

Projet Expert 3 - Extension de l'infrastructure



BTS SIO – Option SISR

Atelier de professionnalisation

Glossaire.....	4
Partie 1 : Proposition technique.....	5
I. Schéma du domaine Experty.....	5
II. Liste du matériel.....	6
A. Serveurs.....	6
B. Routeur.....	7
C. Baie.....	8
D. Câbles complémentaires.....	8
E. Licences windows server 2022.....	8
III. Solutions applicatives.....	9
A. PFSense.....	9
B. GestSup.....	11
C. PRTG Network monitor.....	12
D. Veeam.....	13
E. Teleport.....	15
IV. Politique de Sauvegarde.....	16
Partie 2 : Proposition tarifaire.....	17
I. Proposition pour le matériel.....	17
II. Proposition pour la prestation.....	17
Partie 3 : Planning déploiement.....	18
Annexes.....	19
I. Procédures.....	19
A. Pfsense.....	19
1. Installation de base.....	19
2. OpenVPN.....	23
a. Créer le certificat.....	23
b. Créer les utilisateurs.....	24
c. Création du serveur OpenVPN.....	25
3. IPSec.....	32
4. Ajuster les règles des Firewalls.....	36
B. Linux GetSup.....	37
1. Installation de GestSup.....	37
2. Ajouter le connecteur LDAP pour la connexion à l'Active Directory.....	42

a.	Créer un compte dédié pour Gestsup dans l'Active Directory..	42
b.	Ajout du connecteur LDAP.....	44
c.	Synchronisation de l'Active Directory.....	45
C.	PRTG.....	46
D.	Bastion Teleport.....	49
1.	Installation de Teleport.....	49
2.	Ajout du nom de l'hôte dans le DNS.....	51
3.	Création du compte administrateur.....	53
4.	Ajouter le domaine experty.....	56
a.	Configurations sur le DC.....	56
b.	Configuration sur le serveur Teleport.....	61
c.	Ajouter le rôle dédié à la connection aux windows du domaine	63
E.	Veeam.....	64

Glossaire

Active Directory (AD) : Annuaire des utilisateurs et des ordinateurs présents dans le domaine de l'entreprise

Administrateur : Compte avec des droits supérieurs à ceux d'un utilisateur normal.

Bastion : Permet de protéger l'accès aux ressources en étant le point d'accès centralisé

DHCP : Permet l'attribution des adresses IP à chaque poste. Puis le service DNS qui agit comme un annuaire et permet de convertir les adresses IP vers des Url ou inversement.

Domaine : Structure logique regroupant des utilisateurs, ordinateurs et ressources partageant une base de données Active Directory commune et des politiques de sécurité unifiées.

DNS : Annuaire informatique permettant de convertir les adresses IP vers des URL ou inversement.

Poste de travail : Ordinateur utilisé par un utilisateur

RDP : Protocole permettant à un utilisateur de se connecter à distance sur un poste ou un serveur

Serveur : Ordinateur centralisé fournissant des services et ressources (fichiers, applications, authentification) aux postes de travail du réseau.

Utilisateur : Compte individuel créé dans Active Directory permettant à une personne de s'authentifier et d'accéder aux ressources du domaine selon ses droits.

VPN : Abréviation de Virtual Private Network, connexion sécurisée entre deux réseaux

Partie 1 : Proposition technique

Pour satisfaire aux besoins de l'entreprise Experty, plusieurs solutions doivent être mises en place, que ce soit au niveau matériel ou logiciel.

I. Schéma du domaine Experty

Dans le cadre de l'implémentation de l'infrastructure, la structure suivante avait été implémentée :

- Deux serveurs contrôleurs de domaine
- Deux serveurs de fichiers
- Un serveur d'impression
- Un serveur de sauvegarde
- Un serveur pour les outils d'administration à distance

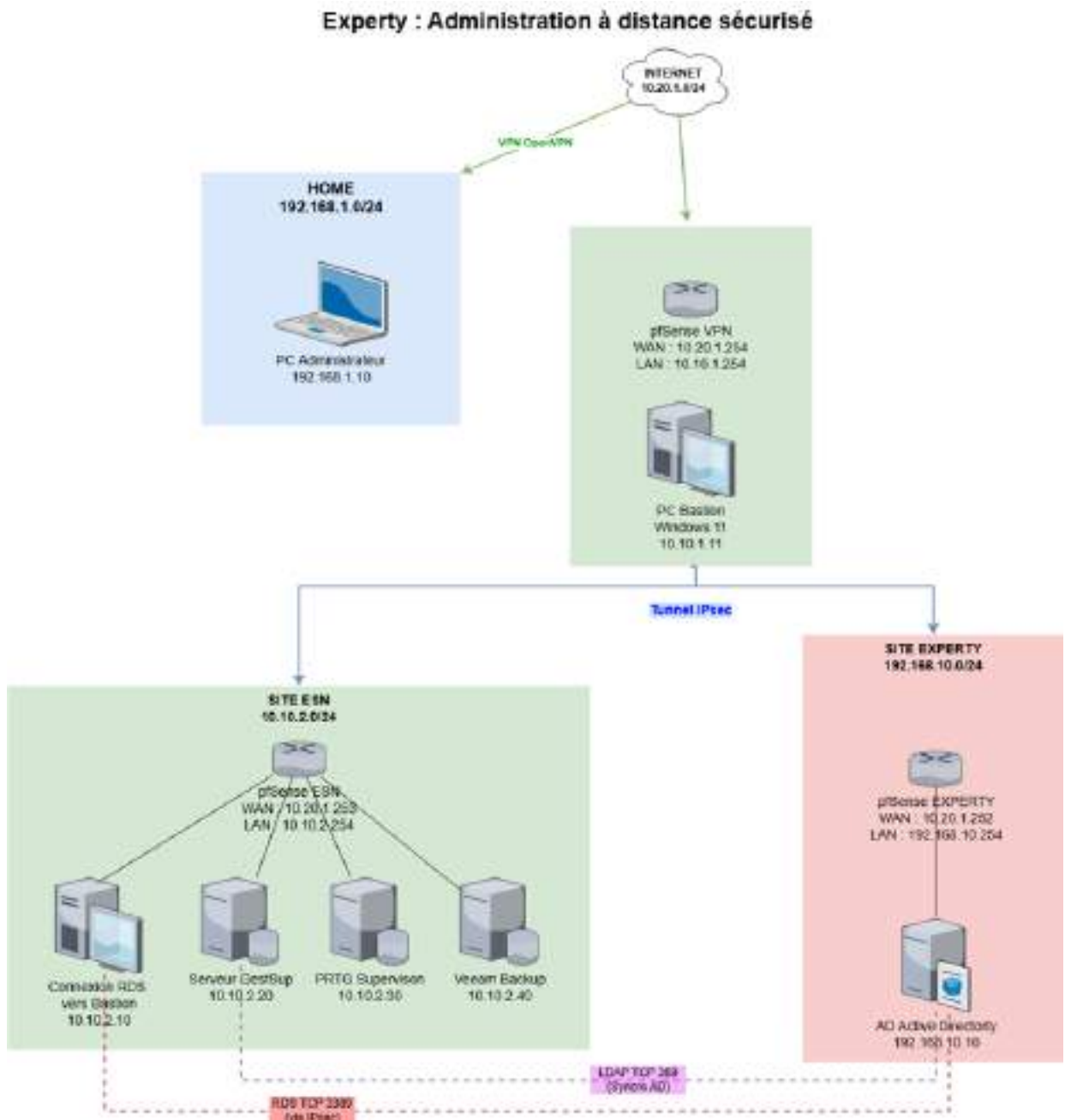
Deux onduleurs sont aussi nécessaires pour garantir un service continu en cas de coupure de courant.

Pour répondre aux nouveaux besoins de l'entreprise Experty, l'infrastructure de l'ESN doit aussi évoluer

Un technicien œuvrant de chez lui ou d'un autre réseau doit pouvoir accéder en toute sécurité aux ressources de l'ESN et de Experty. Pour ce faire, des routeurs Netgate intégrant la solution PFSense doivent être mis en place. La mise en place d'un bastion est aussi nécessaire avec la solution Teleport.

Différentes ressources sont aussi nécessaires pour répondre au besoin de support technique. Pour cela, des serveurs doivent être mis en place comprenant les solutions suivantes :

- GestSup pour la gestion des tickets
- Veeam pour sauvegarder le système GestSup
- PRTG pour la supervision des équipements réseaux



II. Liste du matériel

Plusieurs types de matériel différents sont nécessaires pour la mise en place de l'infrastructure.

A. Serveurs

Tout d'abord, quatre serveurs sont nécessaires. Pour ce faire, les serveurs DELL PowerEdge R660 Serveur rack Smart Selection ont été sélectionnés. Ceux-ci ont un processeur Intel® Xeon® Silver 4410Y 2 GHz, 12C/24T, 16 GT/s, cache 30 Mo, Turbo, HT (150 W), mémoire DDR5 à 4 000 MHz, ainsi qu'une mémoire de 32 Go RDIMM, 5600 MT/s, double rangée. Ils sont aussi équipés de disques SSD 480 Go SATA lecture intensive 6 Gbit/s 512e 2,5" AG à enfichage à chaud, 1 écriture par jour.



Figure 3 Serveur DELL

B. Routeur

Comme évoqué auparavant, des routeurs Netgate 2100 sont nécessaires. Ceux-ci intègrent la solution PFSense et ont une interface web pour les configurer. Ce modèle est prévu pour des petites entreprises.



Figure 4 Routeur Netgate 2100

Voici ces performances :

PERFORMANCE	TECH SPECS
IPERF3 TRAFFIC	IMIX TRAFFIC
L3 Forwarding: 2.20 Gbps	L3 Forwarding: 594 Mbps
Firewall: 964 Mbps (10k ACLs)	Firewall: 249 Mbps (10k ACLs)
IPsec VPN: 254 Mbps (AES-GCM-128 / AES-NI)	IPsec VPN: 90 Mbps (AES-GCM-128 / AES-NI)

Figure 5 Performances Netgate 2100

C. Baie

Une baie est nécessaire pour sécuriser les serveurs, la baie APC NetShelter SX Enclosure with Sides - Rack - noir - 42U - 19" est adaptée de par sa taille et la sécurité qu'elle apporte (fermeture par clé)¹.



Figure 6 Baie APC NetShelter

D. Câbles complémentaires

Des câbles complémentaires à ceux déjà présents dans les locaux peuvent être nécessaires pour connecter les serveurs dans la baie, par exemple des câbles ethernet de 50cm, 1m ou 3m peuvent être nécessaires.

E. Licences windows server 2022

Des licences sont nécessaires pour les serveurs, ici des licences Microsoft Windows Server 2022 Standard - 16 noyaux.

¹<https://www.inmac-wstore.com/apc-netshelter-sx-enclosure-with-sides-rack-42u/p2048821.htm>



Figure 7 Licence Windows Server

III. Solutions applicatives

A. PFSense

PFSense est système d'exploitation permettant la mise en place d'un parefeu. Celui-ci permet de créer des règles pour le trafic.

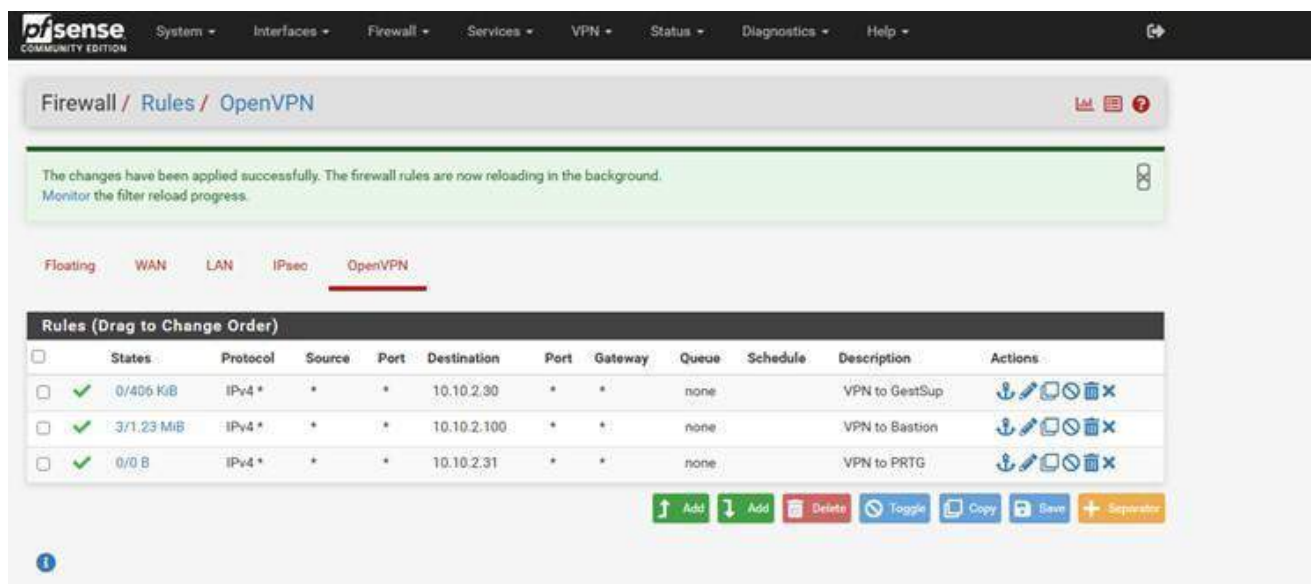


Figure 8 Règles sur le PFSense de l'ESN

Il permet aussi de faciliter la mise en place de VPN, à travers l'outil OpenVPN. La configuration est faite sur le PFSense, puis un client est créé et peut être installé sur différents systèmes d'exploitation, comme Windows 11 par exemple.



Figure 9 OpenVPN sur le PFSense de l'ESN

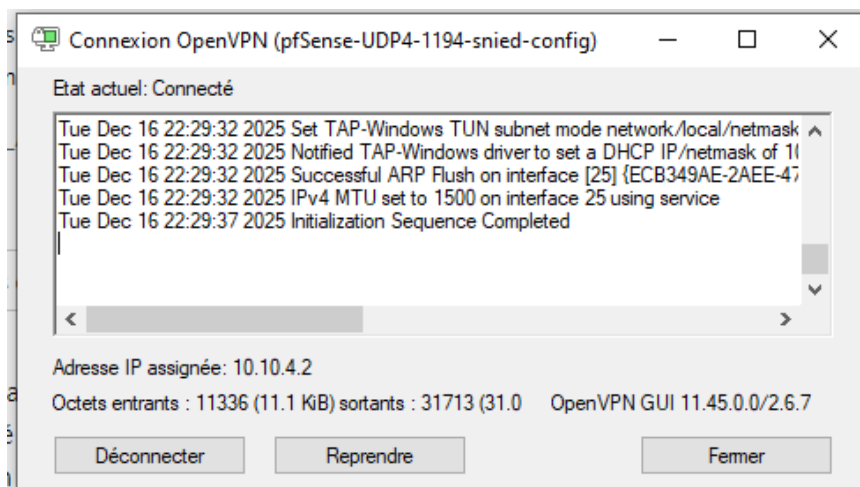


Figure 10 Client OpenVPN sur Windows

PFsense permet aussi de mettre en place des tunnels IPsec. Par exemple ici entre le réseau de l'ESN et le réseau d'Experty.



Figure 11 Tunnel IPsec

PFsense peut aussi servir de DNS si un serveur DNS n'est pas déjà présent dans le réseau.

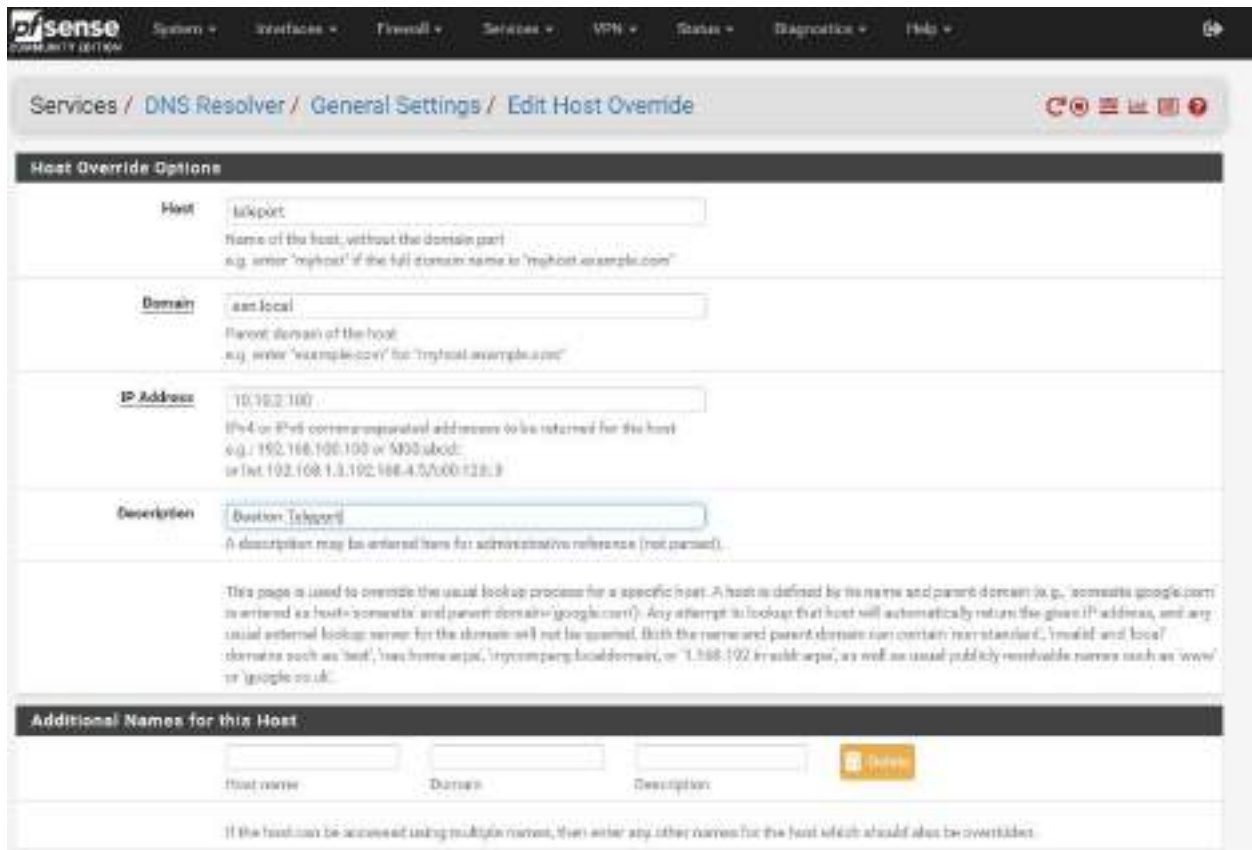


Figure 12 Configuration d'un Host avec le DNS Resolver du PFSense de l'ESN

B. GestSup

GestSup est une solution de gestion de tickets de supports et d'équipements. Elle permet aux utilisateurs d'experty d'ouvrir des tickets lorsqu'un incident survient ou lorsqu'ils ont des requêtes techniques. Les techniciens de l'ESN peuvent alors gérer ces tickets.

Cette solution est connectée à l'active directory d'Experty pour permettre aux utilisateurs de s'identifier avec leurs logins habituels.



Figure 13 Accueil de GestSup avec le compte technicien de l'ESN

C. PRTG Network monitor

PRTG Network Monitor est une solution permettant la supervision des équipements réseaux. Elle permet de surveiller l'état des équipements et d'alerter si un incident survient. Ici, l'infrastructure réseau de l'ESN est celle surveillée, mais il est aussi possible de superviser celle d'Experty si besoin est.



Figure 14 Accueil de la solution PRTG

La solution génère automatiquement une carte réseau, ce qui peut être très pratique pour la documentation ou pour résoudre des incidents.

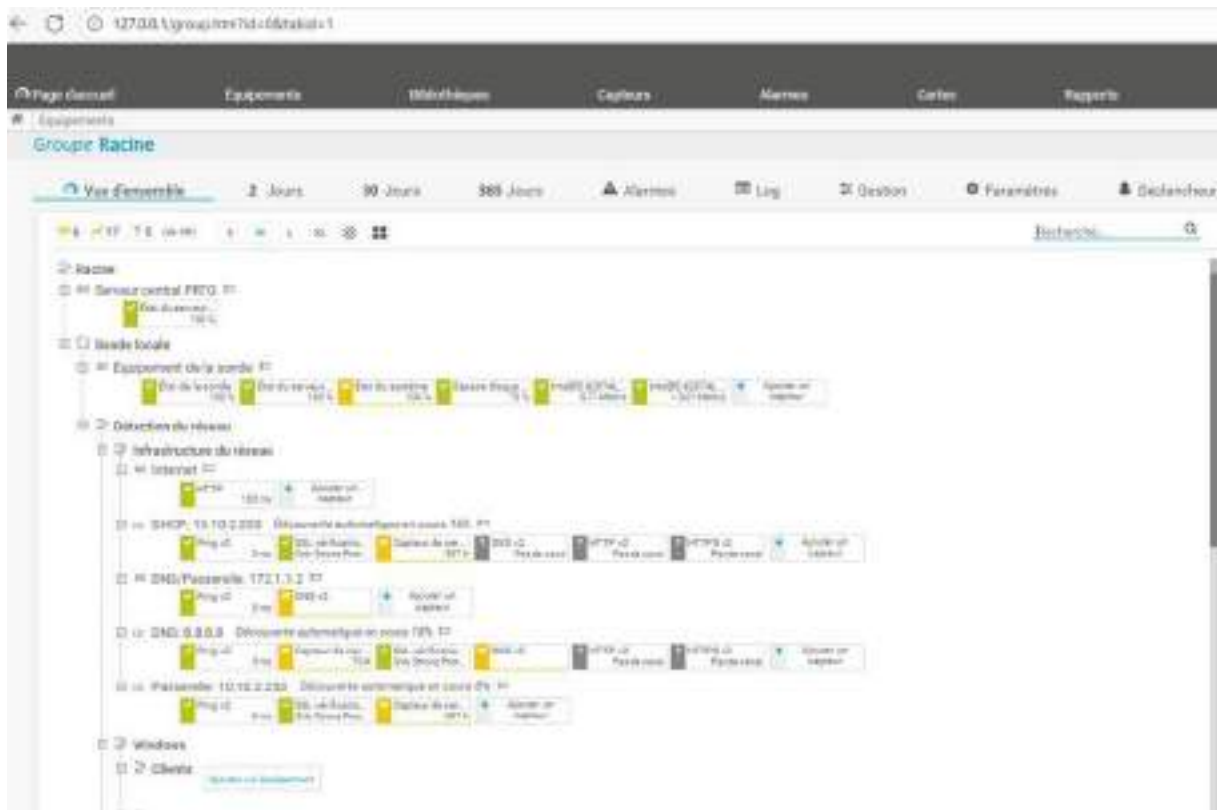


Figure 15 Carte réseau de l'ESN

D. Veeam

Veeam est une solution de sauvegarde et récupération. Veeam va permettre de sauvegarder des systèmes entiers ou juste certains volumes ou fichiers au choix, pour permettre une récupération en cas d'incident.

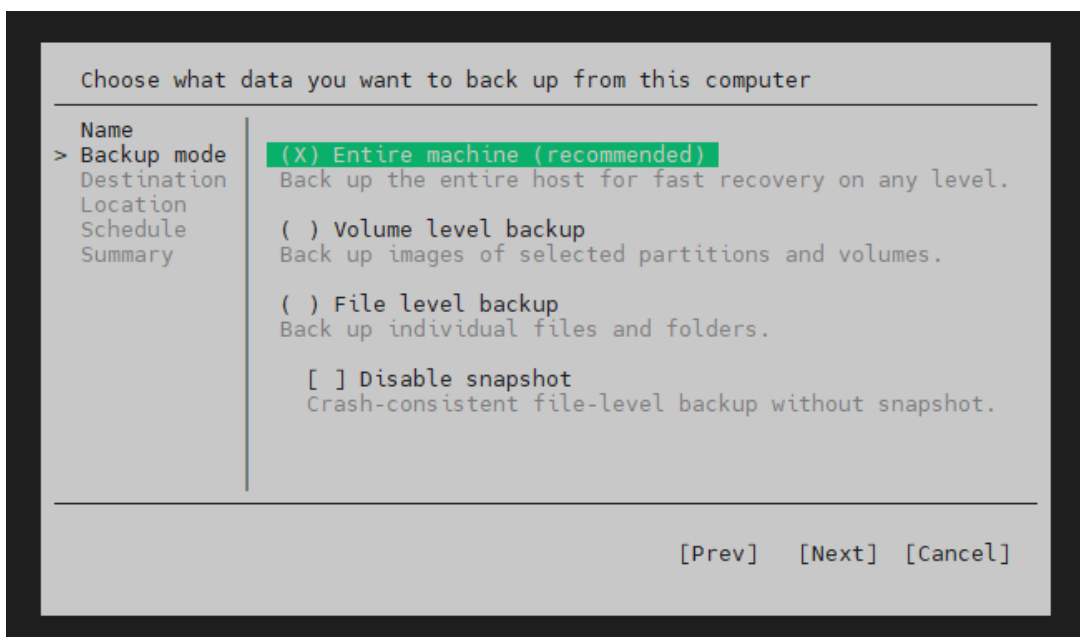


Figure 16 Choix des supports à sauvegarder

Un agent Veeam est installé sur chaque système dont une sauvegarde est souhaitée. Cette sauvegarde peut être faite au rythme souhaité.

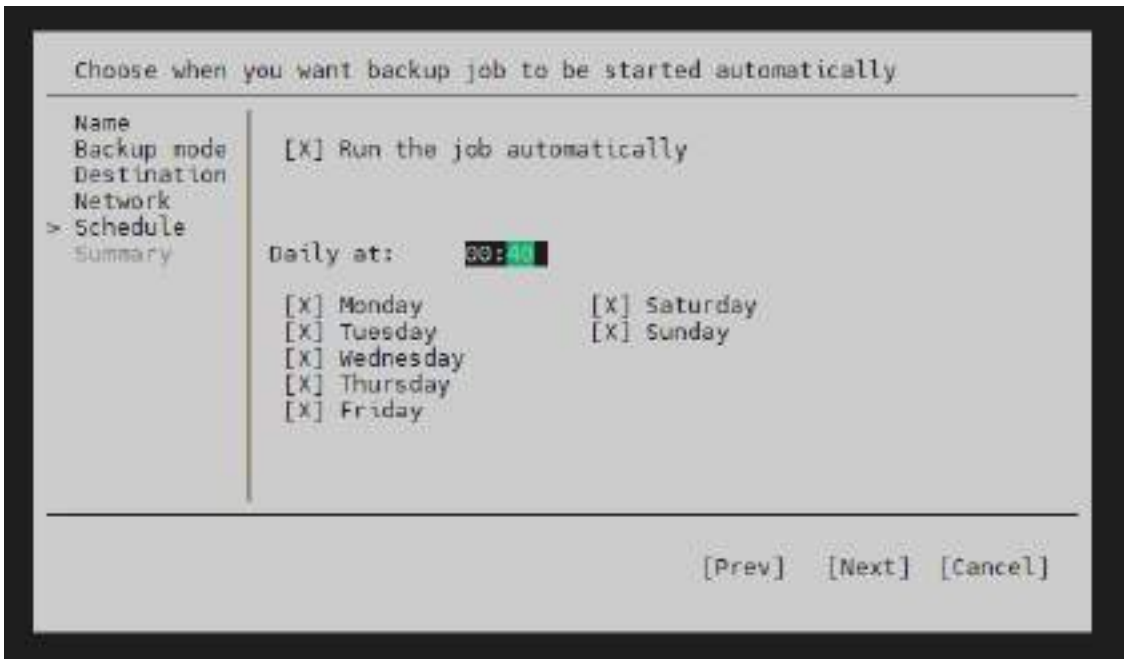


Figure 17 Choix du rythme de la sauvegarde dans Veeam

Elle peut être sauvegardée sur le serveur concerné en local (non recommandé pour des raisons de sécurité), sur un support externe ou dans un dossier partagé, hébergé sur un autre serveur.

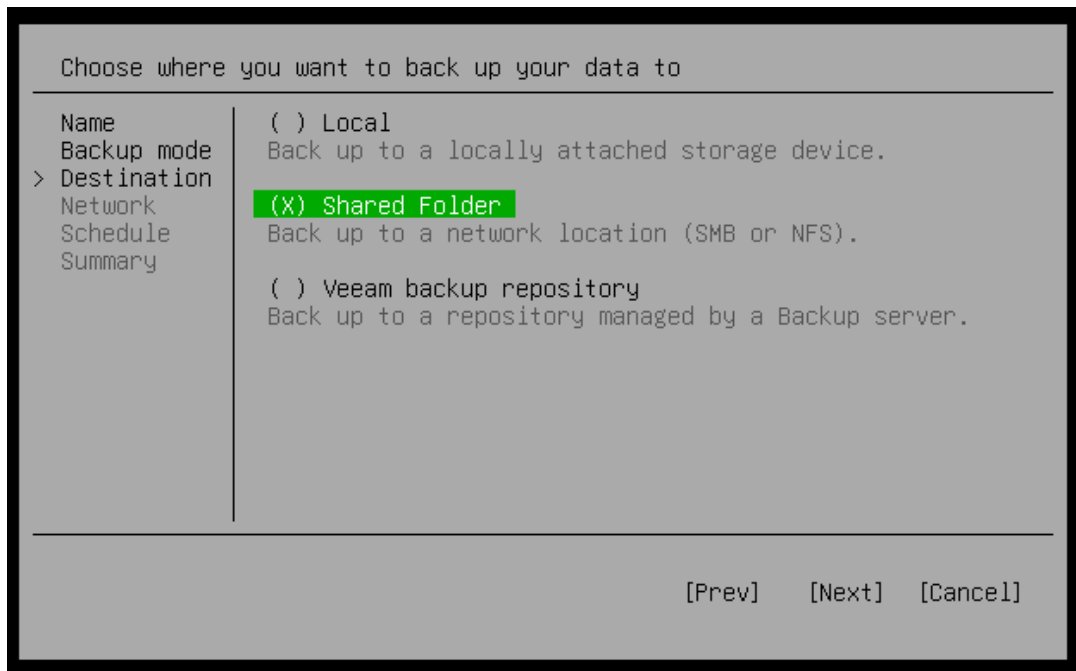


Figure 18 Choix de la destination de la sauvegarde

Pour l'ESN, le choix a été fait de sauvegarder le serveur hébergeant la solution GestSup dans un dossier partagé, hébergé sur un serveur windows dans le même réseau.

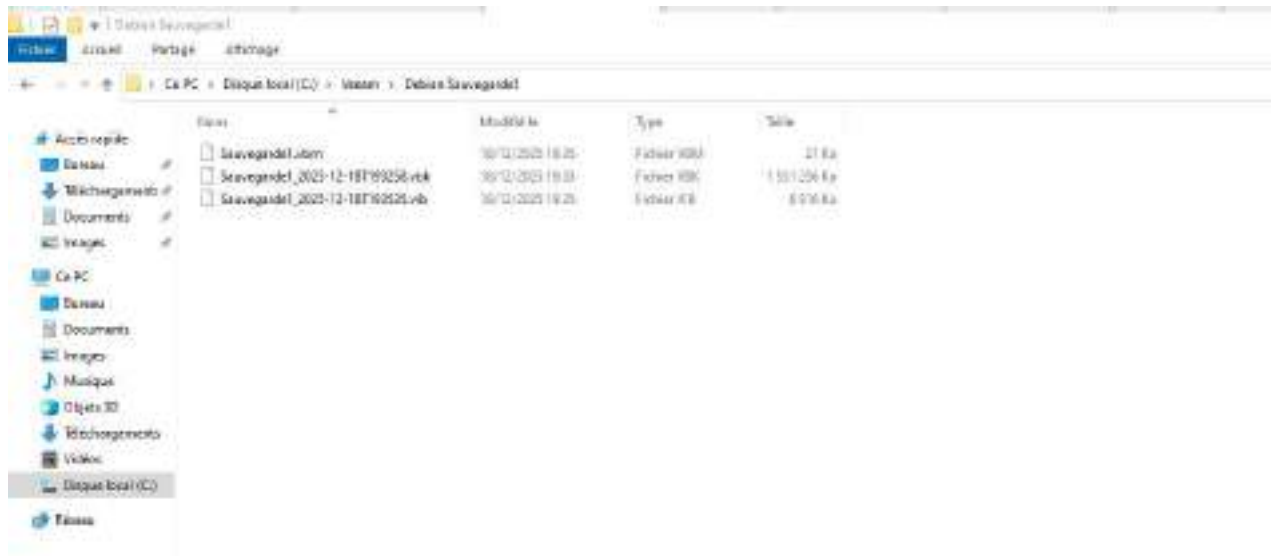


Figure 19 Dossier partagé de sauvegarde veeam

E. Teleport

Teleport est solution permettant un accès Zero Trust aux serveurs et aux applications grâce à différents protocoles. Les utilisateurs ont un utilisateur avec des rôles dédiés dans Teleport leur donnant l'accès que à certaines ressources.

Pour le technicien de l'ESN, celui-ci a accès à Teleport seulement au travers du VPN et a son utilisateur dédié lui permettant seulement l'accès avec son utilisateur de l'Active Directory au domain controller de Experty avec un bureau à distance (RDP).



Figure 20 Accueil de Teleport pour l'administrateur

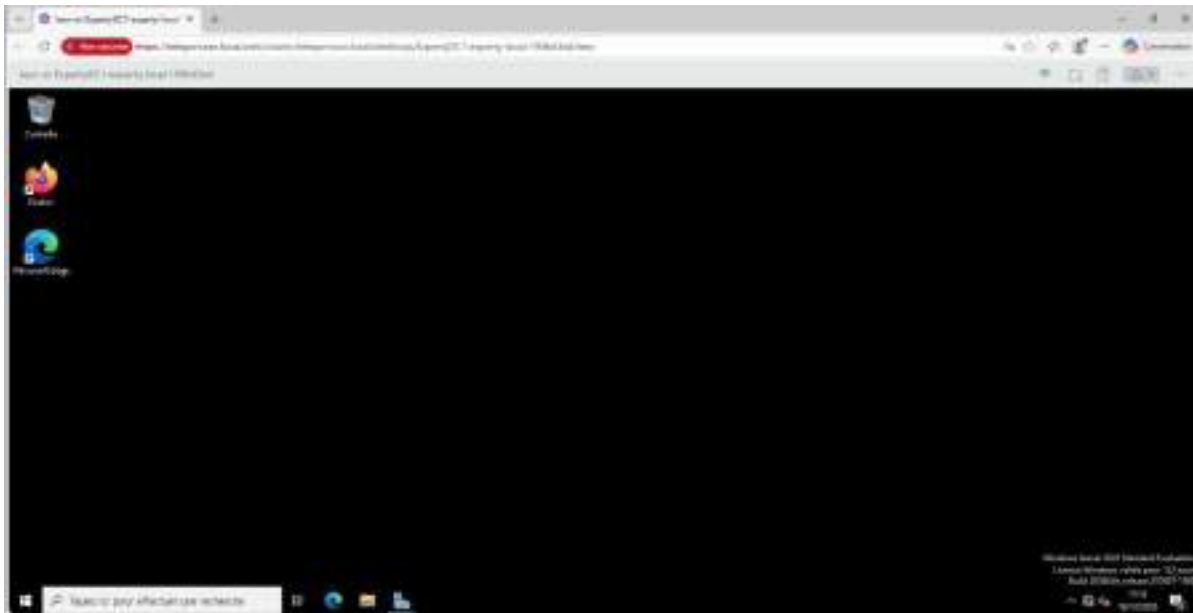


Figure 21 Accès au bureau à distance du DC1 Expert

Teleport permet d'enregistrer les sessions des utilisateurs et de faire des logs des actions.

IV. Politique de Sauvegarde

Tout comme pour le premier projet Expert, une politique de sauvegarde doit être déterminée. Ici il est important de garantir la sécurité du système de support pour avoir un suivi sans encombre.

Pour cela le système GestSup est sauvegardé avec la solution Veeam.

La solution sauvegarde le système entier tous les jours à 00 :40 et la sauvegarde est retenue pendant une période de 7 jours. Cela permet de rétablir le système en cas d'incident.

Partie 2 : Proposition tarifaire

Au sein de la proposition tarifaire doivent être distingués la proposition pour le matériel comprenant les coûts de chaque solution matérielle et la proposition tarifaire pour la prestation réalisée.

I. Proposition pour le matériel

Nom	Quantité	Prix
Serveur	4	25 735 €
Routeurs	2	630 €
Baie	1	1 901,61€
Licences Windows Server 2022	2	748,88€

II. Proposition pour la prestation

Nom	Quantité	Prix
Réalisation de la documentation	1	1 000€
Intervention technicien	2	3 000€
Support technique	1	1 901,61€/ an

Partie 3 : Planning déploiement

Au niveau du déploiement, celui-ci est prévu sur deux jours.

Etape	Nombre de technicien	Durée	Date
Installation physique de la baie avec les serveurs et routeur	1	2h	1 ^{er} jour
Déploiement PFSense	1	5h	1 ^{er} jour
Déploiement de GestSup et la sauvegarde	1	3h	2eme jour
Déploiement Teleport	1	3h	2eme jour
Déploiement PRTG	1	2h	2eme jour

Annexes

I. Procédures

Les procédures qui suivent ont été faites pour le déploiement des différentes solutions évoquées plus haut.

A. Pfsense

1. Installation de base

Assigner les adresses IP aux interfaces LAN et WAN :

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 25bf76fb0e7f3d9e25a1
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      ->
LAN (lan)      -> le1      -> v4: 10.10.2.12/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces         10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system            14) Enable Secure Shell (sshd)
6) Halt system              15) Restore recent configuration
7) Ping host                16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Assigner à l'interface WAN :

Entrer 2 comme option. Ensuite taper 1 pour accéder aux paramètres de l'interface WAN. Mettre n pour le DHCP, puis renseigner l'adresse WAN du pfsense ainsi que le masque de sous-réseau en notation CIDR. Puis renseigner l'adresse de la passerelle

du WAN pour l'upstream gateway adress.

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: 1

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.20.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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

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

Ensuite faire non pour tout ce qui concerne l'IPv6 et refuser l'activation du DHCP sur le WAN :

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

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

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

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Faire de même avec l'interface LAN. Résultat :

```
The IPv4 LAN address has been set to 10.10.1.253/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://10.10.1.253/
```

```
Press <ENTER> to continue.
```

```
VMware Virtual Machine - Netgate Device ID: 25bf76fb0e7f3d9e25a1
```

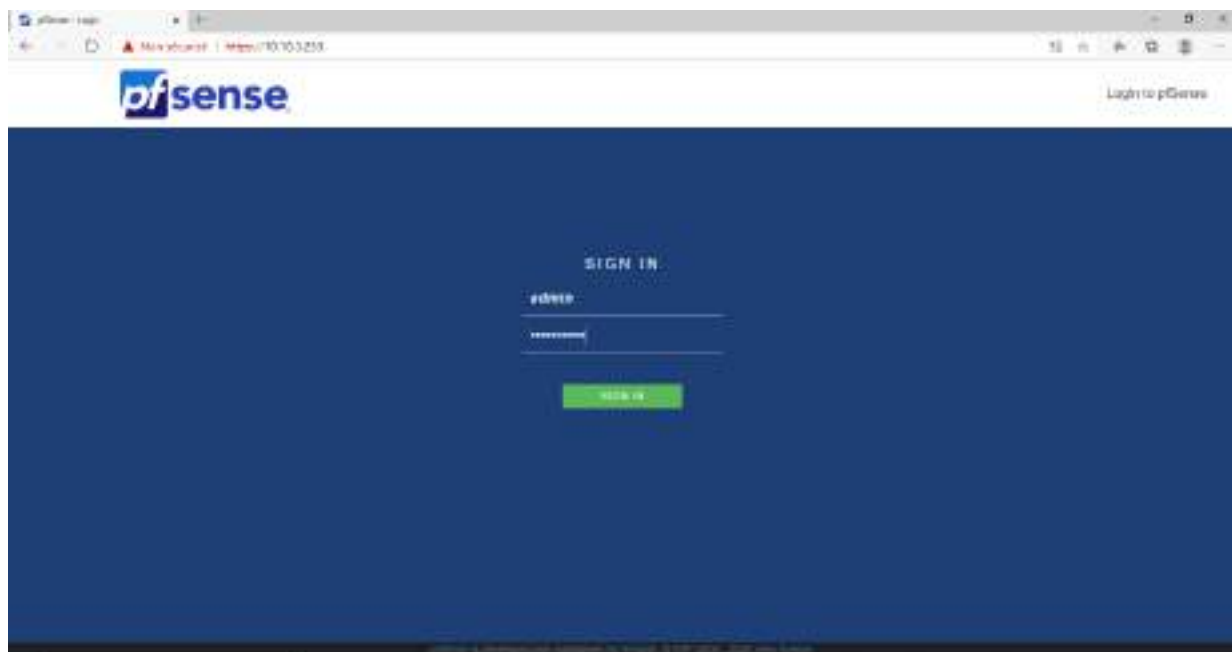
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> le0      -> v4: 10.20.1.1/29
LAN (lan)      -> le1      -> v4: 10.10.1.253/24
```

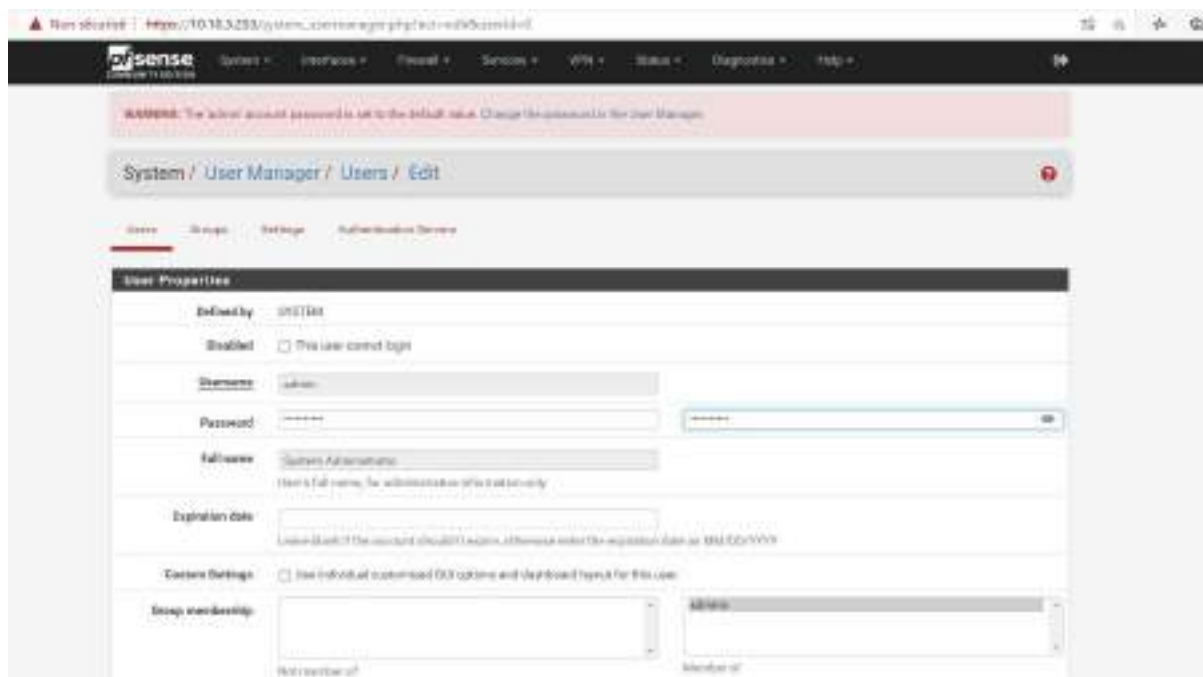
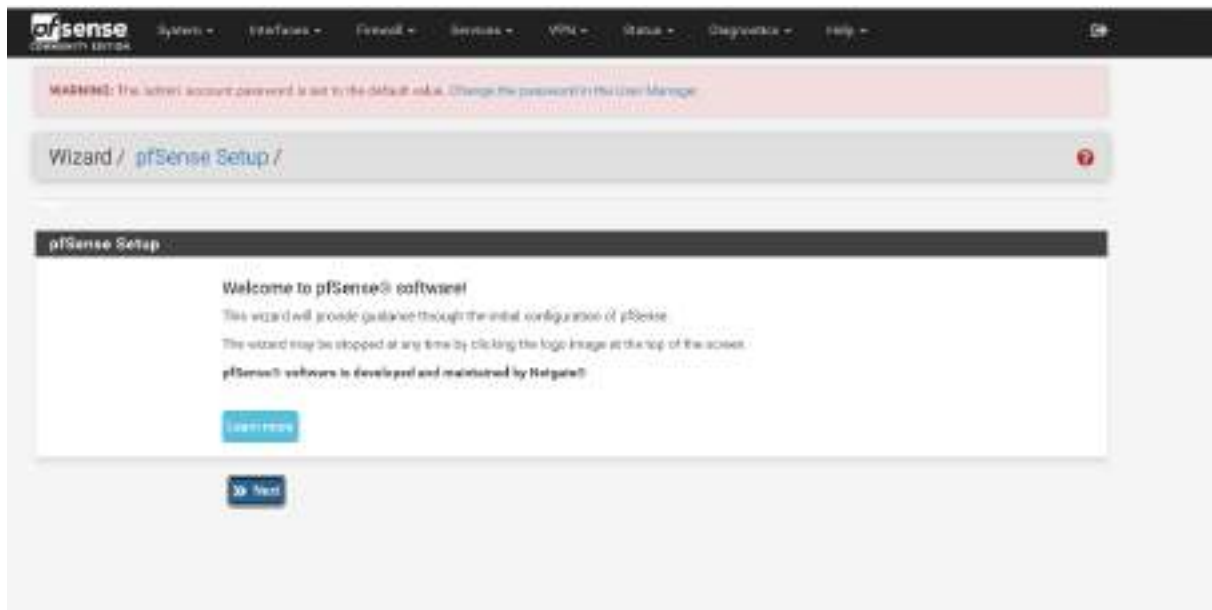
```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

```
Enter an option: S
```

Aller sur un ordinateur/serveur dans le même réseau, sur un navigateur et entrer l'adresse IP LAN du PFSense pour accéder à la page de connexion, utiliser admin/pfsense en login :



Cliquer sur « Change the password in the User Manager” et changer le mot de passe :



Aller dans Interface, WAN, défiler la dernière section intitulée Reserved Networks et désactiver Block private networks et Block bogon networks :



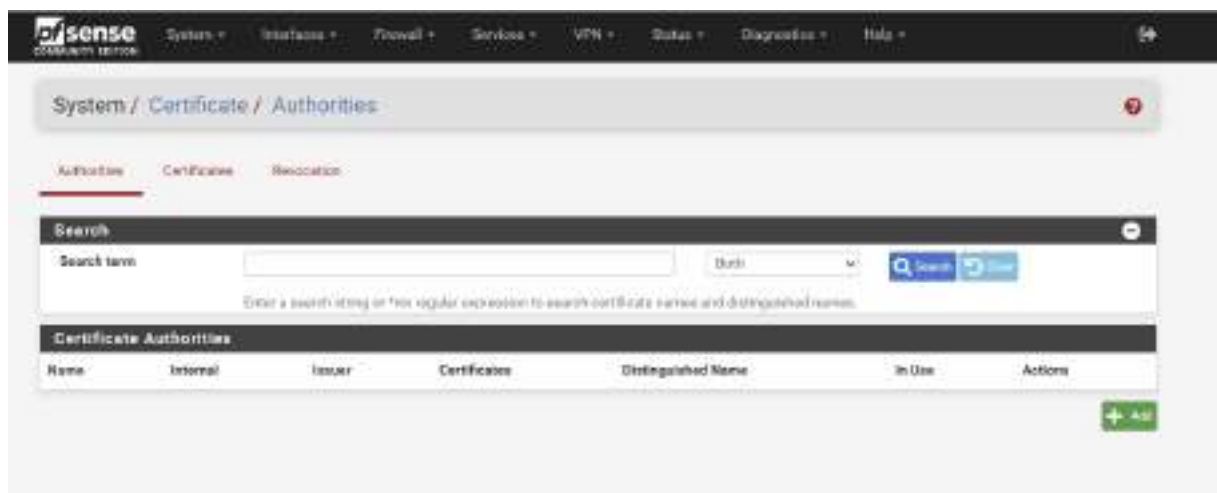
Pour tester si la connexion est bien possible entre les pfSense, rajouter pour le WAN dans Firewall, Rules, WAN, la règle IPv4 ICMP Any et faire un ping :



2. OpenVPN

a. Créer le certificat

Aller dans System, certificates, Authorities et cliquer sur Add :



Renseigner les informations comme suit :

Create / Edit CA

Descriptive name VPN Server CA
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: \, /, <, >, |, ", '.

Method Create an Internal Certificate Authority

Trust Store 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 by the operating system.

Randomize Serial Use random serial numbers when signing certificates
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA
 The length to use when generating a new RSA key, in bits.
 The key length should not be lower than 2048 for some platforms may consider the certificate invalid.

Digest Algorithm sha256
 The digest method used when the CA is signed.
 The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650

Common Name VPNCA
 The following certificate authority subject components are optional and may be left blank.

Country Code FR

State or Province France

City e.g. Austin

Résultat :

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN Server CA	<input checked="" type="checkbox"/>	self-signed	0	ST=France, CN=VPNCA, C=FR <small>Valid From: Tue, 18 Nov 2025 11:30:32 +0000 Valid Until: Fri, 18 Nov 2026 11:30:32 +0000</small>		   

[+ Add](#)

b. Créer les utilisateurs

Aller dans System, User Manager, Users :

System / User Manager / Users

Users Groups Settings Authentication Servers

Username	Full name	Status	Group	Actions
 admin	System Administrator	<input checked="" type="checkbox"/>	admins	

[+ Add](#) [Delete](#)

Cliquer sur Add, remplir les informations nécessaires et cocher Click to create a user certificate :

System / User Manager / Users / Edit

Users | Groups | Settings | Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username:

Password:

Full name:
Use a full name, for administrative information only

Expiration date:
Leave blank if the account should not expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: Use individual/customized UI options and dashboard layout for this user

Group membership:
Not member of Member of

[Add New Group](#) [Add New Member](#)

Hold down CTRL, IPCOMMAND (Mac) key to select multiple items

Certificate: Click to create a user certificate

Create Certificate for User

Descriptive name:

Certificate authority:

Key type:

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.

Digest Algorithm:
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime:

c. Création du serveur OpenVPN

Aller dans VPN, OpenVPN et cliquer sur Wizards :

sense
COMMUNITY EDITION

System | Interfaces | Protocols | Services | VPN | Status | Diagnostics | Help

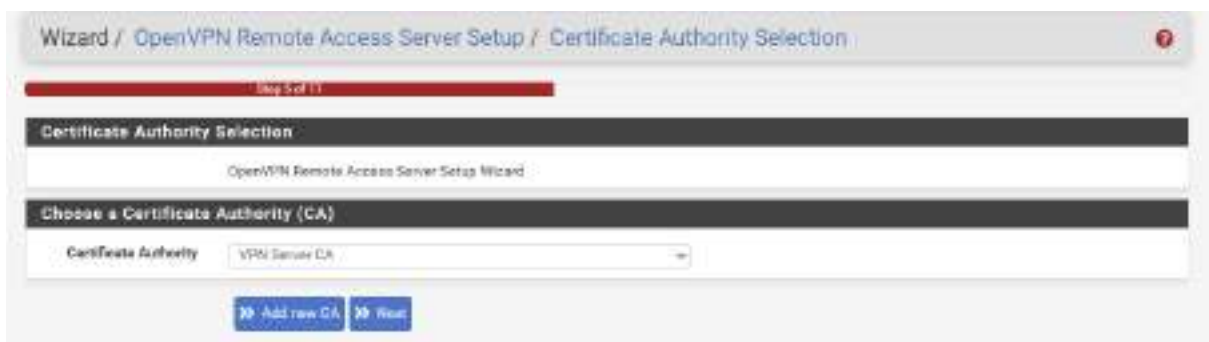
VPN / OpenVPN / Servers

Servers | Clients | Client Specific Overrides | Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
+ Add					

Suivre le wizard :



Ensuite cliquer sur Add new certificate :



Create a New Server Certificate	
Descriptive name	<input type="text" value="CertOpenVPNPrincipal"/> <p>A name for administrative reference, to identify this certificate.</p>
Key length	<input type="text" value="2048 bit"/> <p>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new systems (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com</p>
Lifetime	<input type="text" value="300"/> <p>Lifetime in days. Server certificates should not have a lifetime over 309 days or some platforms may consider the certificate invalid.</p>
Common Name	<input type="text"/> <p>The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of the system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.</p>
Country Code	<input type="text" value="FR"/> <p>Two-letter ISO country code (e.g. US, AU, CN)</p>
State or Province	<input type="text" value="France"/> <p>Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario)</p>
City	<input type="text"/> <p>City or other Locality name (e.g. Austin, Indianapolis, Toronto)</p>
Organization	<input type="text"/> <p>Organization name, often the company or group name.</p>
Organizational Unit	<input type="text"/> <p>Organizational Unit name, often a department or team name.</p>

Renseigner le nom :

Wizard / OpenVPN Remote Access Server Setup / Server Setup	
Step 1 of 1	
Server Setup	
OpenVPN Remote Access Server Setup Wizard	
General OpenVPN Server Information	
Description	<input type="text" value="EOpenVPN"/> <p>A name for this OpenVPN instance, for administrative reference. It can be set to never display, but is often used to distinguish the purpose of the service (e.g. "Private Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.</p>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/> <p>Protocol to use for OpenVPN connections. If unsure, leave this set to UDP</p>
Interface	<input type="text" value="WAN"/> <p>The interface where OpenVPN will listen for incoming connections (typically WAN)</p>
Local Port	<input type="text" value="1194"/> <p>Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.</p>

Renseigner la partie Tunnel settings comme suit :

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.10.0.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.0.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	<input type="text" value="10.10.2.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through the tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text" value="4"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Allow Compression	<input type="text" value="Relax any non-stub compression (Most secure)"/> <small>Allow compression to be used with this VPN instance, which is potentially insecure.</small>
Compression	<input type="text" value="Disable Compression (Dont Preference)"/> <small>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. <small>NOTE: This is not generally recommended, but may be needed for some scenarios.</small>
Duplicate Connection Limit	<input type="text"/> <small>Limit the number of concurrent connections from the same user.</small>

Indiquer l'adresse 10.10.2.254 en serveur DNS et faire next :

Advanced Client Settings	
DNS Default Domain	<input type="text"/> <small>Provide a default domain name to clients.</small>
DNS Server 1	<input type="text" value="10.10.2.254"/> <small>DNS server IP to provide to connecting clients.</small>
DNS Server 2	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>

Cocher Firewall Rule et OpenVPN Rule:

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration ?

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rule

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

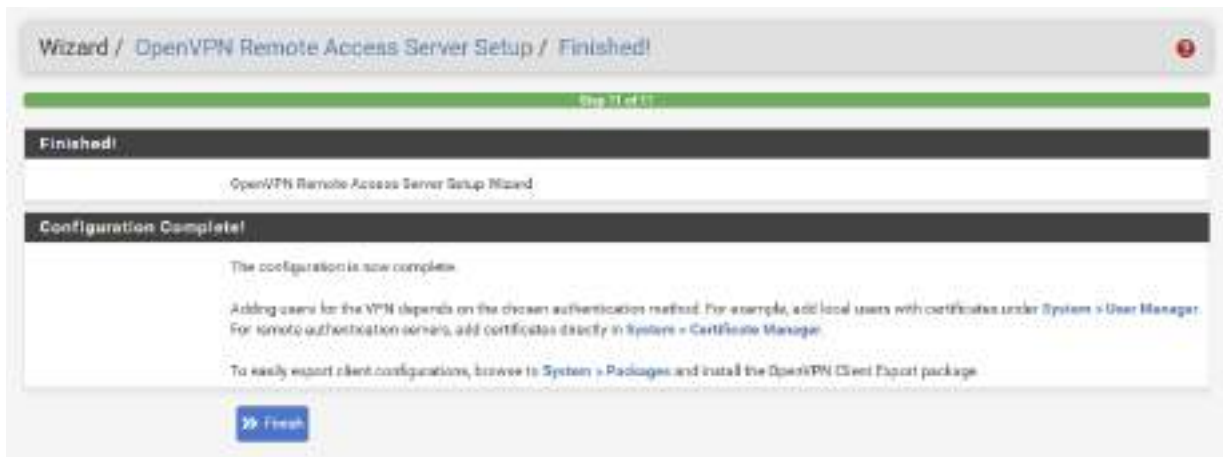
Firewall Rule Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[Next](#)

Terminer le wizard:



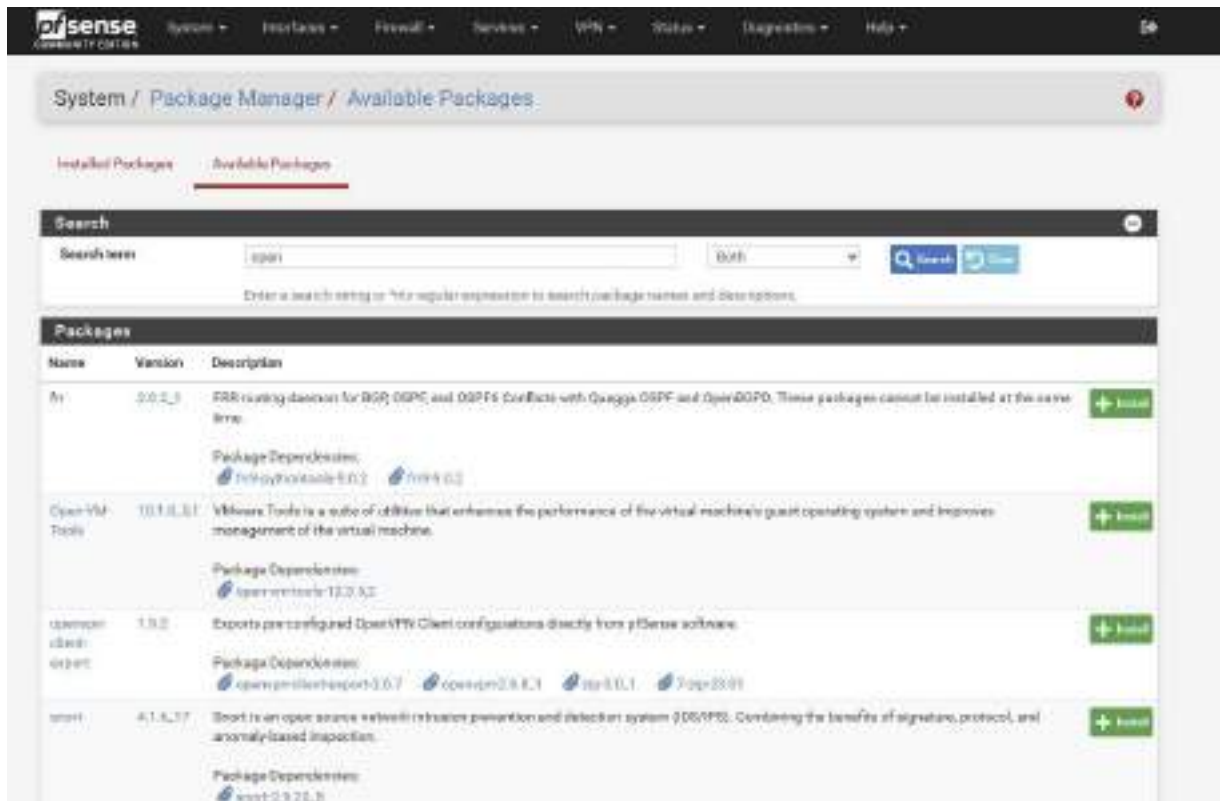
Résultat:



Ensuite vérifier que la règle concernant le VPN s'est bien créée dans Firewall, Rules, WAN :



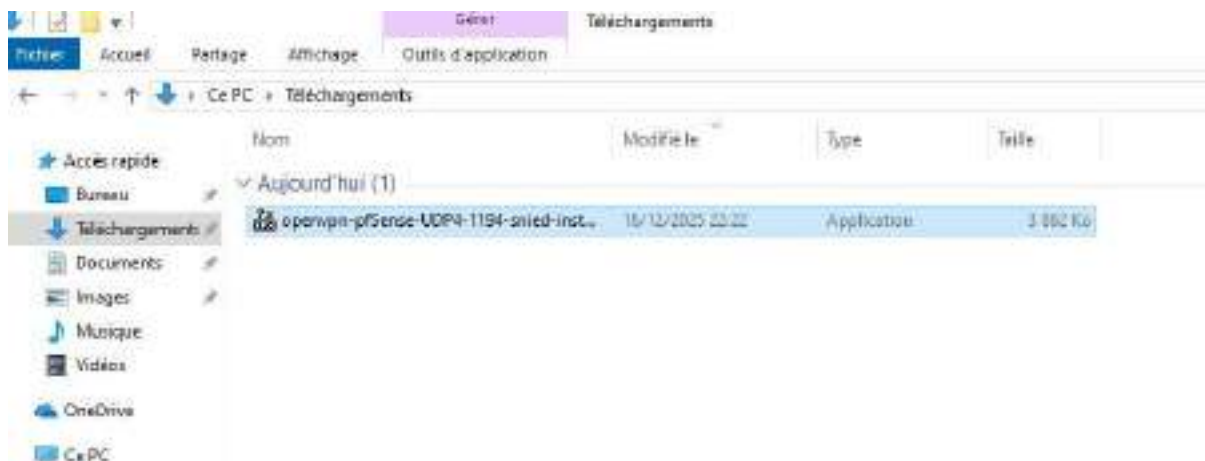
Aller dans System, Package Manager, Available packages et installer openvpn-client-export en cliquant sur install :

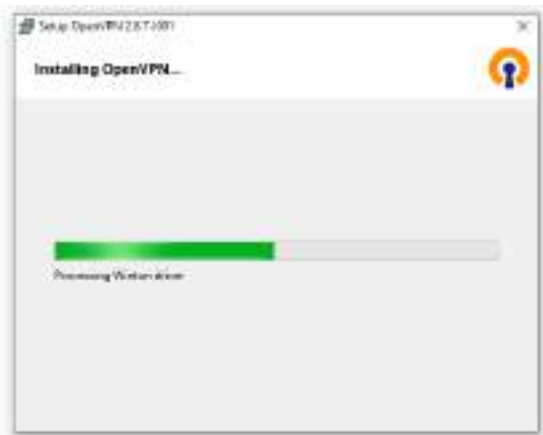


Ensuite aller dans VPN, OpenVPN, Client export et défilez jusqu'à OpenVPN Clients :

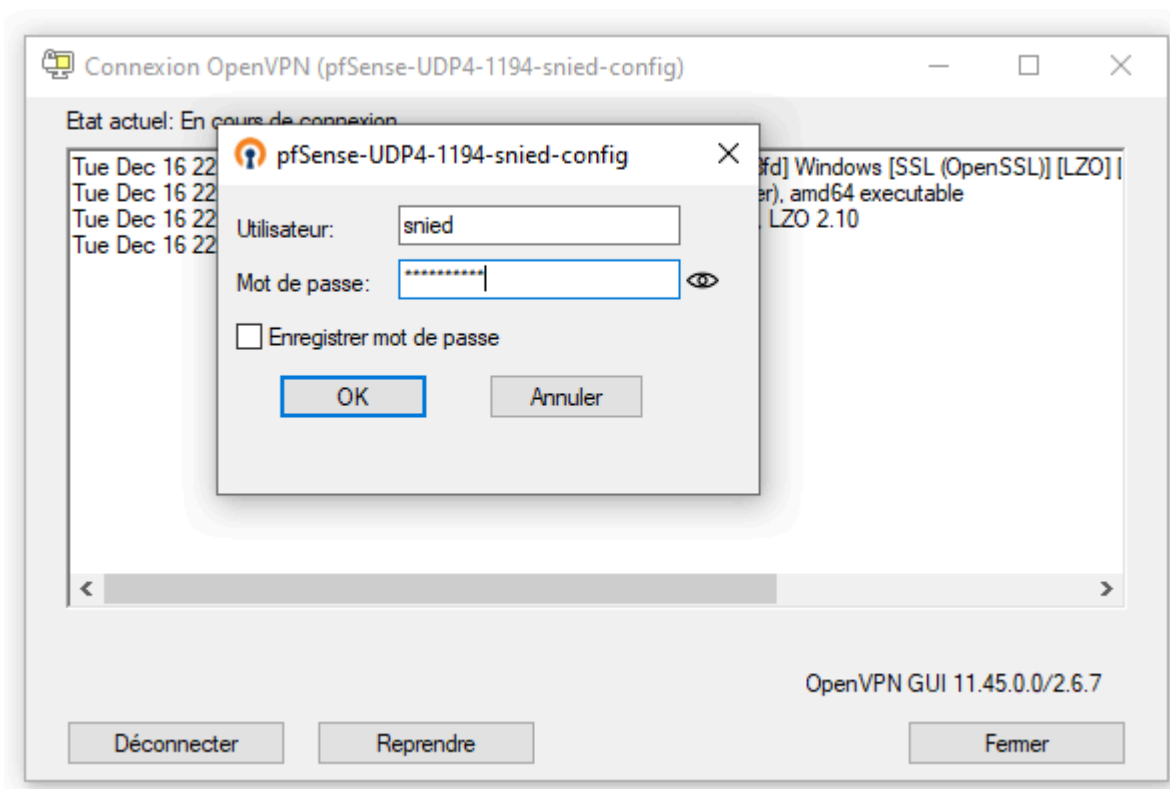


Télécharger le client adapté et l'installer sur le poste cible :

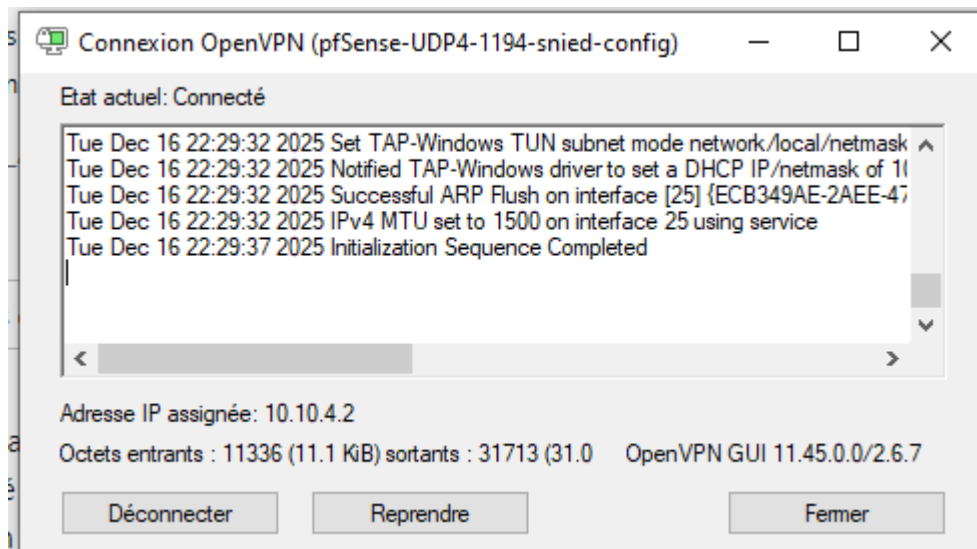




Une fois l'installation terminée, ouvrir OpenVPN GUI et renseigner les identifiants de connexion :



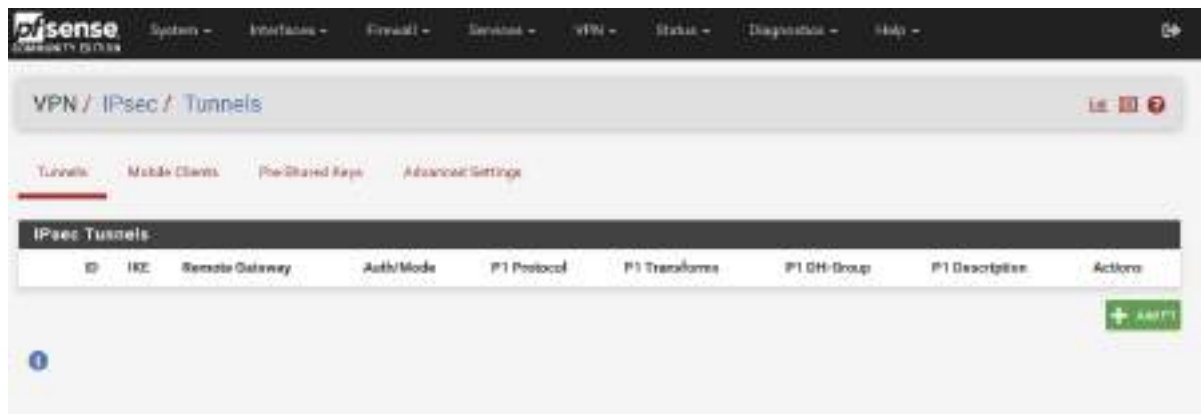
La connexion se fera alors :



Le PC aura alors accès aux ressources du réseau spécifié lors de la création du VPN.

3. IPSec

Aller dans VPN, IPSec :



Le renseigner de la manière suivante en faisant bien attention aux adresses réseaux :

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description IPsec Tunnel Entry
A description may be entered here for administrative reference (not parsed).

Disabled Set this option to disable this phase1 without removing it from the list.

IKE ID 1

IKE Endpoint Configuration

Key Exchange version IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 10.20.1.3
Enter the public IP address or host name of the remote gateway.

Phase 1 Proposal (Authentication)

Authentication Method Mutual PSK
Must match the setting chosen on the remote side.

My identifier My IP address

Peer identifier IP address 10.20.1.3

Pre-Shared Key 6b555a321579a33725e81709f7906dc06613e6e1d789d577afa58c2c
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
[Generate new Pre-Shared Key](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm AES 128 bits SHA256 14 (2048 bit) [Options](#)

Algorithm: Key length: Hash: DH Group:

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

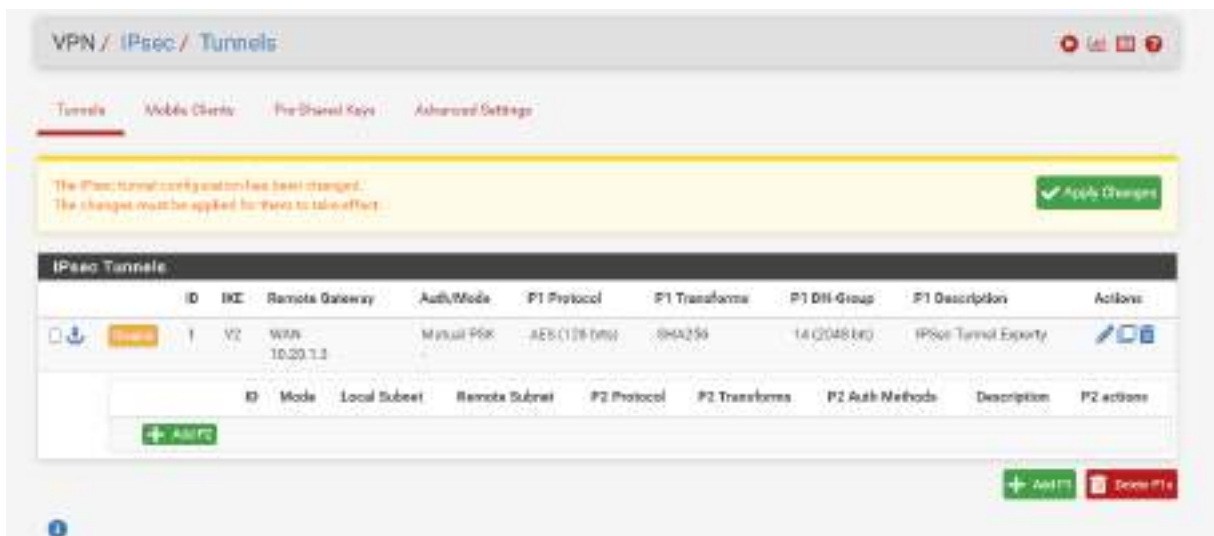
Add Algorithm [+ Add Algorithm](#)

Copier la Pre-Shared Key pour l'utiliser lors de la création du P1 sur l'autre PFSense. Valider.

Retourner sur VPN, IPsec si ce n'est pas déjà le cas, puis cliquer sur Show Phase 2 Entries :



Ensuite cliquer Add P2 :



Renseigner les informations suivantes en faisant bien attention au réseau choisi :

General information	
Description	P2 IPsec Tunnel Exporty A description may be entered here for administrative reference (not passed)
Enabled	<input type="checkbox"/> Enable this phase 2 entry without removing it from the list.
Mode	Tunnel IPv4
Phase 1	IPsec Tunnel To ESPN (IKE ID 1)
Networks	
Local Network	LAN subnet / 0
NAT/BI-NAT translation	None / 0
Remote Network	Network 10.10.2.0 / 28

Valider et faire la même démarche sur l'autre PFSense. Puis aller dans Status, IPsec et cliquer sur Connect P1 and P2s :



Le tunnel s'établit alors :

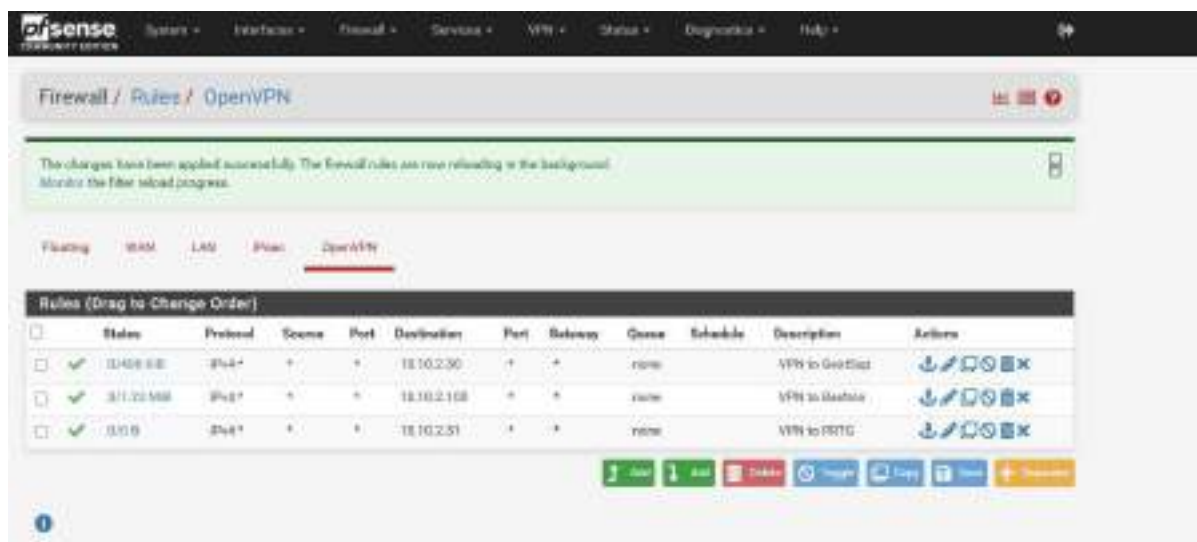


Aller dans Firewall, Rules et ajouter sur les deux Pfsense une règle permettant tout trafic d'un réseau à l'autre. Pour cela cliquer sur Add et renseigner la règle ainsi (en adaptant les réseaux) :

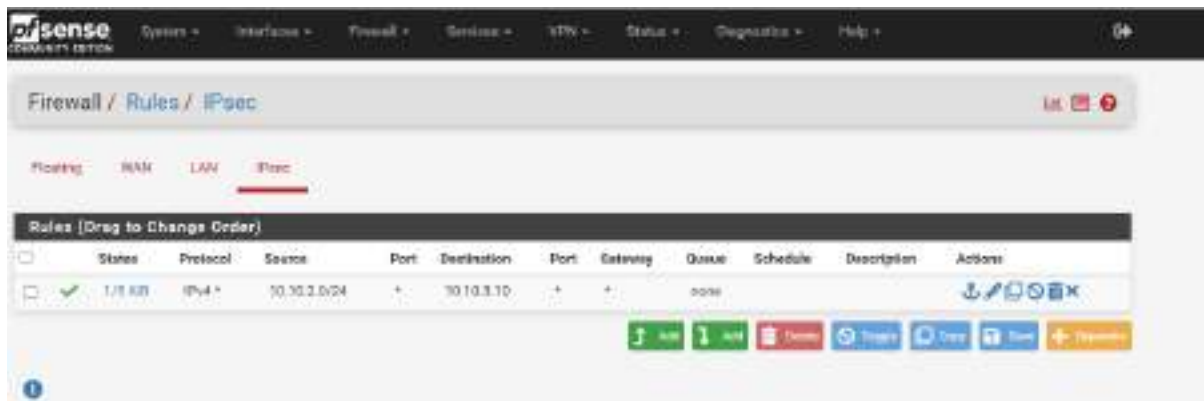


4. Ajuster les règles des Firewalls

Pour le PfSense de l'ESN, aller dans Firewall, Rules, OpenVPN et renseigner des règles permettant le trafic vers chacun des serveurs qui doivent pouvoir être accessibles à partir du VPN, faire Add et renseigner la règle avec l'adresse de destination du serveur :



Pour le PFSense de Experty, aller dans Firewall, Rules, IPsec et créer une règle pour permettre le trafic du réseau de l'ESN vers le domaine controller :



B. Linux GetSup

1. Installation de GestSup

Installer une debian 12, la mettre à jour.

Soit faire une installation automatique en exécutant la commande : `apt install curl -y && curl -s https://gestsup.fr/install.deb12.sh | bash`

Ou alors faire une installation manuelle :

Installer les dépendances nécessaires :

```
apt install apache2 mariadb-server unzip curl ntp
```

```
cron -y apt install php libapache2-mod-php -y
```

```
apt install
```

```
php-{common,curl,gd,imap,intl,ldap,mbstring,mysql,xml,zip} -y
```

Créer l'utilisateur de la base de données dans MariaDB :

```
mariadb -u root
```

```
CREATE USER 'gestsup'@'localhost' IDENTIFIED BY  
'password'; GRANT ALL PRIVILEGES ON *.* TO  
'gestsup'@'localhost'; FLUSH PRIVILEGES;  
exit
```

```
root@Debian:/home/debian# mariadb -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'gestsup'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'gestsup'@'localhost';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> exit
```

Faire `mysql_secure_installation` pour sécuriser la base de données :

```

root@Debian:/home/debian# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

```

Aller dans nano /etc/php/8.2/apache2/php.ini et modifier les paramètres suivants :

max_execution_time = 480

memory_limit = 512M

upload_max_filesize = 8M

date.timezone =

Europe/Paris

```
; Maximum execution time of each script, in seconds
; https://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 480
```

```
; Maximum amount of memory a script may consume
; https://php.net/memory-limit
memory_limit = 512M
```

```
; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 8M
```

```
[Date]
; Defines the default timezone used by the date functions
; https://php.net/date.timezone
;date.timezone = Europe/Paris
```

Puis modifier le fichier de configuration MariaDB nano
/etc/mysql/mariadb.conf.d/50-server.cnf en modifiant ceci, sachant que
pour le innodb, cela doit représenter minimum 25% de la RAM du serveur :

```
innodb_buffer_pool_size =
1G skip-name-resolve
```

```
#
# * InnoDB
#
# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
# Read the manual for more InnoDB related options. There are many!
# Most important is to give InnoDB 80 % of the system RAM for buffer use:
# https://mariadb.com/kb/en/innodb-system-variables/#innodb\_buffer\_pool\_size
innodb_buffer_pool_size = 1G
```

```
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
skip-name-resolve
```

Télécharger le fichier zip de GestSup : `wget -P /var/www/html`
`https://gestsup.fr/downloads/versions/current/version/gestsup_3.2.55.zip` (ne
pas oublier d'ajuster le numéro de version à celle voulue)

Dézipper le fichier : `unzip /var/www/html/gestsup_3.2.55.zip -d`

`/var/www/html` Une fois le fichier dézippé, supprimer le fichier zip et

l'index par défaut :

```
rm
/var/www/html/gestsup_3.2.55.zip
rm /var/www/html/index.html
```

Ajouter l'utilisateur gestsup avec son mot de passe : `adduser gestsup`

--ingroup www-data (si le debian renvoie adduser : command not found, faire export PATH="\$PATH:/sbin:/usr/sbin:/usr/local/sbin" et la commande marchera)

Puis modifier les droits :

```
chown -R gestsup:www-data /var/www/html/  
find /var/www/html/ -type d -exec chmod  
750 {} \; ; find /var/www/html/ -type f -exec  
chmod 640 {} \; ; chmod 770 -R  
/var/www/html/upload  
chmod 770 -R  
/var/www/html/images/model chmod  
770 -R /var/www/html/backup chmod  
770 -R /var/www/html/_SQL  
chmod 660 /var/www/html/connect.php
```

Attribuer une adresse statique à la vm en allant dans
/etc/network/interfaces : allow-hotplug ens37
iface ens37 inet static
address 10.10.2.100/24
gateway 10.10.2.253

Redémarrer le service networking : systemctl restart networking et vérifier
en faisant ip a que l'adresse IP a bien été prise en compte.

Ensuite aller sur l'adresse IP/install et suivre l'installateur, bien mettre
l'utilisateur gestsup et son mot de passe (ici password) comme utilisateur:





Ensuite supprimer le répertoire install : `rm -rf /var/www/html/install/`

Se connecter à l'adresse IP du serveur avec le mot de passe indiqué à la fin de l'installation, puis un pop-up s'ouvre pour demander de changer le mot de passe :

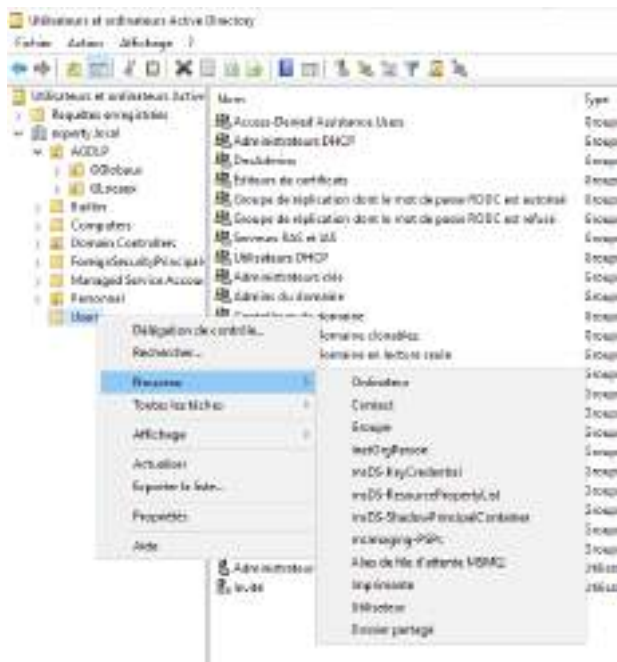


2. Ajouter le connecteur LDAP pour la connexion à l'Active Directory

a. Créer un compte dédié pour Gestsup dans l'Active Directory Aller sur le DC et ouvrir Utilisateurs et ordinateurs Active Directory :



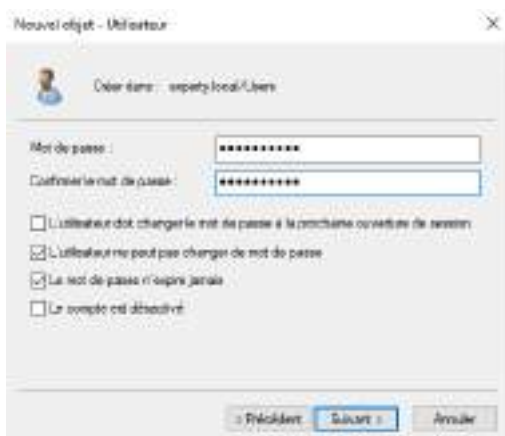
Dérouler experty.local et faire un clic droit sur Users, Nouveau, et cliquer sur Utilisateur :



Renseigner les informations suivantes :



Renseigner le mot de passe, décocher l'utilisateur doit changer et cocher L'utilisateur ne peut pas changer de mot de passe et Le mot n'expire jamais :



Admin.202212

Récupérer le Distinguished Name de cet utilisateur, soit en faisant Affichage, Fonctionnalités Avancées, clic droit sur l'utilisateur, Propriétés, Editeurs d'attributs, distinguishedName, soit en allant sur Powershell et faire cette commande :

```
Get-ADUser -Identity gestsup-ldap | Select-Object
```

DistinguishedName Résultat: CN=GestSup,CN=Users,DC=experty,DC=local

Pour vérifier si le compte marche bien et que la connexion est bien établie, faire apt install ldap-utils -y puis :

```
ldapsearch -x -H ldap://10.10.3.10:389 -D  
"CN=GestSup,CN=Users,DC=experty,DC=local"  
-w "Admin.202212" -b "DC=experty,DC=local"
```

CN=GestSup Service Account,OU=SVC,OU=Experty,DC=experty,DC=local

b. Ajout du connecteur LDAP

Ensuite retourner sur GestSup, aller dans Administration, Paramètres, Connecteurs, LDAP et renseigner les informations suivantes (bien vérifier dans quelle OU se situent les employés) :



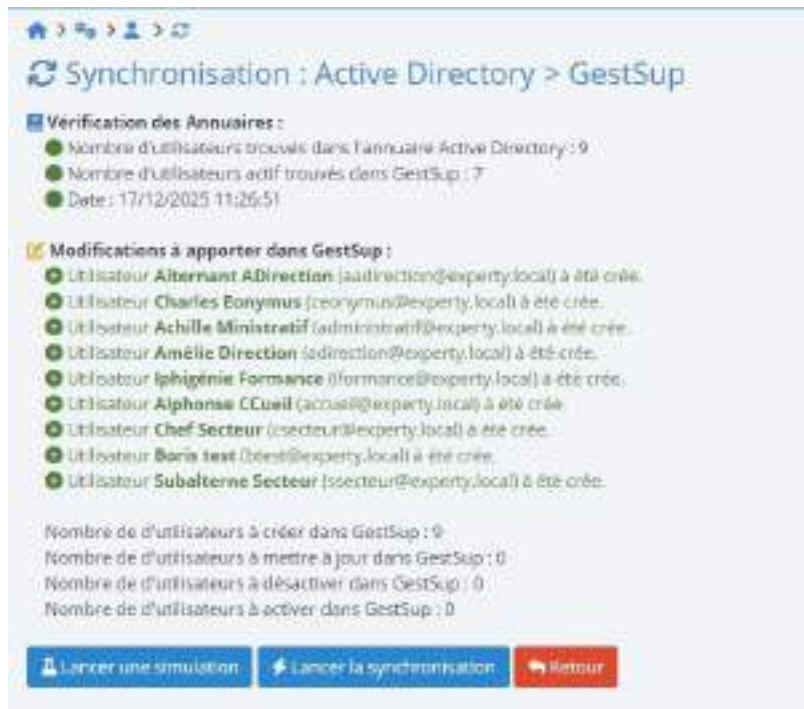
Cliquer sur Test du connecteur LDAP pour vérifier que tout est fonctionnel :



Puis cliquer sur valider.

c. Synchronisation de l'Active Directory

Ensuite aller dans Administration, Utilisateurs et cliquer sur Synchronisation LDAP :



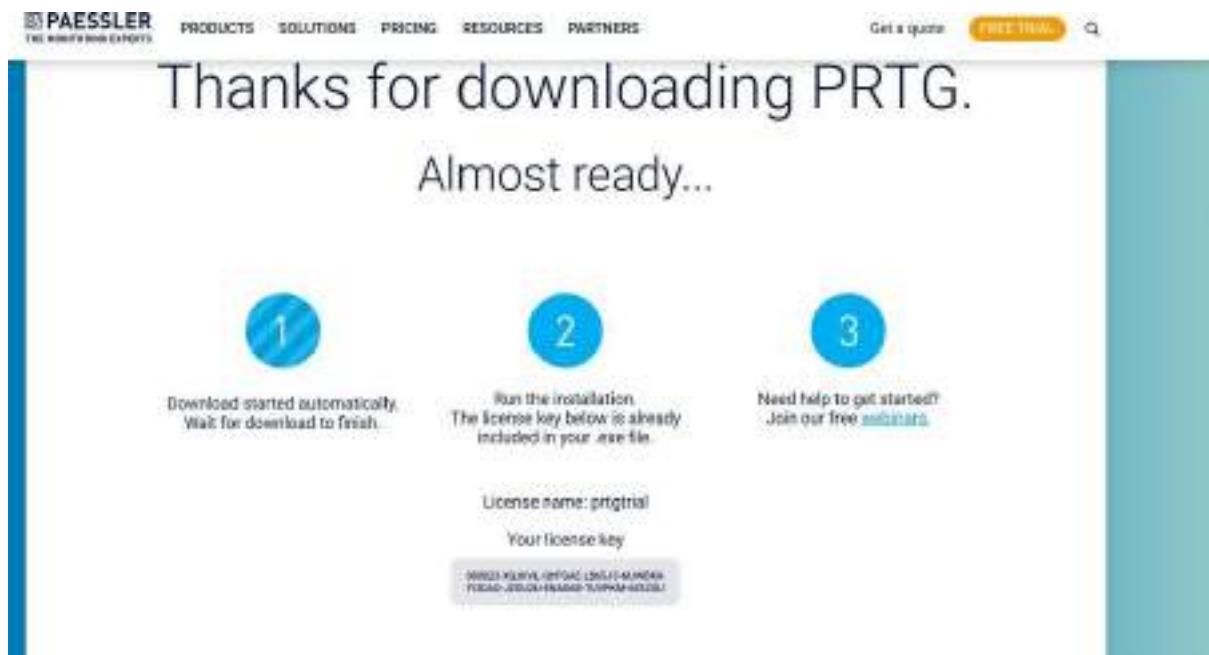
Les utilisateurs peuvent désormais se connecter avec les identifiants de l'Active Directory de Experty. Attention, le serveur AD doit pouvoir être constamment joignable.

C. PRTG

Installer un windows server 2022 et lui attribuer une adresse statique, puis aller sur [Download and Install](#) et télécharger PRTG :



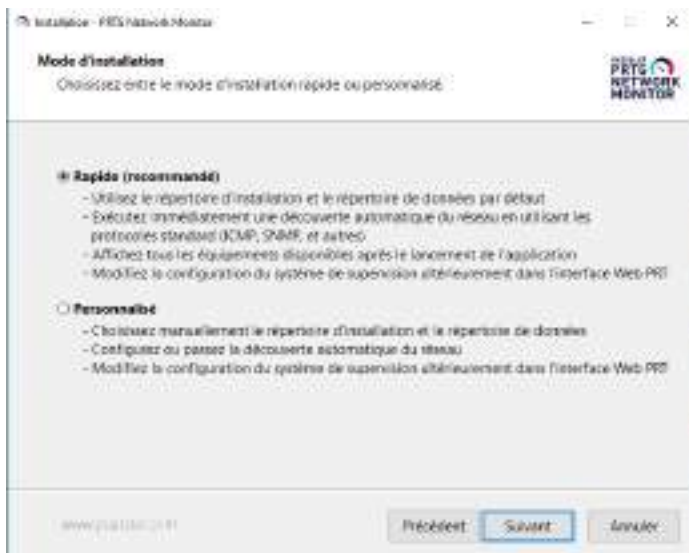
Noter la clé de licence et son nom :



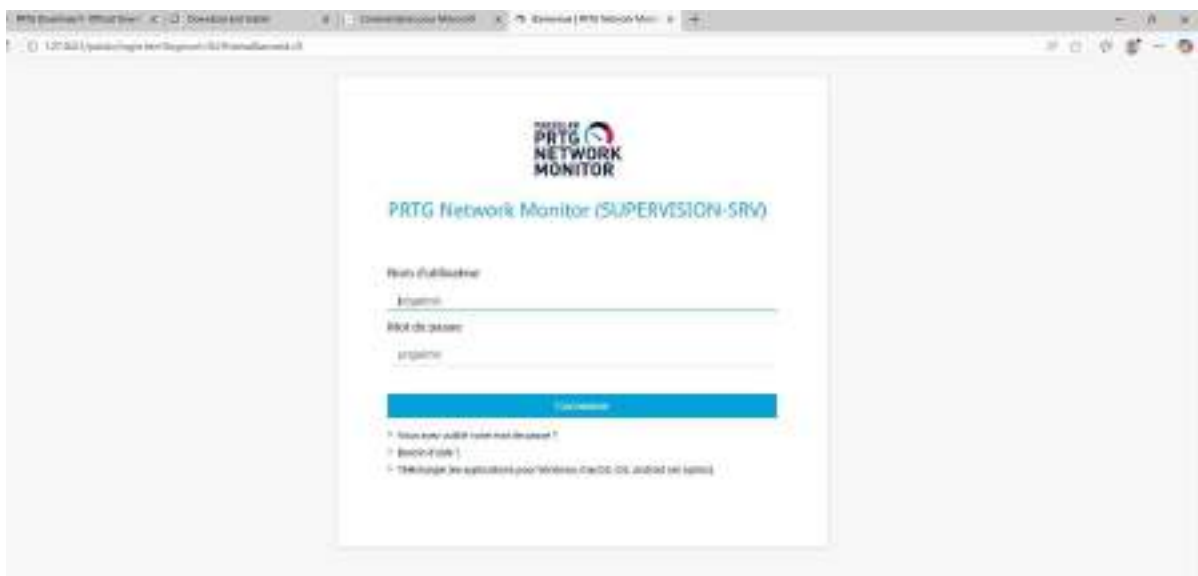
Puis lancer l'assistant d'installation :



Suivre l'installateur et choisir Rapide en mode d'installation :



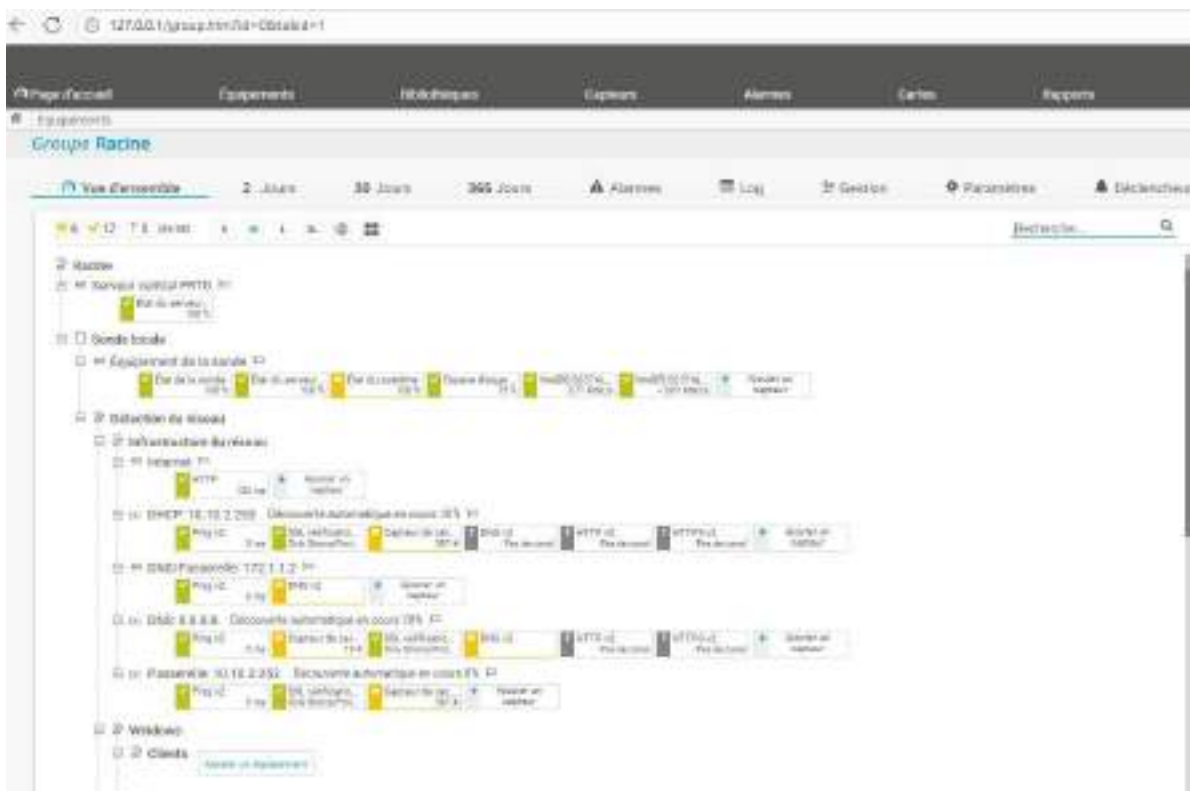
L'installation se poursuit toute seule et se termine en ouvrant cette page :



Faire connexion après avoir modifié le mot de passe pour accéder à la page d'accueil :



Aller sur Equipements pour voir la carte réseau avec les différents équipements détectés par PRTG :



D. Bastion Teleport

1. Installation de Teleport

Installer une debian 12 et lui assigner une adresse IP statique en faisant nano /etc/network/interfaces :

```
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

allow-hotplug ens37
iface ens37 inet static
    address 10.10.2.100/24
    gateway 10.10.2.253
```

```
allow-hotplug ens37
iface ens37 inet static
address 10.10.2.100/24
gateway 10.10.2.253
dns-nameserver
```

10.10.2.253 Faire apt-get install

resolvconf.

Redémarrer le networking : systemctl restart

networking Ensuite créer un répertoire teleport dans

lequel tout sera mis :

```
mkdir -p
/var/lib/teleport cd
/var/lib/teleport
```

Puis générer une clé privée : openssl genrsa -out privkey.pem 2048

Ensuite créer un fichier de configuration OpenSSL nano cert_config.cnf et y coller ceci en adaptant le nom de domaine et l'adresse IP:

```
[req]
default_bits = 2048
prompt = no
default_md =
```

sha256
distinguished_name = dn
req_extensions = v3_req

```
[dn]
C = FR
ST = Grand Est
L = Strasbourg
O = ESN
CN = teleport.esn.local
```

```
[v3_req]
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1 = teleport.esn.local
DNS.2 = *.teleport.esn.local
IP.1 = 10.10.2.100
```

Puis générer le certificate openssl:

```
openssl req -new -x509 -key privkey.pem -out fullchain.pem -days 365 \
-config cert_config.cnf -extensions v3_req
```

Pour verifier si le certificat s'est bien généré : `openssl x509 -in fullchain.pem -text -noout | grep -A1 "Subject Alternative Name"`

```
root@debian:/var/lib/teleport# openssl x509 -in fullchain.pem -text -noout | grep -A1 "Subject Alternative Name"
X509v3 Subject Alternative Name:
    DNS:teleport.esn.local, DNS:*.teleport.esn.local, IP Address:10.10.2.100
```

Ensuite accorder les bons droits :

```
chmod 600 privkey.pem
chmod 644 fullchain.pem
chown -R root:root /var/lib/teleport
```

```
root@debian:/home/debian# mkdir -p /var/lib/teleport
root@debian:/home/debian# cd /var/lib/teleport
root@debian:/var/lib/teleport# openssl genrsa -out privkey.pem 2048
root@debian:/var/lib/teleport# nano cert_config.cnf
root@debian:/var/lib/teleport# openssl req -new -x509 -key privkey.pem -out fullchain.pem -days 365 \
-config cert_config.cnf -extensions v3_req
root@debian:/var/lib/teleport# openssl x509 -in fullchain.pem -text -noout | grep -A1 "Subject Alternative Name"
X509v3 Subject Alternative Name:
    DNS:teleport.esn.local, DNS:*.teleport.esn.local, IP Address:10.10.2.100
root@debian:/var/lib/teleport# chmod 600 privkey.pem
root@debian:/var/lib/teleport# chmod 644 fullchain.pem
root@debian:/var/lib/teleport# chown -R root:root /var/lib/teleport
```

Puis télécharger teleport: `wget -O- https://cdn.teleport.dev/install.sh | bash -s 18.5.1`

```

Lecture des listes de paquets... Fait
+ set +x
+ apt-get install -y teleport-is.9.1
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  teleport
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 214 Mo dans les archives.
Après cette opération, 810 Mo d'espace disque supplémentaires seront utilisés.
Réception de 11 http://apt.releases.teleport.dev/debian bookworm/stable/v18.5.1 amd64 teleport amd64 18.5.1 [214 MB]
214 Mo réceptionnés en 25 (107 Mo/s)
Sélection du paquet teleport précédemment désélectionné.
Lecture de la base de données... 16318 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../teleport_18.5.1_amd64.deb ...
Dépaquetage de teleport (18.5.1) ...
Paramétrage de teleport (18.5.1) ...
Teleport System symlinks creation...
2025-12-17T18:03:28.419+01:00 INFO [UPDATER] Validating binary name:fdpass-teleport agent/validate.go:68
2025-12-17T18:03:28.421+01:00 INFO [UPDATER] Binary does not support version command name:fdpass-teleport agent/validate.go:70
2025-12-17T18:03:28.421+01:00 INFO [UPDATER] Validating binary name:tbot agent/validate.go:68
2025-12-17T18:03:28.481+01:00 INFO [UPDATER] [stdout] Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 agent/logger.go:74
2025-12-17T18:03:28.482+01:00 INFO [UPDATER] Validating binary name:tctl agent/validate.go:68
2025-12-17T18:03:28.569+01:00 INFO [UPDATER] [stdout] Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 agent/logger.go:74
2025-12-17T18:03:28.570+01:00 INFO [UPDATER] Validating binary name:teleport agent/validate.go:68
2025-12-17T18:03:28.664+01:00 INFO [UPDATER] [stdout] Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 agent/logger.go:74
2025-12-17T18:03:28.667+01:00 INFO [UPDATER] Validating binary name:teleport-update agent/validate.go:68
2025-12-17T18:03:28.677+01:00 INFO [UPDATER] [stdout] teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 agent/logger.go:74
2025-12-17T18:03:28.678+01:00 INFO [UPDATER] Validating binary name:tsh agent/validate.go:68
2025-12-17T18:03:28.707+01:00 INFO [UPDATER] [stdout] Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 agent/logger.go:74
2025-12-17T18:03:28.795+01:00 INFO [UPDATER] System configuration synced. unit:teleport.service agent/process.go:1385
2025-12-17T18:03:28.800+01:00 INFO [UPDATER] Successfully linked system package installation. agent/updater.go:1427
+ set +x

Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11 installed successfully!

The following commands are now available:
  teleport - The daemon that runs the Auth Service, Proxy Service, and other Teleport services.
  tsh      - A tool that lets end users interact with Teleport.
  tctl     - An administrative tool that can configure the Teleport Auth Service.
  tbot     - Teleport Machine ID client.
  fdpass-teleport - Teleport Machine ID client.
  teleport-update - Teleport auto-update agent.
root@debian:/var/lib/teleport# teleport version
Teleport v18.5.1 git:v18.5.1-0-g0d82e73 go1.24.11

```

Ensuite faire:

```

teleport configure -o file --cluster-name=teleport.esn.local
--public-addr=teleport.esn.local:443
--cert-file=/var/lib/teleport/fullchain.pem
--key-file=/var/lib/teleport/privkey.pem

```

```

$ teleport configure -o file
2025-12-17T18:03:28.800+01:00 INFO [UPDATER] System configuration synced. unit:teleport.service agent/process.go:1385
2025-12-17T18:03:28.800+01:00 INFO [UPDATER] Successfully linked system package installation. agent/updater.go:1427
+ set +x

```

Puis démarrer le service teleport :

```

root@debian:/var/lib/teleport# systemctl enable teleport
Created symlink /etc/systemd/system/multi-user.target.wants/teleport.service → /lib/systemd/system/teleport.service.
root@debian:/var/lib/teleport# systemctl start teleport

```

2. Ajout du nom de l'hôte dans le DNS

Sur PfSense, cliquer sur Services, DNS Resolver, défiler jusqu'à Host Override et cliquer sur Add :



Puis renseigner de la façon suivante :

pfsense System + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +

Services / DNS Resolver / General Settings / Edit Host Override

Host Override Options

Host
 Name of the host, without the domain part
 e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain
 Parent domain of the host
 e.g. enter "example.com" for "myhost.example.com"

IP Address
 IPv4 or IPv6 comma-separated addresses to be returned for the host
 e.g.: 192.168.100.100 or f00:abcd:
 or list 192.168.1.3,192.168.4.5,600:123:3

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

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., "example.google.com" is entered as host="example" and parent domain="google.com"). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain non-standard, "valid and local" domains such as "local", "yes home.local", "mycompany.localdomain", or "1.988.192.in-addr.arpa", as well as usual publicly resolvable names such as "www" or "google.co.uk".

Additional Names for this Host

Host name Domain Description

If the host can be accessed using multiple names, then enter any other names for the host which should also be overridden.

Faire de même pour expertydc1.experty.local avec en alias expertydc1.local :

Host Override Options

Host
 Name of the host, without the domain part
 e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain
 Parent domain of the host
 e.g. enter "example.com" for "myhost.example.com"

IP Address
 IPv4 or IPv6 comma-separated addresses to be returned for the host
 e.g.: 192.168.100.100 or f00:abcd:
 or list 192.168.1.3,192.168.4.5,600:123:3

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

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., "example.google.com" is entered as host="example" and parent domain="google.com"). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain non-standard, "valid and local" domains such as "local", "yes home.local", "mycompany.localdomain", or "1.988.192.in-addr.arpa", as well as usual publicly resolvable names such as "www" or "google.co.uk".

Additional Names for this Host

Host name Domain Description

Vérifier que teleport fonctionne en allant sur teleport.esn.local :



Si une page blanche est la seule chose qui s'affiche, vérifier que Edge est à jour, minimum au-dessus de 110 pour la version.

Vérifier que la debian teleport peut bien ping expertydc.experty.local.

3. Création du compte

administrateur Créer un utilisateur

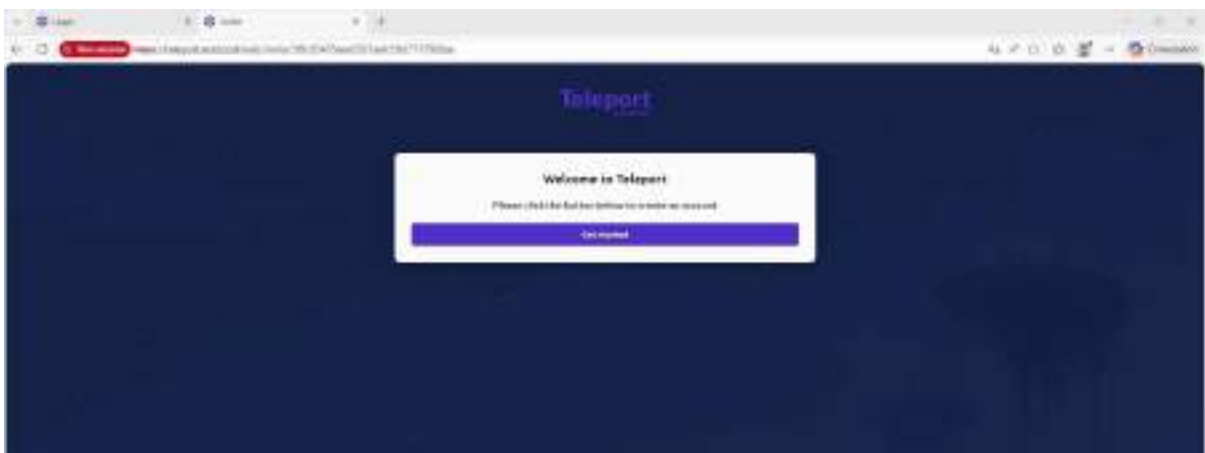
Teleport en faisant

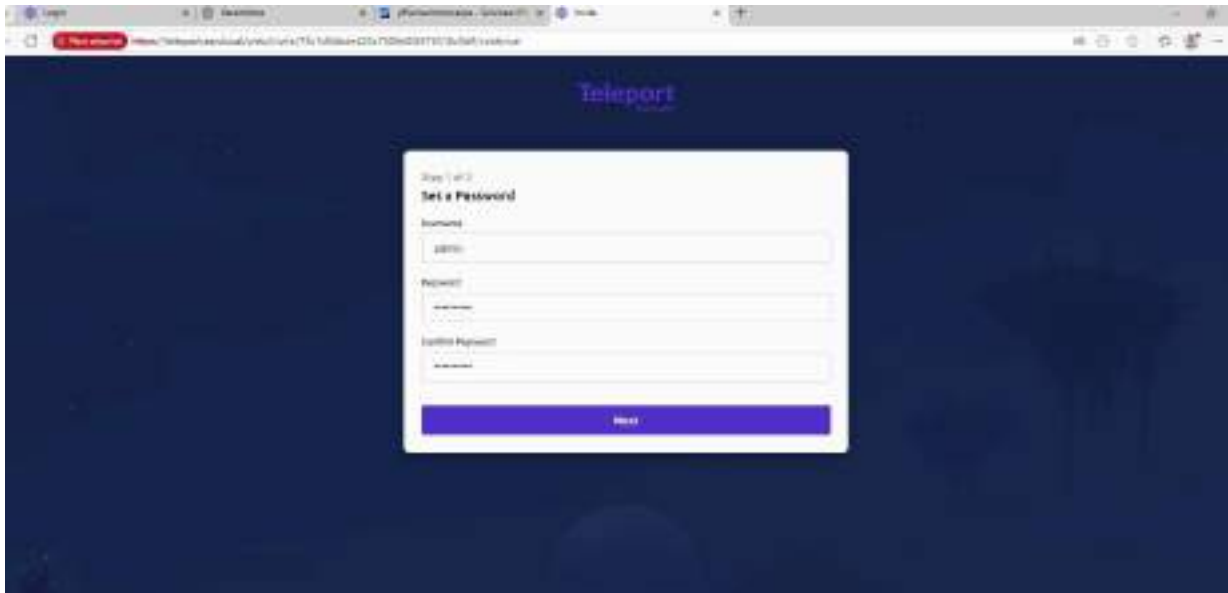
```
tctl users add admin \
  --roles=editor,access \
  --logins=root,debian
```

Cela fera un message comprenant un lien permettant de compléter la création du compte de l'utilisateur :



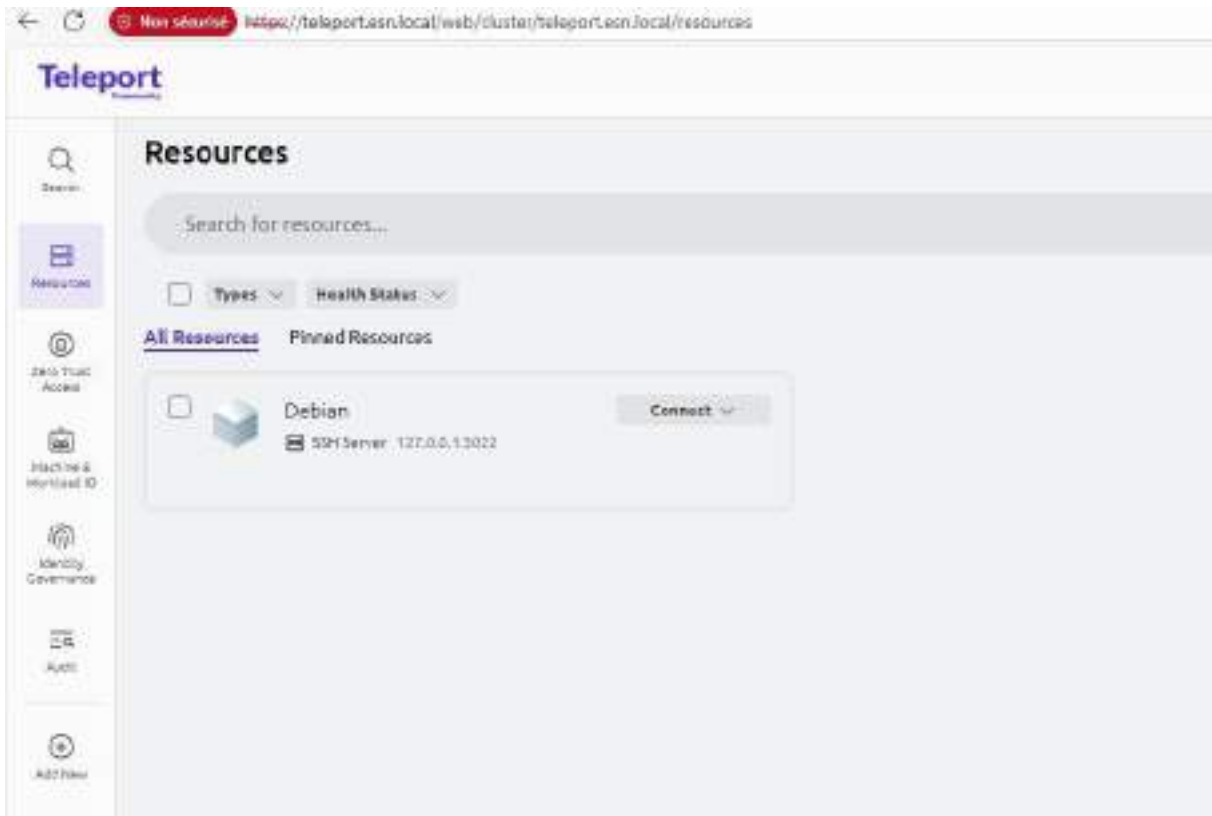
Le suivre et compléter :





Ajouter un moyen de MFA puis accéder à la page d'accueil de Teleport :

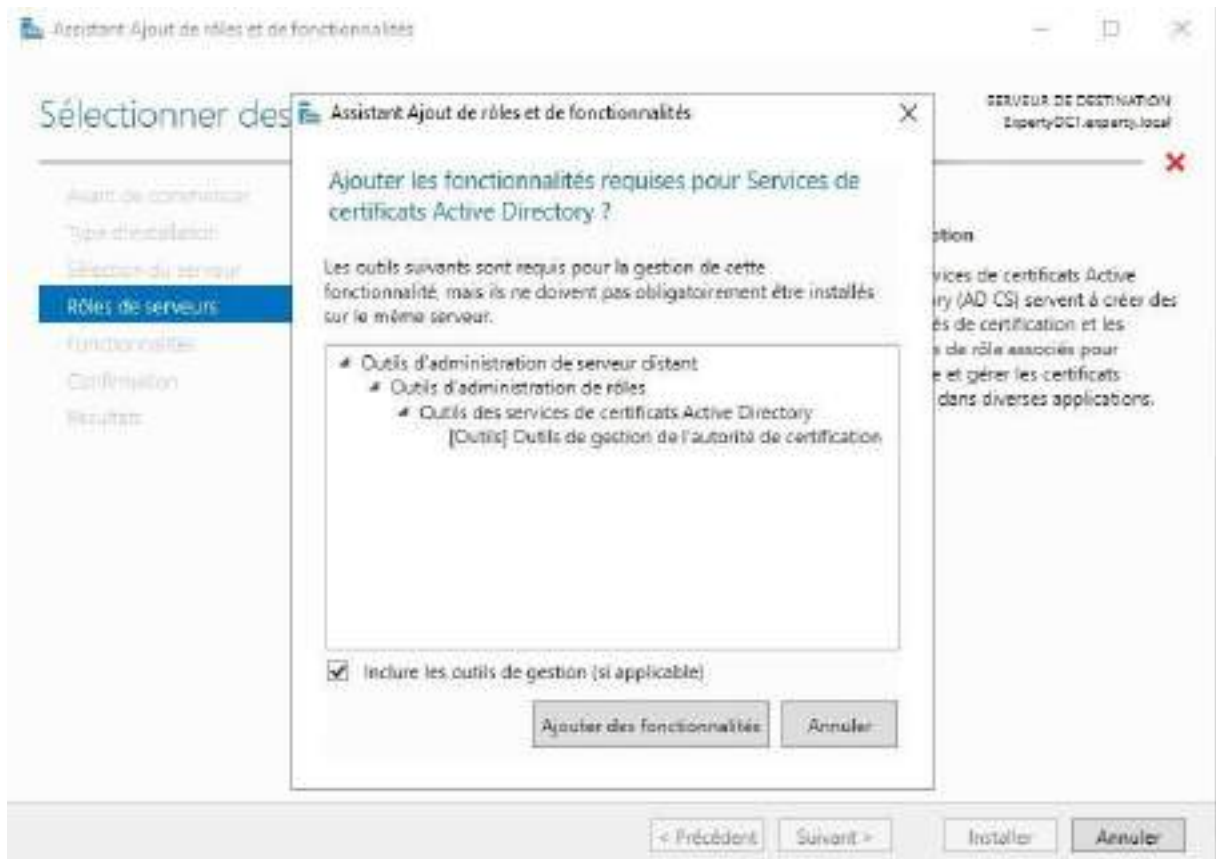




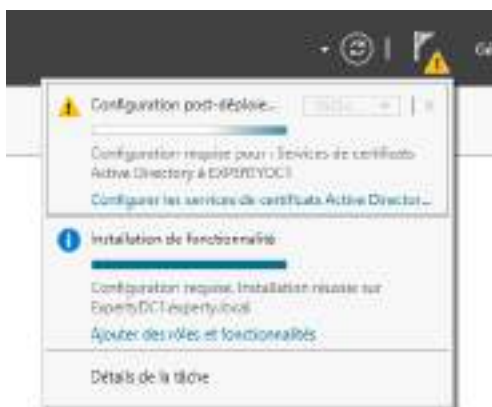
4. Ajouter le domaine experty

a. Configurations sur le DC

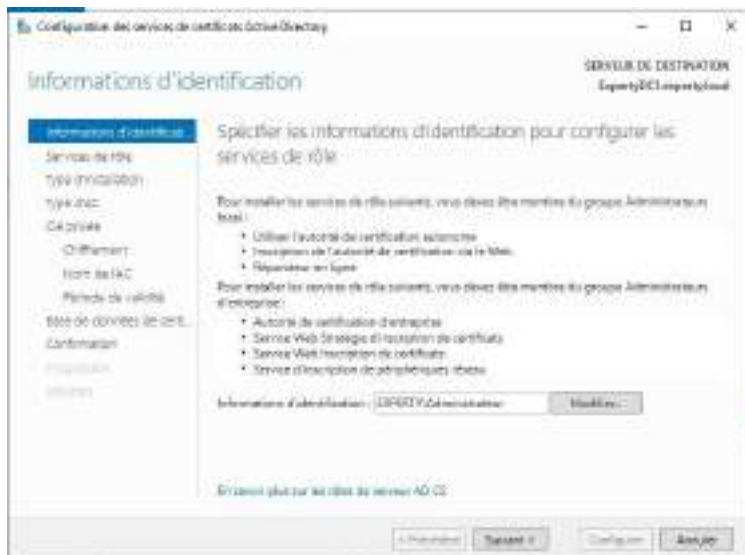
Aller sur le Domaine Controller, sur le gestionnaire de serveur, Gérer, Ajouter, et cliquer sur Services de certificats Active Directory :



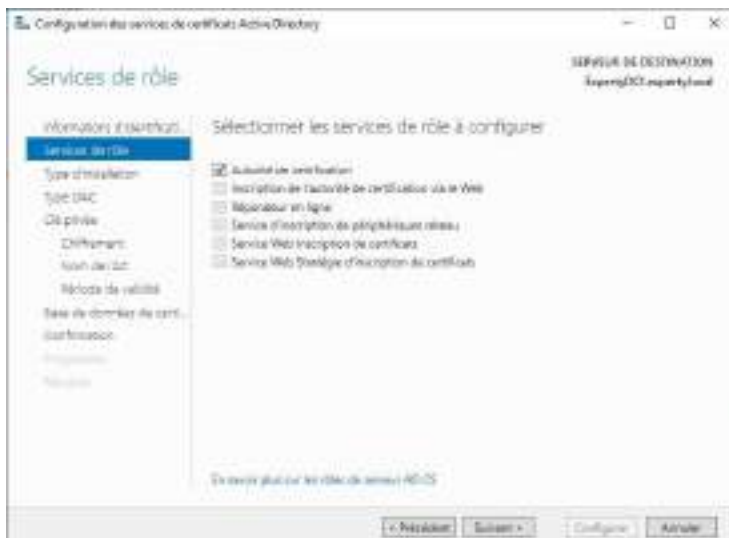
Terminer l'installateur, puis retourner sur le Gestionnaire de serveur, cliquer sur le drapeau puis Configurer les services de certificats Active Directory :



Le configurateur s'ouvre, valider la première page :



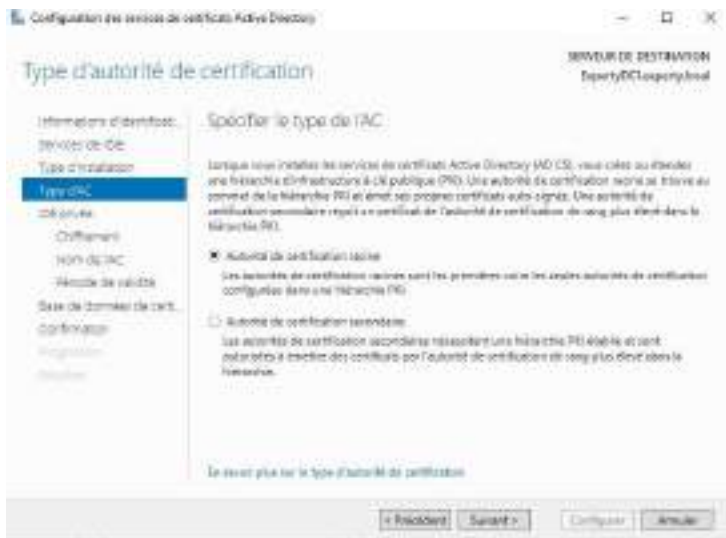
Cocher Autorité de certification :



Puis Autorité de certification autonome :



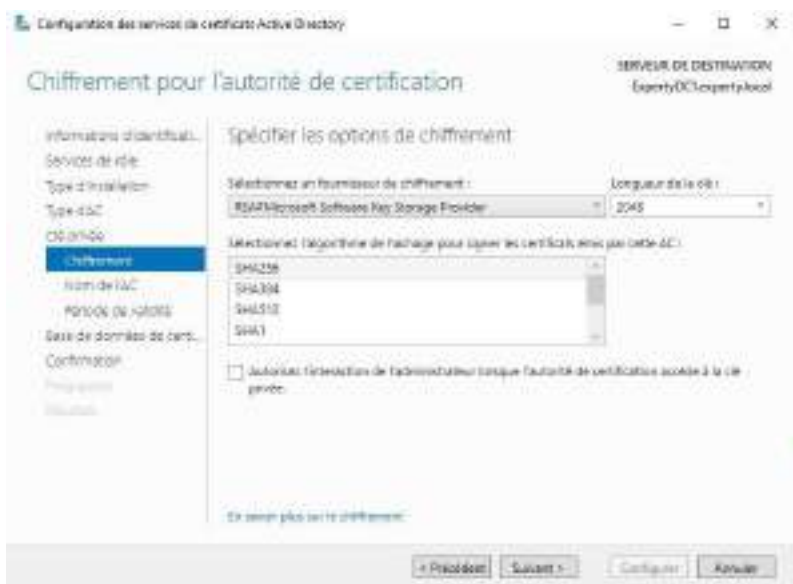
Ensuite autorité de certification racine :



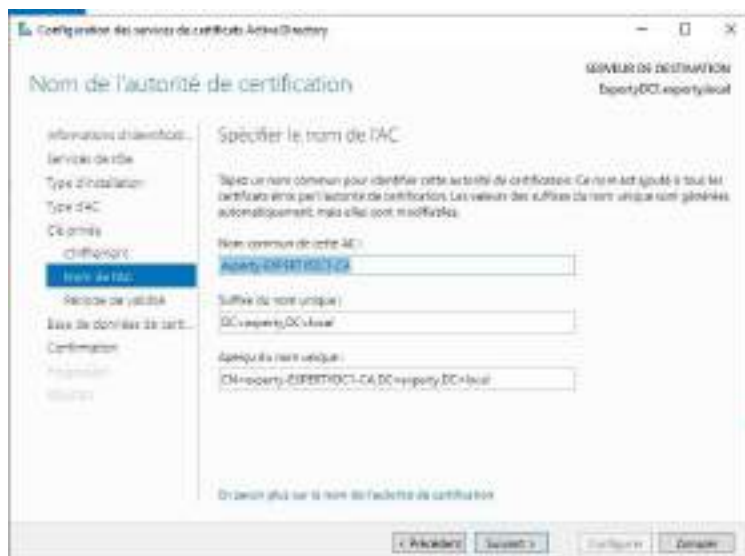
Laisser créer une clé privée :



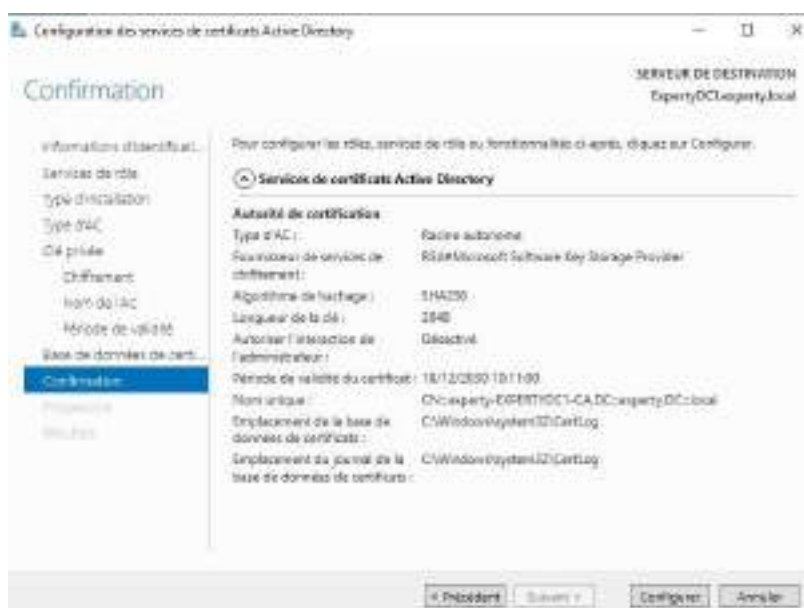
Laisser par défaut le chiffrement :



Donner un nom à l'autorité de certification (ou laisser celui par défaut) :

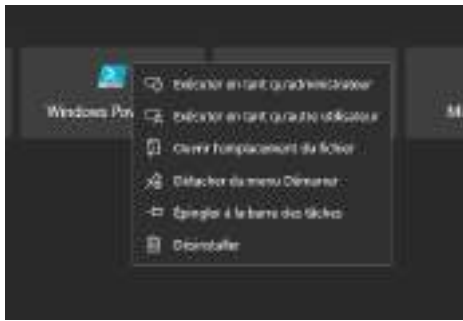


Laisser par défaut le reste puis valider la configuration en appuyant sur Configurer :

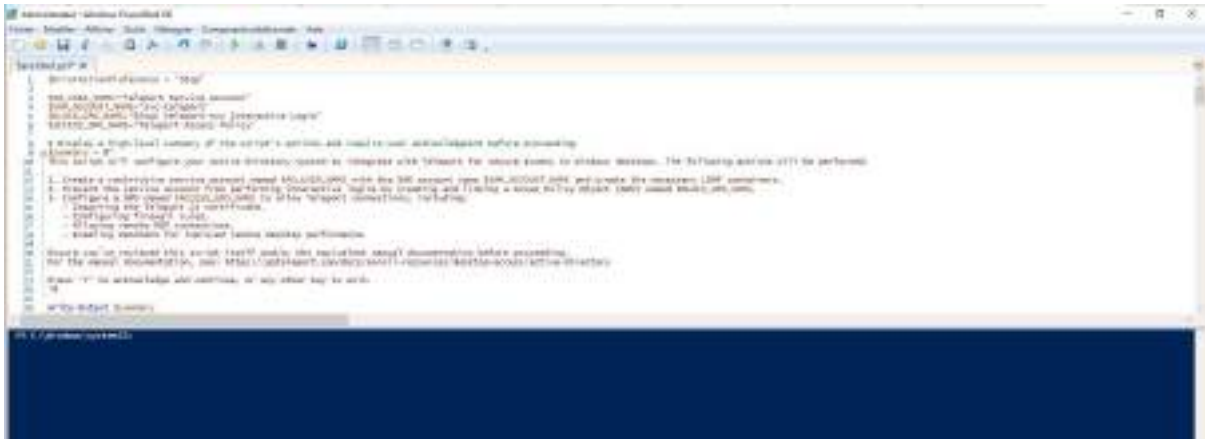


Puis retourner sur la debian hostant Teleport et faire cette commande :
`tctl desktop bootstrap > configure-ad.ps1`. Cela va créer un script qui crée un compte de service pour Teleport sur l'AD et crée deux GPO pour sécuriser la connexion. Faire `cat configure-ad.ps1` pour récupérer le script.

Aller sur le DC et exécuter le script en administrateur :



Coller le script et le lancer :



Une fois le script terminé, faire ceci :

```
$cert = New-SelfSignedCertificate `
  -DnsName "expertydc.experty.local", "experty.local", "10.10.3.10" `
  -CertStoreLocation "Cert:\LocalMachine\My" `
  -KeyUsage KeyEncipherment, DigitalSignature `
  -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.1)" `
  -NotAfter (Get-Date).AddYears(5)
```

Vérifier avec la commande `Get-ChildItem Cert:\LocalMachine\My` qu'il y a bien deux certificats, par exemple :

```
6E73F4F4DAD7A0CC3A06EDB8C943525FF730CFCF
CN=experty-EXPERTYDC-
CA, DC=experty, DC=local
F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9
CN=expertydc.experty.local
```

Puis faire :

```
$thumbprint = "F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9"
$cert = Get-Item "Cert:\LocalMachine\My\$thumbprint"
$store = New-Object
System.Security.Cryptography.X509Certificates.X509Store("Root","LocalMachine ")
```

```
$store.Open("ReadWrite")
$store.Add($cert)
$store.Close()
```

Et relancer le service NDS avec la commande Restart-Service "NTDS"

-Force. Ensuite exporter le script avec la commande :

```
Export-Certificate -Cert
"Cert:\LocalMachine\My\F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9"
-FilePath "C:\teleport-dc.cer" -Type CERT
```

Récupérer ce certificat pour le transférer sur la debian.

b. Configuration sur le serveur Teleport

Aller sur la debian hostant Teleport et créer un dossier pour les certificats : mkdir -p

/var/lib/teleport/certs. Y mettre le certificat créé auparavant.

```
root@debian:/var/lib/teleport# ls
backend cert_config.cnf certs configure-ad.ps1 debug.sock fullchain.pem host_uid log privkey.pem proc
root@debian:/var/lib/teleport# cd certs
root@debian:/var/lib/teleport/certs# ls
certificateExperty.cer
root@debian:/var/lib/teleport/certs#
```

Rajouter une section sur Windows Desktop dans le fichier de configuration de teleport : nano /etc/teleport .yaml (se référer à la section LDAP du script) :

```
windows_desktop_service:
  enabled: "yes"
  listen_addr:
    0.0.0.0:3028 ldap:
      addr: '10.10.3.10:636'
      domain: 'experty.local'
      username: 'EXPERTY\svc-teleport'
      sid: 'S-1-5-21-646546454-2773906599-3909544045-1604'
      server_name: 'ExpertyDC.experty.local'
      insecure_skip_verify: false
      der_ca_file: /var/lib/teleport/certs/teleport-ca.cer
```


c. Ajouter le rôle dédié à la connection aux windows du domaine Créer un fichier windows.yaml et y indiquer ceci :

```
kind: role
version: v5
metadata:
  name: windows
spec:
  allow:
    windows_desktop_labels:
      - "*"
    windows_desktop_logins: ["administrateur", "tesn"]
```

La ligne windows_desktop_logins correspond aux utilisateurs dans l'Active Directory.

Créer le rôle: `tctl create -f windows.yaml`

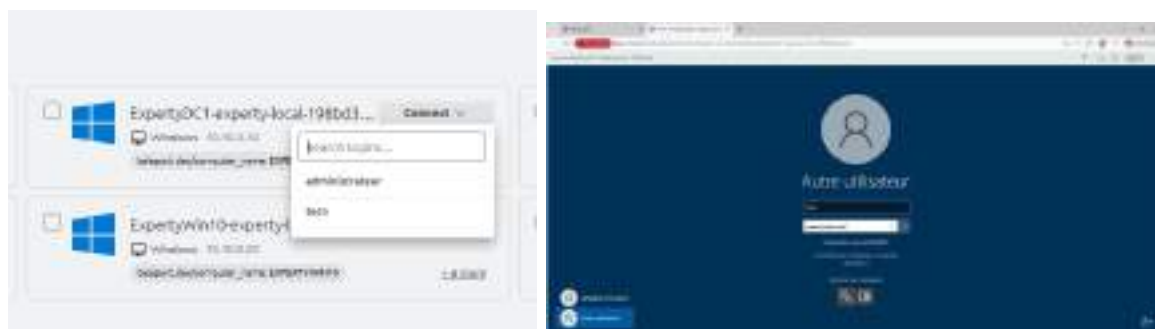
```
root@Debian:/etc# tctl create -f windows.yaml
2025-12-18T15:05:57.676+01:00 WARN Starting Teleport with a self-signed TLS certificate, this is not safe for production clusters.
attacks. config/configuration.go:1287
role "windows" has been created
```

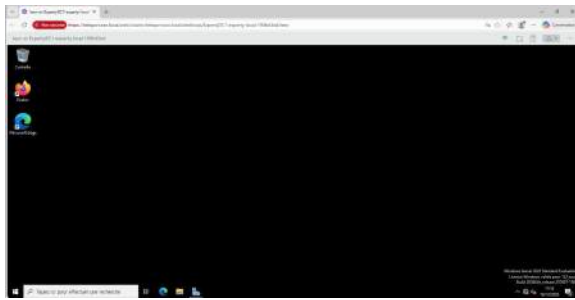
Créer le user pour le technicien et lui donner les bons rôles: `tctl users add tesn --roles=windows,access`

```
root@Debian:/etc# tctl users add tech --roles=windows,access
2025-12-18T15:07:07.202+01:00 WARN Starting Teleport with a self-signed TLS certificate, this is not safe for production clusters.
attacks. config/configuration.go:1287
User "tech" has been created but requires a password. Share this URL with the user to complete user setup. Link is valid for 1h:
https://teleport.esn.local:443/web/ovwite/kf9:769b27f99d11d91ba2692fb12a1
NOTE: Make sure teleport.esn.local:443 points at a teleport proxy which users can access.
root@Debian:/etc#
```

Comme pour l'administrateur, se connecter au lien et suivre l'assistant.

Puis se connecter sur `teleport.esn.local` avec les logins de `tesn` et vérifier qu'il est bien possible de se connecter à ExpertyDC1 :

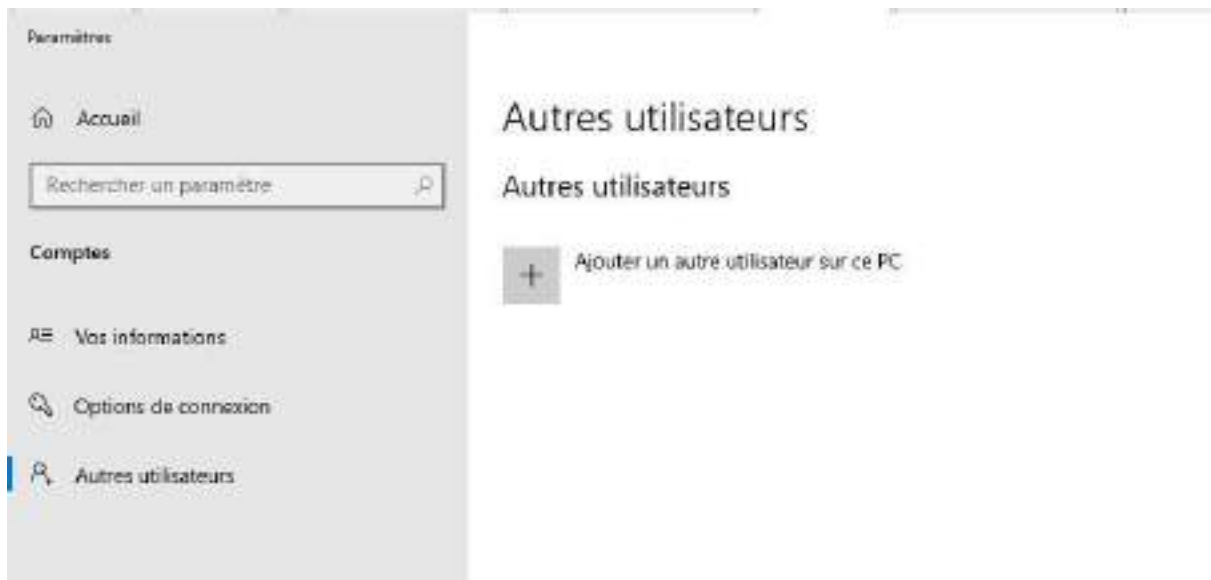




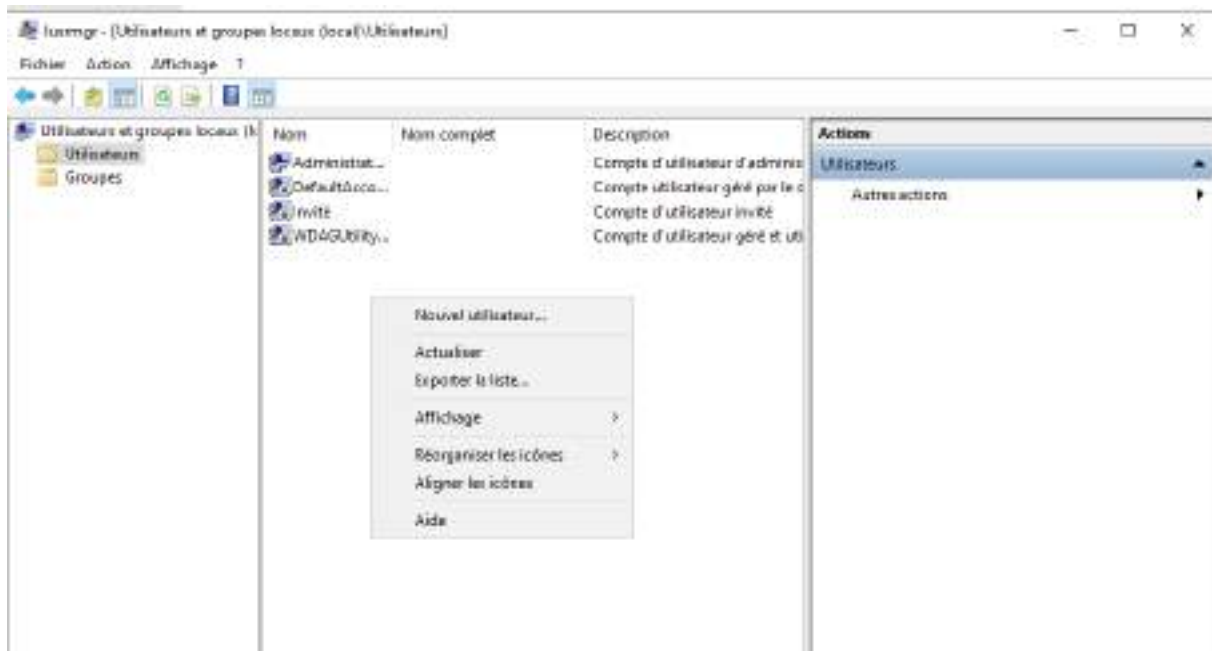
E. Veeam

Avoir un windows server 2022 avec une adresse IP statique.

Si le serveur n'est pas membre d'un domaine, aller dans Paramètres, Comptes, Autres utilisateurs et cliquer sur Ajouter un autre utilisateur sur ce PC pour créer un utilisateur dédié à Veeam :



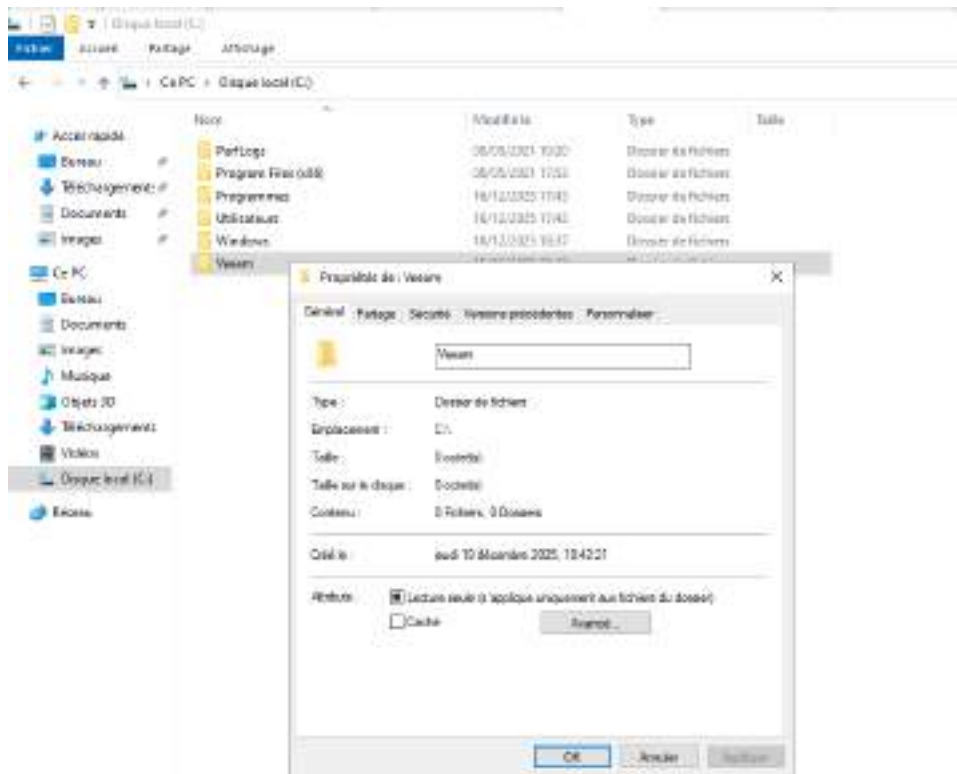
Faire un clic droit dans l'onglet du milieu, cliquer sur Nouvel utilisateur...



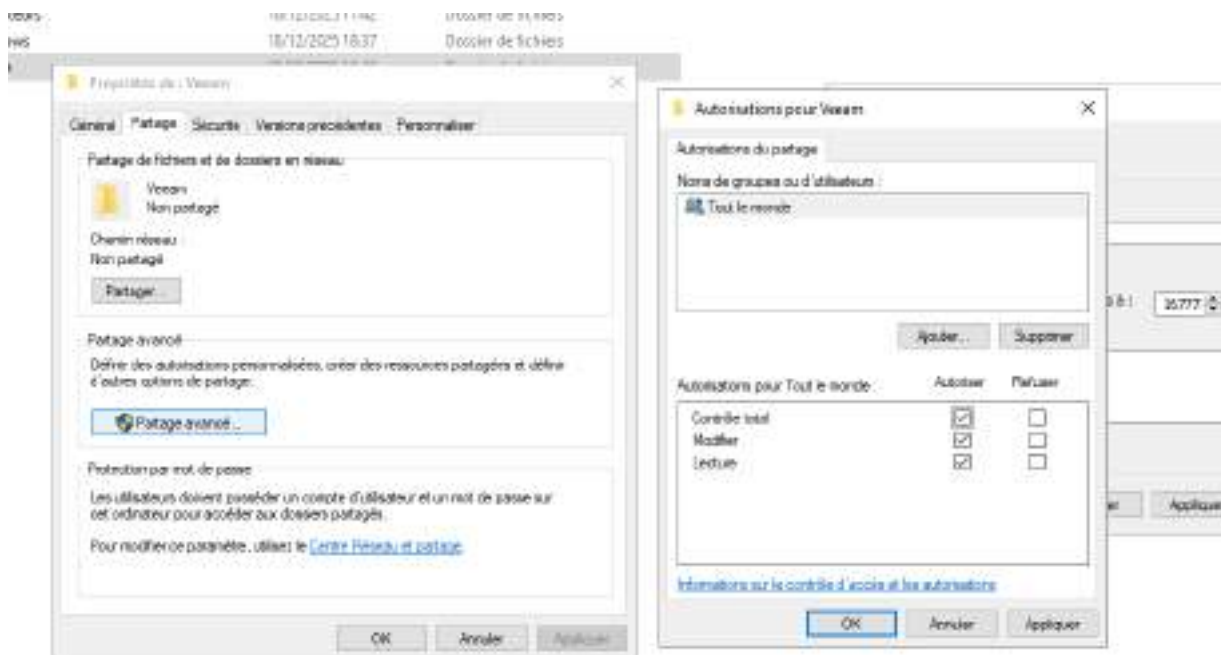
Renseigner les informations nécessaires puis décocher L'utilisateur doit changer le mot de passe et cocher L'utilisateur ne peut pas changer de mot de passe et Le mot de passe n'expire jamais. Cliquer sur Créer :



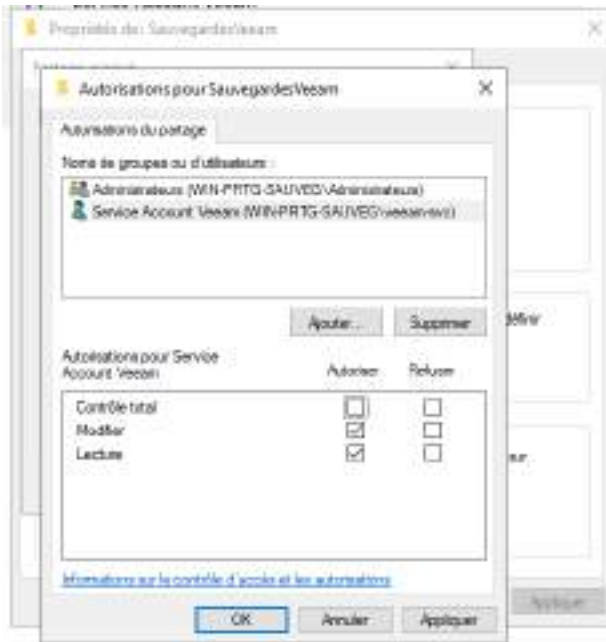
Créer un dossier pour les sauvegardes Veeam, puis faire un clic droit dessus et aller dans les propriétés :



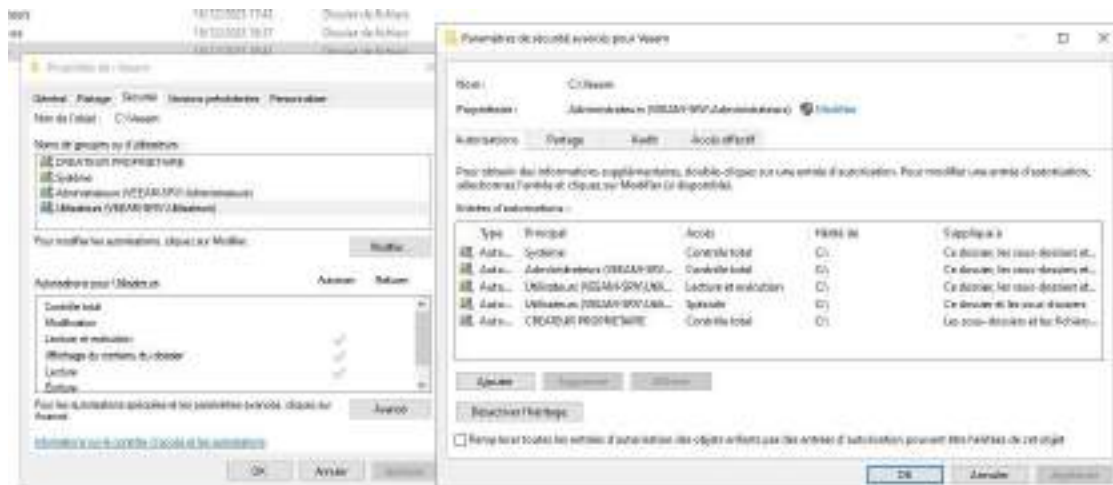
Aller dans Partage et cliquer sur Partage Avancé, supprimer Tout le monde :



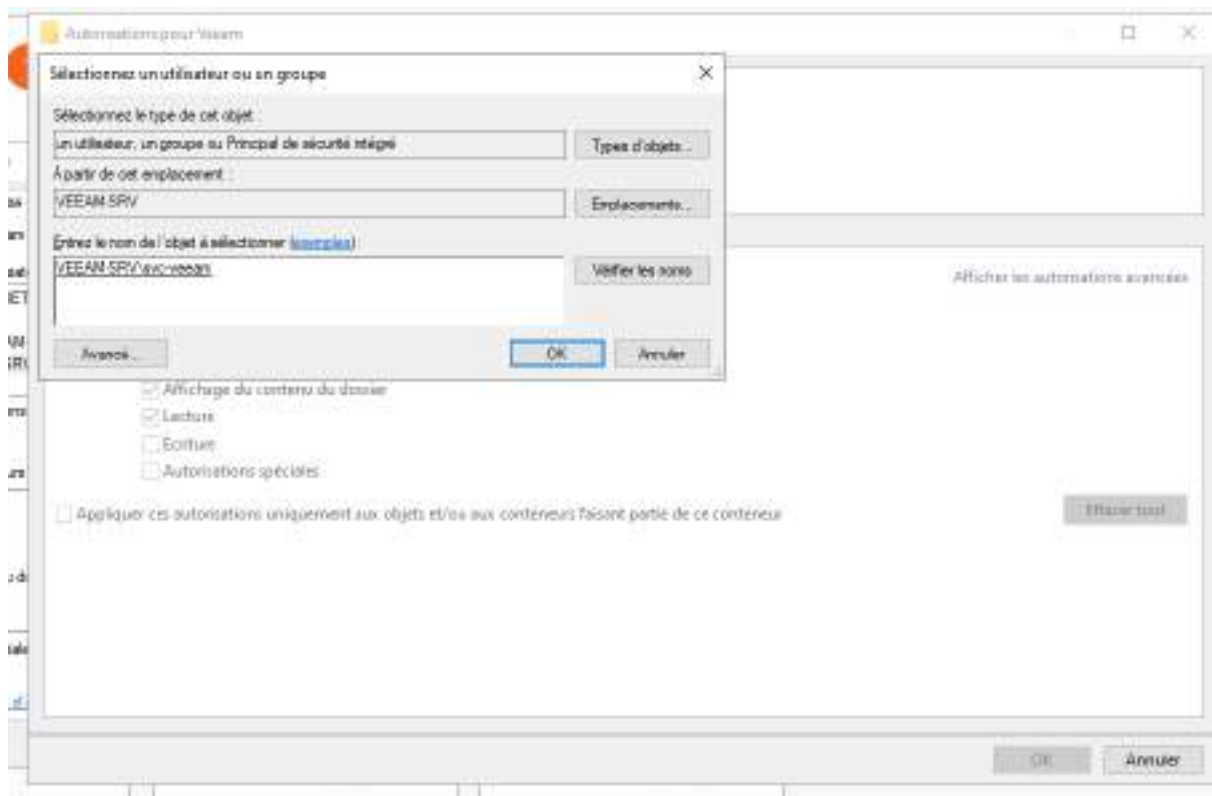
Cliquer sur Ajouter et ajouter le groupe Administrateurs et l'utilisateur dédié :



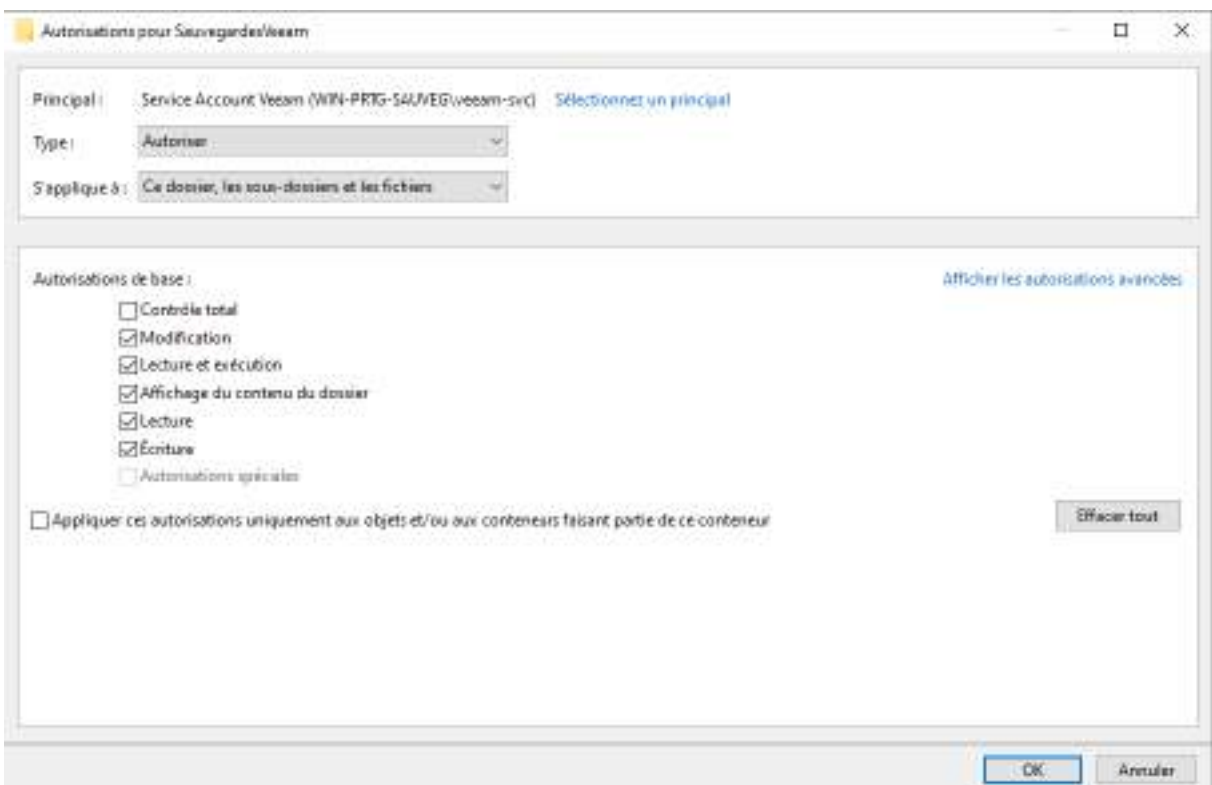
Aller dans l'onglet Sécurité et cliquer sur Avancé, cliquer sur Désactiver l'héritage, supprimer Utilisateurs puis sur cliquer sur Ajouter :



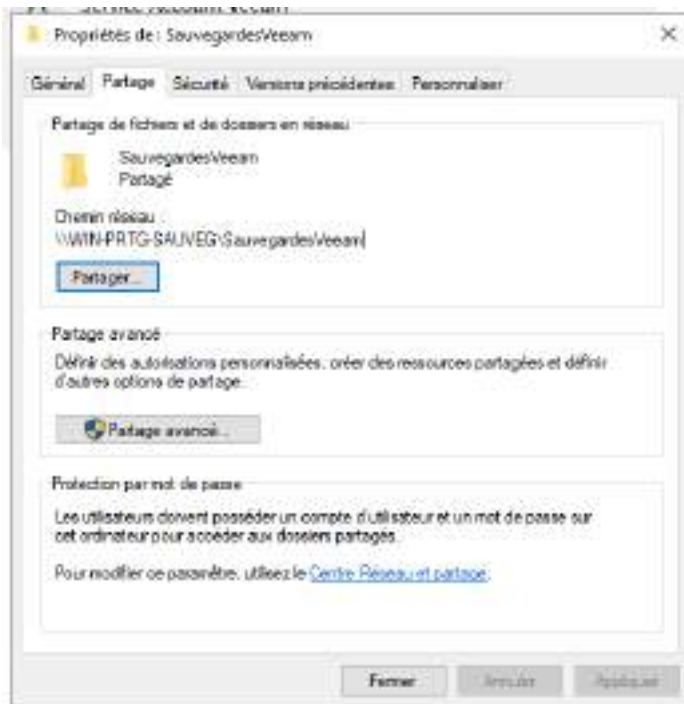
Cliquer sur Sélectionner un principal, renseigner le nom de l'utilisateur veeam :



Puis lui donner les autorisations suivantes :



Valider le tout et retourner dans l'onglet Partage pour noter le chemin réseau :



Aller sur le site de Veeam et télécharger le paquet pour debian :
<https://www.veeam.com/products/physical/linux-backup-recovery-download.html>

Le mettre sur la vm linux que l'on souhaite sauvegarder, ici la debian GestSup. Puis aller dans le répertoire où se trouve le paquet et faire `dpkg -i ./veeam-release* && apt-get update`

```

root@debian:/home/debian# dpkg -i ./veeam-release* && apt-get update
Sélection du paquet veeam-release-deb précédemment désélectionné.
Clarture de la base de données... 37224 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ./veeam-release-deb_11.0.1_amd64.deb ...
Dépaquetage de veeam-release-deb (11.0.1) ...
Paramétrage de veeam-release-deb (11.0.1) ...
Réception de 1) http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Attente 2) http://deb.debian.org/debian bookworm InRelease
Réception de 3) http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Réception de 4) https://repository.veeam.com/back-up/linux/agent-13/deb/debian/public stable InRelease [6 010 B]
Réception de 5) http://security.debian.org/debian-security bookworm-security/main Sources [196 kB]
Réception de 6) http://security.debian.org/debian-security bookworm-security/main amd64 Packages [296 kB]
Réception de 7) https://repository.veeam.com/back-up/linux/agent-13/deb/debian/public stable/veeam amd64 Packages [2 183 B]
597 ko réceptionnés en 0s (1 941 ko/s)
Lecture des listes de paquets... Fait
root@debian:/home/debian#

```

Ensuite faire `apt-get install blksnap veeam` :

```
Building initial module for 6.1.0-41-amd64
Done.

vmevblknrap.ko:
Running module version sanity check.
  Original module
  - No original module exists within this kernel
  - Installation
  - Installing to /lib/modules/6.1.0-41-amd64/updates/dkms/

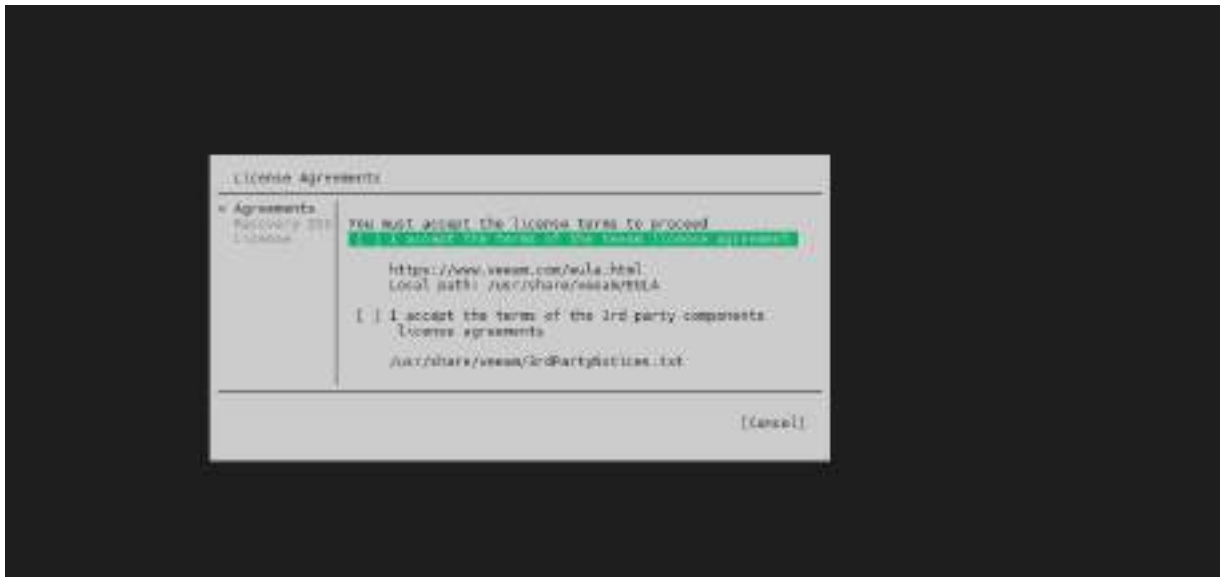
bdevfilter.ko:
Running module version sanity check.
  Original module
  - No original module exists within this kernel
  - Installation
  - Installing to /lib/modules/6.1.0-41-amd64/updates/dkms/

depmod....
Paramétrage de libdevmtd0.03:amd64 (2.02.16-2) ...
Paramétrage de dmccvmd (2:1.02.181-2) ...
Created symlink /etc/systemd/system/sockets.target.wants/dm-event.socket → /lib/systemd/system/dm-event.socket.
dm-event.service is a disabled or a static unit, not starting it.
Paramétrage de lvm2 (2.02.18-2) ...
Created symlink /etc/systemd/system/systemd.target.wants/blk-availability.service → /lib/systemd/system/blk-availability.service.
Created symlink /etc/systemd/system/systemd.target.wants/lvm2-monitor.service → /lib/systemd/system/lvm2-monitor.service.
Created symlink /etc/systemd/system/systemd.target.wants/lvm2-lvmpolld.socket → /lib/systemd/system/lvm2-lvmpolld.socket.
Paramétrage de veeam-lib (1:2.1.04) ...
Paramétrage de veeam (13.0.1.04) ...
Enable veeam.service
Synchronizing state of veeam.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable veeam.service
Created symlink /etc/systemd/system/multi-user.target.wants/veeam.service → /lib/systemd/system/veeam.service.
Try to stop veeam.service
Start veeam.service
Traitement des actions différées (= triggers => pour man-db (2.11.2-2) ...
Traitement des actions différées (= triggers => pour initramfs-tools (1:142+deb12u1) ...
update-initramfs: Generating /boot/initrd.img-6.1.0-41-amd64
Traitement des actions différées (= triggers => pour libc-bin (2.36-9+deb12u12) ...
```

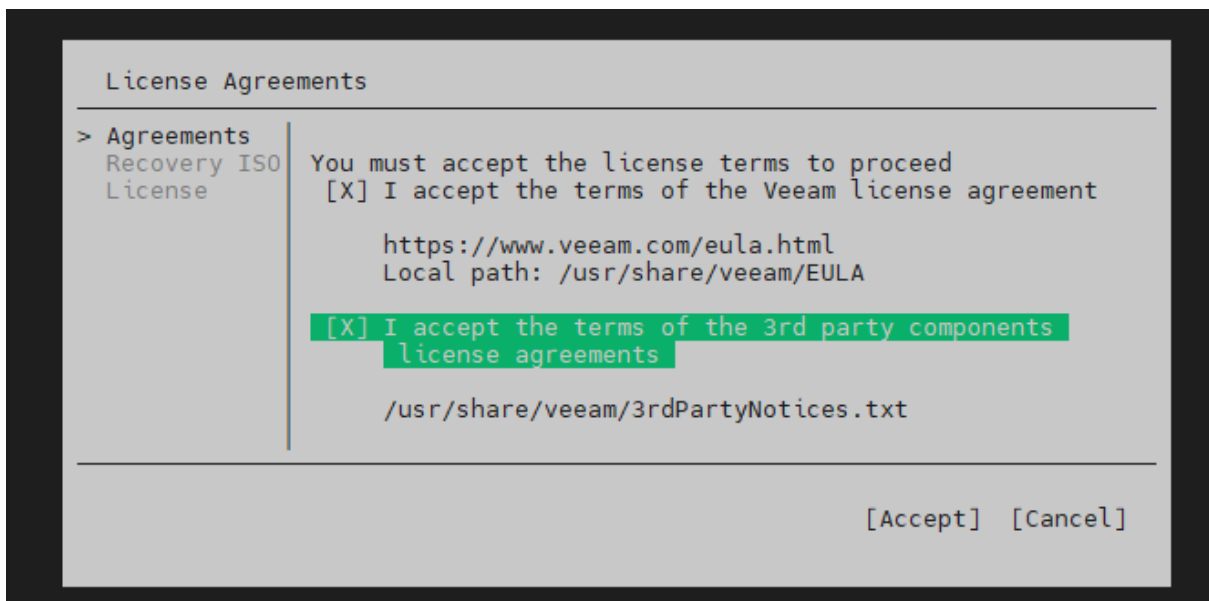
Faire apt-get install cifs-utils:

```
root@debian:/home/roesch# apt-get install cifs-utils
Lecture des listes de paquets... fait
Construction de l'arbre des dépendances... fait
Lecture des informations d'état... fait
Les paquets supplémentaires suivants seront installés :
  libacl1 libblkid1 libbrotli1
Paquets suggérés :
  acl libacl1-dev
Les MOULES suivants seront installés :
  cifs-utils libacl1 libblkid1 libbrotli1
0 octet à télécharger, 0 octet à télécharger, 0 octet à télécharger et 0 octet mis à jour.
1 octet attendu de disque, 22 ko dans les archives.
Après cette opération, 12 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [Y/n] y
Réception de 11 https://deb.debian.org/debian/bookworm/main amd64 libacl1:amd64 2.3.1-1 [25,6 kB]
Réception de 12 https://deb.debian.org/debian/bookworm/main amd64 libblkid1:amd64 2.4.0-1 [129,2ko]
Réception de 13 https://deb.debian.org/debian/bookworm/main amd64 cifs-utils:amd64 2:2.4.1-1 [185,9 kB]
Réception de 14 https://deb.debian.org/debian/bookworm/main amd64 libacl1:amd64 2.3.1-2 [24,5 kB]
229 ko réceptionnés sur 12 ko (84%)
Sélection de paquet libacl1:amd64 précédemment désélectionné.
Lecture de la base de données... 6066 fichiers et répertoires déjà installés.1
Préparation du dossier de paquet libacl1:amd64 (2.3.1-2) ...
Dépaquetage de libacl1:amd64 (2.3.1-2) ...
Sélection de paquet libblkid1:amd64 précédemment désélectionné.
Préparation du dossier de paquet libblkid1:amd64 (2.4.0-1) ...
Dépaquetage de libblkid1:amd64 (2.4.0-1) ...
Sélection de paquet cifs-utils:amd64 précédemment désélectionné.
Préparation du dossier de paquet cifs-utils:amd64 (2:2.4.1-1) ...
Dépaquetage de cifs-utils:amd64 (2:2.4.1-1) ...
Sélection de paquet libacl1:amd64 précédemment désélectionné.
Préparation du dossier de paquet libacl1:amd64 (2.3.1-2) ...
Dépaquetage de libacl1:amd64 (2.3.1-2) ...
Paramétrage de libacl1:amd64 (2.3.1-2) ...
Paramétrage de libblkid1:amd64 (2.4.0-1) ...
Paramétrage de cifs-utils (2:2.4.1-1) ...
update-initramfs: Utilisation de /usr/lib/initramfs-tools/initramfs-tools/cifs-utils/initramfs-tools/cifs-utils en mode automatique
Traitement des actions différées (= triggers => pour libc-bin (2.36-9+deb12u12) ...
Traitement des actions différées (= triggers => pour man-db (2.11.2-2) ...
root@debian:/home/roesch#
```

Et lancer Veeam en faisant simplement la commande veeam :



Faire espace pour cocher puis aller sur Accept

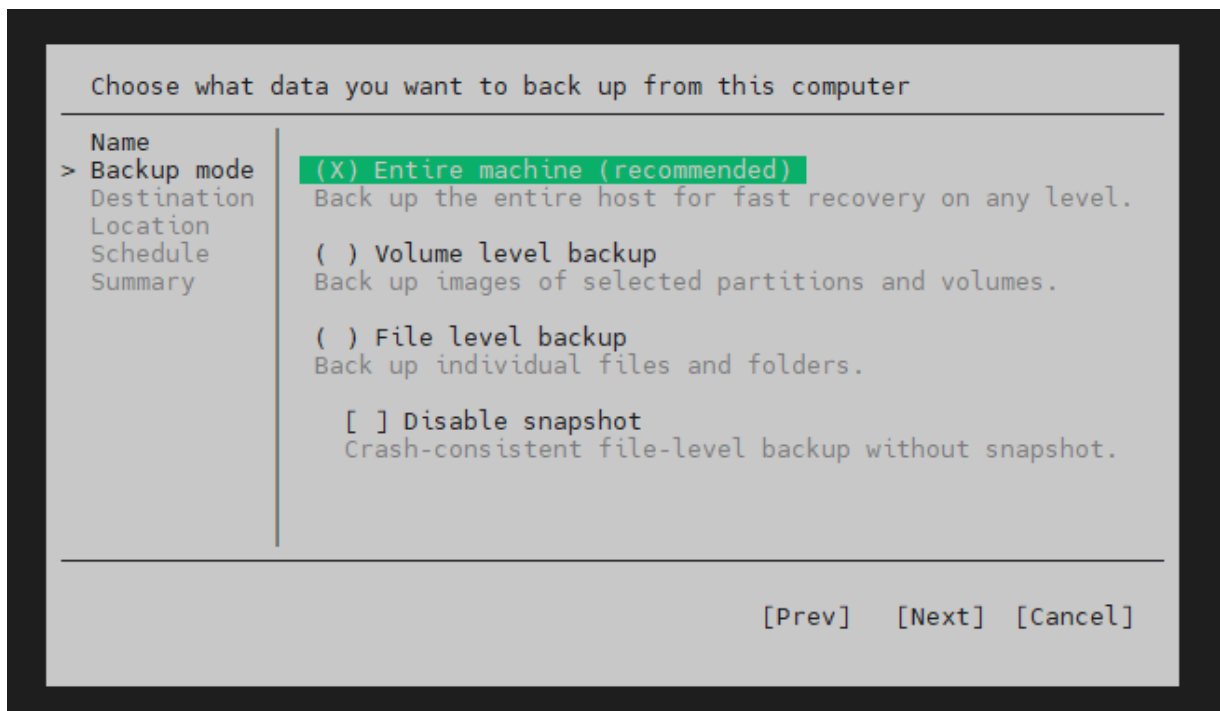


Suivre l'installateur puis faire C pour configurer la sauvegarde :

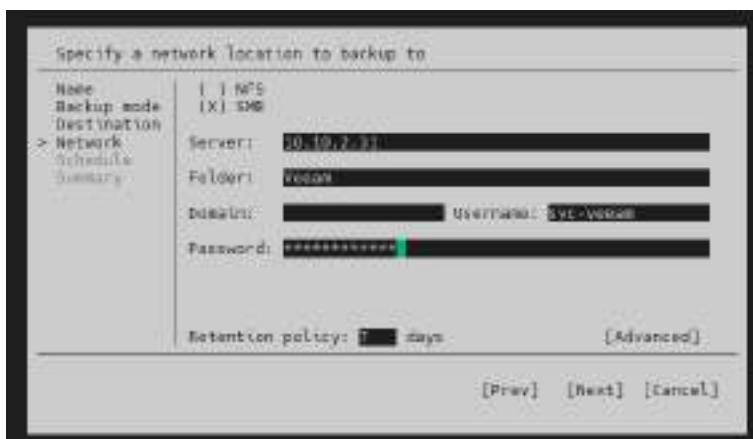


La nommer :

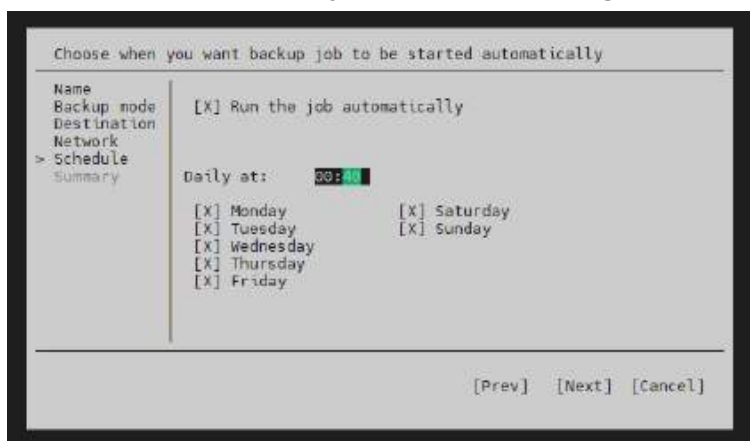




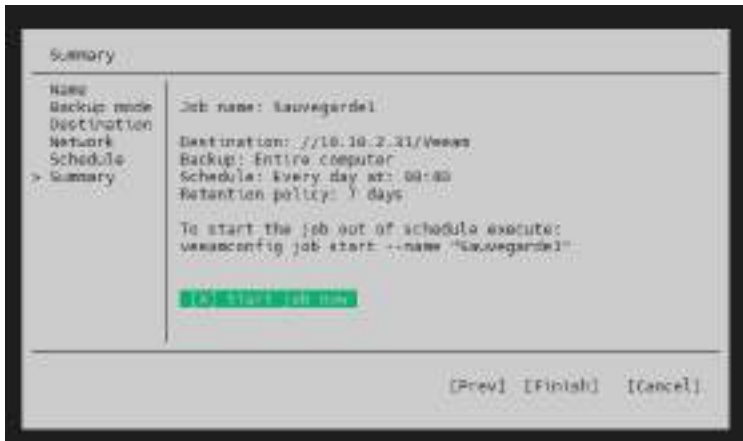
En destination choisir Shared folder puis sélectionner SMB et remplir avec les informations du serveur :



Choisir l'heure et les jours où la sauvegarde est faite :



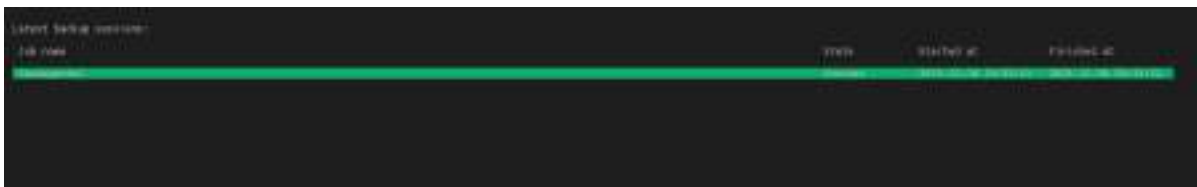
Cocher Start job now et valider:



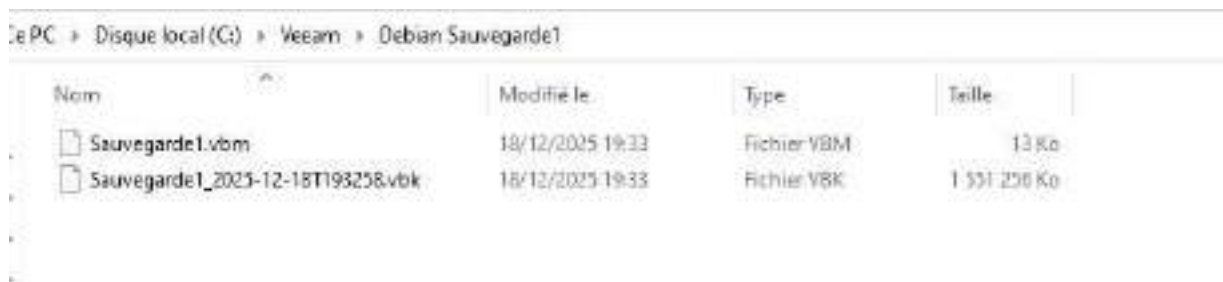
La sauvegarde commence alors:



Attendre qu'elle soit complétée:



Un dossier contenant la sauvegarde apparaît alors sur le serveur windows :



Il est possible de lancer une sauvegarde manuellement en allant sur Veeam, faire S et sélectionner la sauvegarde à réaliser :

