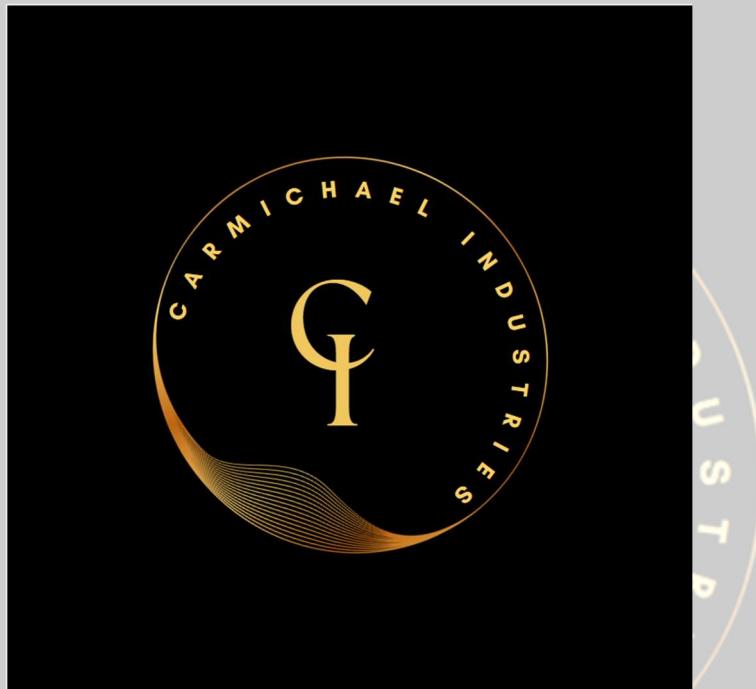


Projet Carmichael Industries

BTS SIO 2023 Option SISR



Epreuve E5

Documentation professionnelle 2

Table des matières

1. DOCUMENTATION TECHNIQUE	4
1.1. Routeurs PFSense	4
1.1.1. Installation de PfSense	4
1.1.2. Configuration de base de PfSense	12
1.1.3. Mise en place du CARP	15
1.1.4. Utilisation des IP virtuelles	18
1.1.5. Synchronisation des PfSense	22
1.1.6. Mise en place des règles de pare-feu	26
1.2. Serveur AD	37
1.2.1. Installation	37
1.2.2. Configuration de base	50
1.2.3. Agrégation de carte réseau (IP Bonding)	55
1.2.4. DHCP	59
1.2.5. ADDS (Active Directory et DNS)	68
1.3. Serveur de Messagerie	71
1.3.1. Installation d'hMailServer	71
1.3.2. Configuration d'hMailServer	77
1.3.3. Ajout du serveur de messagerie dans le DNS	81
1.3.4. Configuration d'hMailServer	83
1.3.5. Ajout du serveur de messagerie dans le DNS	86
1.3.6 Test de la messagerie	91
1.4. Serveur de Téléphonie	93
1.4.1. Installation	93
1.4.2. Configuration	93
1.4.3. Configuration users.conf	95
1.4.4. Configuration Voicemail.conf	96
1.4.5. Configuration extensions.conf	97
1.4.5. Configuration softphone Linphone	98
1.5. Serveur web (eBrigade)	99
1.5.1. Attribution adresse IP	99
1.5.2. Installation des paquets nécessaires à la mise en place d'eBrigade	100
1.5.3. Installation d'eBrigade	101
1.5.4. Crédit de la base de données d'eBrigade	101

1.5.5. Connexion à la page web d'eBrigade	102
1.6. VPN Road Warrior	103
 1.6.1. Crédation groupe uservpn	103
 1.6.2. Installation et configuration serveur RADIUS	103
 1.6.2. OpenVPN	106
1.7. Serveur de supervision	115
 1.7.1. Installation	115



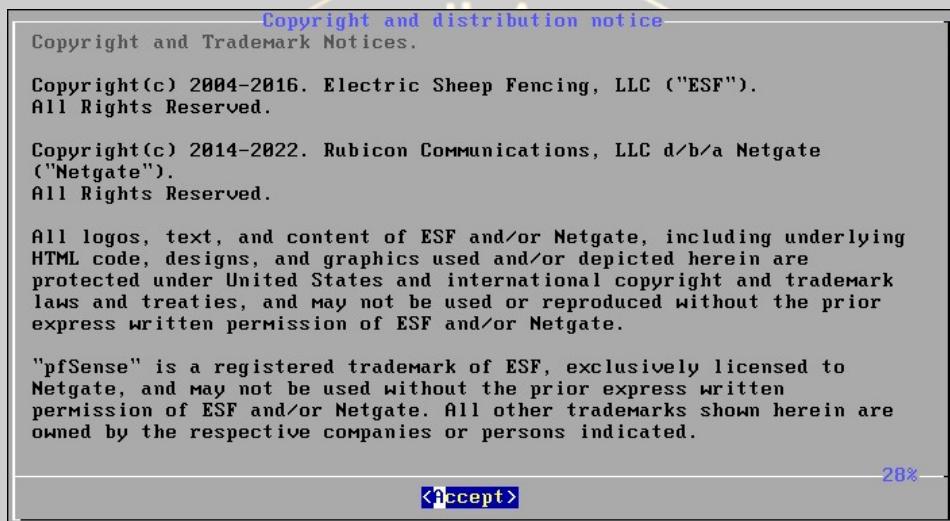
1. DOCUMENTATION TECHNIQUE

1.1. Routeurs PFsense

1.1.1. Installation de PfSense

On télécharge l'image ISO depuis le site officiel : <https://www.pfsense.org/download/> on va créer une machine virtuelle à partir de cette ISO. Nous allons lui attribuer 3 cartes réseaux.

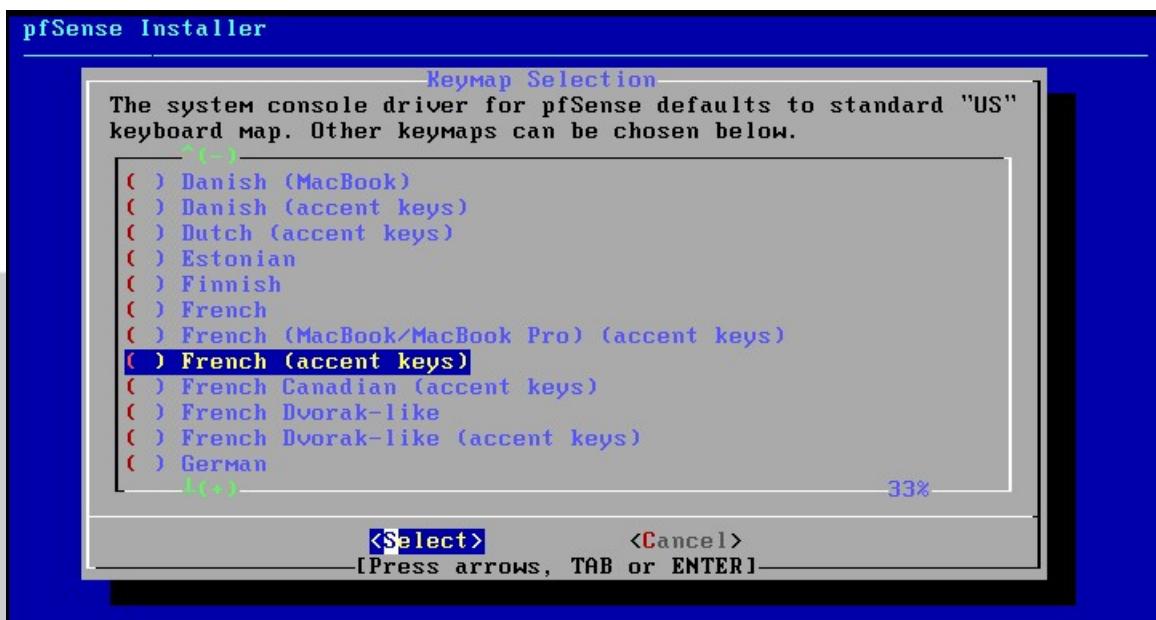
Lorsque vous lancerez la machine sous PfSense, vous tomberez nez à nez avec cette interface dont vous accepterez les termes. Noter que les étapes suivantes concernent les deux serveurs PfSense.



Ensuite, on vous proposera différents choix dont nous choisirons le premier « Install » puisque les autres ne nous correspondent pas.

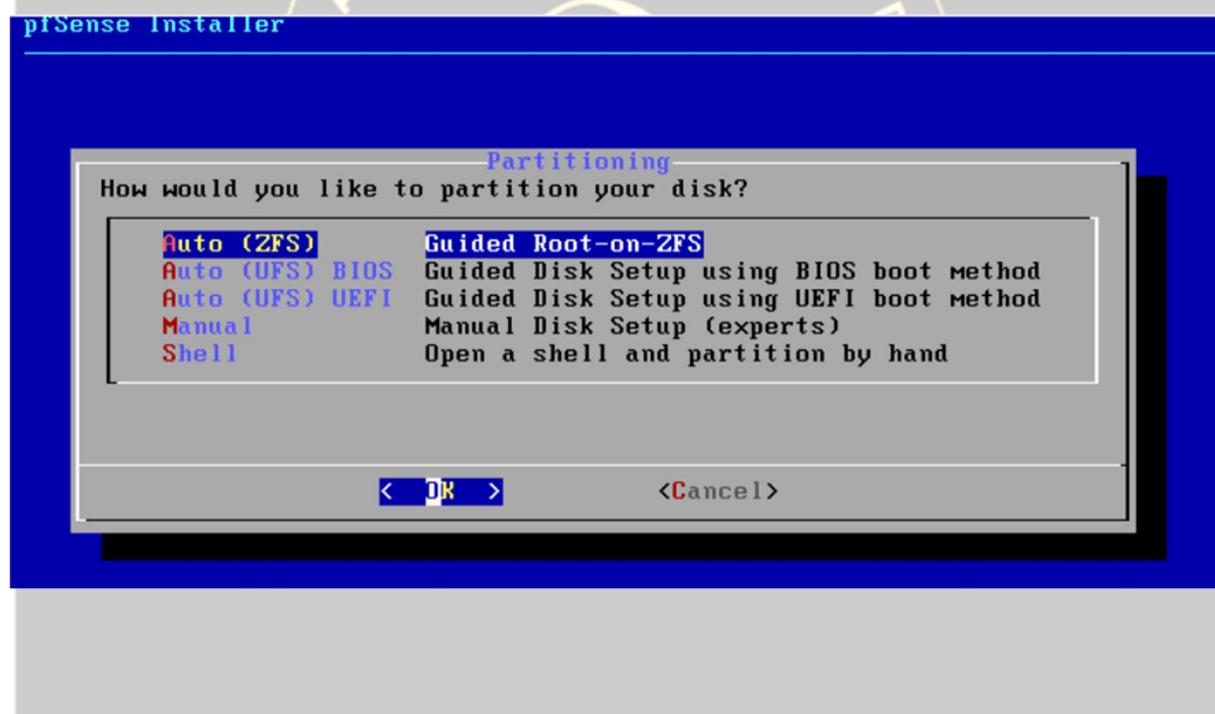


Vous pouvez choisir votre langue.

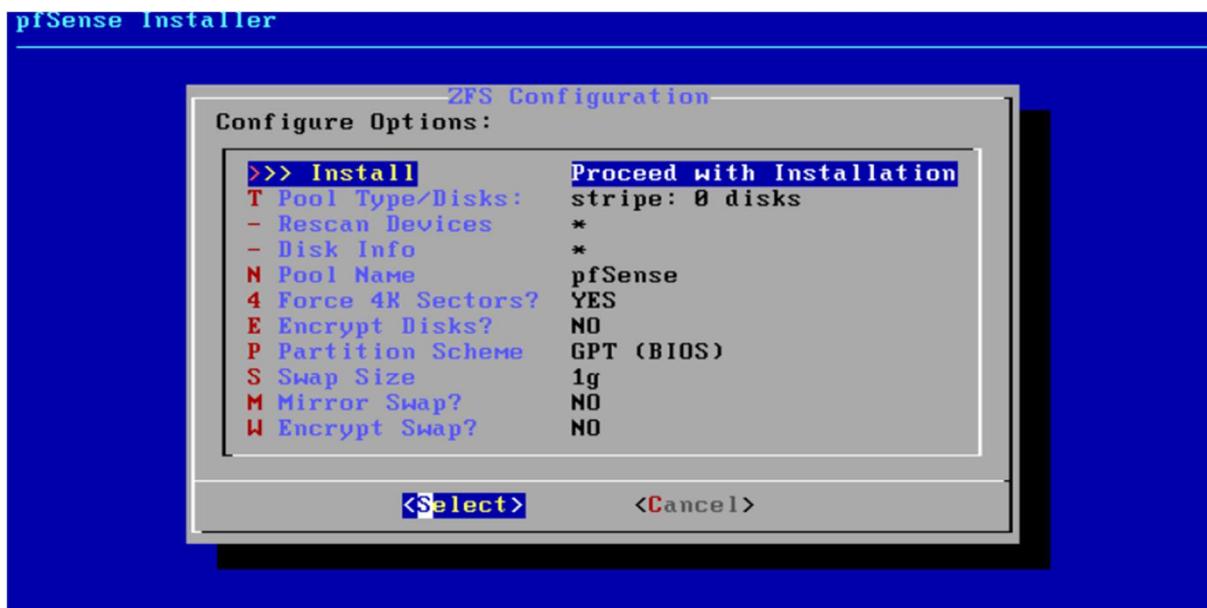


Puis,
on
nous

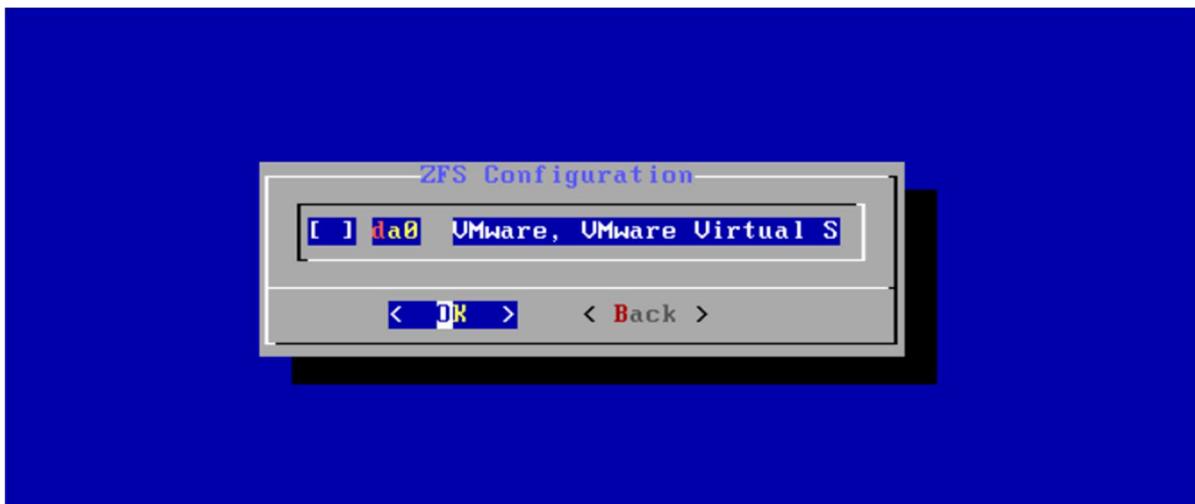
demandera comment on souhaite que notre disque soit partitionné. Dans notre cas, nous laissons le premier choix.



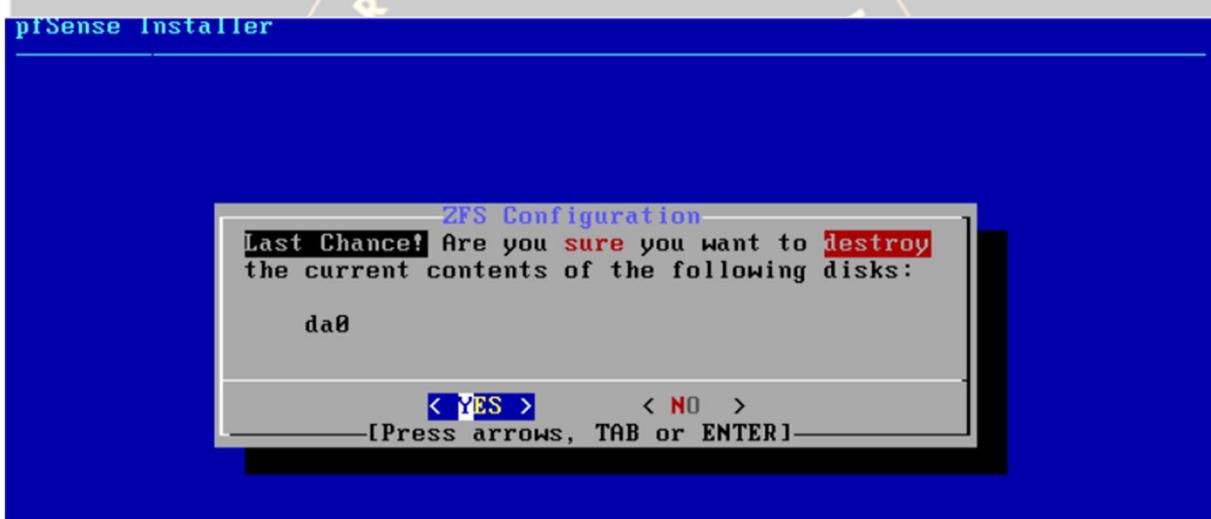
On vérifie les paramètres puis on clique sur « Select »



Le seul disque qu'il me propose est le suivant qui est mon disque virtuel, je clique sur « espace » puis « ok »



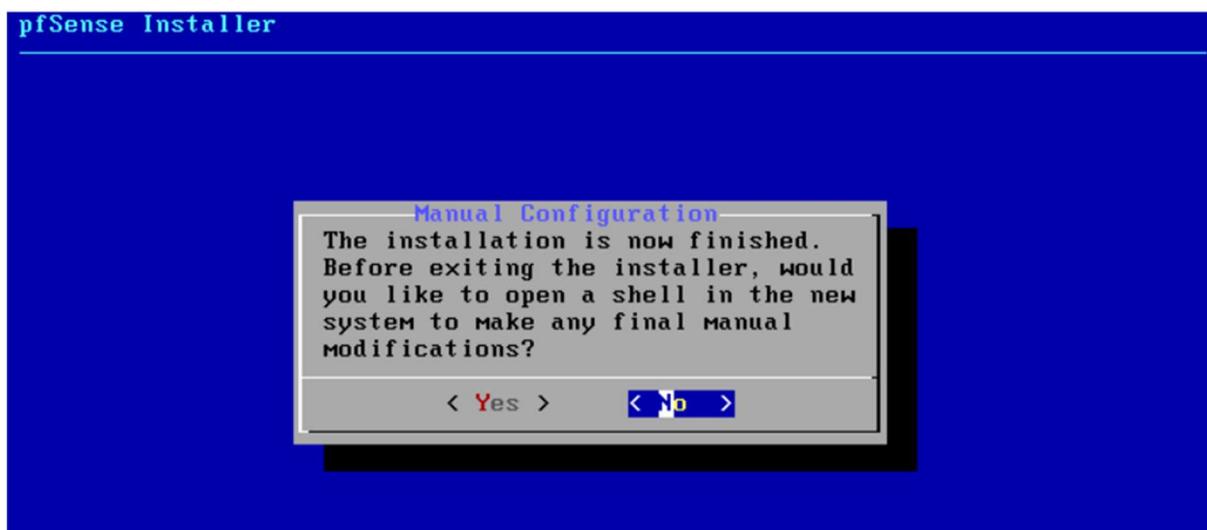
On nous demande ensuite si nous sommes sur de vouloir procéder au risque de perdre les données présents mais vu que nous n'avons aucune donnée présente, nous pouvons accepter.



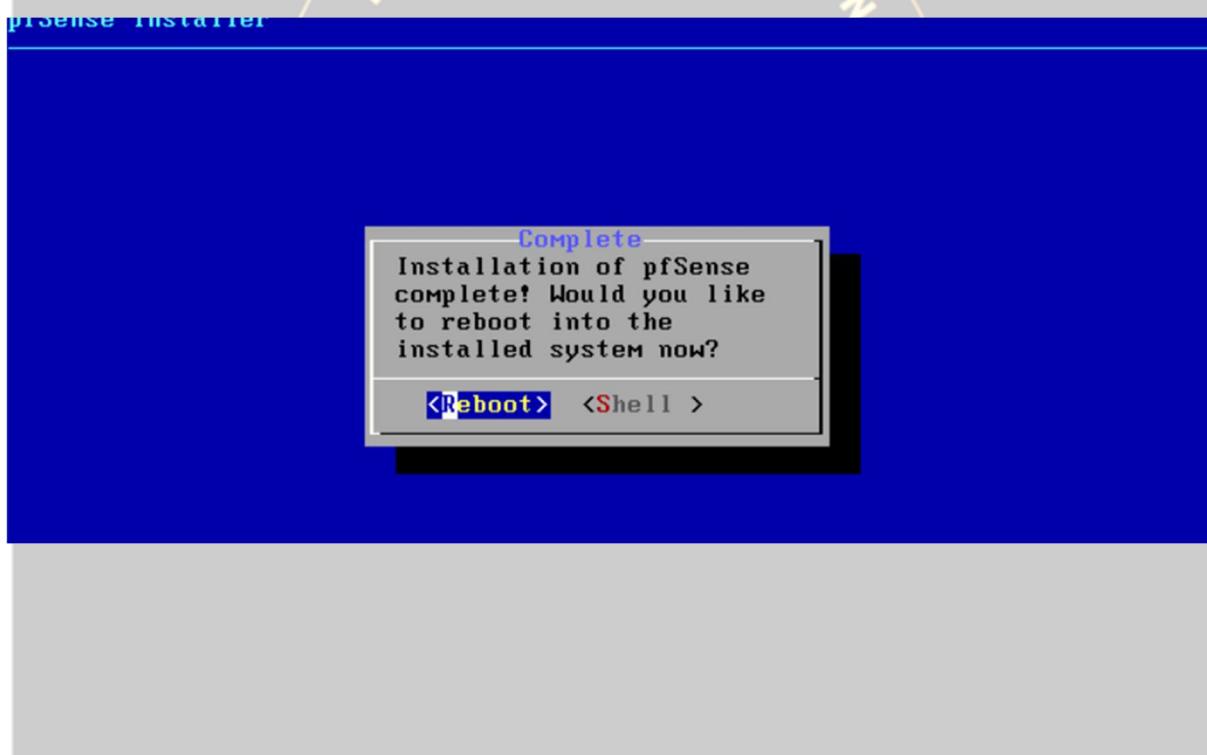
L'installation se lance :



Après que l'installation soit complétée, on nous propose d'ouvrir un terminal pour continuer la configuration. Nous allons dire « non » puisque nous pourrons le faire par la suite.



Puis on clique sur « reboot ».



a. Paramétrage réseau des routeurs

Une fois que la machine a rebooté, nous arriverons sur cette interface qui n'est autre que le menu du serveur pfsense. Ici ce qui nous intéresse et l'attribution de l'adresse IP.

On remarque que l'adresse IP du WAN dispose déjà d'une adresse IP qui correspond à la carte réseau configurée au préalable.

Maintenant on souhaite configurer l'adresse IP du LAN du serveur.

Pour cela, nous entrons l'option 2 puis on a le choix entre configurer le :

- WAN
- LAN
- OPT1

```
FreeBSD/amd64 (SRU-SECURITE01.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 50688ebad0d1963640c5

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on SRU-SECURITE01 ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.40.7/24
LAN (lan)      -> em1      -> v4: 192.168.100.10/24
SECIVDMZ (opt1) -> em2      -> v4: 192.168.200.1/24

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

Enter an option: 1
```

On s'aperçoit que mes interfaces sont déjà configurées mais nous allons voir les étapes pour parvenir à ce résultat.

Dans un premier temps, nous allons assigner nos trois interfaces en cliquant sur l'option 1 :

```
Enter an option: 1
```

Nous ne configurerons pas de VLAN donc on met « n » à la proposition.
Ensuite, attribuez les interfaces de cette manière-ci :

em0 = WAN :

```
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 em2 or a): em0
```

em1 = LAN :

```
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(em1 em2 a or nothing if finished): em1
```

em2 = OPT1

```
Enter the Optional 1 interface name or 'a' for auto-detection  
(em2 a or nothing if finished): em2
```

Une fois cela fait, nous allons configurer les adresses IP. A noter qu'on n'attribuera pas toute suite celle de « l'OPT1 ».

```
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.40.7/24  
LAN (lan)      -> em1      -> v4: 192.168.1.1/24  
OPT1 (opt1)    -> em2      ->  
  
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
```

```
Available interfaces:
```

- 1 - WAN (em0 - dhcp, dhcp6)
- 2 - LAN (em1 - static)
- 3 - OPT1 (em2)

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

On commence par l'interface LAN pour le routeur1 :

```
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.10
```

Pour le routeur 2 :

```
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.20
```

Puis on informe le masque de sous-réseau :

```
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
```

Et on clique sur entrée deux fois puis on dit non pour le DHCP mais on accepte le protocole HTTP :

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

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

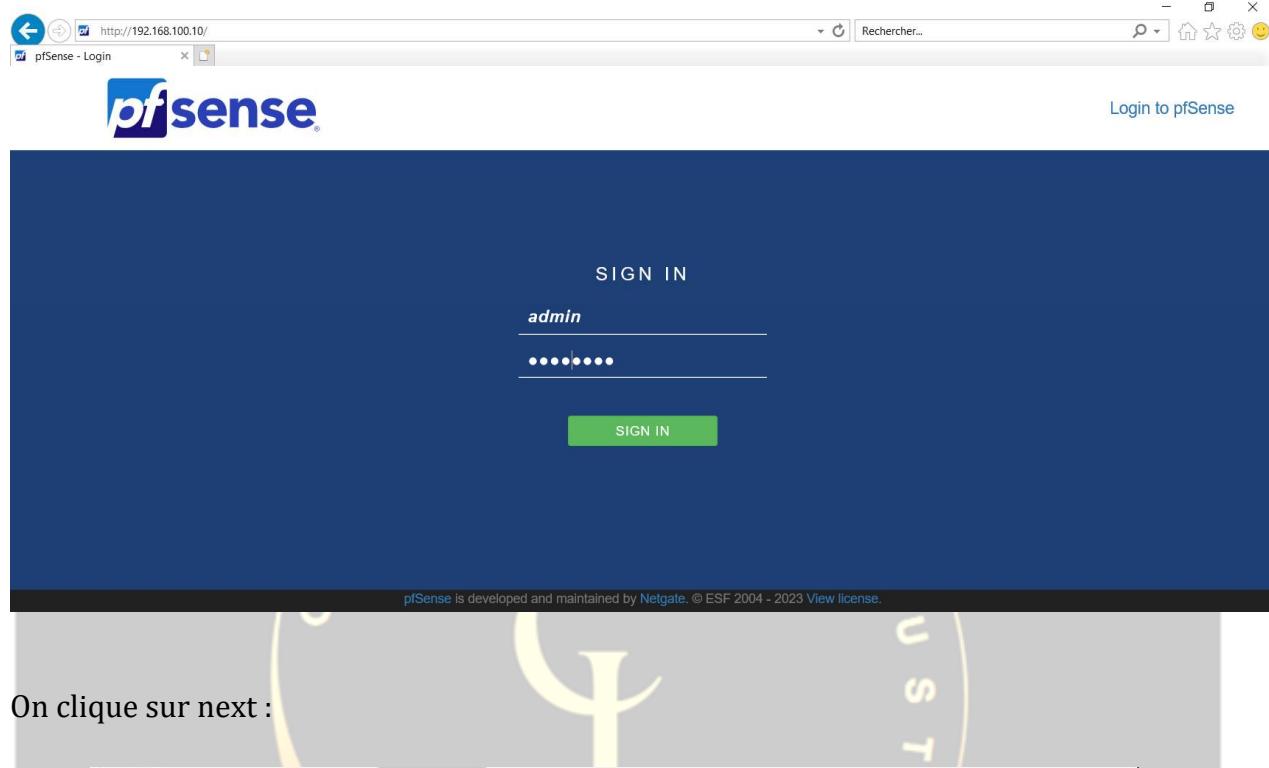
Do you want to enable the DHCP server on LAN? (y/n) n
```

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

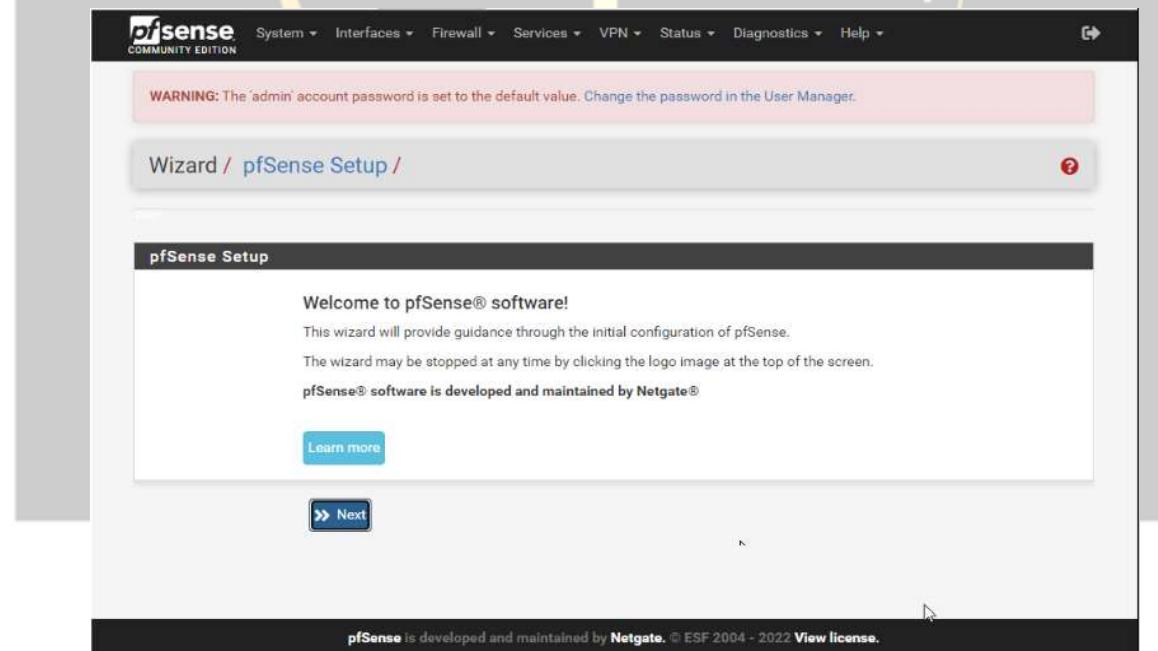
1.1.2. Configuration de base de PfSense

Noter que la procédure suivante est à faire sur les deux routeurs. Les informations par défaut pour se connecter sur la page web pfSense sont :

- Identifiant : admin
- Mot de passe : pfSense



On clique sur next :



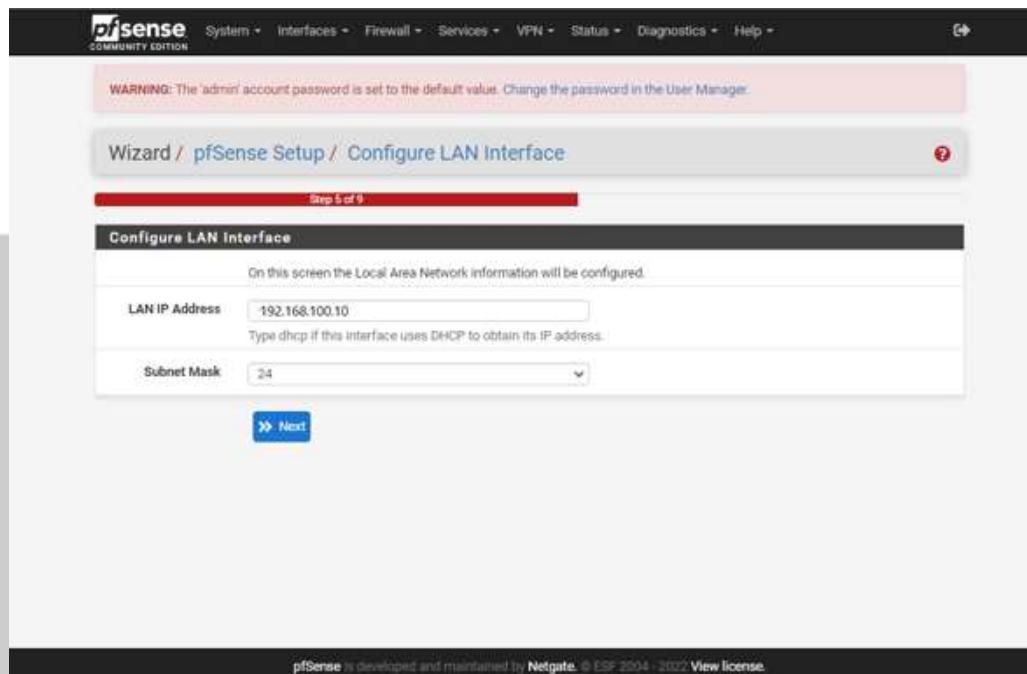
On indique le nom du routeur :

The screenshot shows the pfSense General Information setup screen. At the top, it says "Wizard / pfSense Setup / General Information" and "Step 2 of 9". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The "General Information" section contains fields for Hostname (SRV-SECVRTE01) and Domain (home.arpa). Below these fields is a note about DNS Resolver behavior. There are also fields for Primary DNS Server and Secondary DNS Server, both of which are currently empty. At the bottom of the screen, there is an "Override DNS" button.

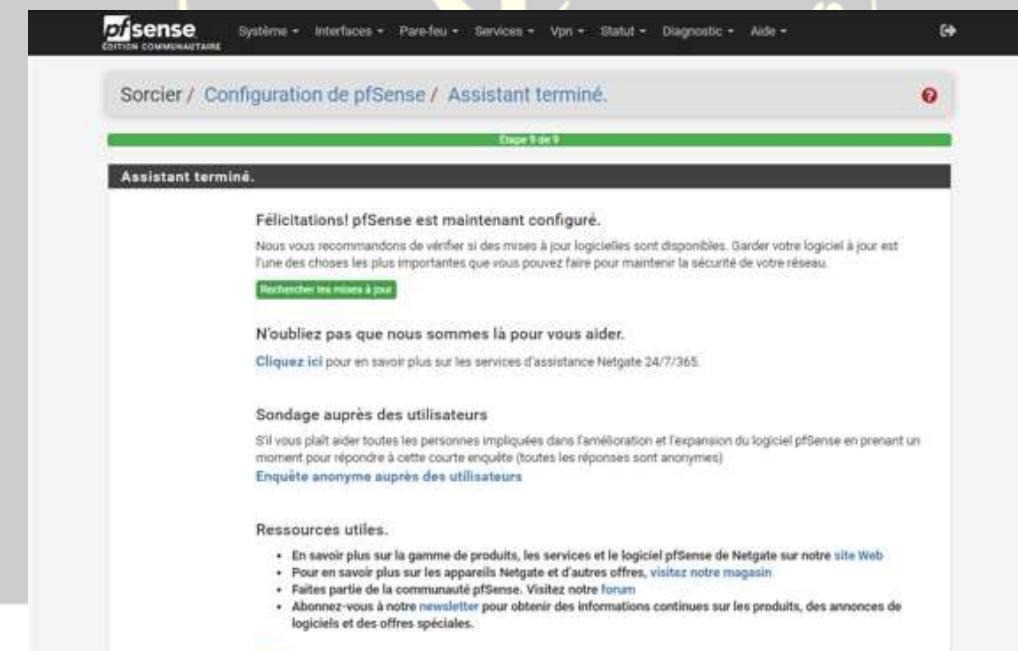
Pour le routeur 2 :

The screenshot shows the pfSense General Information setup screen. At the top, it says "Wizard / pfSense Setup / General Information" and "Step 2 of 9". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The "General Information" section contains fields for Hostname (SRV-SECVRTE02) and Domain (home.arpa). Below these fields is a note about DNS Resolver behavior. There are also fields for Primary DNS Server and Secondary DNS Server, both of which are currently empty. At the bottom of the screen, there is an "Override DNS" button.

On indique à nouveau l'adresse IP du serveur et son masque de sous réseau. Celui-ci correspond au routeur 1, le **routeur 2** il est en **192.168.100.20**.



On continue en cliquant sur « next » jusqu'à atteindre l'option « reload » puis nous arriverons à la fin de la configuration de base.

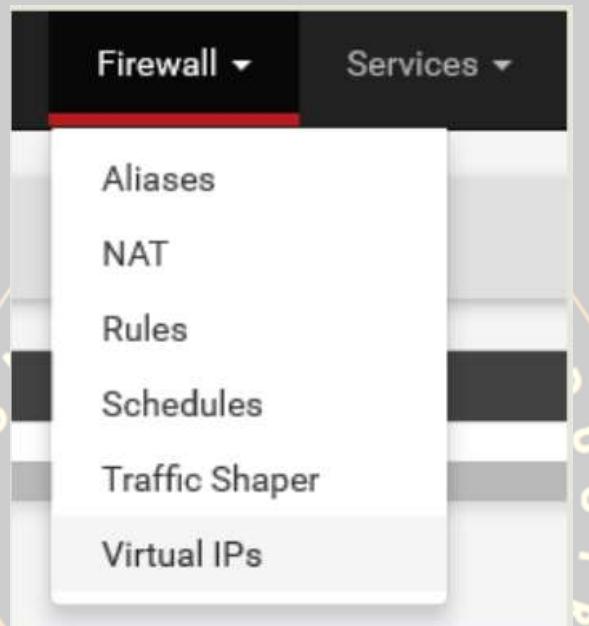


1.1.3. Mise en place du CARP

Pour la mise en place du CARP qui va permettre à nos deux retour de partager la même adresse IP sur un même réseau. Dans notre cas, elles auront les mêmes adresses virtuelles. Elles seront également redondées. Nous allons mettre en place 3 CARP : pour le WAN, le LAN et la DMZ. C'est à reproduire sur le second serveur.

a. CARP WAN :

Tout d'abord, dirigeons-nous vers la page de création d'adresses virtuelles :



Voilà les adresses virtuelles que vous devez créer, pour cela cliquer sur « ADD » :

A screenshot of the pfSense Firewall / Virtual IPs configuration page. The page title is 'Firewall / Virtual IPs'. The table shows three existing entries:

Virtual IP Address	Interface	Type	Description	Actions
192.168.10.10/24 (vhid: 1)	WAN	CARP	CARP-WAN	
192.168.100.254/24 (vhid: 2)	LAN	CARP	CARP-LAN	
192.168.200.254/24 (vhid: 3)	SEC1VDMZ	CARP	CARP-DMZ	

At the bottom right of the table is a green 'Add' button with a '+' icon.

On sélectionne CARP sur l'interface WAN, puis l'adresse virtuelle souhaité avec un mot de passe. On peut ajouter une description pour les différencier et on sauvegarde. On effectue la même procédure pour les CARP LAN et DMZ.

The screenshot shows the 'Edit Virtual IP' configuration for the WAN interface. The 'Type' is set to 'CARP'. The 'Address(es)' field contains '192.168.10.10' with a subnet mask of '/24'. A 'Virtual IP Password' is entered twice. The 'VHID Group' is set to '1'. The 'Advertising frequency' is set to '1' (Base) and '0' (Skew). A description 'CARP-WAN' is provided. A 'Save' button is at the bottom.

b. CARP LAN :

The screenshot shows the 'Edit Virtual IP' configuration for the LAN interface. The 'Type' is set to 'CARP'. The 'Address(es)' field contains '192.168.100.254' with a subnet mask of '/24'. A 'Virtual IP Password' is entered twice. The 'VHID Group' is set to '2'. The 'Advertising frequency' is set to '1' (Base) and '0' (Skew). A description 'CARP-LAN' is provided. A 'Save' button is at the bottom.

c. CARP DMZ :

The screenshot shows the 'Edit Virtual IP' configuration page. The 'Type' is set to 'CARP'. The 'Interface' is 'SECIVDMZ'. The 'Address type' is 'Single address' with value '192.168.200.254' and subnet mask '/24'. The 'Virtual IP Password' is masked. The 'VHID Group' is '3'. The 'Advertising frequency' is '1' (Base) and '0' (Skew). The 'Description' is 'CARP-DMZ'. A note says: 'The mask must be the network's subnet mask. It does not specify a CIDR range.' Below the form is a 'Save' button.

d. Redondance CARP :

La redondance CARP va nous permettre d'assurer la redondance IP entre les deux serveurs. Nous avons besoin, tout simplement, de vérifier qu'elle soit activé. La plupart du temps la redondance s'active automatiquement.

Routeur 1

The screenshot shows the 'Status / CARP' screen. It displays the 'CARP Interfaces' table:

CARP Interface	Virtual IP	Status
WAN@1	192.168.10.10/24	BACKUP
LAN@2	192.168.100.254/24	BACKUP
SECIVDMZ@3	192.168.200.254/24	BACKUP

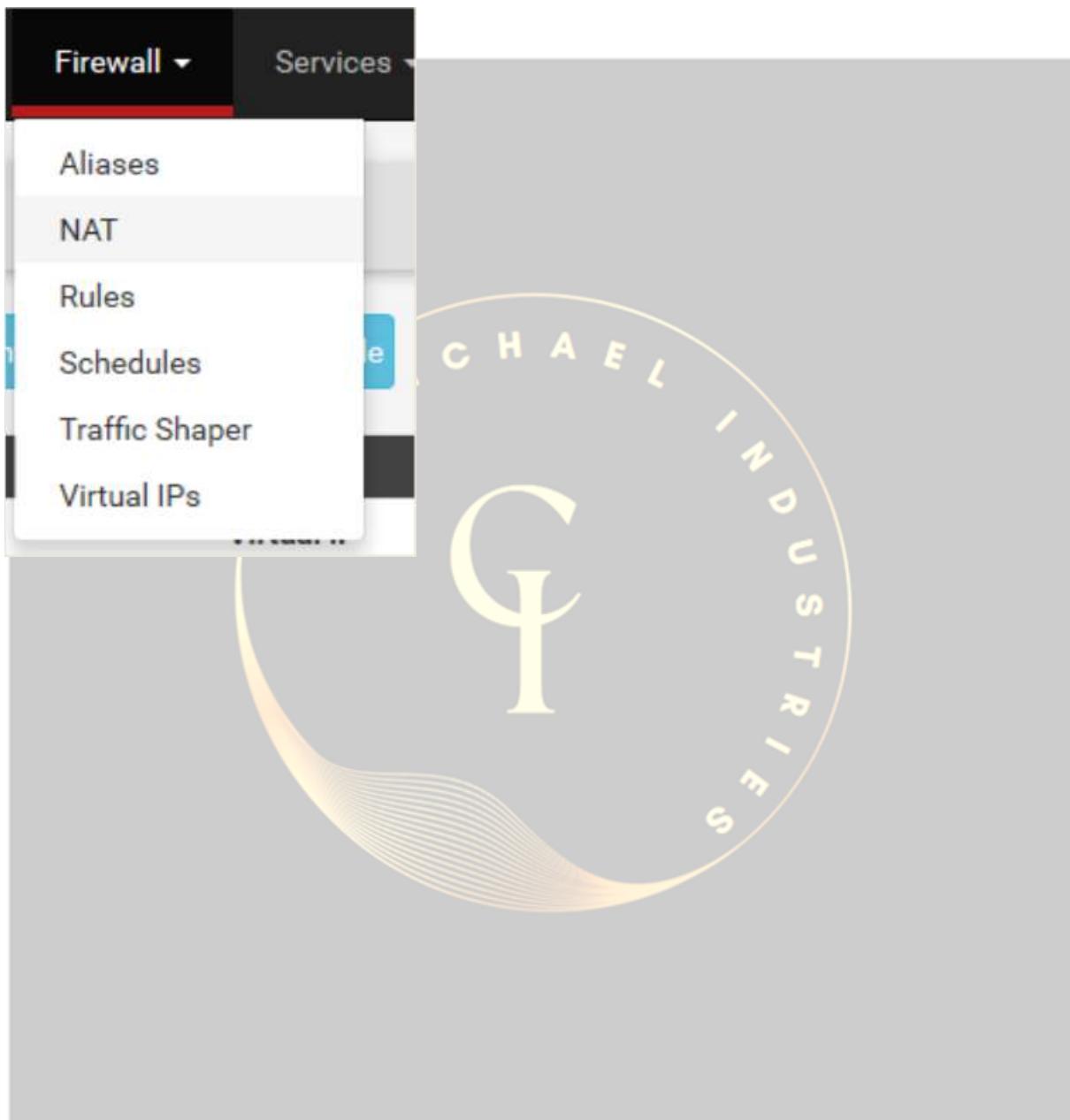
Below the table is the 'pfSync Nodes' section, which lists:

- 9f6aeb45
- c970917f
- d7286578
- f6dd1c5b

Routeur 2

1.1.4. Utilisation des IP virtuelles

Malheureusement, les IP virtuelles doivent être forcées à travers la mise en place d'une règle de redirection. On va se rendre sur la page NAT :



On sélectionne « Outbound » et on sauvegarde.

The screenshot shows the pfSense configuration interface under the Firewall / NAT / Outbound tab. The 'Outbound' tab is active. Under 'Outbound NAT Mode', the 'Hybrid Outbound NAT rule generation' option is selected. There are four modes listed:

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

Puis on va cliquer sur « Add » sous « Mappings ». On va en créer trois pour chaque interface. Voici ce que vous devez avoir à la fin :

The screenshot shows the pfSense configuration interface under the Firewall / NAT / Outbound tab. A green message bar at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, the 'Outbound' tab is active. Under 'Outbound NAT Mode', the 'Hybrid Outbound NAT rule generation' option is selected. The 'Mappings' table shows three entries for different interfaces:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
SECIVDMZ	192.168.200.0/24	*	*	*	192.168.200.254	*			<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
LAN	192.168.100.0/24	*	*	*	192.168.100.254	*		Using-Virtual-IP-LAN	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
WAN	192.168.10.0/24	*	*	*	192.168.10.10	*		Using-Virtual-IP-WAN	<input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

At the bottom, there are buttons for 'Save' and 'Add'. The 'Automatic Rules' table shows two entries:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	*	WAN address	*	✗	Auto created rule

a. Redirection WAN

On informe l'interface, la source et dans « translation » l'ip de la CARP WAN créée auparavant. Il faut effectuer la même procédure pour la redirection LAN et DMZ.

The screenshot shows the 'Edit Advanced Outbound NAT Entry' configuration. Key settings include:

- Interface:** WAN
- Address Family:** IPv4
- Protocol:** any
- Source:** Network 192.168.10.0 / 24
- Destination:** Any
- Translation:** Address 192.168.10.10 (CARP-WAN)

b. Redirection LAN

The screenshot shows the 'Edit Advanced Outbound NAT Entry' configuration. Key settings include:

- Interface:** LAN
- Address Family:** IPv4
- Protocol:** any
- Source:** Network 192.168.100.0 / 24
- Destination:** Any
- Translation:** Address 192.168.100.254 (CARP-LAN)

c. Redirection DMZ

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Outbound / Edit' section. The configuration is for an 'Advanced Outbound NAT Entry'. Key settings include:

- Disabled:** Disable this rule
- Do not NAT:** Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.
- Interface:** SECIVDMZ
- Address Family:** IPv4
- Protocol:** any
- Source:** Network / 192.168.200.0 / 24
- Destination:** Any / 192.168.200.0 / 24
- Not:** Invert the sense of the destination match.
- Translation:**
 - Address:** 192.168.200.254 (CARP-DMZ)
 - Port or Range:** _____ Static Port

N'oubliez pas d'appliquer les changements à chaque fin de redirection.

d. Test des adresses virtuelles

A l'aide de l'invite de commande (touche Windows + r puis cmd) tapez vos adresses ip virtuelles afin de vérifier qu'elles répondent bien et fonctionnent.

IP virtuelle du LAN

```
C:\Users\Administrateur>ping 192.168.100.254

Envoy d'une requête 'Ping' 192.168.100.254 avec 32 octets de données :
Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64
```

IP virtuelle du WAN

```
C:\Users\Administrateur>ping 192.168.10.10

Envoy d'une requête 'Ping' 192.168.10.10 avec 32 octets de données :
Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.10 : octets=32 temps<1ms TTL=64
```

IP virtuelle de la DMZ

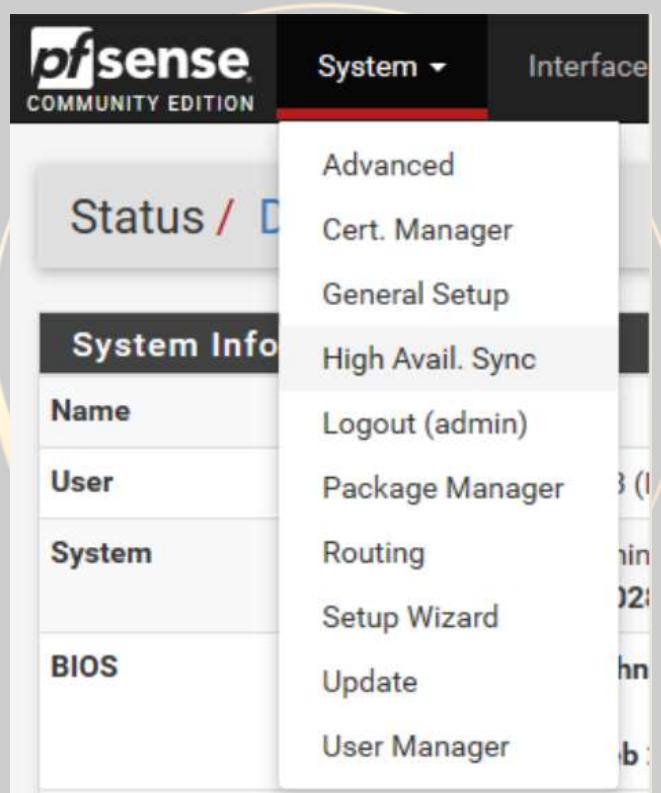
```
C:\Users\Administrateur>ping 192.168.200.254
```

```
Envoi d'une requête 'Ping' 192.168.200.254 avec 32 octets de données :  
Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64  
Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64
```

1.1.5. Synchronisation des PfSense

Maintenant que nous avons mis en place le protocole CARP et la redondance des adresses virtuelles, nous allons configurer la Haute Disponibilité des serveurs. Afin que nos PfSense puisse se synchroniser l'un avec l'autre. Il y aura un master et un esclave. Ce dernier récupérera la configuration du master. Ainsi, si un des deux tombe en panne l'autre pourra prendre le relais.

Rendons-nous sur l'interface High Avail. Sync :



On informe les informations suivantes et on sauvegarde :

- L'interface : LAN
- L'adresse IP du serveur avec qui la synchronisation doit se faire : routeur 2
- L'adresse IP du serveur sur lequel notre routeur 1 va récupérer la configuration
- L'identifiant et le mot de passe du routeur 2
- On coche la case « Synchronise admin »
- On coche toutes les cases

The screenshot shows the pfSense web interface under the 'System / High Availability Sync' section. It displays two main configuration sections:

- State Synchronization Settings (pfsync)**
 - Synchronize states**: Describes pfsync as transferring state insertion, update, and deletion messages between firewalls via multicast on a specified interface.
 - Synchronize Interface**: Set to "LAN". Notes that synchronization is enabled on this interface.
 - pfsync Synchronize Peer IP**: Set to "192.168.100.20". Notes that setting this option will force pfsync to synchronize its state table to this IP address.
- Configuration Synchronization Settings (XMLRPC Sync)**
 - Synchronize Config to IP**: Set to "192.168.100.20". Notes that XMLRPC sync is supported over connections using the same protocol and port.
 - Remote System Username**: Set to "admin". Notes that the webConfigurator username must be entered here.
 - Remote System Password**: Two fields for password and confirmation.
 - Synchronize admin**: A checkbox for "synchronize admin accounts and autoupdate sync password". Notes that by default, the admin account does not synchronize, and each node may have a different admin password.

At the bottom, a sidebar titled "Select options to sync" lists various configuration items with checkboxes, all of which are checked. A "Save" button is at the bottom right.

On fait la même chose sur le

routeur 2, sauf qu'on informe les informations du routeur 1 :

The screenshot shows the pfSense web interface under the 'System / High Availability Sync' section. It includes sections for State Synchronization Settings (pfsync) and Configuration Synchronization Settings (XMLRPC Sync), along with a detailed configuration panel at the bottom.

State Synchronization Settings (pfsync)

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

Synchronize Interface: LAN
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.

pfsync Synchronize: Peer IP: 192.168.100.10
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: 192.168.100.10
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.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync:

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

Toggle All

Save

a. Test de la synchronisation

Sur le routeur 1, nous avons configuré la redirection de la DMZ :

The screenshot shows the Outbound NAT configuration on Router 1. The 'Outbound' tab is selected. Under 'Mode', 'Hybrid Outbound NAT rule generation' is chosen. The 'Mappings' section lists three entries:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
SECIVDMZ	192.168.200.0/24	*	*	*	192.168.200.254	*			
LAN	192.168.100.0/24	*	*	*	192.168.100.254	*		Using-Virtual-IP-LAN	
WAN	192.168.10.0/24	*	*	*	192.168.10.10	*		Using-Virtual-IP-WAN	

The 'Automatic Rules' section shows two entries:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	500	WAN address	*		Auto created rule for ISAKMP
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	*	WAN address	*		Auto created rule

Sur le routeur 2, il a bien été répliqué :

The screenshot shows the Outbound NAT configuration on Router 2. The 'Outbound' tab is selected. Under 'Mode', 'Hybrid Outbound NAT rule generation' is chosen. The 'Mappings' section lists three entries:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
SECIVDMZ	192.168.200.0/24	*	*	*	192.168.200.254	*			
LAN	192.168.100.0/24	*	*	*	192.168.100.254	*		Using-Virtual-IP-LAN	
WAN	192.168.10.0/24	*	*	*	192.168.10.10	*		Using-Virtual-IP-WAN	

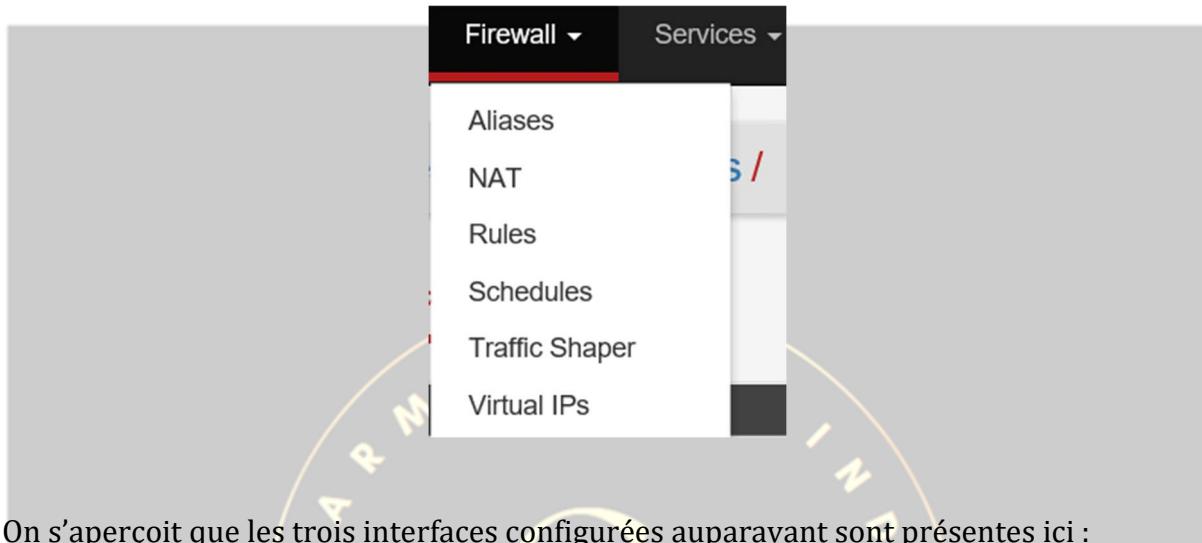
The 'Automatic Rules' section shows two entries:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	500	WAN address	*		Auto created rule for ISAKMP
WAN	127.0.0.0/8 ::1/128 192.168.100.0/24 192.168.200.0/24 192.168.110.0/24	*	*	*	WAN address	*		Auto created rule

1.1.6. Mise en place des règles de pare-feu

A savoir que de base pour vérifier que tout fonctionne au niveau de nos configurations, les règles de pare-feu seront configurées pour que tout puisse traverser et de n'importe quelle source. Sachez aussi qu'il y a un ordre sur les règles, le routeur va les lire de haut en bas.

Par exemple, dirigez-vous ici :



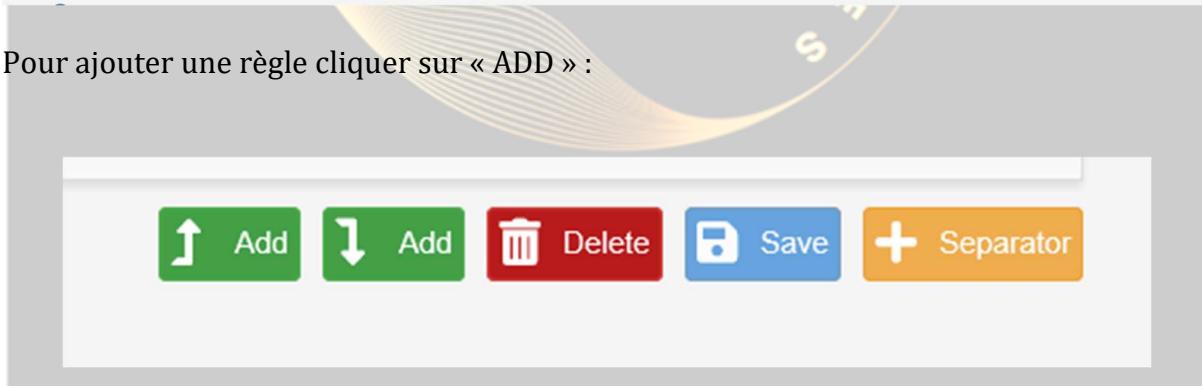
On s'aperçoit que les trois interfaces configurées auparavant sont présentes ici :

A screenshot of a 'Rules' configuration table. At the top, there are tabs for 'Floating', 'WAN' (which is selected and highlighted in red), 'LAN', and 'SECIV/DMZ'. The table has a header row with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are two rows of data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /33 KiB	IPv4 *	*	*	*	*	*	none			
0 /0 B	IPv4 *	*	*	*	*	*	none		BLOCK EVERYTHING	

At the bottom of the table are buttons for 'Add' (with up and down arrows), 'Delete', 'Save', and 'Separator'.

Pour ajouter une règle cliquer sur « ADD » :



Et vous informez les informations suivantes :

- Pass : car on veut tout autoriser
- WAN : car on est sur cette interface mais on procède de la même manière pour les interfaces LAN et DMZ
- Any : pour le protocole, la source et la destination car on accepte tout
- On pense à sauvegarder

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Pass'. The 'Interface' dropdown is set to 'WAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'Any'. Under the 'Source' section, the 'Source' dropdown is set to 'any'. Under the 'Destination' section, the 'Destination' dropdown is set to 'any'. In the 'Extra Options' section, the 'Log' checkbox is unchecked. The 'Description' field contains 'ALLOW EVERYTHING'. The status bar at the bottom shows tabs for Floating, WAN, LAN (which is selected), and SEC1VDMZ.

On reproduit la même chose sur le LAN et la DMZ :

The screenshot shows the 'Firewall / Rules / LAN' configuration page. The 'LAN' tab is selected. There are two rules listed: one for 'any' source and destination with 'Action: Pass', and another for 'any' source and destination with 'Action: Allow Everything'. The status bar at the bottom shows tabs for Floating, WAN, LAN (selected), and SEC1VDMZ.

On cliquera sur ADD aussi et on procède de la même manière :

The screenshot shows the pfSense Firewall Rules Edit screen. The rule being edited has the following settings:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** Any
- Source:** Source: any, Destination: any
- Destination:** Destination: any
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** ALLOW EVERYTHING

Et pour la DMZ :

The screenshot shows the pfSense Firewall Rules Edit screen. The rule being edited has the following settings:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** SECIVDMZ
- Address Family:** IPv4
- Protocol:** Any
- Source:** Source: any, Destination: any
- Destination:** Destination: any
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** ALLOW EVERYTHING

Cependant, ce type de règles n'est absolument pas restrictive, elle accorde l'accès à tout le monde présent sur le réseau. C'est pourquoi, nous allons élaborer d'autres règles et supprimés celles qui autorisent tout.

Tout d'abord, nous bloquerons l'accès à tout. C'est la même procédure qu'avant sauf qu'au lieu de « pass » on renseignera « block ». On effectue ça sur les trois interfaces :

Edit Firewall Rule

Action: Block

Disabled: Disable this rule

Interface: SEC1VDMZ

Address Family: IPv4

Protocol: Any

Source: Source: any, Destination: any

Destination: Destination: any

Extra Options:

- Log: Log packets that are handled by this rule
- Description: BLOCK EVERYTHING

Edit Firewall Rule

Action: Block

Disabled: Disable this rule

Interface: LAN

Address Family: IPv4

Protocol: Any

Source: Source: any, Destination: any

Destination: Destination: any

Extra Options:

- Log: Log packets that are handled by this rule
- Description: BLOCK EVERYTHING

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' dropdown is set to 'WAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'Any'. Under the 'Source' section, the 'Source' dropdown is set to 'any' and the 'Destination' dropdown is also set to 'any'. Under the 'Extra Options' section, the 'Log' checkbox is unchecked. The 'Description' field contains the text 'BLOCK EVERYTHING'.

Ensuite, nous allons accorder un accès aux réseaux que l'on souhaite. Pour le WAN par exemple, on va autoriser les accès provenant du LAN vers le WAN :

The screenshot shows the 'SECIVDMZ' tab selected in the 'Rules' list. There are three rules listed:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	SECIVDMZ net	*	*	none		ALLOW LAN TO DMZ FROM ANY PROTOCOL	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	*	none		ALLOW ALL	
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none		BLOCK EVERYTHING	

At the bottom, there are buttons for 'Add' (green), 'Save' (blue), and 'Separator' (orange).

pfSense 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: LAN

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 LAN net Source Address /

[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

Destination: Invert match Single host or alias 192.168.100.40 /

Destination Port Range: SMTP (25) 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



Puis, sur l'interface LAN, les règles seront beaucoup plus abondantes et restrictives. Nous allons autoriser :

- Tous le protocoles provenant de n'importe quelle source sur le port 80 du LAN (par défaut)

The screenshot shows the pfSense Firewall Rules Edit interface. A new rule is being created with the following settings:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** SEC1VDMZ
- Address Family:** IPv4
- Protocol:** Any
- Source:** Source: LAN net, Invert match:
- Destination:** Destination: SEC1VDMZ net, Invert match:
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** ALLOW LAN TO DMZ FROM ANY PROTOCOL

- Le protocole TCP du LAN à accéder au serveur de messagerie via le port SMTP

The screenshot shows the pfSense Firewall Rules configuration interface. A new rule is being created with the following details:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Source: Single host or alias, Value: 192.168.100.80
- Destination:** Destination: This firewall (self), Destination Address: 192.168.100.80
- Destination Port Range:** From: SNMP (161), To: SNMP (161)

- Le protocole TCP du serveur de

messagerie à accéder à nos deux routeurs via le protocole SNMP

- Le protocole TCP du LAN vers le port 443 de la DMZ

The screenshot shows the pfSense Firewall Rules Edit interface. A new rule is being created with the following settings:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Source: LAN net, Invert match: LAN net
- Destination:** Destination: any, Invert match: any, Destination Address: any
- Extra Options:** Destination Port Range: From: any, To: any, Custom: Custom

protocole TCP du LAN vers tout

Autoriser le LAN à tout (par défaut)

pfSense 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: LAN
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 /

Destination

Destination: Invert match any Destination Address /

Destination Port Range: any 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

- Bloquer tout : règle vu plus haut

Et voilà ce que cela donné :

Floating WAN LAN SECIVDMZ

Rules (Drag to Change Order)

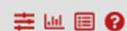
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 /2.75 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0 /0 B	IPv4 TCP	LAN net	*	192.168.100.40	25 (SMTP)	*	none		ALLOW CLIENTS ON LAN TO ACCESS SRV-SECIVMES	
✗ 0 /0 B	IPv4 TCP	192.168.100.80	*	This Firewall	161 (SNMP)	*	none		ALLOW SRV-SECIVSUP TO SRV-SECIVRTE01 THROUGH PROTO SNMP	
✗ 0 /0 B	IPv4 TCP	LAN net	*	SECIVDMZ net	443 (HTTPS)	*	none		ALLOW LAN TO DMZ	
✗ 0 /2.91 MIB	IPv4 TCP	LAN net	*	*	*	*	none		ALLOW REPLICA	
✗ 0 /2.19 MIB	IPv4	*	LAN net	*	*	*	*	none	Default allow LAN to any rule	
✗ 0 /0 B	IPv4	*	*	*	*	*	none		BLOCK EVERYTHING	

Add Add Delete Save Separator

Concernant la DMZ, nous autorisons pour l'instant simplement le réseau LAN vers la DMZ.



Firewall / Rules / Edit



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

Source

Invert match

Source Address /

Destination

Destination

Invert match

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.

Voici les règles de la DMZ :

Floating WAN LAN SECIVDMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 *	LAN net *	*	SECIVDMZ net *	*	*	none		ALLOW LAN TO DMZ FROM ANY PROTOCOL	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 TCP *	*	*	*	*	*	none		ALLOW ALL	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 *	*	*	*	*	*	none		BLOCK EVERYTHING	

Add Add Delete Save Separator

Et ceux du WAN :

The screenshot shows the pfSense Firewall Rules configuration. The WAN tab is selected. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	LAN net	*	*	*	*	none		ALLOW LAN TO WAN	
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/> ✗ 0 / 2 Kib	IPv4 *	*	*	*	*	*	none		BLOCK EVERYTHING	

Buttons at the bottom include Add, Save, and Separator.

Il ne reste plus que les règles pour le vpn :

WAN

<input type="checkbox"/> ✓ 0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN road warrior wizard	
------------------------------------	----------	---	---	-------------	----------------	---	------	--	-----------------------------	--

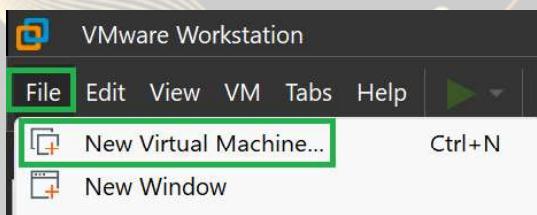
OpenVPN

<input type="checkbox"/> ✓ 0 / 102 Kib	IPv4 *	*	*	*	*	*	none		OpenVPN road warrior wizard	
--	--------	---	---	---	---	---	------	--	-----------------------------	--

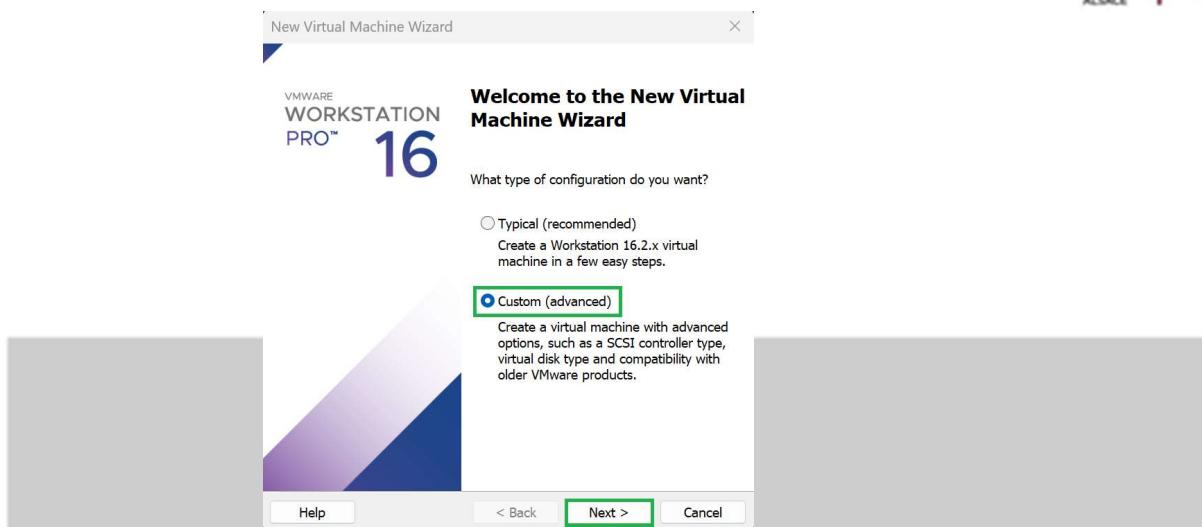
1.2. Serveur AD

1.2.1. Installation

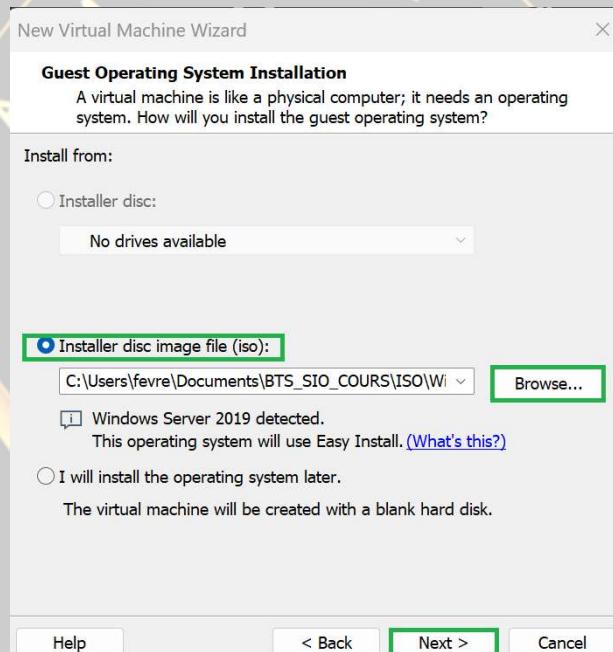
Pour ce projet, nous allons travailler sur Vmware Workstation 16 Pro. Nous allons créer une nouvelle machine virtuelle en cliquant sur File -> New Virtual Machine :



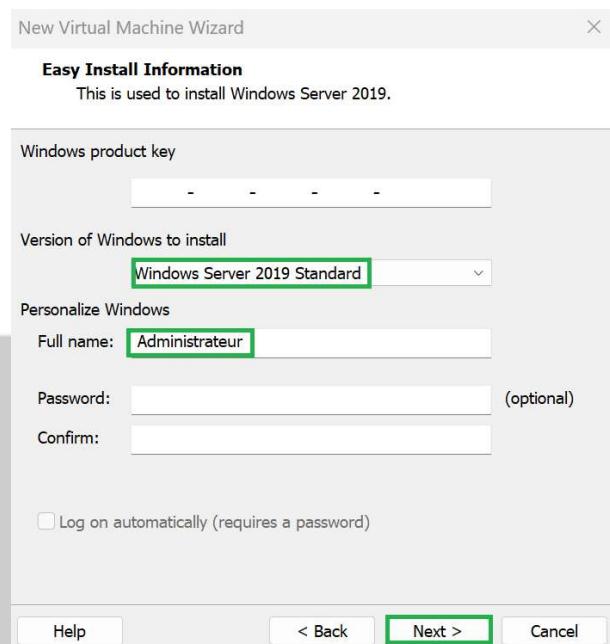
Choisir « Custom » :



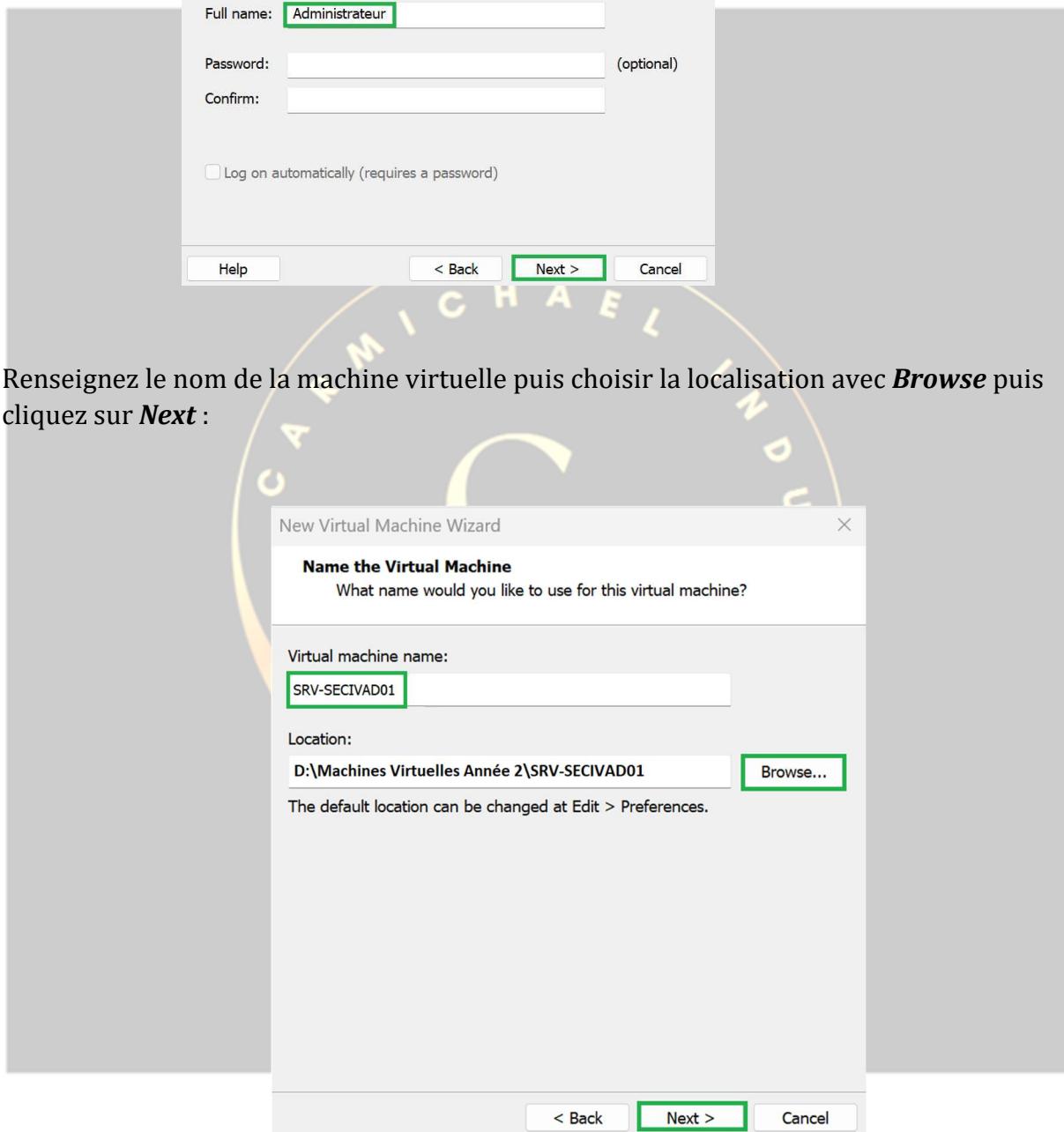
Cliquez ensuite sur **Next**, puis cochez « Installer disc image file (iso) » et cliquez sur **Browse** pour sélectionner le bon fichier iso puis cliquez sur **Next** :



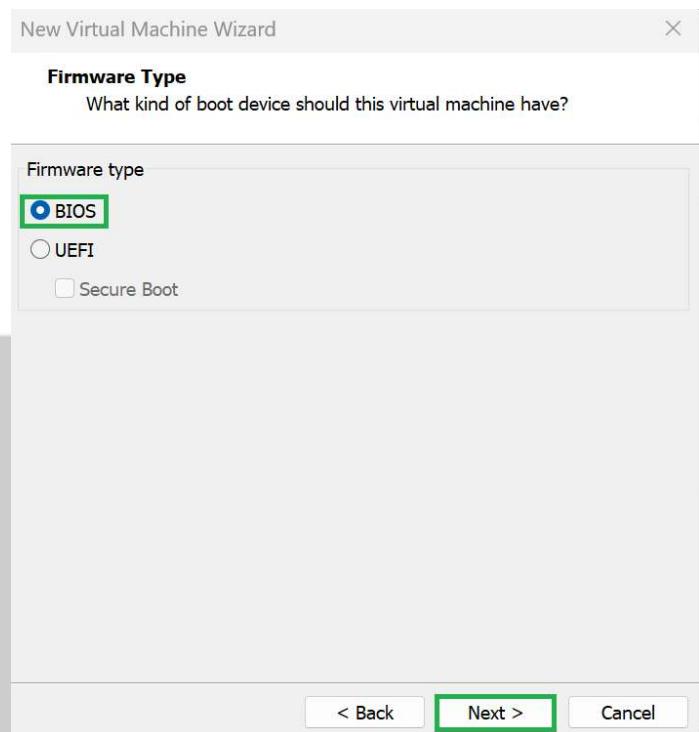
Choisir la version « **Standard** », renseignez un compte pour ouvrir une session au démarrage de la vm (Pour se logger automatiquement, il suffit de cocher « Log on auto » et de renseigner un mot de passe) Nous n'allons pas le faire ici et nous définirons le mot de passe plus tard.
Cliquez sur **Next** :



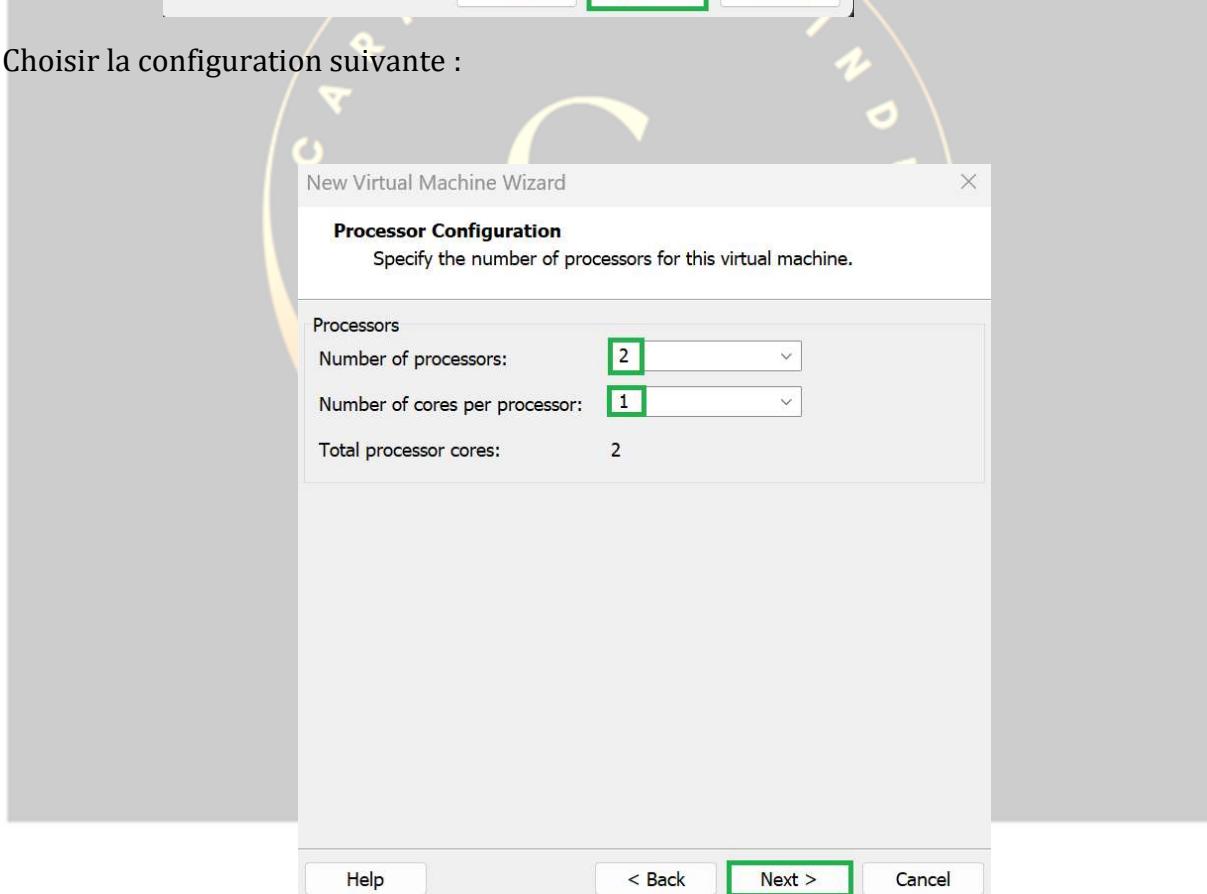
Renseignez le nom de la machine virtuelle puis choisir la localisation avec **Browse** puis cliquez sur **Next** :



Choisir « Bios » puis cliquez sur **Next** :



Choisir la configuration suivante :



Vu le nombre de machine à faire tourner sur le même ordinateur, nous allons lui attribuer le minimum recommandé, à savoir 2GB :

New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB

Memory for this virtual machine: **2048 MB**

Maximum recommended memory: 11.7 GB

Recommended memory: 2 GB

Guest OS recommended minimum: 1 GB

Help

< Back

Next >

Cancel

Ensuite :

New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

- Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
- Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
- Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.
- Do not use a network connection

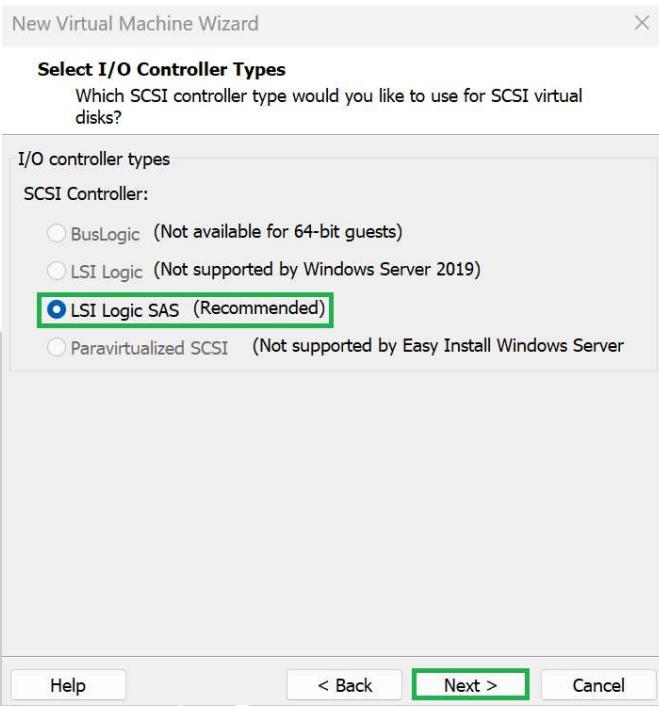
Help

< Back

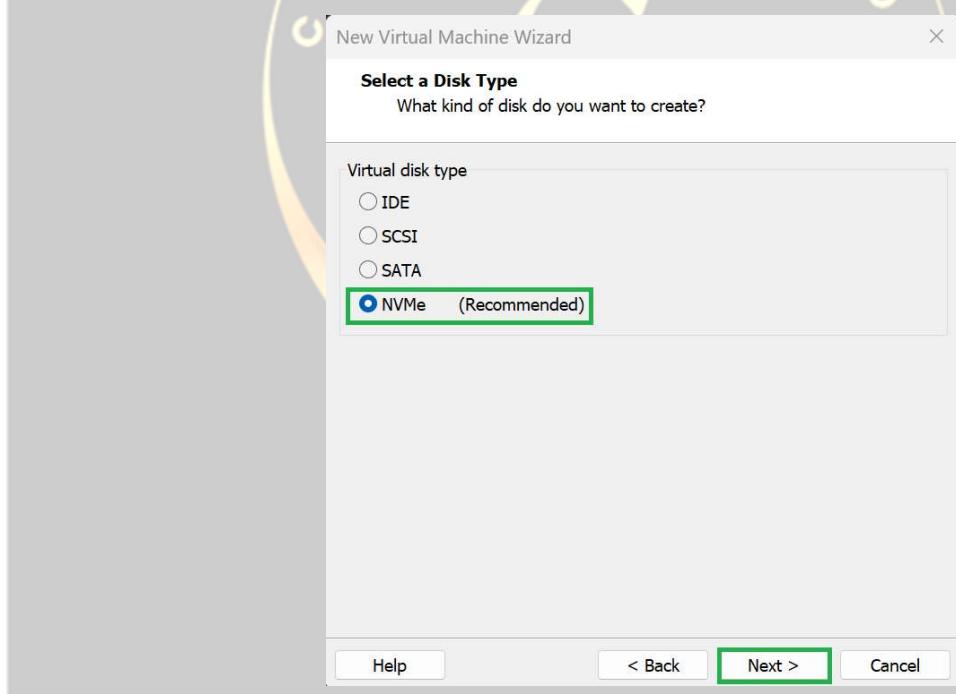
Next >

Cancel

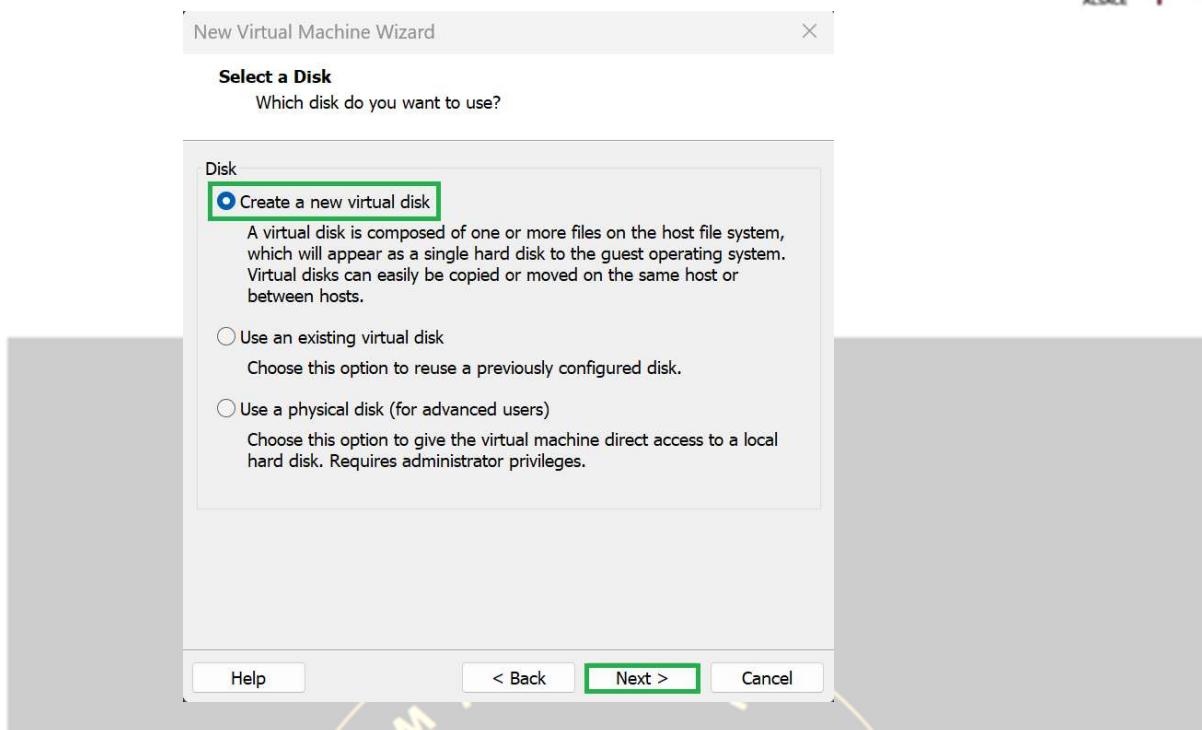
Et :



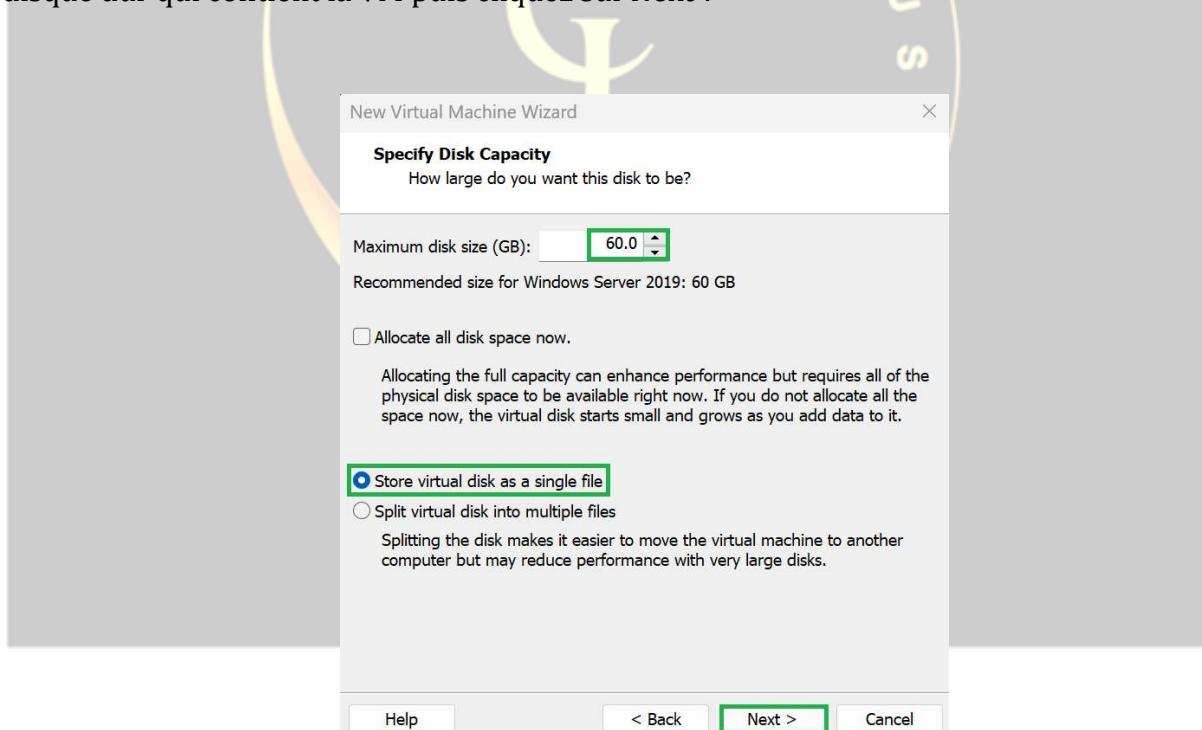
Puis :



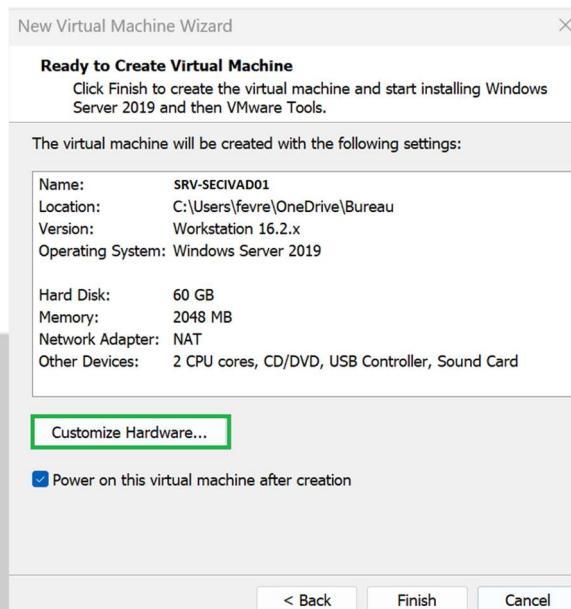
Créer un nouveau disque virtuel et cliquez sur **Next** :



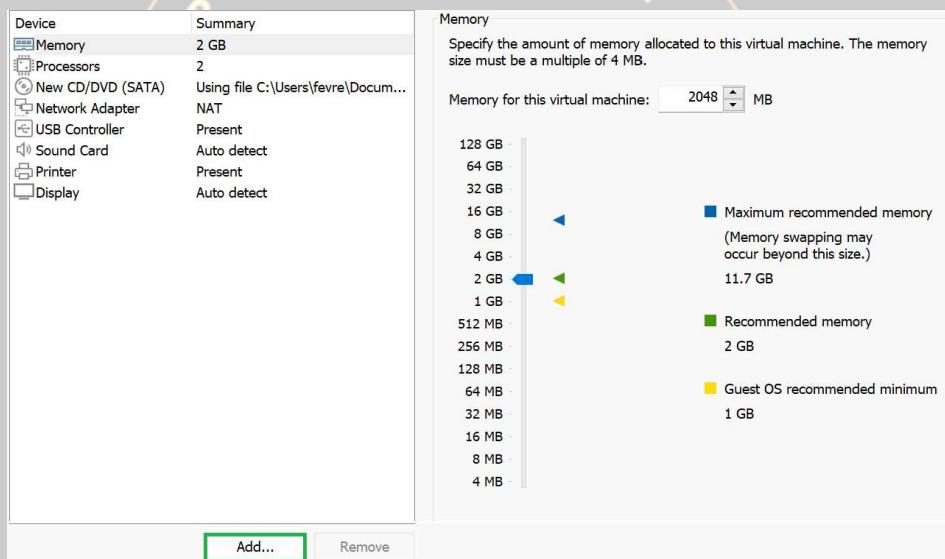
Conformément à la demande du projet, le disque sera de 60 GB et nous allons choisir la première option et surtout de ne pas l'allouer entièrement pour préserver la place sur le disque dur qui contient la VM puis cliquez sur **Next** :



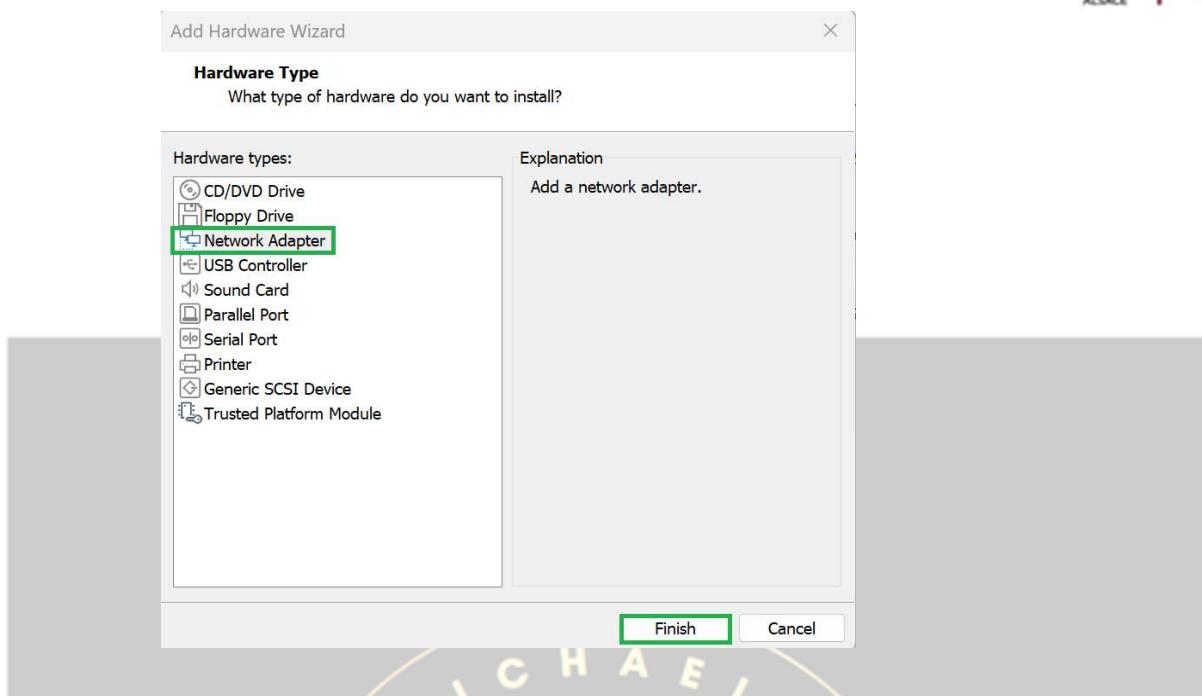
Cliquez sur **Next**, une fenêtre de la sorte se présentera alors à vous. Cliquez sur **Customize Hardware** :



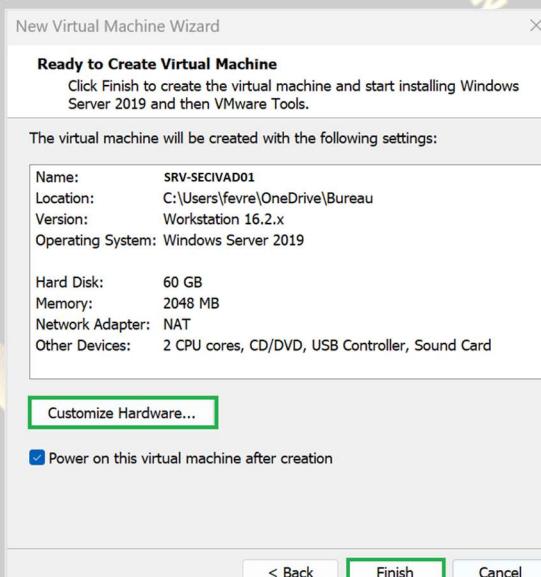
Cliquez sur **Add** :



On va ajouter une deuxième carte réseau, cliquez sur **network Adapter** puis cliquez sur **Next** :



Ensuite cliquez sur **Finish** :

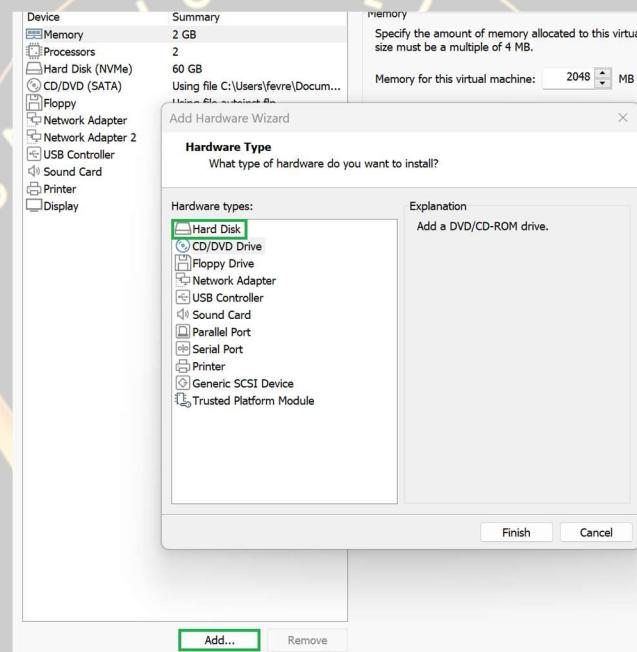


Nous allons maintenant ajouter un deuxième disque comme demander dans les spécifications techniques propre au projet.

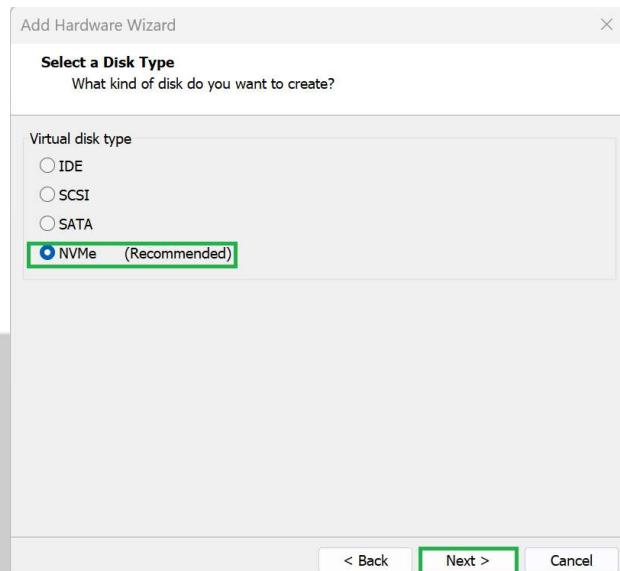
Pour cela, cliquez sur **Edit virtual machine settings** :



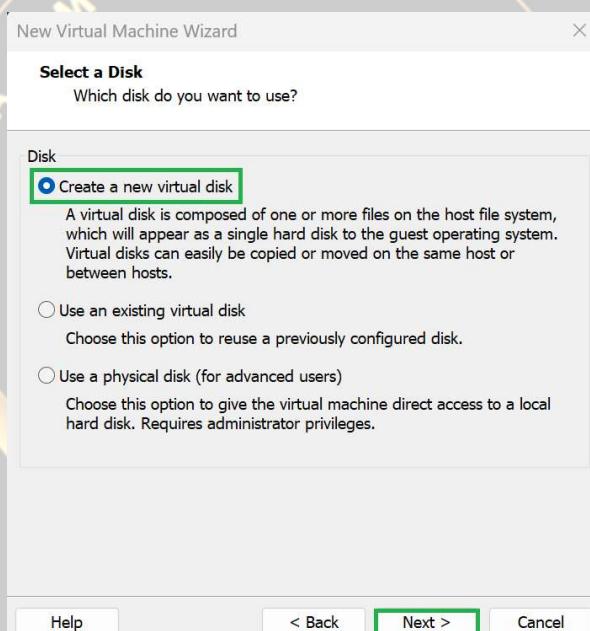
Cliquez sur **Add** puis sur **Hard Disk** :



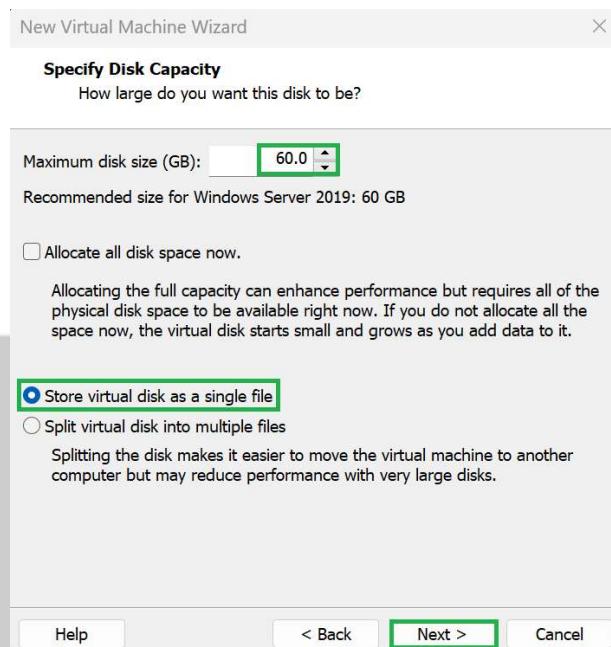
Puis :



Ensuite :



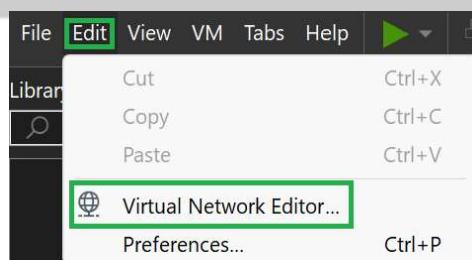
Et comme pour le premier disque :



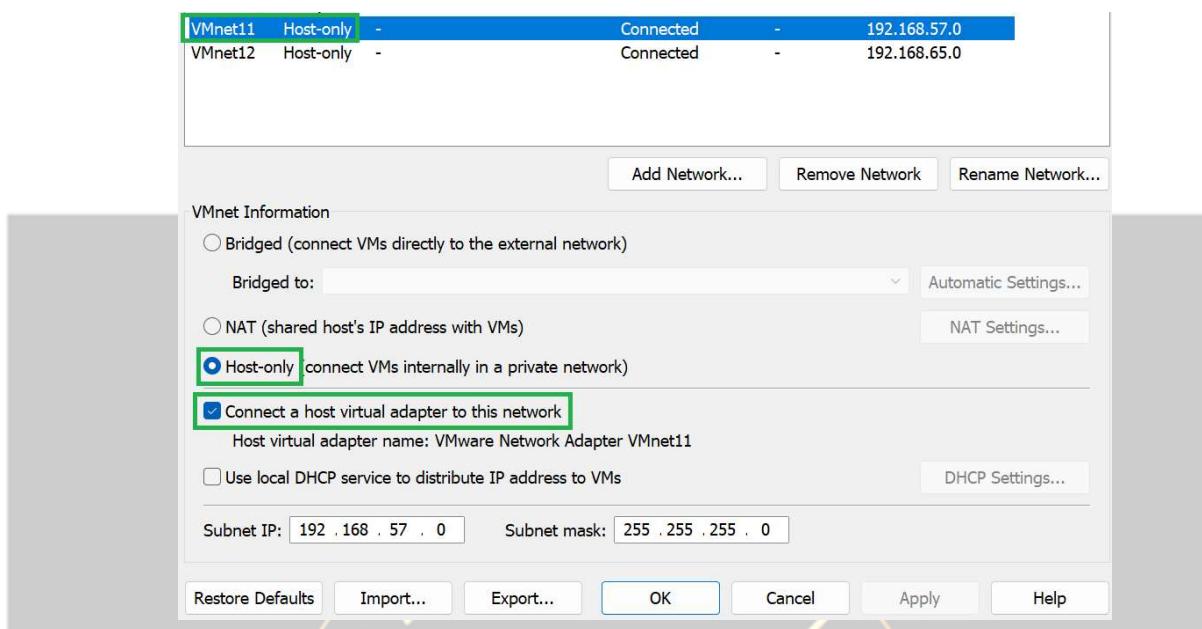
Après validation, nous pouvons voir les deux disques durs ainsi que les deux cartes réseaux qu'on aura mis sur le Vmnet11 en custom :

Hardware Options	
Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	60 GB
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet11)
Network Adapter 2	Custom (VMnet11)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

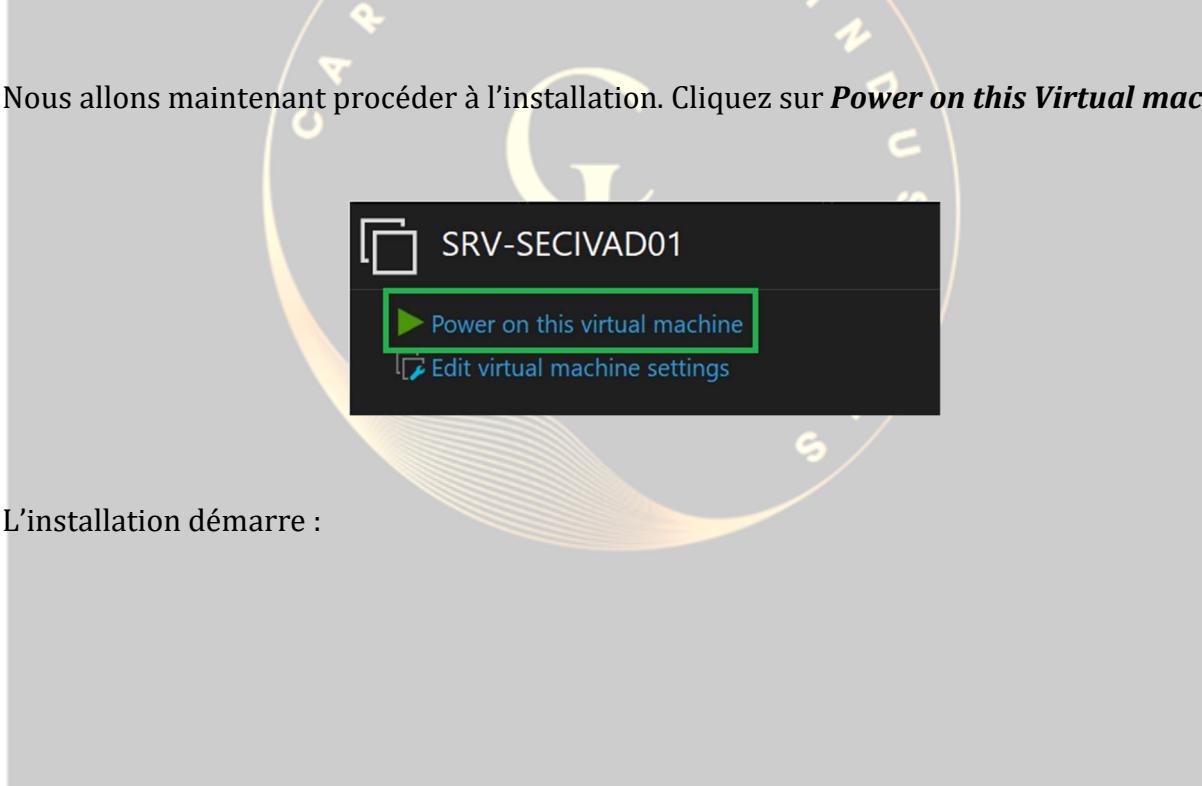
Pour ce qui est du Network Editor :



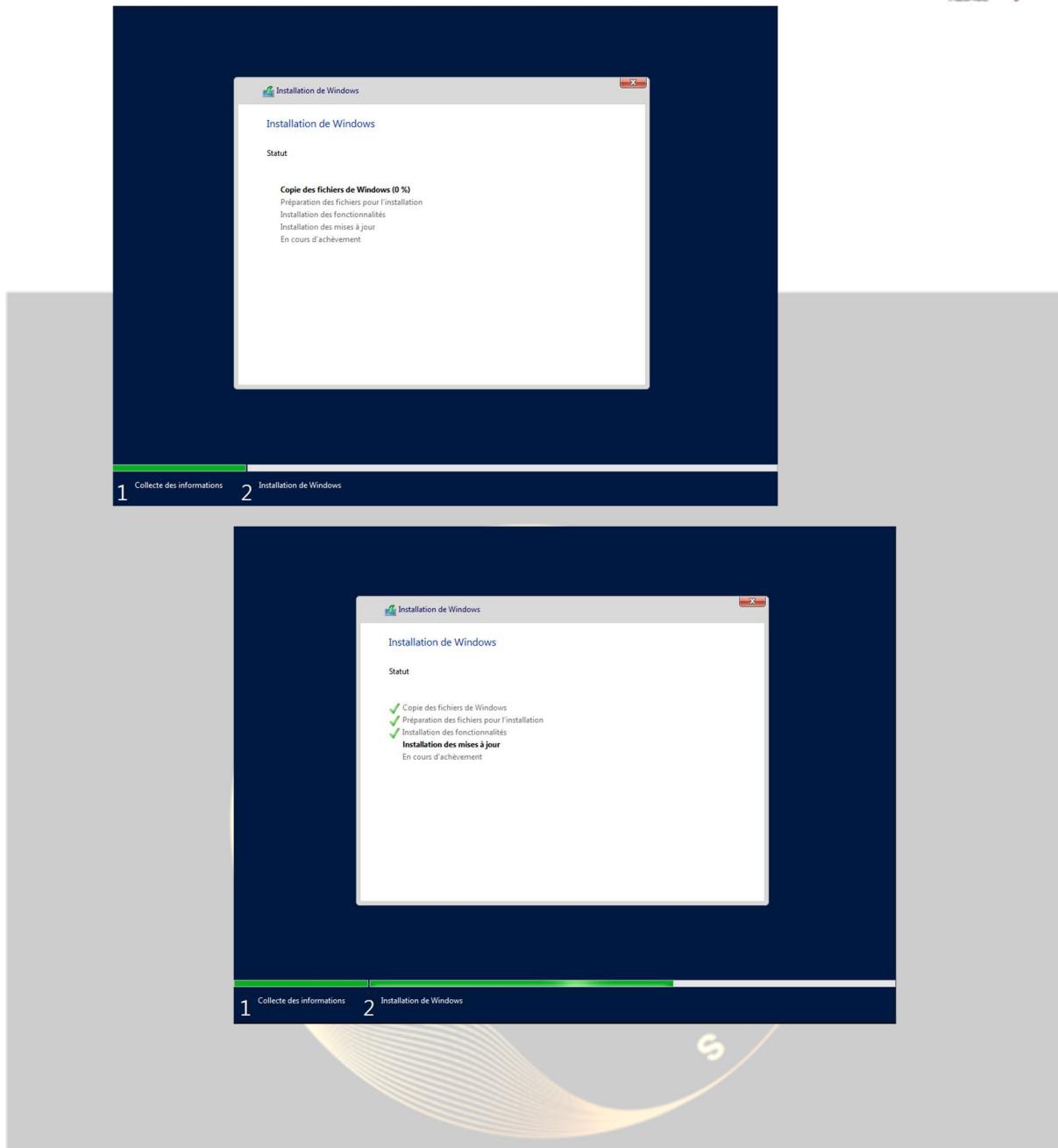
Voici les réglages du vmnet11 :



Nous allons maintenant procéder à l'installation. Cliquez sur **Power on this Virtual machine** :

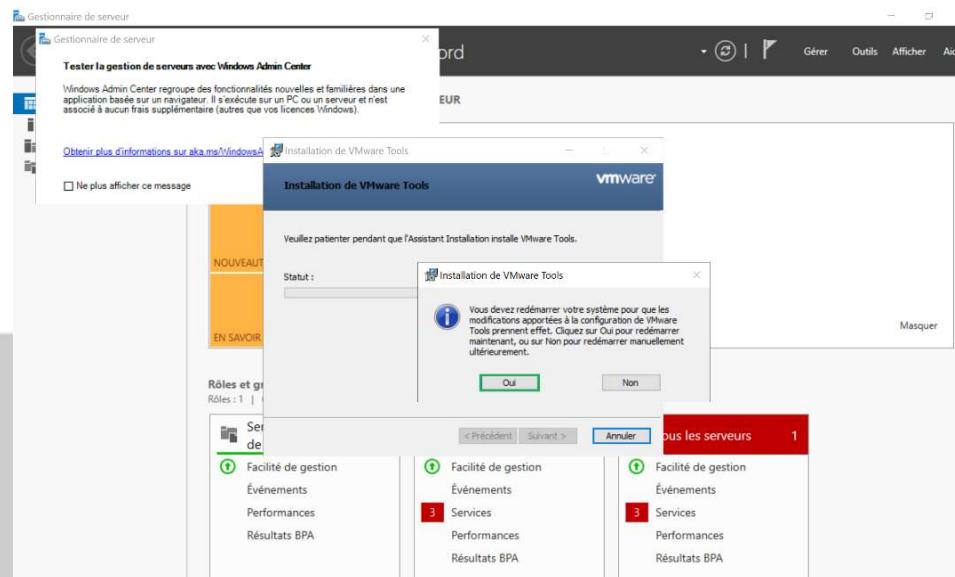


L'installation démarre :



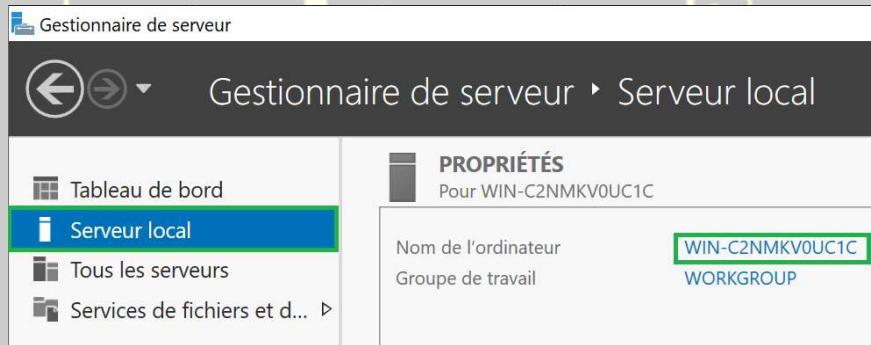
1.2.2. Configuration de base

Une fois tout en vert la vm démarre, on arrive ensuite à l'installation des **Vmware Tools**. Cliquez sur oui pour redémarrer la vm et procéder à l'installation :

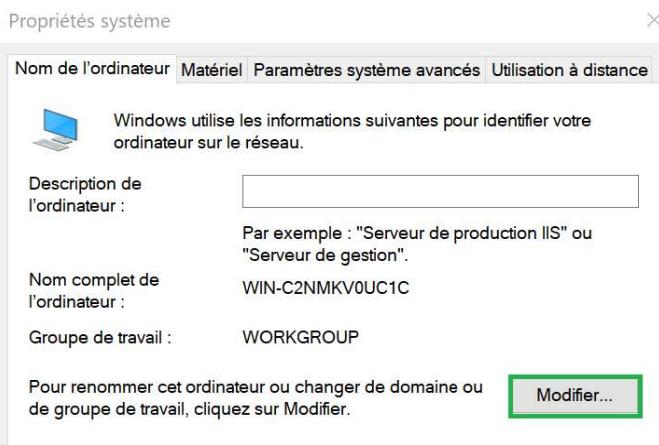


Une fois redémarré, nous allons procéder à la configuration de base de la vm.

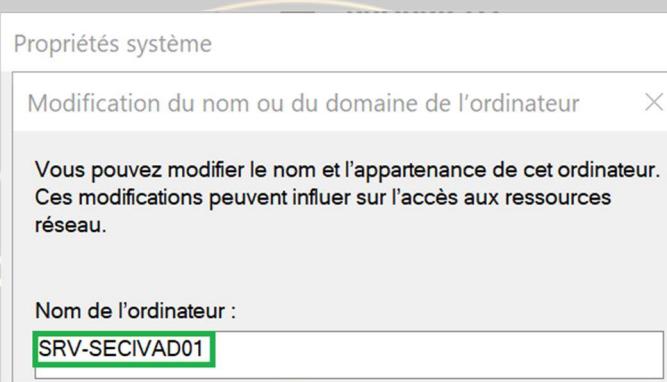
Tout d'abord, nous allons aller dans le gestionnaire de serveur à l'onglet **Serveur local puis** cliquez sur le nom de l'ordinateur :



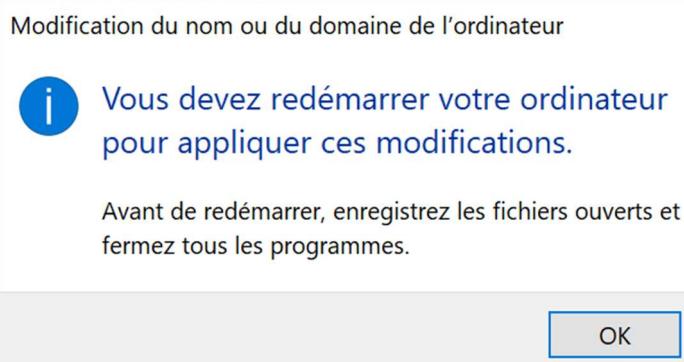
Cliquez sur **modifier** :



Assignez le nom puis valider :



La VM devra redémarrer pour prendre en compte la modification :



Cliquez sur **OK** puis validez le redémarrage :

Microsoft Windows

X

Vous devez redémarrer votre ordinateur pour appliquer ces modifications

Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.

Redémarrer maintenant**Redémarrer ultérieurement**

Dans le même onglet qu'avant, on peut voir que le nom à bien été changé. Cette étape doit impérativement se faire avant l'installation de l'AD.



Une fois l'ordinateur redémarré, rendez-vous une fois de plus dans le **Gestionnaire de serveur**, puis dans **Serveur local**, et dans les **Propriétés**. Nous pouvons observer la ligne spécifiant l'état du pare-feu :

Pare-feu Windows Defender Public : Actif

Et un peu plus loin sur cette même ligne :

Antivirus Windows Defender Protection en temps réel : activée

Ainsi que :

Configuration de sécurité renforcée d'Internet Explorer Actif

Commencez par cliquer sur « **Public : Actif** ». Une fenêtre apparaît :

¶) Pare-feu et protection du réseau

Qui et ce qui peut accéder à vos réseaux.

Réseau avec domaine

Le pare-feu est activé.

Réseau privé

Le pare-feu est activé.

Réseau public (actif)

Le pare-feu est activé.

Cliquez sur chaque ligne bleue puis désactivez les pares-feux.

Pare-feu domaine :

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.



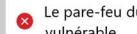
Activé

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.



Désactivé

Pare-feu privé :

Pare-feu Windows Defender

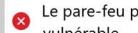
Aide à protéger votre appareil sur un réseau privé.



Activé

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau privé.



Désactivé

Pare-feu public :

Pare-feu Windows Defender

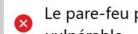
Aide à protéger votre appareil sur un réseau public.



Activé

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau public.



Désactivé

Revenez maintenant dans les propriétés du serveur local, et cliquez sur **Protection en temps réel** :

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.



Activé

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.



Désactivé

Devient

Pour finir nous allons désactiver la sécurité renforcée d'internet explorer :

Administrateurs :

- Activé (recommandé)
- Désactivé

Utilisateurs :

- Activé (recommandé)
- Désactivé

Administrateurs :

- Activé (recommandé)
- Désactivé

Utilisateurs :

- Activé (recommandé)
- Désactivé

Devient

Après actualisation, nous pouvons voir que tout a été pris en compte :

Pare-feu Windows Defender	Public : Inactif
Gestion à distance	Activé
Bureau à distance	Désactivé

Antivirus Windows Defender	Protection en temps réel : désactivée
Commentaires et diagnostics	Paramètres
Configuration de sécurité renforcée d'Internet Explorer	Inactif

1.2.3. Agrégation de carte réseau (IP Bonding)

Comme indiqué dans les spécificités techniques du projet, nous allons procéder à l'IP Bonding. Cela nous permettra une certaine tolérance de panne ainsi qu'une répartition de charges (pour les interfaces réseaux).

Pour réaliser l'agrégation, rendons-nous dans le gestionnaire de serveur, onglet Serveur local. Nous pouvons voir nos deux cartes réseaux :

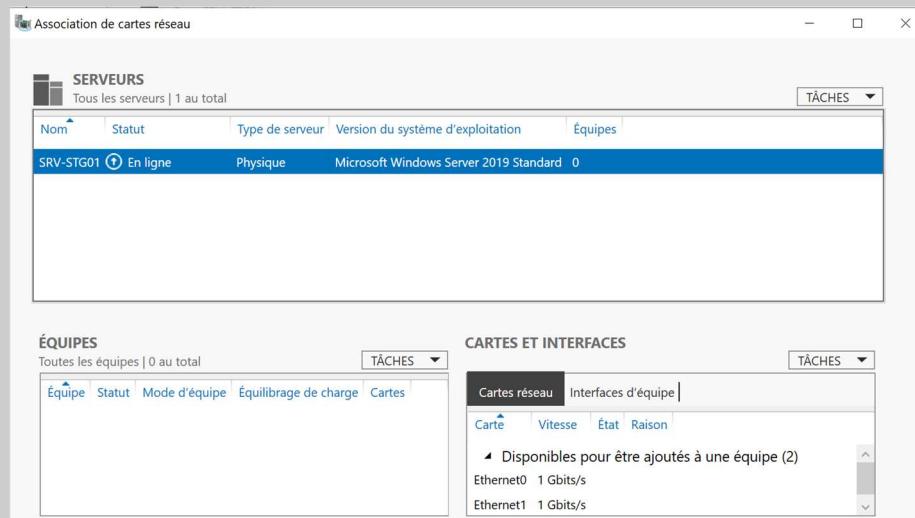
Ethernet0
Ethernet1

Adresse IPv4 attribuée par DHCP, Compatible IPv6
Adresse IPv4 attribuée par DHCP, Compatible IPv6

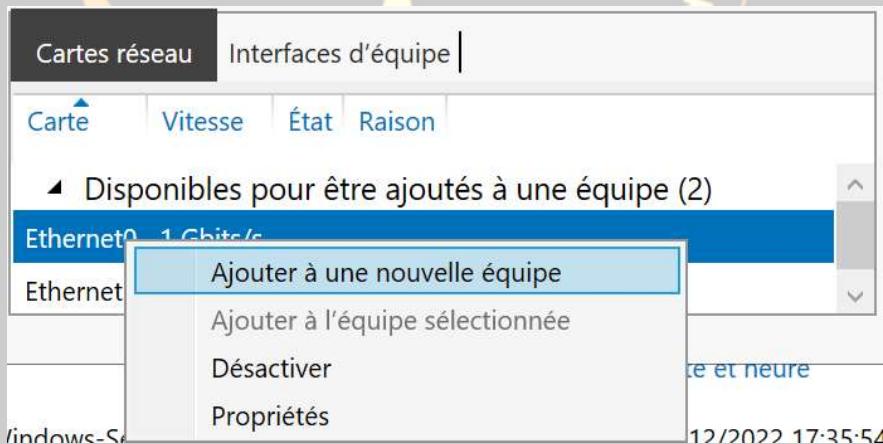
Comme nous l'avons vu plus haut, les deux cartes réseaux sont sur le Vmnet11. Revenez ensuite sur le serveur local dans propriétés et cliquez sur **Désactivé** à droite d'**Association de cartes réseau** :

Association de cartes réseau **Désactivé**

Une fenêtre apparaît :



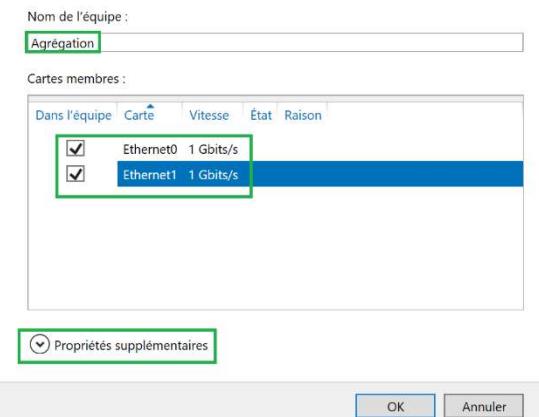
Faites un clic droit sur la première carte puis sélectionnez **Ajoutez à une nouvelle équipe** :



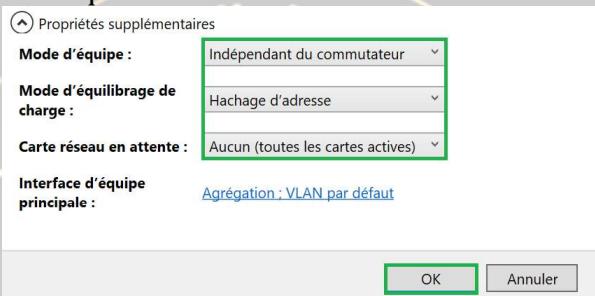
Une fenêtre s'ouvre alors, choisissez le nom puis sélectionnez les deux cartes et cliquez sur **Propriétés supplémentaires** :

Association de cartes réseau

Nouvelle équipe



Configurez comme ceci puis cliquez sur **OK** :



Cela peut prendre quelques minutes avant que les deux cartes soient actives donc pas de panique :

SERVEURS

Tous les serveurs | 1 au total

Nom	Statut	Type de serveur	Version du système d'exploitation	Équipes
SRV-STG01	Avertissement	Physique	Microsoft Windows Server 2019 Standard	1

TÂCHES

ÉQUIPES

Toutes les équipes | 1 au total

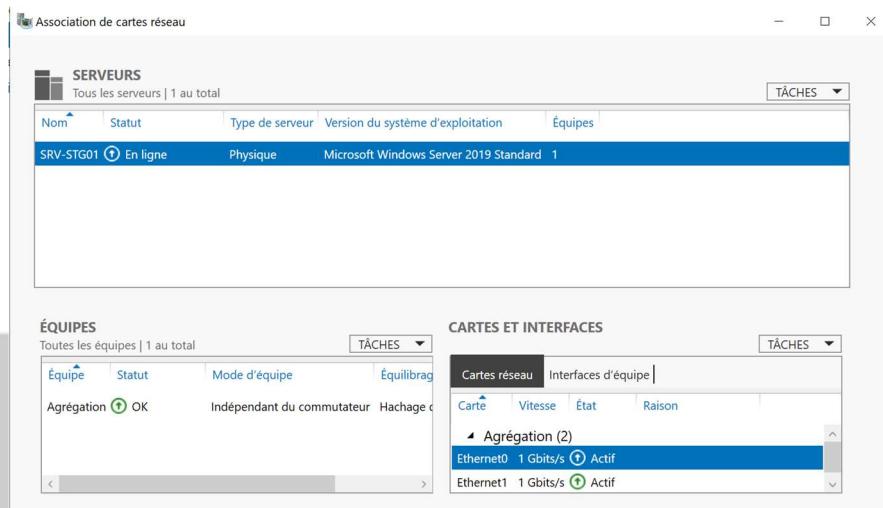
Équipe	Statut	Mode d'équipe	Équilibrage
Agrégation	Avertissement	Indépendant du commutateur	Hachage

TÂCHES

CARTES ET INTERFACES

Cartes réseau	Interfaces d'équipe		
Carte	Vitesse	État	Raison
▲ Agrégation (2)			
Ethernet0	1 Gbits/s	En échec	Connexion en attente
Ethernet1	1 Gbits/s	Actif	

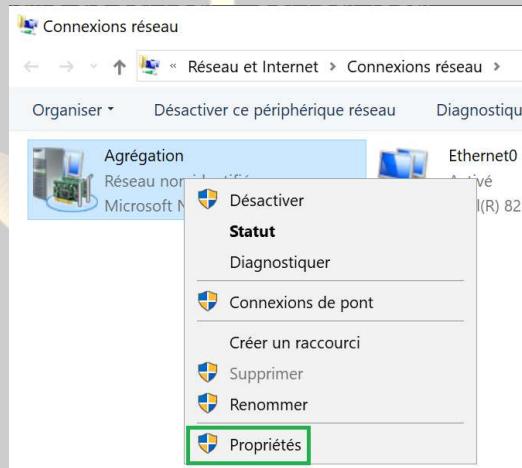
Devient



On peut voir que l'agrégation à bien été prise en compte dans le gestionnaire du serveur local :

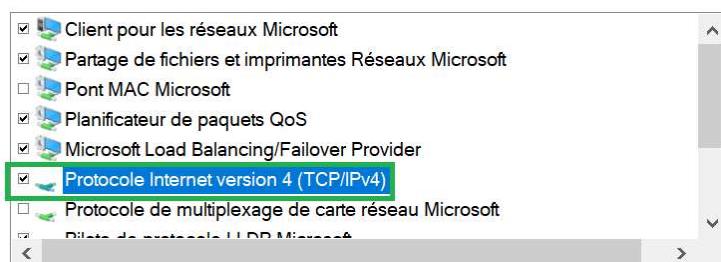


Nous allons maintenant attribuer l'IP statique que nous avons définis dans le tableau d'adressage. Pour cela il suffit de cliquer sur **adresse ipv4** à droite d'**Agrégation**, puis faites un clic droit sur **Agrégation** et cliquez sur **Propriétés** :

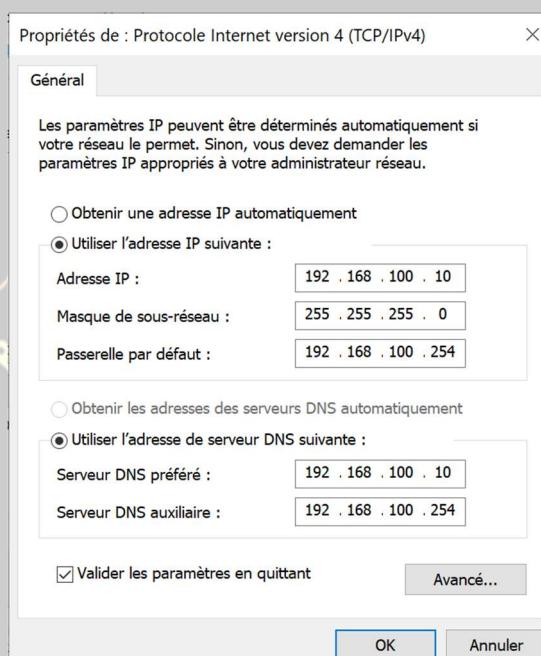


Faites un double clic sur **Protocole Internet version 4** :

Cette connexion utilise les éléments suivants :



Remplir comme ceci et cliquez sur **OK** :



Ce qui nous donne :

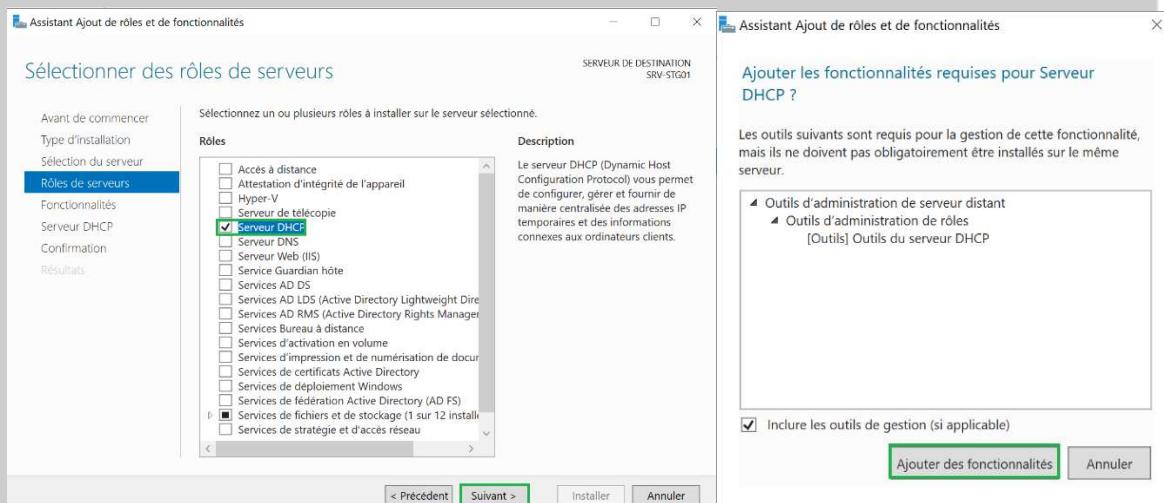
Association de cartes réseau	Activé
Agrégation	192.168.100.10

1.2.4. DHCP

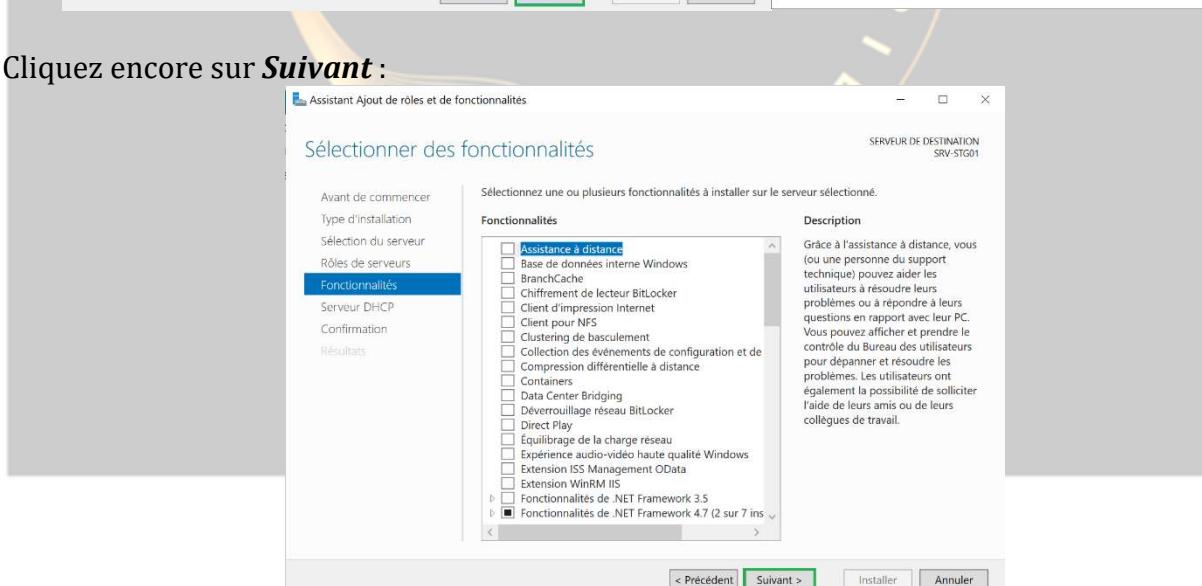
Maintenant que le serveur dispose d'un IP fixe, nous allons pouvoir installer le rôle DHCP. Pour cela, rendez-vous dans le **Tableau de bord** du **Gestionnaire de serveur** et cliquez sur **Ajouter des rôles et des fonctionnalités** :



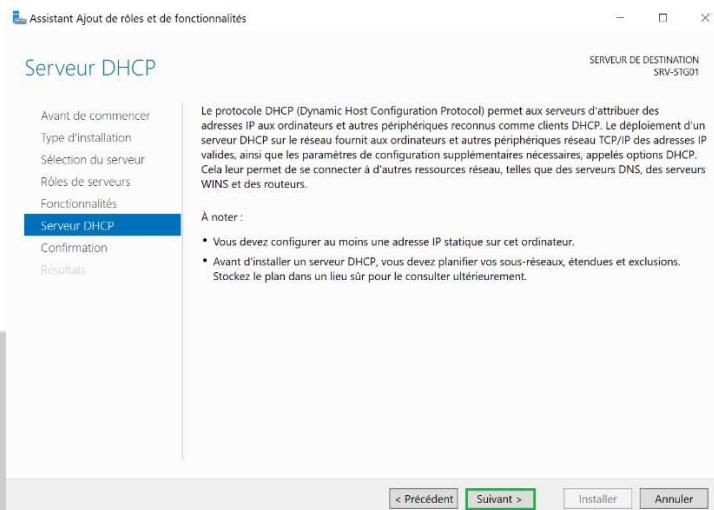
Une fenêtre s'ouvre, cliquez trois fois sur **Suivant** puis sélectionnez le rôle **Serveur DHCP**, une deuxième fenêtre s'ouvre, cliquez sur **Ajouter des fonctionnalités** puis cliquez sur **Suivant** :



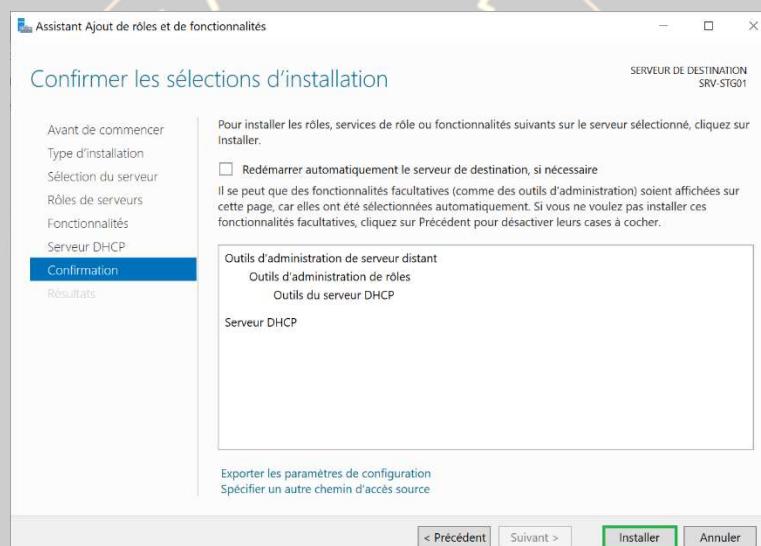
Cliquez encore sur **Suivant** :



Encore une fois **Suivant** :



Ensuite, démarrez l'installation en cliquant sur **Installer** :



L'installation se lance :

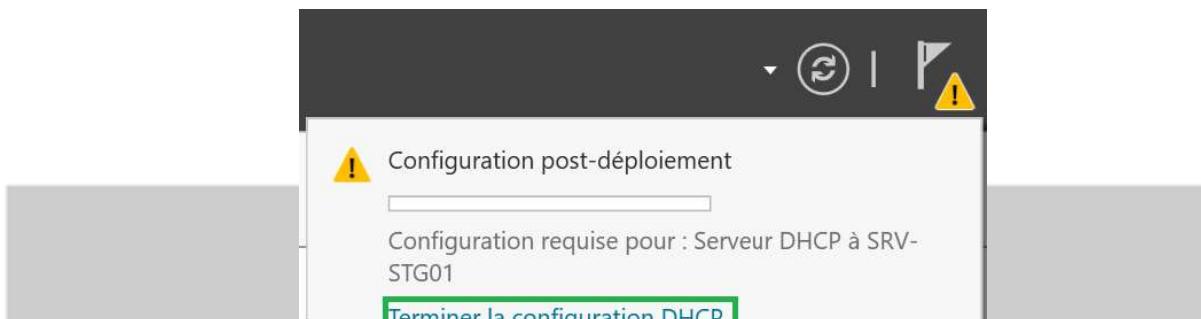


Vous pouvez fermer l'assistant.

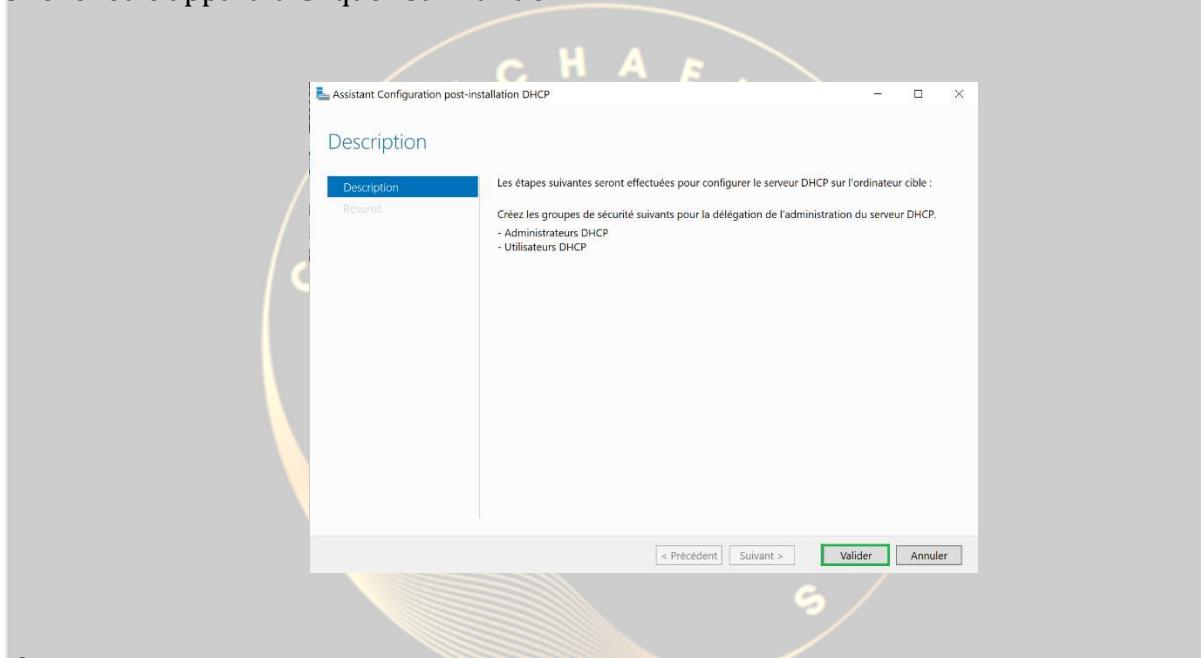
Pour finaliser l'installation du rôle, rendez-vous dans le **Gestionnaire de serveur** et faites un clic gauche sur l'icône comportant un drapeau et un triangle jaune (avec un point d'exclamation)



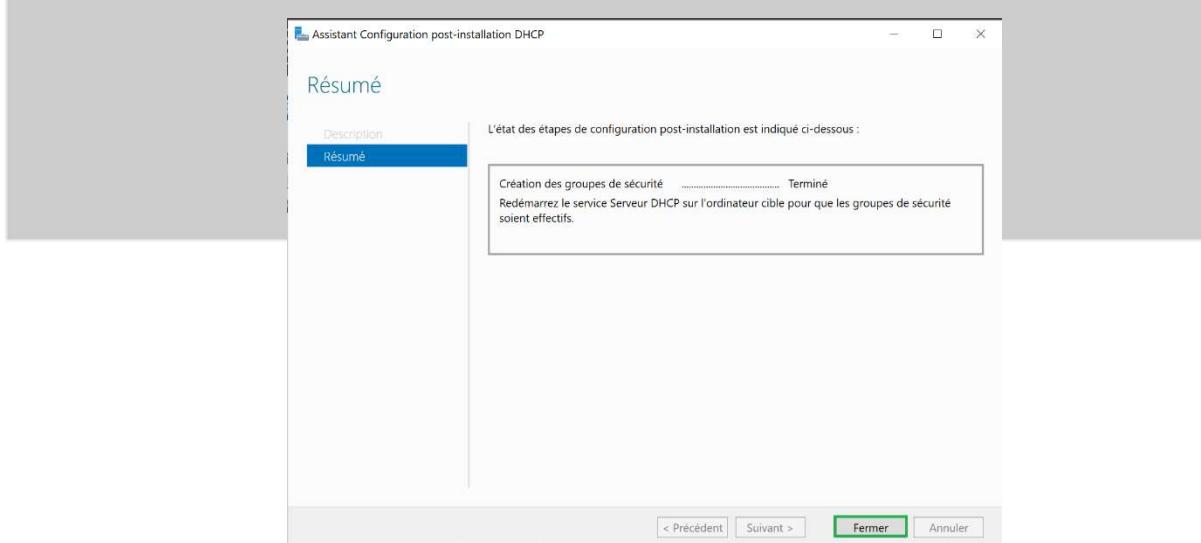
Cliquez ensuite sur **Terminer la configuration DHCP** :



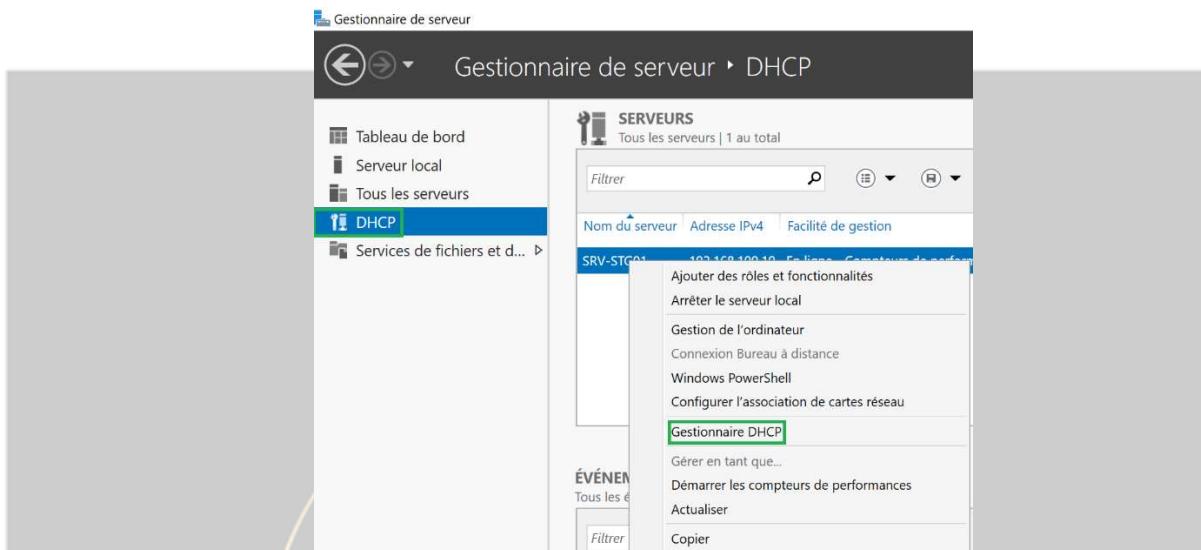
Une fenêtre apparaît. Cliquez sur **Validez** :



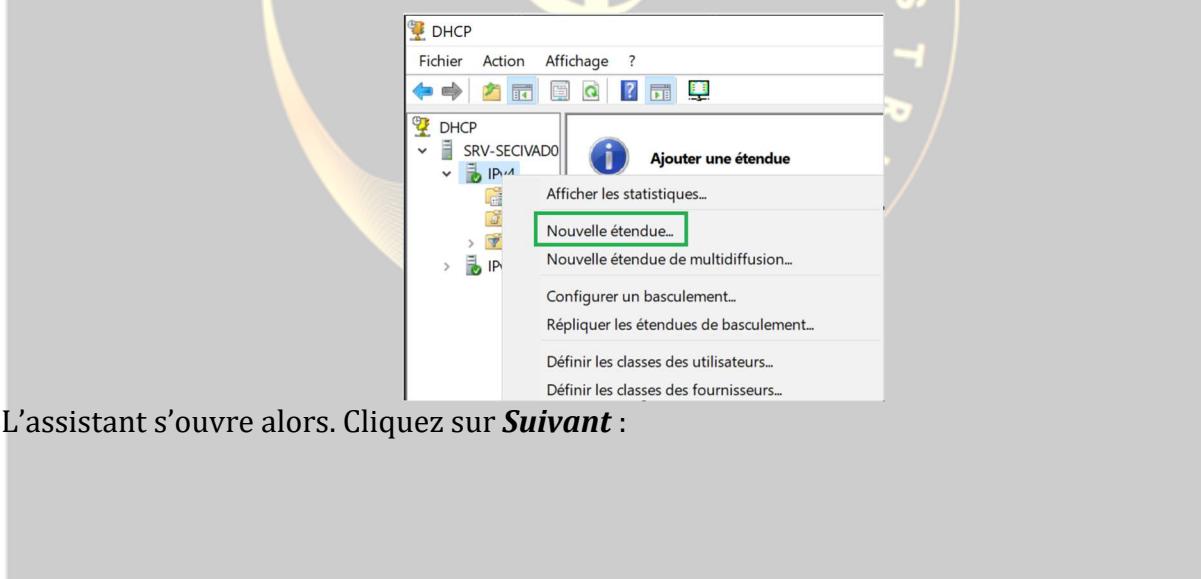
Cliquez sur **Fermer** :



L'installation du rôle DHCP est maintenant terminée. Pour la configuration DHCP, nous allons configurer une étendue pour le site de Strasbourg. Cette étendue sera ensuite répliquée, après l'installation du Serveur CORE de Strasbourg, plus tard dans le livrable. Pour cela, nous allons ouvrir le **Gestionnaire DHCP** :

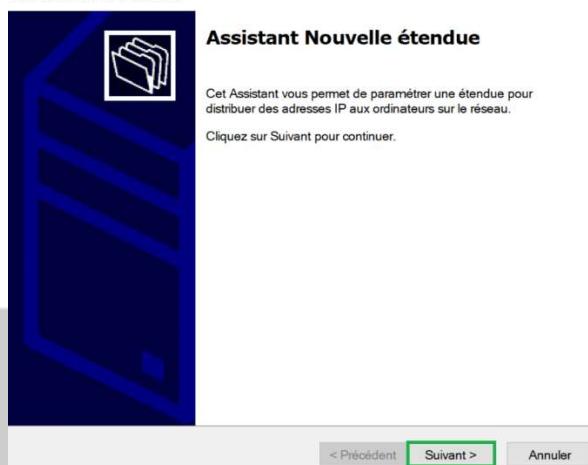


Nous allons dérouler le nom du serveur, puis faire un clic droit sur **IPv4** et sélectionner **Nouvelle étendue** :

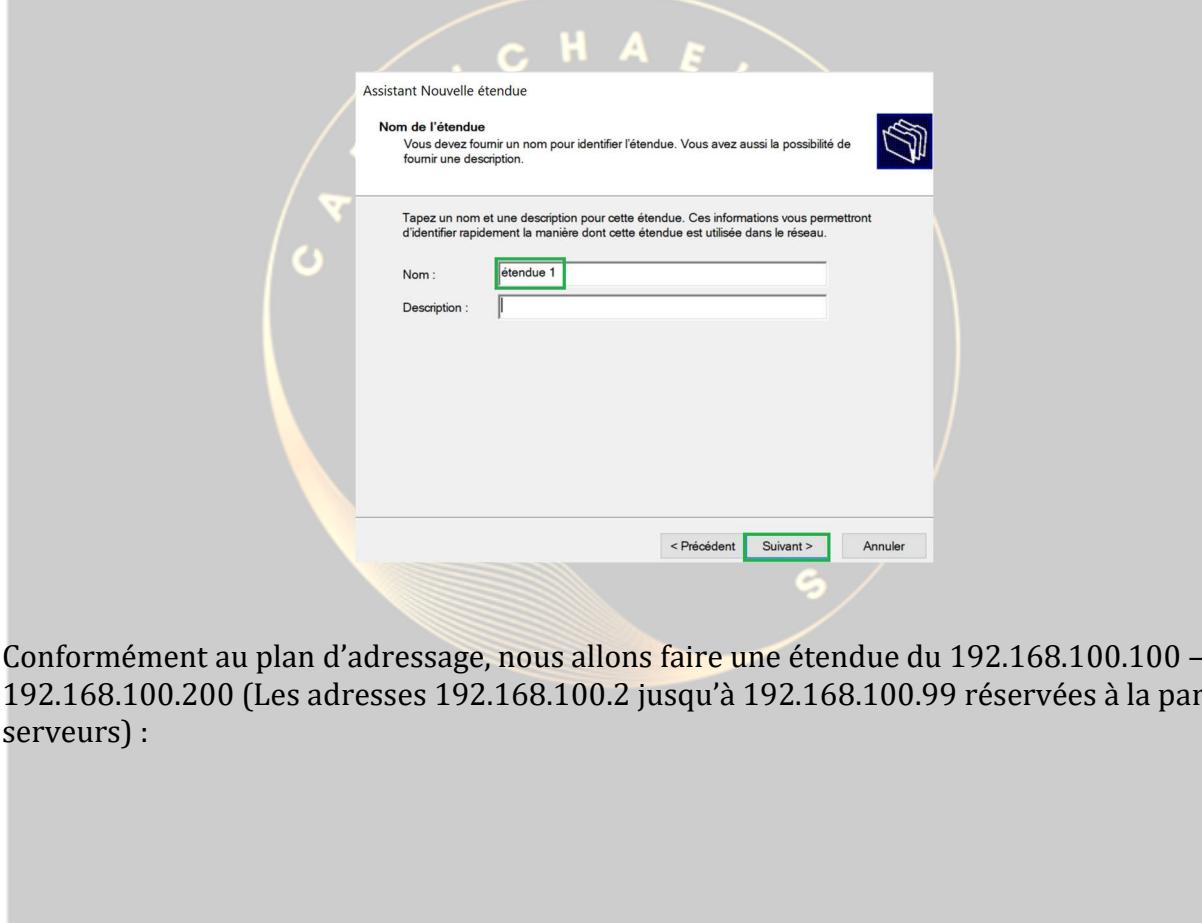


L'assistant s'ouvre alors. Cliquez sur **Suivant** :

Assistant Nouvelle étendue



Rentrez un nom et une description (optionnel) puis cliquez sur **Suivant** :



Conformément au plan d'adressage, nous allons faire une étendue du 192.168.100.100 – 192.168.100.200 (Les adresses 192.168.100.2 jusqu'à 192.168.100.99 réservées à la partie serveurs) :

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

On laisse la durée du bail à 8 jours, cliquez sur **Suivant** :

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

< Précédent Suivant > Annuler

On va configurer les **options DHCP** :

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

Oui, je veux configurer ces options maintenant!

Non, je configurerai ces options ultérieurement

< Précédent Suivant > Annuler

Entrez l'IP de votre futur routeur PFSense, cliquez sur **Ajouter** puis cliquez sur **Suivant** :

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

192 . 168 . 100 . 254

Ajouter

192.168.100.254

Supprimer

Monter

Descendre

< Précédent

Suivant >

Annuler

On laisse tel quel puis on clique sur **Suivant** :

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :

Adresse IP :

Ajouter

192.168.100.10
192.168.100.254

Supprimer

Monter

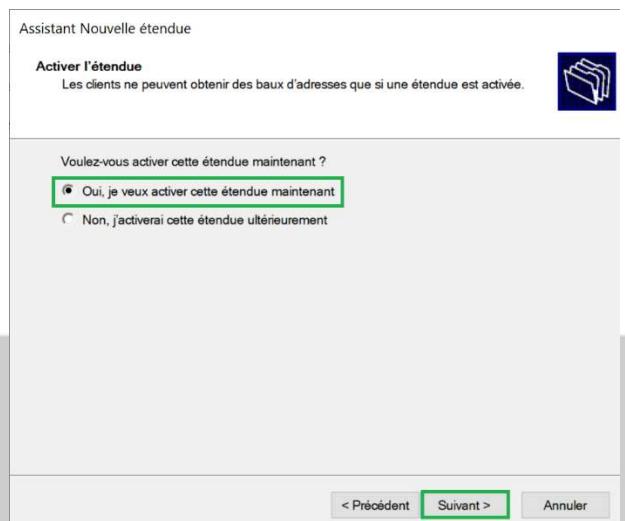
Descendre

< Précédent

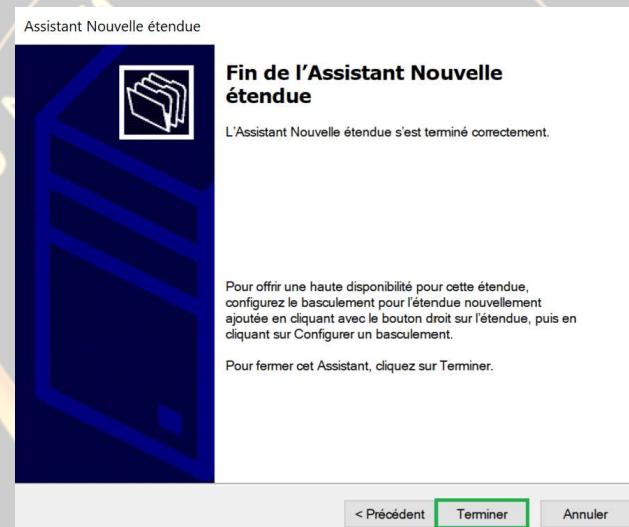
Suivant >

Annuler

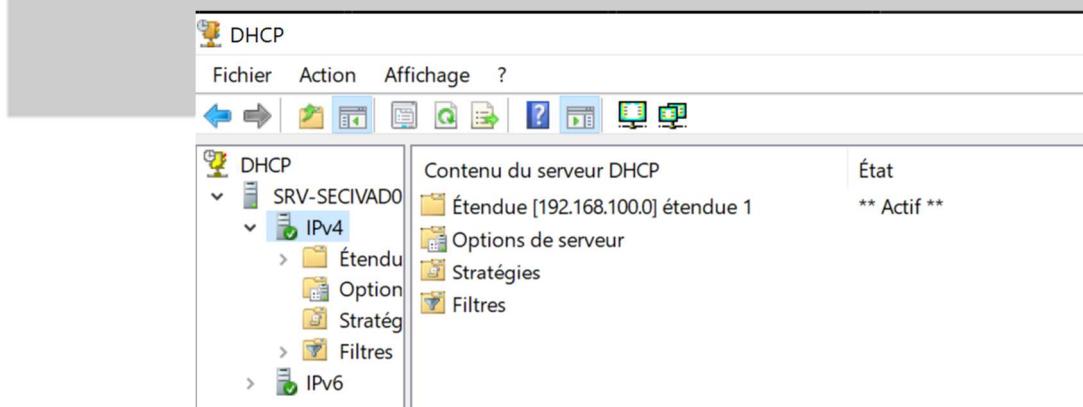
On coche **Oui, je veux activer**, puis on clique sur **Suivant** :



On clique sur **Terminer** :



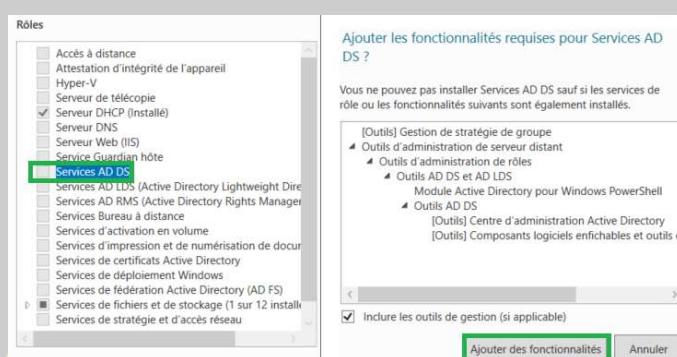
On peut désormais voir que l'étendue est visible dans le **Gestionnaire DHCP** :



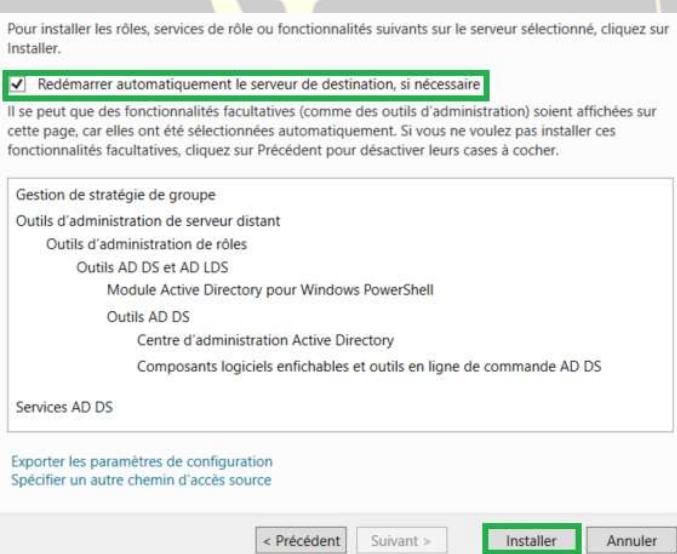
1.2.5. ADDS (Active Directory et DNS)

Nous allons maintenant passer à l'installation du service d'annuaire. Pour cela il existe un rôle qui installe l'Active directory ainsi que le DNS, il s'agit du rôle ADDS.

Cliquez sur **Ajouter des rôles et des fonctionnalités** dans le tableau de bord du **Gestionnaire de serveur**, puis cliquez 3 fois sur **Suivant**. Choisissez ensuite **Services AD DS**, L'assistant s'ouvre, cliquez sur **Ajouter des fonctionnalités** :



Cochez la case pour que le serveur redémarre automatiquement si nécessaire durant l'installation du rôle, puis cliquez sur **Installer** :



L'installation démarre, cela peut prendre quelques minutes.

Une fois le rôle installé, il nous reste quelques manipulations à effectuer. Pour cela, rendez-vous dans le tableau de bord du serveur et cliquer sur le **drapeau** en haut à droite, puis sur **Promouvoir ce serveur en contrôleur de domaine** :



Cochez la case **Ajouter une nouvelle forêt** et mettez le nom de domaine racine selon les spécifications techniques :

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

Nom de domaine racine : SECIV.LAN

Cliquez sur **Suivant**, puis tapez le mot de passe de restauration que vous avez choisi et cliquez sur **Suivant** :

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016
Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

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

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](#)

Ignorez la délégation DNS et faites une nouvelle fois **Suivant** :

Spécifier les options de délégation DNS

Créer une délégation DNS

Le nom de domaine NetBIOS devrait être rempli automatiquement :

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS : SECIV

Cliquez sur **Suivant**, jusqu'à l'étape de l'installation puis cliquez sur Installer :

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

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

⚠ Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer des adresses IP statiques IPv4 et IPv6 aux propriétés IPv4 et IPv6 de la carte réseau physique. Ces affectations d'adresses IP statiques doivent être effectuées sur toutes les cartes réseau physiques pour que l'opération DNS soit fiable.

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour que l'opération DNS soit fiable.

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

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

[< Précédent](#) [Suivant >](#) Installer [Annuler](#)

L'installation débute et puis le serveur va redémarrer pour finaliser l'installation, ce qui peut prendre un certain temps. Une fois redémarré, on nous propose de se connecter en **Administrateur du domaine** :

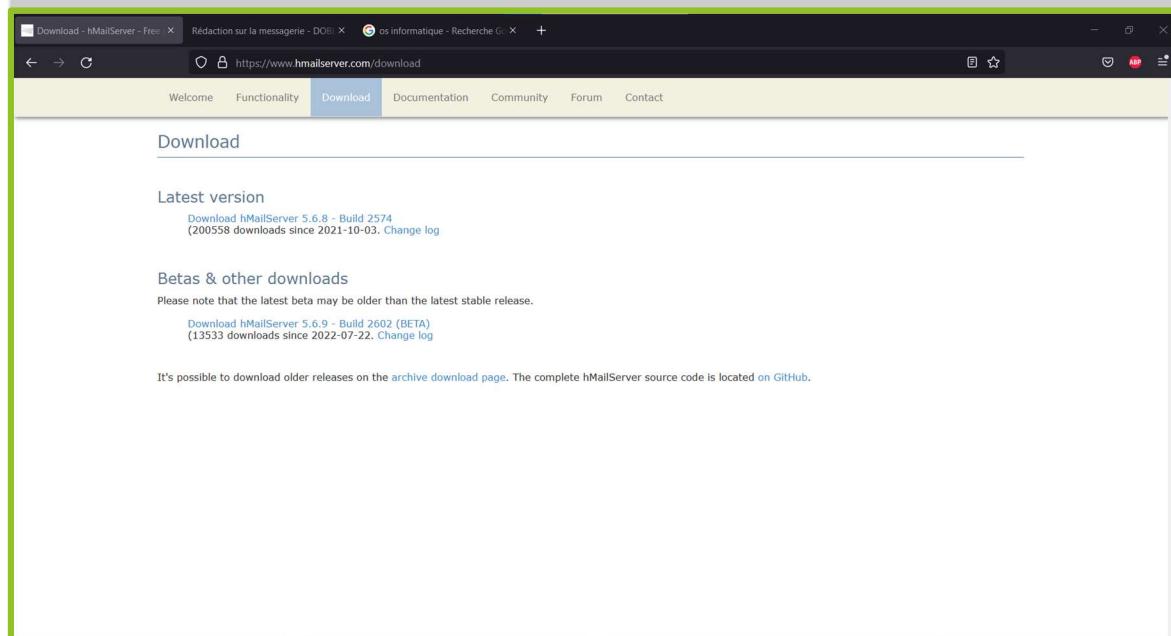


1.3. Serveur de Messagerie

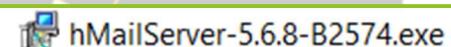
1.3.1. Installation d'hMailServer

Tout d'abord, nous avons décidé que le serveur de messagerie sera hébergé sur le serveur AD principale.

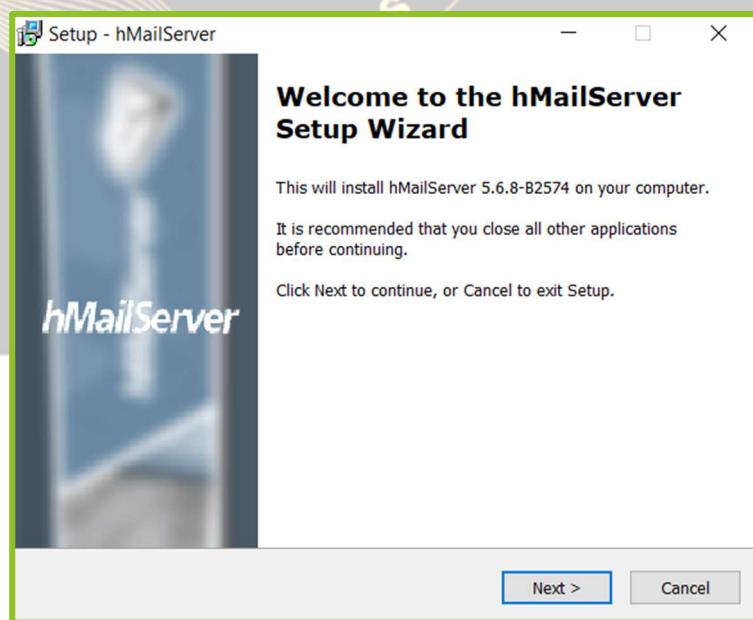
Une fois sur ce dernier, dirigez-vous sur le site : <https://www.hmailserver.com/download> pour télécharger le kit d'installation du serveur de messagerie. Puis, cliquez sur la dernière version à télécharger :



n'avez plus qu'à lancer le kit d'installation :



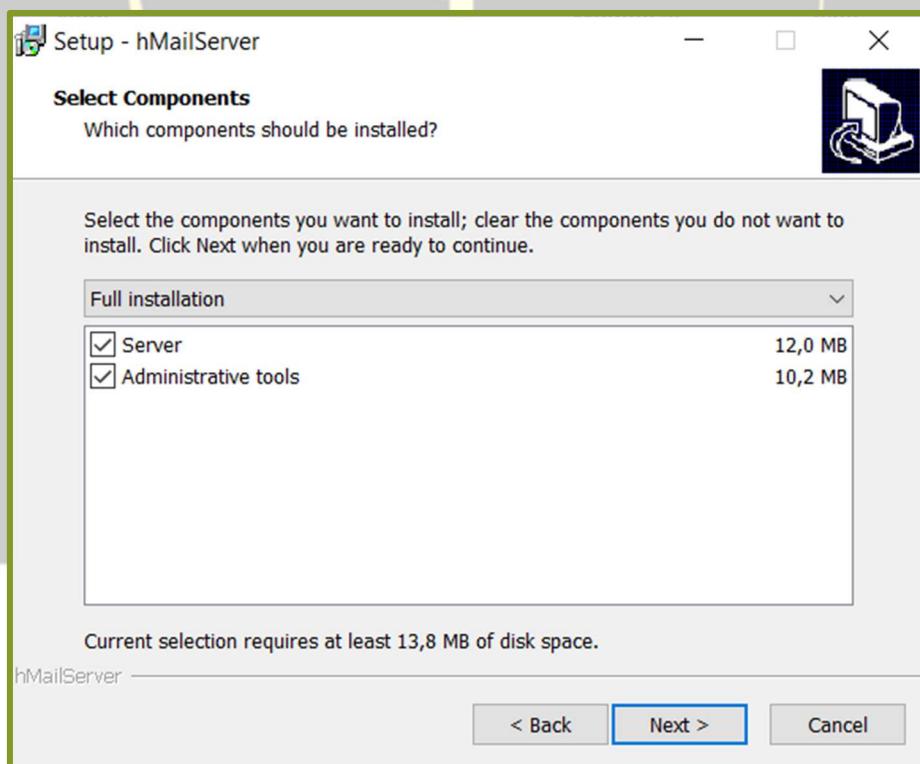
Après avoir lancé le kit d'installation, la fenêtre suivante s'ouvre :



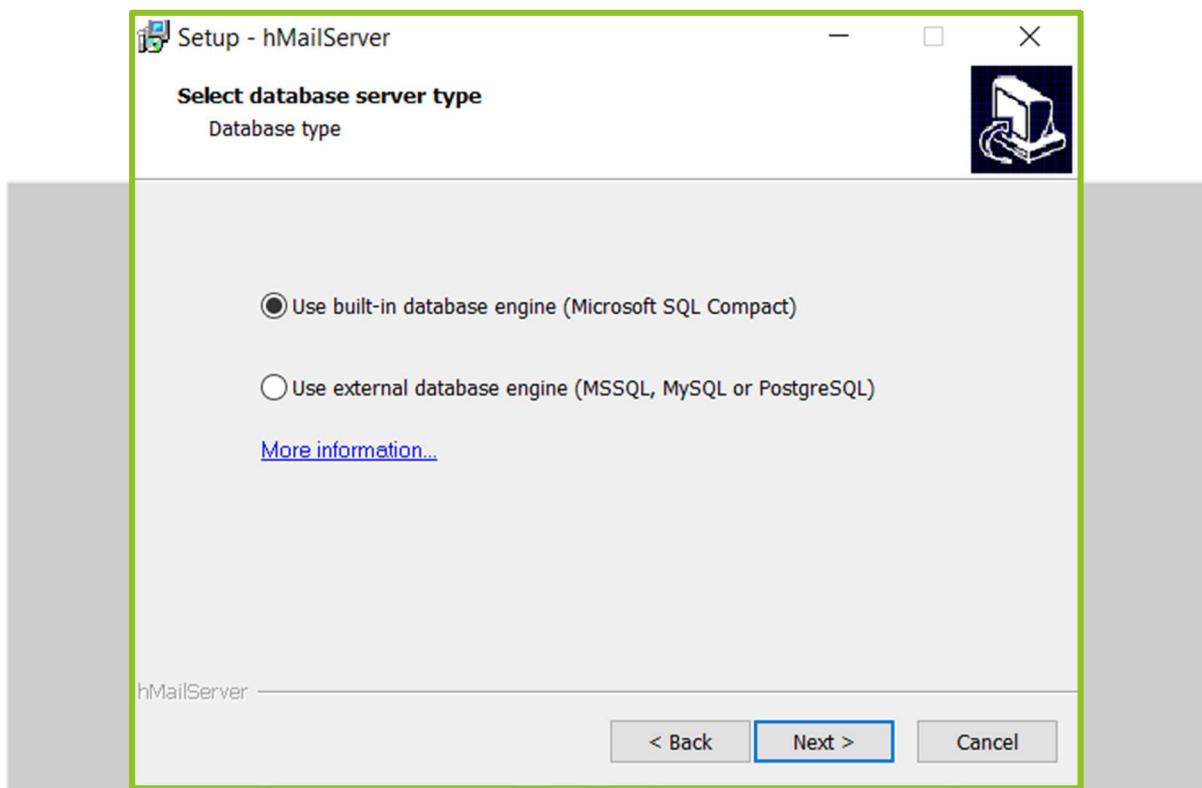
Cliquez sur suivant et accepter les termes d'utilisations de la licence :



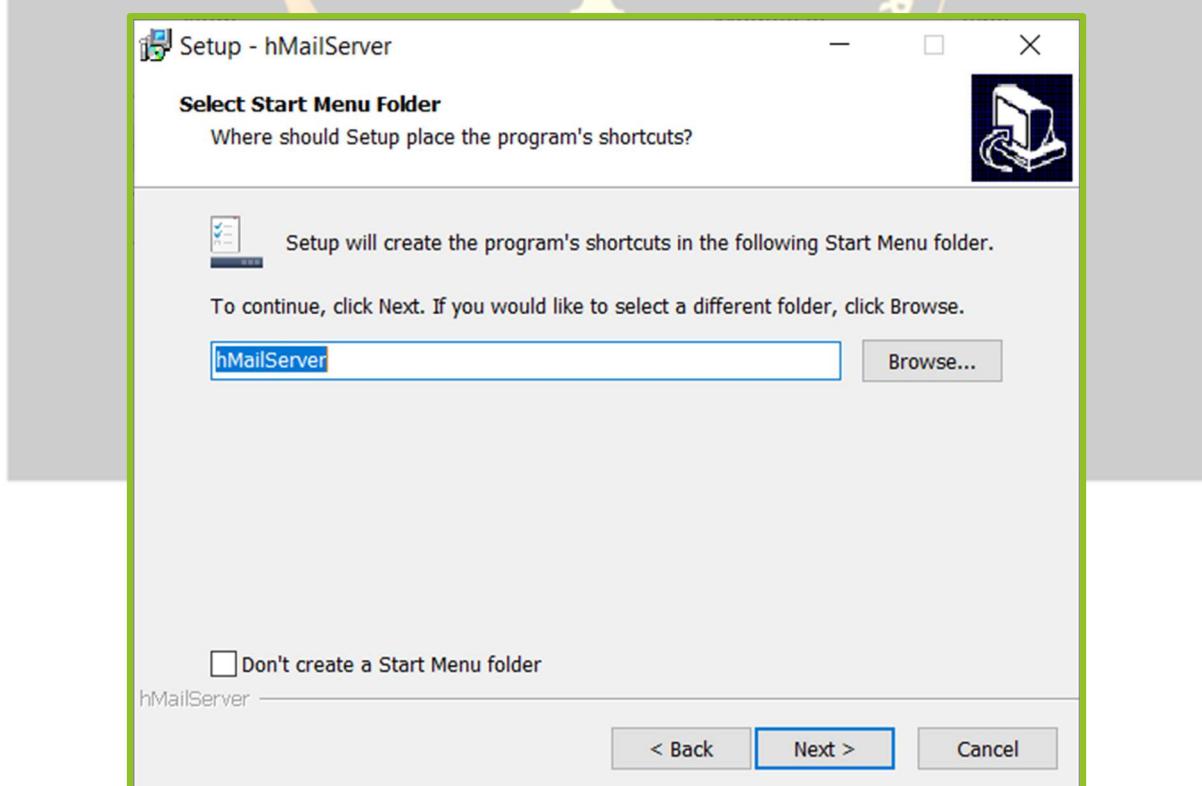
Ensuite, cochez les deux cases proposées. Cela vous permettra d'attribuer votre serveur en tant que serveur de mail et de disposer des droits et des outils d'administration :



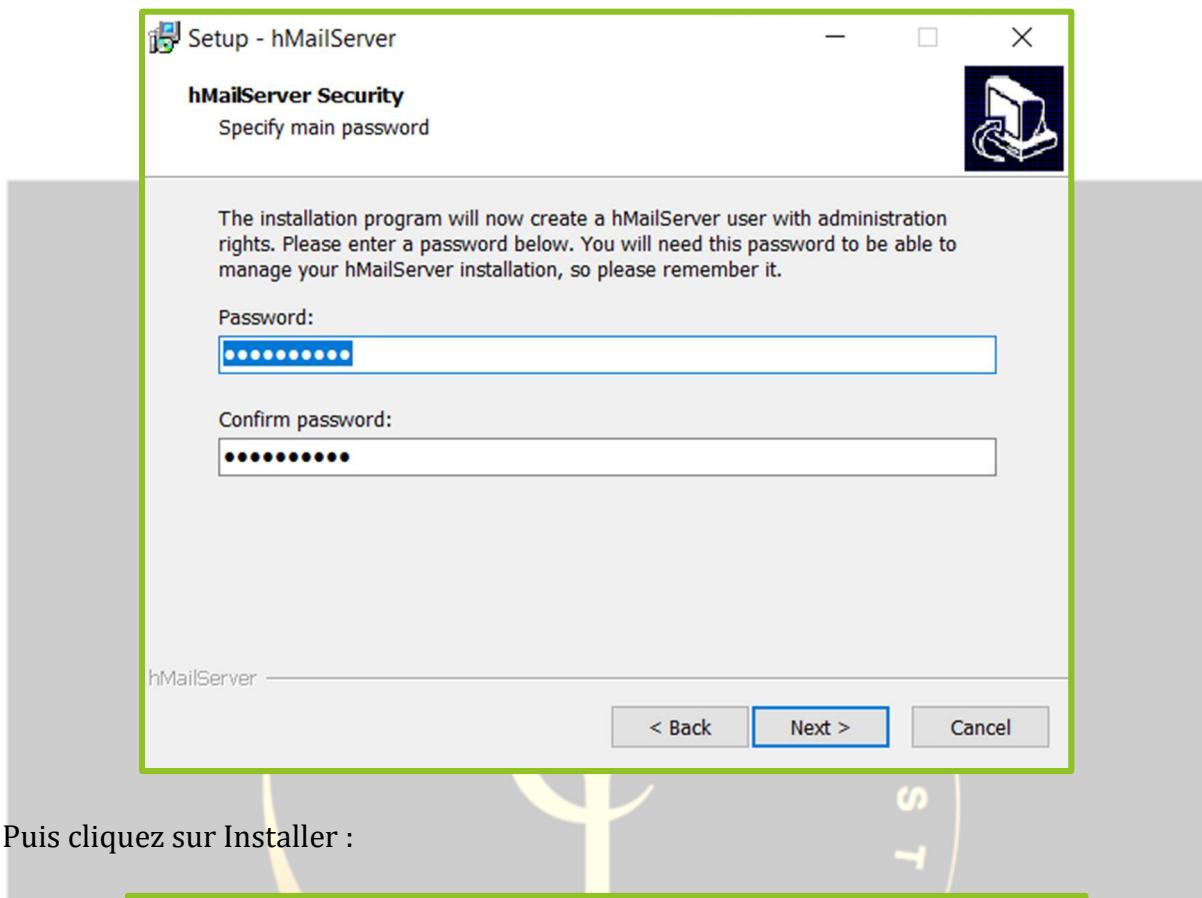
Une fois l'étape suivant passée, la prochaine vous demandera quel type de base de données vous souhaitez avoir. Si vous disposez d'une base de données externe, sélectionnez la deuxième option sinon laissez celle par défaut. Ici, elle sera par défaut :



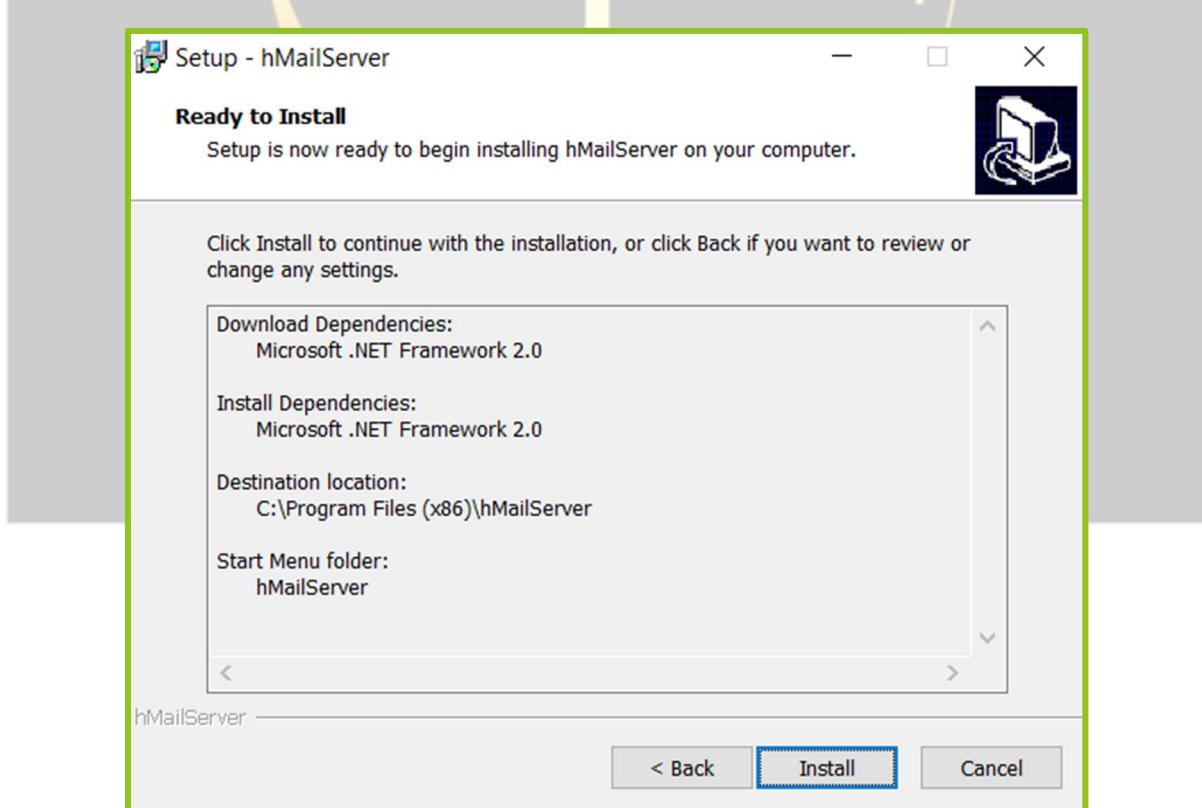
Ici, le logiciel va créer un raccourcie du programme, vous pouvez cliquez sur suivant et laisser la configuration par défaut :



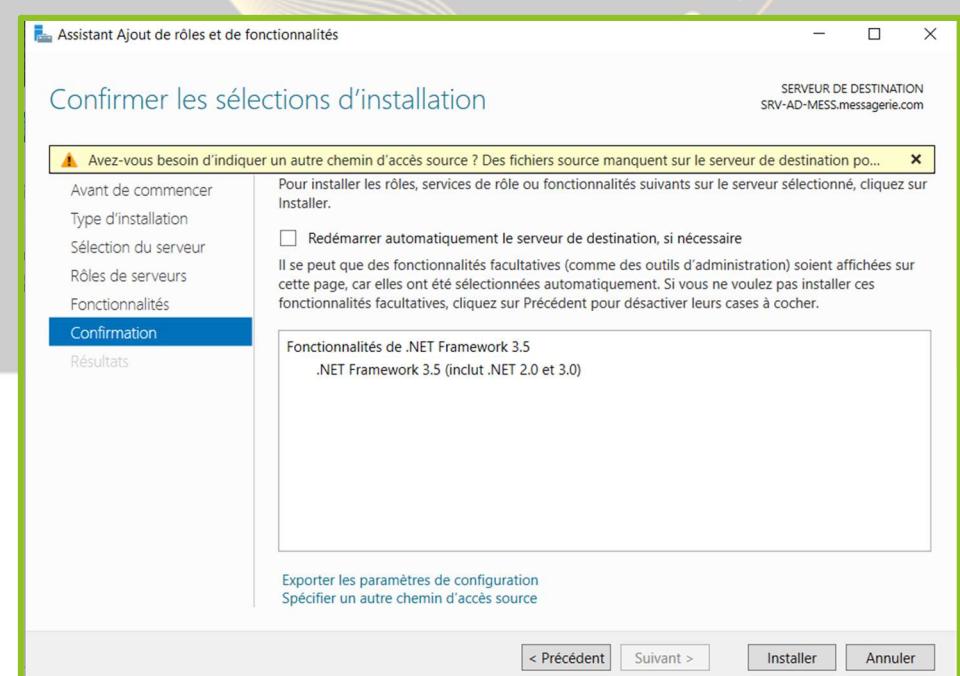
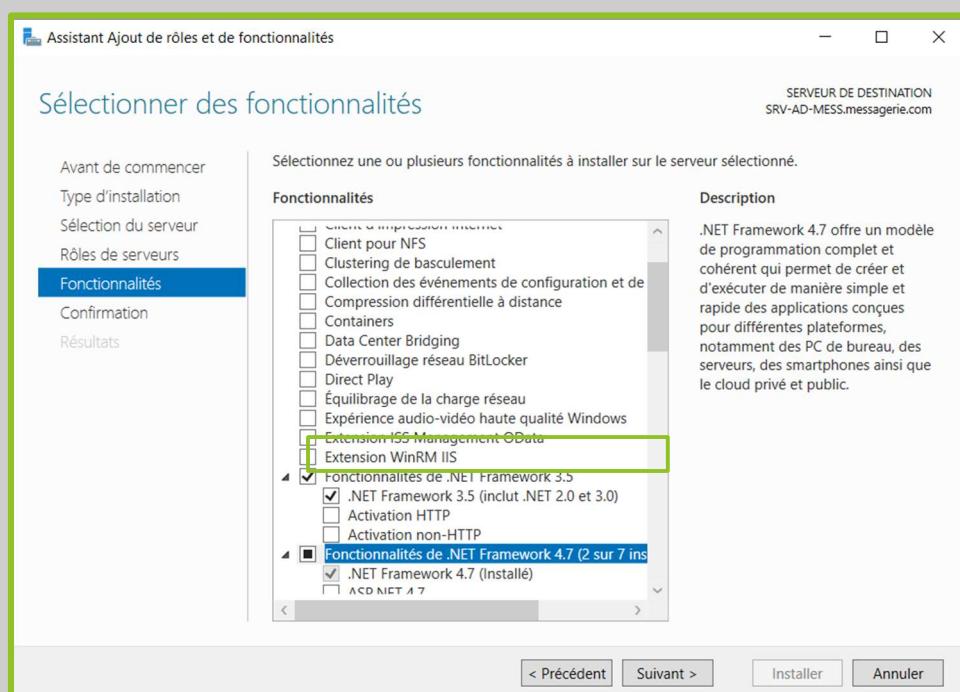
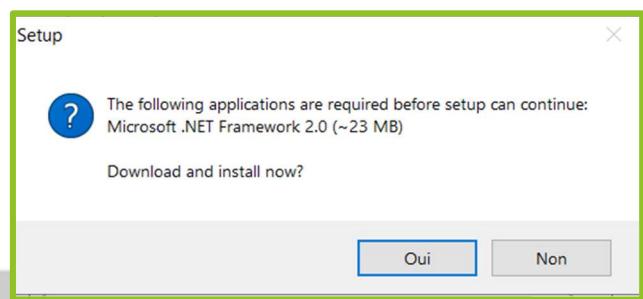
Informez le mot de passe vous permettant de vous connecter sur votre serveur de messagerie :



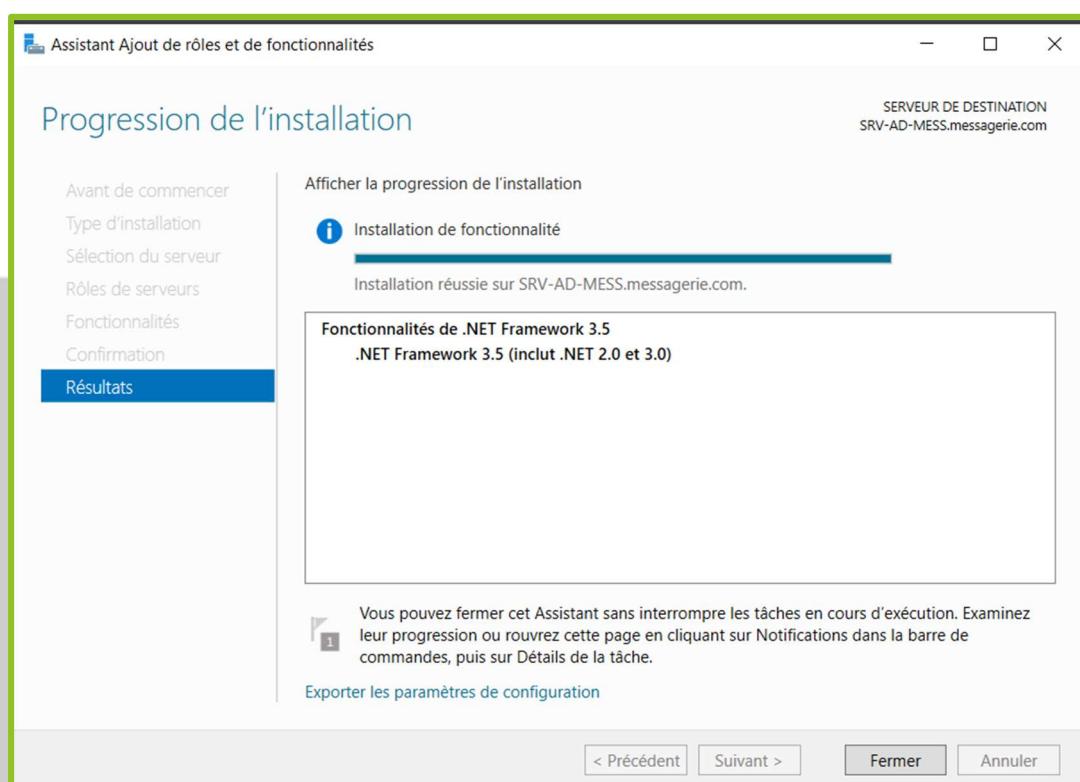
Puis cliquez sur Installer :



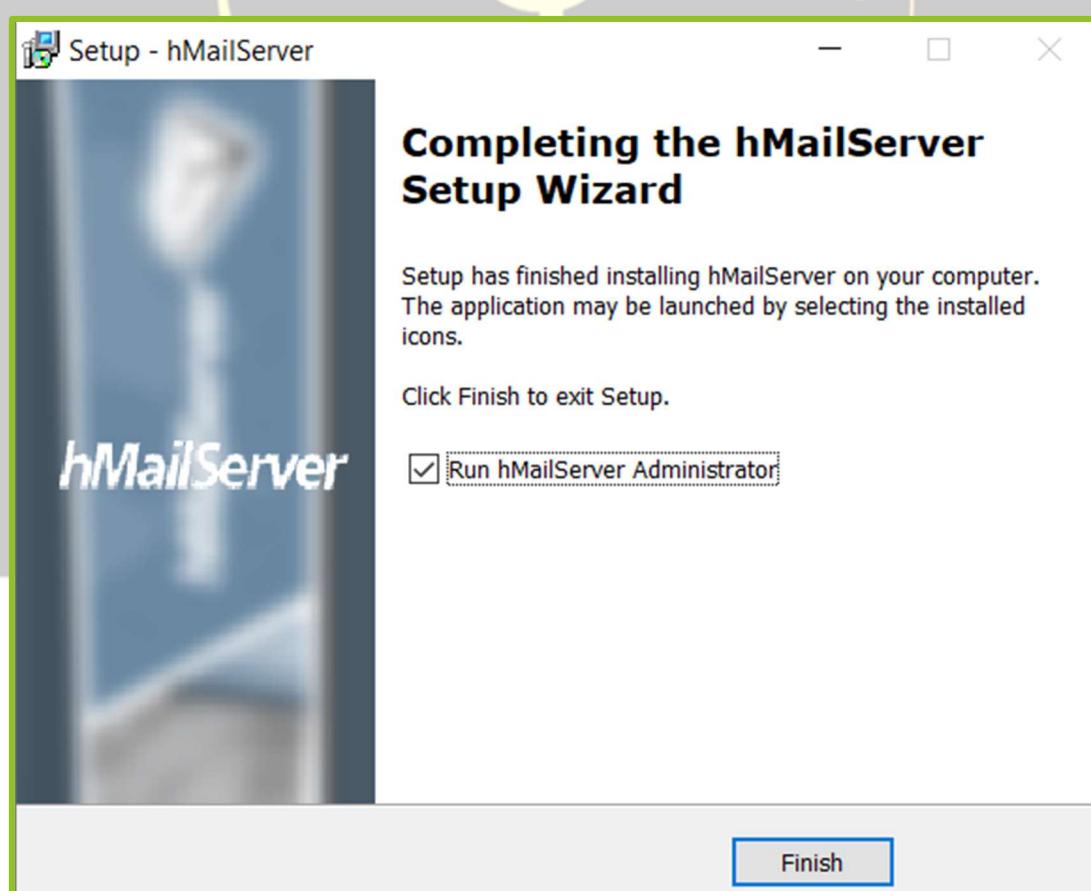
A noter qu'il est possible qu'il, lors de l'installation de hMailServer, ne parvient pas à télécharger via le lien web intégré dans le kit le .NET Framework 2.0. Si cela s'avère être le cas, vous devrez installer la fonctionnalité **.NET Framework 3.5** dans l'assistant d'ajout de rôles et de fonctionnalités de votre gestionnaire de serveur et confirmez l'installation :



Le voilà installé :



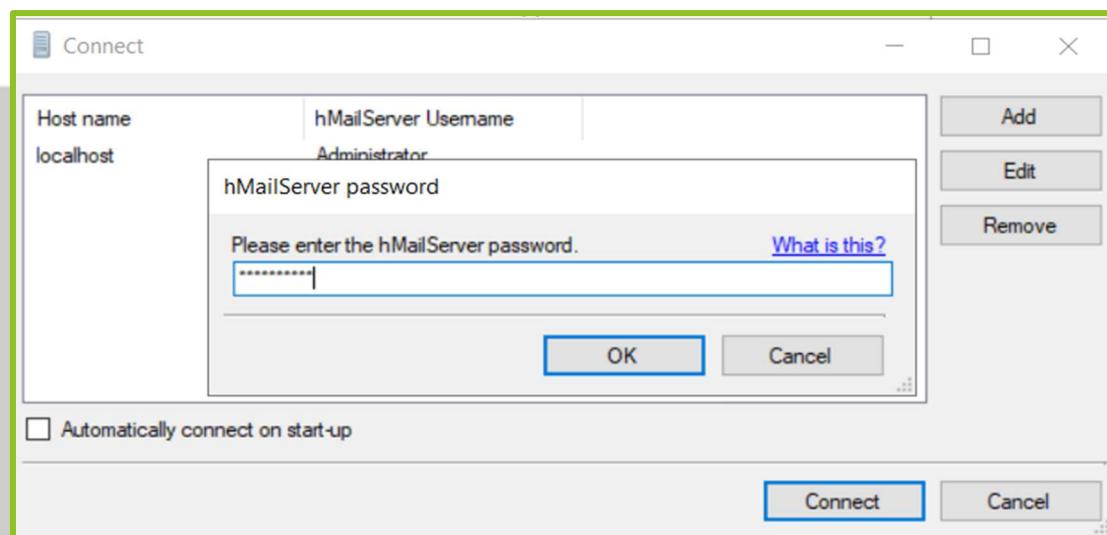
Une fois le Framework installé, vous pouvez reprendre votre installation sans



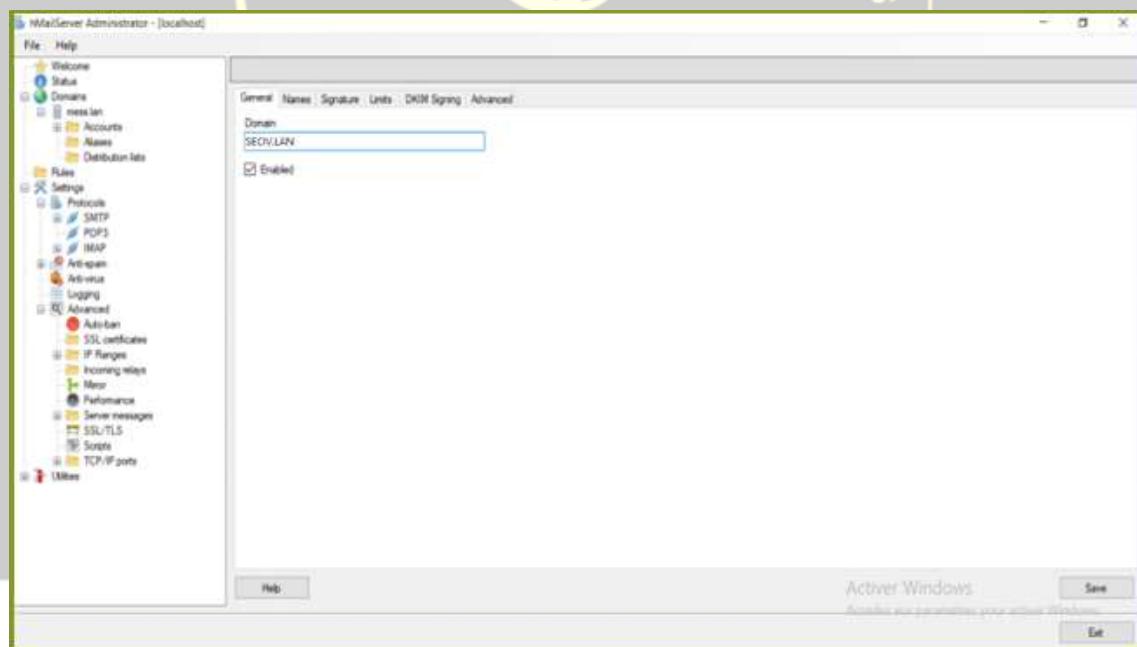
1.3.2. Configuration d'hMailServer

a. Ajout du domaine et des comptes utilisateurs

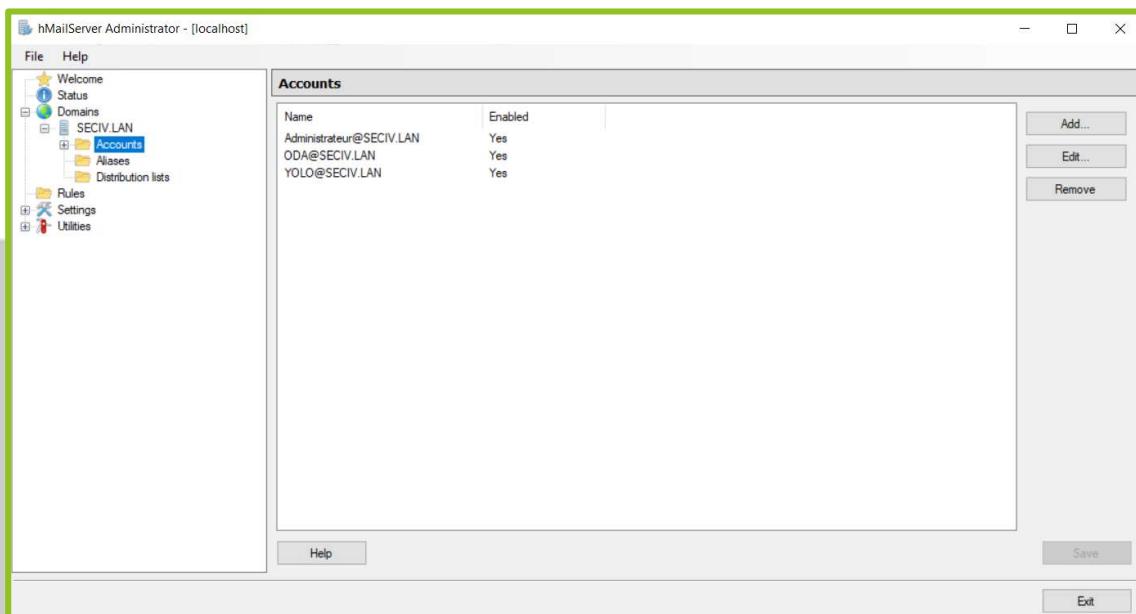
Maintenant que l'installation a été faite, nous pouvons configurer le serveur. Pour cela, tapez le mot de passe que vous avez renseigné lors de l'installation pour pouvoir vous connecter sur le serveur :



La page suivante s'affichera et vous pourrez déjà ajouter un domaine, en cliquant sur « Add domain »

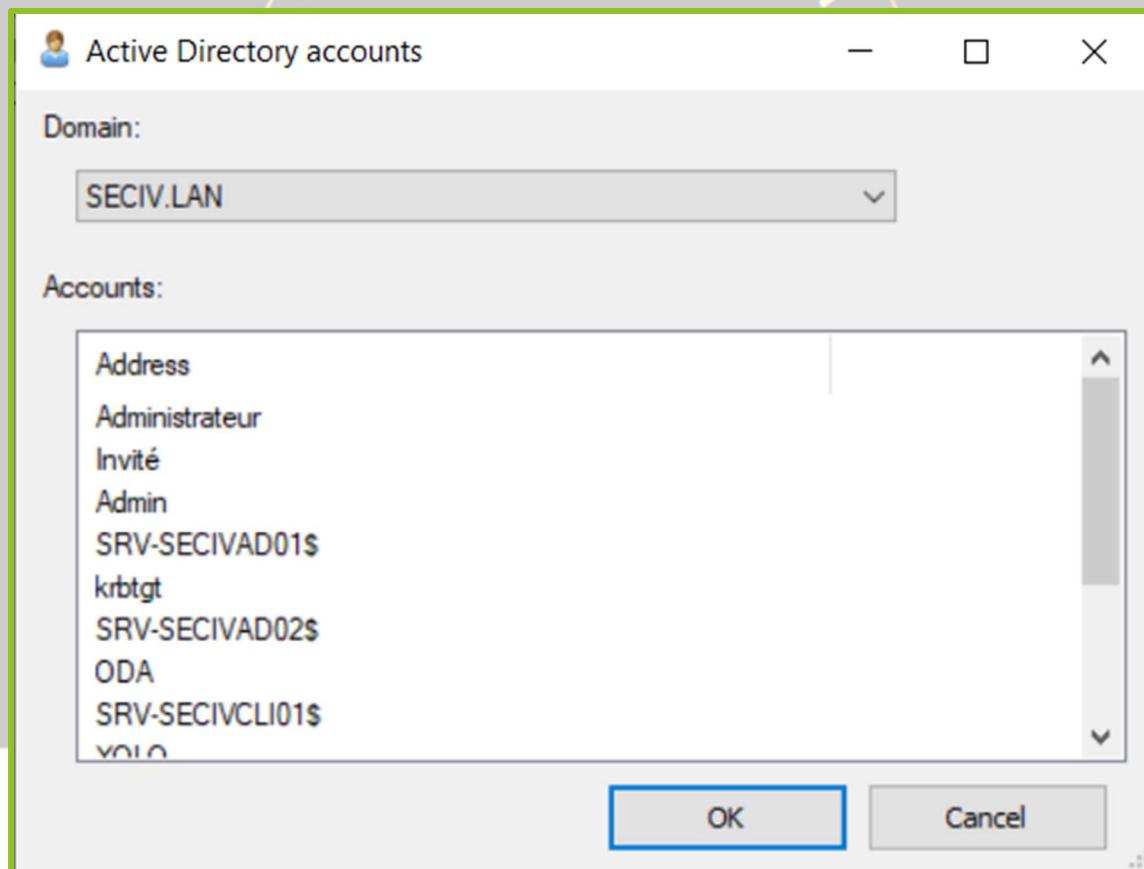


Ensuite, on ajoute des utilisateurs. Vous pouvez sélectionnez ajouter un utilisateur du domaine ou un utilisateur landa et y informer ses informations :

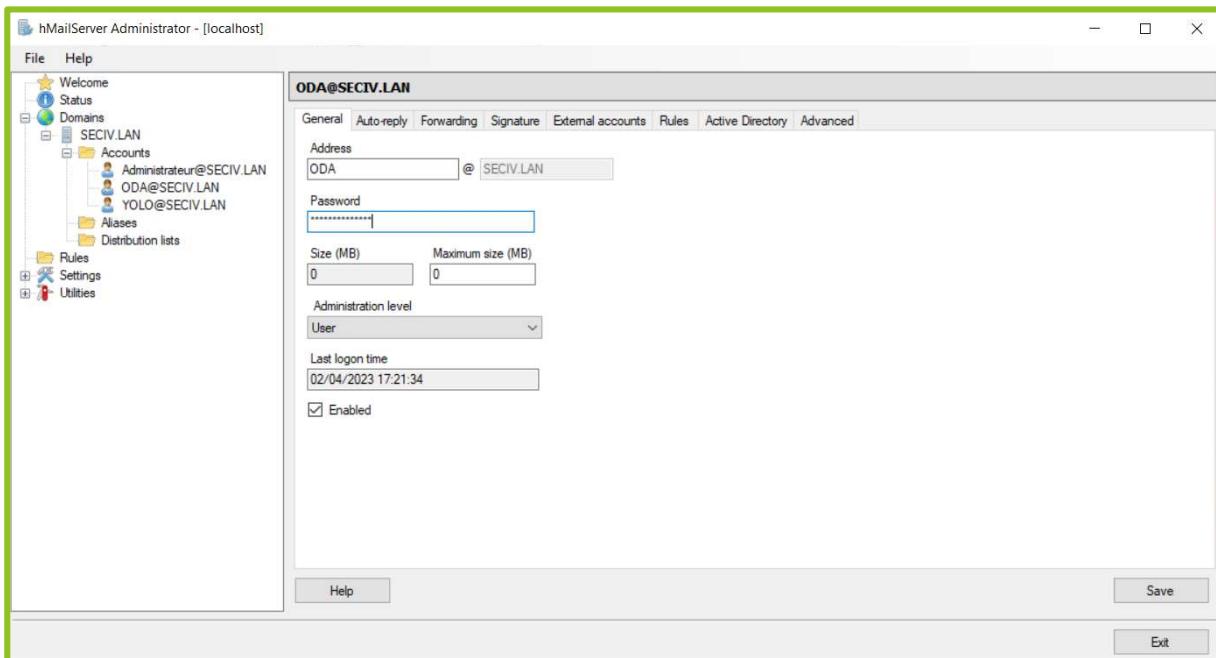


Pour un

utilisateur du domaine, sélectionnez le domaine visé et son utilisateur :



Puis informez son adresse de messagerie du domaine et renseignez le mot de passe qui lui a été donné. Vous pouvez faire la même chose pour tous les utilisateurs du



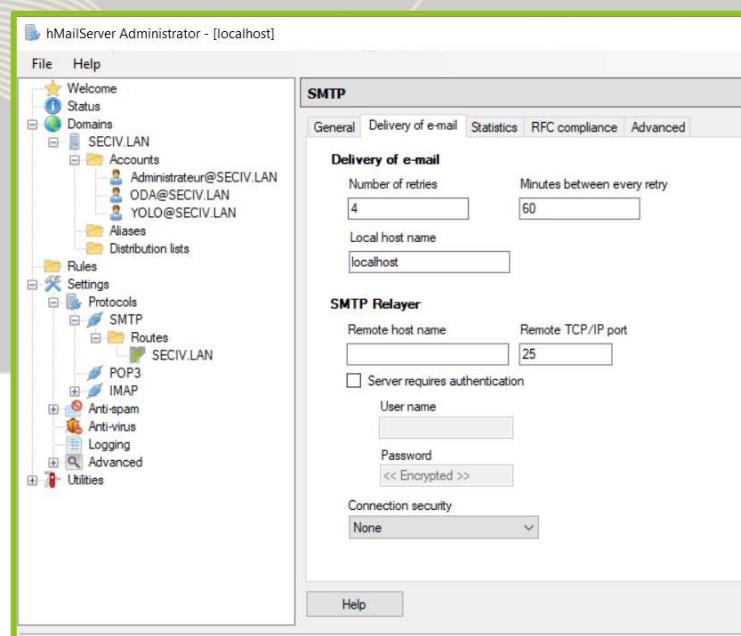
domaine.

b. Configuration du protocole SMTP

Il est impératif de configurer le protocole SMTP afin que le serveur de messagerie soit opérationnel. Celui-ci permet la transmission d'un message d'un point A vers un point B.

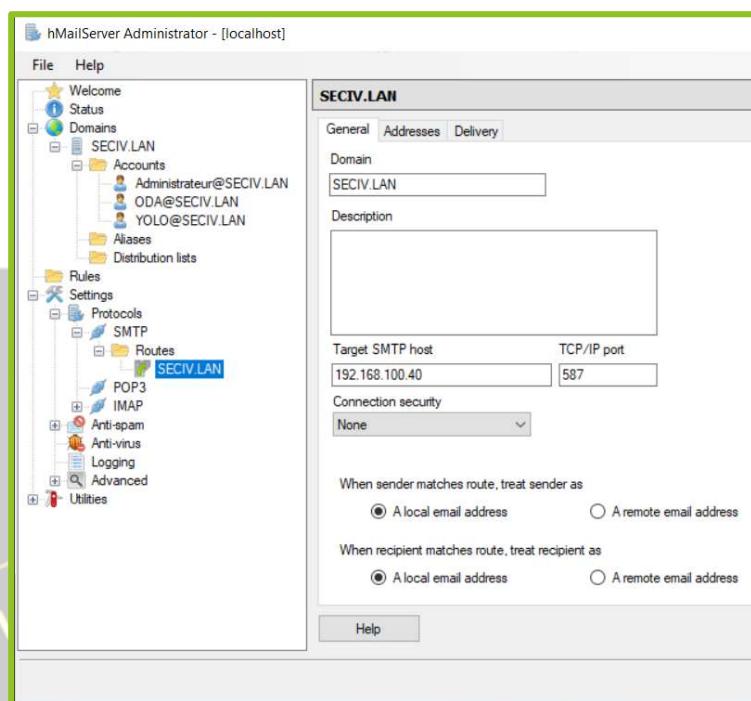
Dans cette fenêtre, il vous faudra informer le local host name. Vous pouvez soit indiquer le **nom du domaine, l'adresse IP** du serveur de messagerie ou taper simplement « **localhost** ». Au final, cela renvoie à la même source : votre serveur.

Etant donné que cette documentation porte sur la mise en œuvre d'un serveur de messagerie avec déploiement de client sous un même client de messagerie alors nous n'avons pas besoin d'informer le relayer SMTP.



Ensuite, nous allons lui renseigner une route avec les informations suivantes à compléter :

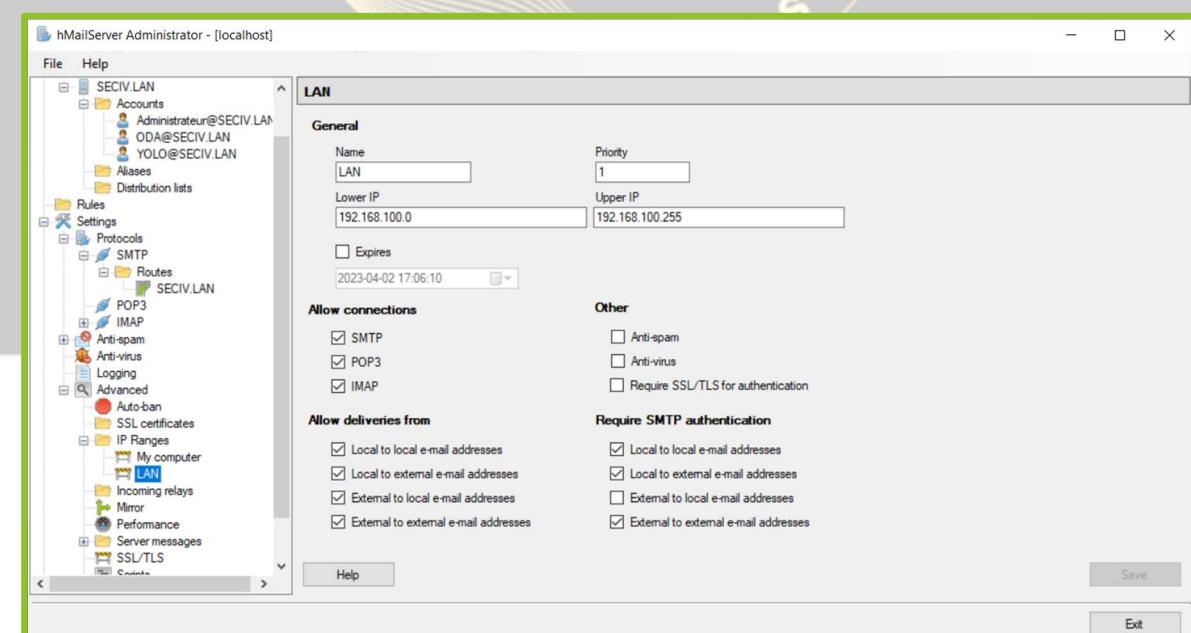
- le nom de domaine
- La cible SMTP : référence à votre serveur
- Le port utilisé : par défaut 587

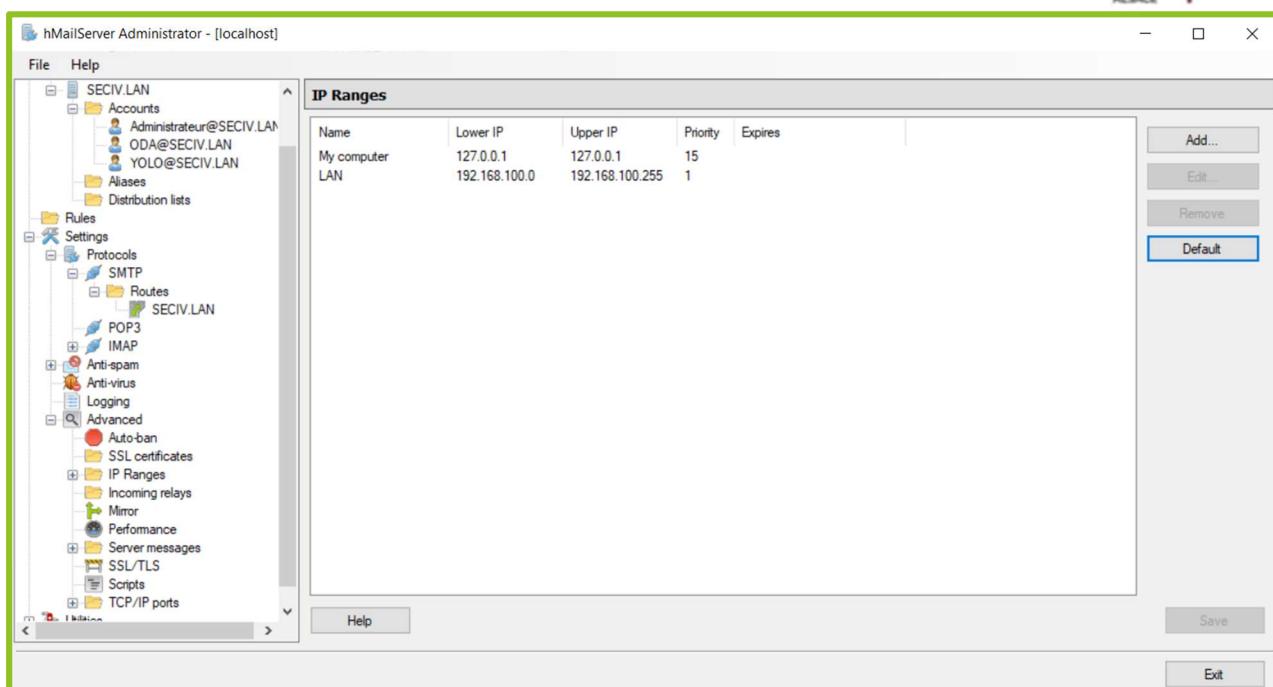


c. Ajout d'une intervalle d'adresse IP

Lorsque vous vous rendez sur Advanced > IP Ranges, vous y trouverez seulement deux intervalles :

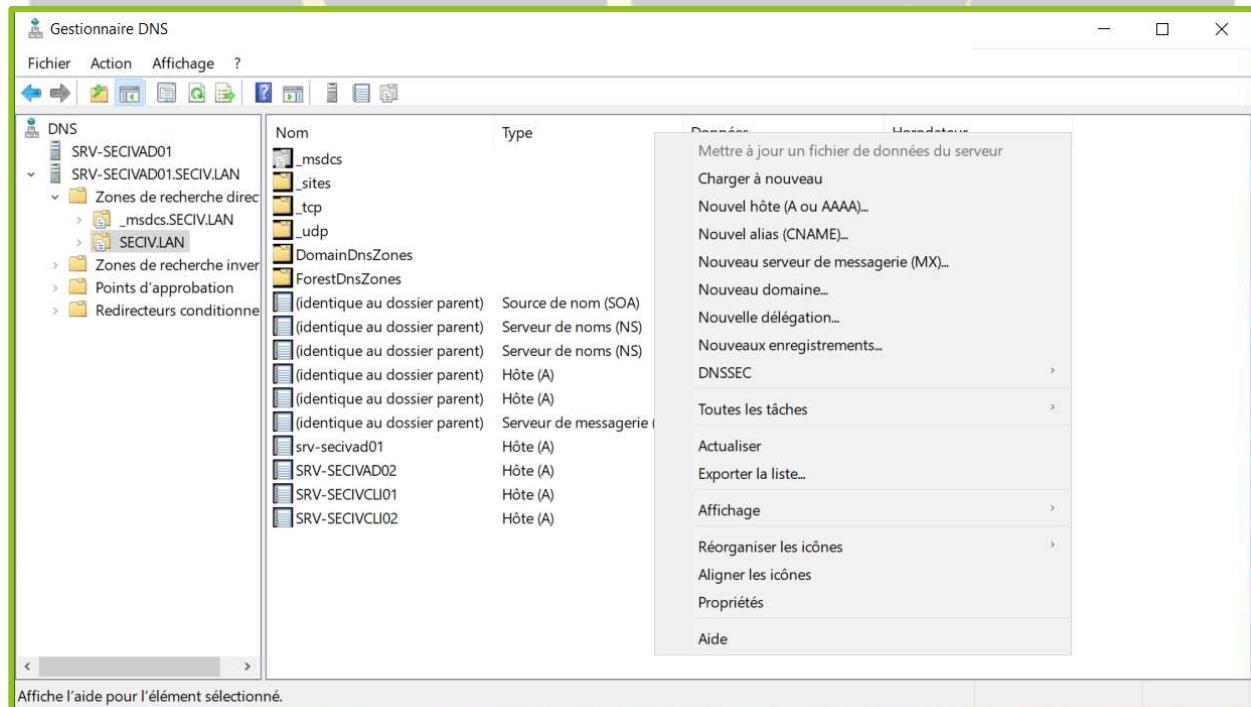
- une avec l'adresse de loopback : 121.0.0.1 qui correspond à votre serveur
- Une adresse en : 0.0.0.0
- Vous supprimerez l'adresse en 0.0.0.0 et ajouterez l'adresse de votre réseau (10.1.1.0 par exemple) comme la plus petite adresse et l'adresse de broadcast en adresse la plus haute. La priorité sera de 1 et on décoche tous les points de « Other ».

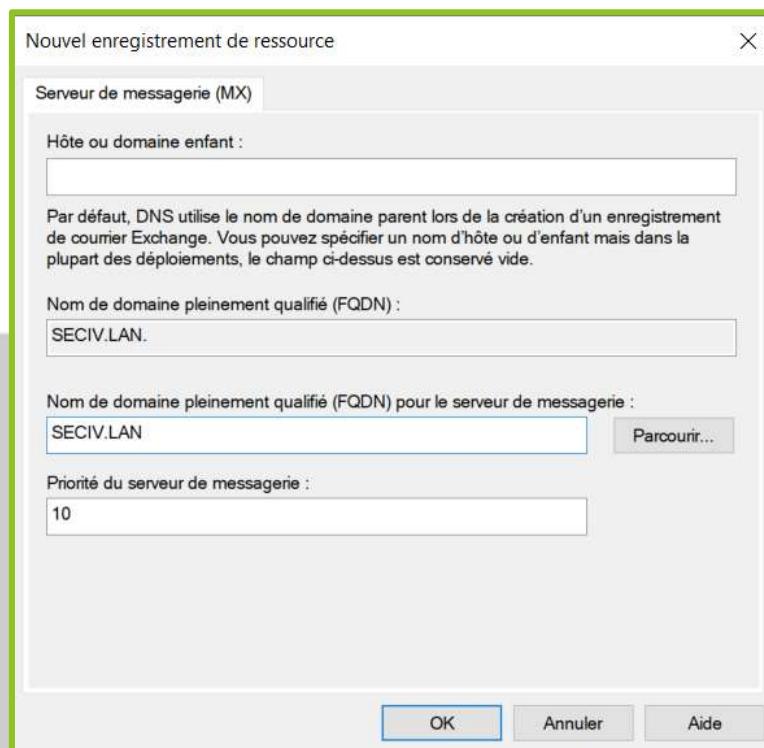




1.3.3. Ajout du serveur de messagerie dans le DNS

Le serveur de messagerie hMailServer étant bien configuré, certains paramètres nécessitent une modification. C'est le cas pour le DNS du domaine AD, nous allons ajouter un nouveau serveur de messagerie :





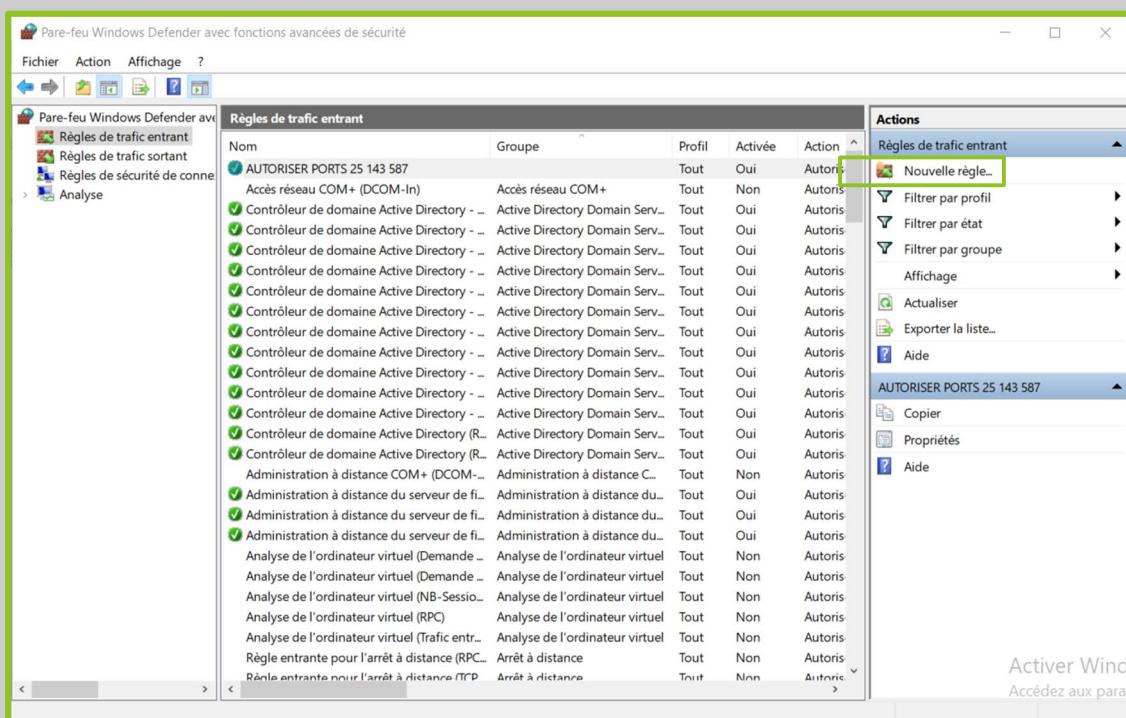
Le voici présent :

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[79], srv-secivad01.seciv.lan....	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-secivad01.seciv.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-secivad02.seciv.lan.	statique
(identique au dossier parent)	Hôte (A)	192.168.100.40	14/04/2023 08:00:00
(identique au dossier parent)	Hôte (A)	192.168.100.50	15/03/2023 14:00:00
(identique au dossier parent)	Serveur de messagerie (...)	[10] SECIV.LAN.	statique
srv-secivad01	Hôte (A)	192.168.100.40	statique
SRV-SECIVAD02	Hôte (A)	192.168.100.50	statique
SRV-SECIVCLI01	Hôte (A)	192.168.100.100	29/03/2023 10:00:00
SRV-SECIVCLI02	Hôte (A)	192.168.100.102	07/04/2023 17:00:00

1.3.4. Configuration d'hMailServer

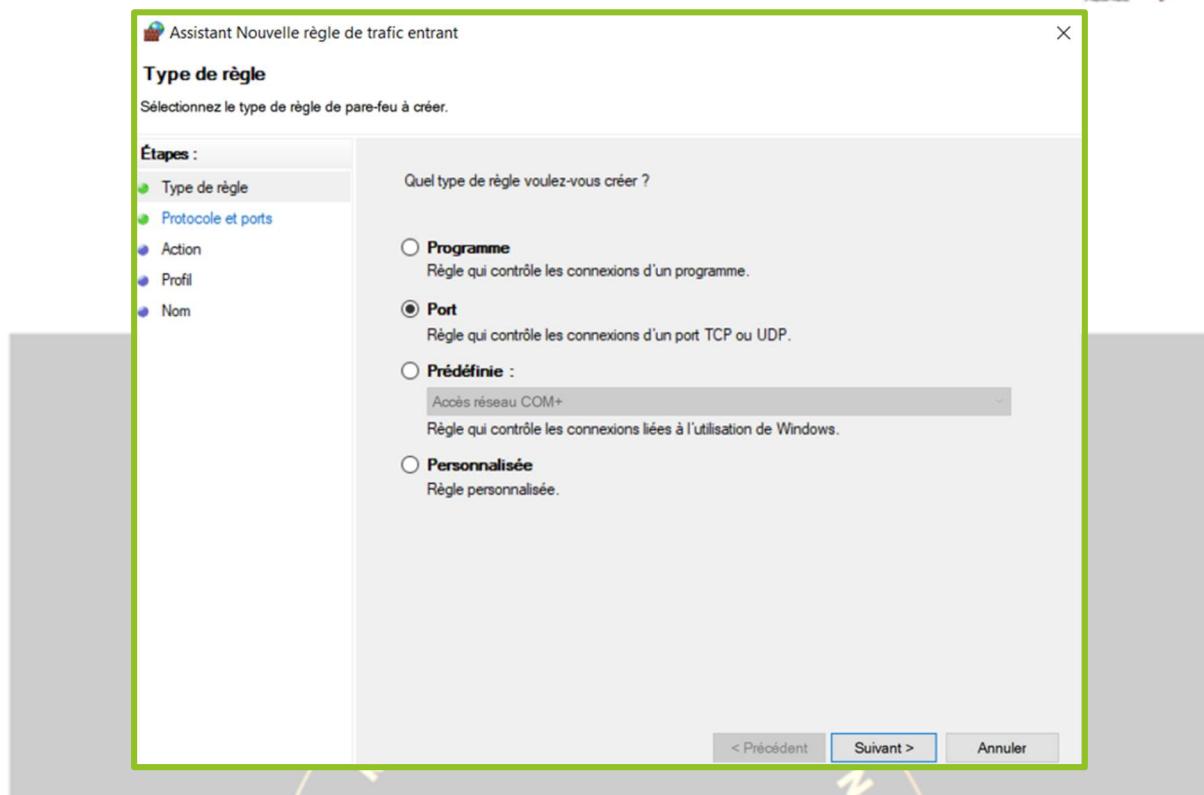
N'oublions pas que le pare-feu Windows Defender vient souvent bloquer les connexions entrantes provenant d'une source dont il ne dispose pas d'information ou car une règle vient barrer sa route. Pour que nos protocoles SMTP, IMAP et POP3 puissent transiter sans problème, nous allons devoir créer une règle autorisant leur port.

Pour cela, tapez sur la barre de recherche du menu démarrer « Pare-feu Windows Defender » et cliquer dessus puis cliquez sur « Paramètres avancés ». Les paramètres du pare-feu s'ouvrent et nous allons nous diriger vers « règles de trafic entrant » et sur « nouvelle règle » :

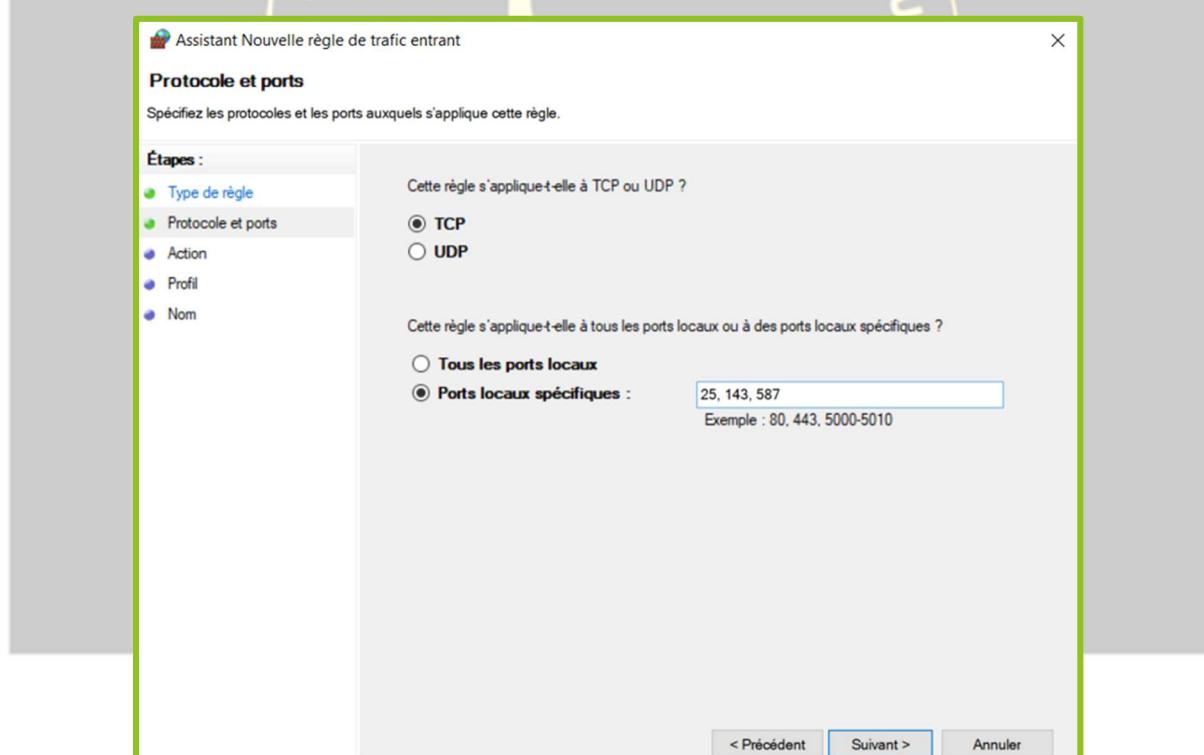


Comme vous pouvez le constater sur l'image précédente, la règle a déjà été créée mais nous allons voir les différentes étapes à passer pour la créer.

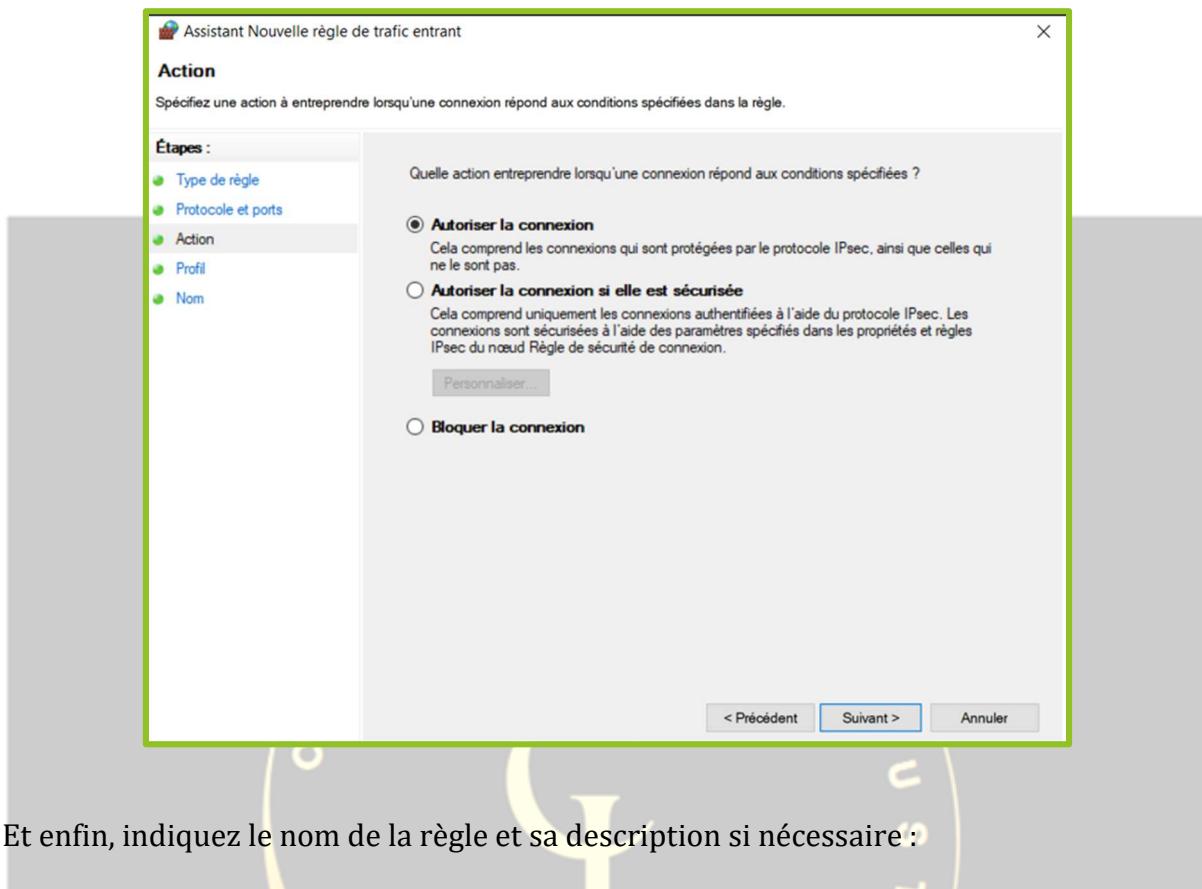
Etant donné que nous voulons créer une règle pour autoriser l'accès aux différents protocoles vus auparavant, il faut autoriser leur port. Ainsi, on choisit comme type de règle, une qui correspond au port.



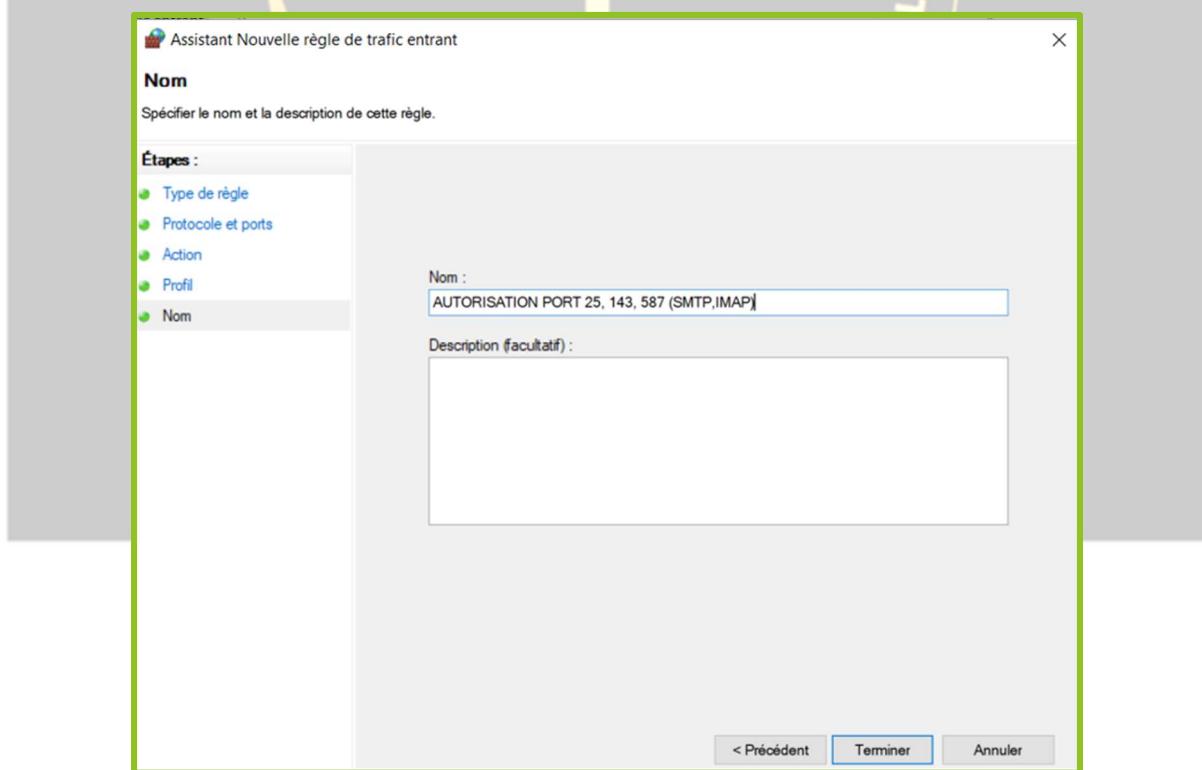
Cette règle s'applique sur le TCP et concerne les ports suivants : 25 (SMTP), 143 (IMAP) et 587 (POP3)



On indique ensuite ce que nous souhaitons entreprendre avec ces protocoles, on l'a évoqué avant c'est-à-dire les autoriser :



Et enfin, indiquez le nom de la règle et sa description si nécessaire :



1.3.5. Ajout du serveur de messagerie dans le DNS

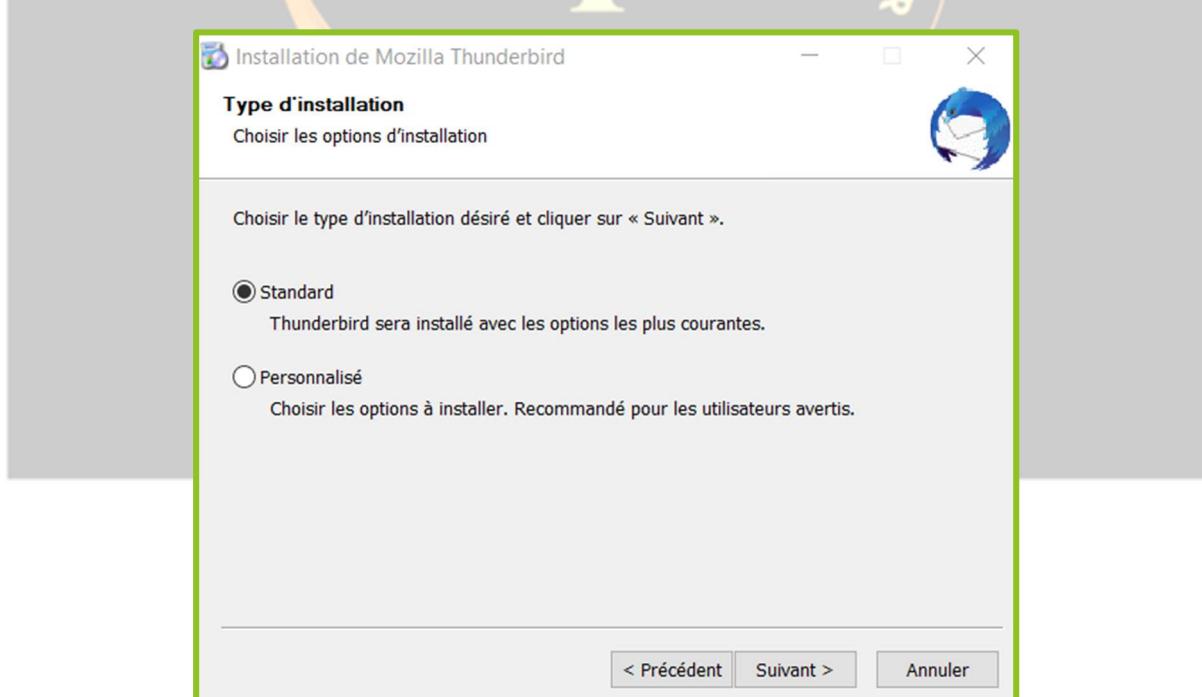
a. Installation de Thunderbird

De la même façon que pour hMailServer, le client de messagerie Thunderbird est téléchargeable sur le site officiel : <https://www.thunderbird.net/fr/>

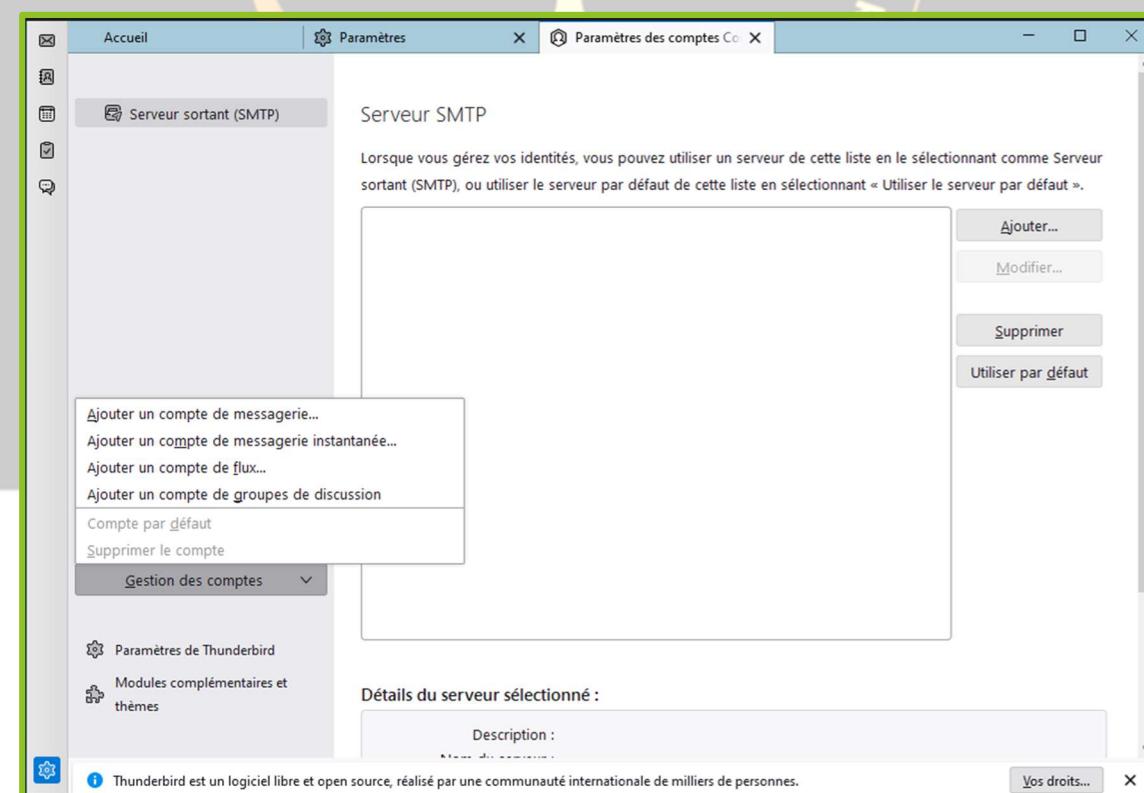
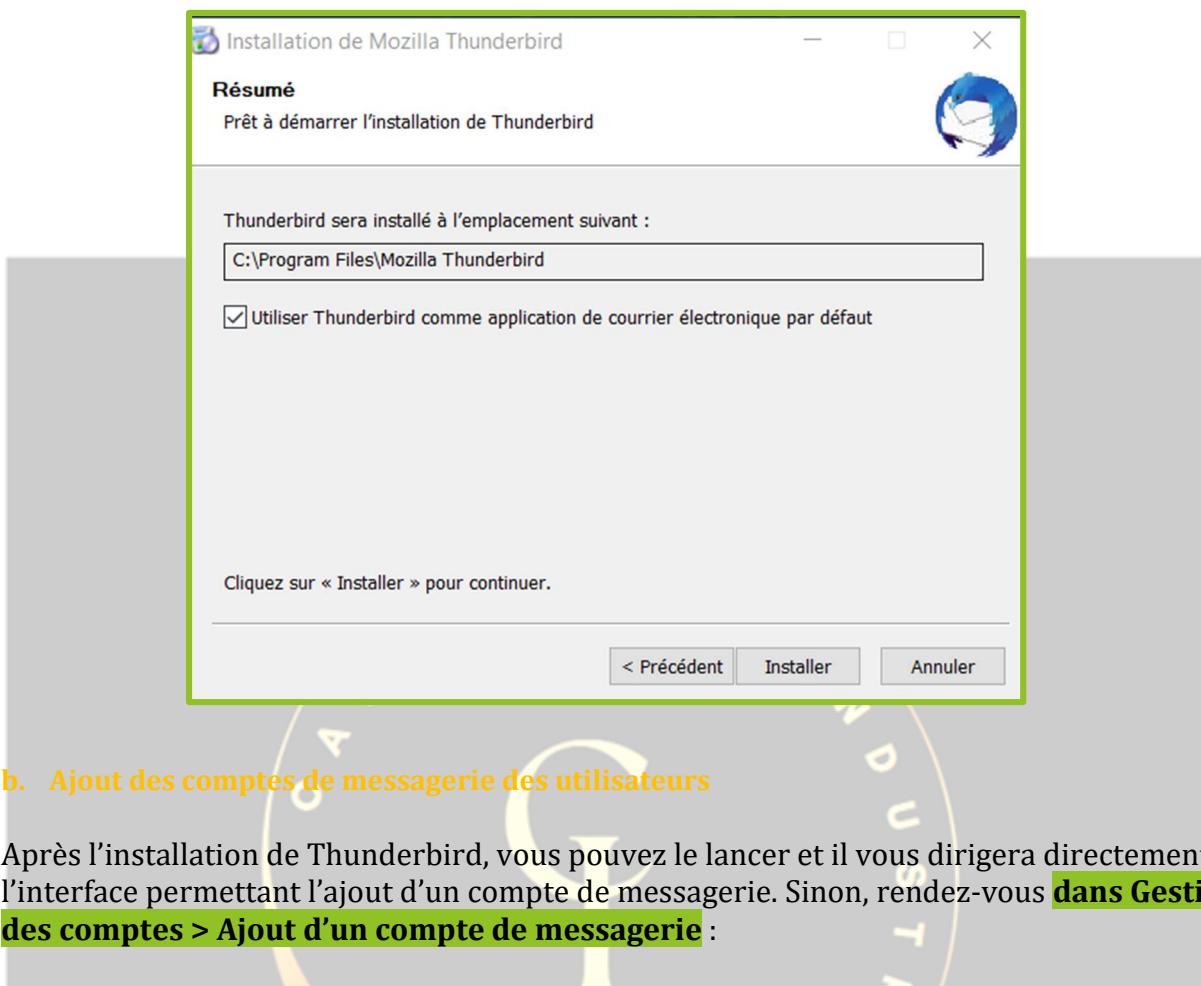
Une fois téléchargé, vous pouvez lancer l'installation et l'interface suivante apparaîtra :



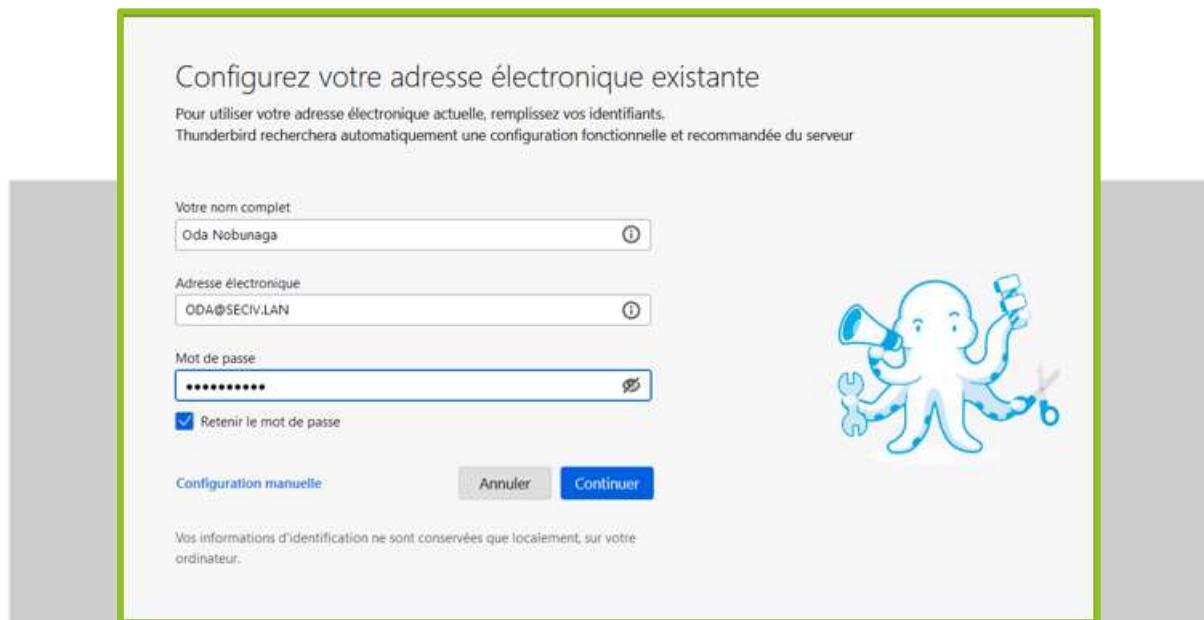
On clique sur suivant puis on choisit l'installation par défaut :



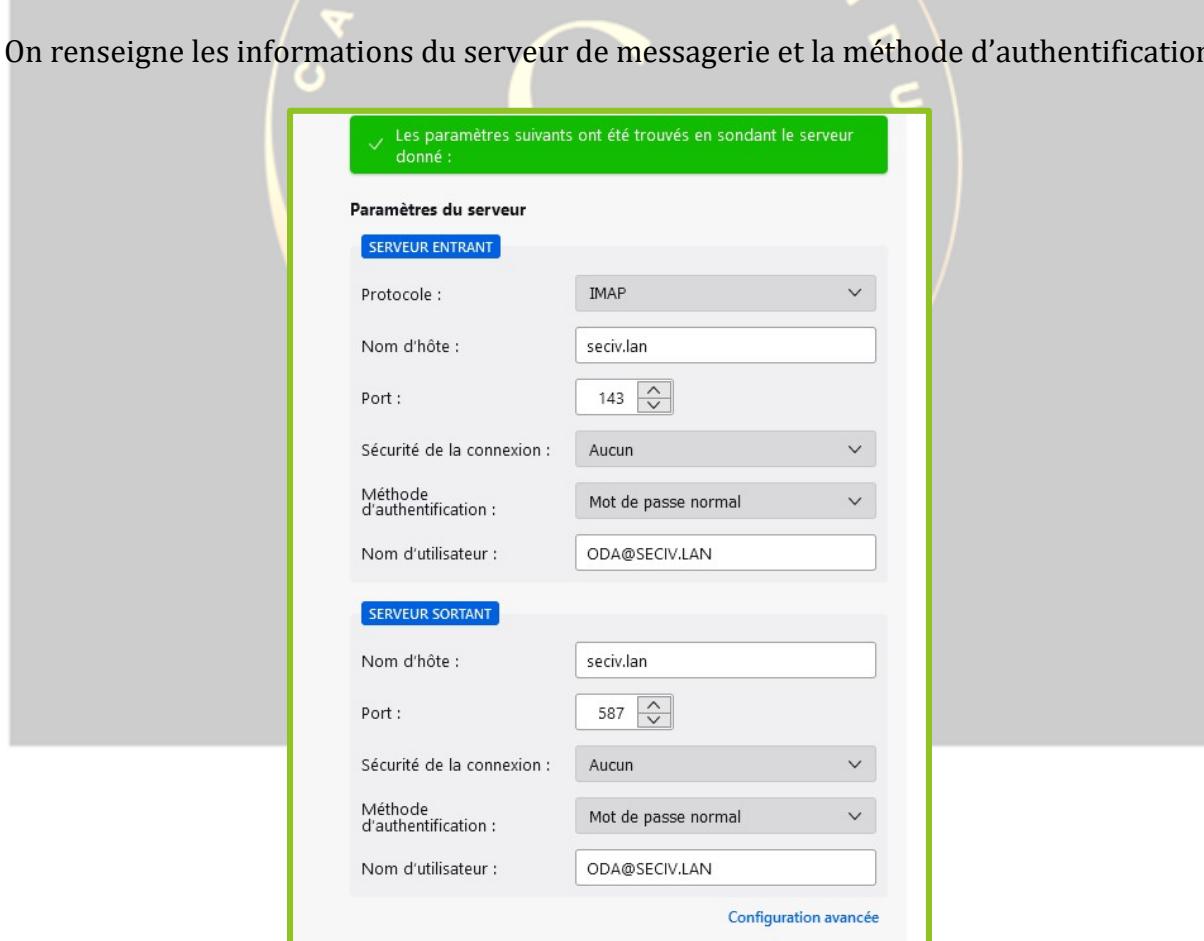
Rien d'important à signaler, on clique sur installer :



Arrivez à la page suivante, vous pouvez informer les informations de l'utilisateur. Ayant un domaine, pour ma part j'indique les données renseignées lors de sa création :



On renseigne les informations du serveur de messagerie et la méthode d'authentification :



Le compte de notre utilisateur a été créé, on effectue la même procédure pour les autres utilisateurs.



The screenshot shows the "Configuration du compte" (Account Configuration) window in Thunderbird. A green box highlights the "Création du compte réussie" (Account creation successful) message at the top. Below it, the account name "Oda Nobunaga ODA@SECIV.LAN" is listed with an "IMAP" icon. There are several configuration options: "Paramètres du compte" (Account settings), "Chiffrement de bout en bout" (End-to-end encryption), "Ajout d'une signature" (Add a signature), and "Téléchargement de dictionnaires" (Download dictionaries). A "Terminer" (Finish) button is at the bottom right. The background shows a blurred version of the same window with a different account name, "Yolo YOLO@SECIV.LAN".

✓ Crédit du compte réussie

Vous pouvez dès maintenant utiliser ce compte avec Thunderbird.
Vous pouvez enrichir l'expérience en connectant des services associés et en configurant des paramètres de compte avancés.

Yolo YOLO@SECIV.LAN POP3

Paramètres du compte Chiffrement de bout en bout

Ajout d'une signature

Téléchargement de dictionnaires

Se connecter à vos services liés

Recherche d'agendas...

Se connecter à un carnet d'adresses CardDAV

Se connecter à un carnet d'adresses LDAP

Se connecter à un agenda distant

Terminer

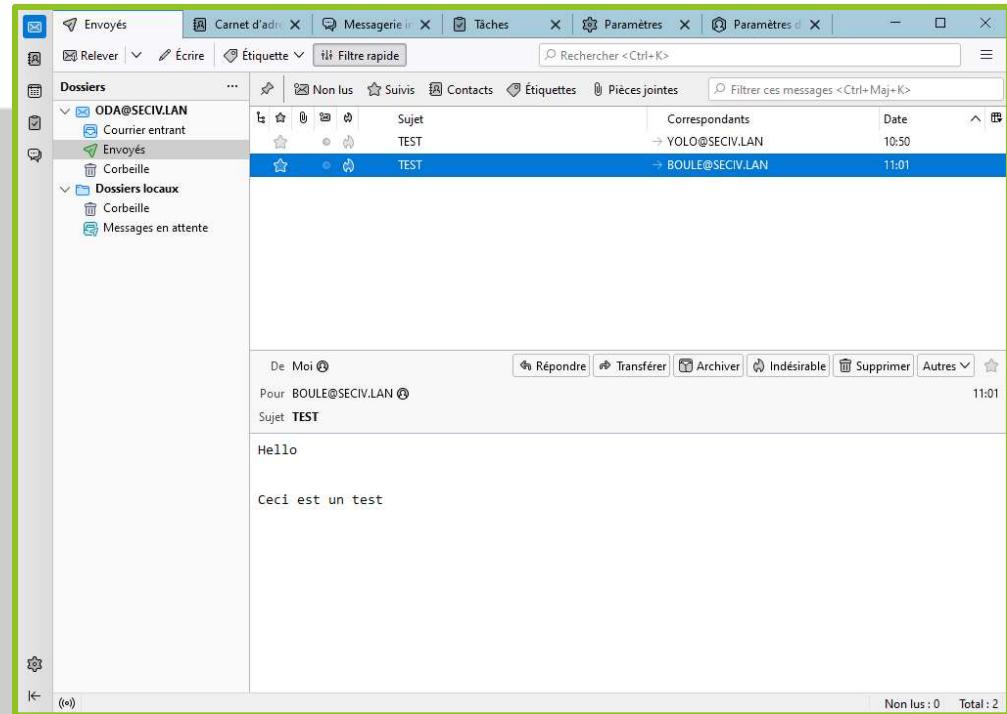
Thunderbird est un logiciel libre et open source, réalisé par une communauté internationale de milliers de personnes.



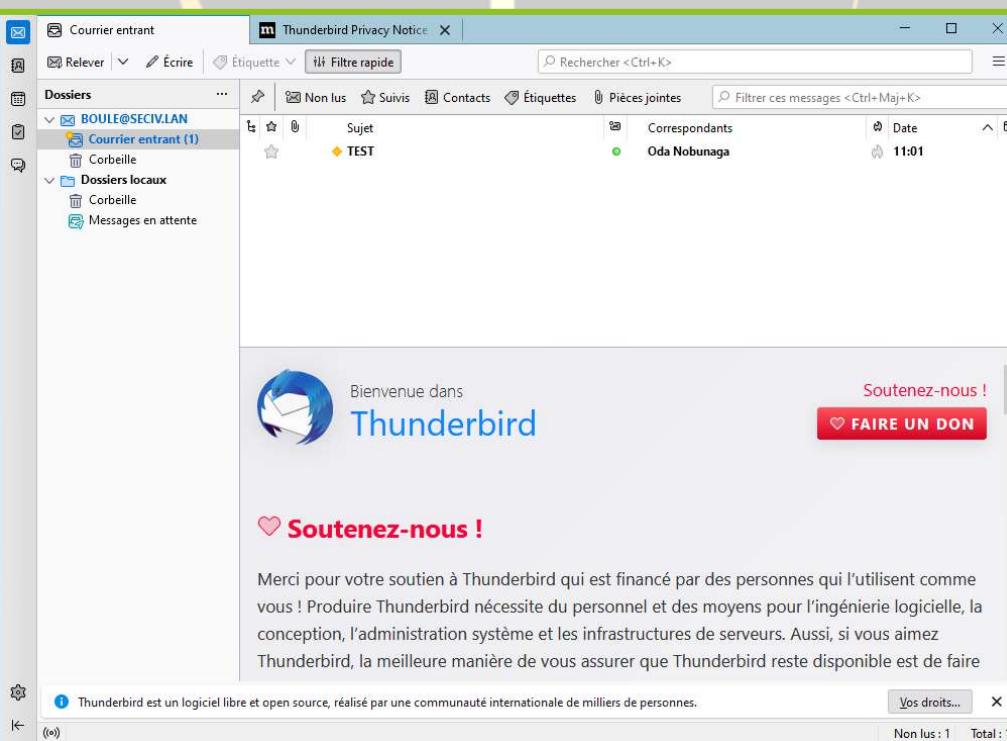
1.3.6 Test de la messagerie

Les comptes de messagerie enfin créés, nous allons tester s'ils peuvent envoyer et recevoir.

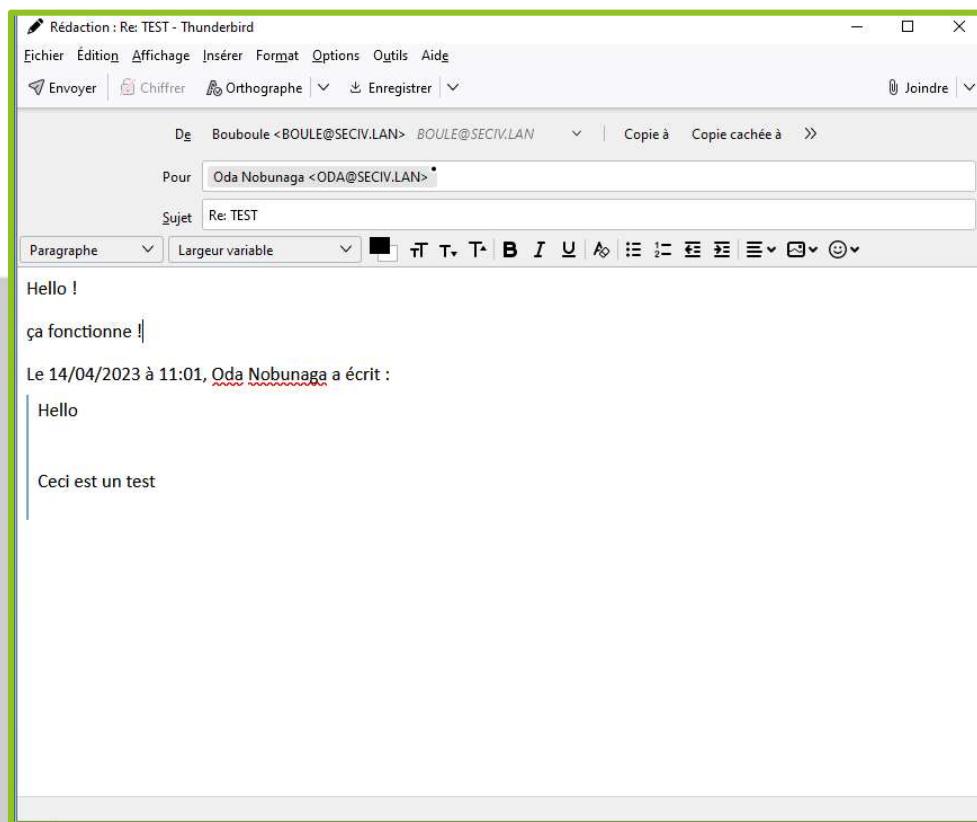
J'envoie avec le compte de mon utilisateur « Oda » à mon utilisateur « Boule » :



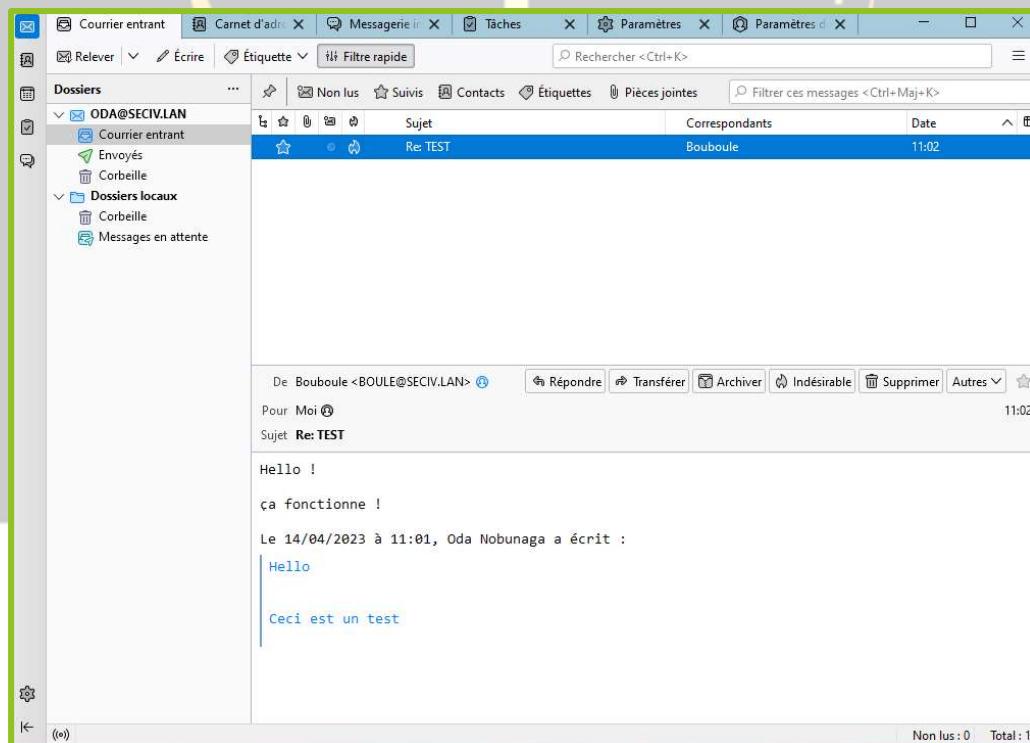
Boule a bien reçu le mail d'Oda :



Maintenant, nous allons lui répondre :



Oda reçoit bien la réponse de Boule. Ainsi tout est opérationnel.



1.4. Serveur de Téléphonie

1.4.1. Installation

Prérequis :

Pour installer notre serveur de téléphonie, il faut avoir un Debian 11, à jour et avec une ip fixe.

Pour changer l'ip de notre serveur, cela se passe dans « /etc/network/interfaces »

```
fevre@SRV-SECIVTEL: ~
GNU nano 5.4          /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 ens33
iface ens33 inet static
    address 192.168.100.60/24
    gateway 192.168.100.14
    dns-nameservers 192.168.100.40
    dns-domain SECIV.LAN
```

Nous allons ensuite installer le paquet asterisk avec la commande suivante :

```
sudo apt install asterisk
```

```
fevre@SRV-SECIVTEL:~$ sudo apt install asterisk
```

Une fois l'installation effectué, on vérifie le statut d'asterisk.

```
sudo systemctl status asterisk
```

```
fevre@SRV-SECIVTEL:~$ sudo systemctl status asterisk
[sudo] Mot de passe de fevre :
● asterisk.service - Asterisk PBX
   Loaded: loaded (/lib/systemd/system/asterisk.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-04-13 13:18:20 CEST; 58min ago
     Docs: man:asterisk(8)
     Main PID: 441 (asterisk)
        Tasks: 68 (limit: 2294)
       Memory: 83.6M
          CPU: 30.133s
        CGroup: /system.slice/asterisk.service
                  └─441 /usr/sbin/asterisk -g -f -p -U asterisk
                      ├─486 astcanary /var/run/asterisk/alt.asterisk.canary.tweet.tweet 441
```

1.4.2. Configuration

Pour la configuration, voici les principaux fichiers à modifier selon le besoin :

FICHIERS	DESCRIPTIONS
sip.conf	Configuration des canaux SIP.
users.conf	Configuration des utilisateurs.
voicemail.conf	Configuration de la messagerie vocale.
extensions.conf	Configuration du DialPlan.

Comme nous avons pu voir que asterisk est activé, nous allons modifier le fichier de configuration dans /etc/asterisk/sip.conf.

`sudo nano /etc/asterisk/sip.conf`

```
fevre@SRV-SECIVTEL:~$ sudo nano /etc/asterisk/sip.conf
```

```
fevre@SRV-SECIVTEL: ~
GNU nano 5.4                                     /etc/asterisk/sip.conf

; SIP Configuration example for Asterisk
;
; Note: Please read the security documentation for Asterisk in order to
; understand the risks of installing Asterisk with the sample
; configuration. If your Asterisk is installed on a public
; IP address connected to the Internet, you will want to learn
; about the various security settings BEFORE you start
; Asterisk.
;
; Especially note the following settings:
;   - allowguest (default enabled)
;   - permit/deny/acl - IP address filters
;   - contactpermit/contactdeny/contactacl - IP address filters for registrations
;   - context - Which set of services you offer various users
;
; SIP dial strings
```

Nous allons décommenter les lignes suivantes :

```
fevre@SRV-SECIVTEL: ~
GNU nano 5.4                                     /etc/asterisk/sip.conf

disallow=all           ; First disallow all codecs
allow=ulaw             ; Allow codecs in order of preference
```

Puis nous allons changer la langue pour français en changeant la ligne suivante :

```
fevre@SRV-SECIVTEL: ~
GNU nano 5.4                                     /etc/asterisk/sip.conf
;language=fr           ; Default language setting for all users/peers
```

Puis on décommente « dtmfmode »

```
fevre@SRV-SECIVTEL: ~
  GNU nano 5.4
/etc/asterisk/sip.conf
dtmfmode = rfc2833 ; Set default dtmfmode for sending DTMF. Default: rfc2833
; Other options:
; info : SIP INFO messages (application/dtmf-relay)
; shortinfo : SIP INFO messages (application/dtmf)
; inband : Inband audio (requires 64 kbit codec -alaw, ulaw)
; auto : Use rfc2833 if offered, inband otherwise
```

on modifie la ligne « videosupport=yes »

```
fevre@SRV-SECIVTEL: ~
  GNU nano 5.4
/etc/asterisk/sip.conf *
videosupport=yes ; Turn on support for SIP video. You need to turn this
; on in this section to get any video support at all.
; You can turn it off on a per peer basis if the general
; video support is enabled, but you can't enable it for
; one peer only without enabling in the general section.
; If you set videosupport to "always", then RTP ports will
; always be set up for video, even on clients that don't
; support it. This assists callfile-derived calls and
; certain transferred calls to use always use video when
; available. [yes|NO|always]
```

1.4.3. Configuration users.conf

Nous allons créer les utilisateurs dans le fichier users.conf qui se trouve dans /etc/asterisk/users.conf.

```
Fevre@SRV-SECIVTEL:~$ sudo nano /etc/asterisk/users.conf
```

```
fevre@SRV-SECIVTEL: ~
  GNU nano 5.4
/etc/asterisk/users.conf
;
; User configuration
;
; Creating entries in users.conf is a "shorthand" for creating individual
; entries in each configuration file. Using users.conf is not intended to
; provide you with as much flexibility as using the separate configuration
; files (e.g. sip.conf, iax.conf, etc) but is intended to accelerate the
; simple task of adding users. Note that creating individual items (e.g.
; custom SIP peers, IAX friends, etc.) will allow you to override specific
; parameters within this file. Parameter names here are the same as they
; appear in the other configuration files. There is no way to change the
; value of a parameter here for just one subsystem.
;

[general]
;
; Full name of a user
;
fullname = New User
;
; Starting point of allocation of extensions
;
userbase = 6000
;
; Create voicemail mailbox and use use macro-stdexten
;
hasvoicemail = yes
;
; Set voicemail mailbox 6000 password to 1234
;
vmsecret = 1234
```

Avant tout, nous allons créer un Template pour éviter de répéter la configuration pour tous les nouveaux utilisateurs :

```
[template]! ;notre template s'appelle template. Le ! Indique qu'il sagit d'un template.
type = friend ;type d'objet SIP.
secret = 1234 ;ici pas besoin de configuration, c'est uniquement un mdp pour l'exemple
host = dynamic ;l'utilisateur n'est pas associé à une IP fixe.
dtmfmode = rfc2833 ;mode DTMF.
disallow = all ;interdit tous les codecs.
allow = ulaw ;autorise le codec ulaw.
allow = alaw ;autorise le codec alaw.
```

Les prochains utilisateurs n'ont désormais besoin que de deux lignes à renseigner pour créer le compte :

```
[1101] (template)
context=utilisateurs
callerid=user01 <1101>

[1102] (template)
context=utilisateurs
callerid=user02 <1102>
```

Il suffit d'enregistrer le fichier, puis de redémarrer les services asterisk avec

sudo systemctl restart asterisk

```
fevre@SRV-SECIVTEL:~$ sudo systemctl restart asterisk
```

Puis on relance la console asterisk avec

sudo asterisk -rvvvv (le nombre de v est modifiable, plus il y a de « v », plus il y a d'informations)

```
fevre@SRV-SECIVTEL:~$ sudo asterisk -rvvvv
Asterisk 16.28.0~dfsg-0+deb11u2, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 16.28.0~dfsg-0+deb11u2 currently running on SRV-SECIVTEL (pid = 1130)
SRV-SECIVTEL*CLI> _
```

Avec la commande « sip show peers », on peut vérifier que les utilisateurs.

```
SRV-SECIVTEL*CLI> sip show peers
Name/username      Host          Dyn Forcerport Comedia   ACL Port    Status     Description
1101                (Unspecified) Auto (No)   No          0          Unmonitored
1102                (Unspecified) Auto (No)   No          0          Unmonitored
template           (Unspecified) D   Auto (No)  No          0          Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 3 offline]
SRV-SECIVTEL*CLI> _
```

1.4.4. Configuration Voicemail.conf

Nous allons configurer la boîte vocale en éditant le fichier Voicemail.conf :

```
fevre@SRV-SECIVTEL:/etc/asterisk$ sudo nano voicemail.conf
```

On va ensuite à la fin du fichier et ajouter ces lignes ci

```
[utilisateurs]
1101 => ,user01
1102 => ,user02
```

On peut également mettre le mot de passe avant la virgule, l'utilisateurs devrait le renseigner pour consulter sa boite vocal.

1.4.5. Configuration extensions.conf

Nous allons maintenant configurer le dialplan.

Pour cela il faut éditer le fichier « /etc/asterisk/extensions.conf »

```
fevre@SRV-SECIVTEL:/etc/asterisk$ sudo nano extensions.conf
```

Et ajouter ce qui suit à la fin du fichier :

```
[utilisateurs]
exten => _110X,1,Dial(SIP/${EXTEN},20)
exten => _110X,2,VoiceMail(${EXTEN}@utilisateurs)

exten => 888,1,VoiceMailMain(${CALLERID(num)}@utilisateurs)
```

Pour plus de compréhension :

- exten => : déclare l'extension (numéros)
- _110X : Prend les extensions (ou numéros) de 1100 à 1109 le « _ » permet d'utiliser des regex
- 1 : Ordre de l'extension
- Dial : application qui va être utilisé
- SIP: Protocol qui va être utilisé
- \${EXTEN} : variable de l'extension composé, si on appelle le 1101 la variable \${EXTEN} prendra comme valeur 1101
- 20: temps d'attente avant de passer à l'étape suivante.

Donc, la première ligne dit quand on compose le numéro 1101, et si au bout de 20 secondes il n'y a pas de réponses on passe à la ligne du dessous.

VoiceMail, pour passer sur la boîte vocale, la troisième ligne est le numéro 888, pour accéder à la boîte vocal.

On enregistre le fichier de configuration et on reload le service asterisk.

```
fevre@SRV-SECIVTEL:/etc/asterisk$ sudo systemctl restart asterisk
```

On retourne sur la console asterisk pour afficher les informations

```

SRV-SECIVTEL*CLI> sip show peers
Name/username      Host          Dyn  Forcerport Comedia   ACL Port
Status      Description
1101/1101        192.168.100.40  D   Auto (No)  No       5060
Unmonitored
1102             (Unspecified)  D   Auto (No)  No       0
Unmonitored
template         (Unspecified)  D   Auto (No)  No       0
Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 1 online, 2 offline]
SRV-SECIVTEL*CLI> sip show users
Username           Secret     Accountcode  Def.Context  ACL  Forcerport
template          1234      public       utilisateurs  No   No
1101              1234      utilisateurs  No   No
1102              1234      utilisateurs  No   No

```

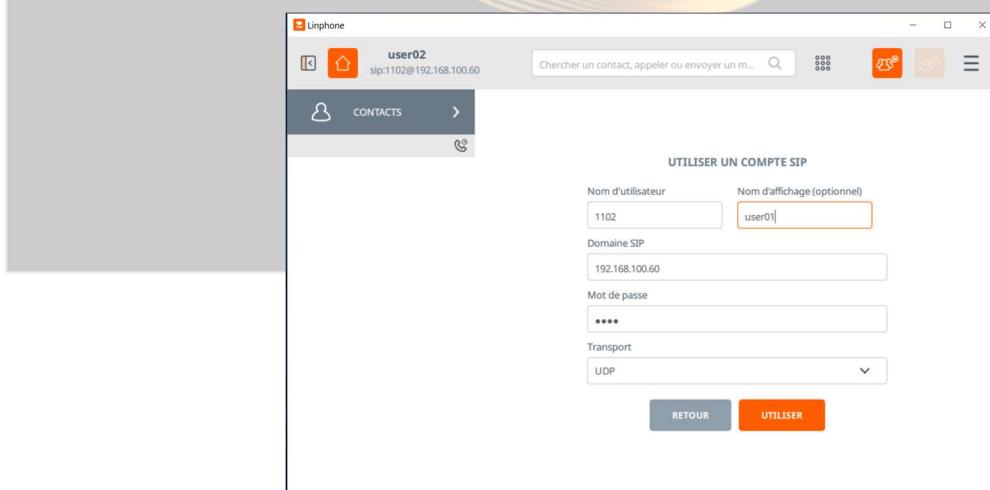
1.4.5. Configuration softphone Linphone

Pour le softphone, nous allons utiliser Linphone qui est très simple d'utilisation. Il suffit de se rendre sur le site <https://www.linphone.org/> et de cliquer sur le logo windows pour télécharger le logiciel linphone desktop.

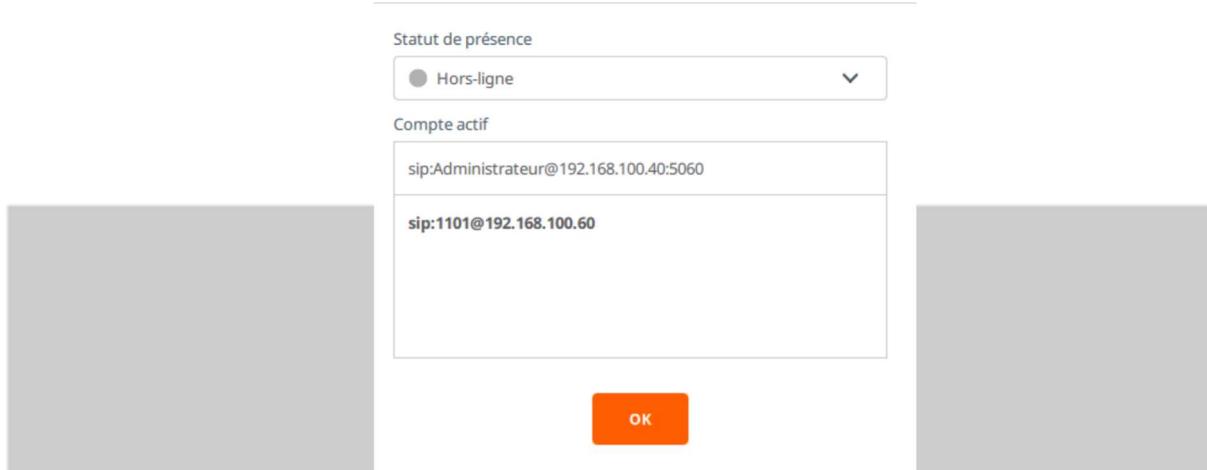
Une fois installé, il suffit de cocher la case « utiliser un compte sip »



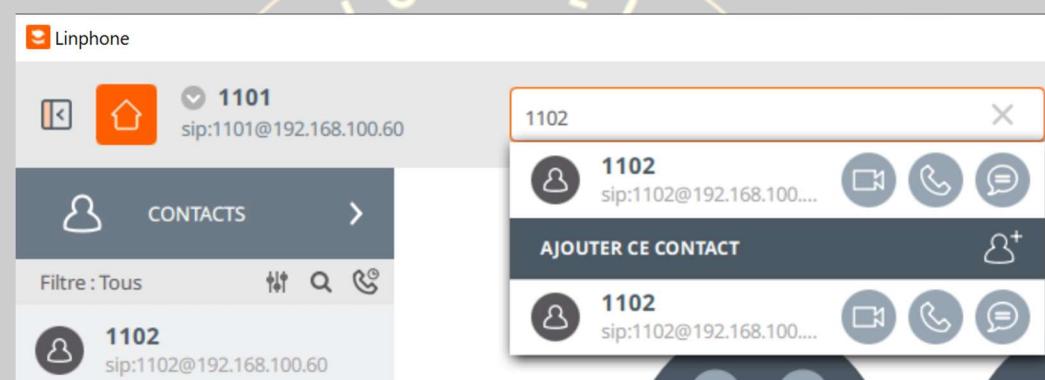
Ensute, on va remplir avec le numéro d'utilisateur, l'adresse ip du serveur de téléphonie puis le mot de passe défini et on valide.



On peut voir que le compte est bien ajouté sur le softphone.



Et on peut voir que le numéro du deuxième compte configuré est accessible également.



1.5. Serveur web (eBrigade)

1.5.1. Attribution adresse IP

L'adresse IP qui sera attribuée à notre serveur web correspondra au réseau de la DMZ créé beaucoup plus tôt et expliqué dans la partie « PfSense ».

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.40.7/24
LAN (lan)      -> em1      -> v4: 192.168.100.10/24
SEC1\DMZ (opt1) -> em2      -> v4: 192.168.200.1/24
```

Le réseau étant en 192.168.200.0, nous mettrons notre serveur en **192.168.200.10**. Nous avons également informé l'adresse virtuelle du CARP en **192.168.200.254** qu'on informera en tant qu'adresse de passerelle.

The terminal window shows the command `ip a` being run, displaying network interfaces `lo` and `ens33` with their respective configurations. Below the terminal is a configuration dialog for DNS, with the "Automatique" toggle switch turned on.

```
administrateur@SRV-SECIVWEB:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2c:5e:1d brd ff:ff:ff:ff:ff:ff
    altnet enp2s1
    inet 192.168.200.10/24 brd 192.168.200.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
administrateur@SRV-SECIVWEB:~$
```

1.5.2. Installation des paquets nécessaires à la mise en place d'eBrigade

Avant d'installer le logiciel, nous allons procéder à l'installation des mises à jours des différents paquets à travers les deux commandes suivantes :

```
sudo apt-get update
```

```
sudo apt-get upgrade -y
```

Pour pouvoir se connecter à distance via le protocole ssh, il vous faudra télécharger le paquet `openssh-server` :

```
sudo apt install openssh-server
```

Puis on l'active via la commande `systemctl` :

```
sudo systemctl enable ssh
```

```
sudo systemctl start ssh
```

Ensuite, nous avons besoin de télécharger plusieurs paquets avant de mettre en place le logiciel eBrigade. Pour cela, nous allons installer la couche LAMP comprenant :

- Apache2
- MariaDB
- PHP

```
sudo apt-get install apache2 mariadb-server php libapache2-mod-php php-mysql php-intl  
php-curl php-json php-gd php-xml php-mbstring php-zip -y
```

Il nous restera plus qu'à démarrer les services :

```
sudo systemctl start apache2
```

```
sudo systemctl start mariadb
```

```
sudo systemctl enable apache2
```

```
sudo systemctl enable mariadb
```

1.5.3. Installation d'eBrigade

Nous avons téléchargé le dossier au format zip et positionné dans le dossier Bureau du serveur Debian. Cependant, nous l'avons dézippé dans le même dossier par la commande suivante :

```
sudo unzip ebrigade_.5.2.0.zip
```

Puis, il faut le déplacer dans le dossier /var/www/html par la commande suivante :

```
administrateur@SRV-SECIVWEB:~/Bureau$ sudo mv ebrigade /var/www/html
[sudo] Mot de passe de administrateur :
administrateur@SRV-SECIVWEB:~/Bureau$ ls
ebrigade_5.2.0.zip
administrateur@SRV-SECIVWEB:~/Bureau$ cd /var/www/html
administrateur@SRV-SECIVWEB:/var/www/html$ ls
ebrigade index.html
administrateur@SRV-SECIVWEB:/var/www/html$ █
```

Ensuite, on attribue des droits sur le dossier ebrigade :

```
administrateur@SRV-SECIVWEB:~$ sudo chown -R www-data:www-data /var/www/html/ebrigade
```

1.5.4. Crédation de la base de données d'eBrigade

Après avoir lancé le service mariadb, il vous suffit de vous connecter dessus avec la commande suivante :

```
sudo mysql
```

Puis les étapes qui suivent vous permettra de créer la base de données :

```
MariaDB [(none)]> CREATE DATABASE ebrigadedb;
```

```
MariaDB [(none)]> CREATE USER 'ebrigadeuser'@'localhost' IDENTIFIED BY 'password';
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigadedb *.* TO ebrigadeuser@localhost
IDENTIFIED BY "password";
```

```
MariaDB [(none)]> FLUSH PRIVILEGES;
```

```
MariaDB [(none)]> exit
```

1.5.5. Connexion à la page web d'eBrigade

Ouvrez un navigateur et tapez : votreipserveurweb/ebrigade

Cela vous redirigera vers la page de connexion à votre serveur où vous renseignerez les identifiants de l'utilisateur créé, auparavant, dans la base de données.

The screenshot shows a two-step process for database setup:

Step 1: Configuration Base de données

Form fields (values shown):

- Server Name: localhost:3308
- User: dbo
- Password: (redacted)
- Database name: ebrigade

Step 2: Confirmation message

Message: ★ initialisation réussie

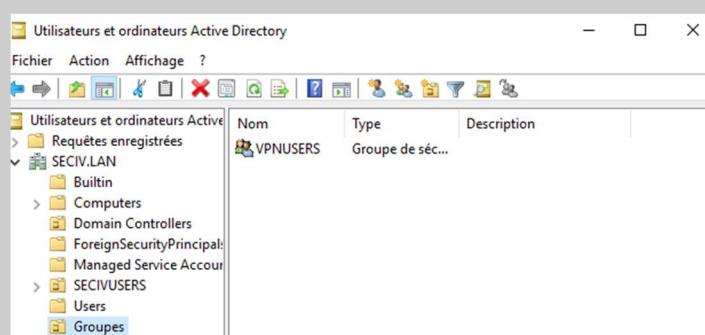
Text: Schéma de base de données importé avec succès. Vous pouvez maintenant vous connecter en utilisant le compte admin.

Button: Choix mot de passe pour admin

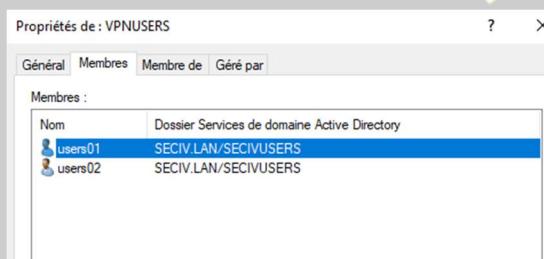
1.6. VPN Road Warrior

1.6.1. Crédation groupe uservpn

Tout d'abord nous allons créer un groupe Ad pour les utilisateur de vpn, Pour cela nous allons dans la console ad :

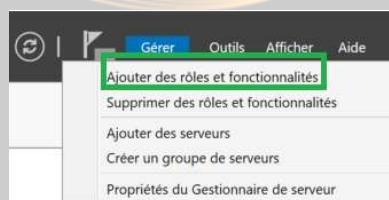


On ajoute ensuite les utilisateurs qui utiliseront le vpn :

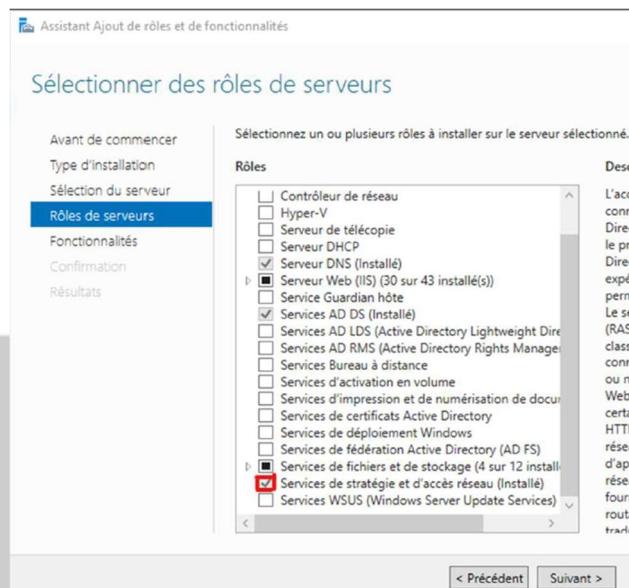


1.6.2. Installation et configuration serveur RADIUS

Nous allons maintenant installer le rôle serveur NPS sur notre serveur AD. Rendez-vous dans Ajouter des rôles et fonctionnalités :



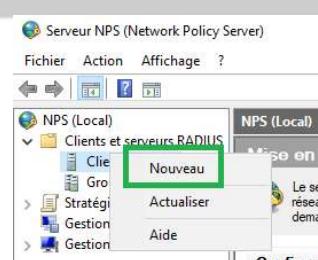
On sélectionne le service de stratégie et d'accès réseau et faire suivant jusqu'à l'installation :



Une fois que le rôle est installé, nous nous rendons dans outils, Serveur NPS pour créer un client RADIUS :



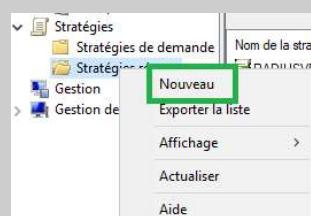
Puis clic droit sur Client RADIUS et Nouveau :



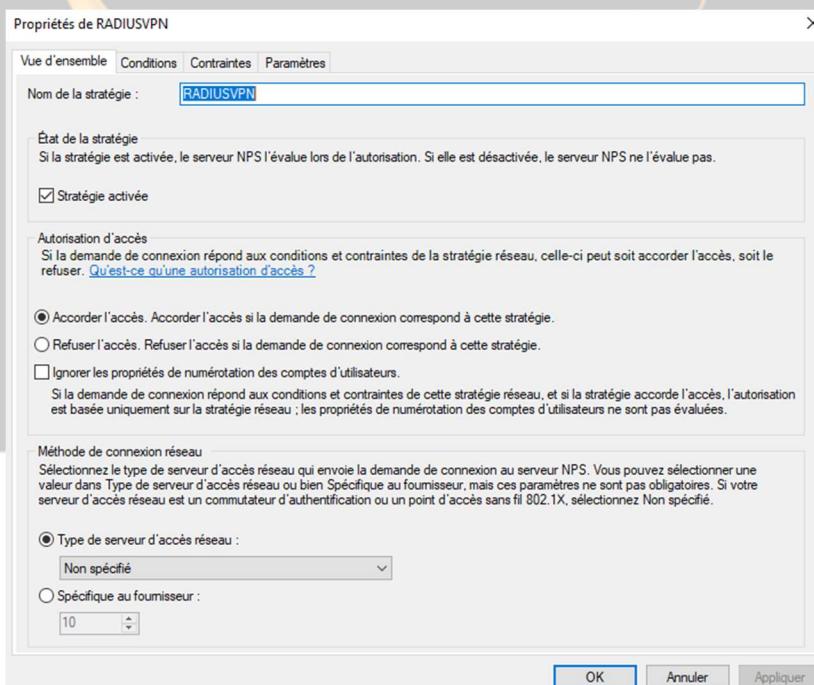
On renseigne comme ceci, l'adresse ip est celle du PFsense (ici c'est l'ip virtuelle) :



Ensuite on va sur stratégie puis on fait un clic droit sur Stratégie réseau et Nouveau :

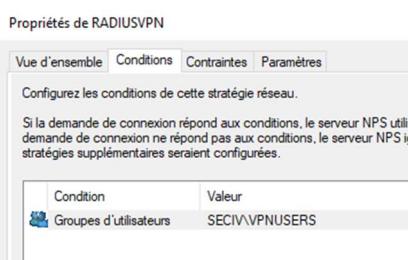


On remplit comme ceci :



On ajoute bien le groupe utilisateurs vpn, le reste de la configuration peut être laissée par

défaut :



1.6.2. OpenVPN

Maintenant, nous allons configurer un serveur d'authentification sur PFSense. Pour cela nous allons dans System/User manager/Authentications Servers. Nous allons cliquer sur Add et configurer comme sur la capture suivante puis nous pouvons cliquer sur Save :

Setting	Value
Descriptive name	RADIUS
Type	RADIUS
Protocol	MS-CHAPv2
Hostname or IP address	192.168.100.40
Shared Secret	(redacted)
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	5
RADIUS NAS IP Attribute	CARP LAN - 192.168.100.254

Ensuite nous allons dans System/Certificate Manager/ Cas puis nous allons créer un nouveau certificat d'autorité comme ceci :

System / Certificate Manager / CAs / Edit

CAs Certificates Certificate Revocation

Create / Edit CA

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

Internal Certificate Authority

<u>Key type</u>	RSA	
<u>Length</u>	1024	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
<u>Digest Algorithm</u>	sha256	The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
<u>Lifetime (days)</u>	3650	
<u>Common Name</u>	vpn-test-ca	
The following certificate authority subject components are optional and may be left blank.		
<u>Country Code</u>	FR	
<u>State or Province</u>	FRANCE	
<u>City</u>	PARIS	
<u>Organization</u>	SECIV.LAN	
<u>Organizational Unit</u>		
Save		

Ensuite nous allons dans System/Certificate Manager/ Certificates pour créer un certificat de server comme ceci :

CAs Certificates Certificate Revocation

Add/Sign a New Certificate

<u>Method</u>	Create an internal Certificate
<u>Descriptive name</u>	vpn-test

Internal Certificate

<u>Certificate authority</u>	Test VPN CA
<u>Key type</u>	RSA
<u>Key length</u>	2048
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest algorithm</u>	sha256
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
<u>Lifetime (days)</u>	
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
<u>Common Name</u>	vpn-test

<u>Country Code</u>	FR
<u>State or Province</u>	FRANCE
<u>City</u>	PARIS
<u>Organization</u>	SECIV.LAN
<u>Organizational Unit</u>	e.g. My Department Name (optional)

Certificate Attributes

<u>Attribute Notes</u>	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.	
<u>Certificate Type</u>	Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.	
<u>Alternative Names</u>	FQDN or Hostname <input type="button" value="Add"/> Type <input type="text"/> Value <input type="text"/>
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.	
<u>Add</u>	<u>+ Add</u>

Nous allons désormais configurer le vpn. Pour cela, il faut se diriger vers VPN/OpenVPN/Servers puis configurer comme ceci :

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#) [Shared Key Export](#)

General Information

Description	<input type="text" value="radius road warrior"/>
A description of this VPN for administrative reference.	
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 2 (ovpns2)

Mode Configuration

<u>Server mode</u>	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
<u>Backend for authentication</u>	<input type="text" value="RADIUS"/> Local Database
<u>Device mode</u>	<input type="text" value="tun - Layer 3 Tunnel Mode"/>
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	

Endpoint Configuration

<u>Protocol</u>	<input type="text" value="UDP on IPv4 only"/>
<u>Interface</u>	<input type="text" value="192.168.10.10 (CARP WAN)"/>
The interface or Virtual IP address where OpenVPN will receive client connections.	
<u>Local port</u>	<input type="text" value="1195"/>
The port used by OpenVPN to receive client connections.	

Cryptographic Settings

<u>TLS Configuration</u>	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
<u>TLS Key</u>	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 9dbf5ca12fd1d1b7493d8aa9391f0b12</pre> Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
<u>TLS Key Usage Mode</u>	<input type="text" value="TLS Authentication"/> In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

<u>TLS keydir direction</u>	<input type="button" value="Use default direction"/> The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
<u>Peer Certificate Authority</u>	<input type="button" value="Test VPN CA"/>
<u>Peer Certificate Revocation list</u>	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
<u>OCSP Check</u>	<input type="checkbox"/> Check client certificates with OCSP
<u>Server certificate</u>	<input type="button" value="vpn-test (Server: Yes, CA: Test VPN CA)"/>
<u>DH Parameter Length</u>	<input type="button" value="1024 bit"/> Diffie-Hellman (DH) parameter set used for key exchange.
Tunnel Settings	
<u>IPv4 Tunnel Network</u>	<input type="button" value="192.168.110.0/24"/> This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
<u>IPv6 Tunnel Network</u>	<input type="button" value=""/> This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 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.
<u>Redirect IPv4 Gateway</u>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<u>Redirect IPv6 Gateway</u>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<u>IPv4 Local network(s)</u>	<input type="button" value="192.168.100.0/24"/> IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.
<u>IPv6 Local network(s)</u>	<input type="button" value=""/> IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases.
Client Settings	
<u>Dynamic IP</u>	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
<u>Topology</u>	<input type="button" value="Subnet – One IP address per client in a common subnet"/> 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".
Advanced Client Settings	
<u>DNS Default Domain</u>	<input checked="" type="checkbox"/> Provide a default domain name to clients
<u>DNS Default Domain</u>	<input type="button" value="SECIV.LAN"/>
<u>DNS Server enable</u>	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
<u>DNS Server 1</u>	<input type="button" value="192.168.100.40"/>

Gateway creation

Both IPv4 only IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

default

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

Save

Maintenant que la configuration du vpn est faites, nous allons créer un certificat utilisateur dans System/Certificate Manager/ Certificate

CAs Certificates Certificate Revocation

Add/Sign a New Certificate

<u>Method</u>	Create an internal Certificate
<u>Descriptive name</u>	user01

Internal Certificate

<u>Certificate authority</u>	Test VPN CA
<u>Key type</u>	RSA
2048	
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest Algorithm</u>	sha256
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
<u>Lifetime (days)</u>	3650
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
<u>Common Name</u>	user01

Country Code: FR

State or Province: FRANCE

City: PARIS

Organization: SECIV.LAN

Organizational Unit: e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes: The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

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

Certificate Type: User Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names: FQDN or Hostname

Type	Value
------	-------

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

Maintenant, nous allons installer l'utilitaire d'export pour l'installation du vpn sur le client. Pour cela, on se dirige vers System/Package Manager/ Installed Packages dans l'onglet Available Packages puis nous allons choisir le packages client_export.

System / Package Manager / Available Packages

Installed Packages Available Packages

Available Packages

Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	

Package Dependencies:
 openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3

= Update = Current
 = Remove = Information = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

Une fois installé, il suffit de retourner sur VPN/OpenVPN/Client Export puis de configurer comme ceci :

OpenVPN / Client Export Utility ?

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote Access Server: radius road warrior UDP4:1195

Client Connection Behavior

Host Name Resolution: Interface IP Address

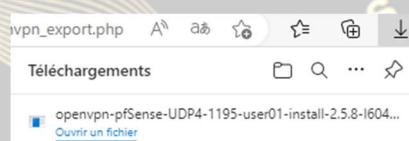
Verify Server CN: Automatic - Use verify-x509-name where possible
Optional: Optionally verify the server certificate Common Name (CN) when the client connects.

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

OpenVPN Clients

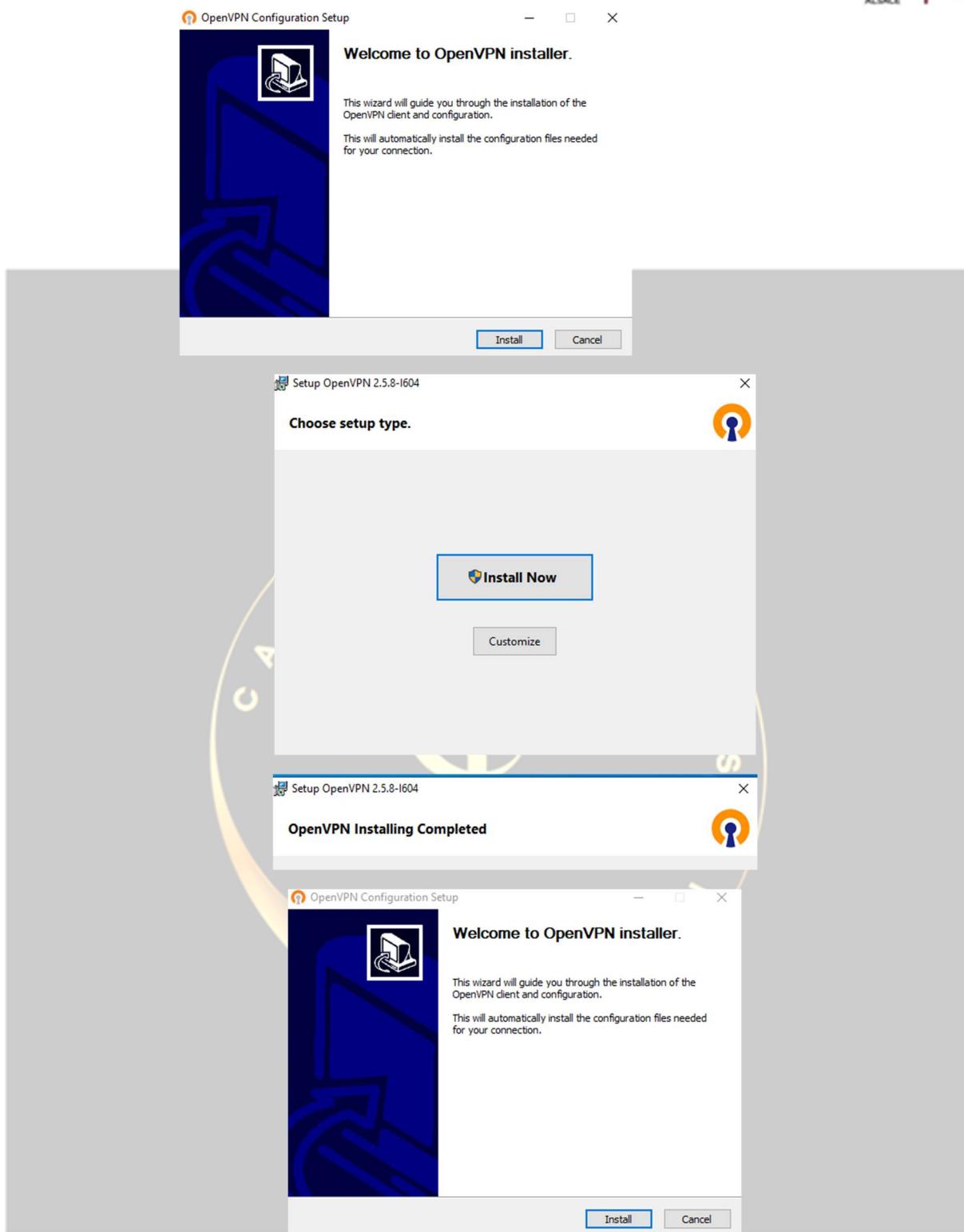
User	Certificate Name	Export
Certificate with External Auth	user01	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.5.8-lx04): 64-bit 32-bit - Legacy Windows Installers (2.4.12-lx01): 10/2016/2019 7/8/8.1/2012/2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

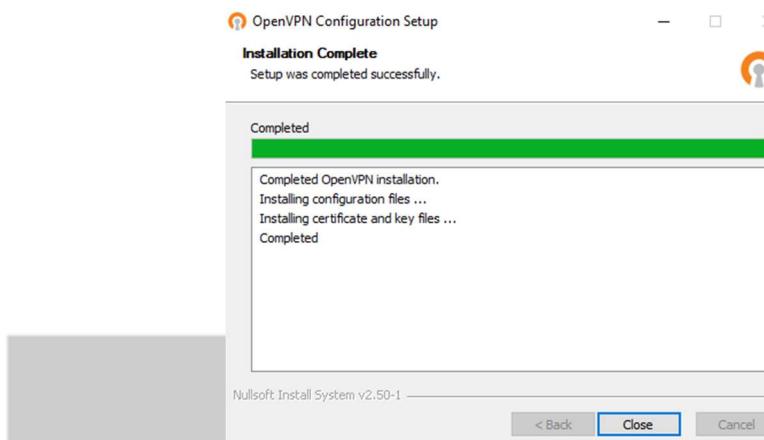
Ensuite il suffit de cliquer sur le package. Cela va télécharger un fichier que nous allons copier sur le client en question.



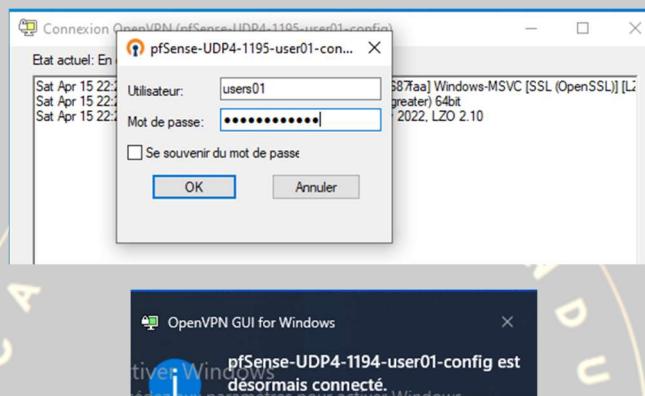
Désormais, il suffit d'installer à partir du fichier.







On va maintenant faire un test de connexion :



1.7. Serveur de supervision

1.7.1. Installation

Prérequis :

Comme pour le serveur de téléphonie, le serveur de supervision tournera sur Debian 11. Les mêmes bases sont nécessaires, à savoir, une ip fixe, et que le serveur soit à jour.

```
GNU nano 5.4                               /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 ens33
iface ens33 inet static
    address 192.168.100.80/24
    gateway 192.168.100.14
    dns-nameservers 192.168.100.80
    dns-domain SECIV.LAN
```

Ensuite, il suffit d'installer mariadb-server avec les commande suivante :

Apt install mariadb-server

Puis

Mysql_secure_installation

Pour l'installation de zabbix, la démarche est très simple, il suffit de se rendre sur le site de zabbix, sur la partie download ([Download and install Zabbix](#)) puis de sélectionner la configuration de notre serveur.

1 Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
6.4	Alma Linux	11 (Bullseye)	Server, Frontend, Agent	MySQL	Apache
6.2	CentOS	10 (Buster)	Proxy	PostgreSQL	Nginx
6.0 LTS	Debian	9 (Stretch)	Agent		
5.0 LTS	Oracle Linux		Agent 2		
4.0 LTS	Raspberry Pi OS		Java Gateway		
	Red Hat Enterprise Linux				

Zabbix nous fournit les lignes de commandes pour l'installation

2 Install and configure Zabbix for your platform

a. Install Zabbix repository

[Documentation](#)

```
# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
# dpkg -i zabbix-release_6.4-1+debian11_all.deb
# apt update
```

b. Install Zabbix server, frontend, agent

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

C'est ce que nous allons faire :

```
wget https://repo.zabbix.com/zabbix/1.4/debian/pool/main/z/zabbix-release/zabbix-
release_1.4-1+debian11_all.deb
```

```
fevre@SRV-SECIVSUPER:~$ wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
--2023-04-14 11:32:56-- https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2: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 : 3740 (3,7K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian11_all.deb »

zabbix-release_6.4-1+debian11_all.deb 100%[=====] 3,65K --.KB/s   ds 0s
2023-04-14 11:32:58 (43,1 MB/s) - « zabbix-release_6.4-1+debian11_all.deb » sauvegardé [3740/3740]
```

```
dpkg -i zabbix-release_1.4-1+debian11_all.deb
```

```
fevre@SRV-SECIVSUPER:~$ sudo dpkg -i zabbix-release_6.4-1+debian11_all.deb
[sudo] Mot de passe de fevre :
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 39339 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.4-1+debian11_all.deb ...
Dépaquetage de zabbix-release (1:6.4-1+debian11) ...
Paramétrage de zabbix-release (1:6.4-1+debian11) ...
```

Ensuite on fait un apt update et on continue par l'installation

b. Install Zabbix server, frontend, agent

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

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

```
fevre@SRV-SECIVSUPER:~$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  fonts-dejavu fonts-dejavu-extra fping libapache2-mod-php libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libltdl7
  libmodbus5 libodbc1 libonig5 libopenipmi0 libsensors-config libsensors5 libsnmp-base libsnmp40 libsshd-4 php-bcmath php-common php-gd php-ldap
  php-mbstring php-mysql php-xml php7.4-bcmath php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-mysql php7.4-opcache
  php7.4-readline php7.4-xml snmpd
Paquets suggérés :
  php-pear libmyodbc odbc-postgresql tdsodbc unixodbc-bin lm-sensors snmp-mibs-downloader snmptrapd zabbix-nginx-conf
Les NOUVEAUX paquets suivants seront installés :
  fonts-dejavu fonts-dejavu-extra fping libapache2-mod-php libapache2-mod-php7.4 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libltdl7
  libmodbus5 libodbc1 libonig5 libopenipmi0 libsensors-config libsensors5 libsnmp-base libsnmp40 libsshd-4 php-bcmath php-common php-gd php-ldap
  php-mbstring php-mysql php-xml php7.4-bcmath php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-mysql php7.4-opcache
  php7.4-readline php7.4-xml snmpd zabbix-agent zabbix-apache-conf zabbix-frontend-php zabbix-server-mysql zabbix-sql-scripts
0 mis à jour, 43 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 31,4 Mo dans les archives.
Après cette opération, 96,5 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [o/n] ■
```

c. Create initial database

Make sure you have database server up and running.

[Documentation](#)

Run the following on your database host.

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

```
mysql -u root -p
```

```
fevre@SRV-SECIVSUPER:~$ mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 40
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

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

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

MariaDB [(none)]>
```

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

```
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,000 sec)
```

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

```
MariaDB [(none)]> create user zabbix@localhost identified by '210612';
Query OK, 0 rows affected (0,001 sec)
```

```
mysql> grant all privileges on zabbix.* to zabbix@localhost;
```

```
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,001 sec)
```

```
mysql> set global log_bin_trust_function_creators = 1;
```

```
MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)
```

```
mysql> quit;
```

On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.

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

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

```
fevre@SRV-SECIVSUPER:~$ sudo zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
fevre@SRV-SECIVSUPER:~$
```

Disable log_bin_trust_function_creators option after importing database schema.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

```
mysql -uroot -p
```

```
fevre@SRV-SECIVSUPER:~$ mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

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

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

MariaDB [(none)]>
```

```
mysql> set global log_bin_trust_function_creators = 0;
```

```
MariaDB [(none)]> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected (0,000 sec)
```

```
mysql> quit;
```

d. Configure the database for Zabbix server

Edit file /etc/zabbix/zabbix_server.conf

```
DBPassword=password
```

```
c:\ fevre@SRV-SECIVSUPER: ~                               /etc/zabbix/zabbix_server.conf *
  GNU nano 5.4
DBUser=zabbix

### Option: DBPassword
#      Database password.
#      Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=210612
```

e. Start Zabbix server and agent processes

Start Zabbix server and agent processes and make it start at system boot.

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

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

```
fevre@SRV-SECIVSUPER:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
```

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

```
fevre@SRV-SECIVSUPER:~$ sudo systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
```

f. Open Zabbix UI web page

The default URL for Zabbix UI when using Apache web server is <http://host/zabbix>

The screenshot shows the initial setup screen for Zabbix 6.4. At the top left, there is a warning icon and the URL "192.168.100.80/zabbix/setup.php". On the right side, there are browser control icons. The main title "ZABBIX" is at the top center. To the left, a sidebar lists navigation options: Bienvenue, Vérification des prérequis, Configurer la connexion à la base de données, Paramètres, Résumé pré-installation, and Installer. The main content area says "Bienvenue dans Zabbix 6.4" and shows the language setting "Langage par défaut: Français (fr_FR)". At the bottom right are "Retour" and "Prochaine étape" buttons.

Nous arrivons sur cette page, il suffit de cliquer sur Prochaine étape.

The screenshot shows the "Vérification des prérequis" (Prerequisite Check) screen. The sidebar on the left remains the same. The main content displays a table of system requirements:

	Valeur actuelle	Requis
Version de PHP	7.4.33	7.4.0 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	sur	OK
mbstring pour PHP	sur	OK
Option PHP "mbstring.func_overload"	inactif	inactif OK

At the bottom right are "Retour" and "Prochaine étape" buttons.

Encore une fois :

ZABBIX

Configurer la connexion à la base de données

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

Bienvenue	Type de base de données	<input type="text" value="MySQL"/>
Vérification des prérequis	Hôte base de données	<input type="text" value="localhost"/>
Configurer la connexion à la base de données	Port de la base de données	<input type="text" value="0"/> 0 - utiliser le port par défaut
Paramètres	Nom de la base de données	<input type="text" value="zabbix"/>
Résumé pré-installation	Stocker les informations d'identification dans	<input type="radio"/> Texte brut <input type="radio"/> Coffre HashiCorp <input type="radio"/> Coffre CyberArk
Installer	Utilisateur	<input type="text" value="zabbix"/>
	Mot de passe	<input type="password" value="*****"/>

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).

[Retour](#) [Prochaine étape](#)

Ici il suffit de renseigner le nom du serveur zabbix puis de valider

ZABBIX

Paramètres

Bienvenue	Nom du serveur Zabbix	<input type="text" value="SRV-SECIVSUPER"/>
Vérification des prérequis	Fuseau horaire par défaut	<input type="text" value="Système: (UTC+00:00) UTC"/>
Configurer la connexion à la base de données	Thème par défaut	<input type="text" value="Bleu"/>
Paramètres		
Résumé pré-installation		
Installer		

[Retour](#) [Prochaine étape](#)

ZABBIX

Résumé pré-installation

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

Bienvenue	Type de base de données	MySQL
Vérification des prérequis	Serveur base de données	localhost
Configurer la connexion à la base de données	Port de la base de données	défaut
Paramètres	Nom de la base de données	zabbix
Résumé pré-installation	Utilisateur base de données	zabbix
Installer	Mot de passe utilisateur de la base de données	*****
	Chiffrement TLS de la base de données	false

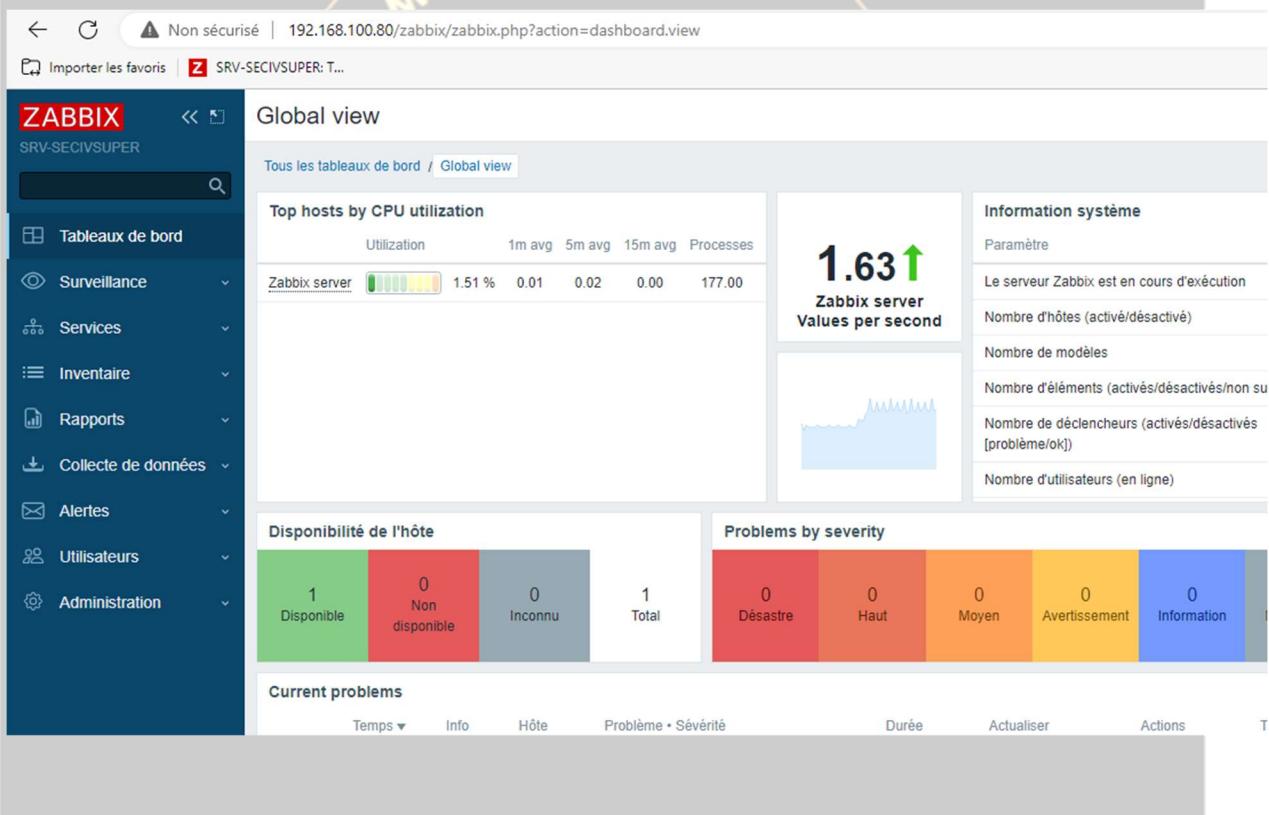
Nom du serveur Zabbix SRV-SECIVSUPER

[Retour](#) [Prochaine étape](#)

Après validation, zabbix est configuré



Voici la vue de la console :



Pour la partie client, il faut installer un agent sur chaque machine de l'infrastructure pour la supervision. L'installation débute également sur le site de zabbix, et il faudra changer selon l'os. Pour les OS Windows, l'agent est disponible avec les informations suivantes :

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		
AIX			5.4		
FreeBSD			5.2		
OpenBSD			5.0 LTS		
Solaris			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

Zabbix Release: 6.4.1

Zabbix agent v6.4.1[Read manual](#)

Packaging: MSI
 Encryption: OpenSSL
 Linkage: Dynamic
 Checksum: sha256: 4e23e2d7084ac856b067e9dd74fcbb6be30fa0b9a07efc9e2d6ccb98ff0d59cf
 shal: 821b38d5be19f32b91cd0018559d798138cab21
 md5: 83b3abdc92f0c81241121c1b4bba2d2e

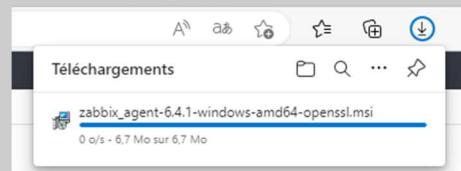
[DOWNLOAD](#)https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.1/zabbix_agent-6.4.1-windows-amd64-openssl.msi

Watch recorded webinar:

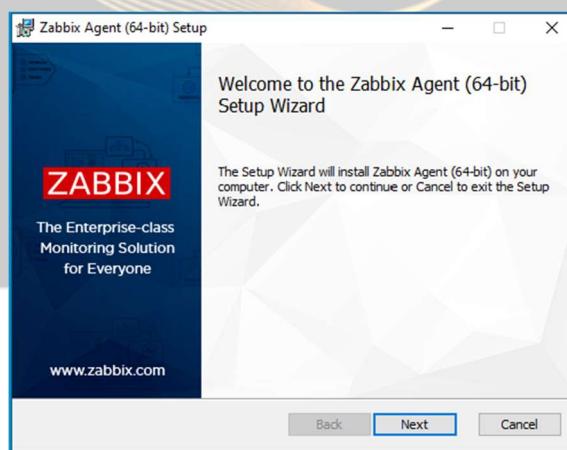


Nous allons procéder à l'installation sur un client Windows 10.

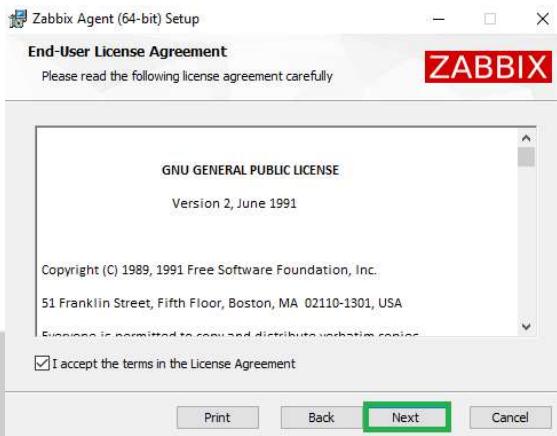
Une fois sur la page précédente, il suffit de cliquer sur DOWNLOAD.



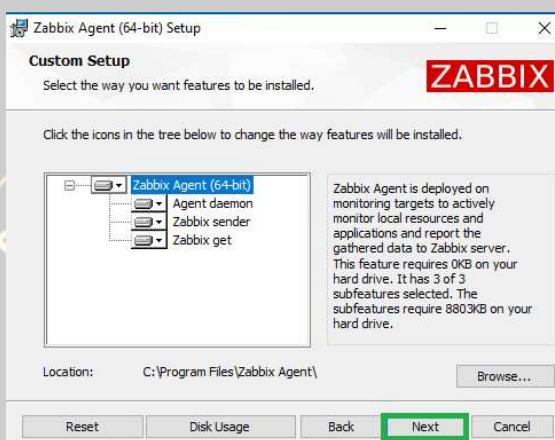
Ensuite, nous allons procéder à l'installation en exécutant le fichier que nous venons de télécharger. Cliquez sur Next :



On accepte les termes puis on clique sur Next :



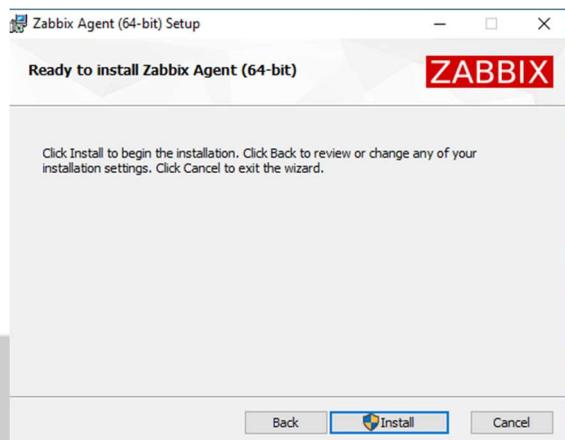
On clique sur Next :



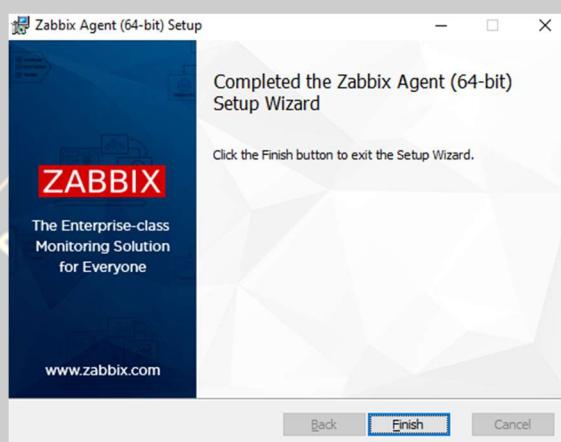
On renseigne l'ip du server de supervision :

Client	Serveur
<p>Zabbix Agent (64-bit) v6.4.1 Setup</p> <p>Zabbix Agent service configuration</p> <p>Please enter the information for configure Zabbix Agent</p> <p>ZABBIX</p> <p>Host name: <input type="text" value="CLIENT-MUL"/></p> <p>Zabbix server IP/DNS: <input type="text" value="192.168.100.80"/></p> <p>Agent listen port: <input type="text" value="10050"/></p> <p>Server or Proxy for active checks: <input type="text" value="127.0.0.1"/></p> <p><input type="checkbox"/> Enable PSK</p> <p><input type="checkbox"/> Add agent location to the PATH</p> <p>Back Next Cancel</p>	<p>Zabbix Agent (64-bit) v6.4.1 Setup</p> <p>Zabbix Agent service configuration</p> <p>Please enter the information for configure Zabbix Agent</p> <p>ZABBIX</p> <p>Host name: <input type="text" value="SRV-SECIVAD01"/></p> <p>Zabbix server IP/DNS: <input type="text" value="192.168.100.80"/></p> <p>Agent listen port: <input type="text" value="10050"/></p> <p>Server or Proxy for active checks: <input type="text" value="127.0.0.1"/></p> <p><input type="checkbox"/> Enable PSK</p> <p><input type="checkbox"/> Add agent location to the PATH</p> <p>Back Next Cancel</p>

Ensuite, on clique sur Install :



Une fois l'installation terminée, on clique sur Finish :



On vérifie dans la console services.msc que le service est bien en cours d'exécution :

SMP de l'Espace de stockag...	Service hôte...	Manuel	Service réseau
Spouleur d'impression	Ce service ...	En co...	Système local
Station de travail	Crée et mai...	En co...	Service réseau
Stockage des données utilis...	Gère le stoc...	En co...	Système local
Stratégie de retrait de la cart...	Autorise le s...	Manuel	Système local
SysMain	Gère et amé...	En co...	Système local
Système d'événement COM+	Prend en ch...	En co...	Service local
Système de fichiers EFS (En...	Fournit la te...	Manuel (Déclenche...	Système local
Télécopie	Vous perme...	Manuel	Service réseau
Téléphonie	Prend en ch...	Manuel	Service réseau
Temps Windows	Conserve la ...	En co...	Manuel (Déclenche...
Thèmes	Fournit un s...	En co...	Système local
Vérificateur de points	Vérifie les e...	Manuel (Déclenche...	Système local
VMware Alias Manager and ...	Alias Mana...	En co...	Système local
VMware Snapshot Provider	VMware Sn...	Manuel	Système local
VMware SVGA Helper Service	Helps VMw...	En co...	Système local
VMware Tools	Fournit un s...	En co...	Système local
WalletService	Objets d'hô...	Manuel	Système local
WarpJITSvc	Provides a Jl...	Manuel (Déclenche...	Service local
WebClient	Permet à un...	Manuel (Déclenche...	Service local
Windows Connect Now - R...	WCNCSCV ...	Manuel	Service local
Windows Installer	Ajoute, mo...	Manuel	Système local
Windows Mixed Reality Op...	Enables Mix...	Manuel	Système local
Windows Search	Fournit des ...	En co...	Automatique (débu...
Windows Update	Active la dé...	En co...	Manuel (Déclenche...
Xbox Accessory Manageme...	This service ...	En co...	Manuel (Déclenche...
Zabbix Agent	Provides sys...	En co...	Automatique

Propriétés de Zabbix Agent (Ordinateur local)

Général Connexion Récupération Dépendances

Nom du service : Zabbix Agent

Nom complet : Zabbix Agent

Description : Provides system monitoring

Chemin d'accès des fichiers exécutables : "C:\Program Files\Zabbix Agent\zabbix_agentd.exe" --config "C:\Program F

Type de démarrage : Automatique

État du service : En cours d'exécution

Démarrer Arrêter Suspender Reprendre

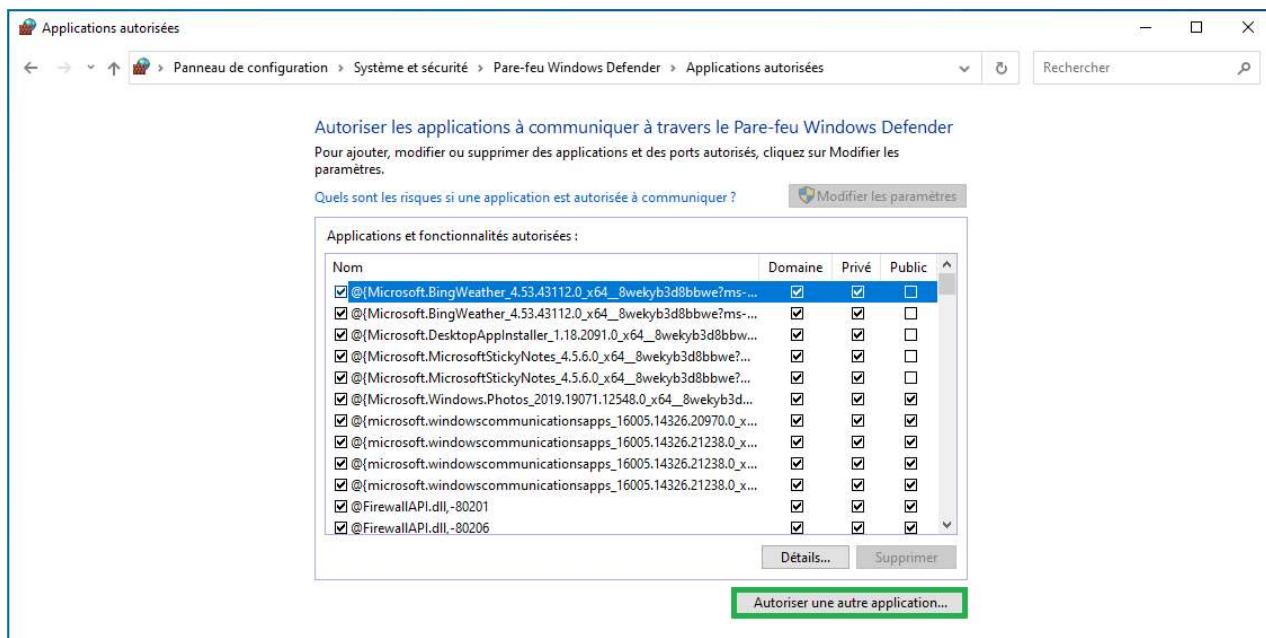
Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du service.

Paramètres de démarrage : [champ vide]

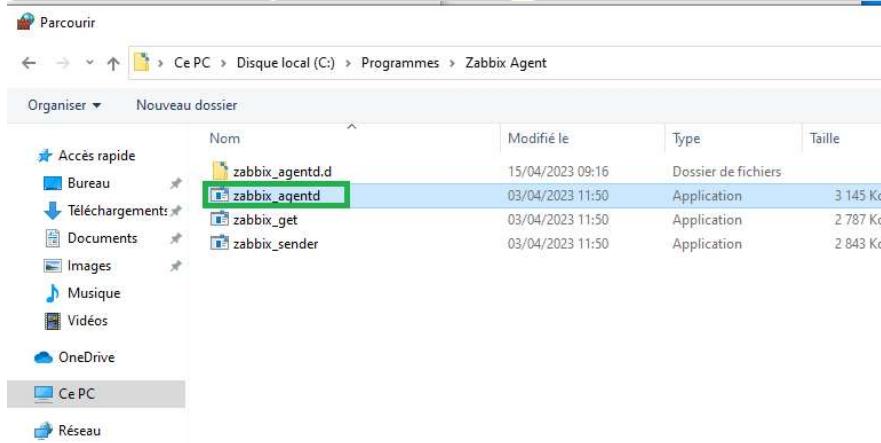
OK Annuler Appliquer

Pour ouvrir le port de l'Agent Zabbix dans le pare-feu de Windows, ouvrez le Panneau de configuration -> Système et Sécurité -> Pare-feu de Windows -> Autoriser

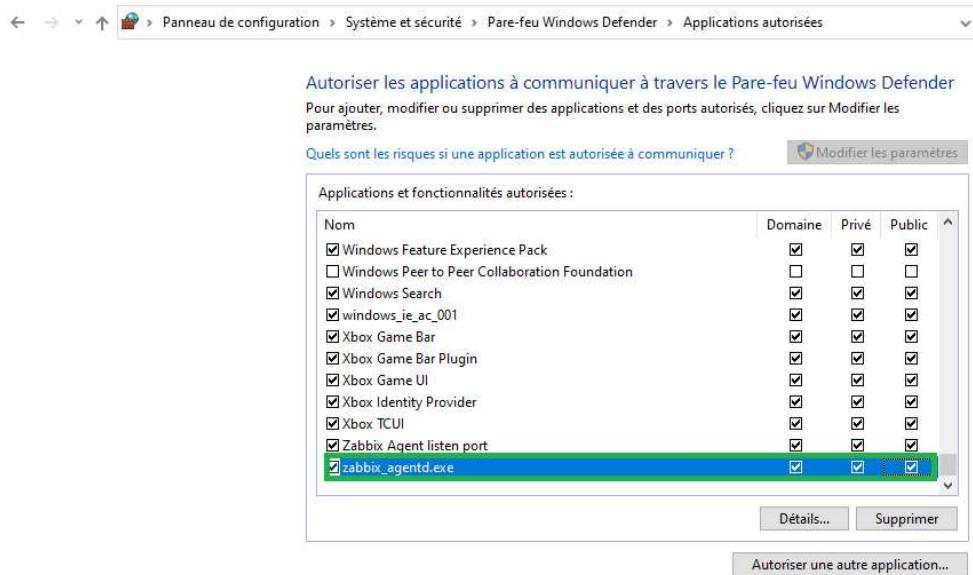
une application ou une fonctionnalité via le Pare-feu Windows. Ensuite cliquez sur « Autoriser une autre application » :



Cliquez sur parcourir et choisissez l'exe « zabbix_agentd » dans le dossier zabbix :



On coche toute les cases :

 Applications autorisées

Panneau de configuration > Système et sécurité > Pare-feu Windows Defender > Applications autorisées

Autoriser les applications à communiquer à travers le Pare-feu Windows Defender
Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si une application est autorisée à communiquer ? [Modifier les paramètres](#)

Nom	Domaine	Privé	Public
<input checked="" type="checkbox"/> Windows Feature Experience Pack	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Windows Peer to Peer Collaboration Foundation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Windows Search	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> windows_ie_ac_001	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Xbox Game Bar	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Xbox Game Bar Plugin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Xbox Game UI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Xbox Identity Provider	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Xbox TCUI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Zabbix Agent listen port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> zabbix_agentd.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Détails... Supprimer

[Autoriser une autre application...](#)

On vérifie que le serveur zabbix a bien accès à l'agent :

```
fevre@SRV-SECIVSUPER:~$ sudo telnet 192.168.100.101 10050
[sudo] Mot de passe de fevre :
Trying 192.168.100.101...
Connected to 192.168.100.101.
Escape character is '^]'.
Connection closed by foreign host.
fevre@SRV-SECIVSUPER:~$
```

Maintenant, on ajoute l'Agent Zabbix de l'hôte Windows à superviser au Serveur Zabbix. On va dans supervision/hôtes puis on clique sur Crée un hôte :

Hôtes [Crée un hôte](#)

CLIENT-MUL

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord
CLIENT-MUL	CLIENT-MUL.SECIV.LAN:10050	ZBX	class: os target: windows	Activé	Dernières données 47	Problèmes	Graphiques 7	Tableaux de bord 2
SRV-SECIVAD01	192.168.100.40:10050	ZBX	class: os target: windows	Activé	Dernières données 129	1	Graphiques 13	Tableaux de bord 2
Zabbix server	127.0.0.1:10050	ZBX SNMP	class: os class: software target: linux	Activé	Dernières données 128	Problèmes	Graphiques 24	Tableaux de bord 4

On remplit comme sur la capture suivante :

Nouvel hôte

Hôte IPMI Tags Macros Inventaire ● Chiffrement Table de correspondance

* Nom de l'hôte	SRV-SECIVAD01				
Nom visible	SRV-SECIVAD01				
Modèles	Windows by Zabbix agent <input type="button" value="X"/> taper ici pour rechercher <input type="button" value="Sélectionner"/>				
* Groupes d'hôtes	Zabbix servers <input type="button" value="X"/> taper ici pour rechercher <input type="button" value="Sélectionner"/>				
Interfaces	Type adresse IP	Nom DNS	Connexion à	Port	Défaut
	Agent	192.168.100.40	IP	DNS	10050 <input type="radio"/> <input checked="" type="radio"/> Supprimer
Ajouter					
Description					
Ajouter Annuler					

Puis on clique sur ajouter. Le serveur est désormais supervisé et visible sur l'interface de supervision :

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord
CLIENT-MUL	CLIENT-MUL.SECIV.LAN:10050	ZBX	class: os target: windows	Activé	Dernières données 110	2	Graphiques 11	Tableaux de bord 2
SRV-SECIVAD01	192.168.100.40:10050	ZBX	class: os target: windows	Activé	Dernières données 129	1	Graphiques 13	Tableaux de bord 2
Zabbix serveur	127.0.0.1:10050	ZBX SNMP	class: os class: software target: linux ***	Activé	Dernières données 128	Problems	Graphiques 24	Tableaux de bord 4

Affichage de 3 sur 3 tro

Pour la partie linux, cela se passe en ligne de commande comme sur les captures suivantes :

1

Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
6.4	Alma Linux	11 (Bullseye)	Server, Frontend, Agent	---	---
6.2	CentOS	10 (Buster)	Proxy		
6.0 LTS	Debian	9 (Stretch)	Agent		
5.0 LTS	Oracle Linux		Agent 2		
4.0 LTS	Raspberry Pi OS		Java Gateway		
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

Detailed Notes C.4

2

Install and configure Zabbix for your platform

a. Install Zabbix repository

[Documentation](#)

```
# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
# dpkg -i zabbix-release_6.4-1+debian11_all.deb
# apt update
```

b. Install Zabbix agent

```
# apt install zabbix-agent
```

