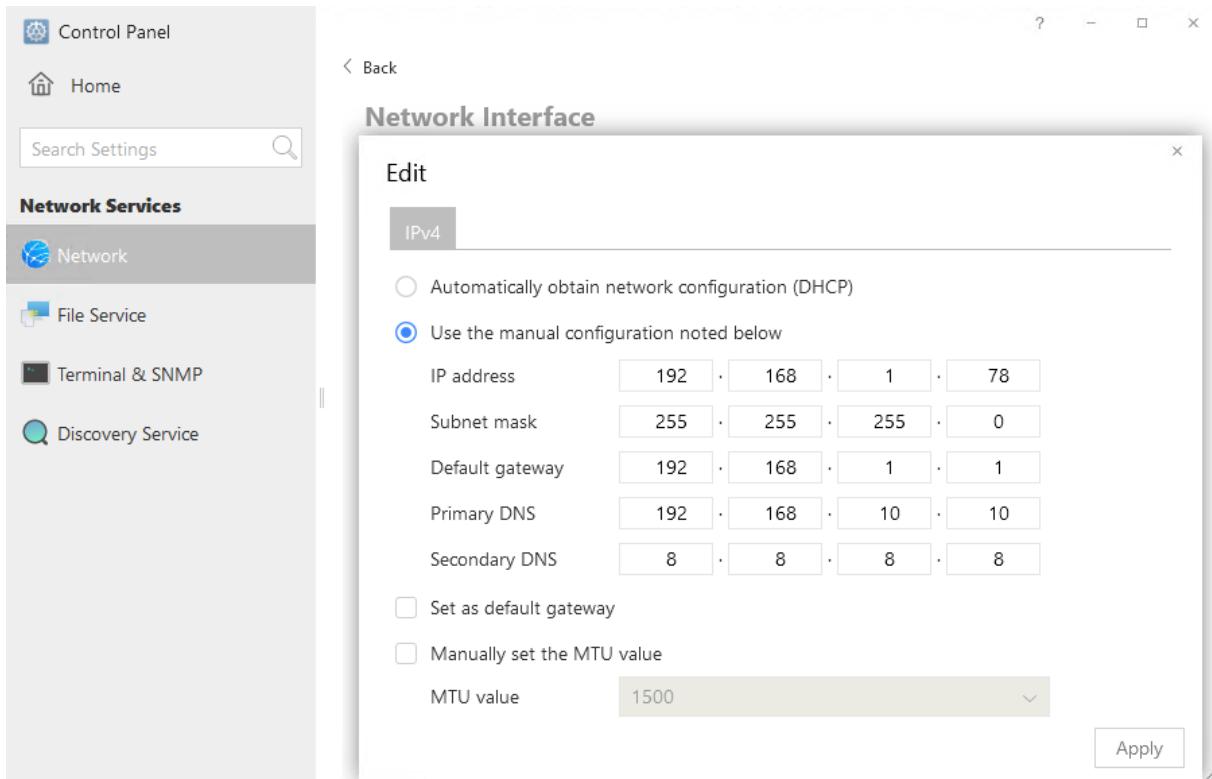
D'un point de vue « moins » sécurité à proprement parlé mais dans le but de garder notre service efficient au maximum, nous avons réglé les mises à jour du NAS en manuelle. De cette façon nous pouvons maîtriser les mises à jour et faire en sorte de ne pas être impacté en cas de mises à jour qui pourraient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



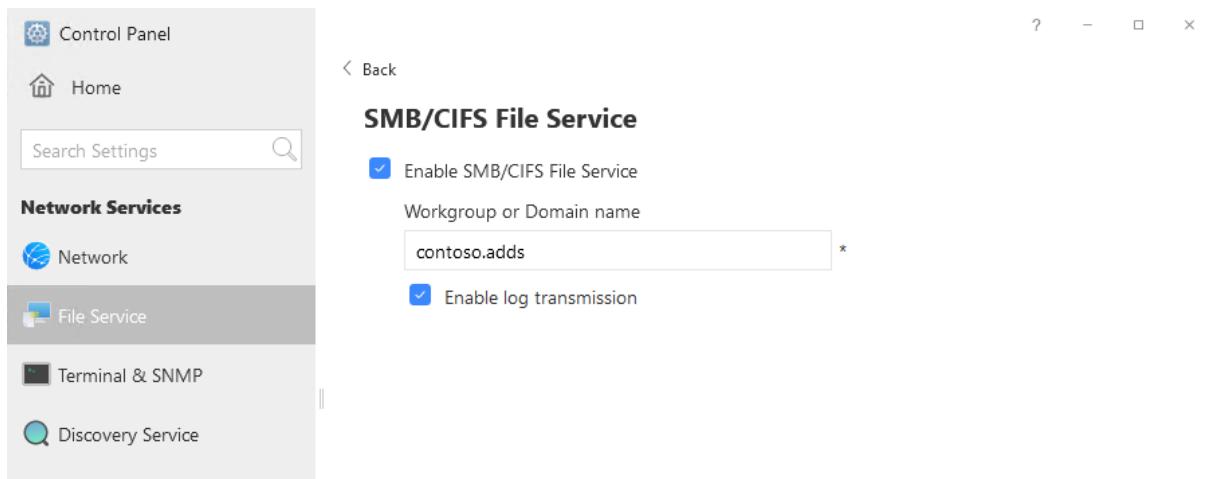
Par la suite nous avons paramétré les services réseau de notre NAS

- Service réseau

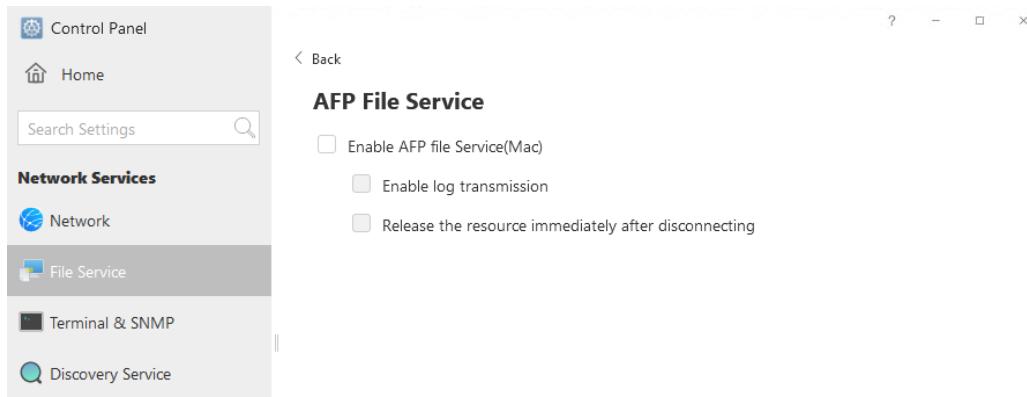
Nous avons commencé par attribuer une adresse IP fixe à notre NAS dans ses paramétrages réseaux.



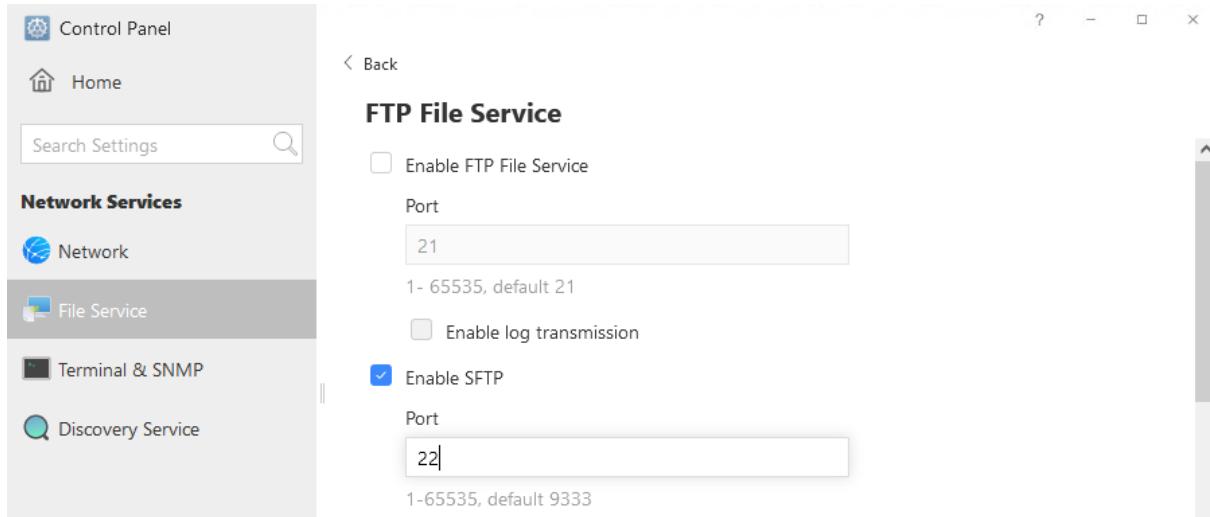
Pour nous permettre un partage de fichiers sur notre environnement Windows nous viendrons activer les options suivantes en renseignant le nom de domaine de notre serveur



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.

The screenshot shows the 'Control Panel' interface with the 'Network Services' section selected. Under 'Terminal & SNMP', the 'Telnet / SSH' settings are displayed. The 'Allow Telnet connection' checkbox is unchecked. The 'Port' field contains '23'. Below it, the 'Allow SSH access' checkbox is checked, and the 'Port' field contains '9222'.

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

The screenshot shows the 'Control Panel' interface with the 'Network Services' section selected. Under 'Terminal & SNMP', the 'SNMP' settings are displayed. The 'Enable SNMP service' checkbox is unchecked. The 'Port' field is empty. Below it, the 'Send events' section includes checkboxes for 'Message', 'Warning', and 'Error'. The 'Received address 1' field is empty.

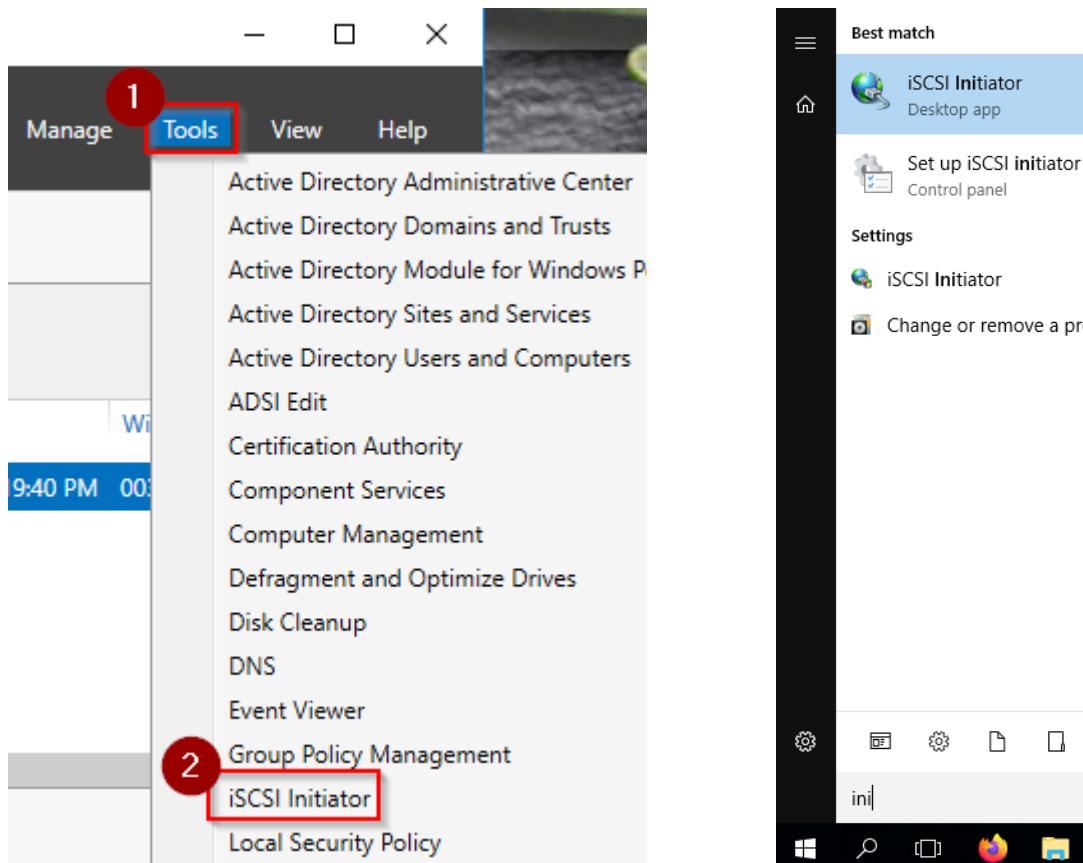
Et enfin nous avons désactivé les options de découverte, comme l'option « Bonjour »

The screenshot shows the 'Control Panel' interface with the 'Network Services' section selected. Under 'Discovery Service', the 'UPnP Discovery' settings are displayed. The 'Enable UPnP discovery service' checkbox is unchecked. A note states: 'You can enable the UPnP discovery service to share the TNAS to other UPnP devices on your local network.' Below it, the 'Bonjour' settings are shown. The 'Enable Bonjour' checkbox is unchecked. A note states: 'Enabling this option will allow Bonjour to detect your TNAS'. The 'Enable Bonjour Time Machine broadcast via AFP' checkbox is checked.

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 provisioning.

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)

The screenshot shows two windows of the iSCSI Target software:

- Create iSCSI LUN (Top Window):**
 - LUN: Volume #1
 - Storage allocation: 200GB
 - Provisioning: Thin provisioning (selected)
 - Location: Volume #1
 - Free space: 5511.34GB
 - Capacity: 200GB
 - Mapped iSCSI Target: Target #1
- Edit iSCSI LUN (Bottom Window):**
 - LUN: Partage NAS
 - Storage allocation: Thin provisioning
 - Location: Volume #1
 - Free space: 5511.34 GB
 - Capacity(GB): 200
 - Mapped iSCSI Target: Target #1

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

The screenshot shows the iSCSI LUN list window:

- Header: Create, Edit, Delete
- Items:
 - Partage NAS** Good (Status)
 - Volume #1 (Name)
 - OKB / 200GB (Capacity)

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

Edit iSCSI Target

General	Advanced settings	LUN
Target	Target #1	
IQN	iqn.2023514.tnas:storage.w4o4e	
<input checked="" type="checkbox"/> Enable CHAP certification		
Username	administrator	
Password	*****	
Confirm password	*****	

Pour affiner la sécurité, à la suite de notre certification CHAP, nous paramètrons également le CHAP mutuel

Comme précédemment il faudra cocher la case pour l'activer et entrer un username ainsi qu'un mot de passe

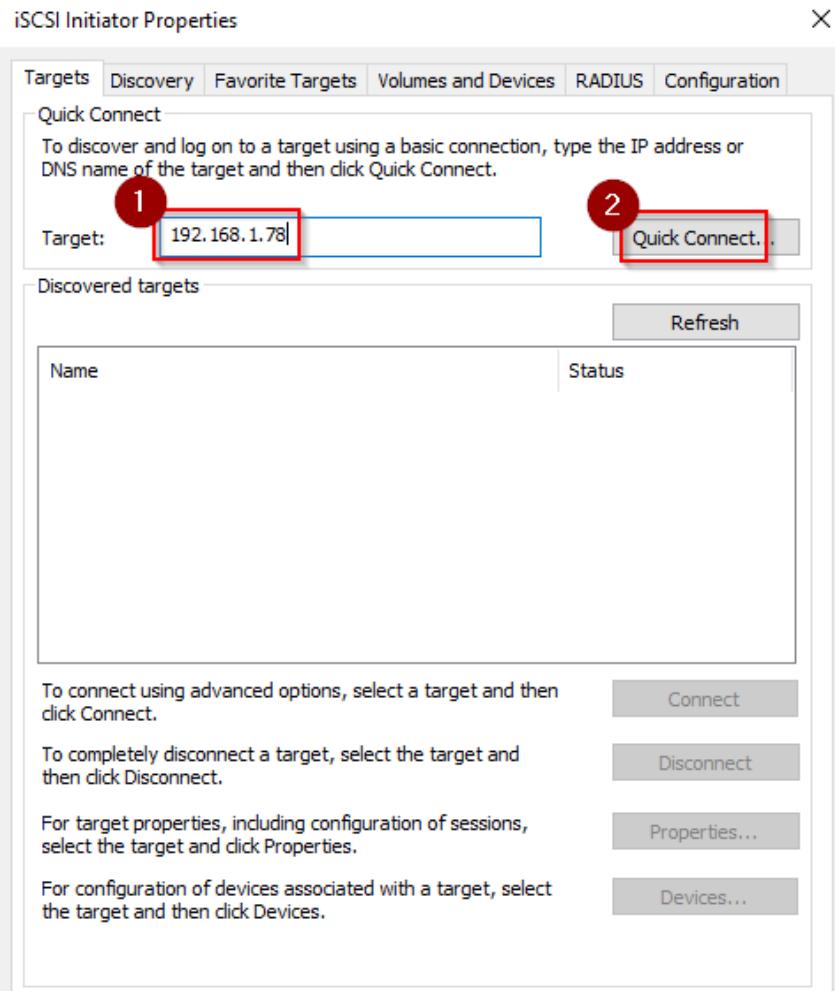
<input checked="" type="checkbox"/> Enable mutual CHAP		
Username	administrator	
Password	*****	
Confirm password	*****	

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

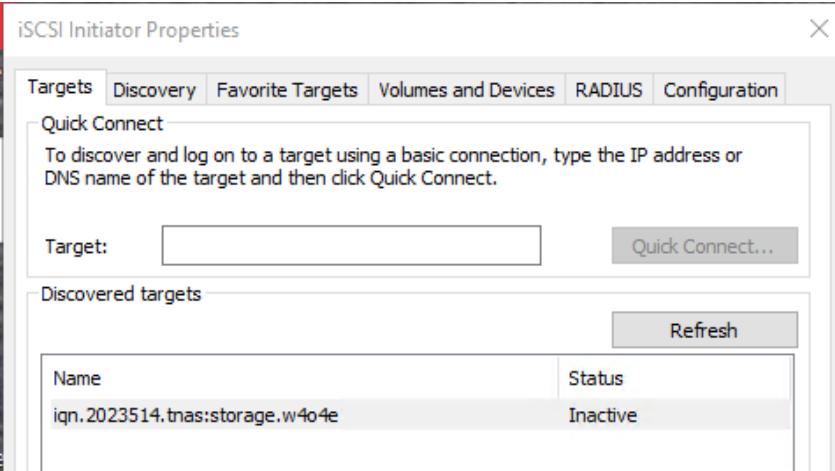
Nous venons trouver notre initiateur ISCSI et l'exécutons



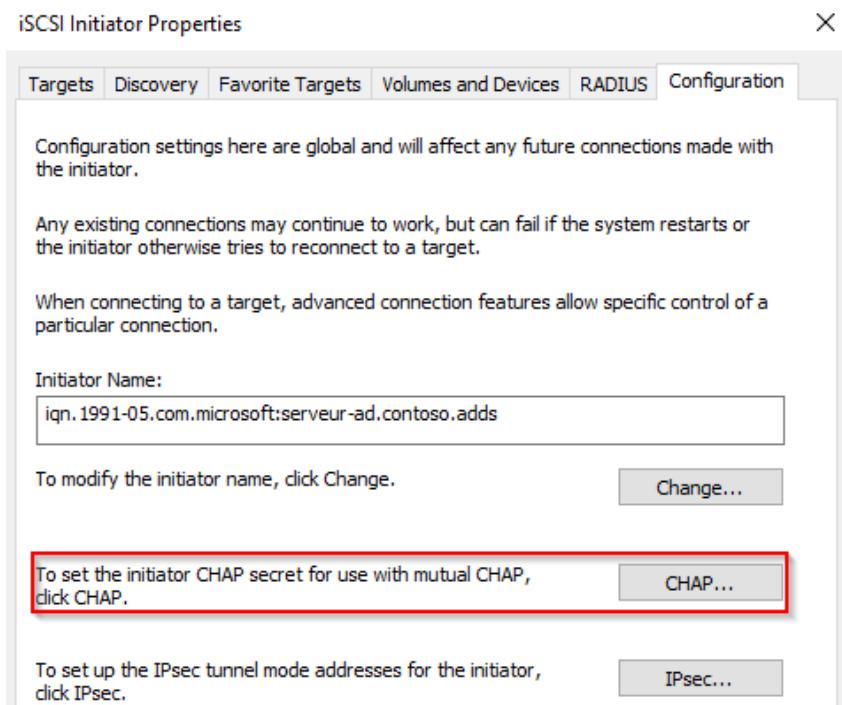
Sur l'interface qui apparait nous venons saisir l'adresse de notre NAS pour établir une connexion avec une potentielle cible ISCSI, si existante.



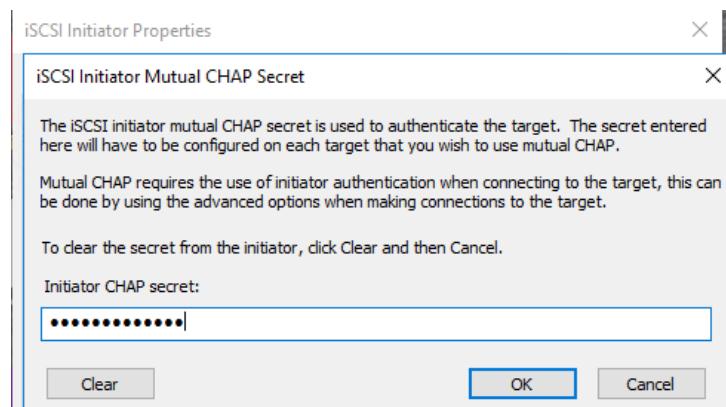
Après validation, on retrouve bien notre cible iSCSI



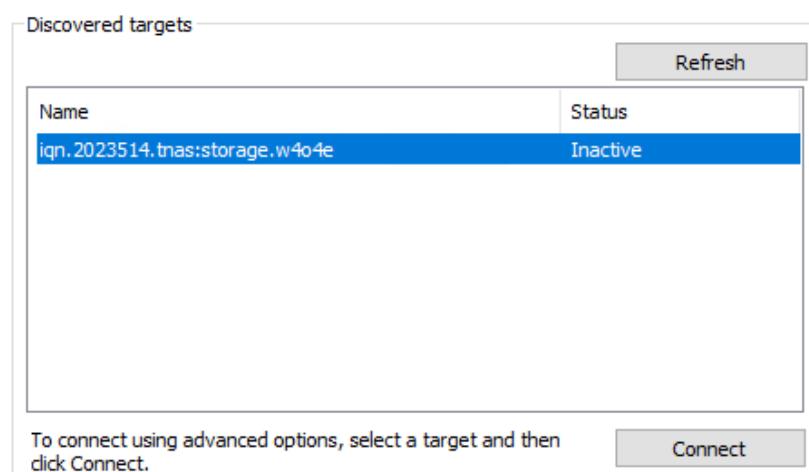
Avant de l'activer, nous allons nous rendre dans l'onglet configuration pour rentrer l'identifiant du chap mutuel pour permettre la connexion du serveur à la cible



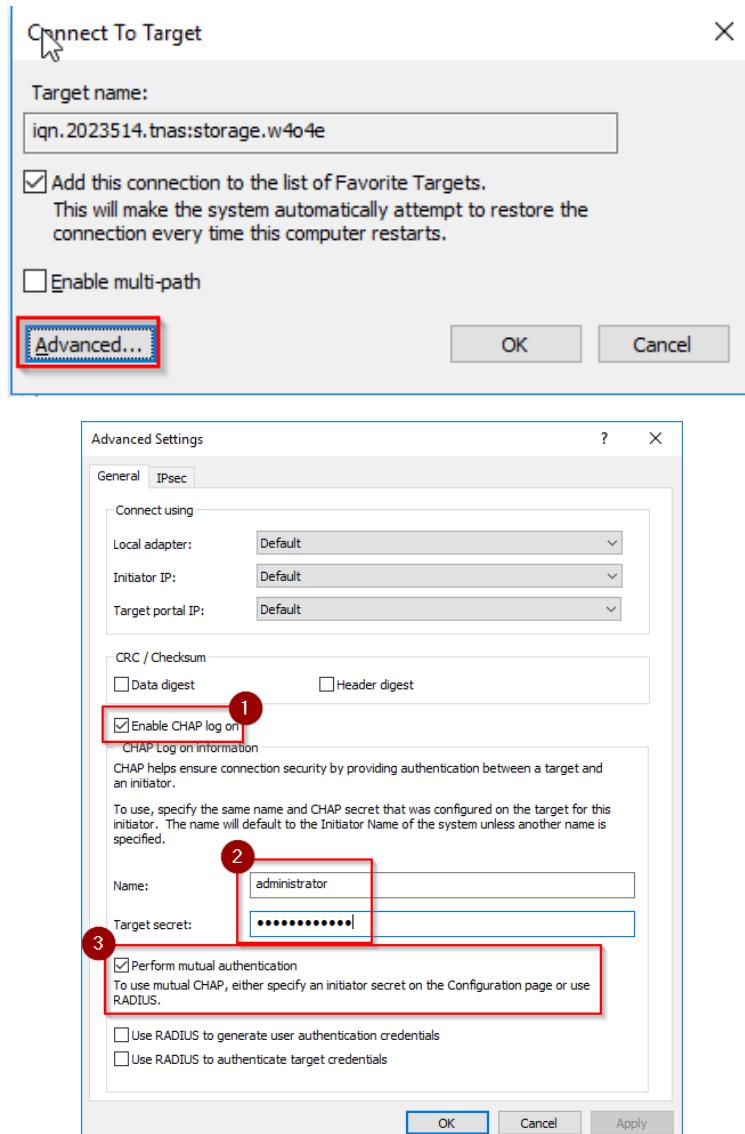
Nous viendrons saisir le mot de passe de notre chap mutuel



Nous reviendrons 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'exécution 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

Discovered targets		Refresh
Name	Status	
iqn.2023514.tnas:storage.w4o4e	Connected	

NAS

iSCSI Target

Create Edit Delete



Target #1 Connected

iqn.2023514.tnas:storage.w4o4e

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 téléchargement et après installation

VeeamAgentWindows_5.0.3.4708 20/02/2022 10:30 ... Application 346,631 KB

Veeam Agent for Microsoft Windows ×

Veeam Agent for Microsoft Windows ×



Installation completed successfully

We recommend that you create Veeam Recovery Media now

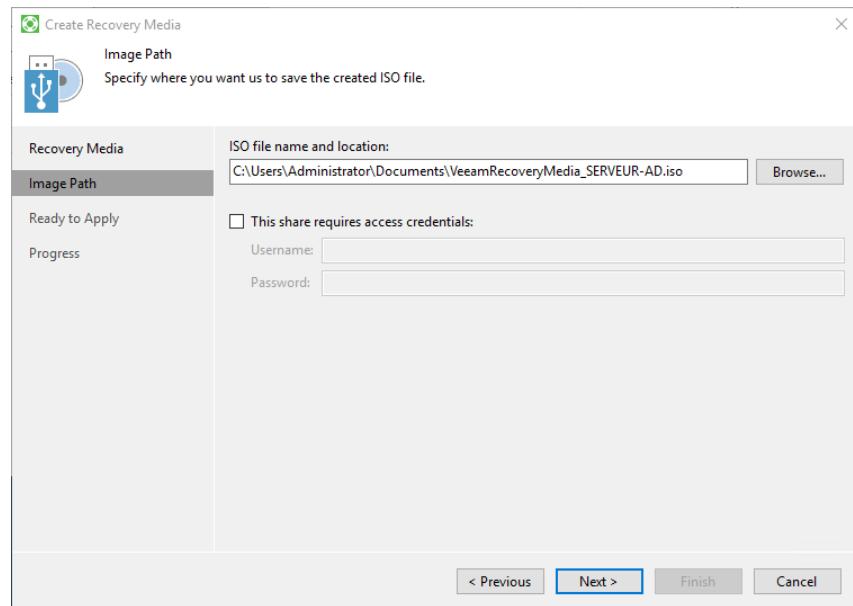
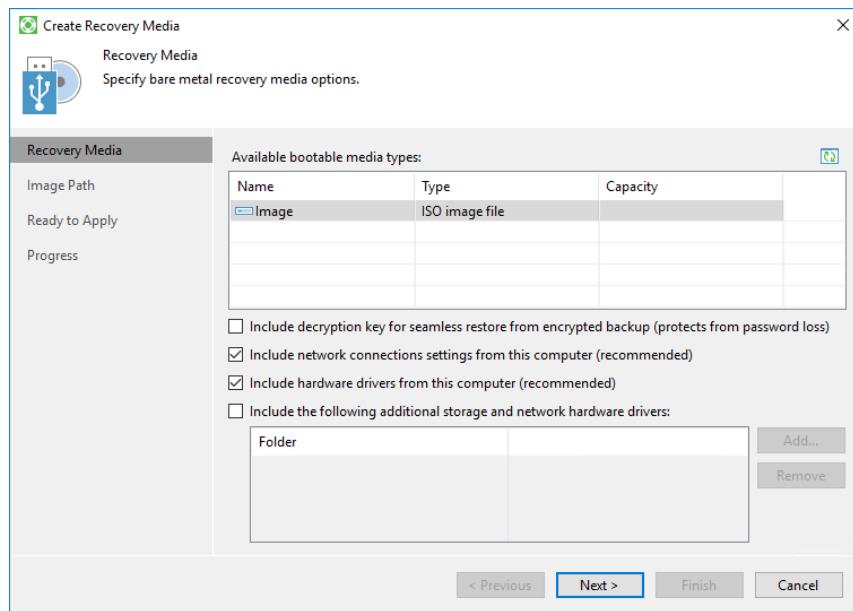
Why is this important?

If you ever need to restore the entire computer, this media will allow you to boot into the recovery environment and initiate so-called Bare Metal Restore. And to ensure smooth recovery, we can even include device drivers and network settings from your computer into the image. Thus, we recommend that you create the media on your own computer, and keep it handy.

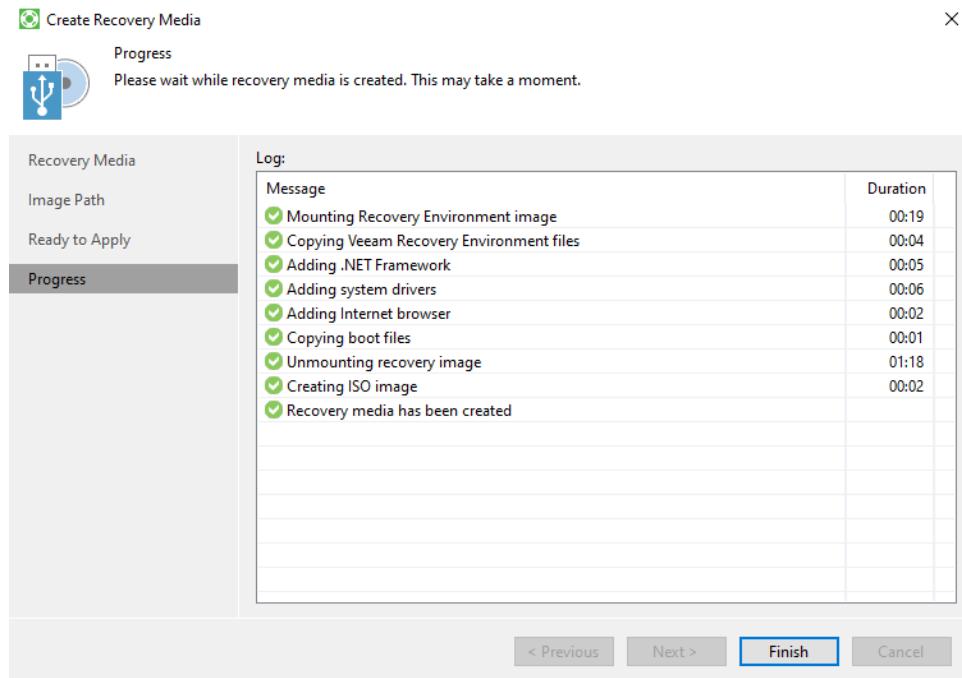
Run Veeam Recovery Media creation wizard

Finish

Suivre les étapes suivantes

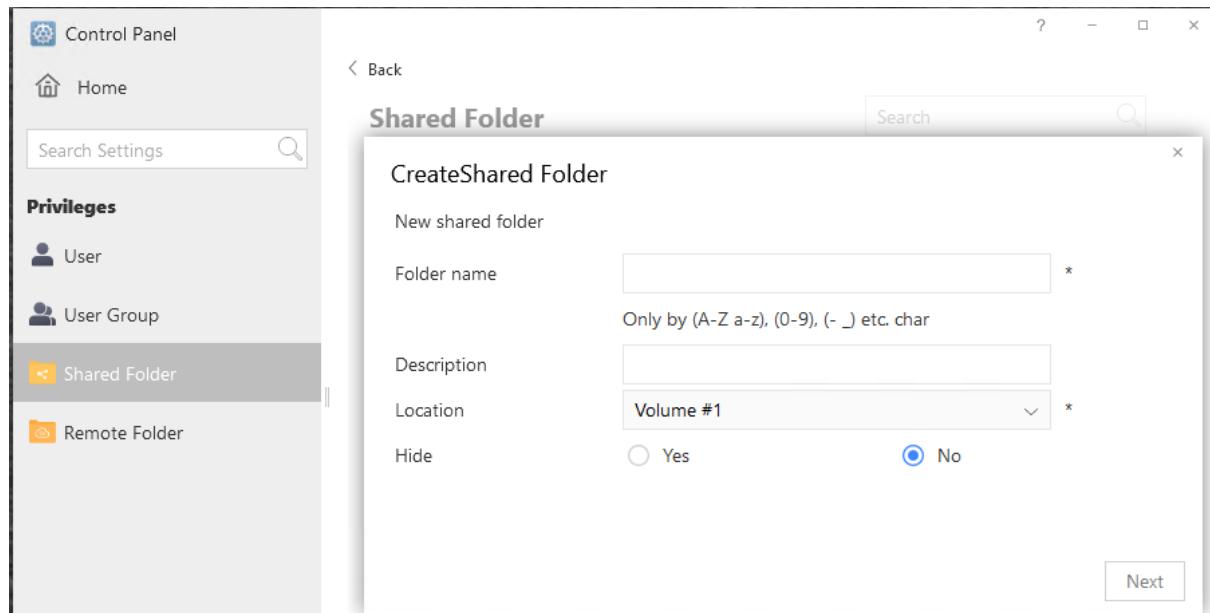


Une fois cette étape terminer notre outil de récupération est créé, nous pouvons continuer



Nous reviendrons ensuite sur le NAS pour créer 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



The screenshot shows the 'Control Panel' interface with the 'Privileges' section selected. Under 'Shared Folder', there is a list of shared folders:

Folder name	Description	Location
appdata		Volume #1
Backup		Volume #1
Backup_PFSense	Backup_PFSense	Volume #1
Professeurs2		Volume #1
public		Volume #1
VEEAM	Backup	Volume #1

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

The screenshot shows the 'Control Panel' interface with the 'Privileges' section selected. Under 'User', a new user is being created:

Create

New user

Username: *

Description:

Password: *

Confirm password: *

Note: Only by (A-Z a-z), (0-9), (- _) etc. char

Note: Password cannot contain fewer than 8 characters, and it must contain one or more characters from 0-9, a-z and A-Z

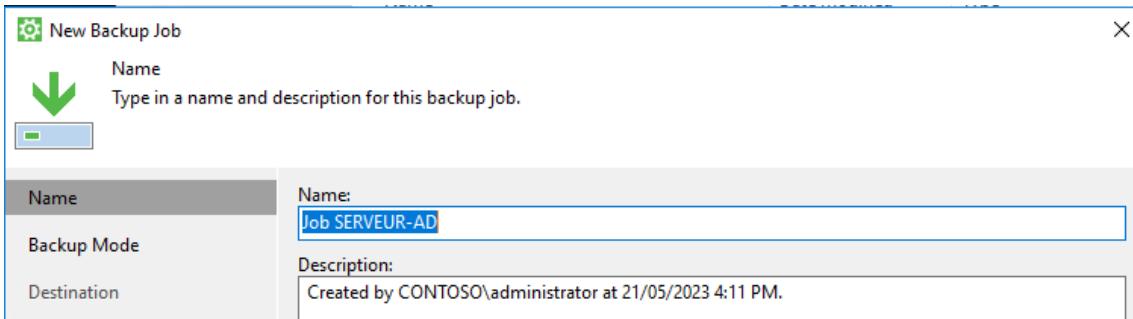
Next

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

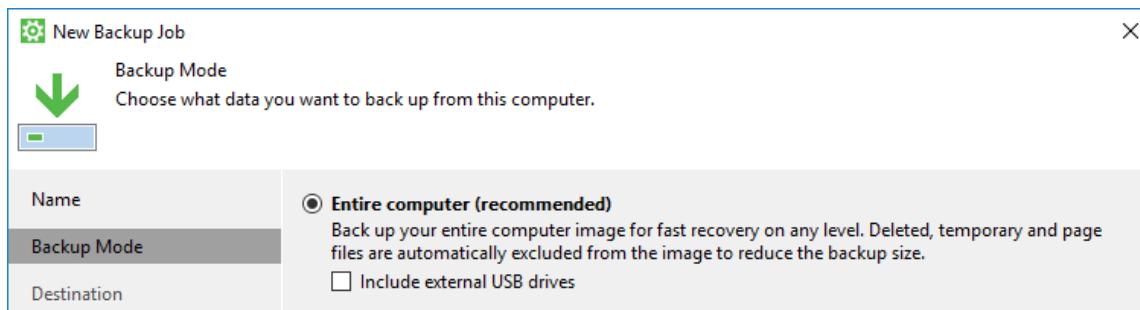
Username	Permission	Deny	Read/Write	Read only
backupadm	Read/Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CGORIE	Deny	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
guest	Deny	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Nous viendrons ensuite paramétrer nos backup comme suit

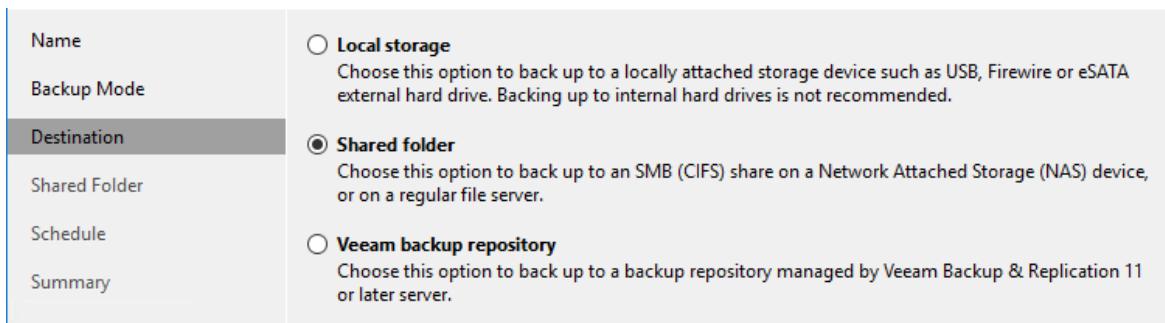
Ouvrir l'outil New Backup Job, auquel nous donnerons un nom



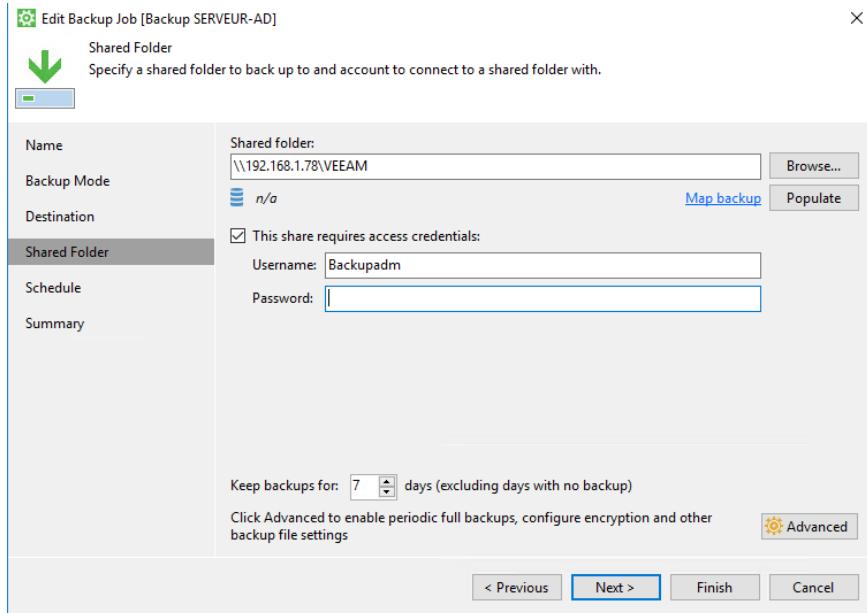
Nous viendrons par la suite sélectionner l'option « Entire computer » pour notre mode de Backup



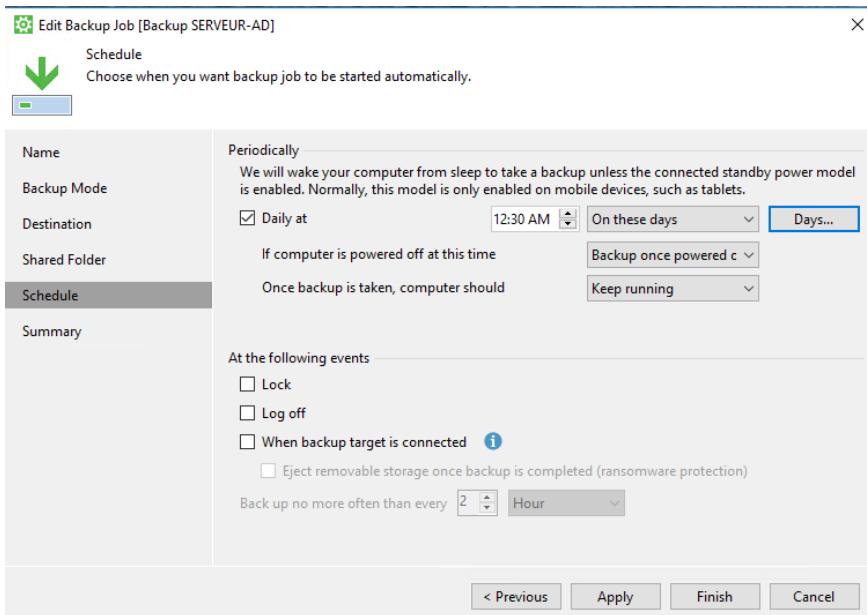
Comme destination de stockage nous viendrons selectionner shared folder pour le stocker sur notre NAS.



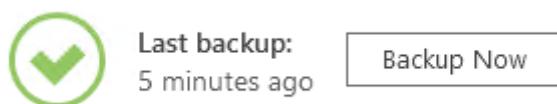
Rentrer le chemin vers le fichier partagé que nous avons créé plus haut avec les identifiants si besoin est. Dans notre cas oui car nous avons créé un utilisateur propriétaire du fichier partagé de backup sur notre NAS.

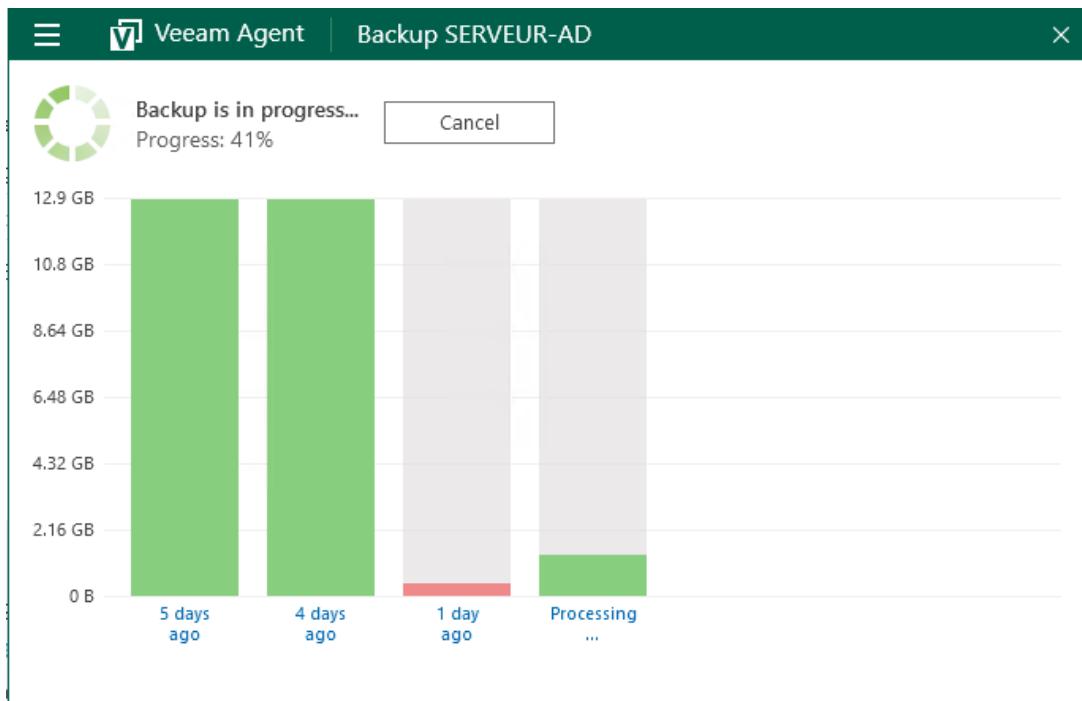


Paramétriser la périodicité de l'exécution des backup du système puis terminer et appliquer



Et lancer une première backup manuellement





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

Ls

The screenshot shows a File Manager interface with the following details:

- File Manager** title bar.
- Toolbar:** Back, Forward, Refresh, Home, Volume #1, VEEAM, Backup SERVEUR-AD, and a search icon.
- Favorites:** Letjeur, public.
- Folders:** Backup, Professeurs2, VEEAM (expanded), Backup SERVEUR-AD (selected), appdata.
- Actions:** Upload, + New, More.
- Files:** Backup SERV EUR-AD.vbm, Backup SERV EUR-AD202, Backup SERV EUR-AD202, Backup SERV EUR-AD202.

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

```
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/veeamss0/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/veeamss0/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/veeamss0/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/veeamss0/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]
```