

Projet Pro. n°4



LIVRABLE 2



UIMM

LA FABRIQUE
DE L'AVENIR

Procédure du projet AP4

Contexte Du Projet

Le projet consiste à mettre en place une infrastructure résiliente pour les Centres Opérationnels Départementaux (COD) afin de garantir une continuité de service en toutes circonstances. Il inclut la mise en œuvre d'une connectivité sécurisée, d'outils de gestion des interventions (eBrigade) et de solutions de supervision pour assurer la protection des données et l'efficacité des opérations.

Objectif

L'objectif de ce document est de recenser l'ensemble des procédures mises en œuvre dans le cadre du projet. Il sert de référence centralisée permettant de regrouper toutes les étapes techniques, organisationnelles et méthodologiques suivies durant la réalisation du projet.

Sommaire

Sommaire	2
Contrôleurs de domaines.....	3
Prérequis.....	3
Installation de l'ADDS.....	3
Redondance de l'AD	9
Création d'unités organisationnelles	15
Création d'un utilisateur	16
Création de groupe de sécurité	17
Intégration de l'utilisateur dans un groupe	18
DHCP	20
Prérequis.....	20
Configuration du DHCP	20
Mise en place de la redondance du DHCP	22
Mise en place du Pare-Feu et du VPN	25
Prérequis.....	25
Installation Pfsense	25
Création des règles du Pare-Feu	32
Mise en place du VPN	35
Mise en place de la redondance CARP et IP virtuelles sur pfSense	53
Configuration DMZ (règle plus installation eBrigade)	62
Procédure Hmailserver	68
Procédure Zabbix	87
Conclusion du livrable	112

Contrôleurs de domaines

Les contrôleurs de domaine jouent un rôle clé dans la gestion des ressources réseau, en assurant l'authentification centralisée, la gestion des comptes utilisateurs et l'application des stratégies de groupe.

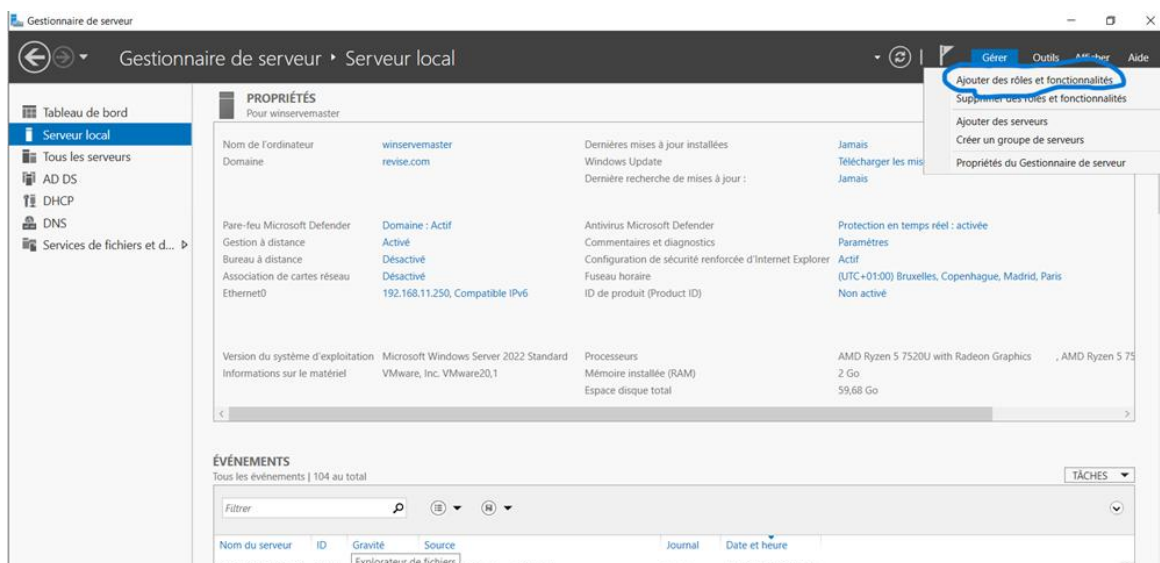
Prérequis

Ressources matériels minimum :

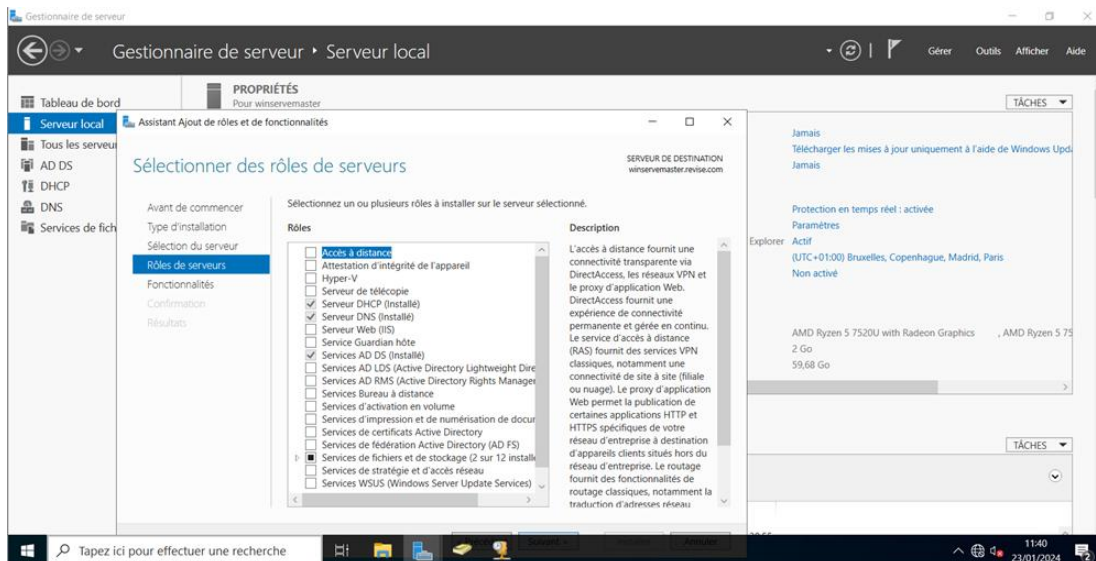
- Processeur : 2vCPU
- RAM : 2 Go
- Stockage : 1 disque de 60 Go pour l'OS
1 disque de 60 Go si le serveur va stocker des données

Installation de l'ADDS

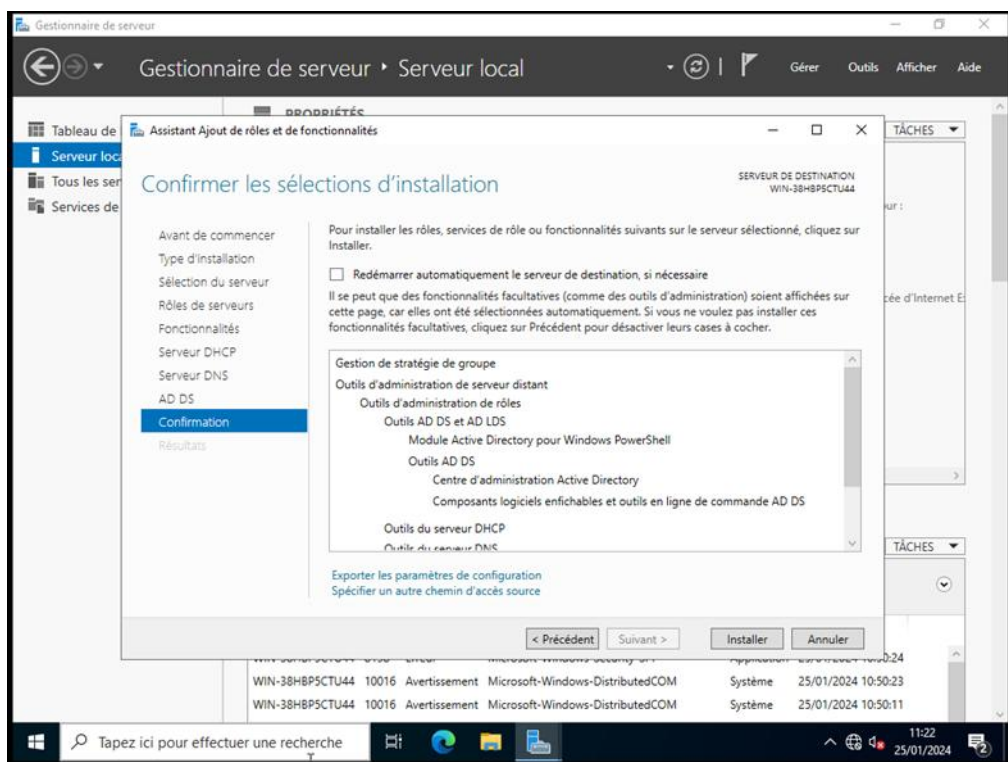
On va sur le gestionnaire de serveur et on clique « Gérer » et « ajouter rôles et fonctionnalités » :



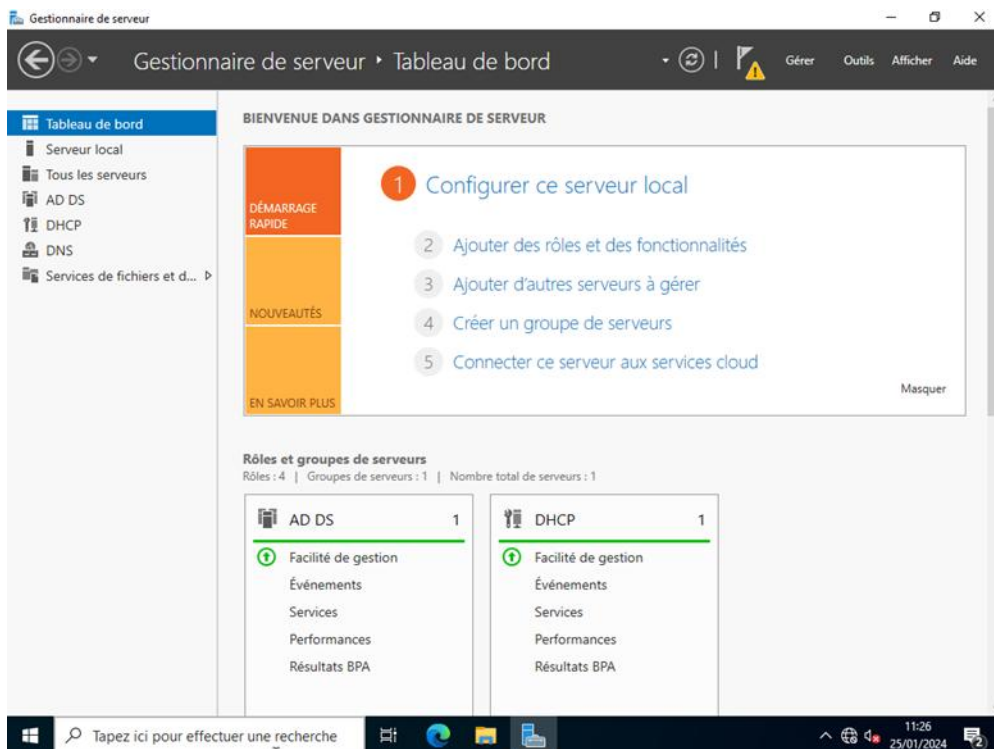
On fait suivant jusqu'à arriver sur cette fenêtre. On coche « Serveur AD DS » quand la fenêtre s'ouvre, cliquer sure « ajouter des fonctionnalités ». On ne décoche rien et suivant.



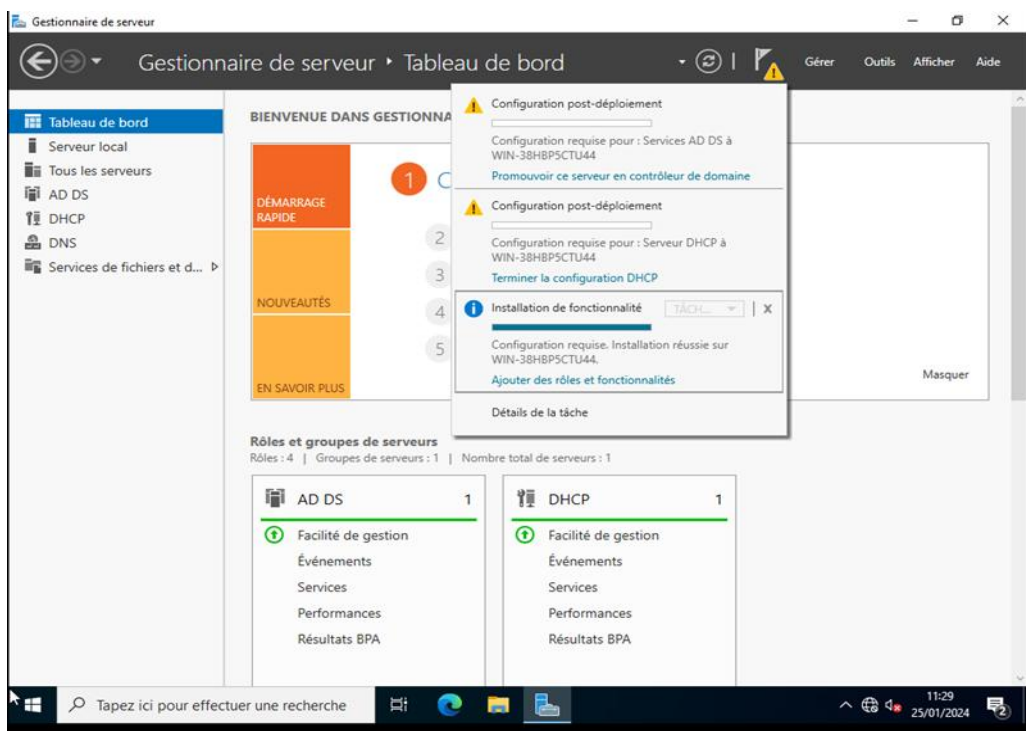
On clique sur Suivant jusqu'à arriver sure cette page. Là on clique sur installez et on attend :



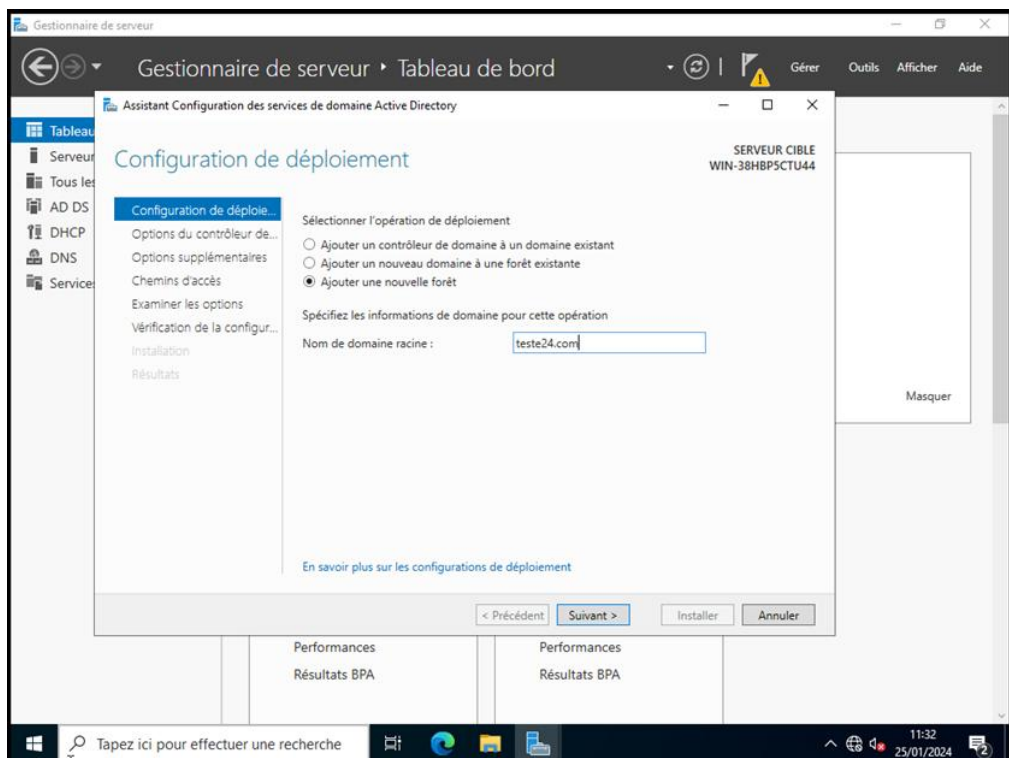
Une fois que tout est installé on clique sur « fermer » et un triangle jaune aura apparu sous le drapeau en haut à droite :



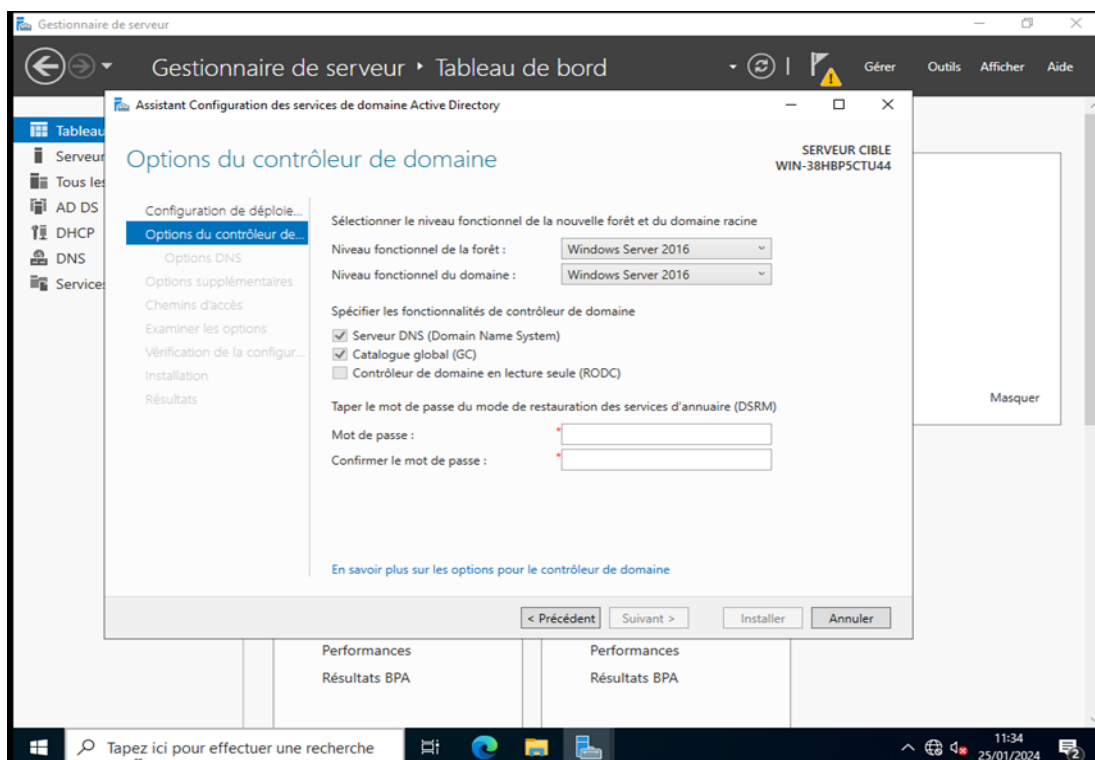
On clique dessus pour commencer à configurer l'AD DS. Une fois le menu ouvert on clique sur les promouvoir ce serveur en contrôleur de domaine :



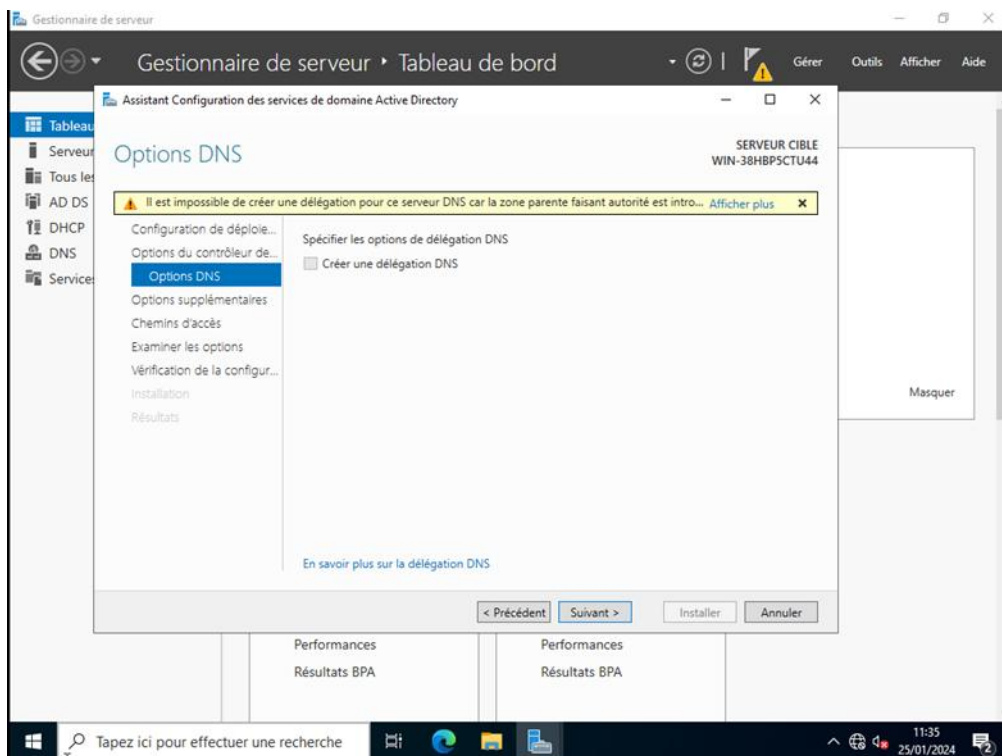
On commence par l'ADDS. On coche « crée une nouvelle forêt » et on lui donne un nom en point. Ici j'ai choisi « test24.com » pour l'exemple puis suivant :



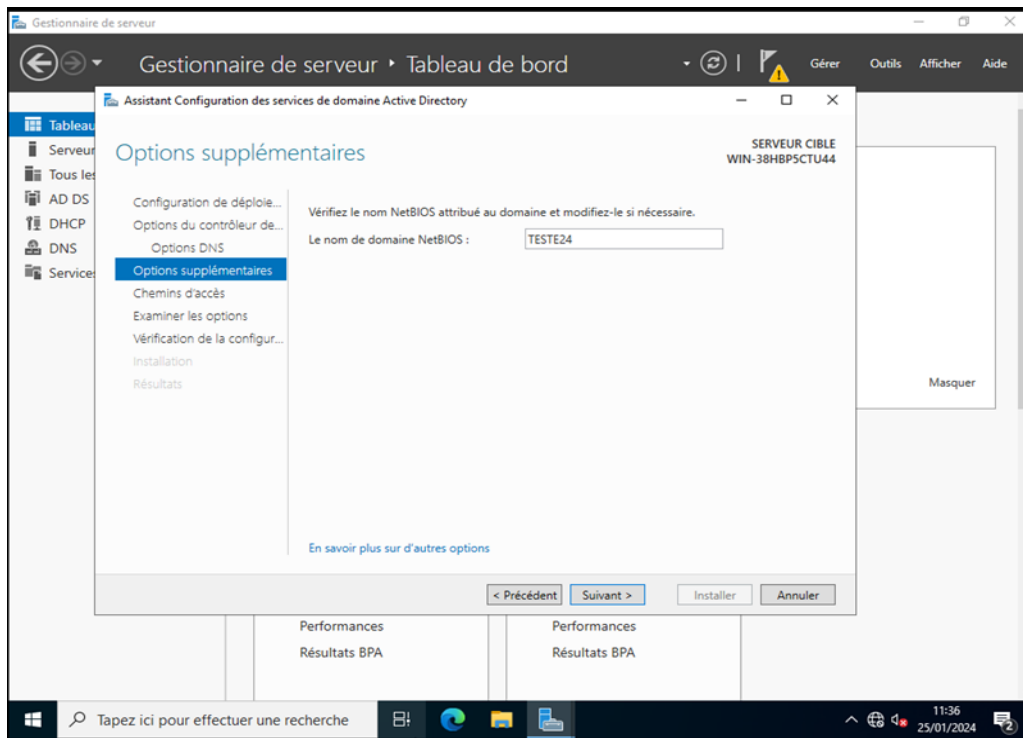
Ici on ne touche uniquement le mot de passe. Une fois renseigné on clique sur suivant :



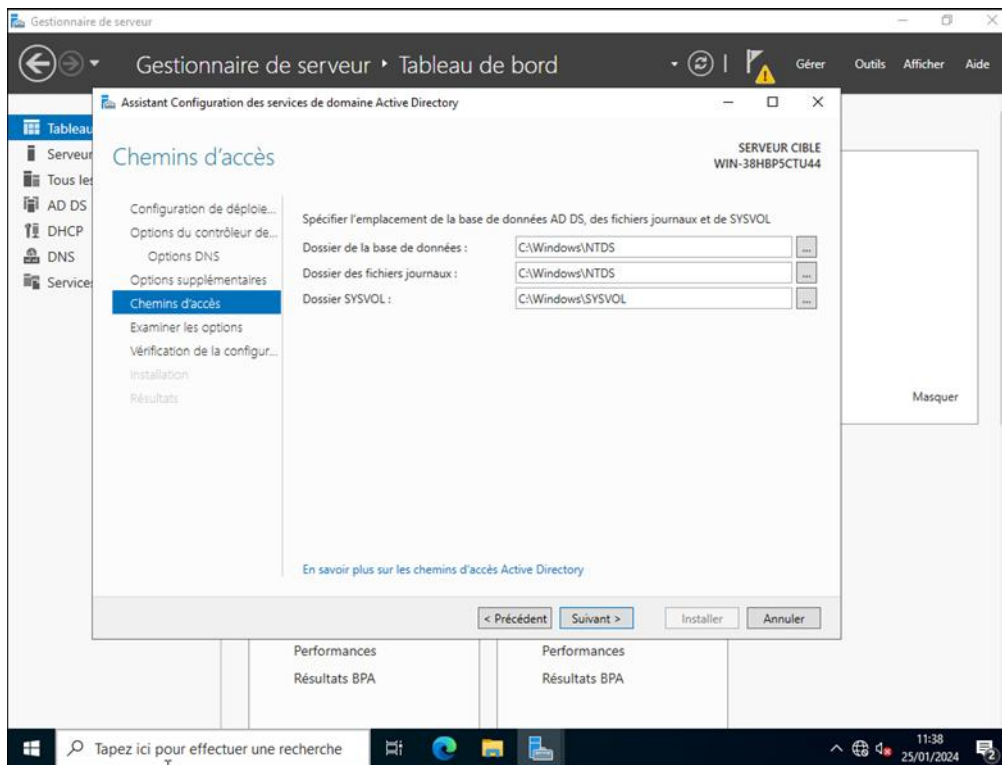
Rien à toucher ici, suivant :



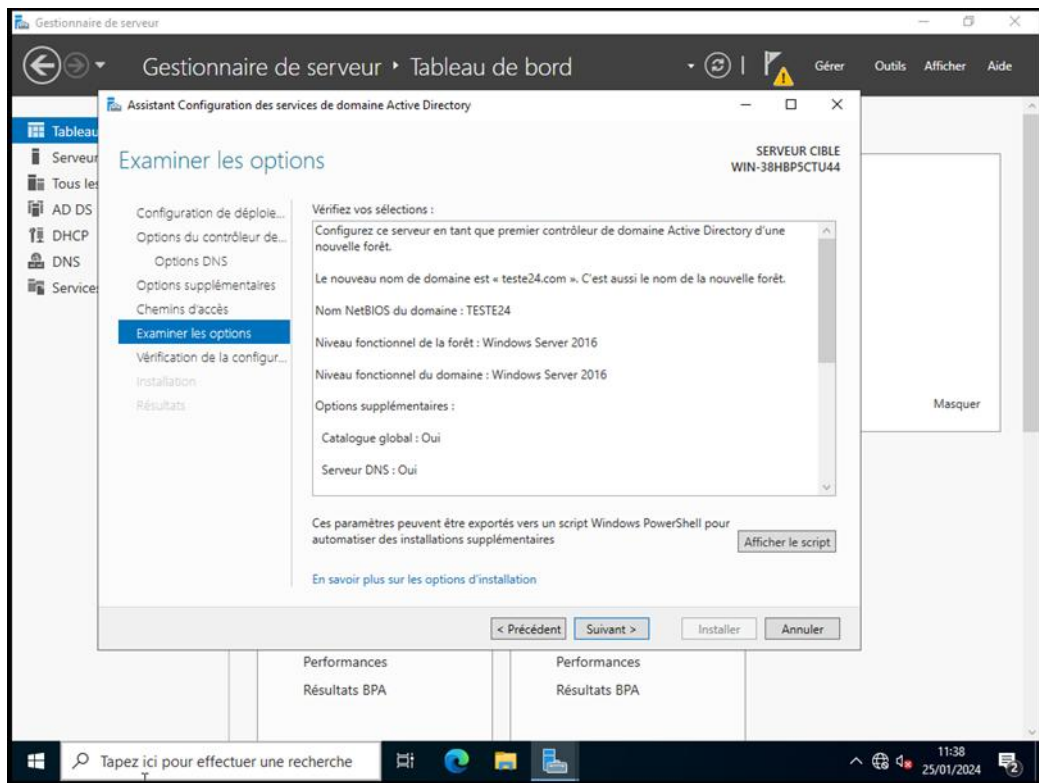
Important, ici Windows va nous « générer » notre nom de domaine, ne pas l'oublier. On fait Suivant :



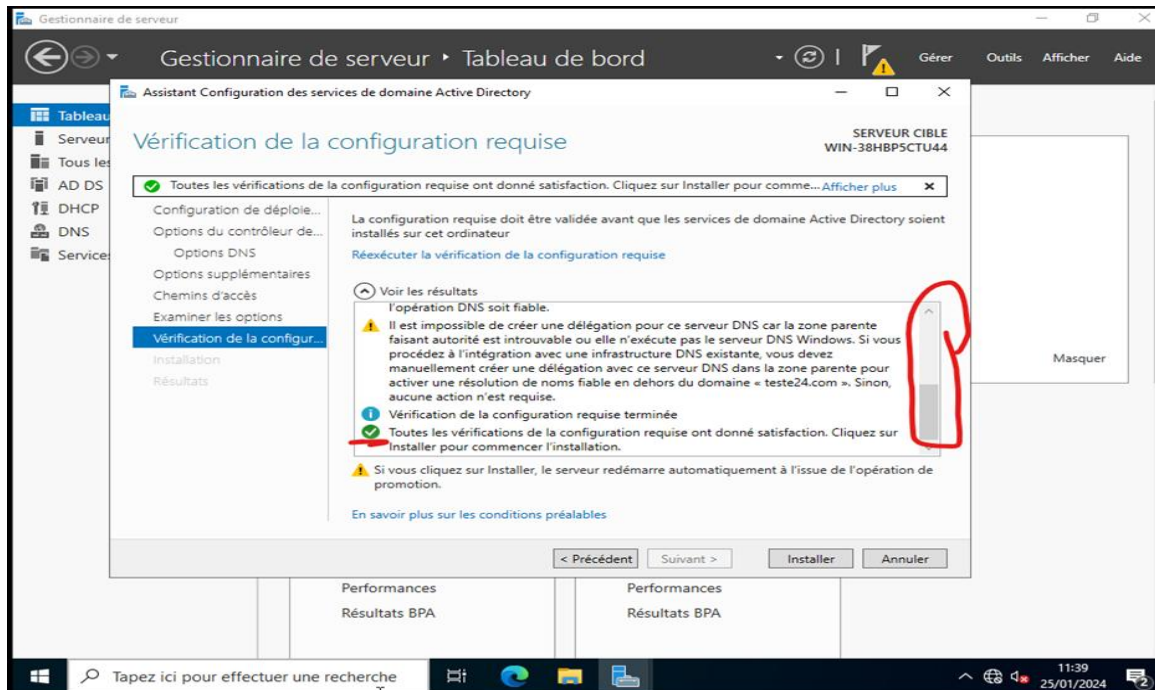
Rien à toucher, suivant :



Rien à toucher, suivant :



Ici on descend pour vérifier que tout est correcte, c'est vert donc on peut installer ADDS. On clique sure Installer :

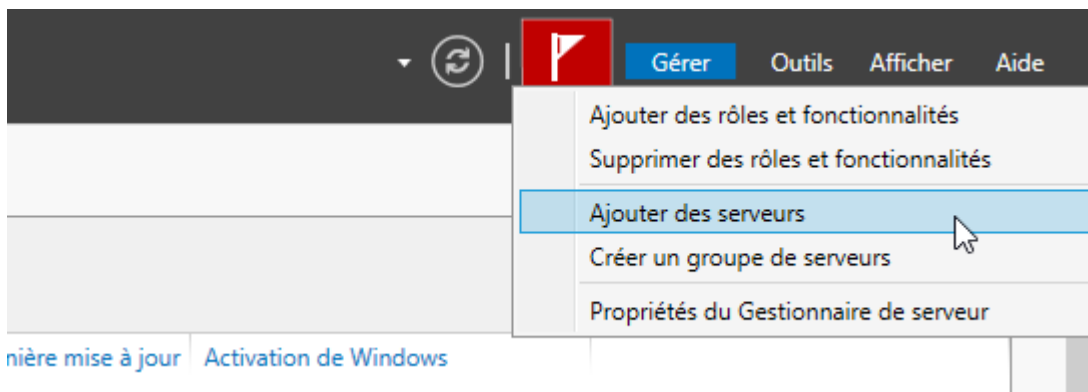


Une fois installé une fenêtre bleue apparait et vous dit de redémarre votre serveur, cliquez sur fermer. Votre serveur va redémarrer et sera contrôleur de domaine.

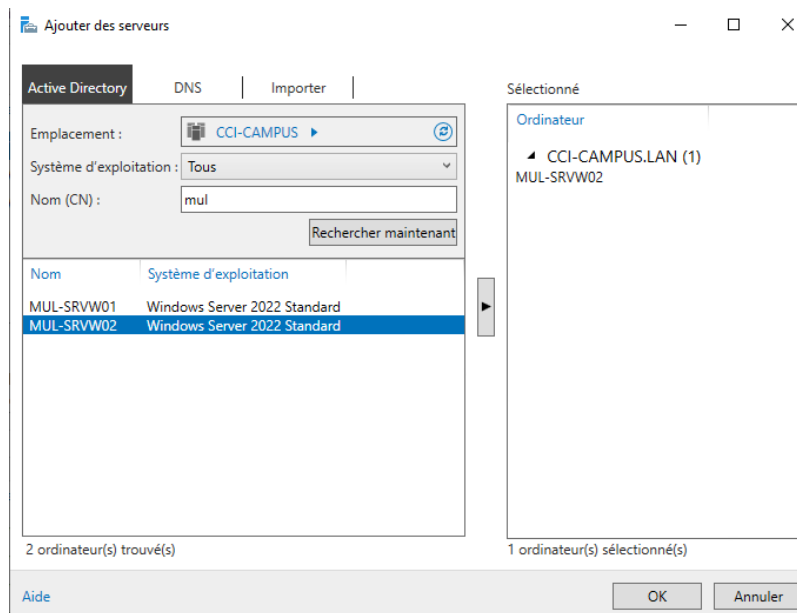
Redondance de l'AD

Vous pouvez ajouter votre serveur en version core au serveur que vous gérer depuis une version avec UI.

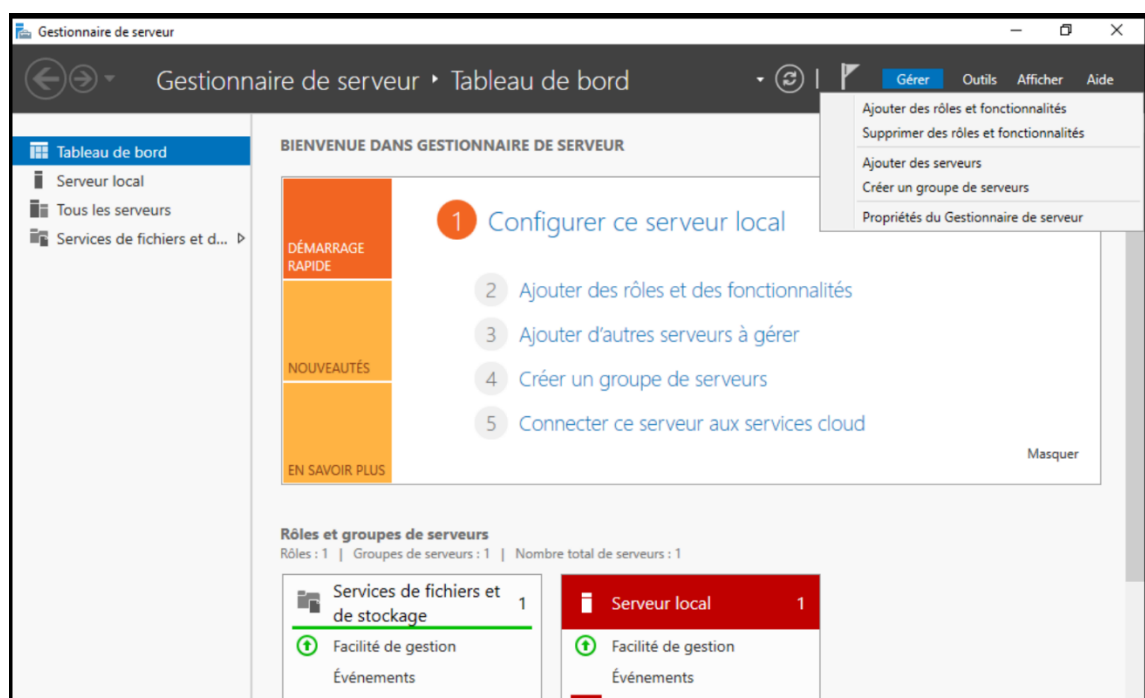
Pour cela allez dans gérer et ajouter des serveurs.



Sélectionner ensuite le serveur que vous voulez gérer



Allez dans Gérer, Ajouter des rôles et fonctionnalités.



Faites Suivant jusqu'à cette page ou vous choisissiez sur quel serveur ajouter le rôle.

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window. The title bar reads 'Assistant Ajout de rôles et de fonctionnalités'. The main heading is 'Sélectionner le serveur de destination'. In the top right corner, it says 'SERVEUR DE DESTINATION MUL-SRVW01.CCI-CAMPUS.LAN'. On the left, a navigation pane lists: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur' (highlighted), 'Rôles de serveurs', 'Fonctionnalités', 'Confirmation', and 'Résultats'. The main area contains the instruction: 'Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.' Below this are two radio buttons: 'Sélectionner un serveur du pool de serveurs' (selected) and 'Sélectionner un disque dur virtuel'. Under the heading 'Pool de serveurs', there is a 'Filtre :' text box. Below the filter is a table with three columns: 'Nom', 'Adresse IP', and 'Système d'exploitation'. The table contains two rows: 'STG-SRVW01.CCI-CAMP...' with IP '192.168.100.1' and 'MUL-SRVW01.CCI-CAM...' with IP '192.168.200.1', both running 'Microsoft Windows Server 2022 Standard'. The second row is highlighted. Below the table, it says '2 ordinateur(s) trouvé(s)'. A paragraph explains that the page shows servers running Windows Server 2012 or later, added via the 'Ajouter des serveurs' command in the Server Manager. At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
MUL-SRVW01.CCI-CAMPUS.LAN

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

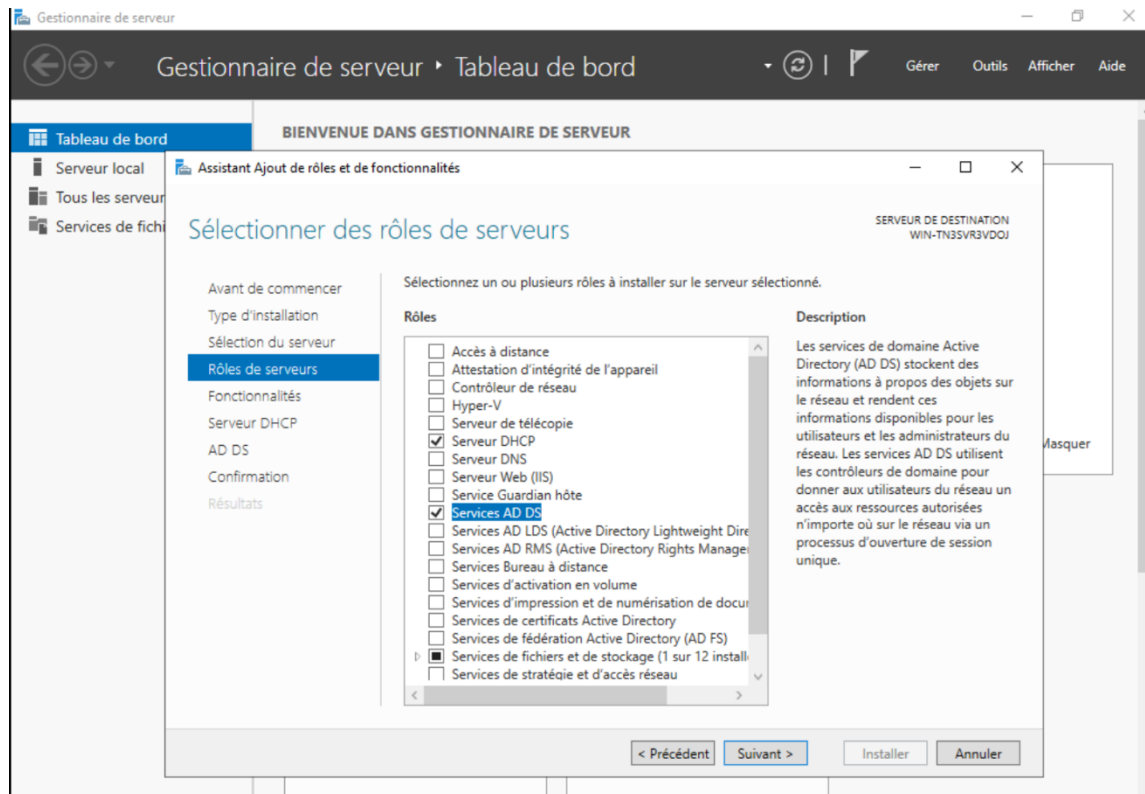
Nom	Adresse IP	Système d'exploitation
STG-SRVW01.CCI-CAMP...	192.168.100.1	Microsoft Windows Server 2022 Standard
MUL-SRVW01.CCI-CAM...	192.168.200.1	Microsoft Windows Server 2022 Standard

2 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

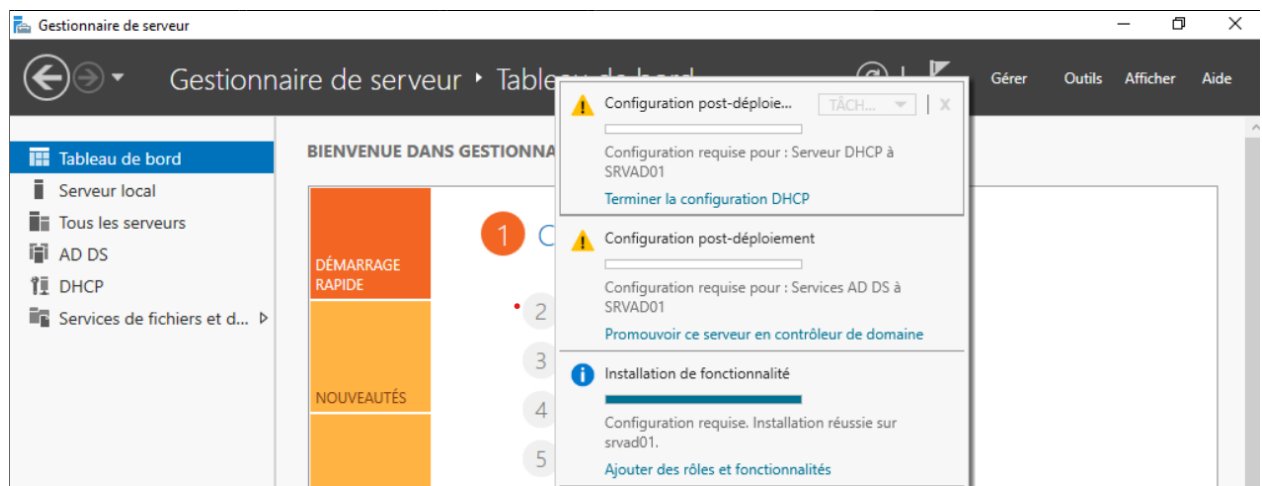
< Précédent Suivant > Installer Annuler

Sélectionnez AD DS.
Refaites Suivant puis Installer



Cliquez sur le drapeau

Cliquez sur Promouvoir ce serveur en contrôleur de domaine



Ajoutez un contrôleur au domaine et rentrez un compte administrateur

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
srvad03.ADS.TEST

- Configuration de déploie...
- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configur...
- Installation
- Résultats

Sélectionner l'opération de déploiement

- ☒ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine :

Fournir les informations d'identification pour effectuer cette opération

SRVAD03\Administrateur (Utilisateur actuel)

[En savoir plus sur les configurations de déploiement](#)

< Précédent **Suivant >** Installer Annuler

Rentrez un mot de passe

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
srvad03.ADS.TEST

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)
☒ Catalogue global (GC)
☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site : Default-First-Site-Name

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

Cliquez sur suivant jusqu'à arriver sur cette page

Assistant Configuration des services de domaine Active Directory

Vérification de la configuration requise

SERVEUR CIBLE
srvad03.ADS.TEST

Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation. [Afficher plus](#)

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

Voir les résultats

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...

Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

< Précédent Suivant > **Installer** Annuler

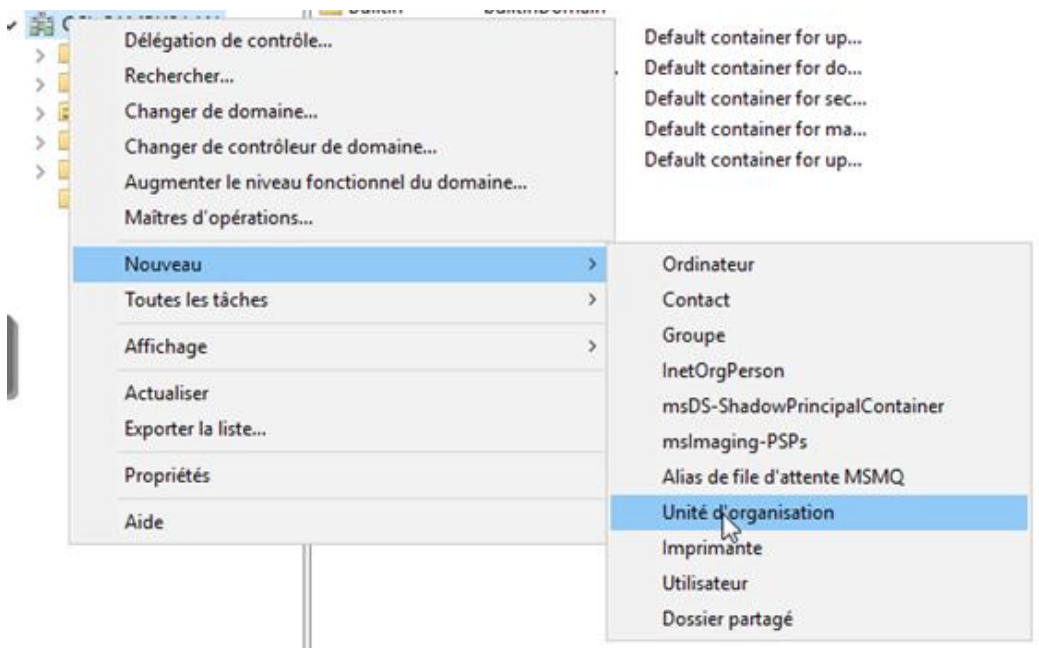
Si vous avez tout bien fait vous n'aurez pas d'erreur ici cliquez sur installer. Après le redémarrage votre AD est redondant.

Création d'unités organisationnelles

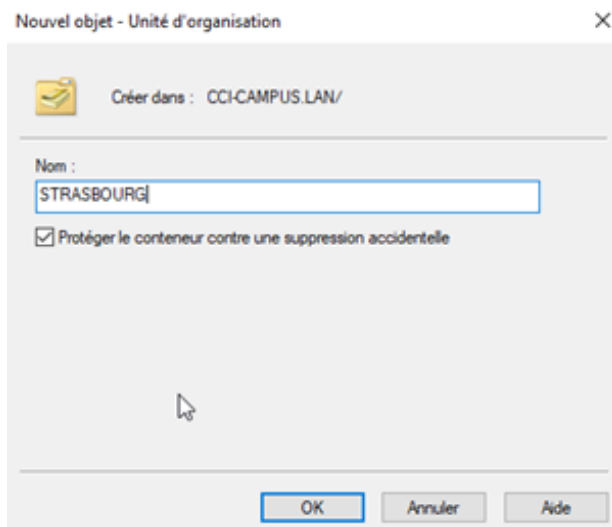
Allez dans outils puis dans utilisateurs et ordinateurs Active Directory



Cliquez sur nom de domaine puis :

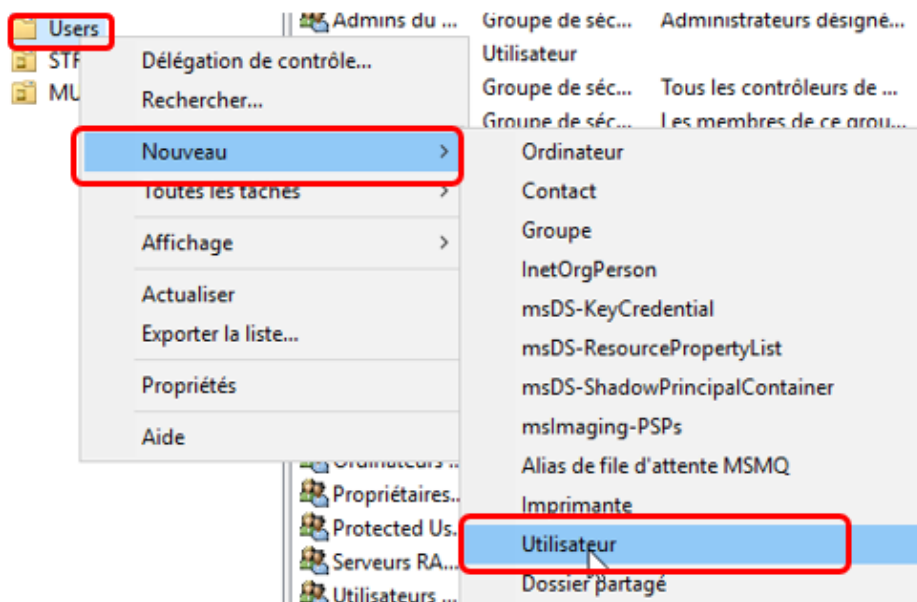


Nommez votre unité



Création d'un utilisateur

Toujours dans la gestion active directory sélectionner l'UI où vous voulez créer votre utilisateur puis :



Nommez votre utilisateur et donnez-lui son identifiant

Nouvel objet - Utilisateur

Créer dans : CCI-CAMPUS.LAN/Users

Prénom : Initiales :

Nom :

Nom complet :

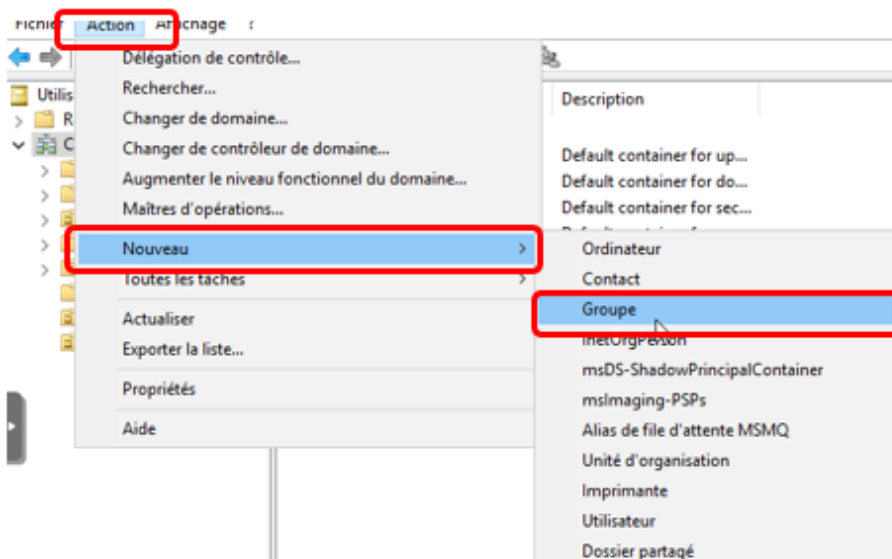
Nom d'ouverture de session de l'utilisateur :
 @CCI-CAMPUS.LAN

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

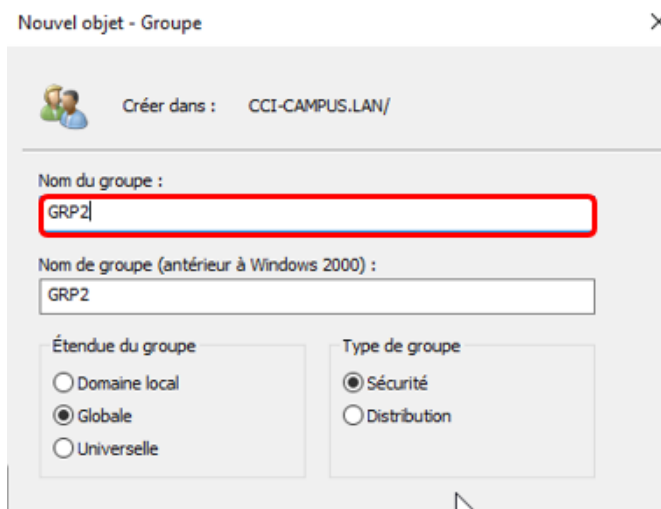
< Précédent **Suivant >** Annuler

Création de groupe de sécurité

Dans la console de gestion faites :

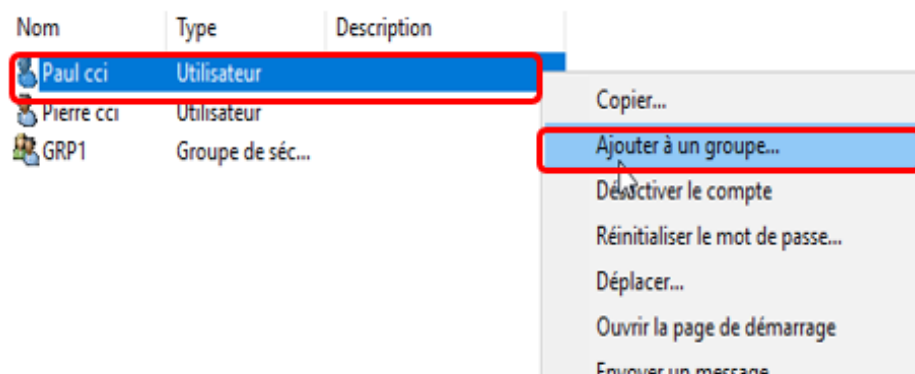


Nommez le groupe

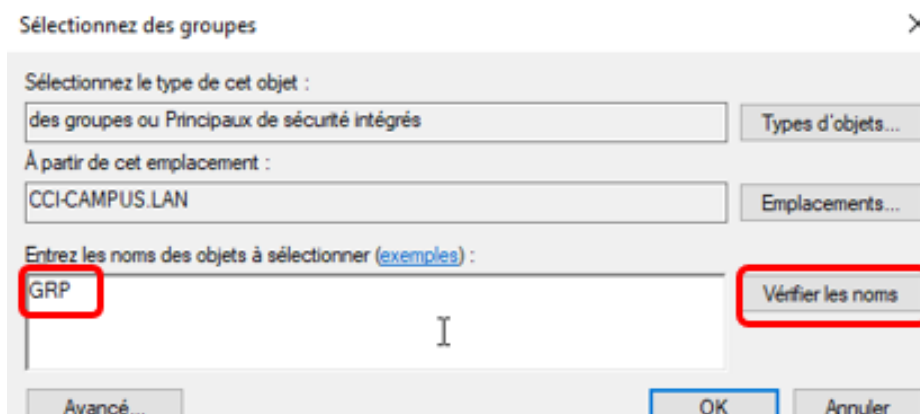


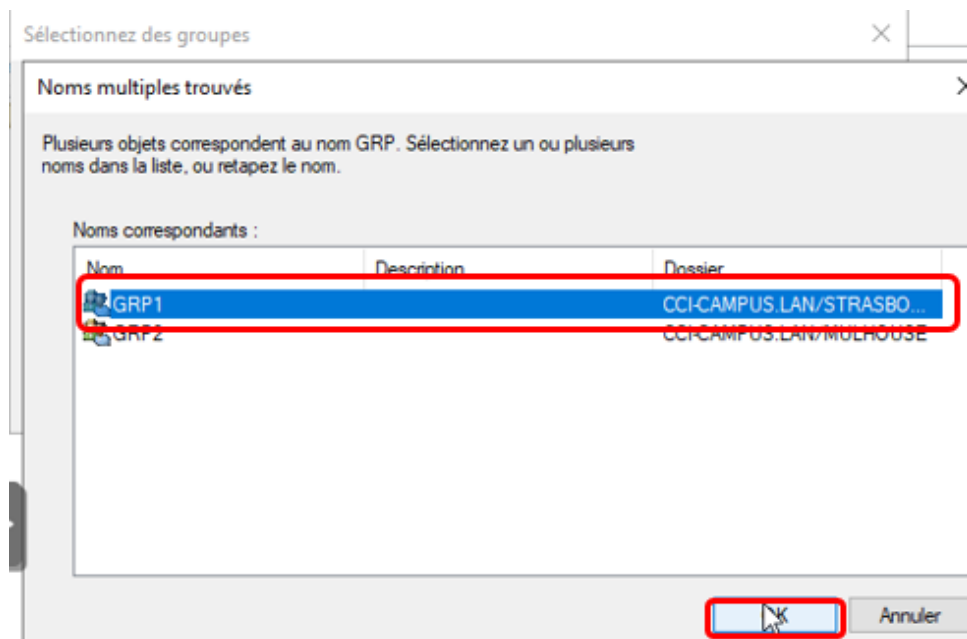
Intégration de l'utilisateur dans un groupe

Sélectionner un utilisateur et :



Choisissez le groupe de sécurité auquel il doit appartenir.





DHCP

Le service DHCP (Dynamic Host Configuration Protocol) permet l'attribution automatique des adresses IP et des configurations réseau aux dispositifs connectés.

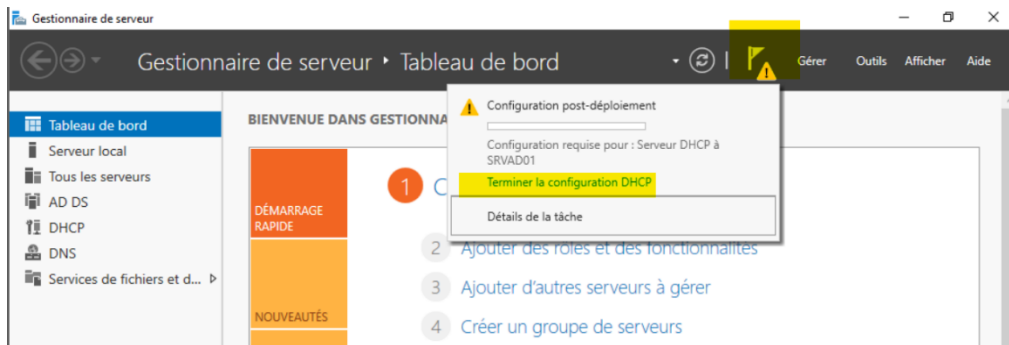
Prérequis

Infrastructure :

- Deux serveurs ADDS (Active Directory Domain Services) avec le rôle DHCP installé.

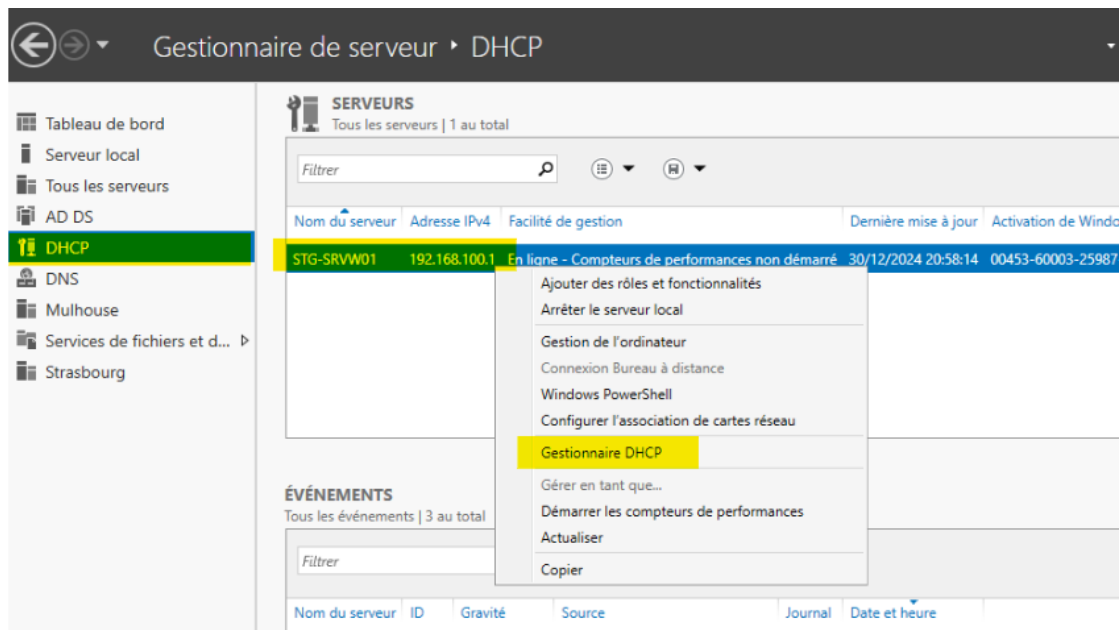
Configuration du DHCP

Cliquez sur le drapeau et terminez la configuration DHCP

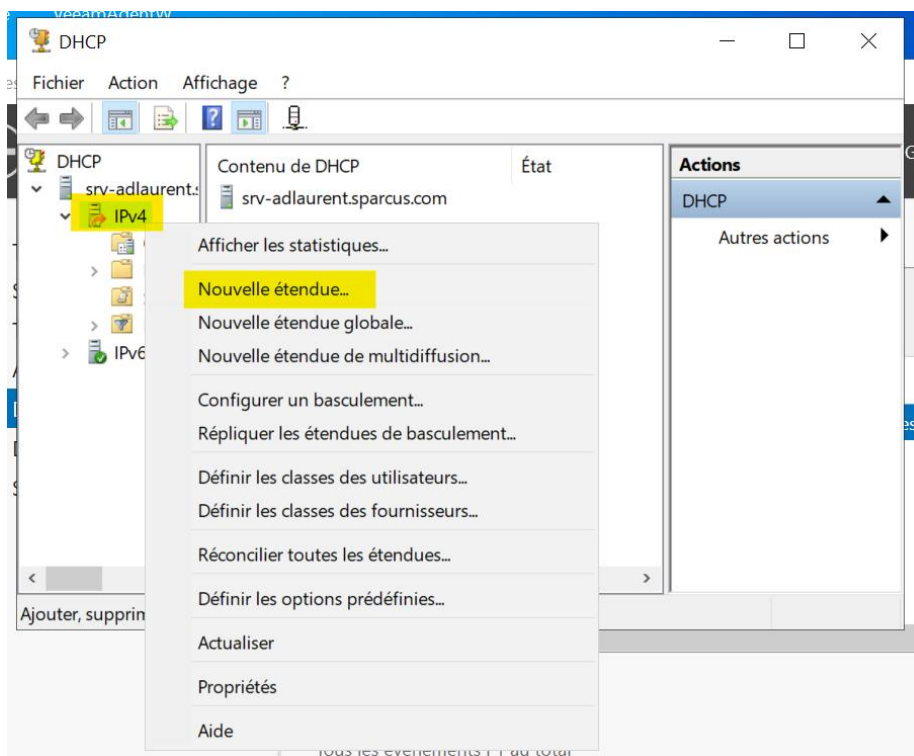


Cliquez sur suivant puis continuez.

Allez ensuite sur DHCP Faites clic droit sur votre serveur puis Gestionnaire DHCP.



Dans votre serveur faites clic droit sur IPv4 puis nouvelle étendue.



Donnez un nom à votre étendu puis suivant.
Ici rentrez l'a première IP puis la dernière.

Assistant Nouvelle étendue

Plage d'adresses IP
 Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

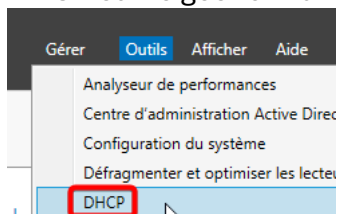
< Précédent Suivant > Annuler

Vous pouvez cliquer sur suivant et terminer.

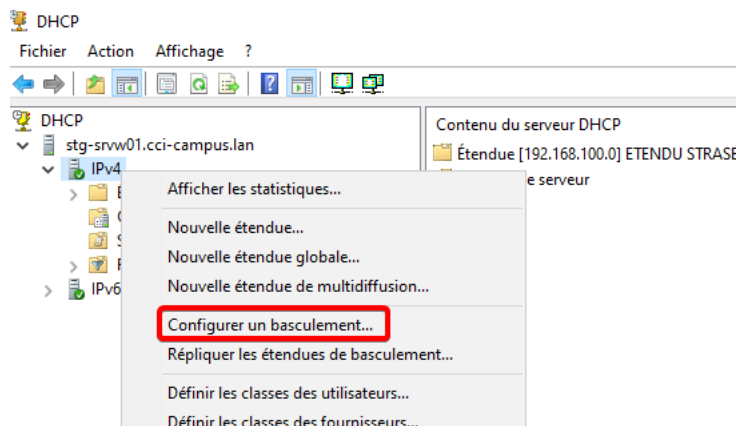
Vous avez maintenant votre DHCP fonctionnel.

Mise en place de la redondance du DHCP

Pour réaliser la redondance du serveur DHCP, il est nécessaire de créer un basculement DHCP entre les serveurs concernés. Pour se faire, aller dans Outils > DHCP sur le gestionnaire de serveur :



Puis développer le nœud qui correspond à votre serveur, et faire clic droit sur IPv4, puis "Configurer un basculement..." :



On sélectionne nos étendues :



Puis on choisit le serveur partenaire :

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire : 192.168.100.2

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent Suivant > Annuler

Enfin, on choisit le mode "Serveur de secours" pour de la redondance efficace, on attribue 10% d'adresses de secours et on rentre un secret partagé :

Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire 192.168.100.2

Nom de la relation : stg-srvw01.cci-campus.lan-192.168.100.2

Délai de transition maximal du client (MCLT) : 1 heures 0 minutes

Mode : Serveur de secours

Configuration du serveur de secours

Rôle du serveur partenaire : Veille

Adresses réservées pour le serveur de secours : 10 %

☐ Intervalle de basculement d'état : 60 minutes

☒ Activer l'authentification du message

Secret partagé : *****

< Précédent Suivant > Annuler

Pour finir, on peut cliquer sur Terminer
Le basculement est maintenant opérationnel.

Mise en place du Pare-Feu et du VPN

Un pare-feu est un élément clé de la sécurité réseau, chargé de filtrer et de contrôler les flux entrants et sortants il protège les systèmes des menaces extérieures. Quand au VPN il permet de créer un tunnel sécurisé entre les deux sites distants, garantissant la sécurité des données.

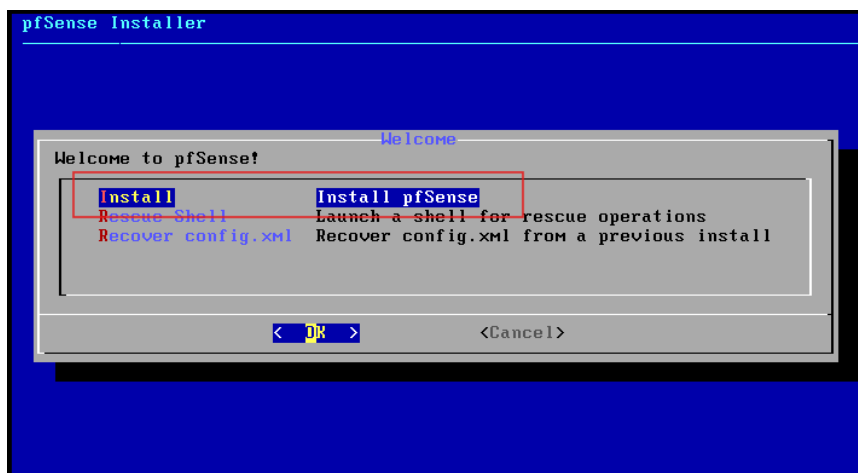
Prérequis

Ressources matériels minimum :

- Processeur : Minimum 1 GHz
- RAM : 512 Mo
- Stockage : 1 disque de 8 Go
- Interface réseau. : 2 interfaces Ethernet (WAN/LAN)

Installation Pfsense

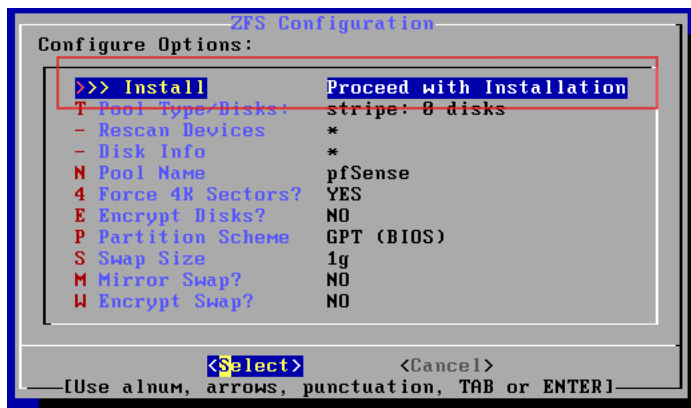
Lancez l'installation de Pfsense.



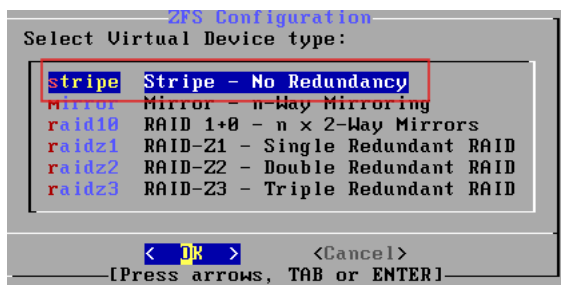
Ici sélectionnez la première option.



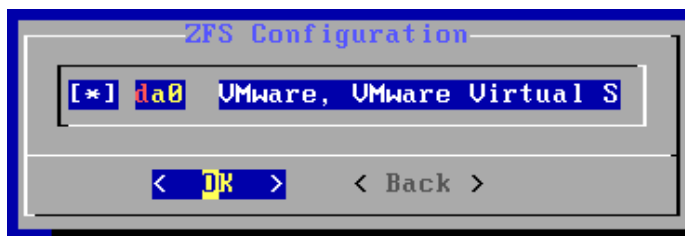
Lancez l'installation



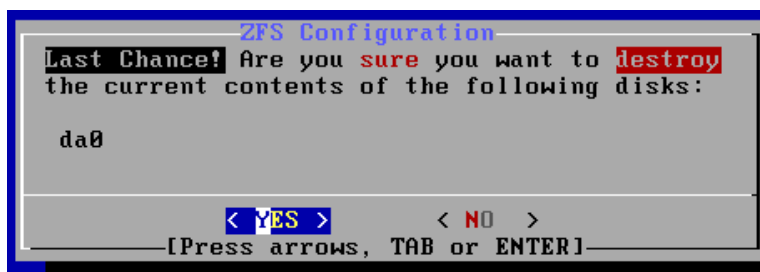
Ici nous ne voulons pas faire de redondance donc nous allons sélectionner la première option.



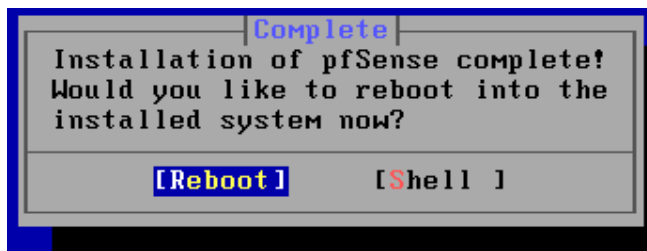
On choisit le disque sur le quelle on va installer le système.



On nous dit que le disque va être effacer et on accepte.



L'installation à réussit on redémarre la machine.



Au redémarrage nous allons configurer nos carte réseaux et pour cela nous allons rentrer dans l'option 1.

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 966e707275112f0c66aa
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.67.138/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: 1
```

Nous n'allons pas configurer de VLANs donc on commence par rentrer « N ». Ensuite nous devons déterminer quelle interface sera le WAN. PFSENSE le fait automatiquement si on rentre « A ».

```
Valid interfaces are:
em0      00:0c:29:7c:1f:ee (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:7c:1f:f8 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y:n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): a
```

Notre interface vers le WAN à bien été détecté on peut maintenant sélectionner l'autre interface pour notre LAN.

```

Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.

Detected link-up on interface em1.

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em0 a or nothing if finished): em0

```

On répond « Y » à la vérification

```

The interfaces will be assigned as follows:

WAN -> em1
LAN -> em0

Do you want to proceed [y/n]? y

```

Notre interface WAN prend son IP par DHCP il nous faut donc configurer l'IP de notre interface LAN. Pour ceci on entre l'option 2

```

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

WAN (wan)      -> em1      -> v4/DHCP4: 192.168.1.100/24
LAN (lan)      -> em0      -> v4: 192.168.1.1/24

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: 2

```

On choisit notre interface LAN

```

Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

```

On dit non au DHCP puis on rentre notre IP et notre masque.

```

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254

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 LAN IPv4 subnet bit count (1 to 32):
> 24

```

On nous demande une gateway. Comme nous sommes sur une interface LAN on ne rentre rien.


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

On ne configure pas notre IPV6 donc on dit non au DHCP et on ne rentre pas d'adresse.

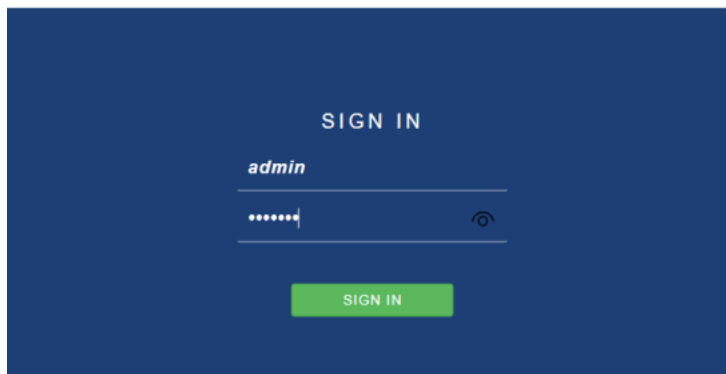
```
Configure IPv6 address LAN interface via DHCP6? (y/n) n  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
> █
```

On répond « n » à toutes les prochaines questions et notre interface est maintenant prête.

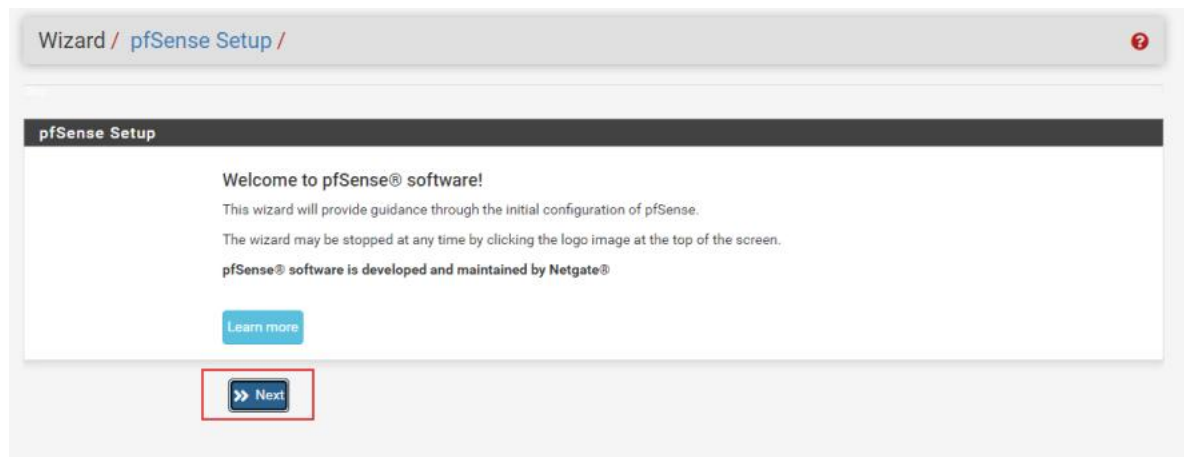
```
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
Please wait while the changes are saved to LAN... █
```

On peut maintenant se connecter à l'UI via une machine client sur le LAN pour ceci rentrez l'adresse IP de votre PFSense dans un navigateur. On arrive sur une page de connexion. Les identifiants par défaut sont admin pour le nom d'utilisateur et Pfsense pour le mot de passe.

← → ↻ ⚠ Non sécurisé | https://192.168.100.254 🔍 ⚙️ ⭐ 📄 👤 ...



On rentre dans la configuration de PFSense on clique sur next



On reclique sur next et on rentre le nom que l'on veut donner à notre DNS son domaine et ces DNS

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

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

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

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

Primary DNS Server

Secondary DNS Server

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

[Next](#)

On clique sur next jusqu'à ce que l'on rentre le mot de passe Admin

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

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

Admin Password

Admin Password AGAIN

[Next](#)

On clique sur reload

Wizard / pfSense Setup / Reload configuration

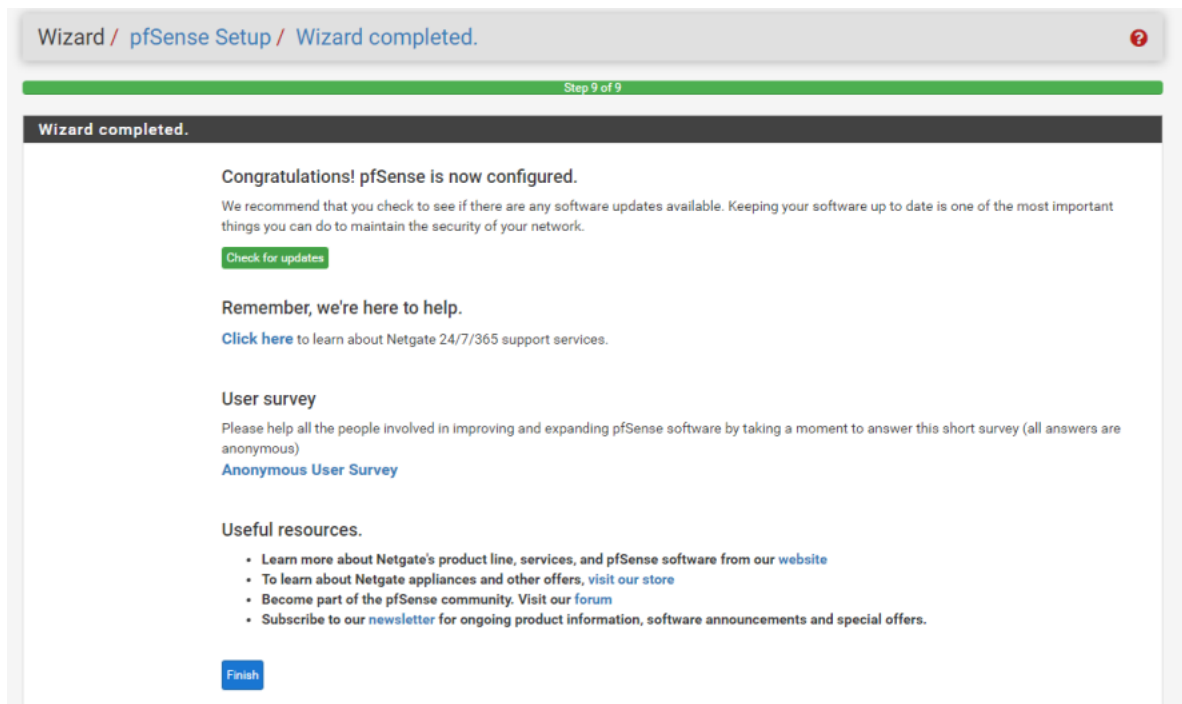
Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

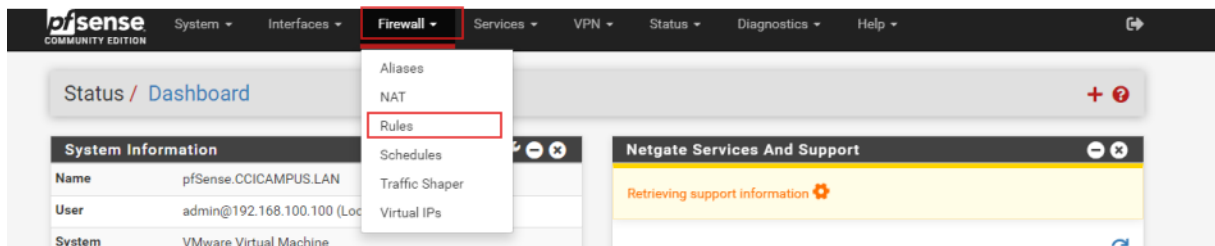
[Reload](#)

Après le chargement notre PFSense est configuré et prêt à être utilisé.

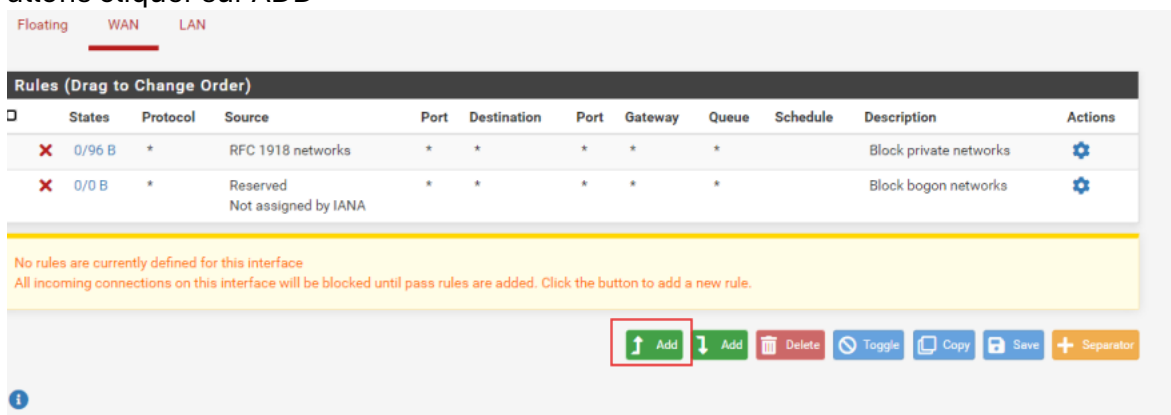


Création des règles du Pare-Feu

Nous allons créer des règles de Pare-Feu. Pour ceci nous allons aller dans Firewall puis Rules



La première chose à faire est de bloquer toutes les communications pour cela nous allons cliquer sur ADD



En action nous allons mettre block en protocole any. Également any en source et en destination.

Edit Firewall Rule

Action Block
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface WAN
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol Any
 Choose which IP protocol this rule should match.

Source
Source ☐ Invert match Any Source Address /

Destination
Destination ☐ Invert match Any Destination Address /

Extra Options

Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Notre règle est bien apparue on clique sur apply changes

Firewall / Rules / WAN

The firewall rule configuration has been changed.
 The changes must be applied for them to take effect. [Apply Changes](#)

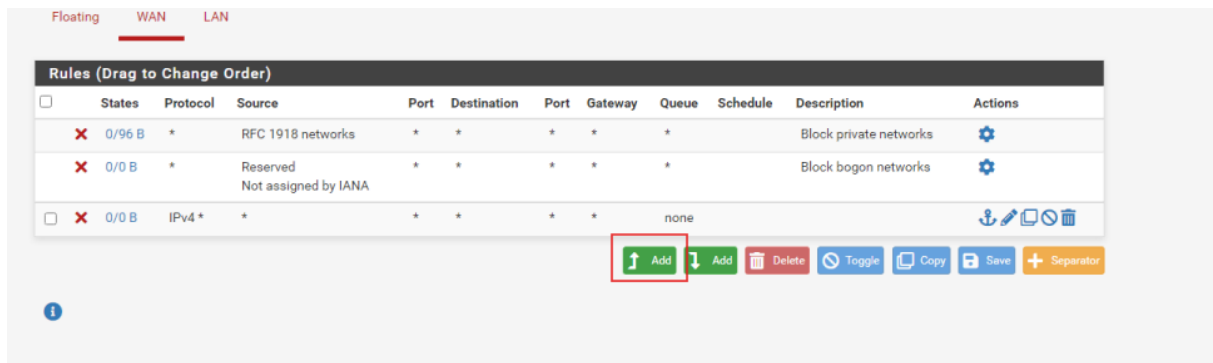
Floating **WAN** LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/96 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	Settings
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	Settings
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none			Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Maintenant nous pouvons n'importe quelle règle pour gérer les autorisations. Pour cela on va cliquer sur ADD



On commence par indiquer Pass dans action, on peut ensuite choisir le protocole puis la source, la destination ainsi que son port.

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

☐ Invert match /

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

☐ Invert match /

Destination Port Range

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

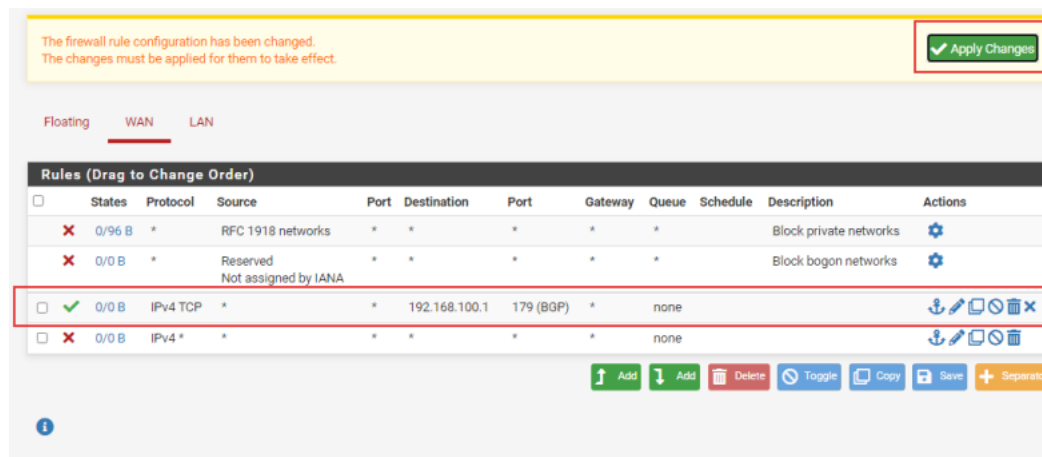
Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

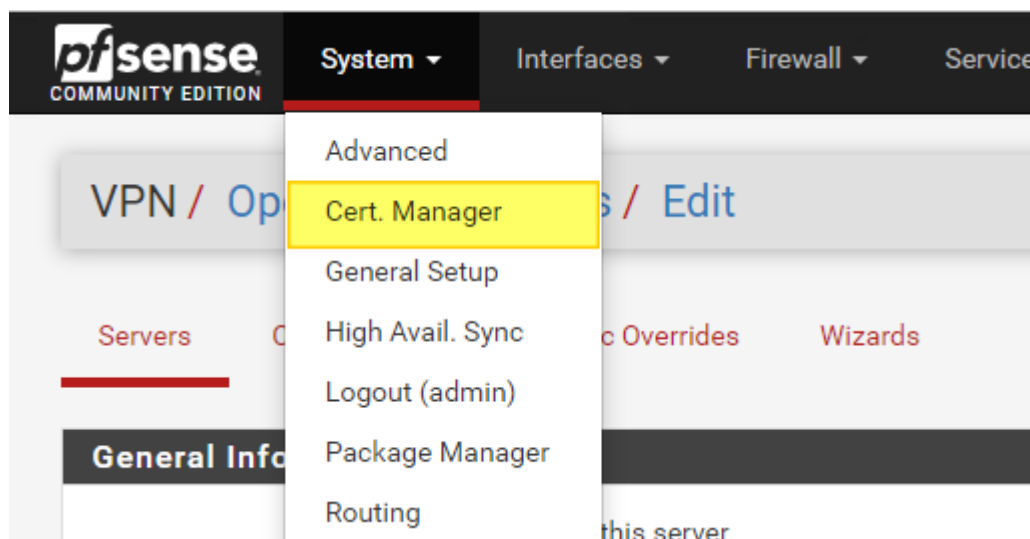
On clique sur Save on vérifie que notre règle est bien apparue et on clique sur Apply Changes.



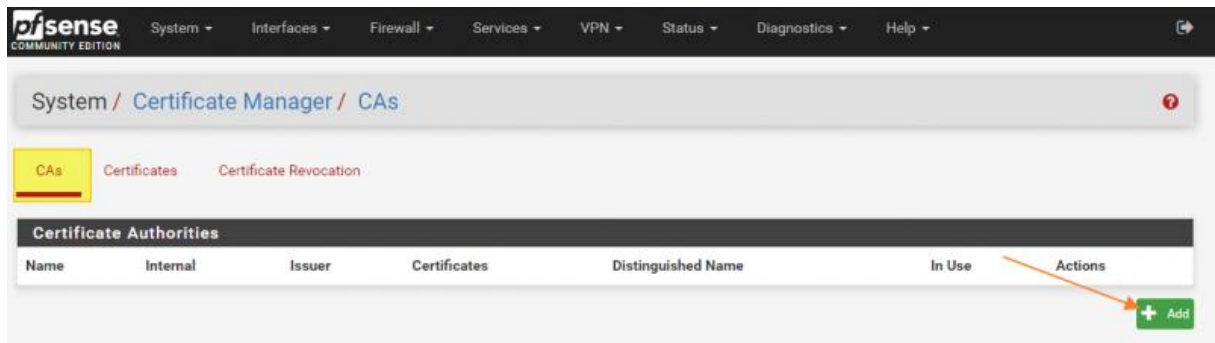
Mise en place du VPN

A. Créer l'autorité de certification

Pour créer l'autorité de certification sur pfSense (si vous n'en avez pas déjà une), vous devez accéder au menu : **System > Cert. Manager**



Dans l'onglet "**CAs**", cliquez sur le bouton "**Add**".



Donnez un nom à l'autorité de certification, par exemple "**CA-ITCONNECT-OPENVPN**", ce nom sera visible seulement dans PfSense. Choisissez la méthode "**Create an internal Certificate Authority**".

Concernant le nom qui sera **affiché dans les certificats**, il s'agit du champ "**Common Name**", j'indique "it-connect" pour ma part. Remplissez les autres valeurs : la région, la ville, etc... et cliquez sur "**Save**" pour créer la CA.

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name

Method Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

Common Name

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


Country Code FR

State or Province







City

Organization

Organizational Unit

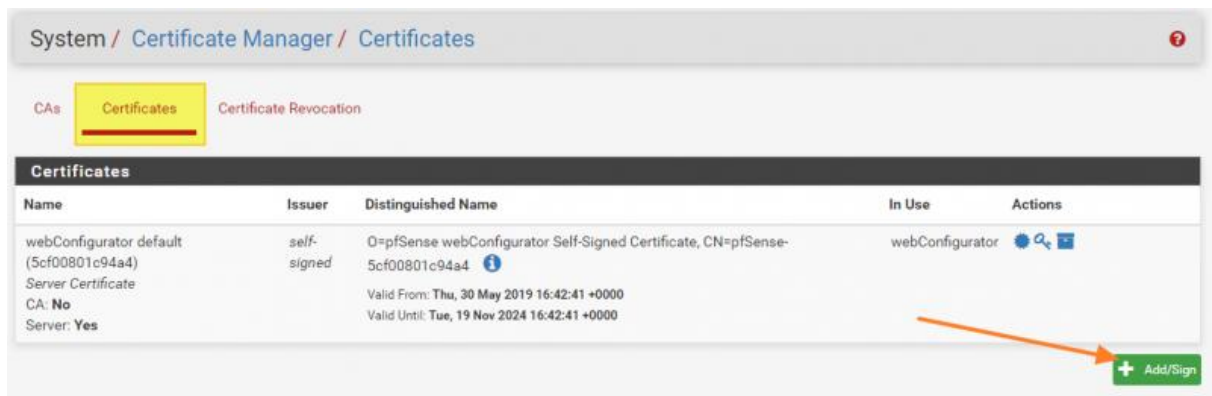
 Save

L'autorité de certification doit apparaître dans l'interface, comme ceci :

CA-RESICIVILE-OPENVPN	✓	self-signed	2	ST=Alsace, O=RESICIVILE, L=Mulhouse, CN=RESICIVILE, C=FR		    
Valid From: Mon, 27 Jan 2025 09:47:27 +0100						
Valid Until: Thu, 25 Jan 2035 09:47:27 +0100						

B. Créer le certificat Server

Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "**Certificate Manager**", cette fois-ci dans l'onglet "**Certificates**", cliquez sur le bouton "**Add/Sign**".



Choisissez la méthode **"Create an Internal Certificate"** puisqu'il s'agit d'une création, donnez-lui un nom (**VPN-SSL-REMOTE-ACCESS**) et sélectionnez l'autorité de certification au niveau du paramètre **"Certificate authority"**.

Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le **"Common Name"** correspond là aussi au nom intégré dans le certificat, **si vous souhaitez établir une connexion VPN basée sur un nom de domaine**, il est préférable d'indiquer cette valeur ici.

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

VPN-SSL-REMOTE-ACCESS

Internal Certificate

Certificate authority

CA-RESICIVILE-OPENVPN

Key length

2048

Digest Algorithm

sha256

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

3650

Common Name

vpn.it-connect.local

The following certificate subject components are optional and may be left blank.

Country Code

FR

State or Province

Normandie

City

Caen

Choisissez bien le **type de certificat (Certificate Type)** suivant : **Server Certificate**.

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and requests when they are created or signed in selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions

Alternative Names

FQDN or Hostname

vpn.it-connect.local

TypeValue

Enter additional identifiers for the certificate in this list. The Common Name field is automatically populated. A signing CA may ignore or change these values.

Add

+ Add

Save

Après avoir cliqué sur "**Save**" pour **valider la création du certificat**, il apparaît dans la liste des certificats du Pare-feu :

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Name	Issuer	Distinguished Name	In
webConfigurator default (5cf00801c94a4) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5cf00801c94a4 Valid From: Thu, 30 May 2019 16:42:41 +0000 Valid Until: Tue, 19 Nov 2024 16:42:41 +0000	w
VPN-SSL-REMOTE-ACCESS Server Certificate CA: No Server: Yes	CA-ITCONNECT-OPENVPN	ST=Normandie, O=IT-Connect, L=Caen, CN=vpn.it-connect.local, C=FR Valid From: Fri, 22 May 2020 04:46:57 +0000 Valid Until: Mon, 20 May 2030 04:46:57 +0000	

La partie certificat est terminée, passons à la suite.

III. Créer les utilisateurs locaux

Comme je le disais en introduction, nous allons utiliser une base de compte interne au Pare-feu dans cet exemple. Je vais donc **créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN**.

Note : si vous utilisez l'Active Directory comme source d'authentification, vous devez tout de même générer au moins un certificat utilisateur (possible directement via le menu Certificate Manager)

Pour créer l'utilisateur, il faut indiquer un identifiant, un mot de passe... Ainsi que cocher l'option "**Click to create a user certificate**" : cela va ajouter le formulaire de

création du certificat juste en dessous. Pour créer le certificat, on se base sur notre autorité de certification.

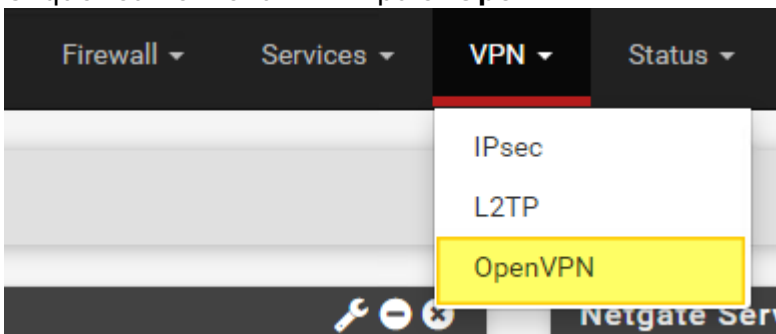
Lorsque l'utilisateur est créé, il apparaît bien dans la base locale :

System / User Manager / Users		
Users Groups Settings Authentication Servers		
Users		
Username	Full name	Status
<input type="checkbox"/> admin	System Administrator	✓
<input type="checkbox"/> itconnect.vpn.fb	Florian BURNEL - Compte VPN	✓

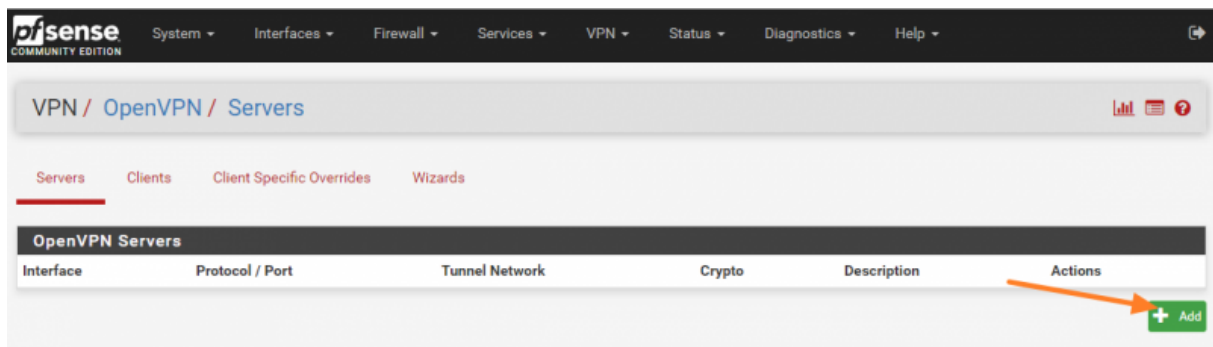
IV. Configurer le serveur OpenVPN

Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.

Cliquez sur le menu "VPN" puis "OpenVPN"



Dans l'onglet "Servers", cliquez sur "Add" pour créer une nouvelle configuration.



La première chose à faire, c'est de choisir le **"Server Mode"** suivant : **Remote Access (SSL/TLS + User Auth)**.

Pour le VPN, le protocole s'appuie sur de l'UDP, avec le **port 1194** par défaut : **je vous recommande d'utiliser un port différent**. Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

Au niveau de la partie chiffrement, un peu plus bas dans la page, vous devez sélectionner votre autorité de certification au niveau du champ **"Peer Certificate Authority"**. En complément, sélectionnez le certificat Server au niveau du champ **"Server certificate"**.

Cryptographic Settings

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

☒ Automatically generate a TLS Key.

Peer Certificate Authority CA-ITCONNECT-OPENVPN

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

Server certificate VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-ITCONNECT-OPEN)

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

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

Encryption Algorithm AES-128-CBC (128 bit key, 128 bit block)
 The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Enable NCP ☒ Enable Negotiable Cryptographic Parameters
 Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below. ⓘ

NCP 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-128-GCM
--	-------------

Pour l'algorithme de chiffrement (**Encryption Algorithm**), nous pouvons passer sur de l'**AES-256-CBC** plutôt que de l'AES-128-CBC. La sécurité sera renforcée, mais cela impact légèrement les performances, car le processus de chiffrement est alourdi : il sera toujours possible de modifier cette valeur. Il n'est pas nécessaire de modifier les autres options liées au chiffrement.

Encryption Algorithm AES-256-CBC (256 bit key, 128 bit block)
 The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Passons maintenant à la configuration de notre tunnel VPN en lui-même.

- **IPv4 Tunnel Network** : adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il obtiendra une adresse IP dans ce réseau au niveau de la carte réseau locale du PC
- **Redirect IPv4 Gateway** : si vous cochez cette option, vous passez sur un full tunnel c'est-à-dire que tous les flux réseau du PC distant vont passer dans le VPN, sinon nous sommes en split-tunnel
- **IPv4 Local network** : les adresses réseau des LAN que vous souhaitez rendre accessibles via ce tunnel VPN. Dans mon exemple, je souhaite rendre accessible le réseau 192.168.1.0/24 via le VPN. Si vous avez plusieurs valeurs à indiquer, il faut les séparer par une virgule
- **Concurrent connections** : le nombre de connexions VPN simultanés que vous autorisez.

Tunnel Settings	
IPv4 Tunnel Network	10.10.10.0/24 <small>This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.0.0/24). 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.</small>
IPv6 Tunnel Network	 <small>This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.1.0/24 <small>IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
IPv6 Local network(s)	 <small>IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent connections	10 <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Compression	Disable Compression, retain compression packet framing (compress) <small>Compress tunnel packets using the LZO algorithm. 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. 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>
Push Compression	<input type="checkbox"/> Push the selected Compression setting to connecting clients.

Pour les paramètres des clients, je vous **recommande de cocher l'option "Dynamic IP"** : si l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN. C'est surtout utile si vous avez des personnes qui se connectent via une connexion 4G et en mobilité.

Au niveau de la **"Topology"**, **remarque très importante à prendre en compte** : pour des raisons de sécurité, il vaut mieux utiliser la topologie **"net30 - isolated /30 network per client"** pour que **chaque client soit isolé dans un sous-réseau (de la plage réseau VPN) afin que les clients ne puissent pas communiquer entre eux !**

Cela n'est pas sans conséquence : plutôt qu'une connexion VPN consomme une adresse IP sur la plage réseau dédiée au VPN, **elle va consommer 4 adresses IP** : une adresse IP pour le PC, une adresse IP pour le pare-feu et les adresses de réseau et broadcast du sous-réseau en /30.

- Si vous avez besoin de plus de 60 connexions VPN en simultanés, vous ne devez pas utiliser un réseau VPN en /24, mais vous devez prendre plus large. Dans ce cas, modifiez la valeur **"IPv4 Tunnel Network"** définie précédemment.

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	net30 - Isolated /30 network per client <small>Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to 'subnet' even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require 'net30'.</small>

Si vous avez besoin d'utiliser la résolution DNS interne de votre entreprise, dans ce cas vous pouvez diffuser un serveur DNS. Cochez l'option **"Provide a DNS server list to clients. Addresses may be IPv4 or IPv6"** et indiquez en dessous la ou les adresses IP de vos serveurs DNS.

Cochez également l'option "**Provide a default domain name to clients**" pour indiquer votre nom de domaine local.

Note : si vous rencontrez des problèmes avec la résolution DNS sur des PC Windows 10, vous pouvez forcer l'utilisation du DNS diffusé via le VPN en activant l'option "**Block Outside DNS**".

Advanced Client Settings	
DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	<input type="text" value="it-connect.local"/>
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	<input type="text" value="192.168.1.10"/>
DNS Server 2	<input type="text"/>
DNS Server 3	<input type="text"/>
DNS Server 4	<input type="text"/>
Block Outside DNS	<input type="checkbox"/> Make Windows 10 Clients 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.
Force DNS cache update	<input type="checkbox"/> Run 'net stop dnscache', 'net start dnscache', 'ipconfig /flushdns' and 'ipconfig /registerdns' on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	<input type="checkbox"/> Provide an NTP server list to clients
NetBIOS enable	<input type="checkbox"/> Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Descendez dans la page... On s'approche de la fin. Dans la zone "**Custom options**", indiquez : **auth-nocache**. Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

Advanced Configuration	
Custom options	<input type="text" value="auth-nocache"/> <small>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"</small>
UDP Fast I/O	<input type="checkbox"/> Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
Send/Receive Buffer	<input type="text" value="Default"/> <small>Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.</small>
Gateway creation	<input checked="" type="radio"/> Both <input type="radio"/> IPv4 only <input type="radio"/> IPv6 only <small>If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.</small>
Verbosity level	<input type="text" value="default"/> <small>Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output. None: Only fatal errors. Default through 4: Normal usage range 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets. 6-11: Debug info range</small>

Validez la configuration... Votre configuration VPN est prête :

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	10.10.10.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	VPN SSL - IT-Connect (tun)	 

V. Exporter la configuration OpenVPN



Pour télécharger la configuration au format ".ovpn", il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu. Rendez-vous dans le menu suivant : **System > Package Manager > Available Packages**.

Recherchez "openvpn" et installez le paquet : **openvpn-client-export**.

System / Package Manager / Available Packages


Installed Packages Available Packages





Search

Search term Both  Search  Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
openvpn-client-export	1.4.23	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	 Install

Package Dependencies:  openvpn-client-export-2.4.9  openvpn-2.4.9  zip-3.0_1  p7zip-16.02_2

Lorsque c'est fait, retournez dans le menu "**OpenVPN**" puis dans l'onglet "**Client Export**".

Si vous souhaitez utiliser l'adresse IP publique pour vous connecter, utilisez l'option "**Interface IP Address**" pour l'option "**Host Name Resolution**". Il y a d'autres options possibles, notamment par nom de domaine.

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards **Client Export** Shared Key Export

OpenVPN Server

Remote Access Server VPN SSL - IT-Connect UDP4:1194

Client Connection Behavior

Host Name Resolution Interface IP Address

Verify Server CN Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible

Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.

Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.

With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.

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 2.4 settings in the client configuration. When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-incompatible settings such as Negotiable Cryptographic Parameters (NCP) into the client configuration.

Use Random Local Port ☐ Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

Les autres options peuvent être laissées par défaut... Il y a seulement notre option **"auth-nocache"** à reporter dans la section des options additionnelles.

Certificate Export Options

PKCS#11 Certificate Storage ☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage ☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate ☐ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.

Proxy Options

Use A Proxy ☐ Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options **auth-nocache**

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.

EXAMPLE: remote-random;

Save as default

Cliquez sur le bouton **"Save as default"** en bas de page.

En dessous de la part configuration, vous avez la possibilité de télécharger la configuration. **Pour utiliser OpenVPN Community, il faudra prendre la configuration "Bundled Configuration"**, au format archive pour récupérer tous les fichiers nécessaires.

Pour l'utilisation sur mobile avec OpenVPN Connect, prenez la configuration **"Inline Configuration"**.

Si vous avez besoin de récupérer le client OpenVPN pour Windows (ou Mac via Viscosity), vous pouvez l'avoir depuis cette page également - *Sinon, il y a un lien plus bas dans cet article.*

Search

Search term Search Clear

Enter a search string or *nix regular expression to search.

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, TLS Encryption+Authentication, ECDH, LZ4 Compression and other non-legacy compression choices, IPv6 DNS servers, and more.

OpenVPN Clients

User	Certificate Name	Export
itconnect.vpn.fb	VPN-SSL-RA-FB	<p>- Inline Configurations:</p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installer (2.4.9-lx01):</p> <p>7/8.1/2012/2 10/2016/2019</p> <p>- Old Windows Installers (2.3.18-lx02):</p> <p>x86-xp x64-xp x86-win6 x64-win6</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle Viscosity Inline Config</p>

Only OpenVPN-compatible certificates are shown

Voici le contenu de l'archive ZIP téléchargée :

< Téléchargements > FW-PFSENSE-UDP4-1194-itconnect.vpn.fb-config.zip > FW-PFSENSE-UDP4-1194-itconnect.vpn.fb

Nom	Type	Taille compressée	Protégé
FW-PFSENSE-UDP4-1194-itconnect.vpn.fb.ovpn	Fichier OVPN	1 Ko	Non
FW-PFSENSE-UDP4-1194-itconnect.vpn.fb.p12	Échange d'informations p...	4 Ko	Non
FW-PFSENSE-UDP4-1194-itconnect.vpn.fb-tls.key	Fichier KEY	1 Ko	Non

VI. Créer les règles de firewall pour OpenVPN

D'une part, nous devons **créer une règle pour autoriser les clients à monter la connexion VPN**, et d'autre part nous devons **créer une ou plusieurs règles pour autoriser l'accès aux ressources** : serveur en RDP, serveur de fichiers, application web, etc.

A. Autoriser le flux OpenVPN

Cliquez sur le menu "Firewall" > "WAN". Il est nécessaire de créer une nouvelle règle pour l'interface WAN, en sélectionnant le **protocole UDP**.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface WAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol UDP

Choose which IP protocol this rule should match.

La destination ce sera notre adresse IP publique donc sélectionnez "WAN address". Pour le port, prenez OpenVPN dans la liste ou alors indiquez votre port personnalisé.
Si vous le souhaitez, vous pouvez ajouter une description à cette règle et activer les logs.

Destination

Destination ☐ Invert match. **WAN address** Destination Address /

Destination Port Range **OpenVPN (1194)** From Custom To **OpenVPN (1194)** Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1590124355
Created	5/22/20 05:12:35 by admin@192.168.1.30 (Local Database)
Updated	5/22/20 05:12:35 by admin@192.168.1.30 (Local Database)

[Save](#)

Validez la création de la règle et appliquez la configuration.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating **WAN** LAN LAN2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 5 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	Settings
<input checked="" type="checkbox"/>	0 / 33 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	Settings
<input type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Autoriser le VPN SSL	Settings Add Edit Delete

À partir de ce moment-là, il est possible de monter le tunnel VPN sur un PC, mais les ressources de votre entreprise seront inaccessibles.

B. Autoriser les flux vers les ressources

Ajoutez une nouvelle règle, cette fois-ci sur l'interface OpenVPN.

La règle qui suit sert à **autoriser l'accès en RDP à l'hôte 192.168.1.30** (qui fait bien parti du réseau autorisé dans la configuration du VPN) au travers du tunnel VPN.

Vous devez créer une ou plusieurs règles en fonction des ressources auxquelles vos utilisateurs doivent accéder via le VPN, en limitant les flux au maximum.

- Si vous utilisez le DNS de votre entreprise via le VPN, pensez à autoriser le flux DNS vers votre serveur DNS.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface OpenVPN
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol TCP
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. any Source Address /

Pour la destination, ce sera donc mon hôte et le port 3389 pour le RDP. De la même façon que pour la règle précédente, indiquez une description et activez la journalisation si vous le souhaitez.

Destination

Destination ☐ Invert match. Single host or alias 192.168.1.30 /

Destination Port Range (other) 3389 (other) 3389
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

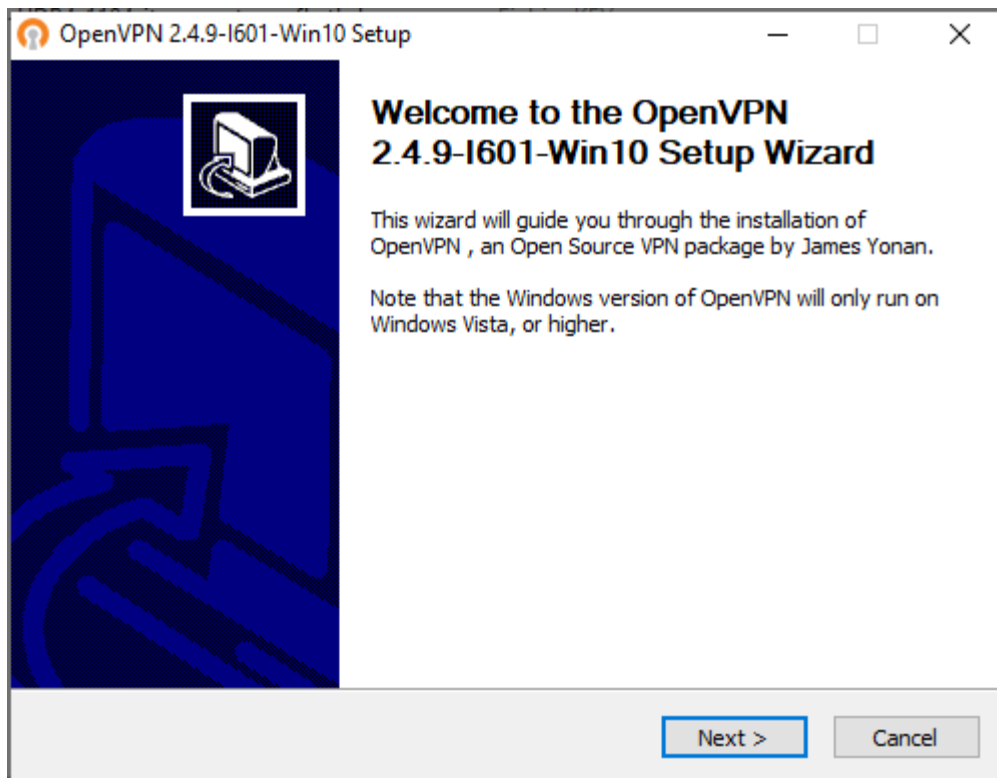
Description Autoriser RDP vers PC Windows 10
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

La configuration est terminée... Il ne reste plus qu'à tester !

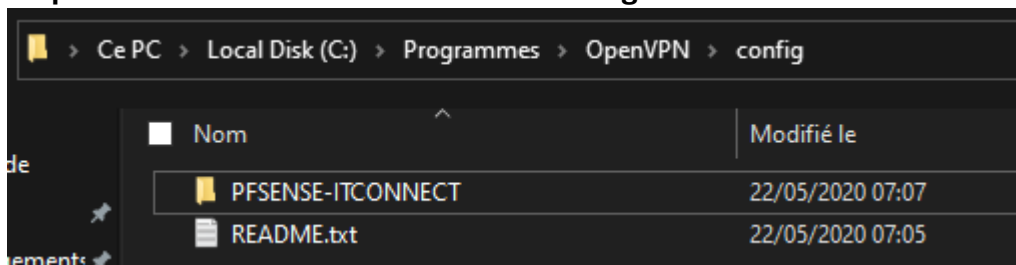
VII. Tester l'accès distant depuis un poste client

Sur mon PC Windows 10, je commence par installer le client OpenVPN... Ce qui se fait très facilement, sans difficulté particulière !

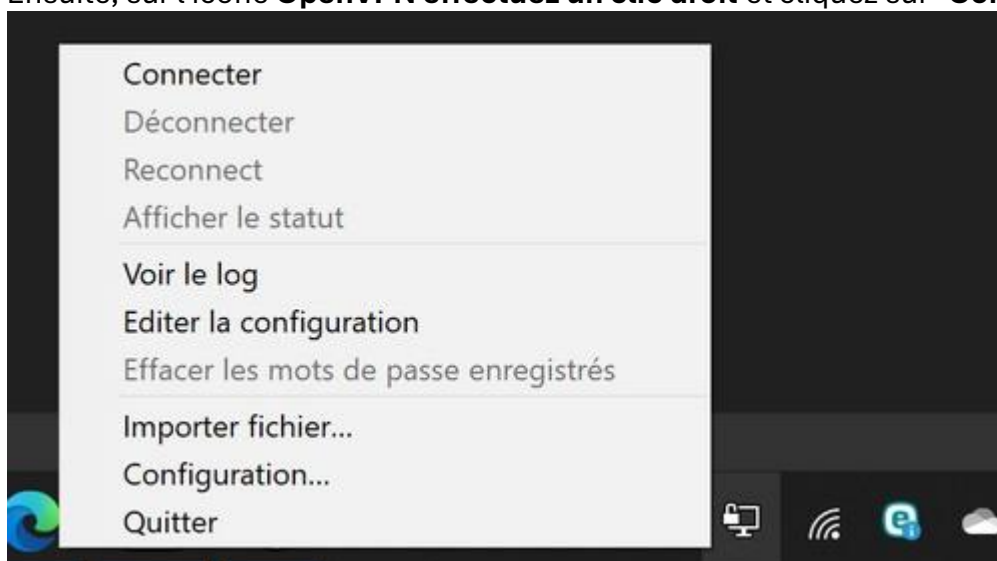


Dans le dossier "**C:\Programmes\OpenVPN\Config**" vous devez **extraire le contenu de l'archive ZIP** téléchargée depuis le Pfsense et qui **contient la configuration**. Vous pouvez créer un sous-dossier dans le dossier "config" si vous voulez.

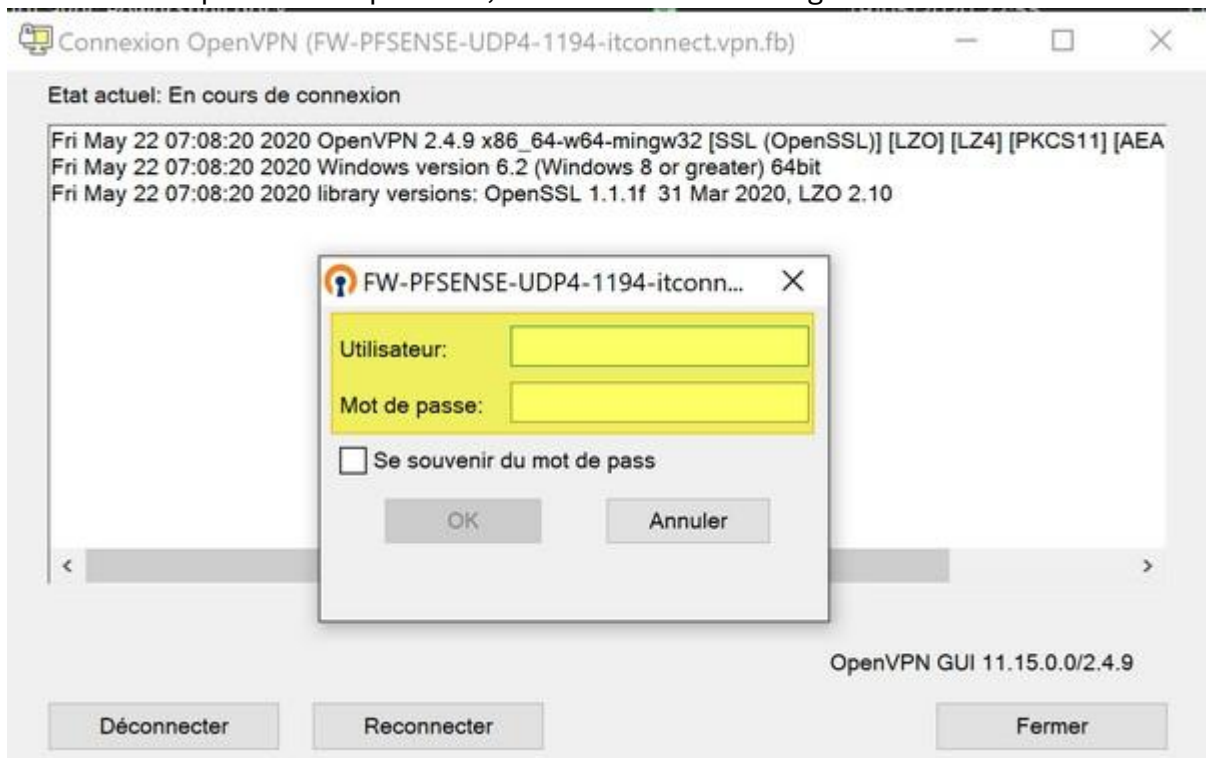
- **Pour donner un nom plus corporate à la connexion VPN, renommez le fichier .ovpn : son nom sera celui donné à la configuration.**



Ensuite, sur l'icône **OpenVPN** effectuez un **clic droit** et cliquez sur "**Connecter**".



Vous devez fournir le nom d'utilisateur et le mot de passe, correspondant à un compte AD ou un compte local du pare-feu, en fonction de la configuration.



Lorsque le tunnel VPN est monté et actif, l'icône devient vert :



Si l'on effectue un **ipconfig** sur le PC, nous pouvons voir que l'on a bien une adresse IP sur la plage 10.10.10.0, avec un sous-réseau en /30 pour l'isolation des clients.

```
Carte inconnue Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . : it-connect.local
    Description. . . . . : TAP-Windows Adapter V9
    Adresse physique . . . . . : 00-FF-34-DB-69-62
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::9a8:a3a9:4124:ac26%46(préféré)
    Adresse IPv4. . . . . : 10.10.10.6(préféré)
    Masque de sous-réseau. . . . . : 255.255.255.252
    Bail obtenu. . . . . : vendredi 22 mai 2020 07:14:47
    Bail expirant. . . . . : samedi 22 mai 2021 07:14:47
    Passerelle par défaut. . . . . :
    Serveur DHCP . . . . . : 10.10.10.5
    IAID DHCPv6 . . . . . : 771817268
    DUID de client DHCPv6. . . . . : 00-01-00-01-25-24-20-B1-B8-31-B5-3C-74-F9
    Serveurs DNS. . . . . : 192.168.1.10
    NetBIOS sur Tcpip. . . . . : Activé
```


Mise en place de la redondance CARP et IP virtuelles sur pfSense

1) Configuration des adresses IP router.

Pour permettre une redondance du wan, nous allons monter 2 nouvelle carte virtuelle. La premiere, nommé **OPT1**, sur **chaque** router.

Pfsense root automatiquement les différentes interfaces. Ce qui permet une haute tolérance a la panne car, le pfsense sera redondé sur une deuxième carte.

Puis nous ajoutons une deuxième interface nommée **DMZ** qui sera utile pour la suite du Projet. Ce qui nous donne ceci :

Sur le router 1 :

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.76/24
                                   v6/DHCP6: 2a01:e0a:a59:7790:be24:11ff:fe7b:aab
5/64
LAN (lan)      -> vtnet1      -> v4: 192.168.10.254/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.20.253/24
DMZ (opt2)     -> vtnet3      -> v4: 192.168.30.253/24
```

Sur le router 2 :

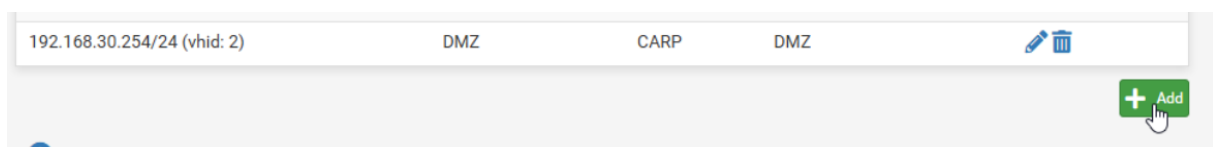
```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.49/24
                                   v6/DHCP6: 2a01:e0a:a59:7790:be24:11ff:fe22:f81
1/64
LAN (lan)      -> vtnet1      -> v4: 192.168.10.253/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.20.252/24
DMZ (opt2)     -> vtnet3      -> v4: 192.168.30.252/24
```

Une fois les interface ajouter au router, adresse ip attribué, et renommé pour une simplification de la configuration.

On se rend dans l'interface web de pfsense, puis dans virutal ip :



Appuyer sur **add**



Sur l'interface suivante établir la configuration suivante :

Sélectionner le type : **CARP**

Choisir l'interface a redondé : **LAN**

Adress : **RENSEIGNER L'ADRESSE IP VIRUTEL SOUHAITE**

Virutal IP Password : **RENSIENGER UN MOT DE PASSE QUI VA ASSURER LA REDONDANCE ENTRE LES DEUX INTERFACES**

VHID GROUP : 1 (**Changer si plusieurs IP VIRUTEL**)

Nous Repettons l'opération sur le router 2 :

Edit Virtual IP

Type: ☒ IP Alias ☒ **CARP** ☐ Proxy ARP ☐ Other

Interface: LAN

Address type: Single address

Address(es): 192.168.10.252 / 24

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

Virtual IP Password: [masked] [masked]

VHID Group: 1

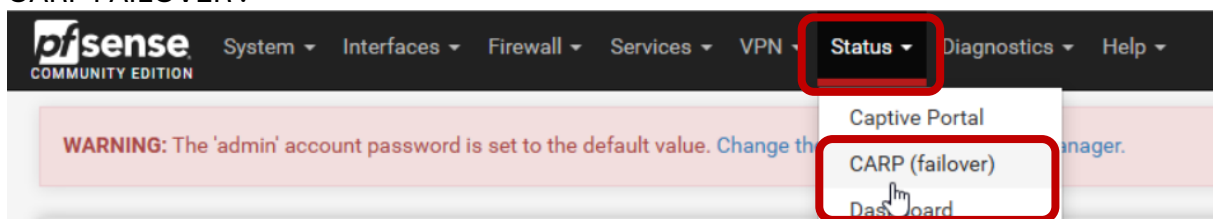
Advertising frequency: 1 Base Skew: 100

Description: redondancewan

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

Save

Désormais pour vérifier la configuration, nous pouvons nous rendre sur STATUS -> CARP FAILOVER :



On se rend bien compte que le **ROOTER 1**, a un **CARP** considéré comme **MASTER** Sur l'interface **LAN**.

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.10.252/24	redondancewan	 MASTER

Sur le ROOTER 2, le réplica du CARP en **BACKUP**.

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.10.252/24	redondancewan	 BACKUP

Nous pouvons maintenant renseigner cette IP VIRUTEL en passerelle par défaut sur les machines de notre parc.

Comme dit précédemment **Pfsense ROOT AUTOMATIQUEMENT** les interface entre elle, c'est pour cela, que grâce a al'interface une redondance **wan** est donc effective, car une root redirige vers l'interface **wan** de **pfsense**.

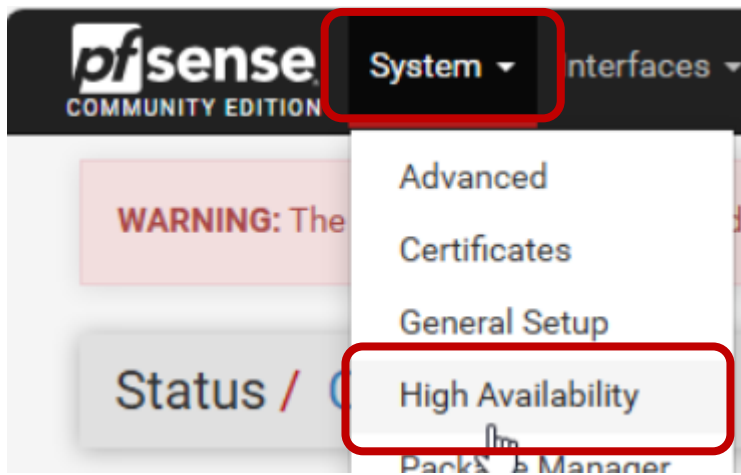
Pour l'interface **DMZ**, suivre les mêmes étapes en prenant en considération le plan réseau pour être en accord avec les attentes sans oublier les règles de firewall.

Configuration du HA (High Availability) sur Pfsense.

Cela va permettre la réplication de la configuration du router 1 vers le router 2.

Pour ce faire suivre les étapes suivante :

Sur le **router 1** se rendre dans :



Puis renseigner la configuration suivante :

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states

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

Synchronize Interface

OPT1

It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
 An IP must be defined on each machine participating in this failover group.
 An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

d03a5d62

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

pfsync Synchronize Peer

192.168.20.253

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

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

192.168.20.252

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

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

Remote System Username

admin

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

Remote System Password

Confirm

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

Synchronize admin

☐ synchronize admin accounts and autoupdate sync password.

SORG Benjamin
ALTUN Yanis

BTS SIO || AP4
58

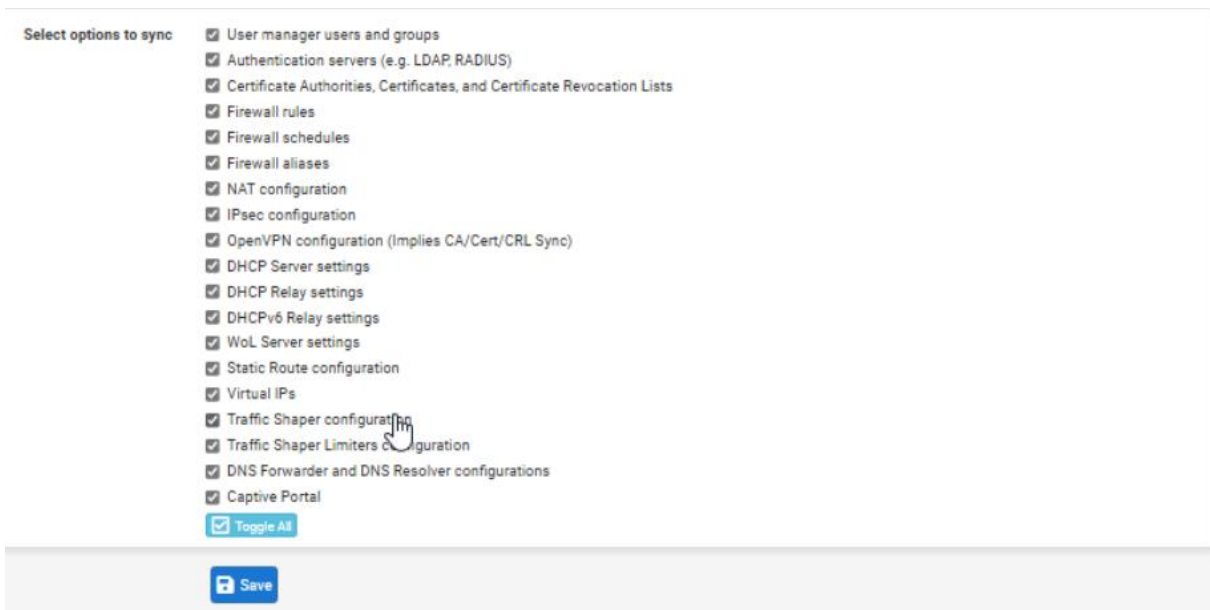
Cocher la case : **PFSYNC**

Nous sélectionnons la deuxième interface que nous avons rajoutée a notre router : **opt1**

Pfsync synchronise peer : **192.168.20.253 (adresse du router 1)**

Synchronize Config to IP : **192.168.20.252 (adresse router 2)**

Renseigner les informations d'un compte administrateur.



Select options to sync

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

☒ Toggle All

Puis sélectionner toutes les options qui auront lieu dans la réplication de configuration.

Sur le **ROOTER 2** :

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

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

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

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

Configuration Synchronization Settings (XMLRPC Sync)

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

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

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

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

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

Select options to sync ☐ User manager users and groups

Cocher la case : **PFSYNC**

Nous sélectionnons la deuxième interface que nous avons rajoutée a notre rooter : **opt1**

Pfsync synchronise peer : **192.168.20.253 (adresse du rooter 1)**

Synchronize Config to IP : **on ne renseigne rien**

Renseigner les informations d'un compte administrateur.

Ne rien cocher en option de réplication :

Select options to sync

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

☒ Toggle All

Une fois cela fait, le **rooter 1** va se répliquer sur le **rooter 2**.

Configuration DMZ

Afin de créer notre DMZ (« Zone démilitarisée » partie isolée du réseau) il va falloir au préalable préparer :

- Une nouvelle carte réseau virtuelle liée directement à la VM PfSense, puis son initialisation sur pfsense avec attribution d'adresse ip v4

Assignez donc l'interface de la nouvelle carte réseau liée à la VM dans PfSense :

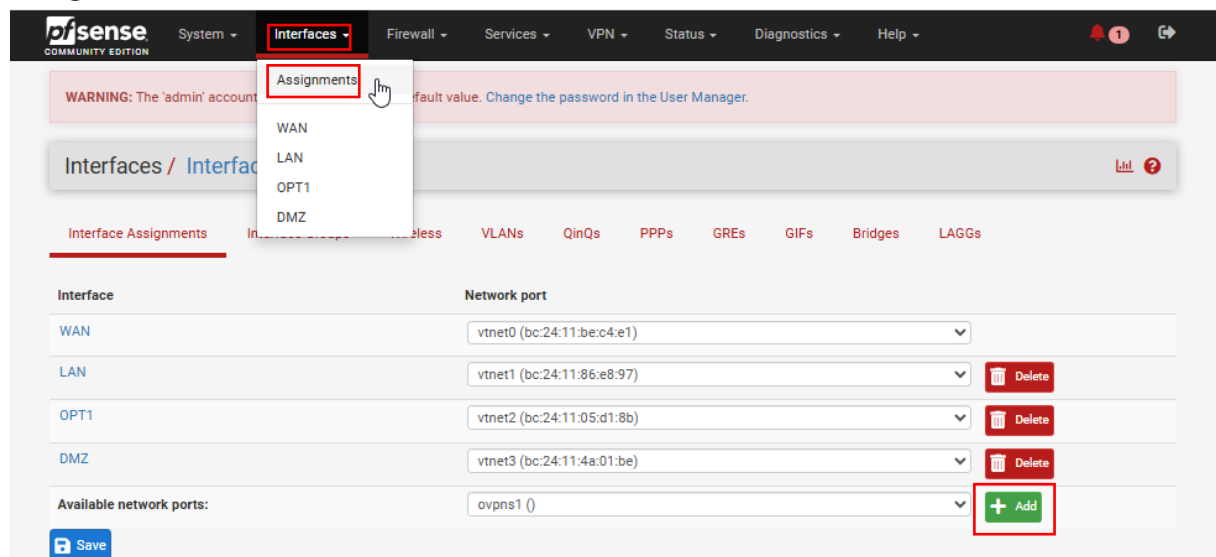
```
12.7.2-RELEASE1[root@pfSense.resicivile.fr]/root: exit
exit
QEMU Guest - Netgate Device ID: 030357f6dcb593f39b12

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.158/24
                v6/DHCP6: 2001:861:4f42:ade0:be24:11ff:febe:c4
/64
LAN (lan)      -> vtnet1      -> v4: 192.168.2.254/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.4.1/24
DMZ (opt2)     -> vtnet3      -> v4: 192.168.3.1/24

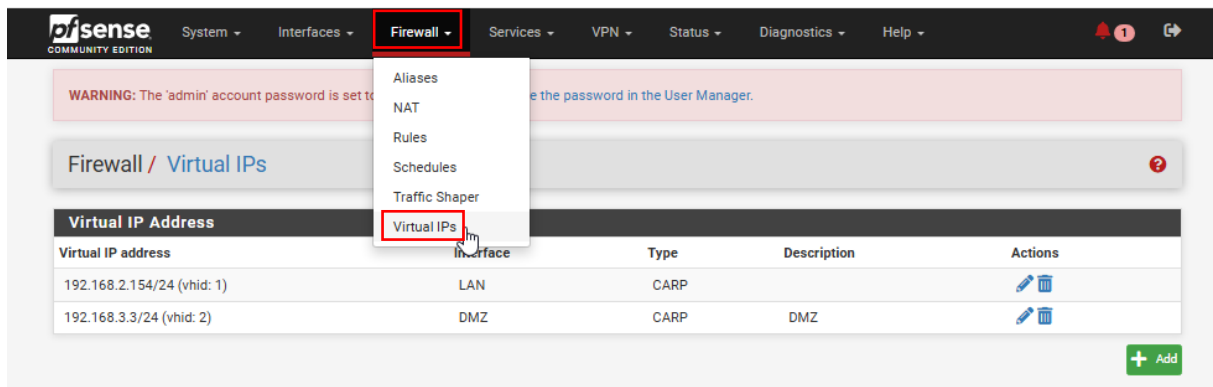
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable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

Ensuite rendez vous sur l'interface d'administration de PfSense puis dans « Interfaces > Assignments » :



Cliquez ensuite sur « Add » pour ajouter une nouvelle. Nommez là et assignez lui une interface réseau que nous avons préconfigurée sur la machine.

Une fois que c'est fait, rendez-vous sur « Firewall < Virtual IP's » puis cliquez sur « Add » :

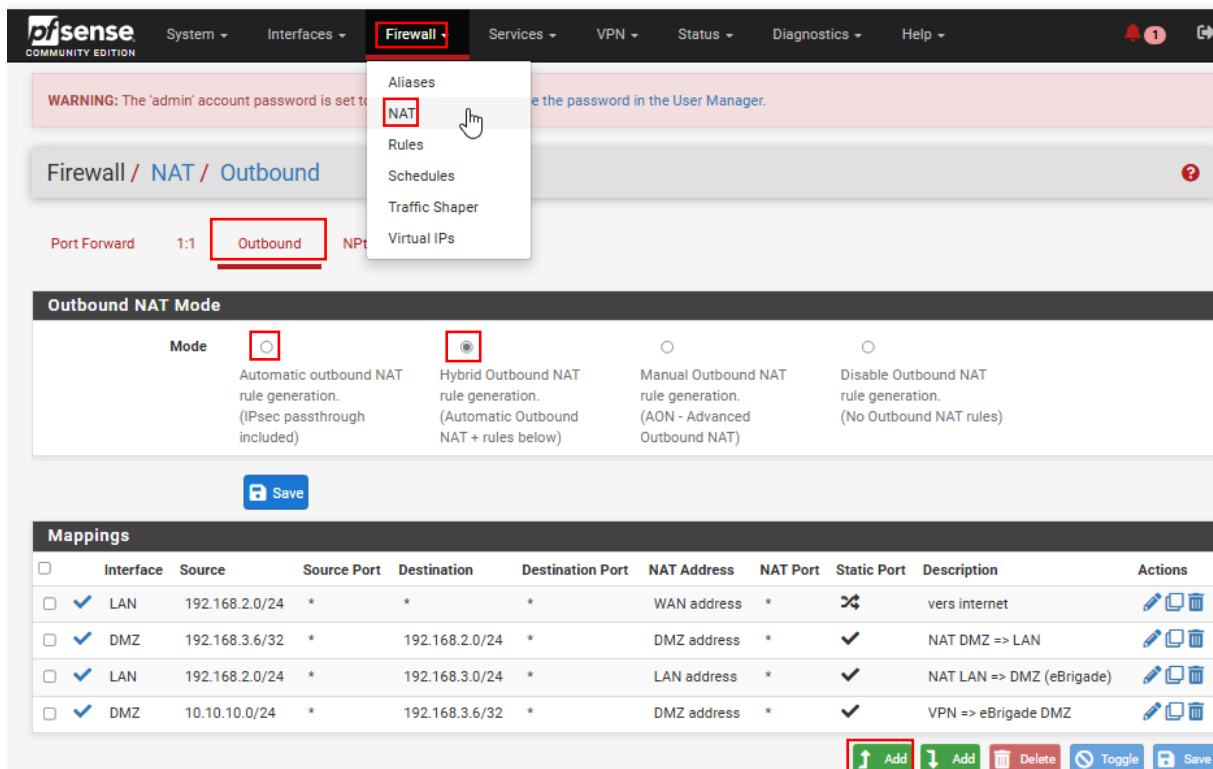


Choisissez ensuite la plage réseau qu'aura votre DMZ, il s'agit ici de sélectionner un vlan différent de celui sur lequel votre infrastructure est montée. Le protocole utilisé sera donc le CARP (Common Address Redundancy Protocol) qui permet à un hôte de segmenter une partie de son flux pour le rediriger vers un autre vlan et assurer la connectivité via une ip virtuelle.

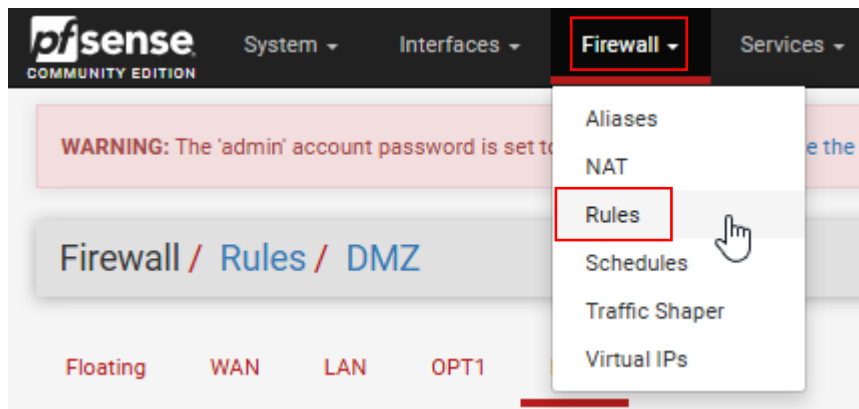
A partir de cette étape, vous avez deux choix :

- Utiliser le routage automatique de PfSense qui garantit une route entre chaque réseaux segmentés afin d'en assurer la communication.
- Utiliser le routage hybride incluant la création de règles de routage à la main.

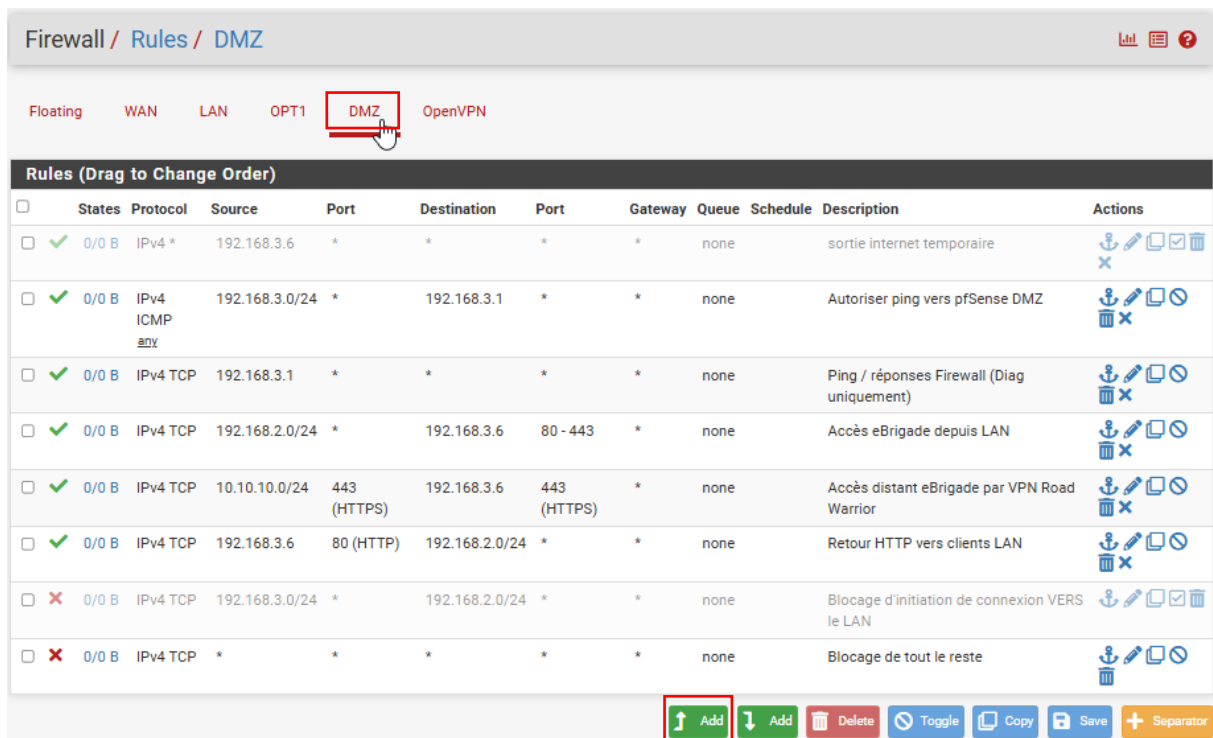
Rendez-vous sur « Firewall < NAT » puis choisissez « Hybrid Outbound NAT » ou « Automatic NAT rules generation »



Pour finir sur la DMZ, il va falloir ensuite créer les règles de Pare-Feu afin de sécuriser les communications entrantes et sortantes de la DMZ. Rendez-vous sur « Firewall < Rules » :




Il faut ensuite sélectionner l'interface « DMZ » et ajouter manuellement les règles que vous trouverez sur la capture suivante :



Installation de eBrigade :

Pour installer cette application web, il vous faut avant tout télécharger un exemplaire de son répertoire. Dans notre cas, un fichier compressé nous a été transmis :

 ebrigade-5.3.2.zip

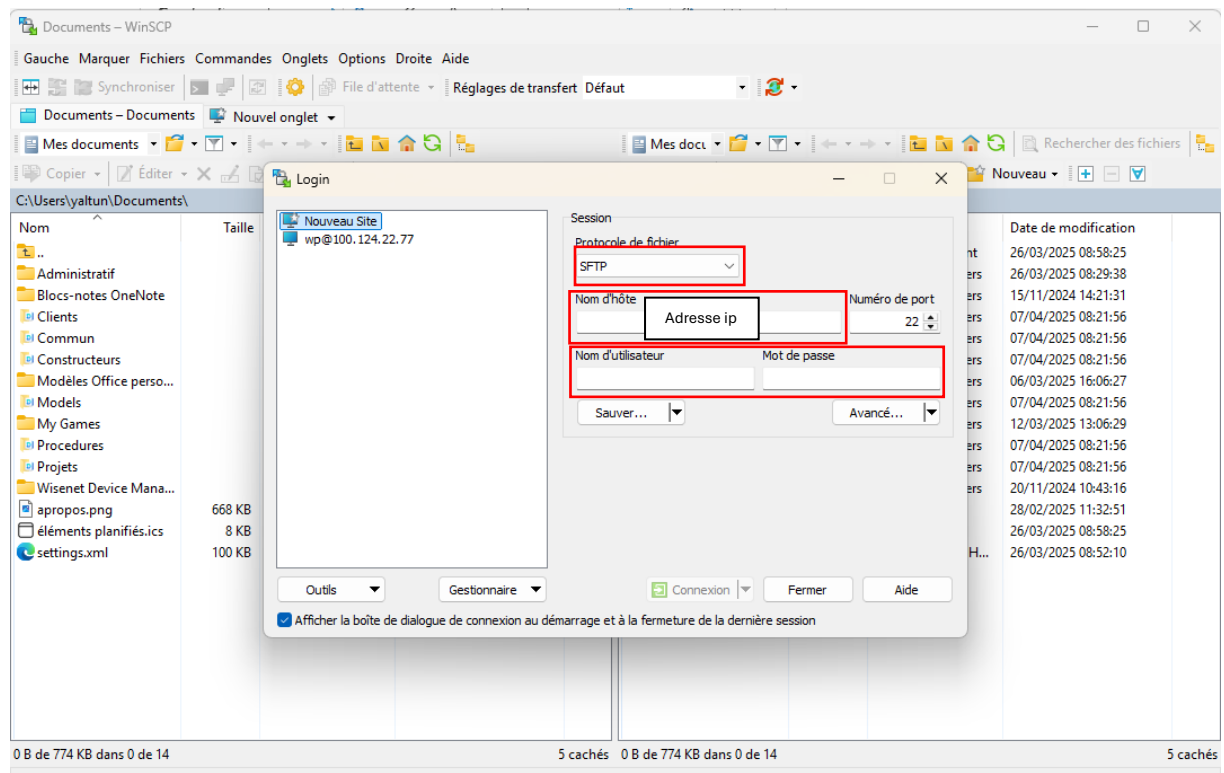
Il faut donc le décompresser et transférer son contenu sur la machine virtuelle qui contiendra l'application.

Créez une machine virtuelle sous Debian 12 avec minimum 2 Go de RAM et 2 cœurs de processeur attribués. Procédez à l'installation du système puis une fois arrivé sur l'interface GUI ou CLI :

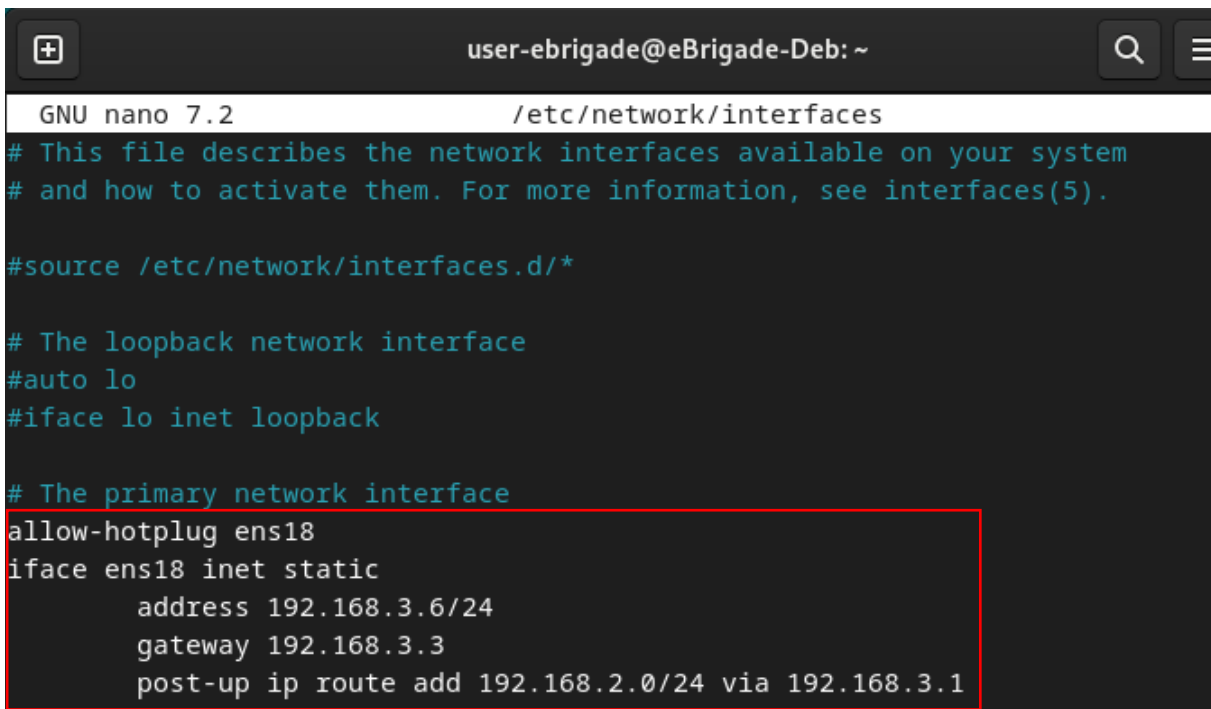
- Ouvrez un terminal, faites « su - » puis renseignez votre mot de passe root afin d'avoir tous les droits.
- Tapez « apt update && apt upgrade -y » pour mettre à jour les paquets de votre installation neuve.
- Tentez de passer votre machine virtuelle dans un réseau privé type Tailscale afin de pouvoir transférer des fichiers depuis un poste local :

(`curl -fsSL https://tailscale.com/install.sh | sh`)

Téléchargez ensuite le logiciel WinSCP afin d'initier une connexion avec votre hôte distant (Machine Debian) en protocole SFTP. Renseignez votre utilisateur et votre mot de passe de l'hôte distant puis sélectionnez le chemin que vous voulez.



- Installez sur la machine Debian les dépendances nécessaires à eBrigade : « *sudo apt install apache2 mariadb-server php php-mysql php-gd php-xml php-mbstring php-curl unzip -y* » (A SAVOIR QUE EBRIGADE FONCTIONNE SUR PHP JUSQU'À LA VERSION 7.4)
- Faites un « *nano /etc/network/interfaces* » et modifiez votre interface réseau (la même que la DMZ et une adresse dans la plage du network DMZ créé précédemment) :



```

GNU nano 7.2 /etc/network/interfaces
# 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 ens18
iface ens18 inet static
    address 192.168.3.6/24
    gateway 192.168.3.3
    post-up ip route add 192.168.2.0/24 via 192.168.3.1

```

Ensuite, initiez la configuration sécurisée d'une base de donnée sous MariaDB :

« *mysql_secure_installation* »

Puis connectez vous à la base de données grâce aux accès créés :

« *mysql -u root -p* »

Ensuite, nous allons utiliser le langage SQL afin d'ordonner à la base de données de créer une table et un utilisateur (avec des droits privilégiés) :

« *CREATE DATABASE ebrigade_db CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;*

CREATE USER 'ebrigade_user'@'localhost' IDENTIFIED BY 'MotDePasseFort123!';

GRANT ALL PRIVILEGES ON ebrigade_db. TO 'ebrigade_user'@'localhost';*

FLUSH PRIVILEGES;

EXIT; »

Déploiement de l'application :

Il faut ensuite transférer l'intégralité du fichier décompressé dans un répertoire attribué à sa fonction : `/var/www/html/ebrigade` puis modifier les droits de lecture/écriture sur le répertoire :

```
« mv /home/user/ebrigade /var/www/html/ebrigade
```

```
chown -R www-data:www-data /var/www/html/ebrigade
```

```
chmod -R 755 /var/www/html/ebrigade »
```

Création d'un hôte virtuel : il faut ici créer un fichier `ebrigade.conf` afin d'y renseigner des variables d'identification et de localisation : « `nano /etc/apache2/sites-available/ebrigade.conf` »

Le fichier en question devra contenir :

```
« <VirtualHost *:80>
```

```
    ServerAdmin admin@resicivile.fr
```

```
    DocumentRoot /var/www/html/ebrigade
```

```
    ServerName ebrigade.local
```

```
<Directory /var/www/html/ebrigade>
```

```
    AllowOverride All
```

```
    Require all granted
```

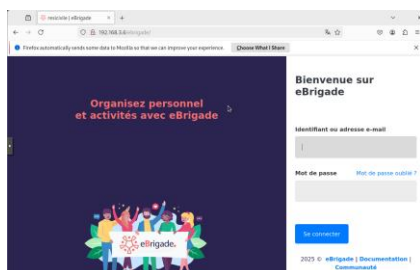
```
</Directory>
```

```
    ErrorLog ${APACHE_LOG_DIR}/ebrigade_error.log
```

```
    CustomLog ${APACHE_LOG_DIR}/ebrigade_access.log combined
```

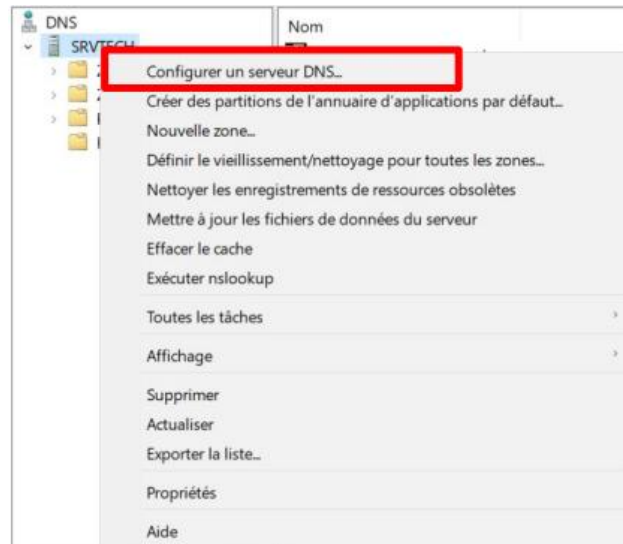
```
</VirtualHost> »
```

Puis se rendre sur un navigateur et taper l'adresse ip de la machine (ou la dénomination DNS si vous l'avez déjà créée) afin de débiter l'installation Web. A la fin, vous obtiendrez ce résultat :



Procédure Hmailserver

Etape 1 : Configuration DNS



Sélectionnez une action de configuration

Vous pouvez sélectionner les types de zones de recherche appropriés à la taille de votre réseau. Les administrateurs avancés peuvent configurer des indications de racine.



Sélectionnez l'action que vous voulez que l'Assistant effectue :

- ☒ Créer une zone de recherche directe (recommandé pour les petits réseaux)
Ce serveur fait autorité pour les noms DNS des ressources locales mais transfère toutes les autres requêtes vers un fournisseur de services Internet ou d'autres serveurs DNS. L'Assistant va configurer les indications de racine mais ne créera aucune zone de recherche inversée.
- ☐ Créer des zones de recherche directe et inversée (pour les grands réseaux)
Ce serveur peut faire autorité sur les zones de recherche directe et inversée. Il peut être configuré pour effectuer des résolutions récursives, pour transférer des requêtes à d'autres serveurs DNS, ou les deux. L'Assistant configurera les pointeurs de serveurs racine.
- ☐ Configurer les indications de racine uniquement (réservé aux utilisateurs expérimentés)
L'Assistant ne va configurer que les indications de racine. Vous pourrez configurer ultérieurement les zones de recherche directe et inversée et les redirections.

< Précédent

Suivant >

Annuler

Assistant Configuration d'un serveur DNS



Emplacement du serveur principal

Vous pouvez choisir où s'effectue la maintenance de vos données DNS pour vos ressources réseau.



Quel serveur DNS assure la maintenance de votre zone de recherche directe principale ?

- ☒ Ce serveur assure la maintenance de la zone
Cet Assistant vous aidera à créer une zone de recherche directe principale.
- ☐ Un fournisseur de services Internet gère la zone, et une copie secondaire en lecture seule réside sur ce serveur
Cet Assistant vous aidera à créer une zone de recherche directe secondaire.

< Précédent

Suivant >

Annuler

Attribuer un nom pour la nouvelle zone

Assistant Nouvelle zone

Nom de la zone
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :
mailtech.local

< Précédent **Suivant >** Annuler

Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☐ Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☒ Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent **Suivant >** Annuler

Renseigner les adresse 1.1.1.1 et 8.8.8.8

Assistant Configuration d'un serveur DNS

Redirecteurs
Les redirecteurs sont des serveurs DNS vers lesquels ce serveur envoie les requêtes auxquelles il ne peut pas répondre.

Ce serveur DNS doit-il rediriger des requêtes ?

☒ Oui, il doit rediriger les requêtes vers les serveurs DNS ayant les adresses IP suivantes :

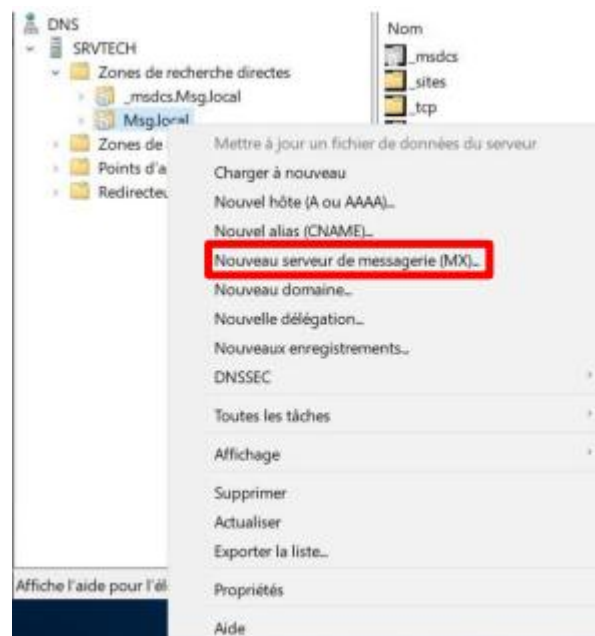
Adresse IP	Nom de domaine co...	Validé
Cliquez ici pour ajouter une adresse IP ou un nom DNS		
1.1.1.1	<Tentative de résolu...	Validation en cours...
8.8.8.8	<Tentative de résolu...	Validation en cours...

☐ Non, il ne doit pas rediriger les requêtes
Si ce serveur n'est pas configuré pour utiliser des redirecteurs, il peut toujours résoudre des noms en utilisant des serveurs de noms racines.

< Précédent **Suivant >** Annuler



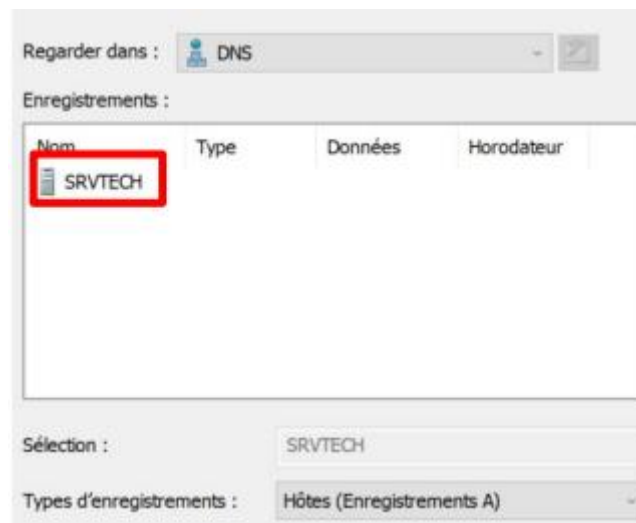
Cliquer terminer



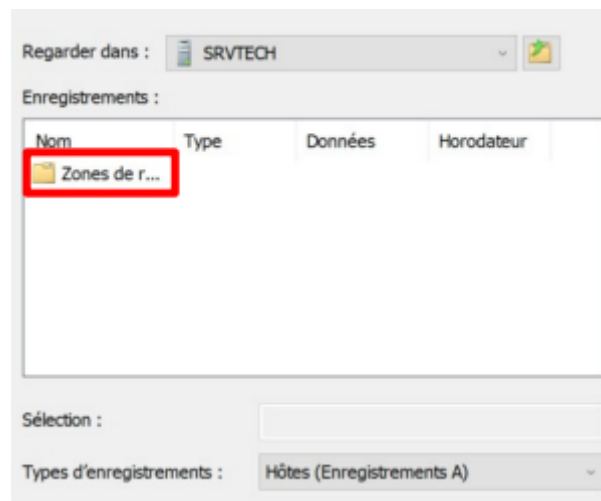
Faire un clic droit sur notre dossier Msg.local puis choisir nouveau serveur de messagerie (MX)



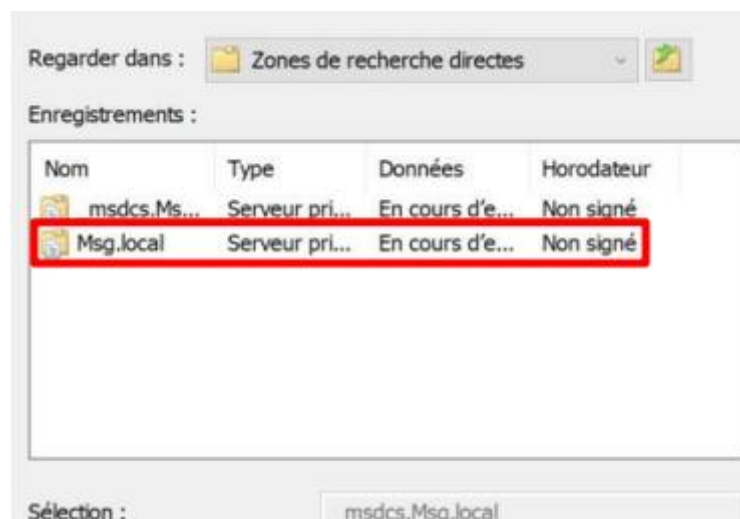
Dans nom de domaine choisir parcourir puis suivez les étapes



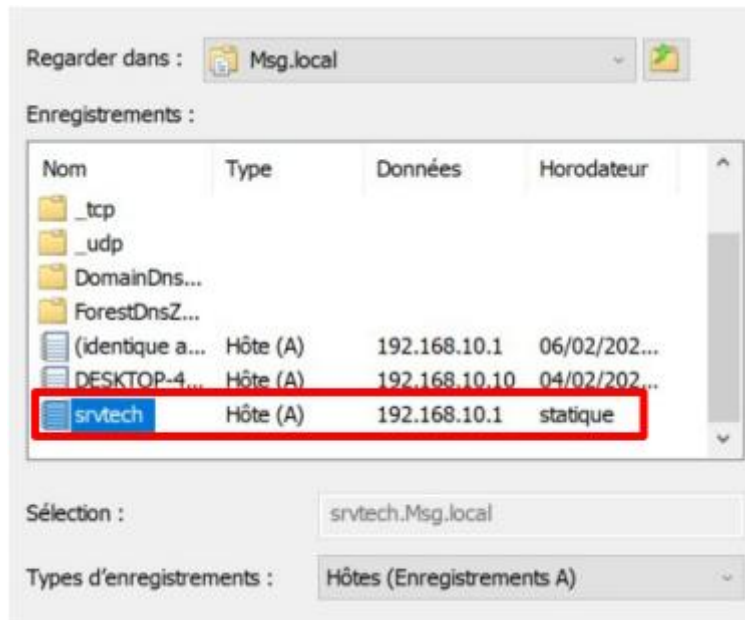
Cliquer sur le nom



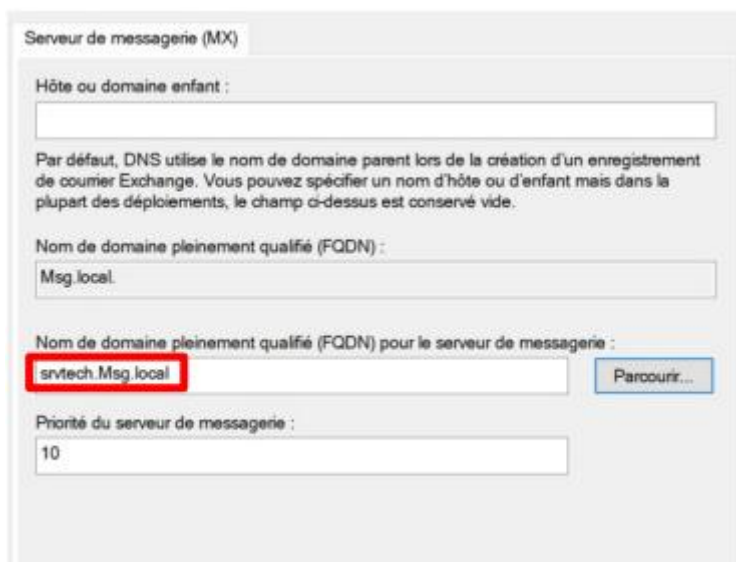
Cliquer sur le dossier



Cliquer sur le dossier Msg.local



Cliquer sur le nom du serveur

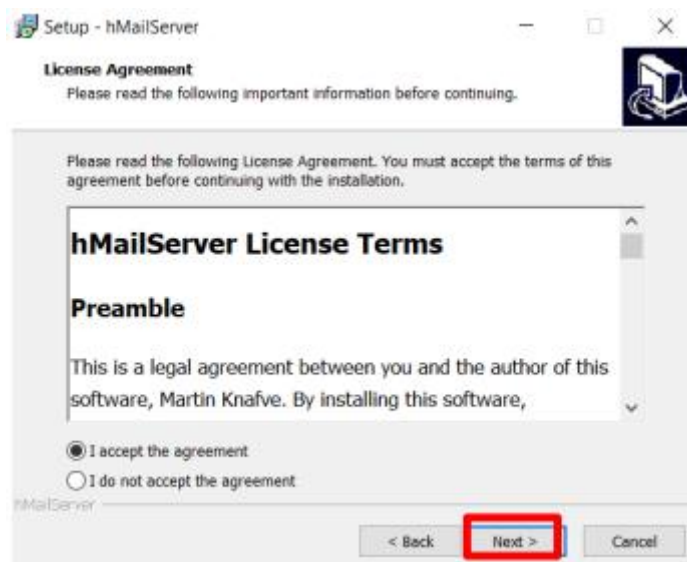


Cliquer sur terminer pour valider

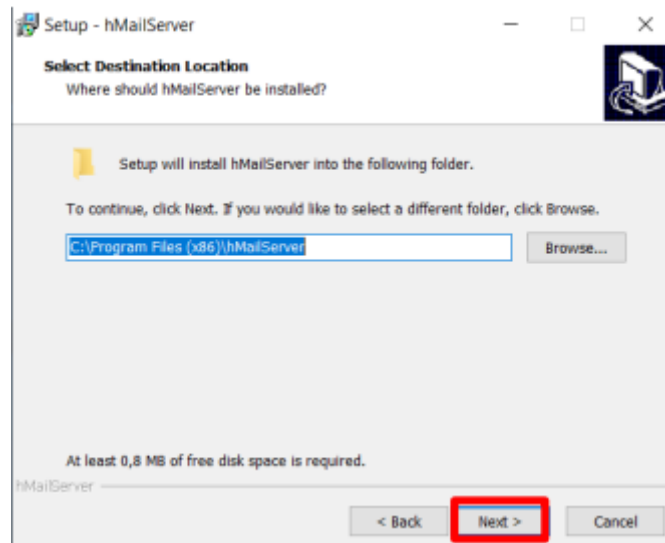
Etape 2 : Installation de hmail server



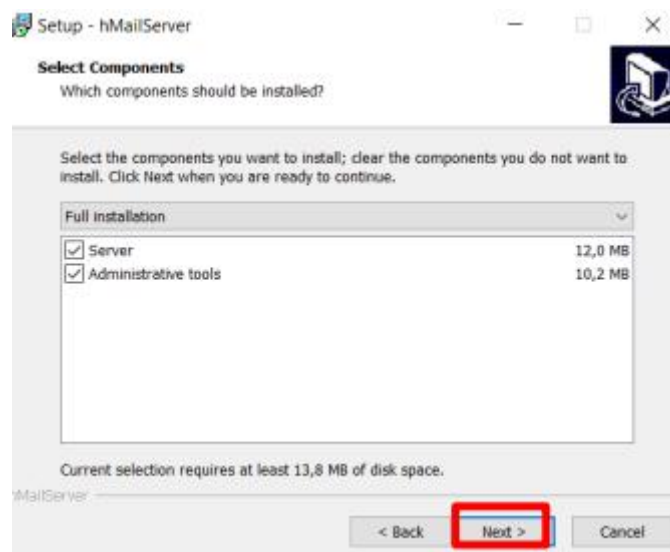
Next



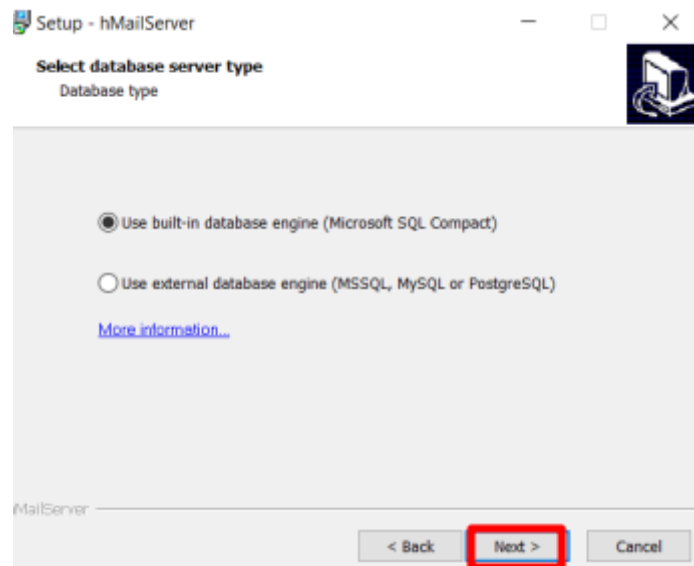
Next



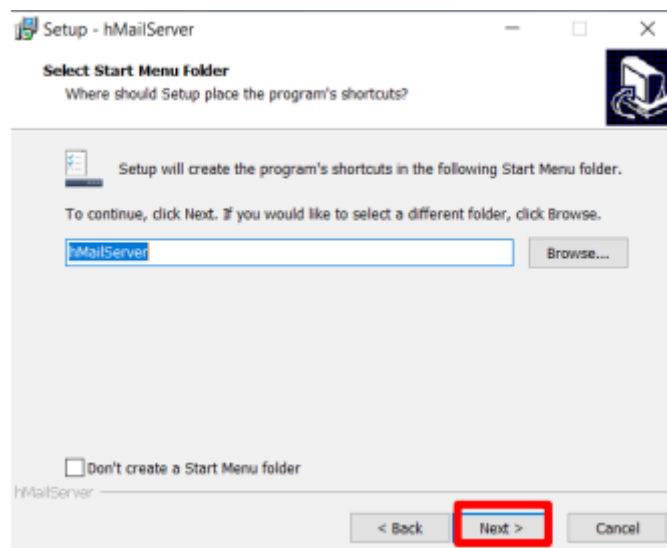
Next



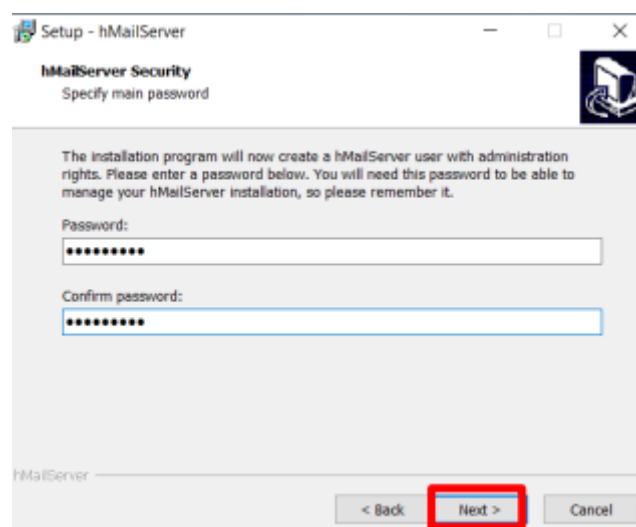
Next



Next

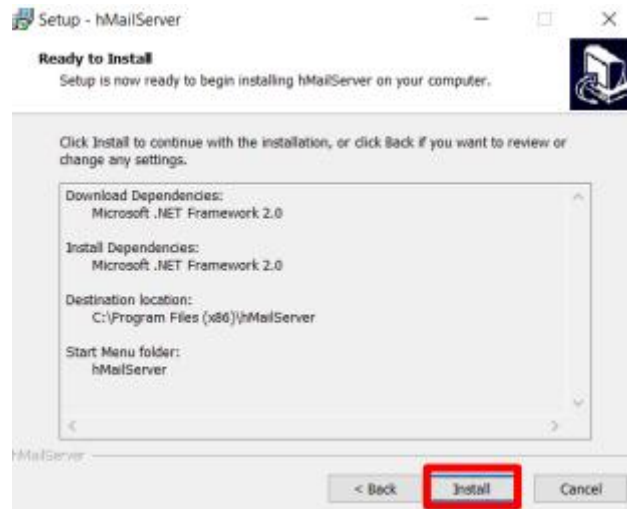


Next

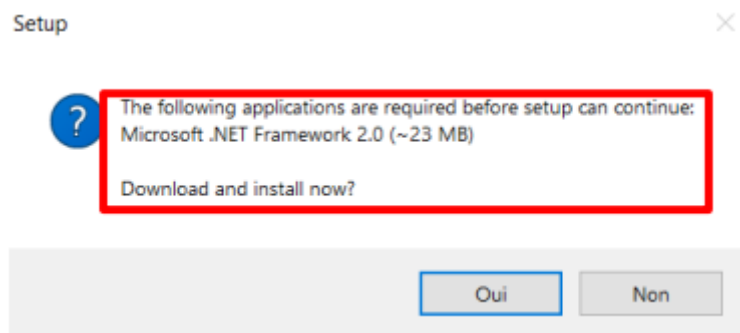


RENSEIGNER
MOT DE PASSE
ADMINISTRATE
UR DE
HMAILSERVER

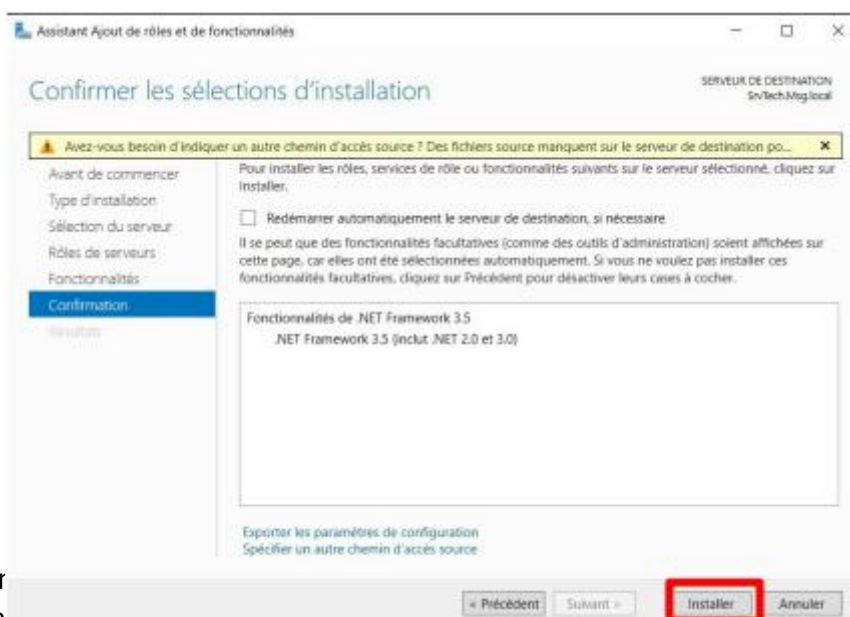
Next



Install



L'exécutable nous demande d'installer le Framework Microsoft .net 2.0 on va donc se rendre dans notre gestionnaire de serveur et ajouter des rôles et des fonctionnalités

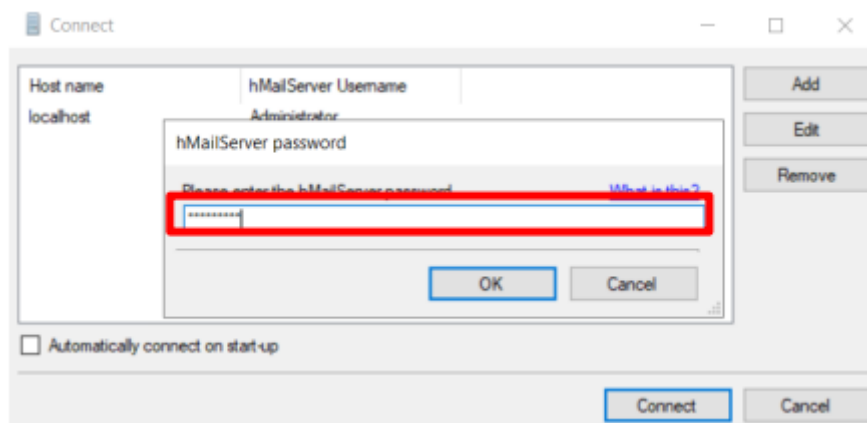


Si erreur, passer par l'invité de commande et renseigner la commande suivante :

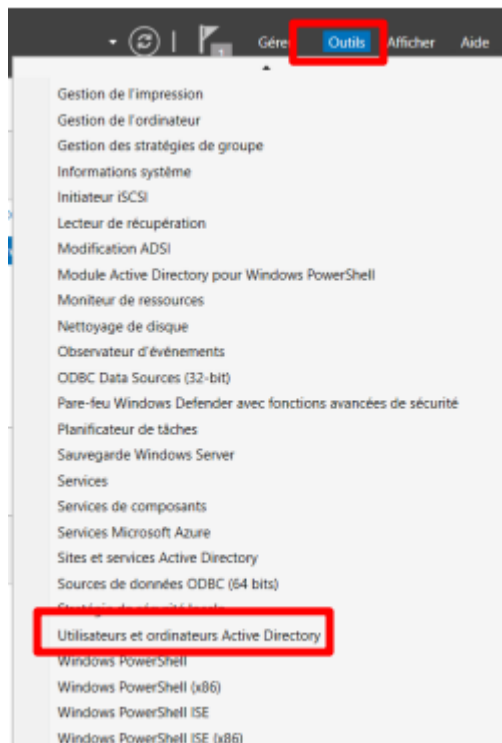
```
Console

Dism /online /enable-feature /featurename:NetFx3 /All
```

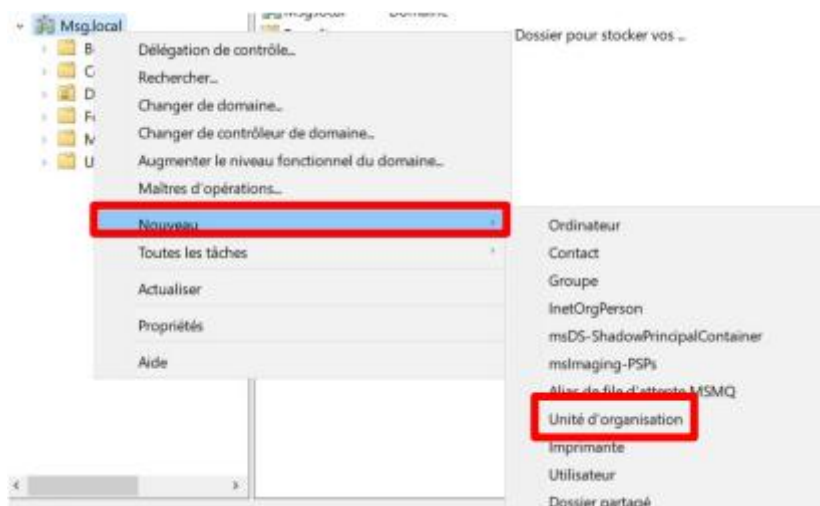
Après l'installation on va pouvoir relancer l'installation de hmailserver.



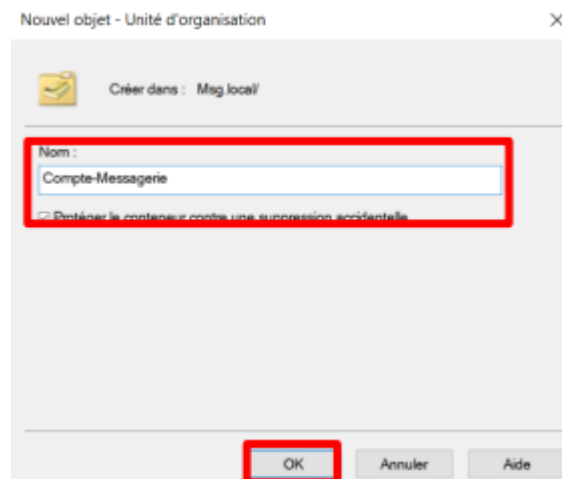
A la fenêtre de connexion de Hmailserver, renseigner le MDP admin rentrer précédemment



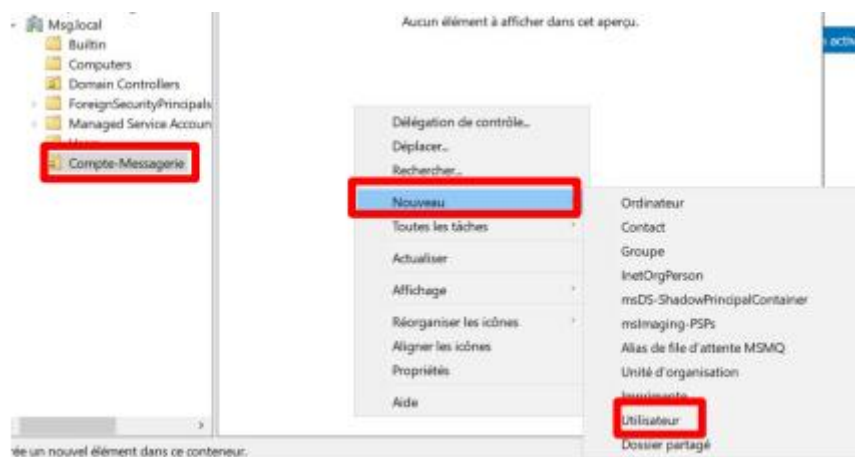
Créer deux comptes utilisateur qu'on va ajouter par la suite sur hmailserver



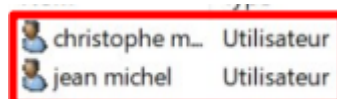
On va créer une nouvelle unité d'organisation

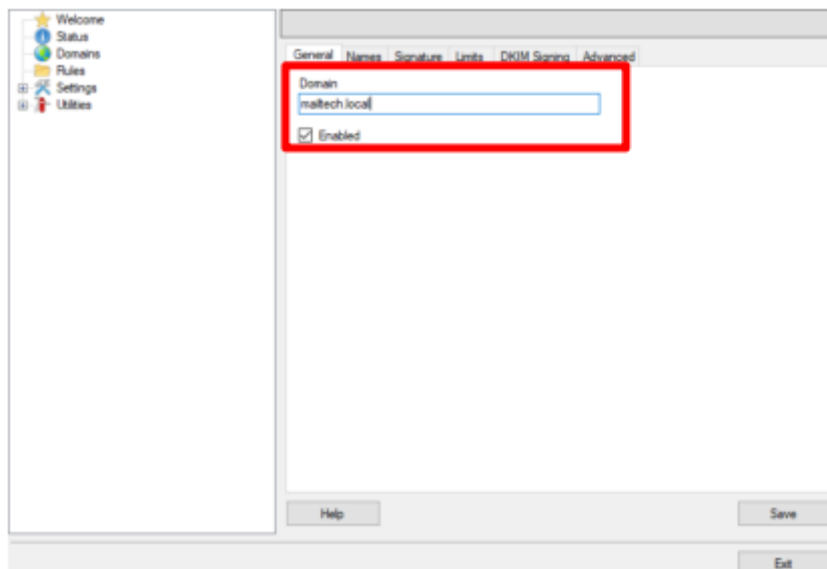


Ok après avoir définis un nom



On se rend ensuite dans notre nouvelle unité d'organisation et on va créer deux comptes

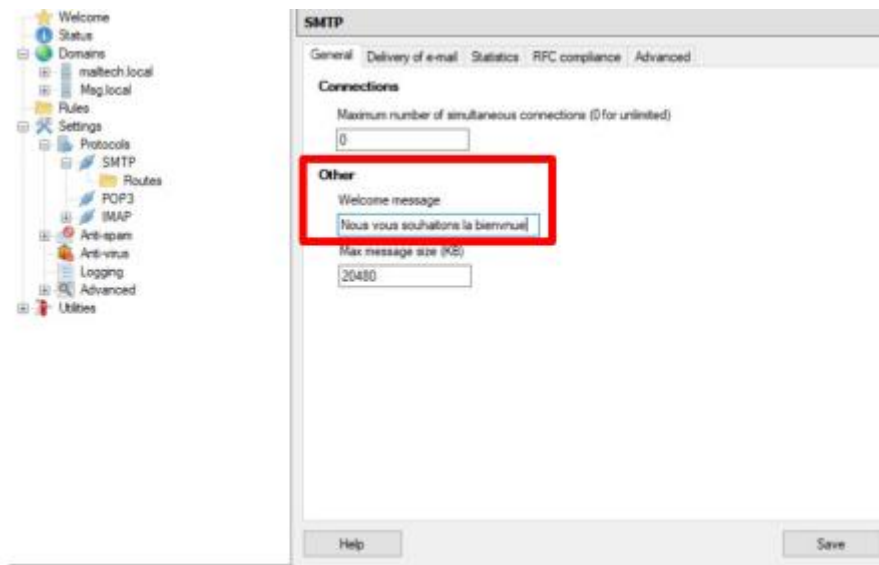




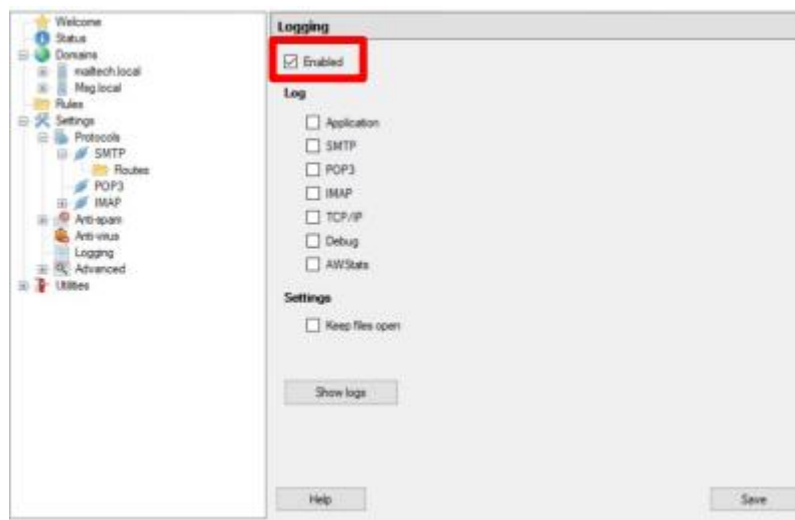
Après s'être connecter on va ajouter le domaine pour le mail, puis notre domaine créer sur le serveur.



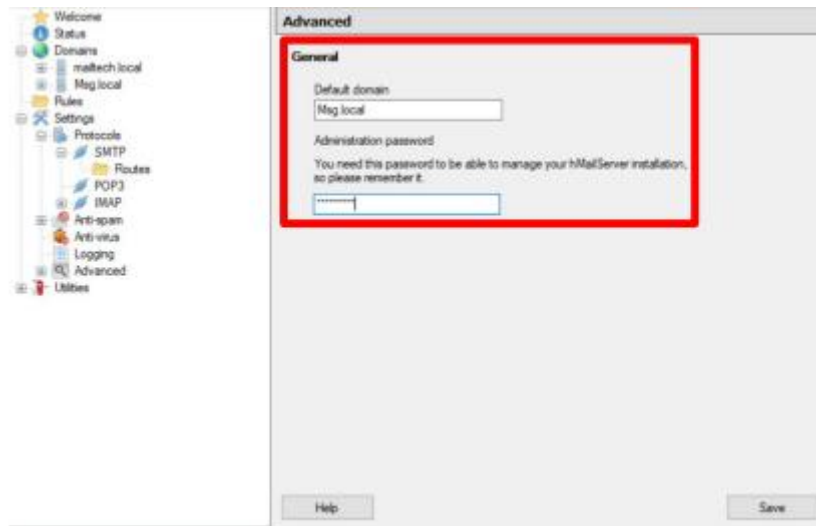
Deux domaines ont été ajouté on va maintenant tout paramétrer



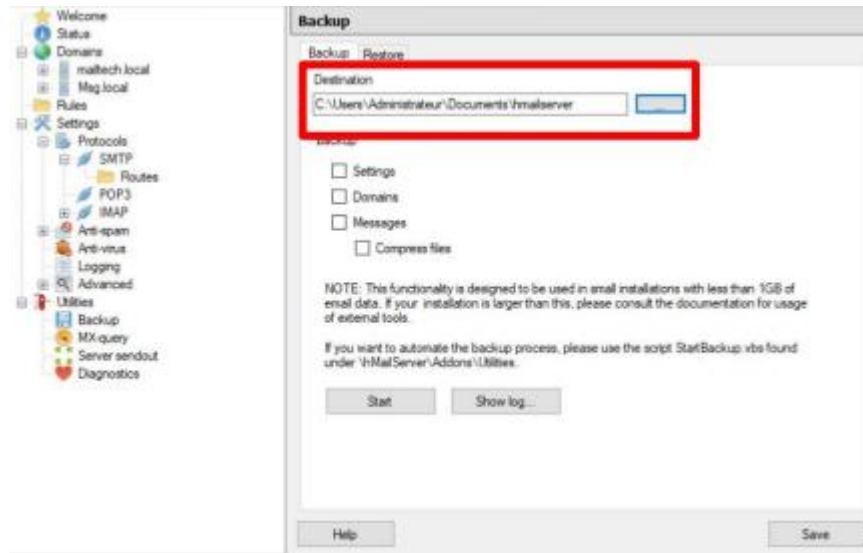
Pour la configuration SMTP laisser par défaut, vous pouvez ajouter un message de bienvenue Puis sauvegarder les paramètres SMTP Le paramètre anti-spam et anti-virus on n'y touche pas On va configurer le paramètre logging



Pour la partie logging on va simplement cocher la case Enabled

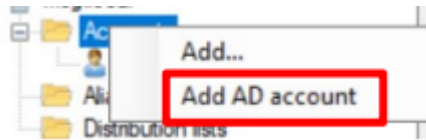


La partie advanced, on va mettre le domaine et le mot de passe de hmailserver administrator puis on sauvegarde

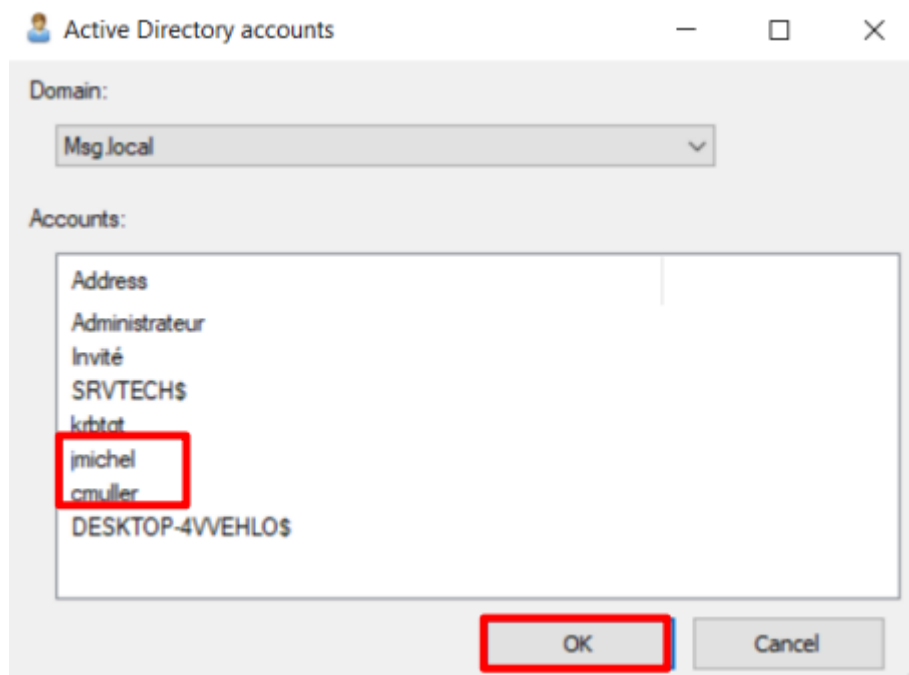


Dans la partie backup on va choisir un emplacement pour la sauvegarde

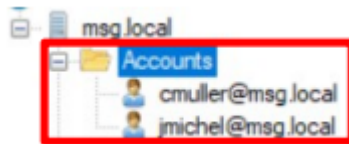
Dans la partie diagnostic on peut vérifier notre diagnostic de notre serveur Après avoir fait le tour des paramètres, on va ajouter nos deux utilisateurs Pour ce faire il faut se rendre dans, dans notre domaine, puis accounts et ajouter nos deux utilisateurs depuis l'active directory



On clique droit sur Accounts puis ADD AD account



Dans le menu déroulant on va choisir le domaine Msg.local et choisir nos deux utilisateurs



Nos deux utilisateurs sont ajoutés

Etape 3 : Installer thunderbird

Après avoir installé Thunderbird il faut se connecter avec un compte qui a été ajoutés

Avertissement !

Paramètres du courrier entrant :

msg.local n'utilise pas de chiffrement.

Les serveurs de courrier non sécurisés n'utilisent pas de connexions chiffrées pour protéger vos mots de passe et vos informations privées. En vous connectant à ce serveur, vous pourriez exposer votre mot de passe et vos informations privées.

Paramètres du courrier sortant :

msg.local n'utilise pas de chiffrement.

Les serveurs de courrier non sécurisés n'utilisent pas de connexions chiffrées pour protéger vos mots de passe et vos informations privées. En vous connectant à ce serveur, vous pourriez exposer votre mot de passe et vos informations privées.

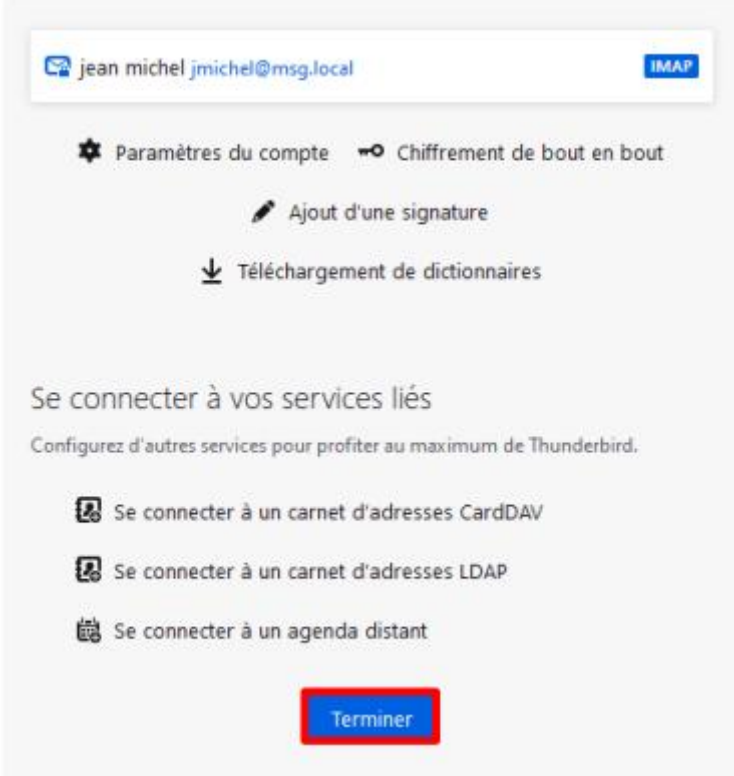
Thunderbird peut vous permettre d'accéder à vos courriels en utilisant les configurations fournies. Cependant, vous devriez contacter votre administrateur ou votre fournisseur de messagerie au sujet de ces connexions incorrectes. Consultez la [FAQ de Thunderbird](#) pour plus d'informations.

☒ Je comprends les risques

Modifier les paramètres

Confirmer

Cocher la case « je comprends les risques » puis cliquer sur confirmer



The screenshot shows the Thunderbird account configuration window for the email address 'jean michel jmichel@msg.local'. At the top, there is a header bar with the email address and an 'IMAP' button. Below this, there are several settings options: 'Paramètres du compte' (Account Settings), 'Chiffrement de bout en bout' (End-to-end encryption), 'Ajout d'une signature' (Add signature), and 'Téléchargement de dictionnaires' (Download dictionaries). A section titled 'Se connecter à vos services liés' (Connect to your linked services) contains three options: 'Se connecter à un carnet d'adresses CardDAV', 'Se connecter à un carnet d'adresses LDAP', and 'Se connecter à un agenda distant'. At the bottom of the window, there is a blue 'Terminer' (Finish) button.

Procédure Zabbix

1^{ère} étape : ajout du référentiel Zabbix pour Debian 12

- Connectez-vous en SSH à votre machine Debian qui servira de serveur Zabbix
- Saisissez les commandes suivantes :

wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-1+debian12_all.deb

```
root@debian-master:~# wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-1+debian12_all.deb
--2024-06-23 13:50:20-- https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-1+debian12_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com): 178.128.6.101, 2604:a890:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)[178.128.6.101]:443_ connecté.
requête HTTP transmise, en attente de la réponse_ 200 OK
Taille : 5820 (5,7K) [application/octet-stream]
Sauvegarde en : « zabbix-release_7.0-1+debian12_all.deb »

zabbix-release_7.0-1+debian12_all.deb 100%[=====] 5,68K --KB/s ds 0s
2024-06-23 13:50:21 (369 MB/s) - « zabbix-release_7.0-1+debian12_all.deb » sauvegardé [5820/5820]
```

dpkg -i zabbix-release_7.0-1+debian12_all.deb

```
root@debian-master:~# dpkg -i zabbix-release_7.0-1+debian12_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 33740 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_7.0-1+debian12_all.deb ...
Dépaquetage de zabbix-release (1:7.0-1+debian12) ...
Paramétrage de zabbix-release (1:7.0-1+debian12) ...
```

2^{ème} étape : installation des paquets ZABBIX

- Saisissez la commande suivante :

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y

3^{ème} étape : installation de mariaDB

- Saisissez la commande suivante :

apt install mariadb-server -y

4^{ème} étape : création de la base de données et de l'utilisateur Zabbix

- Saisissez les commandes suivantes :

Accès à mariaDB (en tant que "root" ici) :

mysql -u root

Création de la base de données "Zabbix" :

```
create database zabbix character set utf8mb4 collate utf8mb4_bin;
```

Création de l'utilisateur "Zabbix" avec le mot de passe "password" :

```
create user zabbix@localhost identified by 'password';
```

Élévation des privilèges pour l'utilisateur "Zabbix" et sortie :

```
grant all privileges on zabbix.* to zabbix@localhost; set global  
log_bin_trust_function_creators = 1; quit
```

5^{ème} étape : importation du schéma de la base de données créée

- Saisissez la commande suivante :

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-  
set=utf8mb4 -uzabbix -p zabbix
```

Lorsque demandé, saisissez le mot de passe "password" et patientez pendant l'initialisation (cela peut prendre plusieurs minutes).

6^{ème} étape : désactivation de la fonction "log_bin_trust_function_creators" dans mariaDB

- Saisissez les commandes suivantes :

```
mysql -u root  
set global log_bin_trust_function_creators = 0; quit
```

7^{ème} étape : configuration de la base de données pour le serveur Zabbix

- Saisissez la commande suivante :

```
nano /etc/zabbix/zabbix_server.conf
```

- Modifiez la rubrique « **Option : DBPassword** » en décommentant la ligne **#DBPassword**

```
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=
```

- Saisissez le mot de passe comme ci-dessous :

```
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
```

Quittez et enregistrez les modifications dans le fichier : **CTRL + X --- O** et « **Entrée** »

8^{ème} étape : démarrage et activation des processus Zabbix

- Saisissez les commandes suivantes :

```
systemctl restart zabbix-server zabbix-agent apache2 systemctl enable zabbix-
server zabbix-agent apache2
```

Votre serveur Zabbix est prêt. Il faut maintenant lancer un navigateur web afin d'accéder à l'interface web de gestion du serveur Zabbix :

- Dans un onglet du navigateur, saisissez l'adresse « Red » (votre WAN) suivie de **/zabbix** comme ceci :

http://ip_machineDebian/zabbix

Si vous n'accédez pas à l'interface web de Zabbix, assurez-vous de bien avoir le port « 80 » sur votre routeur IPFIRE et d'avoir créé une règle DNAT vers votre machine Debian Zabbix (voir tutoriels sur notre site ou notre chaîne en cas de problème).

L'assistant de configuration de Zabbix se lance (en mode web) pour terminer l'installation ; cliquez le bouton « **Prochaine étape** » :



Si les étapes de l'installation se sont bien déroulées, Zabbix affiche la fenêtre suivante :

ZABBIX

Vérification des prérequis

	Valeur actuelle	Requis	
Version de PHP	8.2.20	8.0.0	OK
Option PHP "memory_limit"	128M	128M	OK
Option PHP "post_max_size"	16M	16M	OK
Option PHP "upload_max_filesize"	2M	2M	OK
Option PHP "max_execution_time"	300	300	OK
Option PHP "max_input_time"	300	300	OK
support de bases de données par PHP	MySQL		OK
bcmath pour PHP	actif		OK
mbstring pour PHP	actif		OK
Option PHP "mbstring.func_overload"	inatif	inatif	OK

Retour
Prochaine étape

- Cliquez le bouton bleu « **Prochaine étape** » et complétez la configuration de la connexion :



Configurer la connexion à la base de données

Veillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

Type de base de données

Hôte base de données

Port de la base de données 0 - utiliser le port par défaut

Nom de la base de données

Stocker les informations d'identification dans

Utilisateur

Mot de passe

Chiffrement TLS de la base de données *La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).*

- Complétez les paramètres et cliquez le bouton « **Prochaine étape** » :

ZABBIX

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

Paramètres

Nom du serveur Zabbix

Fuseau horaire par défaut

Thème par défaut

- Testez vos paramètres en cliquant le bouton « **Prochaine étape** » :

ZABBIX

Résumé pré-installation

Veillez vérifier les paramètres de configuration. Si tout est correct, appuyez sur le bouton "Prochaine étape" ; sinon, le bouton "Retour" pour changer les paramètres.

Type de base de données	MySQL
Serveur base de données	localhost
Port de la base de données	défaut
Nom de la base de données	zabbix
Utilisateur base de données	zabbix
Mot de passe utilisateur de la base de données	*****
Chiffrement TLS de la base de données	false
Nom du serveur Zabbix	ZABBIX

Retour

Prochaine étape

Si tous les paramètres sont corrects, Zabbix affiche ceci ; cliquez le bouton « **Terminer** »

ZABBIX

Installer

Félicitations ! Vous avez installé l'interface Zabbix avec succès.

Fichier de configuration "conf/zabbix.conf.php" créé.

Retour

Terminé

La fenêtre d'identification à l'interfacedegestion de Zabbix s'affiche :

ZABBIX

Nom d'utilisateur

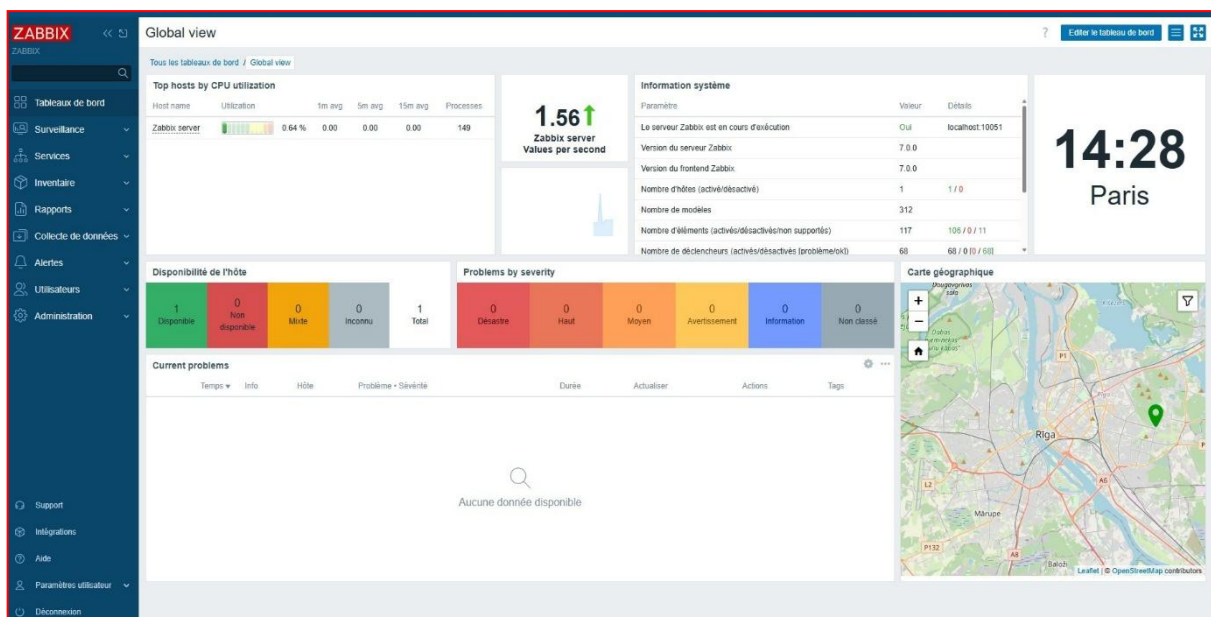
Mot de passe

☒ Me rappeler toutes les 30 jours

S'enregistrer

- Saisissez le nom d'utilisateur par défaut : « **Admin** » (avec le **A en majuscule**)
- Saisissez le mot de passe par défaut « **zabbix** » (en minuscules)
- Cliquez le bouton « **S'enregistrer** »

Une fois identifié, le Tableau de Bord ZABBIX s'affiche



3 – AJOUTER UN HÔTE LINUX DANS ZABBIX 7.0 (LTS)

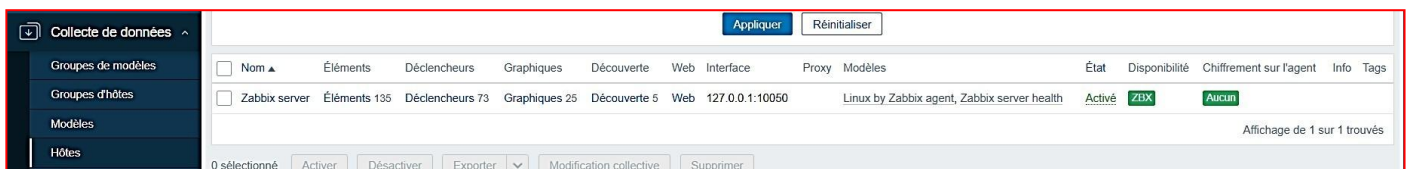
Dans cette partie **nous allons ajouter un nouvel hôte, de manière « manuelle », dans Zabbix**. Pour cela, nous avons créé une nouvelle machine virtuelle Debian 12.5. Cette machine a été connectée au réseau « Green ».

Nous verrons plus loin qu'il est aussi possible d'ajouter un hôte de manière « automatisée » dans Zabbix mais il est important, pour une bonne compréhension, de maîtriser dans un premier temps l'ajout manuel d'un hôte dans Zabbix.

Un hôte dans Zabbix **est une entité connectée au réseau** (entité physique ou virtuelle) que vous souhaitez surveiller. La définition de ce qui peut être un « hôte » dans Zabbix est assez flexible. Il peut s'agir d'un **serveur physique**, d'un **commutateur réseau**, d'une **machine virtuelle** ou d'une **application**.

Dans l'interface web de Zabbix, on peut déjà surveiller le serveur Zabbix précédemment installé en faisant ceci :

- Cliquez « **Collecte de données** » et « **Hôtes** » ; le serveur Zabbix est affiché dans la liste :



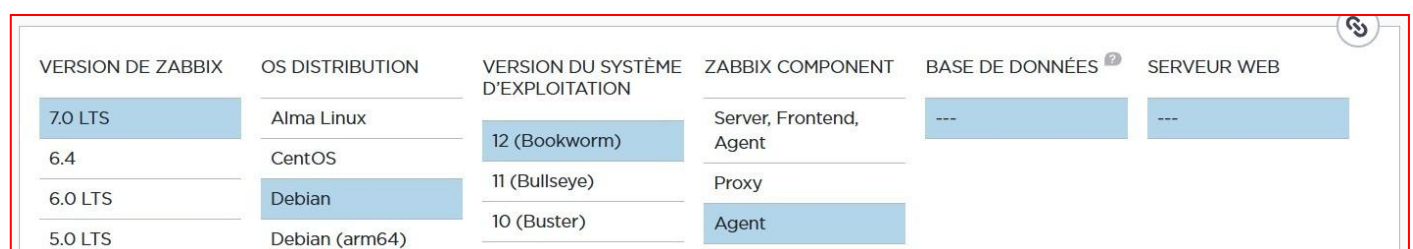
Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent	Info	Tags
Zabbix server	Éléments 135	Déclencheurs 73	Graphiques 25	Découverte 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Activé	ZBX	AUCUN		

La colonne « **Disponibilité** » contient des indicateurs de disponibilité de chaque hôte pour comprendre leur disponibilité :

- **ZBX** - le statut d'hôte n'a pas été établi ; aucune vérification métrique n'a encore eu lieu
- **ZBX** - l'hôte est disponible, une vérification des métriques a réussi
- **ZBX** - L'hôte n'est pas disponible, une vérification de métrique a échoué (déplacez le curseur de votre souris sur l'icône pour voir le message d'erreur). Il peut y avoir une erreur de communication qui peut être causée par des informations d'identification d'interface incorrectes. Vérifiez que le serveur Zabbix est en cours d'exécution et essayez également d'actualiser la page.

Pour que la machine Debian « hôte » puisse communiquer avec Zabbix, nous allons devoir installer un « **agent** » sur cette dernière.

La plateforme de téléchargement de Zabbix nous donne le lien de téléchargement suivant :



VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
7.0 LTS	Alma Linux	12 (Bookworm)	Server, Frontend, Agent	---	---
6.4	CentOS	11 (Bullseye)	Proxy		
6.0 LTS	Debian	10 (Buster)	Agent		
5.0 LTS	Debian (arm64)				

1^{ère} étape : installer le référentiel Zabbix sur la machine hôte

Connectez-vous en SSH à votre machine hôte (plus simple pour exécuter les commandes sinon il faudra les saisir avec l'utilisateur « root » ou un utilisateur disposant des droits « sudo ») et saisissez les commandes suivantes :

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-1+debian12_all.deb
```

```
dpkg -i zabbix-release_7.0-1+debian12_all.deb apt update -y
```

2^{ème} étape : installer l'agent Zabbix sur la machine hôte

```
apt install zabbix-agent -y
```

3^{ème} étape : démarrer et activer les processus de l'agent Zabbix

```
systemctl restart zabbix-agent systemctl enable zabbix-agent
```

L'agent est maintenant installé sur la machine hôte. Bien que Zabbix supporte le cryptage par certificat, la mise en place d'une autorité de certification dépasse le cadre de ce tutoriel. Vous pouvez utiliser des clés pré-partagées (PSK) pour sécuriser la connexion entre le serveur et l'agent.

L'agent Zabbix peut collecter des métriques en mode actif ou passif (simultanément). **Un contrôle passif est une simple demande de données. Le serveur Zabbix demande certaines données** (par exemple, la charge du processeur) **et l'agent Zabbix renvoie le résultat au serveur.**

Les contrôles actifs nécessitent un traitement plus complexe. L'agent doit d'abord extraire du ou des serveurs une liste d'éléments à traiter indépendamment, puis renvoyer les données en bloc.

Les modèles de surveillance fournis par Zabbix offrent généralement deux alternatives : un modèle pour l'agent Zabbix et un modèle pour l'agent Zabbix actif.

Avec la première option, l'agent collectera des métriques en mode passif. Ces modèles fourniront des résultats de surveillance identiques mais en utilisant des protocoles de communication différents.

4^{ème} étape : vérification du hostname de la machine hôte (Debian dans ce tutoriel)

Avant de configurer l'ajout de l'hôte dans Zabbix, il convient de vérifier le nom d'hôte de la machine que nous voulons surveiller (nous en aurons besoin plus loin).

Ici, nous avons créé une nouvelle machine Debian que nous allons ajouter en tant qu'hôte dans Zabbix.

La vérification du nom d'hôte se fait à l'aide de la commande suivante sur la machine Debian :

hostname -f

Dans notre cas, nous obtenons ceci :

```
root@debian:~# hostname -f
debian.local
```

5^{ème} étape : modification du fichier de configuration de l'agent Zabbix

Sur la machine hôte, effectuez les manipulations suivantes :

nano /etc/zabbix/zabbix_agentd.conf

Vous allez devoir modifier différents éléments dans le fichier de configuration de l'agent Zabbix (voir pages suivantes).

- Indiquez, sur la ligne « **Server=** », l'adresse IP du serveur Zabbix :

```
### Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
Server=192.168.168.19
```

- Indiquez, sur la ligne « **ServerActive=** », l'adresse IP de votre serveur Zabbix :

```

### Option: ServerActive
# Zabbix server/proxy address or cluster configuration to get active checks from.
# Server/proxy address is IP address or DNS name and optional port separated by colon.
# Cluster configuration is one or more server addresses separated by semicolon.
# Multiple Zabbix servers/clusters and Zabbix proxies can be specified, separated by comma.
# More than one Zabbix proxy should not be specified from each Zabbix server/cluster.
# If Zabbix proxy is specified then Zabbix server/cluster for that proxy should not be specified.
# Multiple comma-delimited addresses can be provided to use several independent Zabbix servers.
# If port is not specified, default port is used.
# IPv6 addresses must be enclosed in square brackets if port for that host is specified.
# If port is not specified, square brackets for IPv6 addresses are optional.
# If this parameter is not specified, active checks are disabled.
# Example for Zabbix proxy:
# ServerActive=127.0.0.1:10051
# Example for multiple servers:
# ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]:30051
# Example for high availability:
# ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051;zabbix.cluster.node3:20051
# Example for high availability with two clusters and one server:
# ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051,zabbix.cluster.node3:20051
#
# Mandatory: no
# Default:
ServerActive=192.168.168.19

```

- Indiquez, sur la ligne « **Hostname=** », le nom d'hôte de la machine à surveiller

```

### Option: Hostname
# List of comma delimited unique, case sensitive hostnames.
# Required for active checks and must match hostnames as configured on the server.
# Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=
Hostname=debian.local

```

- Quittez et sauvegardez les modifications (**CTRL + X – O** et pressez la touche « **Entrée** »)
- Relancez l'agent Zabbix avec la commande suivante :

systemctl restart zabbix-agent

6^{ème} étape : ajout manuel d'un nouvel hôte sur le serveur Zabbix et configuration en mode « actif »

L'installation d'un agent sur une machine que vous souhaitez surveiller ne représente que la moitié du processus. Chaque hôte que vous souhaitez surveiller doit être enregistré sur le serveur Zabbix, ce que vous pouvez faire via l'interface web.

Connectez-vous à l'interface web de votre serveur Zabbix et effectuez les manipulations suivantes :

- Cliquez sur « Collecte des données » - « Hôtes » et « Créer un hôte » (complétez les champs) :

Indication du nom de l'hôte :

- Saisissez le nom d'hôte de la machine à surveiller (le « hostname » vu précédemment) :



Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte

Nom visible

Choix du modèle à utiliser :

- Cliquez le bouton « **Sélectionner** » à droite de la rubrique « **Modèles** » :



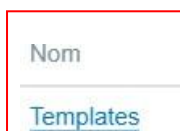
Modèles Sélectionner

- Dans la rubrique « **Groupe de modèles** », cliquez le bouton « **Sélectionner** » à droite :



Groupe de modèles Sélectionner

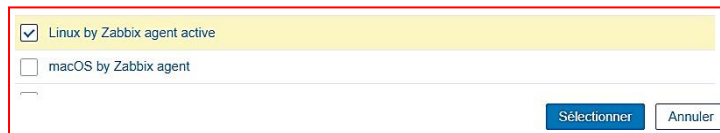
- Cliquez « **Templates** » :



Nom

Templates

- Dans la liste des templates, sélectionnez « **Linux by Zabbix agent active** » et cliquez « **Sélectionner** » :

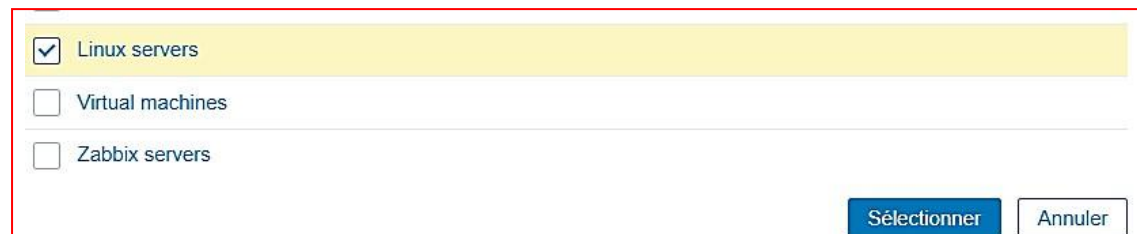


Choix du groupe d'hôtes :

- Dans la rubrique « **Groupes d'hôtes** », cliquez le bouton « **Sélectionner** » :

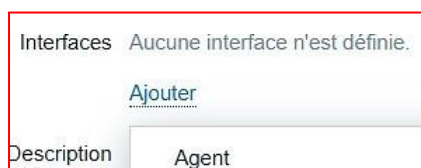


- Choisissez un groupe (par exemple, ici, « **Linux servers** ») et cliquez « **Sélectionner** » :



Choix de l'interface

- Cliquez le lien « **Ajouter** » et sélectionnez « **Agent** » :



- Saisissez l'adresse IP de l'agent (le nom DNS n'est pas obligatoire) ; dans notre cas, nous avons ceci :

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		192.168.168.20	debian.local	<input checked="" type="radio"/> IP <input type="radio"/> DNS	10050	<input checked="" type="radio"/> Supprimer

On configure l'adressage IP de l'agent. Bien que ce ne soit pas un champ obligatoire techniquement, une interface hôte est nécessaire pour collecter certaines métriques. La configuration du nouvel hôte peut ressembler à celle-ci par exemple :

Hôte

Hôte

IPMI

Tags

Macros

Inventaire

Chiffrement

Table de correspondance

* Nom de l'hôte

debian.local

Nom visible

debian.local

Modèles

Nom

Linux by Zabbix agent active

Action

Supprimer lien

Supprimer lien et nettoyer

taper ici pour rechercher

Sélectionner

* Groupes d'hôtes

Linux servers

taper ici pour rechercher

Sélectionner

Interfaces

Type

adresse IP

Nom DNS

Connexion à

Port

Défaut

Agent

192.168.168.20

debian.local

☒ IP ☐ DNS

10050

☒ Supprimer

Ajouter

Description

Surveillé par

Serveur

Proxy

Groupe de proxy

Activé

☒

Assurez-vous que la case « **Activé** » est bien cochée et cliquez sur « **Ajouter** » si les paramètres saisis sont corrects.

Votre nouvel hôte devrait être visible dans la liste des hôtes avec le mode de disponibilité « **ZBX** » en vert. **Patiencez quelques instants si le statut n'est pas passé au vert et actualisez l'affichage si nécessaire :**

<input type="checkbox"/> Nom ▲	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent	Info	Tags
<input type="checkbox"/> debian.local	Éléments 69	Déclencheurs 27	Graphiques 14	Découverte 3	Web	192.168.168.20:10050		Linux by Zabbix agent active	Activé	ZBX	Aucun		
<input type="checkbox"/> Zabbix server	Éléments 135	Déclencheurs 73	Graphiques 25	Découverte 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Activé	ZBX	Aucun		

4 – AJOUTER UN HÔTE WINDOWS DANS ZABBIX 7.0 (LTS)

Dans cette partie nous allons ajouter un nouvel hôte dans Zabbix. Pour cela, nous avons créé une nouvelle machine virtuelle Windows 11 qui est connectée, elle aussi, au réseau « Green » de notre infrastructure.

On démarre la machine Windows et on télécharge l'agent Zabbix pour Windows ici : [Lien ZABBIX AGENT](#) et on sélectionne la bonne plateforme (dans notre cas, package MSI pour Zabbix 7.0 LTS et architecture 64 bits)

Download pre-compiled Zabbix agent binaries

For Agent DEBs and RPMs please visit [Zabbix packages](#)

☐ Show legacy downloads

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.0 LTS	OpenSSL	MSI
Linux		i386	6.4	No encryption	Archive

- Cliquez le bouton vert « **Download** » pour télécharger l'agent Zabbix pour Windows :

Zabbix Release: 7.0.0

Zabbix agent v7.0.0

Packaging: MSI
Encryption: OpenSSL
Linkage: Dynamic
Checksum: sha256: 1260c36454ec0bbe5bc723c75f934dc8cfb520785e5643387b9504f78cfc284
 sha1: 0b3a37ca226d42f0ec0e10af0b7e7abe2ac6317a
 md5: 8fdaaaebde14fac88c0dc408cc1f4571

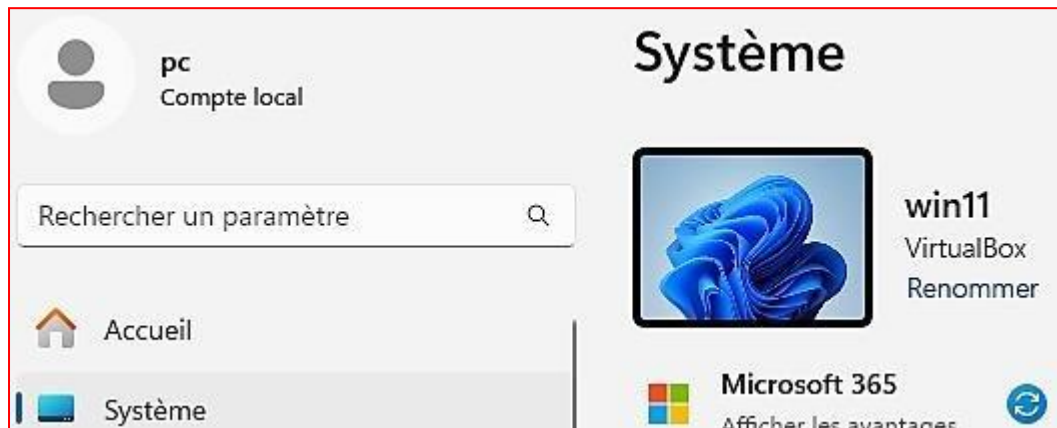
DOWNLOAD

https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.0/zabbix_agent-7.0.0-windows-amd64-openssl.msi

Avant de lancer l'installation de l'agent, il convient d'identifier le nom d'hôte de notre machine. Ici nous possédons une machine virtuelle Windows 11 nommé « win11 ». Pour vérifier le "hostname" de votre machine Windows 11, procédez ainsi :

- Faites un **clic droit sur le bureau Windows 11** et cliquez « **Personnaliser** »

- Dans le volet de gauche, cliquez « **Système** » ; le nom de votre machine s'affiche :



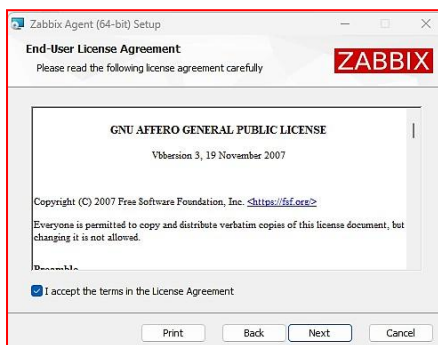
Si votre machine porte un nom de type "DESKTOP-xxxxxx", cliquez le lien « **Renommer** » et définissez un nom permettant de bien identifier votre machine ; un redémarrage de cette dernière sera nécessaire pour valider le changement de nom.

Nous pouvons maintenant **installer l'agent téléchargé en double-cliquant le fichier téléchargé** ; un assistant d'installation se lance :

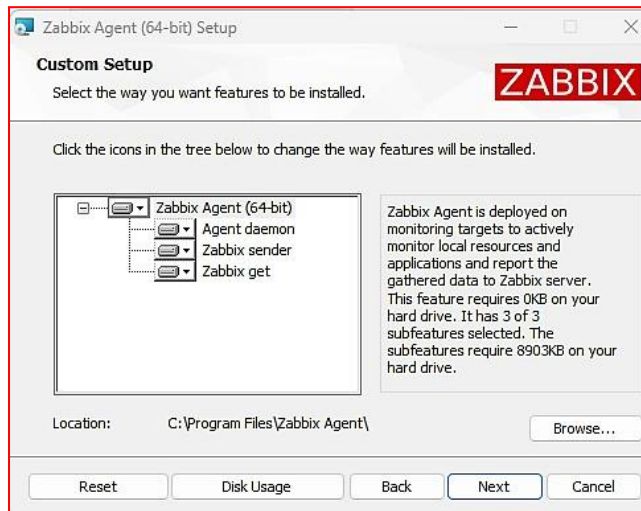
- Cliquez le bouton « **Next** » :



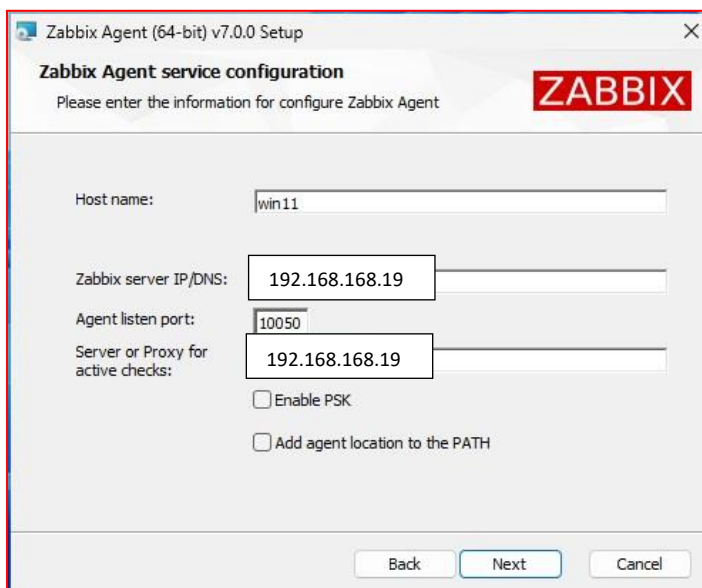
- Acceptez les termes du contrat de licence et cliquez le bouton « **Next** » :



- Laissez les options d'installation de l'agent par défaut et cliquez le bouton « **Next** » :



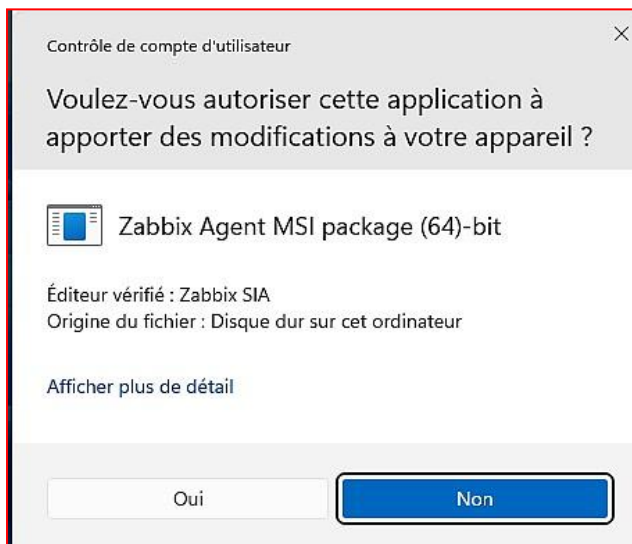
- Complétez la fenêtre avec les paramètres correspondant à votre infra et cliquez le bouton « **Next** » :



- Cliquez le bouton « **Install** » pour lancer la procédure d'installation de l'agent :



- Autorisez l'installation de l'agent en cliquant le bouton « **Oui** » :



- Cliquez le bouton « **Finish** » une fois l'agent installé :



Maintenant que l'agent est installé sur la machine Windows, nous allons créer l'hôte sur le serveur Zabbix. Pour cela :

- Connectez-vous à l'interface web de votre serveur Zabbix
- Cliquez, dans le volet de gauche, sur « **Collecte de données** » et « **Hôtes** »
- Cliquez, en haut à droite de la fenêtre, sur « **Créer un hôte** » et complétez la fenêtre :

Saisie du nom d'hôte de la machine Windows à enregistrer dans Zabbix :



Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte win11

Nom visible win11

- Sélectionnez le modèle « **Windows by Zabbix agent active** » :



Modèles	Nom	Action
	Windows by Zabbix agent active	Supprimer lien Supprimer lien et nettoyer

taper ici pour rechercher Sélectionner

Saisie du groupe d'hôtes à appliquer :

- Sélectionnez un groupe d'hôtes (« **Virtual machines** » par exemple) :



* Groupes d'hôtes Virtual machines X

taper ici pour rechercher Sélectionner

Saisie de l'adresse IP de la nouvelle machine à intégrer :

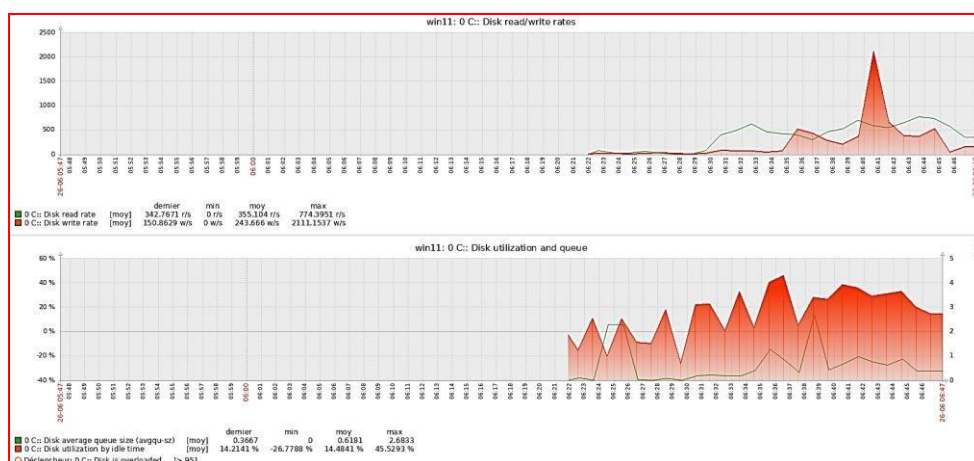
- Saisissez l'adresse IP de votre nouvel hôte :

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		192.168.168.21		IP	DNS	10050
Ajouter						

Lorsque tous les paramètres sont saisis, validez vos choix : la nouvelle machine hôte apparaît dans la liste des hôtes. **Patientez quelques minutes** afin que le statut de disponibilité passe à « **ZBX** » sur fond vert comme ci- dessous :

<input type="checkbox"/> Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent
<input type="checkbox"/> debian.local	Éléments 69	Déclencheurs 27	Graphiques 14	Découverte 3	Web	192.168.168.20:10050		Linux by Zabbix agent active	Activé	ZBX	Aucun
<input type="checkbox"/> win11	Éléments 34	Déclencheurs 14	Graphiques 5	Découverte 4	Web	192.168.168.21:10050		Windows by Zabbix agent active	Activé	ZBX	Aucun
<input type="checkbox"/> Zabbix server	Éléments 135	Déclencheurs 73	Graphiques 25	Découverte 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Activé	ZBX	Aucun

Comme pour une machine Linux, vous pouvez maintenant suivre les métriques de vos machines Windows ! Pour cela, cliquez les liens bleus ou cliquer, dans le volet de gauche, sur « **Surveillance** » – « **Hôtes** » – « **Dernières données** ». Nous pouvons obtenir différents types de rapports/graphiques/métriques comme :



5 – REMONTER AUTOMATIQUEMENT UN HÔTE WINDOWS DANS ZABBIX 7.0 A L'AIDE D'UNE « ACTION »

Avec Zabbix, il est possible d'effectuer une remontée automatisée des hôtes connectés au réseau **en utilisant la méthode des « actions » dans Zabbix**. Pour réaliser cette étape, **nous avons créé une nouvelle machine Windows** qui n'a pas été encore importée dans Zabbix.

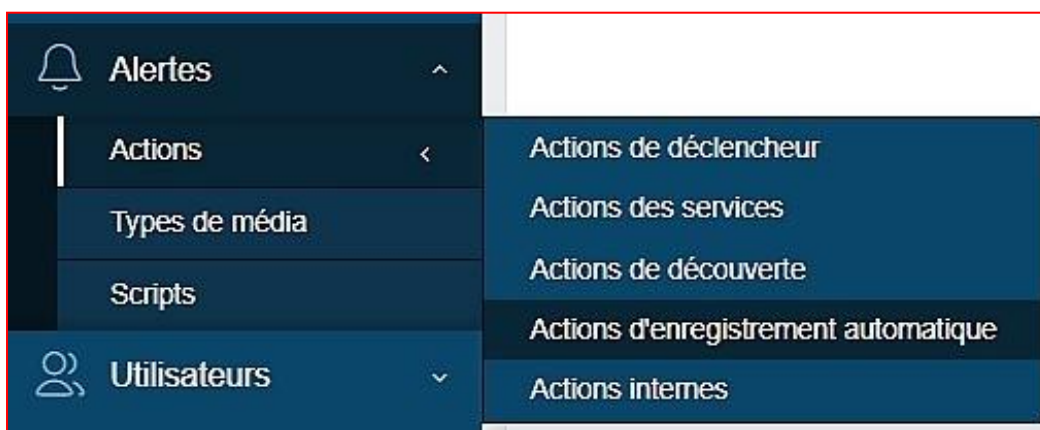
Une fois la machine créée et connectée au réseau « Green » de notre infrastructure, nous installons l'agent Zabbix (voir étapes précédentes). Nous allons, maintenant, effectuer la remontée automatisée de la nouvelle machine dans Zabbix. Cette nouvelle machine porte le nom « win11-2 ».

Dans l'interface web de Zabbix, en cliquant « **Collecte de données** » - « **Hôtes** » on peut afficher les hôtes déjà créés manuellement :

<input type="checkbox"/> Nom ▲	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent
<input type="checkbox"/> debian.local	Éléments 69	Déclencheurs 27	Graphiques 14	Découverte 3	Web	192.168.168.20:10050		Linux by Zabbix agent active	Activé	ZBX	Aucun
<input type="checkbox"/> win11	Éléments 34	Déclencheurs 14	Graphiques 5	Découverte 4	Web	192.168.168.21:10050		Windows by Zabbix agent active	Activé	ZBX	Aucun
<input type="checkbox"/> Zabbix server	Éléments 135	Déclencheurs 73	Graphiques 25	Découverte 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Activé	ZBX	Aucun

Pour lancer la collecte automatique du nouvel hôte « win11-2 », appliquez la procédure suivante :

- Cliquez, dans le volet de gauche, le menu « **Alertes** » et « **Actions** »
- Sélectionnez « **Actions d'enregistrement automatique** » :



- Dans la fenêtre affichée, cliquez « **Créer une action** » en haut à droite :

Actions d'enregistrement automatique ▾

? [Créer une action](#)

- Saisissez un nom pour l'action (par exemple « windows ») et cliquez le lien bleu « **Ajouter** » :

Nouvelle action

Action

Opérations

* Nom

Conditions

Étiquette

Ajouter

Nom

- Saisissez la condition ; ici nous avons indiqué que le nom de l'hôte à ajouter devait contenir « win »
- Cliquez le bouton « **Ajouter** » :

Nouvelle condition ✕

Type

Opérateur

* Valeur

- Cliquez ensuite l'option « **Opérations** » et le lien bleu « **Ajouter** » :

Nouvelle action

Action Opérations

Opérations	Détails	Action
	Ajouter	

* Au moins une opération doit exister.

- Sélectionnez, dans la rubrique « **Opérations** », « **Ajouter au groupe d'hôtes** » • Choisissez un groupe d'hôtes (ici, nous avons choisi « **Virtual machines** » par défaut)
- Cliquez le bouton bleu « **Ajouter** » :

Détails de l'opération ✕

Opération

* Groupes d'hôtes

- Une fois la première opération ajoutée, cliquez à nouveau sur le lien bleu « **Ajouter** »
- Sélectionnez l'opération « **Lier le modèle** » et cliquez « **Sélectionner** » dans la rubrique « **Modèles** » :

Détails de l'opération ✕

Opération

* Modèles

Cliquez « **Sélectionner** » dans la rubrique « **Modèles** » :

Modèles

Groupe de modèles

Sélectionner

- Cliquez sur « **Templates/Operating systems** » :

Groupes de modèles

Nom

[Templates](#)

[Templates/Applications](#)

[Templates/Cloud](#)

[Templates/Databases](#)

[Templates/Network devices](#)

[Templates/Operating systems](#)

- Sélectionnez « **Windows by Zabbix agent active** » et cliquez le bouton bleu « **Sélectionner** » et « **Ajouter** » :

☒ Windows by Zabbix agent active

Sélectionner

Annuler

On obtient ceci avec les 2 opérations ci-dessus :

Détails de l'opération

Opération

Lier le modèle

* Modèles

Windows by Zabbix agent active x

taper ici pour rechercher

Sélectionner

Ajouter

Annuler

- Validez les choix, on obtient ceci :

Actions d'enregistrement automatique ▾

☒ Action mise à jour

Nom
 État Tous Activé Désactivé

Appliquer Réinitialiser

☐ Nom ▲ Conditions Opérations

☐ windows Nom de l'hôte contient win
 Ajouter aux groupes d'hôtes: Virtual machines
 Lier les modèles: Windows by Zabbix agent active

Patiencez quelques minutes le temps que la remontée soit réalisée dans Zabbix. Depuis l'interface web de Zabbix, cliquez, dans le volet de gauche, sur « **Collecte de données** » - « **Hôtes** » ; le nouvel hôte « win11-2 » doit apparaître (sinon actualisez l'affichage) avec le statut de disponibilité sur « **ZBX** » avec un fond vert :

Collecte de données ▾												
<input type="checkbox"/> Nom ▲ Éléments Déclencheurs Graphiques Découverte Web Interface Proxy Modèles État Disponibilité Chiffrement sur l'agent												
<input type="checkbox"/>	debian.local	Éléments 69	Déclencheurs 27	Graphiques 14	Découverte 3	Web	192.168.168.20:10050	Linux by Zabbix agent active	Activé	ZBX	Aucun	
<input type="checkbox"/>	win11	Éléments 105	Déclencheurs 72	Graphiques 12	Découverte 4	Web	192.168.168.21:10050	Windows by Zabbix agent active	Activé	ZBX	Aucun	
<input type="checkbox"/>	win11-2	Éléments 105	Déclencheurs 72	Graphiques 12	Découverte 4	Web	192.168.168.22:10050	Windows by Zabbix agent active	Activé	ZBX	Aucun	
<input type="checkbox"/>	Zabbix server	Éléments 135	Déclencheurs 73	Graphiques 25	Découverte 5	Web	127.0.0.1:10050	Linux by Zabbix agent, Zabbix server health	Activé	ZBX	Aucun	

La remontée automatisée du nouvel hôte a bien été réalisée et des métriques sont déjà mis à disposition pour cette nouvelle machine.

Pour consulter ces métriques, cliquez dans le volet de gauche, sur « **Surveillance** » - « **Hôtes** » et cliquez sur le lien « **Dernières données** » du nouvel hôte (ici « win11-2 ») :

Surveillance

Problèmes

Hôtes

Dernières données

Cartes

Découverte

Services

Inventaire

Rapports

Collecte de données

Alertes

Groupes d'hôtes

aperçu pour rechercher

Sélectionner

IP

DNS

Port

tag

Contient

valeur

Ajouter

Afficher les hôtes en maintenance

Afficher les problèmes supprimés

Sévérité

Non classé

Avertissement

Haut

Information

Moyen

Désastre

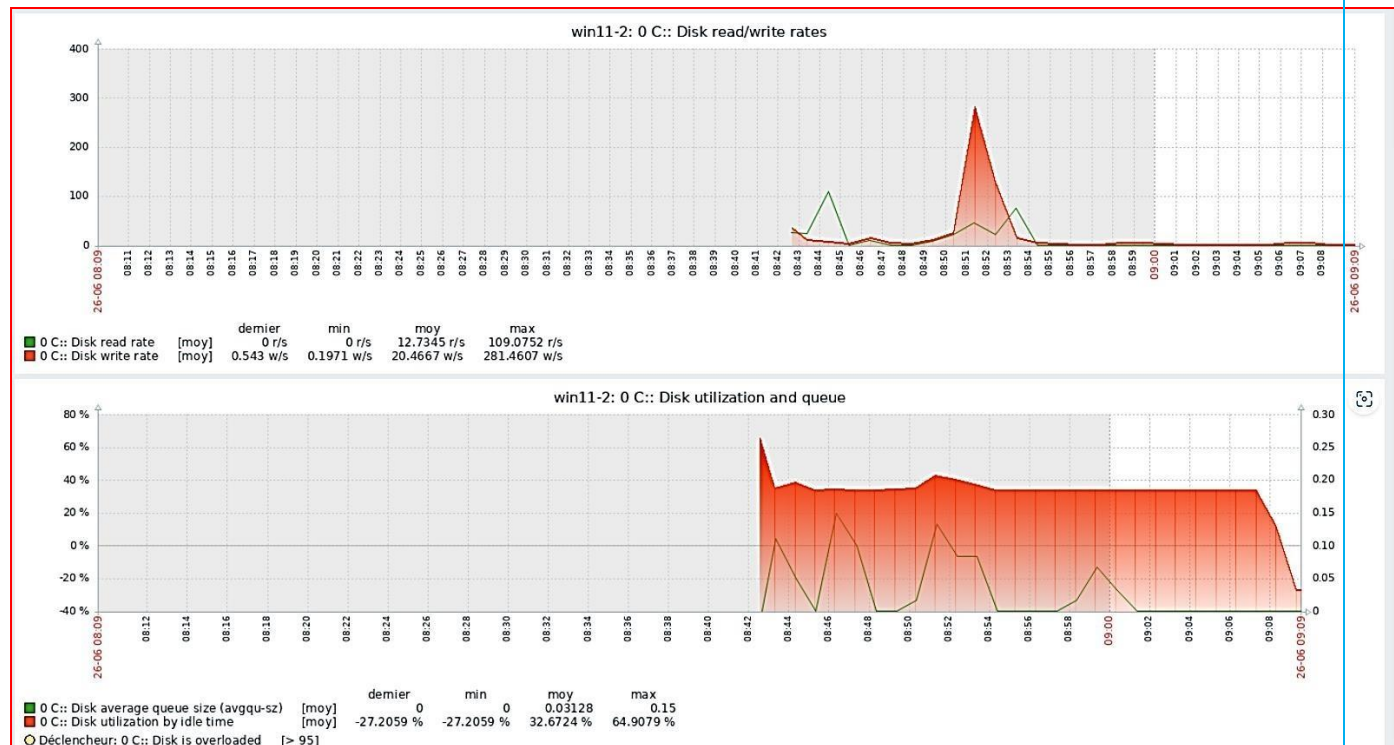
Enregistrer sous

Appliquer

Réinitialiser

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord
debian.local	192.168.168.20:10050	ZBX	class: os target: linux	Activé	Dernières données 69	Problèmes	Graphiques 14	Tableaux de bord 3
win11	192.168.168.21:10050	ZBX	class: os target: windows	Activé	Dernières données 105	Problèmes	Graphiques 12	Tableaux de bord 3
win11-2	192.168.168.22:10050	ZBX	class: os target: windows	Activé	Dernières données 105	Problèmes	Graphiques 12	Tableaux de bord 3
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Activé	Dernières données 135	Problèmes	Graphiques 25	Tableaux de bord 5

Nous pouvons afficher les métriques pour cet hôte :



Conclusion du livrable

Ce projet a permis de concevoir, déployer et documenter une infrastructure réseau sécurisée, redondée et fonctionnelle, en s'appuyant sur des technologies professionnelles et des outils open-source.

Parmi les principaux aboutissements techniques :

- Mise en place d'un **cluster pfSense en haute disponibilité (CARP + pfsync)** avec synchronisation des configurations et bascule automatique en cas de panne,
- Création d'une **DMZ sécurisée** pour héberger des services exposés (ex. **eBrigade**), avec une politique stricte de filtrage et des règles de NAT,
- Installation et configuration de **HmailServer** pour la gestion interne des services mail,
- Structuration du réseau autour de **VLANs**, d'une passerelle unique virtuelle, et d'un routage propre depuis Proxmox en mode trunk.

Ce projet nous a permis de **développer nos compétences en administration réseau, sécurité, virtualisation, et documentation technique**, tout en adoptant une démarche rigoureuse orientée production et fiabilité.

L'ensemble des procédures techniques produites dans ce livrable permet à tout technicien de **reprendre, comprendre et faire évoluer l'infrastructure**, ce qui en fait une base solide pour un environnement professionnel.