

Projet Ripple

-

BTS SIO SISR

DOCUMENTATION TECHNIQUE & MODE D'EMPLOI



Sommaire

Documentation technique & mode d'emploi	3
Routeur & pare-feu – Pfsense.....	3
VPN RW – OpenVPN / Pfsense.....	28
Annuaire Active Directory redondé – Windows Server 2019.....	42
Messagerie – hMailServer & Thunderbird (Serveur & Client).....	61
Téléphonie – 3CX & Client softphone	75
Serveur WEB (Application eBrigade) – Ubuntu (LAMP).....	87
Serveur de monitoring – Zabbix.....	96

Documentation technique & mode d'emploi

Routeur & pare-feu – Pfsense

Environnement virtuel

Pour chaque routeur nous aurons besoin de 3 interfaces réseau : 1 WAN, 1 LAN, 1 DMZ, dans la mise en place finale une interface WAN sera ajoutée (avec 2 accès internet distincts)

Récapitulatif de l'état des deux routeurs :

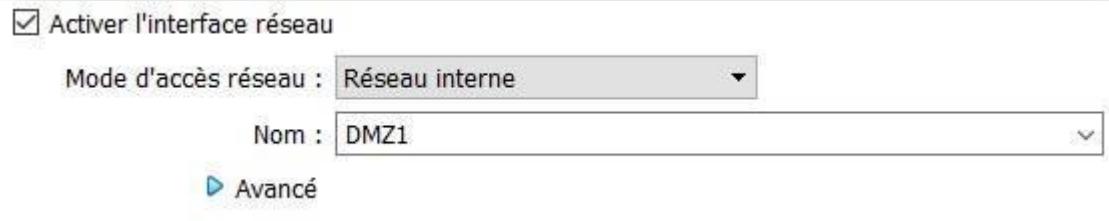
WAN :

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Activer l'interface réseau			
Mode d'accès réseau :	Accès par pont		
Nom :	Qualcomm Atheros QCA61x4A Wireless Network Adapter		
Avancé			

LAN :

<input checked="" type="checkbox"/> Activer l'interface réseau	
Mode d'accès réseau :	Réseau interne
Nom :	SECNET1
Avancé	

DMZ :



Configuration réseau final Routeur

1 :

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.139.57/24
LAN (lan)      -> em1      -> v4: 192.168.100.253/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.2/29
```

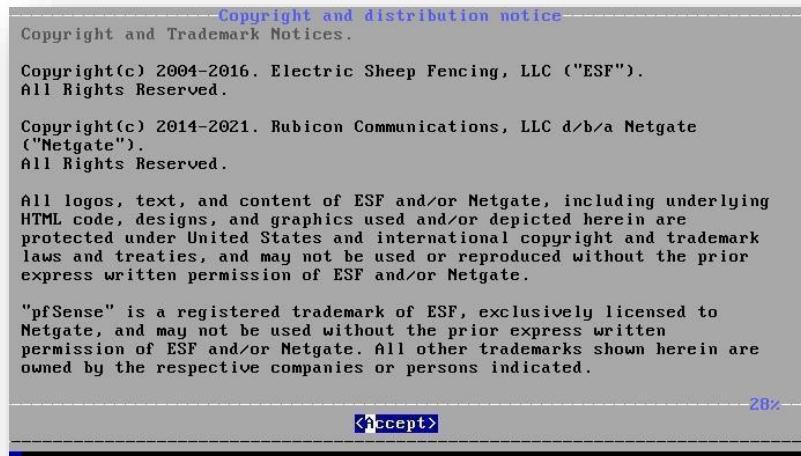
Routeur 2 :

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.139.128/24
LAN (lan)      -> em1      -> v4: 192.168.100.252/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.3/29
```

Installation pfSense

Après avoir installé l'ISO de Pfsense disponible [ici](#), nous pouvons monter nos VM et procéder à l'installation :

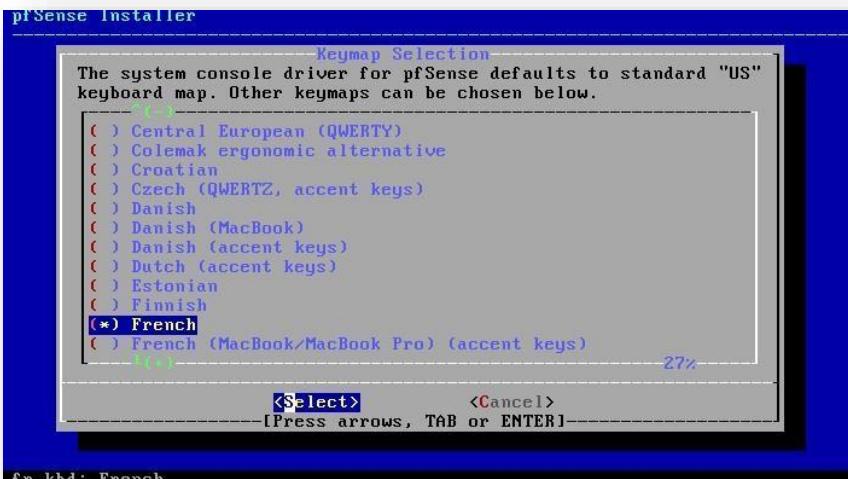
- Appuyez sur **entrer** pour accepter les termes



- Sélectionner « **Install** » puis appuyez sur **entrer**.



- Chercher le clavier « **French** » puis faites **entrer** pour valider le choix



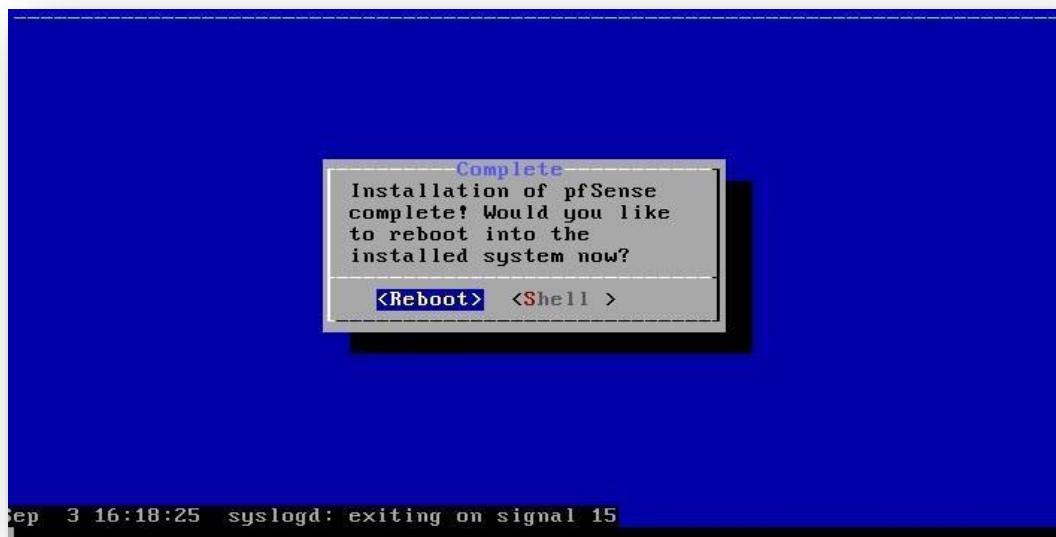
- Sélectionner « **Auto (UFS) BIOS** » puis appuyer sur **entrer**. (Installation / partitionnement du disque dur)



- Sélectionner « **No** » puis faites **entrer**



- Une fois l'installation achevée, ce message vous demandera de rebooter le système, faites **entrer**. Si le système reboot sur l'installateur, expulser l'iso de votre machine virtuelle.



- Initialisation du système et premier démarrage, il faut attendre que tout se mette en place.

```
.... done.  
Initializing..... done.  
Starting device manager (devd)...done.  
Loading configuration.....done.  
Updating configuration.....done.  
Checking config backups consistency...done.  
Setting up extended sysctls...done.  
Setting timezone...done.  
Configuring loopback interface...lo0: link state changed to UP  
done.  
Starting syslog...done.  
Starting Secure Shell Services...done.  
Setting up interfaces microcode...done.  
Starting PC/SC Smart Card Services...done.  
Configuring loopback interface...done.  
Creating wireless clone interfaces...done.  
Configuring LAGG interfaces...done.  
Configuring VLAN interfaces...done.  
Configuring QinQ interfaces...done.  
Configuring LAM interface...done.  
Configuring WAM interface...■
```

Le routeur finira par démarrer, vous arriverez sur cette page avec différents menus de configuration.

```

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.42.175/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

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

```

Nous allons passer à présent à la configuration de Pfsense.

Configuration

- Pour pouvoir assigner nos interfaces réseaux tapez 1. Puis assignez les interfaces comme ceci : em0 -> wan, em1 -> lan, em2 -> dmz

```

Enter an option: 1

Valid interfaces are:

em0      08:00:27:12:5b:9d  (up) Intel(R) PRO/1000 Network Connection
em1      08:00:27:b9:fc:84  (up) Intel(R) PRO/1000 Network Connection
em2      08:00:27:33:4d:17  (up) Intel(R) PRO/1000 Network Connection

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]? 

```

- Ensuite nous devrons configurer les cartes de nos routeurs. Pour réaliser cela, tapez 2 « **Set interface(s) IP address** ».

```

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

```

- Nous ne toucherons pas la carte WAN pour l'instant. Nous allons configurer la carte LAN.

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp)  
2 - LAN (em1 - static)
```

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

- Renseignez l'adresse IP du routeur souhaitée, puis faites entrer. Pour ce projet, nous avons mis **.253** et **.252** (se référer au schéma réseau)

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

- Tapez 24 (masque de sous-réseau) puis faites **entrer**

```
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 31):  
> 24
```

- Faites **entrer**

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

- Faites entrer

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

- Tapez « **y** » ou « **n** » puis faites entrer. (Activation ou non du DHCP pour le réseau local). Si vous activez le DHCP, vous devrez ensuite paramétrer la plage d'adresse IP.

```
Do you want to enable the DHCP server on LAN? (y/n) y  
Enter the start address of the IPv4 client address range: 192.168.100.10  
Enter the end address of the IPv4 client address range: 192.168.100.80 █
```

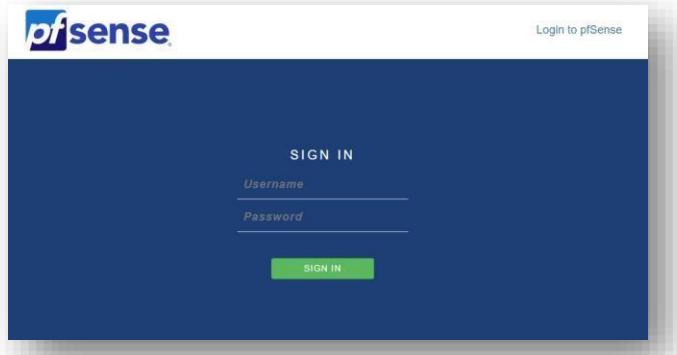
- Faites « **n** » pour la configuration du protocole web.

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

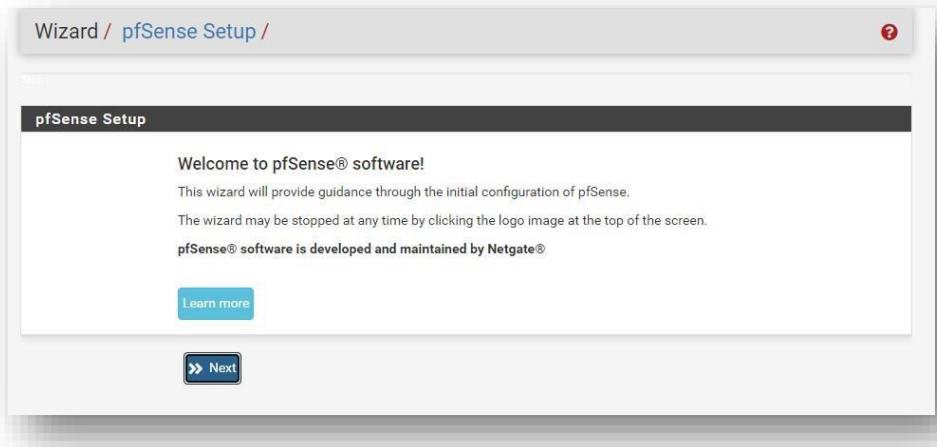
- Nous pouvons à présent accéder à la page web de configuration de PfSense en renseignant l'adresse IP ci-dessous (depuis une VM Windows 10 se trouvant dans le même réseau local (192.168.100.0/24)) :

```
The IPv4 LAN address has been set to 192.168.100.254/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
https://192.168.100.254/
```

- Poursuivons la configuration depuis l'interface web.
Login : admin
Password : pfsense



- Cliquez sur « **Next** » :



-

Renseignez ici un nom d'hôte, domaine, serveur dns... puis faites **next** :

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="pfSense"/>
EXAMPLE: myserver	
Domain	<input type="text" value="home.arpa"/>
EXAMPLE: mydomain.com	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

>> Next

- Indiquez la bonne Timezone

Time Server Information

Please enter the time, date and time zone.

Time server hostname	<input type="text" value="2.pfsense.pool.ntp.org"/>
Enter the hostname (FQDN) of the time server.	
Timezone	<input type="text" value="Europe/Paris"/>

- Laissez le WAN en DHCP

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

- Si besoin, la configuration d'IP fixe se fait un peu plus bas :

Static IP Configuration

IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="32"/>
Upstream Gateway	<input type="text"/>

- Désactivez les deux options situées ici, sinon le trafic entrant sur l'interface WAN sera bloquée, faites ensuite next. Nous mettrons en place d'autres règles afin de gérer ces flux :

RFC1918 Networks

Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

- Ici, nous n'avons rien à modifier, cette partie a déjà été configuré au début, cliquez sur **next** :

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.100.254
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	24

>> Next

- Modifier les identifiants par défaut du compte admin de pfsense :

Set Admin WebGUI Password

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

Admin Password
Admin Password AGAIN 

- Cliquez sur **reload** :

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

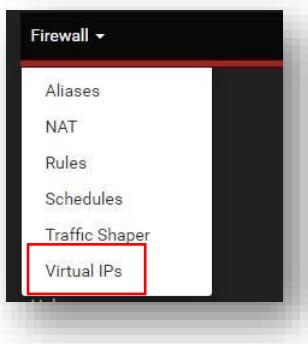
- L'installation et la configuration de Pfsense est terminée. **La même procédure doit être adoptée sur le second routeur en adaptant les paramètres réseaux.**

Configuration IP virtuelle / redondance (CARP – pfsync – XML RPC)

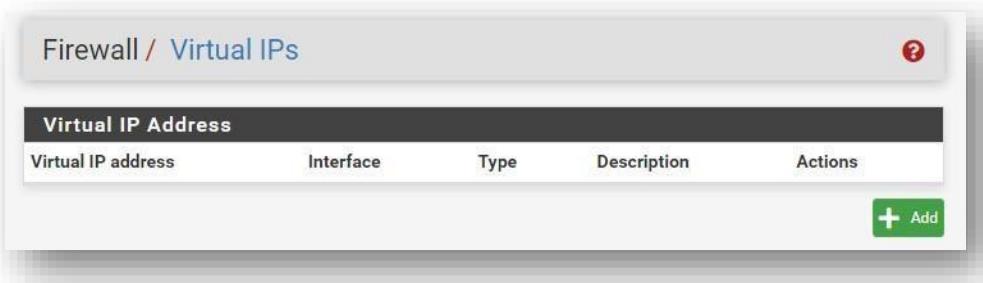
Etape 1 : Création d'une IP virtuelle commune aux deux routeurs (pour le LAN, la même configuration devra être effectuée pour les autres interfaces) (CARP) :

Sur le routeur principal **et** le secondaire :

- Dans Firewall, cliquez sur « **Virtual IPs** »



- Ajouter une IP virtuelle en cliquant sur « **+ Add** »



- Configuration de l'IP virtuelle, la configuration doit être identiques sur les deux routeurs.

Edit Virtual IP

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	192.168.100.254		/	24
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP		
Password	Enter the VHID group password.		Confirm	
VHID Group	1			
Enter the VHID group that the machines will share.				
Advertising frequency	1	Base	0	Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	IPV LAN			
A description may be entered here for administrative reference (not parsed).				

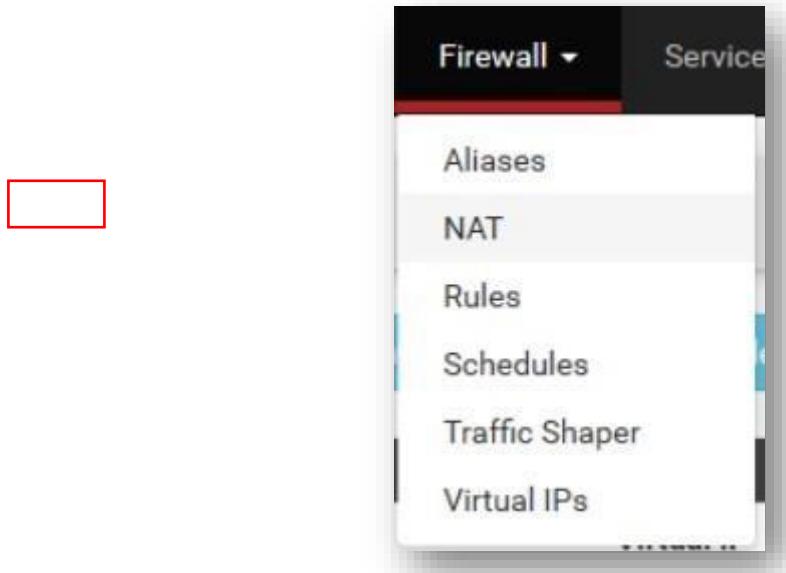
- Résultat :

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.100.254/24 (vhid: 1)	LAN	CARP	IPV LAN	

NB : Le « Skew » doit être plus élevé sur le routeur secondaire.

Forcer l'utilisation de l'IP virtuelle.

- Dans **Firewall**, allez dans **NAT**



- Rendez-vous dans **Outbound**, puis cliquez « **Hybrid Outbound NAT..** » puis faites « **SAVE** »

The screenshot shows a configuration interface for Outbound NAT. At the top, there are tabs: Port Forward, 1:1, Outbound (which is selected and highlighted in red), and NPt. Below the tabs, the title is "Outbound NAT Mode". There is a legend for "Mode":

Mode	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automatic outbound NAT rule generation. (IPsec passthrough included)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Disable Outbound NAT rule generation. (No Outbound NAT rules)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

- Cliquez sur « **Add** » pour créer une nouvelle règle.

Mappings										
	Source	Destination	NAT	NAT	Static					
Interface	Source Port	Destination Port	Address	Port	Port	Description	Actions			
							Add	Add	Delete	Save

- Dans « **Interface** », choisissez LAN. Dans « **Source** » indiquez le réseau local. Dans « **Translation** » > « **Address** » indiquez l'IPV LAN que nous avons créée précédemment.

Edit Advanced Outbound NAT Entry

Disabled	<input type="checkbox"/> Disable this rule				
Do not NAT	<input type="checkbox"/> 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	LAN				
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.					
Address Family	IPv4				
Select the Internet Protocol version this rule applies to.					
Protocol	any				
Choose which protocol this rule should match. In most cases "any" is specified.					
Source	Network	192.168.100.0	/	24	Port or Range
Type	Source network for the outbound NAT mapping.				
Destination	Any	/	24	Port or Range	
Type	Destination network for the outbound NAT mapping.				
<input type="checkbox"/> Not Invert the sense of the destination match.					

Translation

Address	192.168.100.254 (IPV LAN)
Connections matching this rule will be mapped to the specified Address . The Address can be an Interface, a Host-type Alias, or a Virtual IP address.	

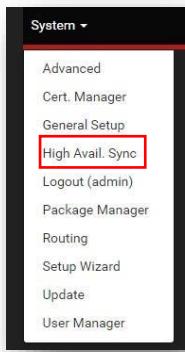
- Récapitulatif de la règle

Mappings								
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port
<input type="checkbox"/>	LAN	192.168.100.0/24	*	*	*	192.168.100.254	*	

- Faites la même chose pour les autres interfaces, en adaptant.

Etape 2 : Synchronisation des deux routeurs – Mise en place de la haute disponibilité (pfsync / XMLRPC)

Sur le routeur principal :



- Utilisez les mêmes paramètres que ci-dessous. Dans « **pfsync Synchronize Peer IP** », indiquez l'IP du routeur secondaire, ici 192.168.100.252. Puis adaptez le reste des paramètres comme ci-joint.

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PF SYNC 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	192.168.100.252 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize
Config to IP

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

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

Remote System Username

Enter the webConfigurator username of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Confirm

Enter the webConfigurator password of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin

synchronize admin accounts and autoupdate sync password.

By default, the admin account does not synchronize, and each node may have a different admin password.

This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

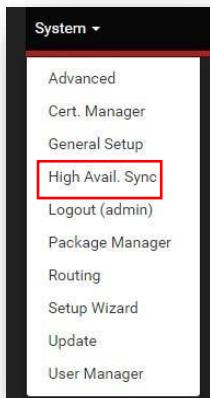
Select options to sync

- User manager users and groups
- 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
- 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**

Sur le routeur secondaire :



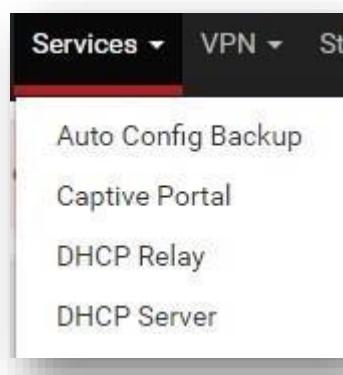
- Utilisez les mêmes paramètres que ci-dessous, dans « **pfsync Synchronize Peer IP** », indiquez l'IP du routeur principal ici 192.168.100.253.

State Synchronization Settings (pfsync)

Synchronize states	<input checked="" type="checkbox"/> 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	<input type="text" value="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	<input type="text" value="192.168.100.253"/> Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Paramètres DHCP – Pfsense (assigner l'IPV comme gateway par défaut)

- Cliquez sur « **DHCP Server** »



- Activez le DHCP pour l'interface LAN si cela n'est pas déjà fait
- Dans « **Other Options** », dans « **Gateway** », renseignez l'**IP VIRTUELLE** de l'interface LAN

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Tests de haute disponibilité

- Création de règles sur le routeur principal :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 /2.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 /9.37 MiB	IPv4 PFSYNC	LAN net	*	This Firewall	*	*	none		Autoriser PFSYNC	
<input type="checkbox"/>	0 /0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Autoriser XMLRPC	

- Ici on peut voir qu'elles ont bien été répliquées sur l'autre routeur

Firewall / Rules / LAN

Filtering WAN LAN IPsec

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 6 / 8.61 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ 1 / 165 KiB	IPv4 PFSYNC	LAN net	*	This Firewall	*	*	none		Autoriser PFSYNC	
✓ 0 / 0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Autoriser XMLRPC	

Test IP virtuelle

(IPV = 192.168.100.254/24

IP LAN RTE1 = 192.168.100.253/24

IP LAN RTE2 = 192.168.100.252/24)

- Sur une machine du réseau LAN, faites un **ipconfig /all**

Carte Ethernet Ethernet :

```

Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-2A-AB-E5
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::8882:b012:acba:5f33%6(préféré)
Adresse IPv4. . . . . : 192.168.100.10(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 1 avril 2022 09:36:02
Bail expirant. . . . . : vendredi 1 avril 2022 11:19:55
Passerelle par défaut. . . . . : 192.168.100.254
Serveur DHCP . . . . . : 192.168.100.253
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-29-44-EE-78-08-00-27-2A-AB-E5
Serveurs DNS. . . . . : 192.168.100.253
NetBIOS sur Tcpip. . . . . : Activé

```

C:\Users\Joe>

Nous pouvons voir que la passerelle est bien notre IP virtuelle et que le serveur DHCP fournissant une IP au client est le serveur principal.

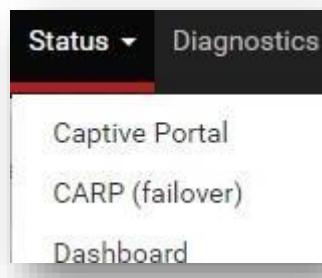
- Coupez le serveur principal puis faites un **ipconfig /release** puis **ipconfig /renew** puis refaites un **ipconfig /all**

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-2A-AB-E5
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::8882:b012:acba:5f33%6(préféré)
Adresse IPv4. . . . . : 192.168.100.10(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 1 avril 2022 09:40:26
Bail expirant. . . . . : vendredi 1 avril 2022 11:40:25
Passerelle par défaut. . . . . : 192.168.100.254
Serveur DHCP . . . . . : 192.168.100.252
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-29-44-EE-78-08-00-27-2A-AB-E5
Serveurs DNS. . . . . : 192.168.100.252
NetBIOS sur Tcpip. . . . . : Activé
```

On peut voir que le serveur secondaire a bien pris le relai.

Lorsque les deux routeurs tournent en même temps, l'un d'entre eux a le statut MASTER et le second le statut BACKUP. Le statut peut être consulté en cliquant sur **CARP (failover)**



Routeur principal :

CARP Interfaces		
CARP Interface	Virtual IP	Status
LAN@1	192.168.100.254/24	MASTER

Routeur secondaire :

CARP Interfaces		
CARP Interface	Virtual IP	Status
LAN@1	192.168.100.254/24	BACKUP

Récapitulatif des autres IPV

Pour les besoins du projet, d'autres IPV ont été créées, une pour notre DMZ et une autre pour notre interface WAN. Si les autres étapes ont été correctement suivies, vous n'aurez besoin de créer ces IPV que sur le routeur principal, elles seront ensuite répliquées sur le routeur secondaire automatiquement.

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.100.254/24 (vhid: 1)	LAN	CARP	IPV LAN	
192.168.242.100/24 (vhid: 2)	WAN	CARP	IPV WAN	
192.168.200.1/29 (vhid: 3)	DMZ	CARP	IPV DMZ	

Création des règles pare-feu

Récapitulatif des différentes règles mises en place sur nos routeurs.

Règles WAN :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0 / 0 B	IPv4 *	WAN net	*	DMZ net	*	*	none	WAN -> DMZ	
<input type="checkbox"/>		0 / 190 KiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN wizard	
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	*	*	DMZ address	80 (HTTP)	*	none	NAT	

Redirection du trafic WAN vers la DMZ

Règles LAN :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	6 /22.27 MiB	*	*	*	LAN Address 80	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 ICMP any	LAN net	*	*	*	*	none		Autoriser ping LAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 50 /268 KiB	IPv4 TCP/UDP	192.168.100.5	*	*	10050	*	none		Autorisation Zabbix	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 3 /367 KiB	IPv4 *	LAN net	*	DMZ net	*	*	none		Autorisation flux LAN -> DMZ	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Les deux dernières règles sont désactivées.

Autorisation LAN -> DMZ & Autorisation ICMP sur le lan & Autorisation Zabbix

Règles DMZ :

Floating	WAN	LAN	DMZ	OpenVPN							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /73 KiB	IPv4 *	DMZ net	*	LAN net	*	*	none		Blocage DMZ vers LAN	

Blocage des flux de la DMZ vers le LAN

VPN RW – OpenVPN / Pfsense

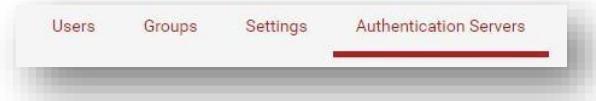
La configuration de notre VPN RW s'effectuera sur nos routeurs pfsense

Liaison LDAP :

- Dans « **System** », cliquez sur « **User Manager** »



- Puis allez dans « **Authentication Servers** » et cliquez sur « **+ Add** »



- Voici un aperçu de la liaison LDAP réalisée pour ce projet.

Users	Groups	Settings	Authentication Servers																		
<h3>Server Settings</h3> <table border="1"> <tr> <td><u>Descriptive name</u></td> <td>SECU-CIV.LAN</td> </tr> <tr> <td><u>Type</u></td> <td>LDAP</td> </tr> </table>				<u>Descriptive name</u>	SECU-CIV.LAN	<u>Type</u>	LDAP														
<u>Descriptive name</u>	SECU-CIV.LAN																				
<u>Type</u>	LDAP																				
<h3>LDAP Server Settings</h3> <table border="1"> <tr> <td><u>Hostname or IP address</u></td> <td>192.168.100.1</td> </tr> <tr> <td colspan="2">NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.</td> </tr> <tr> <td><u>Port value</u></td> <td>389</td> </tr> <tr> <td><u>Transport</u></td> <td>Standard TCP</td> </tr> <tr> <td><u>Peer Certificate Authority</u></td> <td>Global Root CA List</td> </tr> <tr> <td colspan="2">This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.</td> </tr> <tr> <td><u>Protocol version</u></td> <td>3</td> </tr> <tr> <td><u>Server Timeout</u></td> <td>25</td> </tr> <tr> <td colspan="2">Timeout for LDAP operations (seconds)</td> </tr> </table>				<u>Hostname or IP address</u>	192.168.100.1	NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.		<u>Port value</u>	389	<u>Transport</u>	Standard TCP	<u>Peer Certificate Authority</u>	Global Root CA List	This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.		<u>Protocol version</u>	3	<u>Server Timeout</u>	25	Timeout for LDAP operations (seconds)	
<u>Hostname or IP address</u>	192.168.100.1																				
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.																					
<u>Port value</u>	389																				
<u>Transport</u>	Standard TCP																				
<u>Peer Certificate Authority</u>	Global Root CA List																				
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.																					
<u>Protocol version</u>	3																				
<u>Server Timeout</u>	25																				
Timeout for LDAP operations (seconds)																					
<h3>Search scope</h3> <table border="1"> <tr> <td><u>Search scope</u></td> <td>Level</td> </tr> <tr> <td colspan="2">Entire Subtree</td> </tr> <tr> <td colspan="2">Base DN</td> </tr> <tr> <td colspan="2">DC=SECU-CIV,DC=LAN</td> </tr> </table>				<u>Search scope</u>	Level	Entire Subtree		Base DN		DC=SECU-CIV,DC=LAN											
<u>Search scope</u>	Level																				
Entire Subtree																					
Base DN																					
DC=SECU-CIV,DC=LAN																					
<h3>Authentication containers</h3> <table border="1"> <tr> <td><u>CN=Users,DC=SECU-CIV,DC=LAN</u></td> <td>Select a container</td> </tr> <tr> <td colspan="2">Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers</td> </tr> </table>				<u>CN=Users,DC=SECU-CIV,DC=LAN</u>	Select a container	Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers															
<u>CN=Users,DC=SECU-CIV,DC=LAN</u>	Select a container																				
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers																					
<table border="1"> <tr> <td><u>Extended query</u></td> <td><input type="checkbox"/> Enable extended query</td> </tr> <tr> <td><u>Bind anonymous</u></td> <td><input type="checkbox"/> Use anonymous binds to resolve distinguished names</td> </tr> <tr> <td><u>Bind credentials</u></td> <td>Administrateur@SECU-CIV.LAN</td> </tr> <tr> <td><u>User naming attribute</u></td> <td>samAccountName</td> </tr> <tr> <td><u>Group naming attribute</u></td> <td>cn</td> </tr> <tr> <td><u>Group member attribute</u></td> <td>memberOf</td> </tr> </table>				<u>Extended query</u>	<input type="checkbox"/> Enable extended query	<u>Bind anonymous</u>	<input type="checkbox"/> Use anonymous binds to resolve distinguished names	<u>Bind credentials</u>	Administrateur@SECU-CIV.LAN	<u>User naming attribute</u>	samAccountName	<u>Group naming attribute</u>	cn	<u>Group member attribute</u>	memberOf						
<u>Extended query</u>	<input type="checkbox"/> Enable extended query																				
<u>Bind anonymous</u>	<input type="checkbox"/> Use anonymous binds to resolve distinguished names																				
<u>Bind credentials</u>	Administrateur@SECU-CIV.LAN																				
<u>User naming attribute</u>	samAccountName																				
<u>Group naming attribute</u>	cn																				
<u>Group member attribute</u>	memberOf																				
<h3>RFC 2307 Groups</h3> <table border="1"> <tr> <td><input type="checkbox"/> LDAP Server uses RFC 2307 style group membership</td> </tr> <tr> <td>RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).</td> </tr> </table>				<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership	RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).																
<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership																					
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).																					
<h3>Group Object Class</h3> <table border="1"> <tr> <td>posixGroup</td> </tr> <tr> <td>Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".</td> </tr> </table>				posixGroup	Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".																
posixGroup																					
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".																					
<h3>Shell Authentication Group DN</h3> <table border="1"> <tr> <td>If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com</td> </tr> </table>				If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com																	
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com																					
<h3>UTF8 Encode</h3> <table border="1"> <tr> <td><input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server.</td> </tr> <tr> <td>Required to support international characters, but may not be supported by every LDAP server.</td> </tr> </table>				<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server.	Required to support international characters, but may not be supported by every LDAP server.																
<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server.																					
Required to support international characters, but may not be supported by every LDAP server.																					
<h3>Username Alterations</h3> <table border="1"> <tr> <td><input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.</td> </tr> </table>				<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.																	
<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.																					
<h3>Allow unauthenticated bind</h3> <table border="1"> <tr> <td><input type="checkbox"/> Allow unauthenticated bind</td> </tr> <tr> <td>Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.</td> </tr> </table>				<input type="checkbox"/> Allow unauthenticated bind	Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.																
<input type="checkbox"/> Allow unauthenticated bind																					
Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.																					

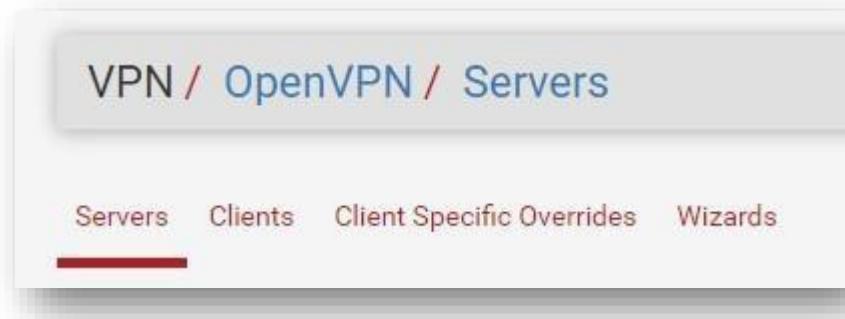
*Une fois la configuration achevée, cliquez sur « **Save** »*

Mise en place serveur VPN

- Rendez-vous dans « **VPN** » puis « **OpenVPN** »



- Cliquez sur « **Wizards** »



- Dans « **Type of Server** », choisissez « **LDAP** »



- Sélectionnez le serveur LDAP que nous avons configuré en première partie.

LDAP Authentication Server List

LDAP servers

SECU-CIV.LAN

>> Add new LDAP server

>> Next

- A présent nous allons configurer le CA. Suivez les paramètres comme ci-joint.

Create a New Certificate Authority (CA) Certificate

Descriptive name

openvpn

A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length

2048 bit

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime

3650

Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code

FR

Two-letter ISO country code (e.g. US, AU, CA)

State or Province

Alsace

Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City

Strasbourg

City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

- A présent, nous devons créer un certificat serveur

Create a New Server Certificate

Descriptive name	<input type="text" value="openvpn_cert"/>	A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length	<input type="text" value="2048 bit"/>	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	<input type="text" value="398"/>	Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Country Code	<input type="text" value="FR"/>	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	<input type="text" value="Alsace"/>	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	<input type="text" value="Strasbourg"/>	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

- Maintenant nous devons configurer les informations générales

General OpenVPN Server Information

Interface	<input type="text" value="WAN"/>	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="UDP on IPv4 only"/>	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="1194"/>	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	<input type="text" value="VPN SSL OpenVPN"/>	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

- Ici, indiquez le l'adresse du tunnel VPN et le réseau LAN qu'il doit atteindre.

Tunnel Network	<input type="text" value="192.168.230.0/24"/>	This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway	<input type="checkbox"/>	Force all client generated traffic through the tunnel.
Local Network	<input type="text" value="192.168.100.0/24"/>	This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

- Ici, vous avez la possibilité d'activer des règles par défaut pour OpenVPN. La configuration est à présent terminée !

Firewall Rule Configuration	
OpenVPN Remote Access Server Setup Wizard	
Firewall Rule Configuration	
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.	
Traffic from clients to server	
Firewall Rule	<input checked="" type="checkbox"/>
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.	
Traffic from clients through VPN	
OpenVPN rule	<input checked="" type="checkbox"/>
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.	

Les règles créées par défaut sont les suivantes :

Dans WAN :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4	*	*	WAN address	1194	*	none	OpenVPN VPN SSL
			UDP			(OpenVPN)				OpenVPN wizard

Dans OpenVPN :

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	*	*	*	*	*	none		OpenVPN VPN SSL OpenVPN wizard	

- Lorsque vous retournez dans « **Servers** » dans « **VPN** » > « **OpenVPN** » vous pouvez avoir un aperçu de votre serveur VPN (OpenVPN)

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.230.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		

- A présent nous allons installer l'outil nous permettant d'exporter la configuration vers un client distant. Dans « **System** » cliquez sur « **Package Manager** »



- Rendez-vous dans « **Available Packages** » puis cherchez le paquet « **openvpn-client-export** ». Installez-le.

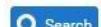
Installed Packages Available Packages

Search

Search term

openvpn

Both



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

Packages

Name	Version	Description
openvpn-client-export	1.6_4	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-2.5.2 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3



- Confirmez l'installation

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-openvpn-client-export

Confirm

- « **openvpn-client-export** » a bien été installé.

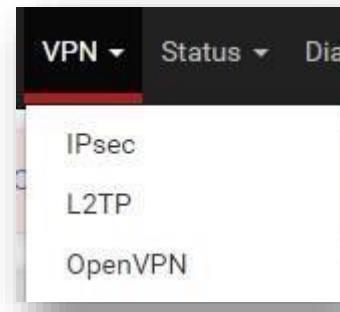
Installed Packages

Name	Category	Version	Description	Actions
openvpn-client-export	security	1.6_4	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-2.5.2 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3

- A présent rendons nous dans « **VPN** » puis « **OpenVPN** ». Ensuite, sélectionnez « **Client Export** »

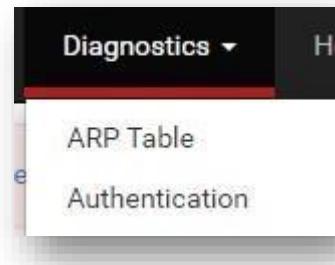


- Descendez jusqu'à « **OpenVPN Clients** » puis sélectionnez « **Archive** ». Récupérez le dossier qui devra être envoyé sur le pc distant

OpenVPN Clients		
User	Certificate Name	Export
Jean	openvpnuser	<ul style="list-style-type: none"> - Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.5.2-lx01): 64-bit 32-bit - Legacy Windows Installers (2.4.11-lx01): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Vérification liaison LDAP

- Pour vérifier la liaison LDAP, rendez-vous dans « **Diagnostics** » puis « **Authentication** »



Dans « **Authentication Server** » sélectionnez votre domaine AD. Puis dans « **Username** » & « **Password** » renseignez les identifiants de l'un des utilisateurs du domaine. Si la liaison fonctionne un message le stipulant apparaîtra :

User Anakin authenticated successfully. This user is a member of groups:

Authentication Test

<u>Authentication Server</u>	SECU-CIV.LAN
Select the authentication server to test against.	
<u>Username</u>	Anakin
<u>Password</u>
Test	

- C'est bien l'un des utilisateurs de l'AD

Users	UnsUpdateProxy	Groupe de sec...
	Éditeurs de certificats	Groupe de séc...
	Groupe de réPLICATION dont le mot de ...	Groupe de séc...
	Groupe de réPLICATION dont le mot de ...	Groupe de séc...
	Invité	Utilisateur
	Invités du domaine	Groupe de séc...
	Ordinateurs du domaine	Groupe de séc...
	Propriétaires créateurs de la stratégie d...	Groupe de séc...
	Protected Users	Groupe de séc...
	Serveurs RAS et IAS	Groupe de séc...
	Utilisateurs DHCP	Groupe de séc...
	Utilisateurs du domaine	Groupe de séc...
	Anakin	Utilisateur

Déploiement OpenVPN Connect & Configuration

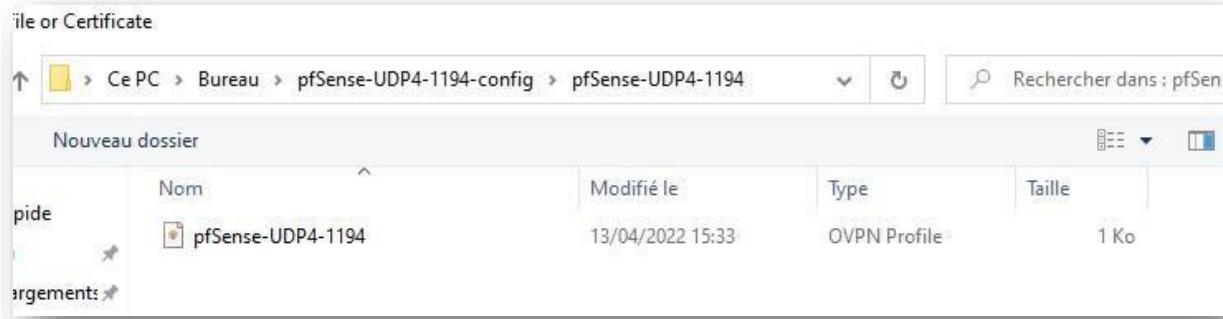
- OpenVPN Connect est téléchargeable en suivant [ce lien](#)

The screenshot shows a web browser window with the URL <https://openvpn.net/client-connect-vpn-for-windows/>. The page features the OpenVPN logo and the text "OFFICIAL OPENVPN CONNECT CLIENT PROGRAM". A large heading "OpenVPN Connect for Windows" is displayed. Below the heading, a text box states: "This is the official OpenVPN Connect client software for Windows workstation". To the right, a button labeled "Download OpenVPN Connect v3" is visible. The browser interface includes standard navigation and search bars at the top.

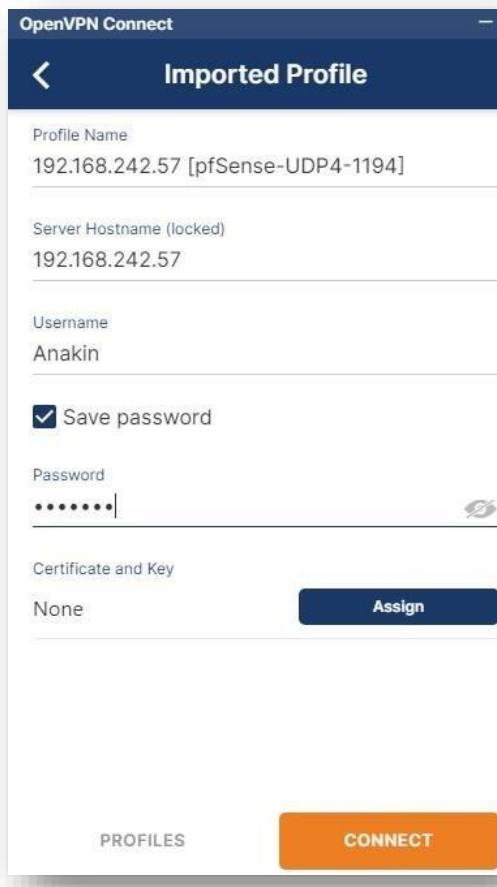
- Réalisez l'installation puis lancez le logiciel
- Rendez-vous dans « **File** », puis cliquez sur « **Browse** » nous allons importer la configuration que nous avons précédemment exportée.



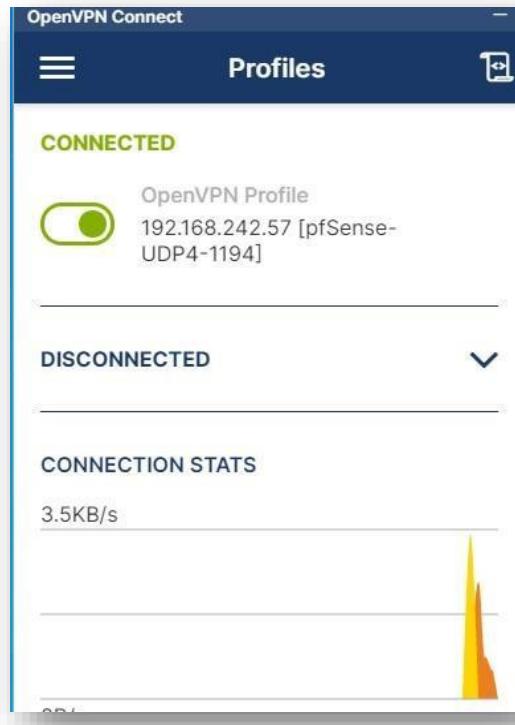
- Sélectionnez-le profile OpenVPN



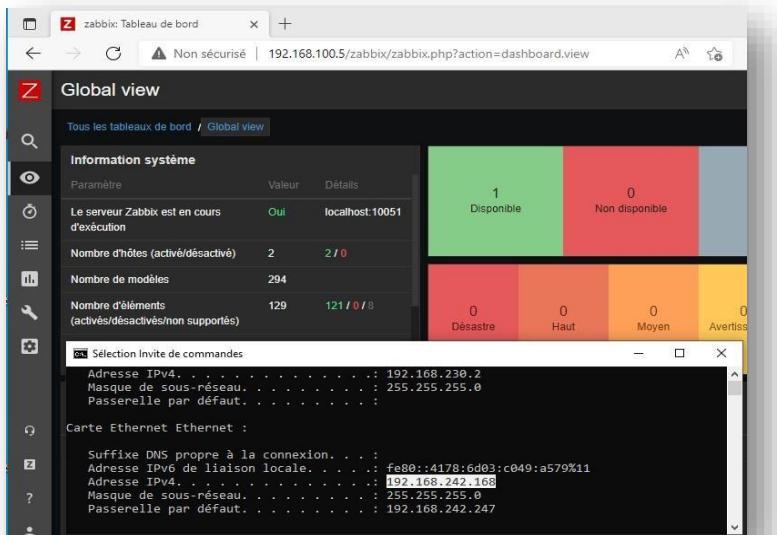
- Si la liaison LDAP a été effectuée, renseignez le nom de votre utilisateur dans l'AD ainsi que son mot de passe puis cliquez sur « **Connect** ».



- La connexion est effectuée :

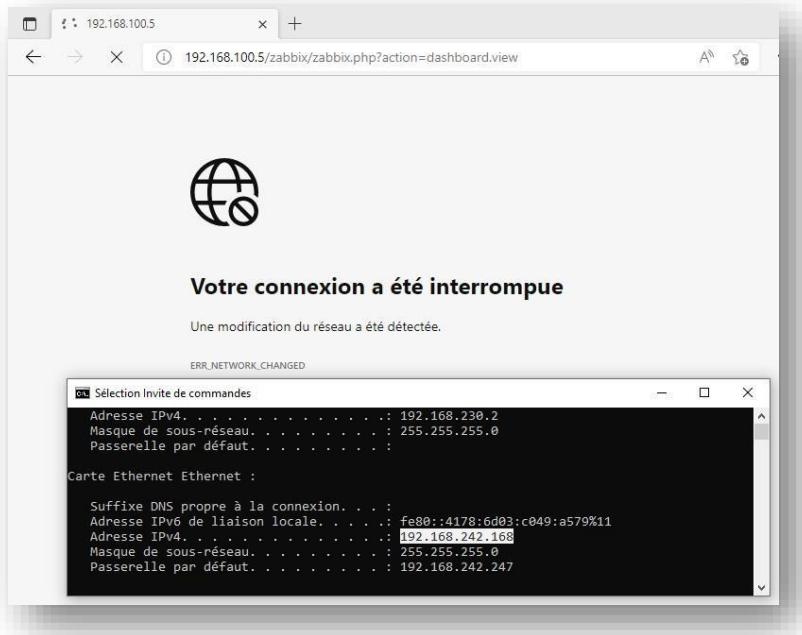


- Essayons d'accéder à l'interface web d'une de nos machines sur le LAN distant :



Nous y parvenons.

- Réessayons en coupant la liaison VPN



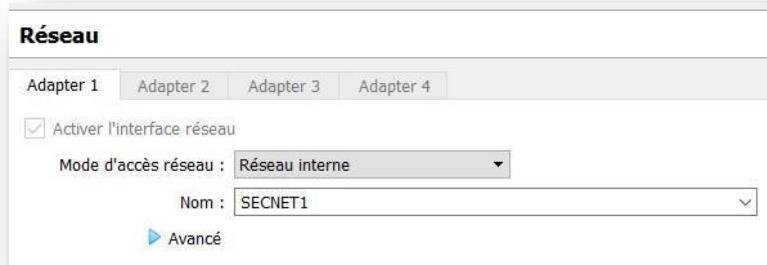
Ce n'est plus possible

Annuaire Active Directory redondé – Windows Server 2019

Certains noms de domaine/IP ont pu évoluer comparé à la documentation décrite ci-après
Environnement virtuel

2 VM Windows Server (1 Windows Server GUI / 1 Windows Server CORE) Interface

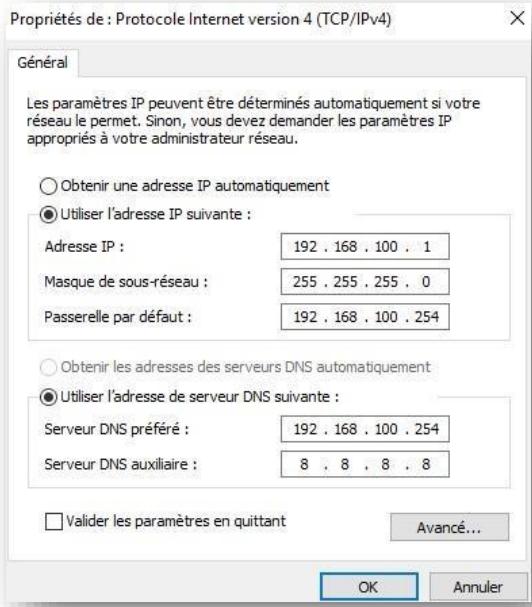
réseau :



Identique à l'interface LAN de nos routeurs

Configuration réseau final

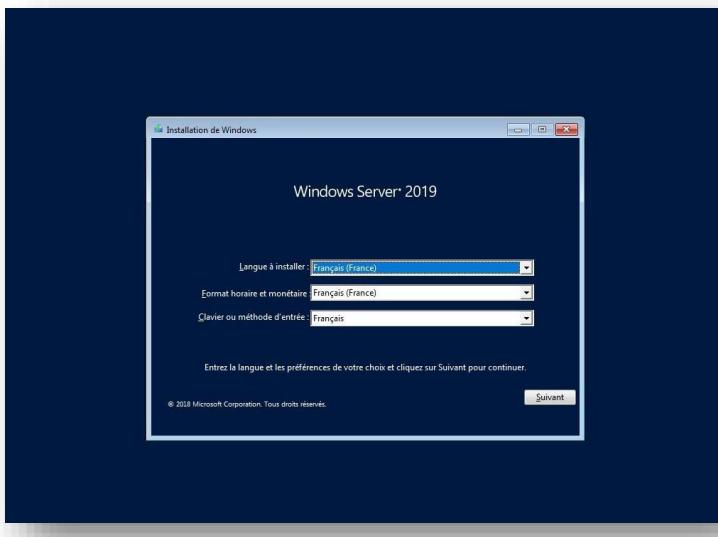
SRVW01 (.254/24 étant l'IPV de nos routeurs sur le LAN) :



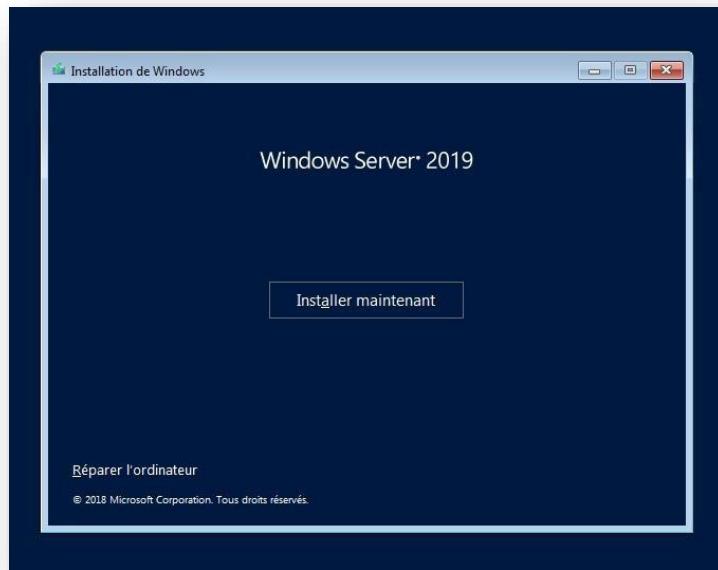
SRVW02. La configuration est similaire sur le serveur secondaire (.2/24) avec pour DNS 192.168.100.1 (SRV GUI)

Installation Windows Server 2019 (GUI & CORE)

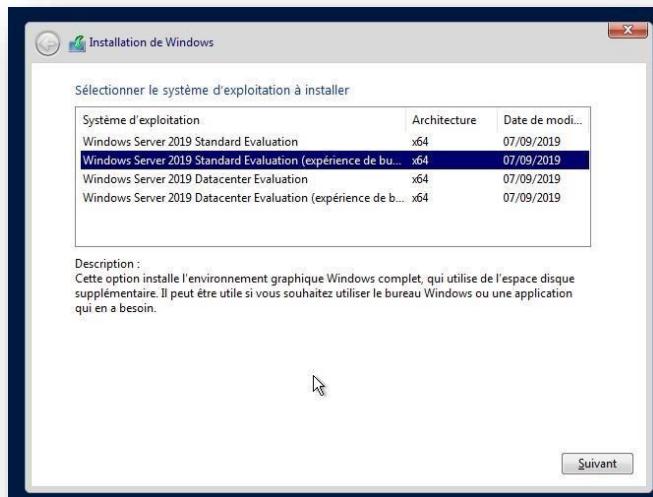
- Sélectionnez les bons réglages de langue puis cliquez sur suivant.



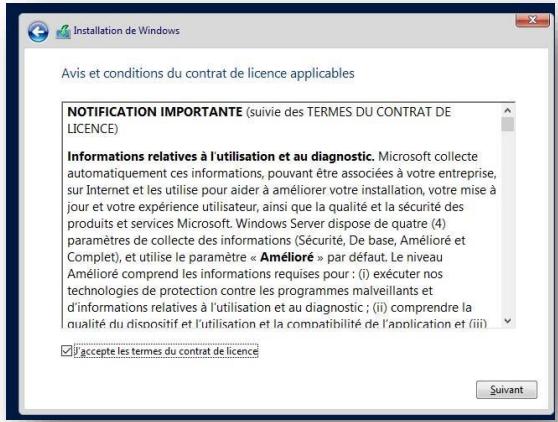
- Cliquez sur « **Installer maintenant** »



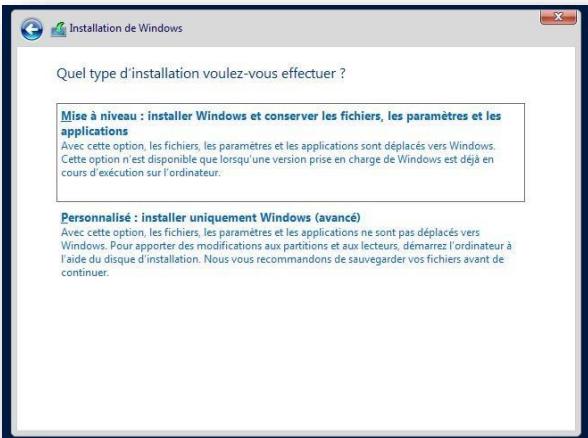
- Sélectionner « Windows Server 2019 Standard Evaluation (expérience du bureau) » pour le Windows Server avec interface graphique, et « Windows Server 2019 Standard Evaluation » pour le Windows Server sans interface graphique.



- Cliquez sur « j'accepte » puis « suivant »



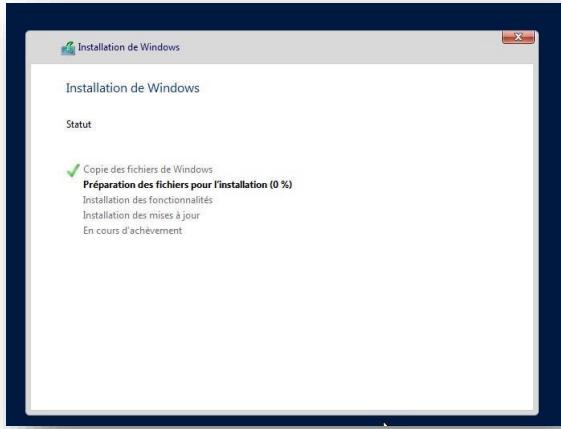
- Cliquez sur « Personnalisé : installer uniquement Windows (avancé) »



- Installer Windows sur la partition de base



- Attendez la fin de l'installation

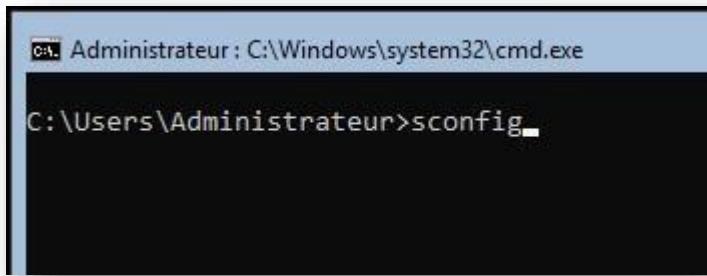


Ensuite, redémarrez le serveur. Vous devrez configurer un mot de passe pour le compte administrateur.

Vous pouvez dans un premier temps faire les mises à jour des deux serveurs.

Pour faire les mises à jour sur le server CORE :

- Tapez « **sconfig** » et faites entrer



- Entrez le nombre **6**, puis faites entrer

```
C:\ Administre: C:\Windows\system32\cmd.exe -sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. Tous droits réservés.

Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail : Groupe de travail: WORKGROUP
2) Nom d'ordinateur : WIN-LG2GSL8K04S
3) Ajouter l'administrateur local
4) Configurer l'administration à distance Activé
5) Paramètres de Windows Update : DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance : Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie Inconnu
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option :
```

- Tapez T pour rechercher les mises à jour.

```
Rechercher (T)outes les mises à jour ou uniquement les mises à jour (R)ecommandées ? T
Recherche de toutes les mises à jour applicables...
```

- Tapez T à nouveau.

```
Listes des éléments applicables sur l'ordinateur :
1> 2021-09 Préversion de la mise à jour cumulative pour .NET Framework 3.5, 4.7.2 et 4.8 pour Windows Server 20
ystèmes x64 (KB5005653)
2> Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1489.0)
3> 2021-09 Mise à jour cumulative pour Windows Server 2019 (1809) pour les systèmes x64 (KB5005568)

Sélectionnez une option :
(T)outes les mises à jour, aucu(N)e mise à jour ou (S)électionner une mise à jour unique ? T
```

Vous pouvez également changer le nom du serveur par la même occasion :

Renommer votre PC

Renommer votre PC

Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.

Nom actuel du PC : WIN-NQ6HDKBFD5M

STG-SRVW01



Suivant

Annuler

De même pour le serveur CORE :

- Depuis sconfig

```
Administrator : C:\Windows\system32\cmd.exe - sconfig

=====
Configuration du serveur
=====

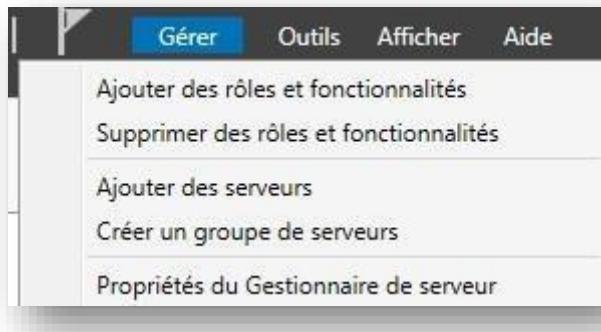
1) Domaine ou groupe de travail : Groupe de travail: WORKGROUP
2) Nom d'ordinateur : WIN-LG2GSL8K04S
3) Ajouter l'administrateur local
4) Configurer l'administration à distance Activé
5) Paramètres de Windows Update : DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance : Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie Inconnu
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 2

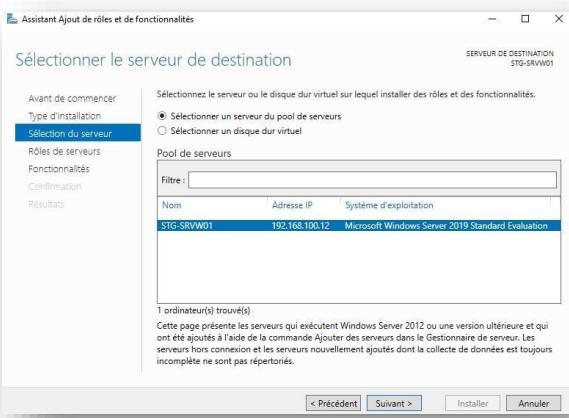
Nom de l'ordinateur
Entrer un nouveau nom d'ordinateur (Vide=Annuler) : STG-SRVW02
```

Installation / configuration ADDS / DNS (GUI)

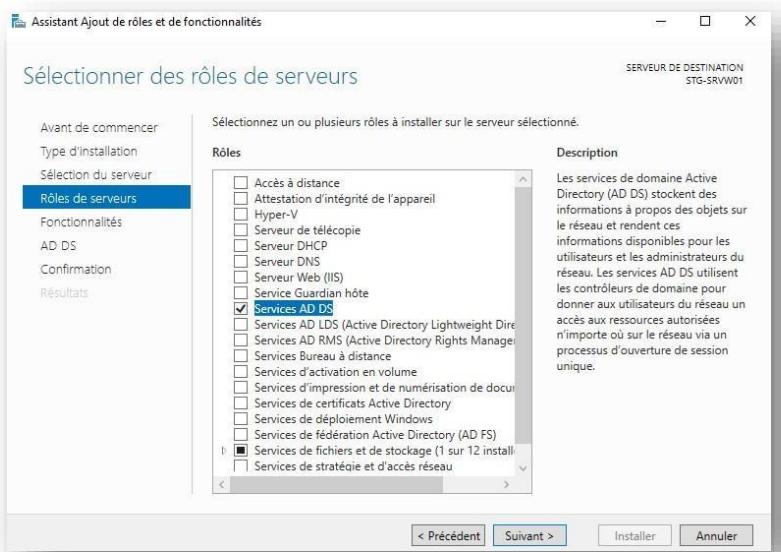
- Tout d'abord, renseignez une IP statique pour le serveur.
- Cliquez sur « Ajouter des rôles et fonctionnalités »



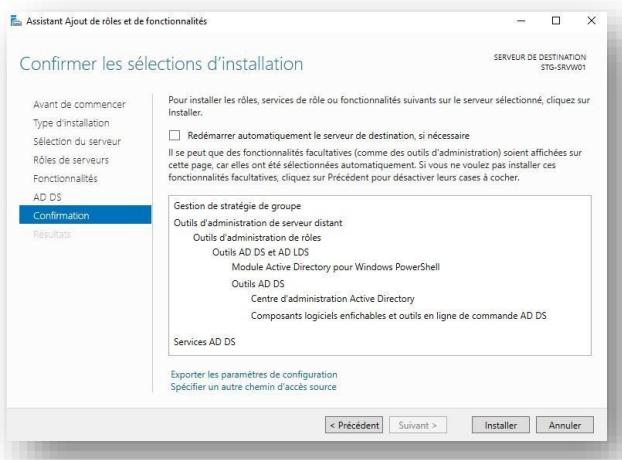
- Dans sélection du serveur, sélectionnez le serveur



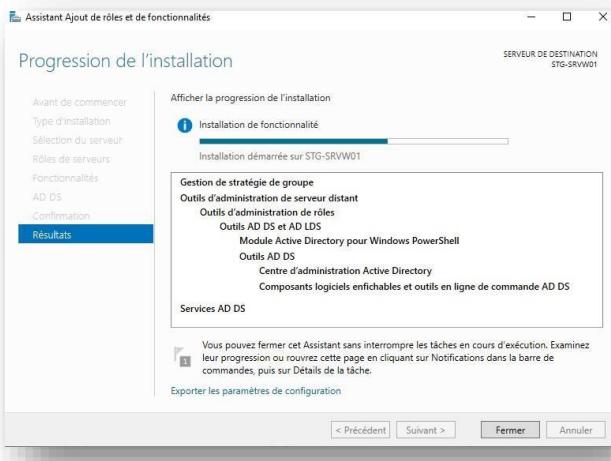
- Sélectionner le rôle AD DS



- **Cliquez sur « Installer »**

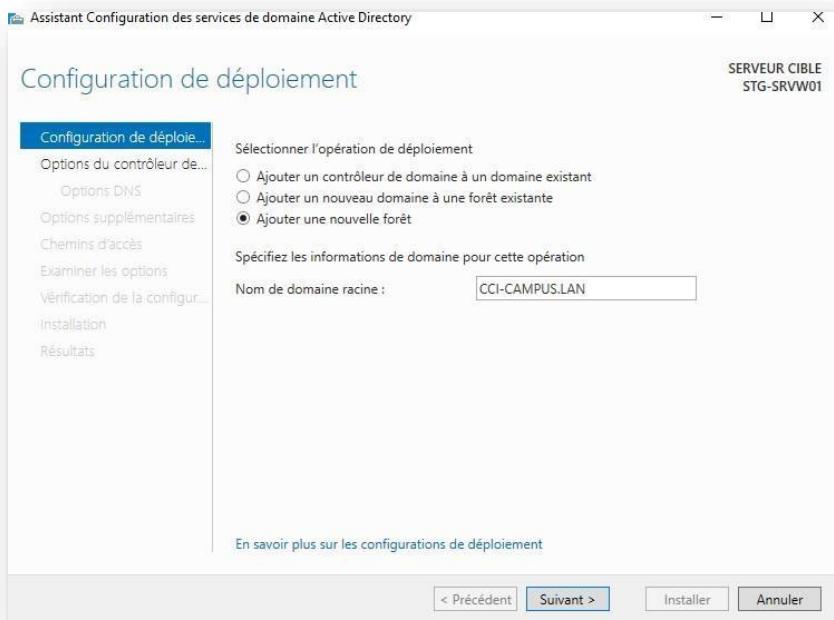


- **Attendez la fin de l'installation**

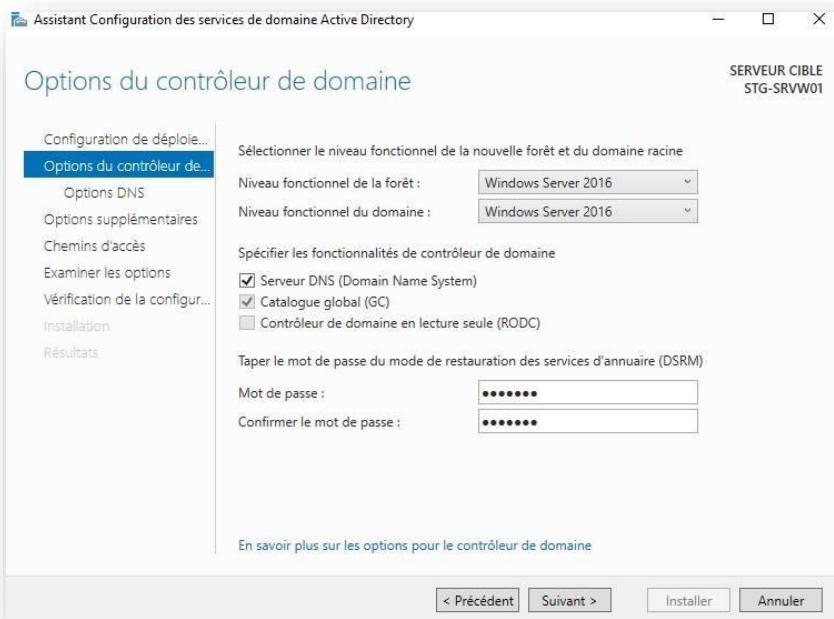


Nous pouvons à présent configurer l'AD :

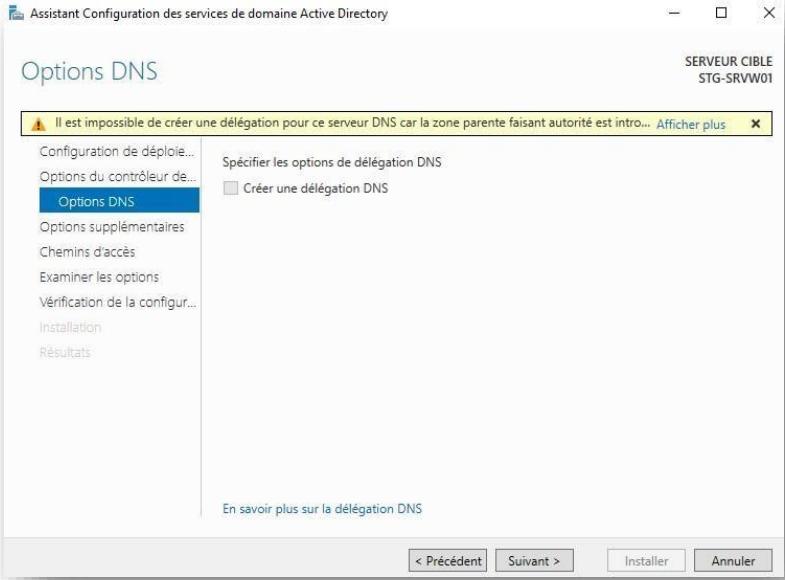
- « Ajouter une nouvelle forêt », puis renseigner un nom de domaine



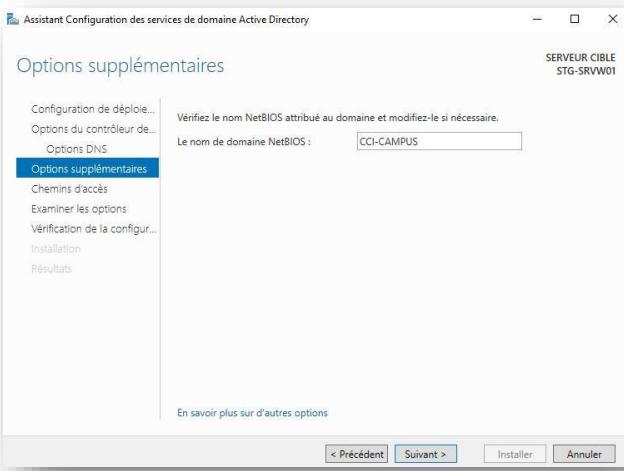
- Renseignez un mot de passe pour le mode de restauration des services d'annuaire



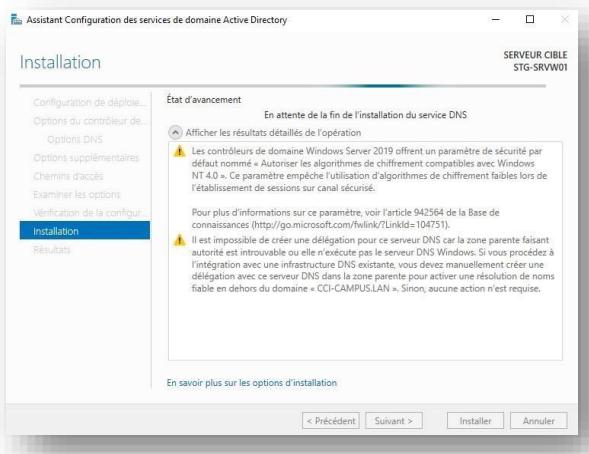
Cliquez sur « suivant »



- Laissez par défaut.



- Vous pouvez réaliser l'installation

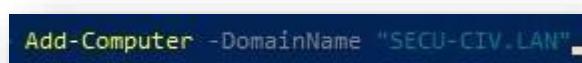


Installation / configuration ADDS / DNS (sur le serveur CORE) (+ Promotion contrôleur de domaine depuis un domaine existant)

- Dans un premier temps, modifier le serveur DNS préféré et renseignez l'IP du serveur principal (GUI), mettez également une IP statique pour le serveur. Cela se fait depuis sconfig



- Ajouter le serveur Core dans le domaine, vous devrez renseigner des crédenciales.



•

Rebootez le serveur :

```
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur STG-SRVW02.  
PS C:\Users\Administrateur> shutdown /r /t 0.
```

Serveur GUI

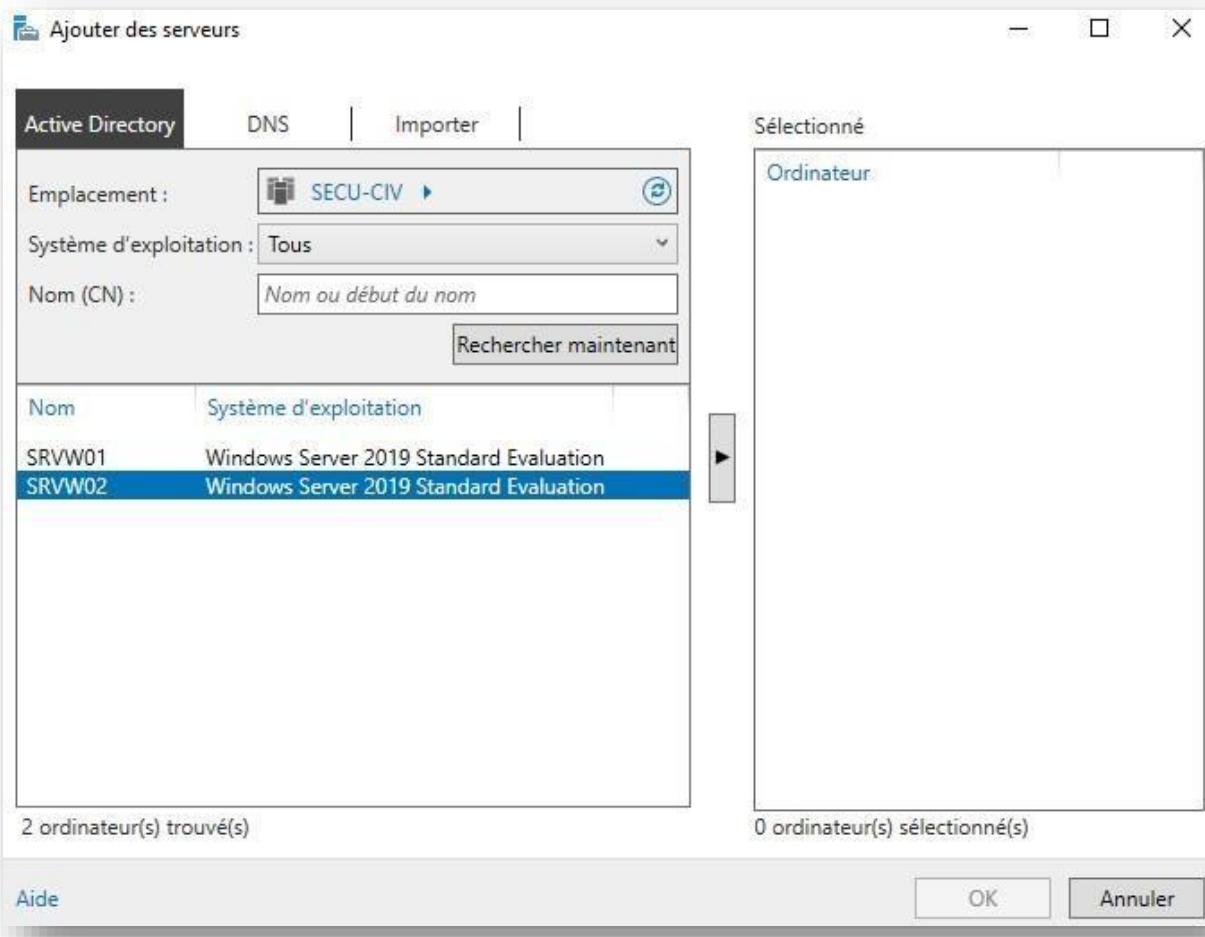
- Le serveur devrait apparaître dans le domaine, pour vérifier, regarder sur votre serveur principal (GUI)

Nom	Type
STG-SRVW02	Ordinateur

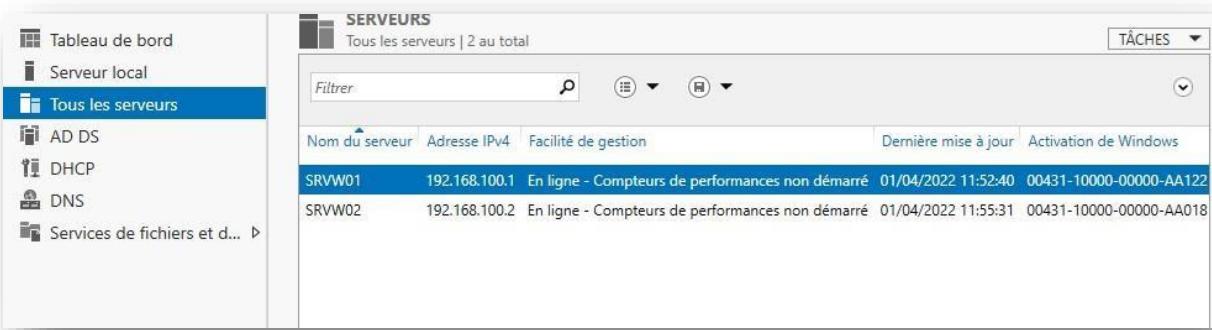
- Dans le gestionnaire de serveur, sur le tableau de bord, cliquez sur « **Ajouter d'autres serveurs à gérer** »



- Cliquez sur « Rechercher maintenant » puis sélectionnez le serveur Core « **SRVW02** » puis cliquez sur « **Ok** ».



- Le serveur apparaît à présent dans « **tous les serveurs** » :



A présent, installons l'AD/DNS et promouvons le serveur CORE en contrôleur de domaine (les manipulations se font depuis le serveur principal (GUI)) :

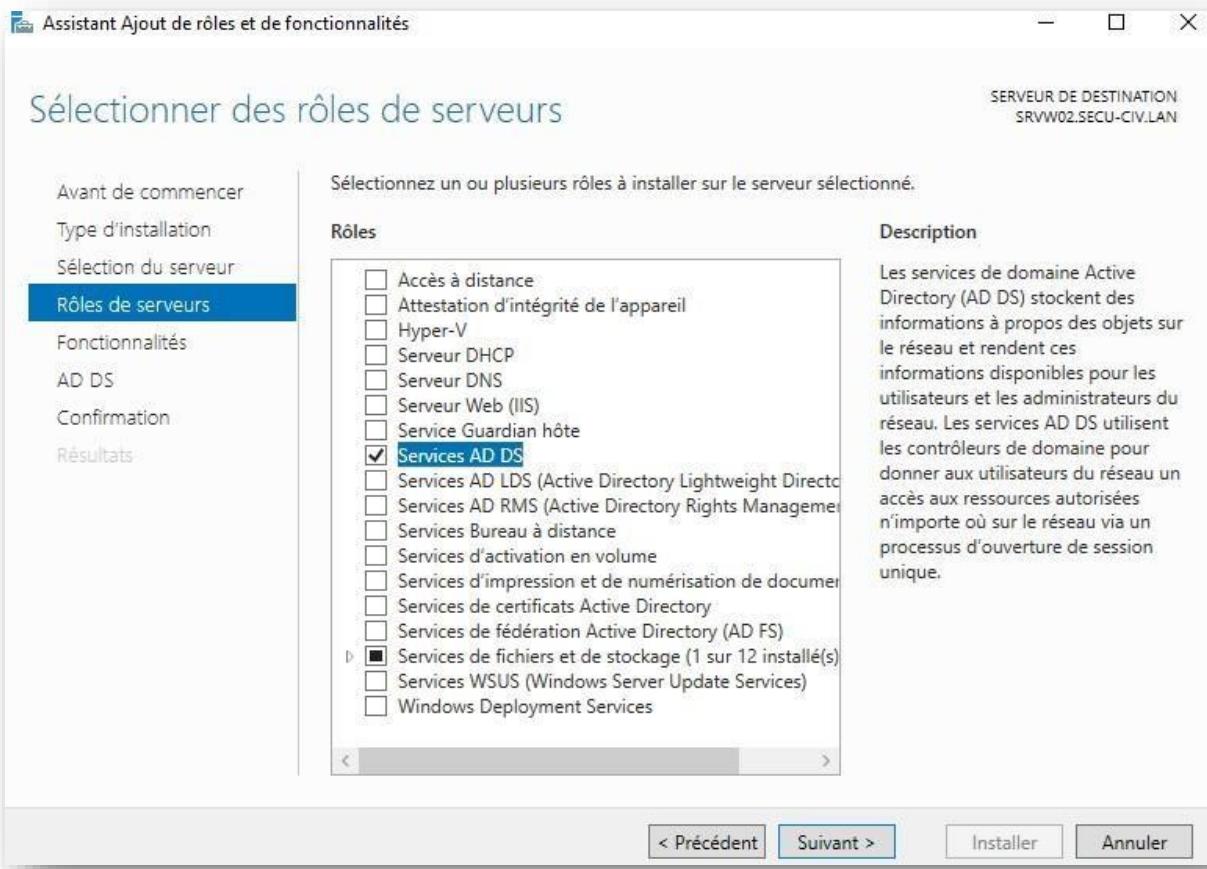
- Cliquez sur « Ajouter des rôles et des fonctionnalités »



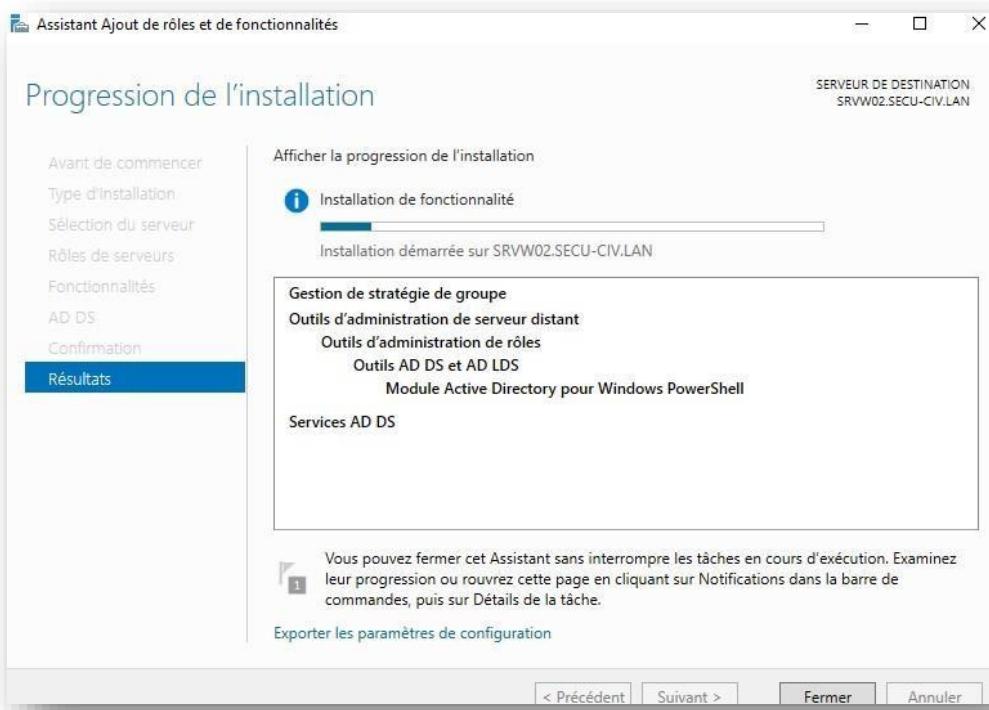
- Dans « Sélection du serveur », sélectionnez le serveur CORE :

The screenshot shows the 'Select destination server' dialog box. On the left, there's a sidebar with tabs: Avant de commencer, Type d'installation, Sélection du serveur (which is highlighted in blue), Rôles de serveurs, Fonctionnalités, Confirmation, and Résultats. The main area has a heading 'Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.' Below it, there are two radio buttons: 'Sélectionner un serveur du pool de serveurs' (selected) and 'Sélectionner un disque dur virtuel'. Underneath is a 'Pool de serveurs' section with a 'Filtre:' input field and a table. The table has columns: Nom, Adresse IP, and Système d'exploitation. It contains two rows: SRVW02.SECU-CIV.LAN (192.168.100.2, Microsoft Windows Server 2019 Standard Evaluation) and SRVW01.SECU-CIV.LAN (192.168.100.1, Microsoft Windows Server 2019 Standard Evaluation). The top right corner of the dialog box shows 'SERVEUR DE DESTINATION SRVW02.SECU-CIV.LAN'.

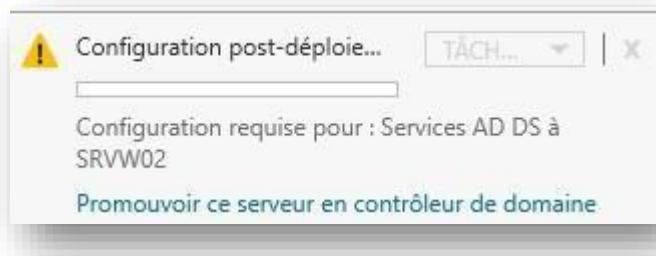
- Sélectionnez le rôle AD DS



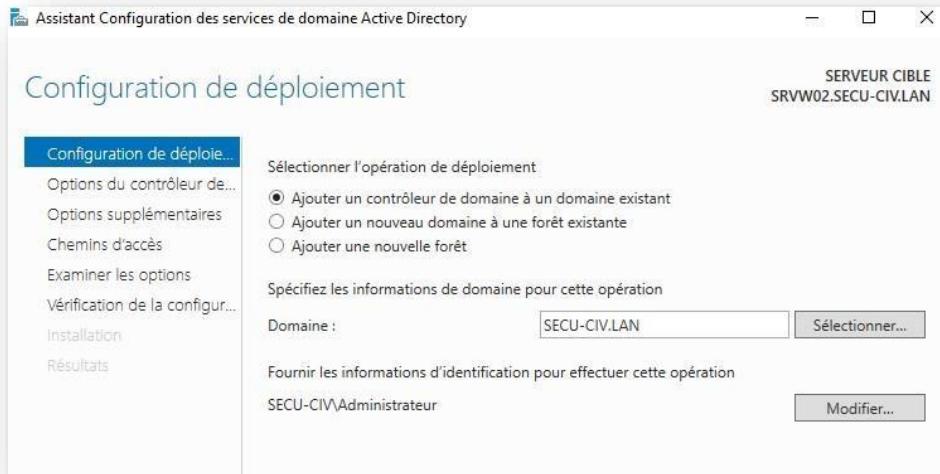
- Réalisez l'installation



- Une fois achevée, vous devez promouvoir le serveur en contrôleur de domaine.



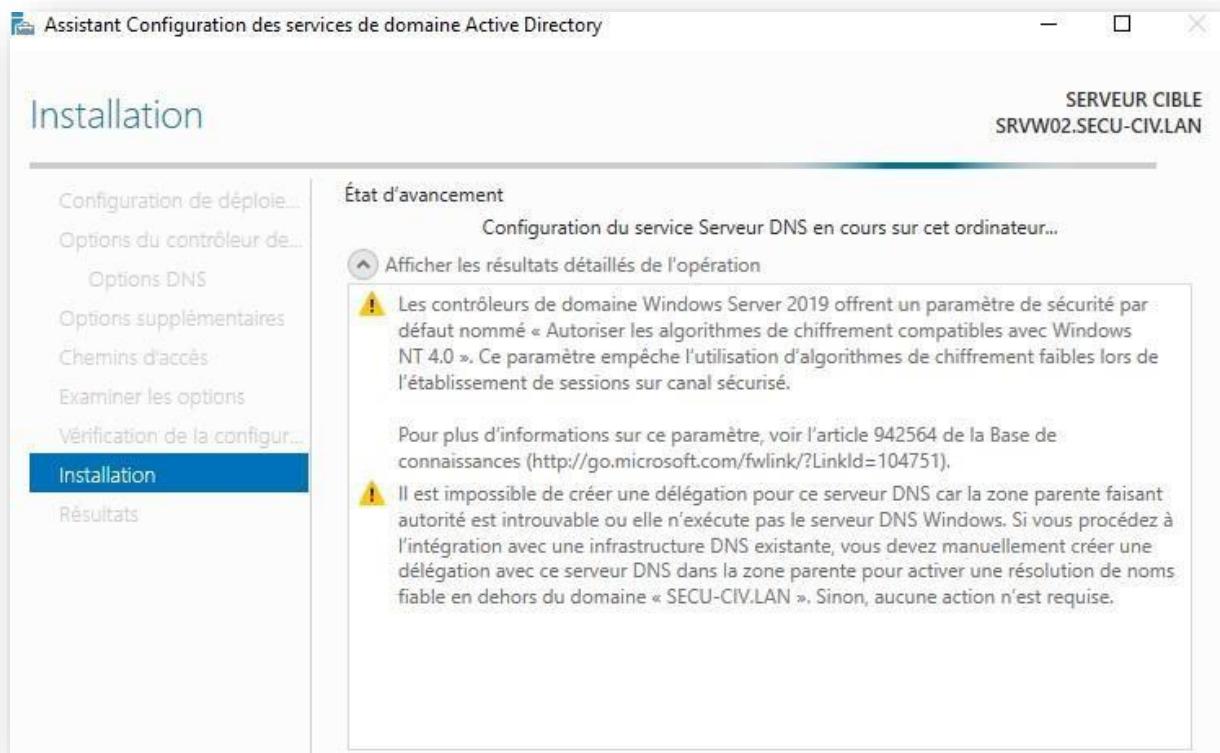
- Cliquez sur « Ajouter un contrôleur de domaine à un domaine existant », cliquez sur « Modifier » puis indiquez les credentials du compte administrateur du domaine :



- Faites suivant + renseignez les mots de passe demandés jusqu'à « **Options supplémentaires** ». Ici, cliquez sur « **Tout contrôleur de domaine** », et sélectionner le serveur principal (GUI)



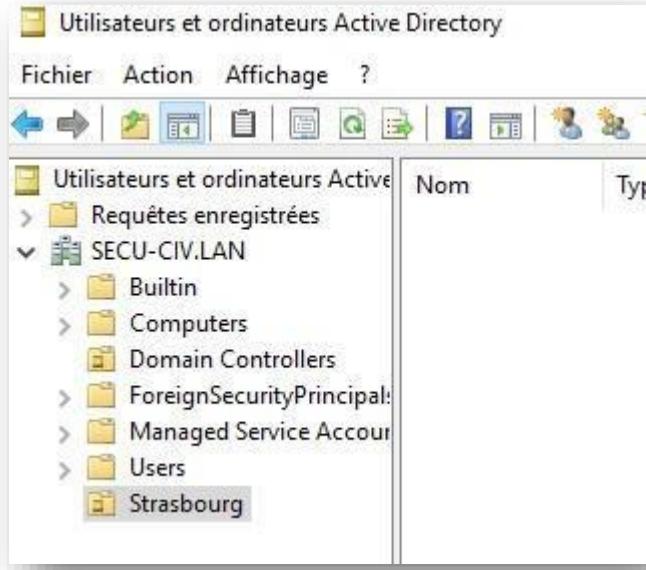
- Cliquez sur suivant jusqu'à « **Vérification de la configuration** » puis cliquez sur « **Installer** »



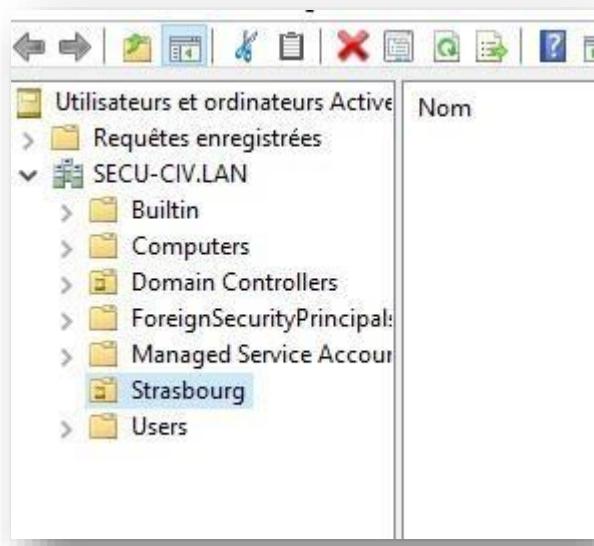
- Le serveur secondaire (CORE) est contrôleur de domaine, l'AD/DNS du serveur principal est redondé dessus.

Utilisateurs et ordinateurs Active Directory					
Fichier	Action	Affichage	?		
Utilisateurs et ordinateurs Active	SRVW01	Ordinateur	GC	Default-First-Si...	
Requêtes enregistrées	SRVW02	Ordinateur	GC	Default-First-Si...	
SECU-CIV.LAN					
Builtin					
Computers					
Domain Controllers					
ForeignSecurityPrincipal					
Managed Service Account					
Users					

- Créons une UO sur le serveur principal :



- Résultat sur le serveur secondaire :



Notre UO a bien été répliquée

Messagerie – hMailServer & Thunderbird (Serveur & Client)

Environnement virtuel hMailServer sera installé

sur le serveur SRVW01.

Installation

- Rendez-vous sur [ce site](#)
- Puis cliquez sur download :



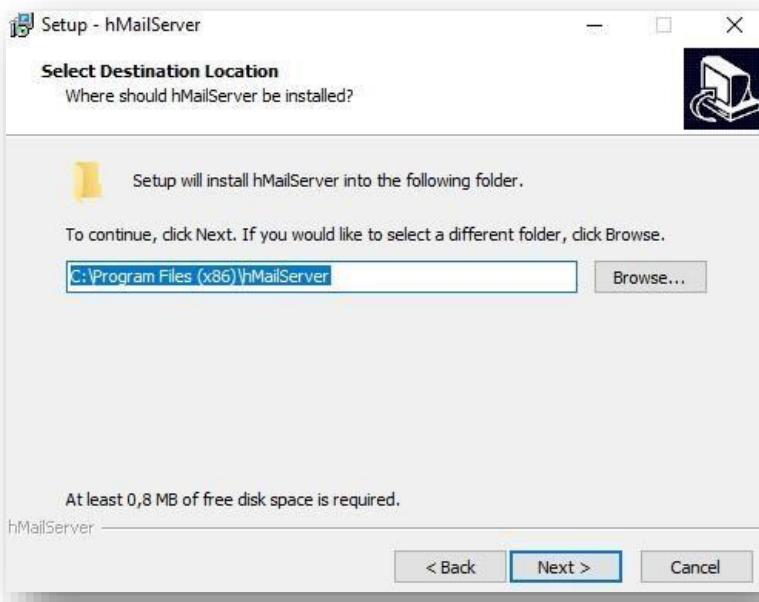
- Lancez ensuite le setup, ici cliquez sur « **Next** »



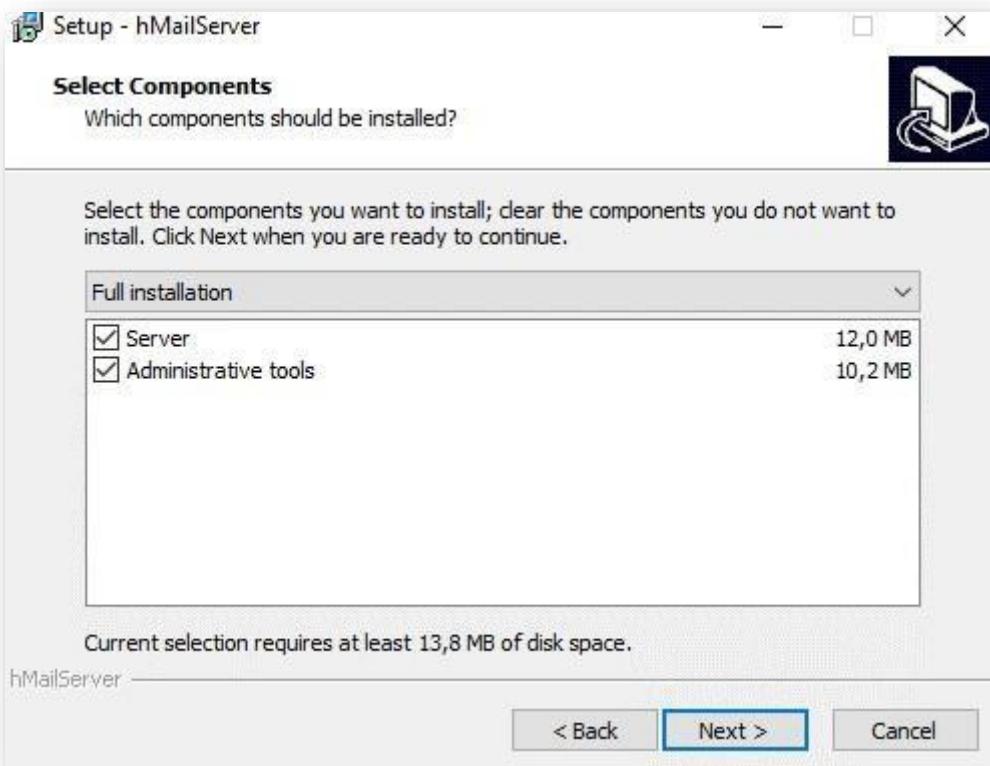
- Acceptez les termes



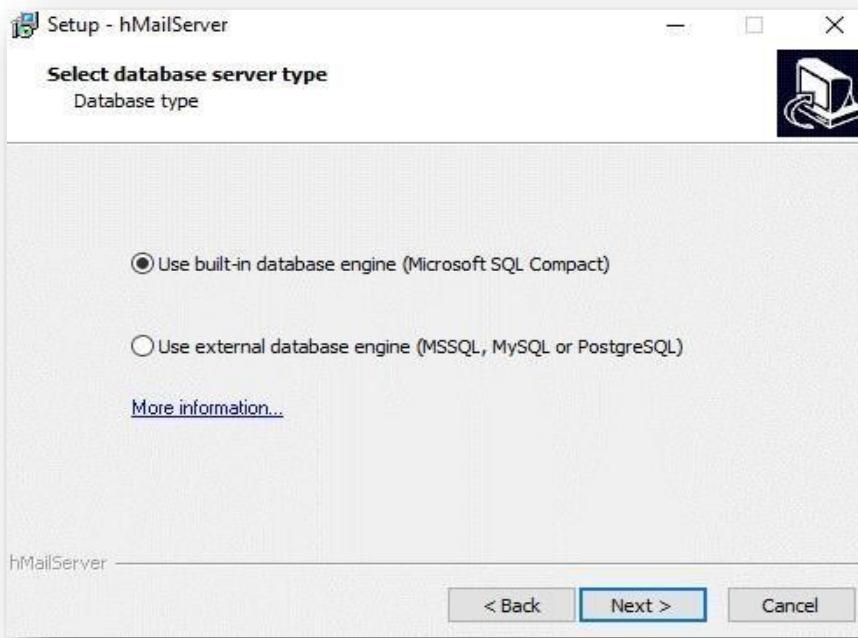
- Choisissez le dossier d'installation



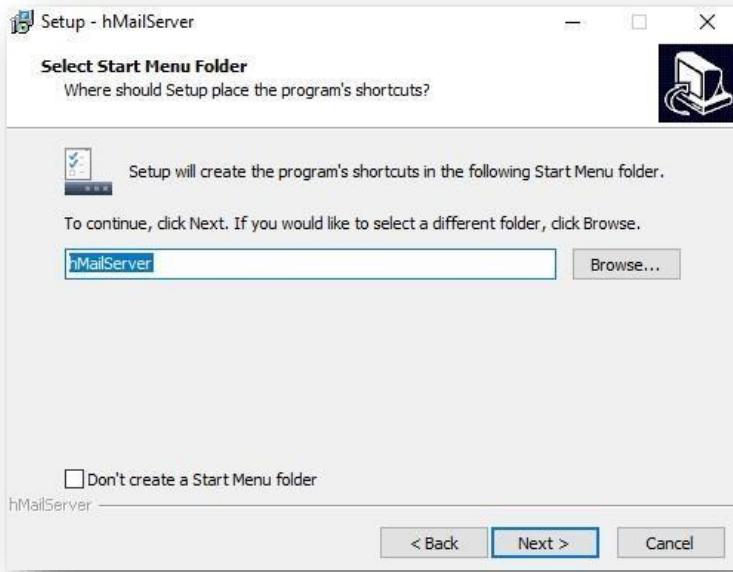
- Sélectionnez full installation avec « **Server** » et « **Administrative tools** » puis faites « **next** »



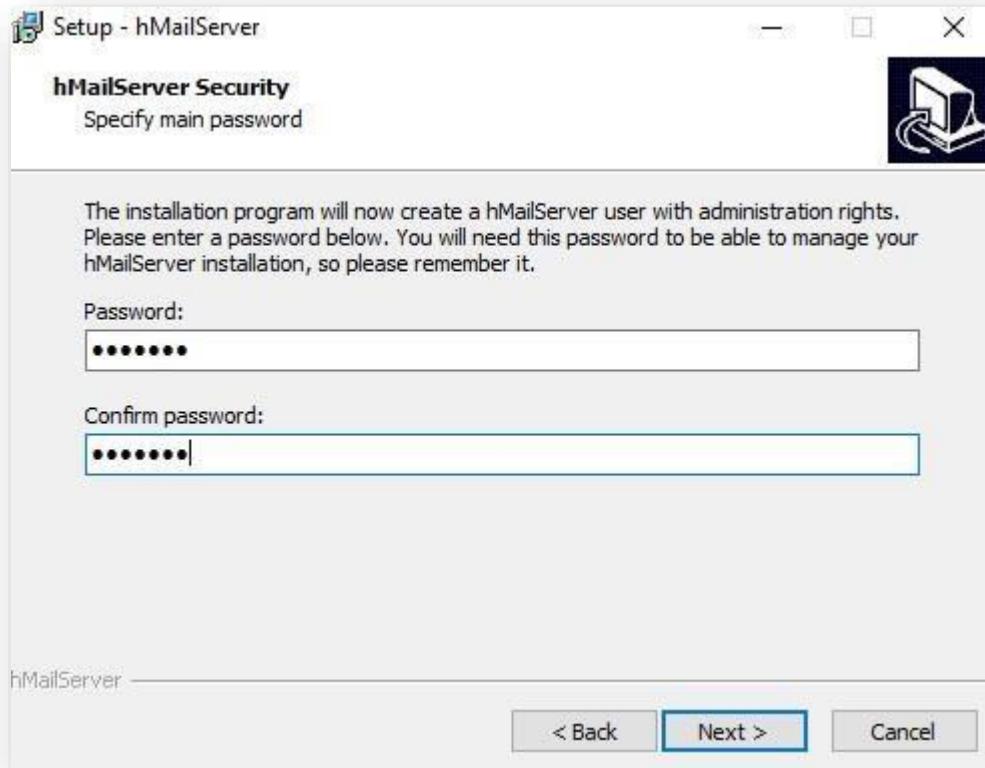
- Laissez l'option par défaut



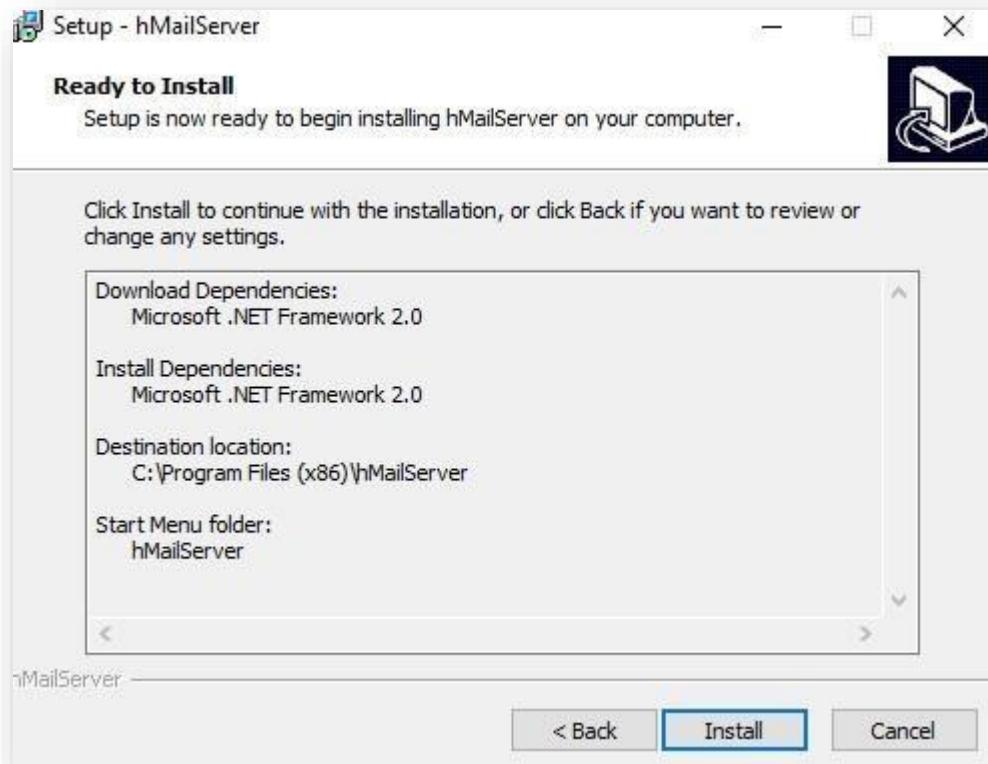
- Laissez par défaut



- Choisissez un mot de passe pour le compte administrateur hMailServer. Ce dernier est important, il ne faut pas l'oublier.



- Cliquez sur « **Install** »



- Une fois l'installation achevée, lancez hmailServer Administrator



L'installation est à présent achevée

Si l'installation ne s'effectue pas ou si des erreurs apparaissent pendant celle-ci, ajoutez la fonctionnalité net framework 3.5 sur le serveur.

Configuration

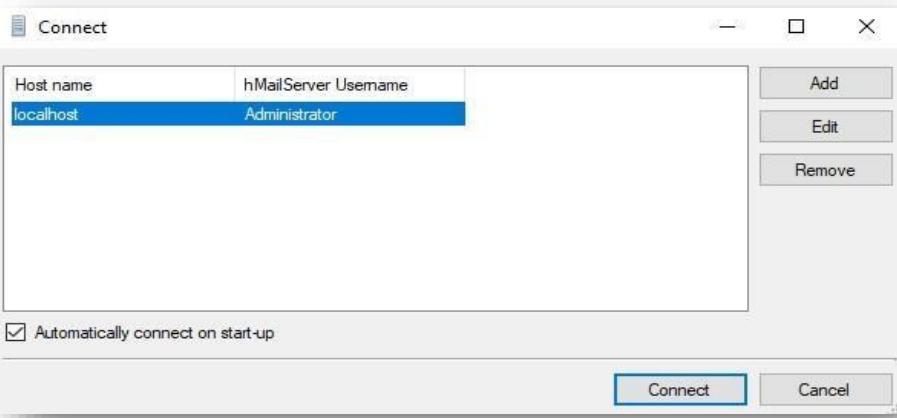
Configuration DNS Serveur

- Ajouter un enregistrement MX dans les paramètres DNS du serveur. Celui-ci permet de définir quel serveur gère les mails.

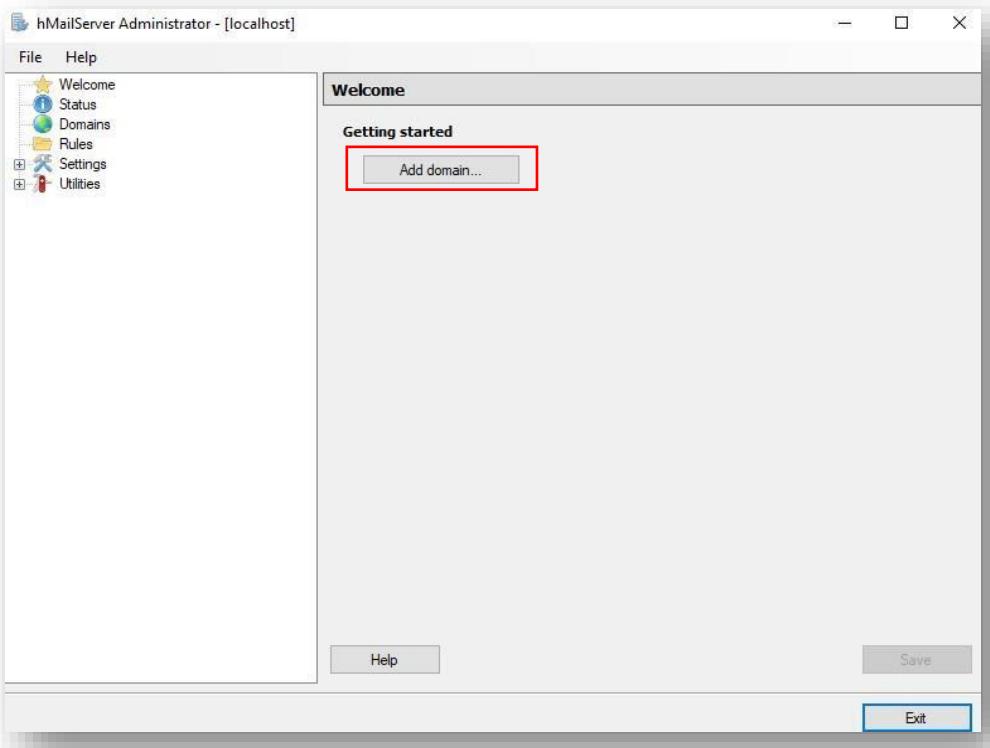
Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[112], srww01.secu-civ.lan....
(identique au dossier parent)	Serveur de noms (NS)	srww01.secu-civ.lan.
(identique au dossier parent)	Serveur de noms (NS)	srww02.secu-civ.lan.
(identique au dossier parent)	Hôte (A)	192.168.1.13
(identique au dossier parent)	Hôte (A)	192.168.100.1
(identique au dossier parent)	Hôte (A)	192.168.100.2
DESKTOP-0LQV59L	Hôte (A)	192.168.100.150
srww01	Hôte (A)	192.168.100.1
SRWW02	Hôte (A)	192.168.100.2
(identique au dossier parent)	Serveur de messagerie (...)	[10] srww01.SECU-CIV.LAN

Configuration hMailServer

- Après avoir lancé hMailServer Administrator, connectez-vous avec votre compte administrateur que vous avez créé pendant l'installation, en cliquant sur celui-ci puis en cliquant sur « **Connect** ». Vous pouvez également cliquer sur « **Automatically connect on start-up** ».



- Nous allons ajouter un domaine pour notre messagerie. Cliquez sur « **Add domain...** »



- Ensuite spécifiez un nom pour votre domaine, cliquez ensuite sur « **Enabled** » puis « **Save** » en bas à droite.

Domain
secu-civ.lan

Enabled

- Une fois le domaine créé d'autres paramètres doivent être configurés. Dans « **Settings** » puis « **Protocols** » puis « **SMTP** » puis « **Routes** », renseignez les paramètres suivants (en adaptant) puis enregistrez :

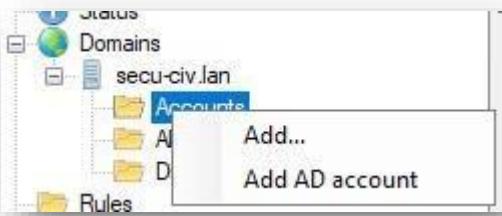
General	Addresses	Delivery
Domain secu-civ.lan		
Description		
Target SMTP host 192.168.100.1		
TCP/IP port 25		
Connection security None		

- Dans **Settings > Protocols > SMTP > Delivery of e-mail**, ajoutez l'hostname du serveur où hMailServer est lancé.

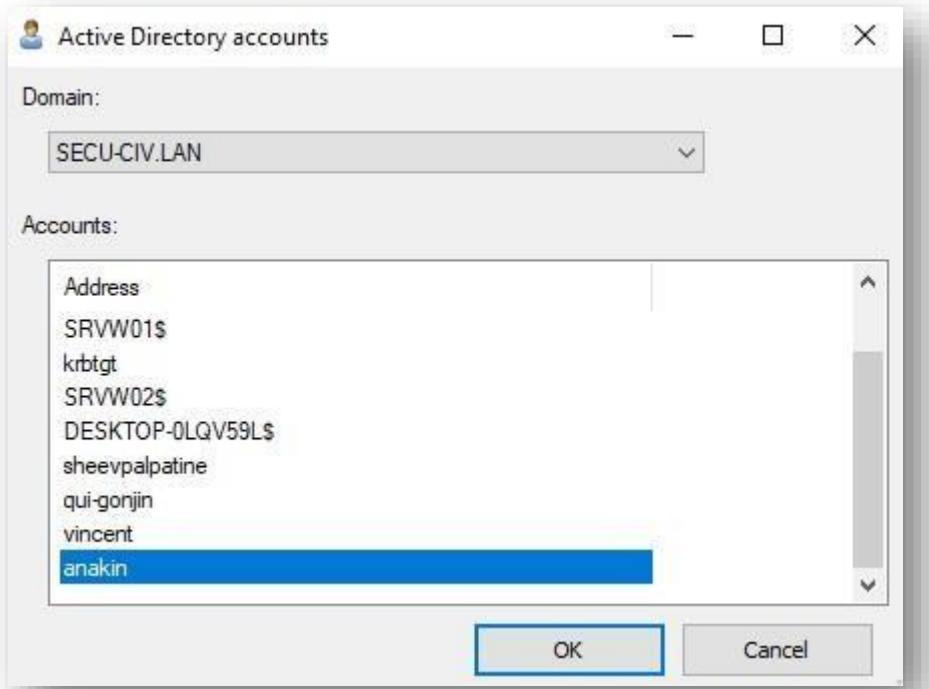
Delivery of e-mail	
Number of retries 4	Minutes between every retry 60
Local host name SRVW01	

Ajout d'un utilisateur de l'AD

- Toujours dans hMailServer Admin, dans le domaine que nous venons de créer. Faites un clic droit sur « **Accounts** » puis cliquez sur « **Add AD account** »



- Sélectionnez le domaine puis un utilisateur à ajouter

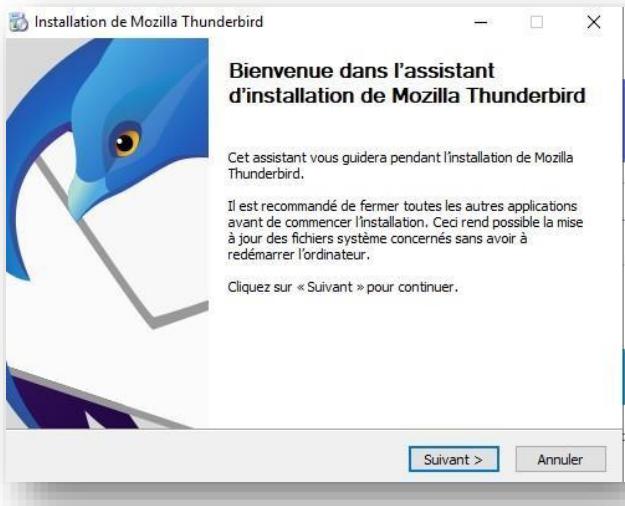


- L'utilisateur a été ajouté

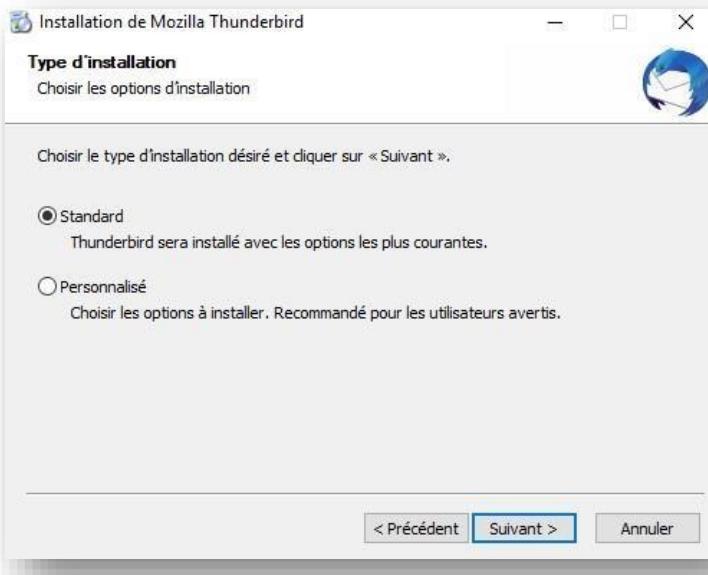
Accounts	
Name	Enabled
anakin@secu-civ.lan	Yes

Installation & configuration Thunderbird

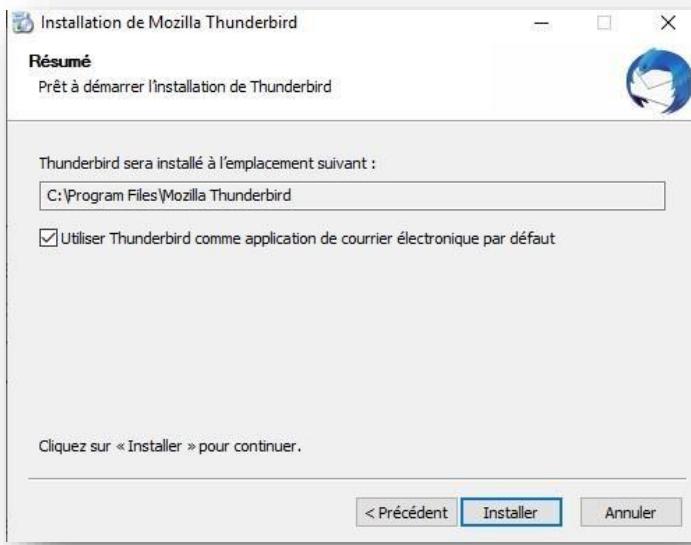
- Rendez-vous sur [ce site](#). Cliquez sur télécharger. Puis lancez l'installateur.
- Cliquez sur « suivant »



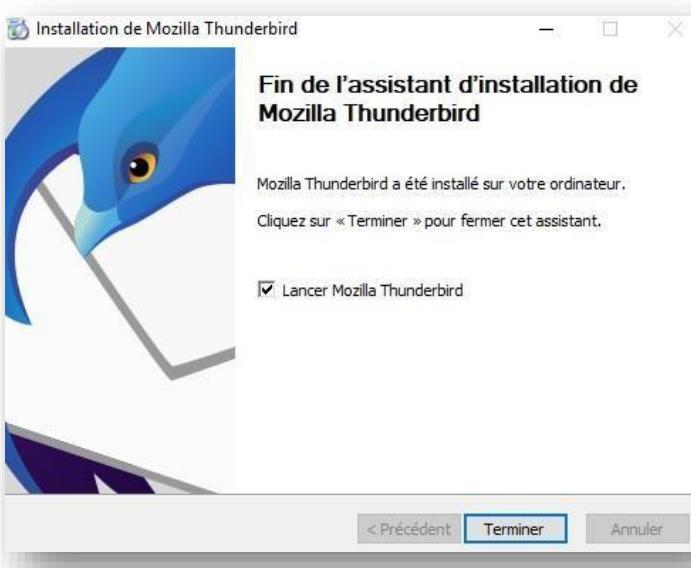
- Sélectionnez l'installation « **standard** »



- Choisissez le dossier d'installation de Thunderbird. Puis cliquez sur « **Installer** »



- Une fois l'installation achevée, vous pouvez lancer Thunderbird.



- Connectez-vous avec les utilisateurs que vous avez précédemment créés sur votre serveur de messagerie.

Votre nom complet
 i

Adresse électronique
 i

Mot de passe
 o

Retenir le mot de passe

[Configuration manuelle](#) [Annuler](#) [Continuer](#)

- Cliquez sur « Configuration manuelle » pour adapter les paramètres comme ci-dessous.

Paramètres du serveur

SERVEUR ENTRANT

Protocole :	IMAP
Nom d'hôte :	secu-civ.lan
Port :	143
Sécurité de la connexion :	Aucun
Méthode d'authentification :	Mot de passe normal
Nom d'utilisateur :	anakin@secu-civ.lan

SERVEUR SORTANT

Nom d'hôte :	secu-civ.lan
Port :	587
Sécurité de la connexion :	Aucun
Méthode d'authentification :	Mot de passe normal
Nom d'utilisateur :	anakin@secu-civ.lan

[Configuration avancée](#)

- Si tout est conforme, lorsque vous cliquez sur le bouton « **Retester** » tout en bas, ce message apparaîtra. Vous pouvez ensuite vous connecter :



- Félicitations, votre compte a été créé

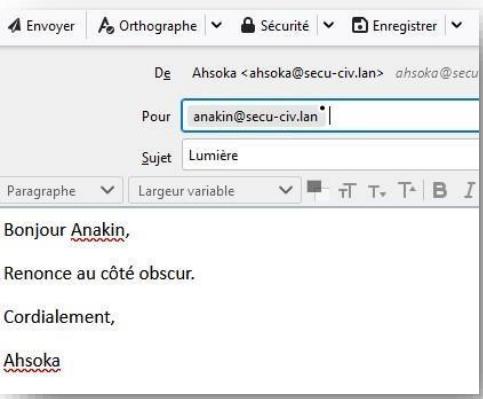
✓ Crédit de la création réussie

Vous pouvez dès maintenant utiliser ce compte avec Thunderbird.

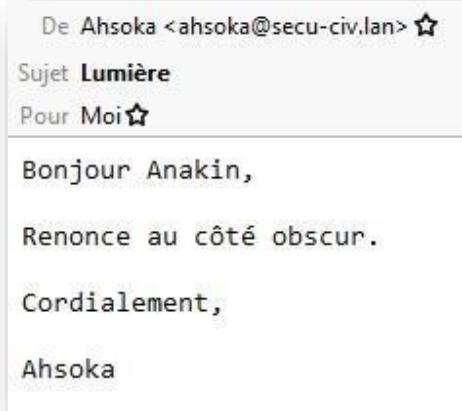
Vous pouvez enrichir l'expérience en connectant des services associés et en configurant des paramètres de compte avancés.

Test d'envoi de courriels

- Envoyons un mail avec un de nos utilisateurs



- Regardons si le partenaire a bien récupéré le mail

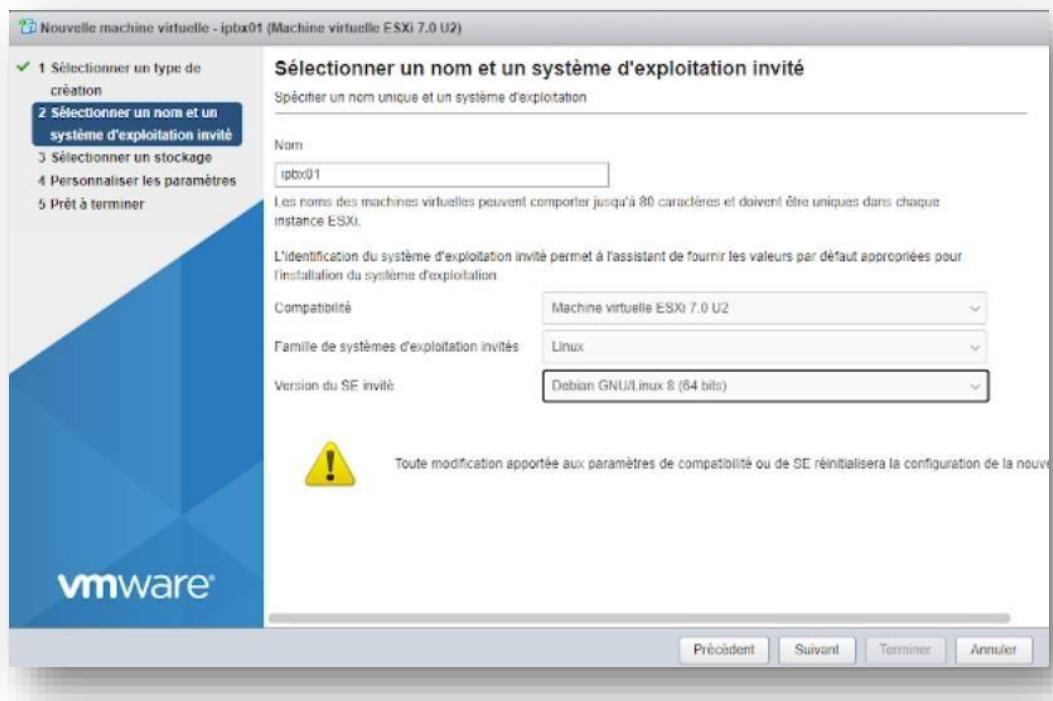


Le courriel a bien été transmis

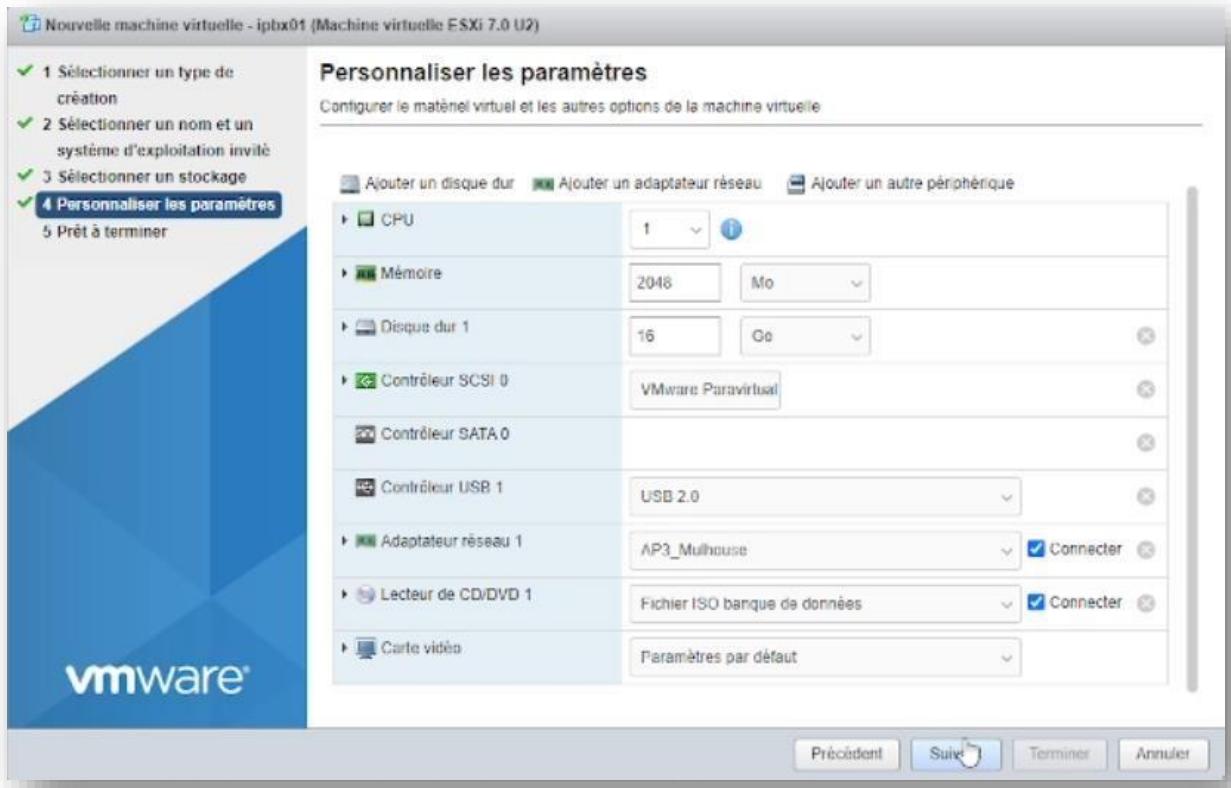
Téléphonie – 3CX & Client softphone

Environnement virtuel

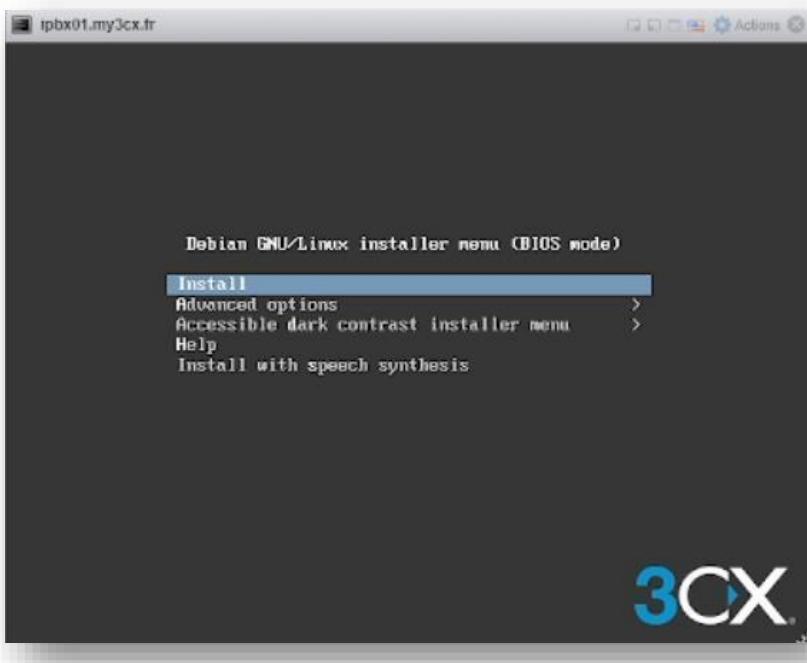
Nous allons créer une machine virtuelle 3CX



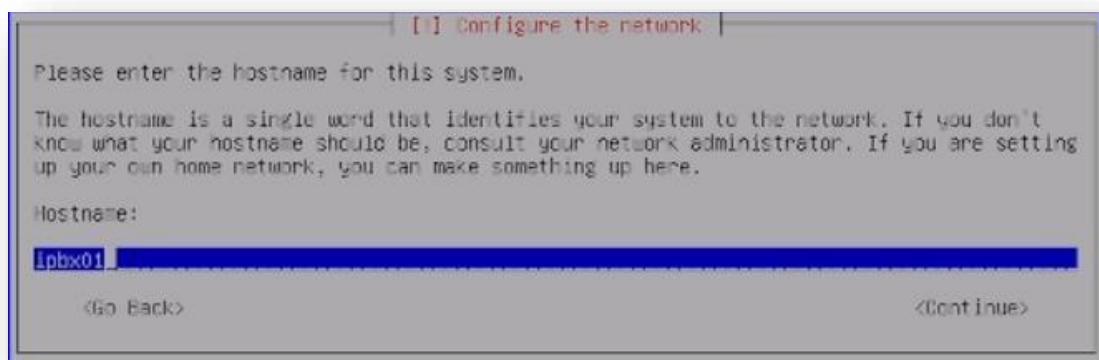
Ici nous configurons les bon paramètres de la vm.



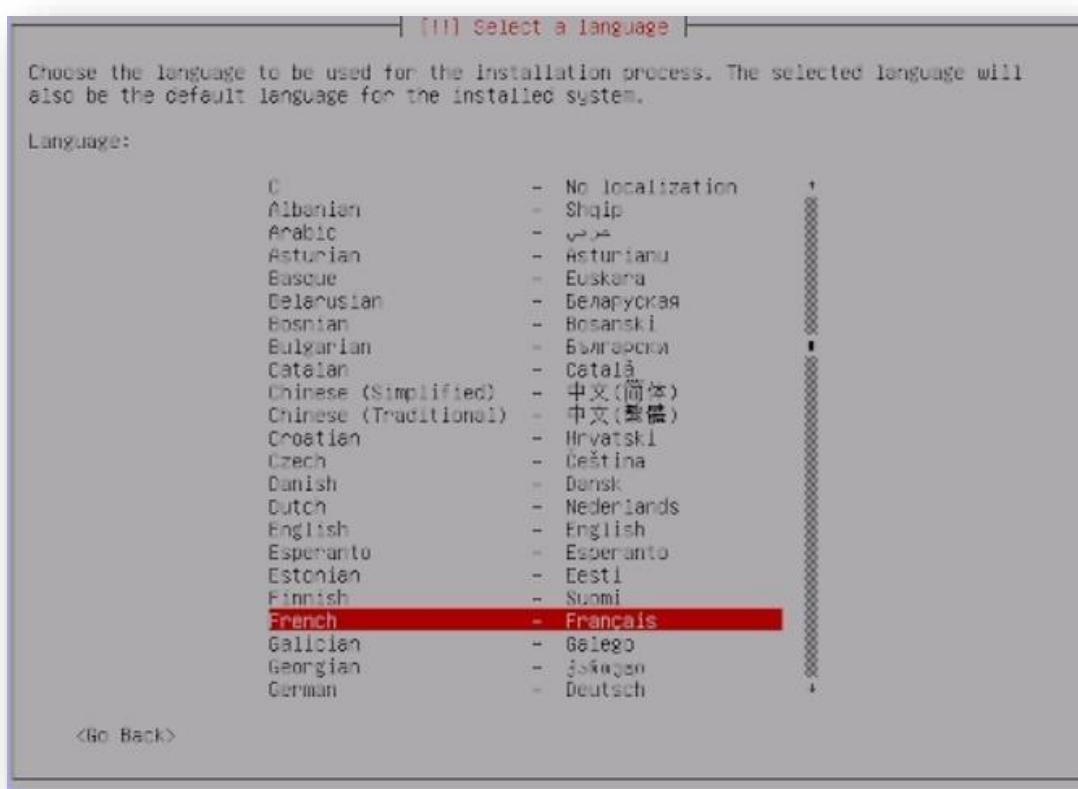
Nous la démarrons et cliquons sur « **install** »



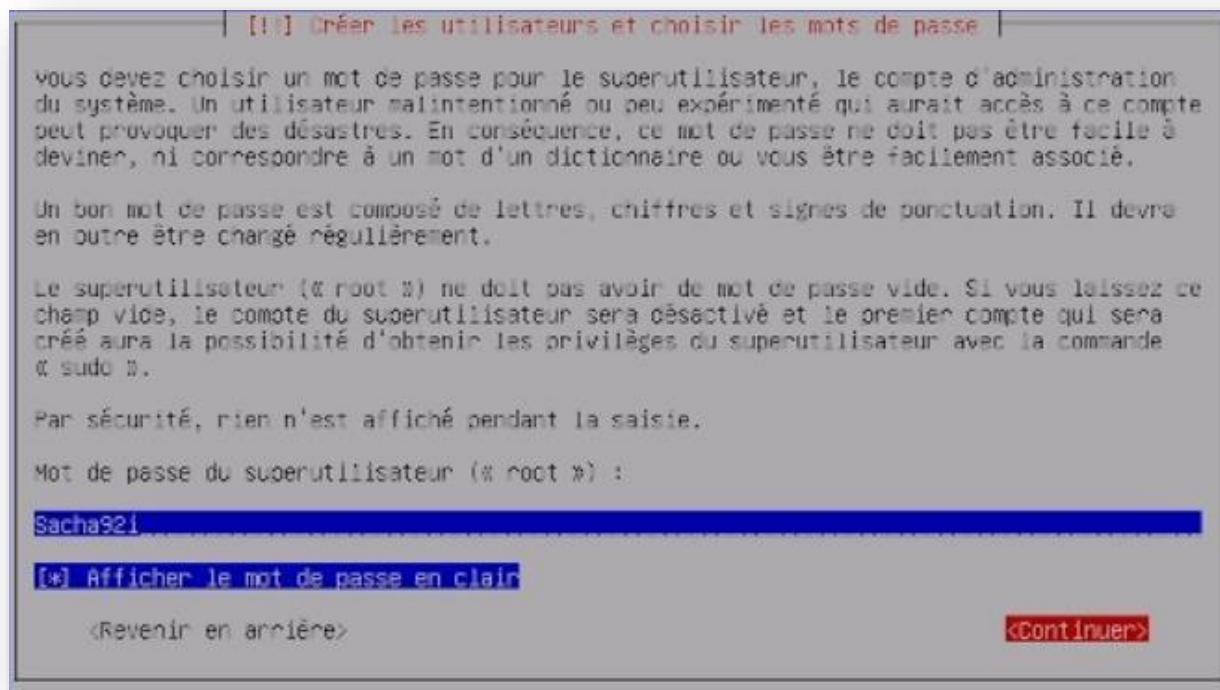
On entre le nom de la vm, ici ipbx01



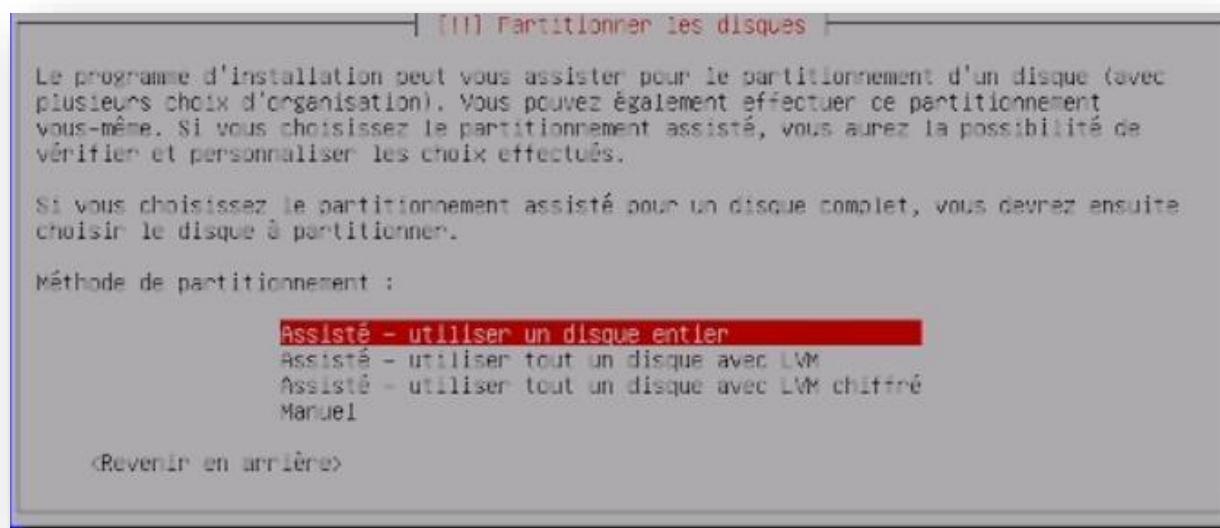
On choisit la langue, français.



On entre ici le mot de passe de l'utilisateur root.



Enfin ont choisi quel disque utiliser puis le type de partitionnement, (on aurait dû choisir LVM afin de pouvoir augmenter la taille du disque plus tard si les enregistrements audios prennent trop d'espace)



| [!!] Partitionner les disques |

Veuillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI1 (0,0,0) (sda) - 17.2 GB VMware Virtual disk

<Revenir en arrière>

| [!!] Partitionner les disques |

Disque partitionné :

SCSI1 (0,0,0) (sda) - VMware Virtual disk: 17.2 GO

Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.

Schéma de partitionnement :

Tout dans une seule partition (recommandé pour les débutants)
Partition /home séparée
Partitions /home, /var et /tmp séparées

<Revenir en arrière>

| [!!] Partitionner les disques |

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

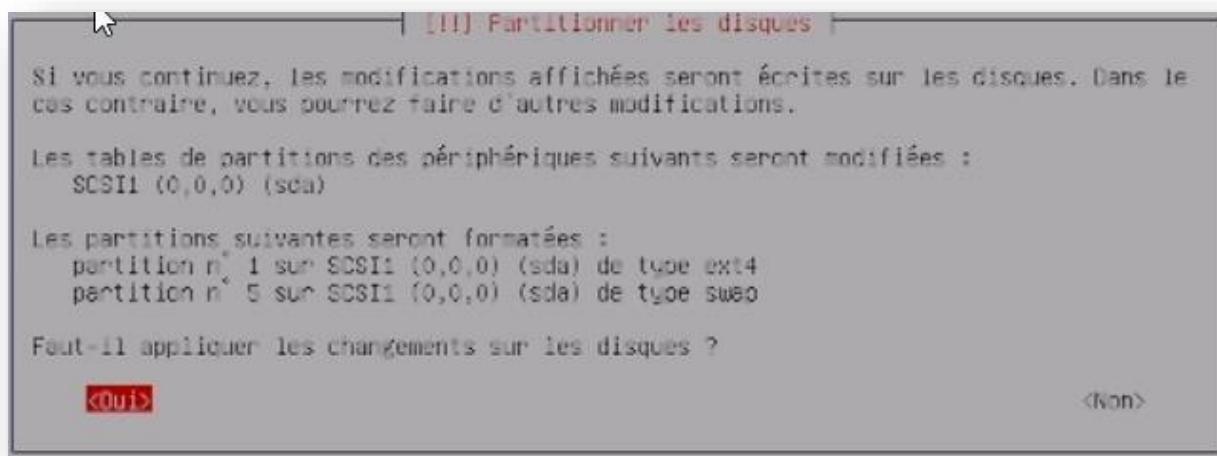
SCSI1 (0,0,0) (sda) - 17.2 GB VMware Virtual disk

n° 1	primaire	16.2 GB	f	ext4	/
n° 5	logique	1.0 GB	f	swap	swap

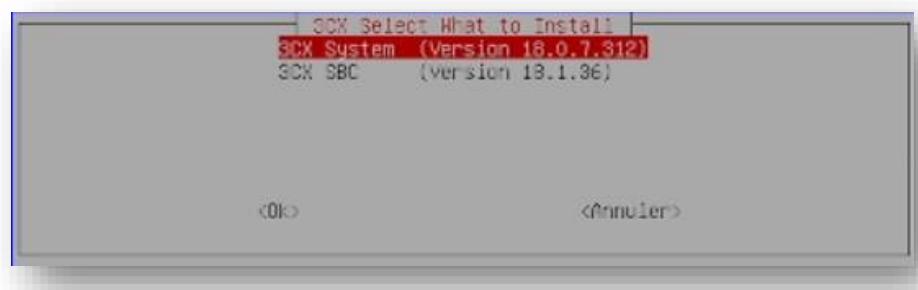
Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

Une fois les paramètres choisis on clique sur **terminer** puis **oui** pour confirmer



Une fois cela fait on choisit d'installer le système 3cx



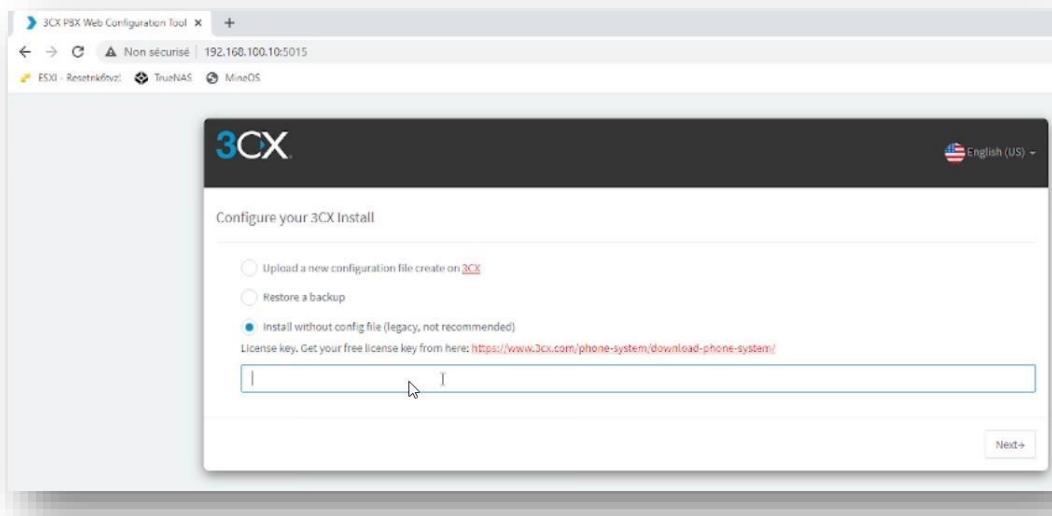
Après l'installation la vm va redémarrer. On tape alors 1 pour configurer depuis le panel web.



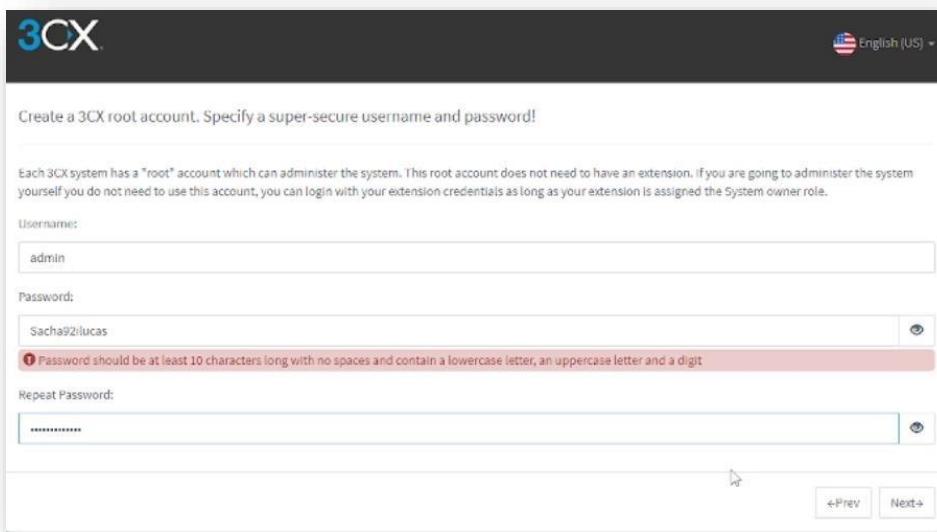
```
Select how to run the tool:
(1) Using a Web Browser
(2) From command line
Enter option: 1

Starting PBX Web configuration tool..
Launch this URL from a browser on another machine:
http://192.168.100.10:5015?v=2
TIP: If this is a cloud machine and the link shows a local IP address then you need to replace the local IP with your public IP Address.
```

On peut enfin passer à la partie web via l'adresse ip sur le port 5001.



Ici on entre la clé de licence préalablement récupérer chez 3cx. Puis on créer un compte admin pour la configuration.



Ont choisi ici d'utiliser l'IP Wan et de la configurer en statique.



Enfin on confirme les ports automatiques proposé par 3cx qu'on ouvrira plus tard sur le pare-feu.

The screenshot shows the 'Port selection for Web services (HTTPS/HTTP) and VoIP (SIP and Tunnel)' configuration screen. It includes fields for entering ports: 5001 for HTTPS, 5000 for HTTP, 5060 for SIP, and 5090 for Tunnel. Navigation buttons '« Prev' and 'Next »' are at the bottom right.

Port selection for Web services (HTTPS/HTTP) and VoIP (SIP and Tunnel)

Select the ports required for the management console, web client and VoIP services. You can leave the default options or choose other ports. Not all ports are permitted and ports cannot be changed after. These ports are automatically opened on your Windows or Linux local firewalls but you will need to port forward these ports on your border firewall device. More information [here](#).

Enter a FREE port for HTTPS. Recommended 443 or 5001.

5001

Enter a FREE port for HTTP. Recommended port 80 or 5000.

5000

Enter a FREE port for the SIP server. Default 5060.

5060

Enter a FREE Tunnel Port. Default 5090.

5090

« Prev Next »

Ici on entre le FQDN créé par 3CX lors de la création de la licence afin de relié le domaine au pbx.

The screenshot shows the 'Select the default network adapter' configuration screen. It includes a dropdown menu set to '192.168.100.10 ens192 {ens192}', a 'Use FQDN or IP' section, and a question about DNS configuration with two radio button options. Navigation buttons '« Prev' and 'Next »' are at the bottom right.

Select the default network adapter

192.168.100.10 ens192 {ens192}

Use FQDN or IP

To make 3CX easier to use for team members working out of the office, you need to configure a single FQDN that works both in and out of office (so as not to require multiple links for the webclient and meetings). This requires a DNS server and some configuration. See this [article](#) on how to configure it.

Yes I have a DNS server and will configure a single FQDN that works both in and out of the office

Enter your FQDN:

ipbx01.my3cx.fr

No, I do not have a DNS server and will use a local IP

« Prev Next »

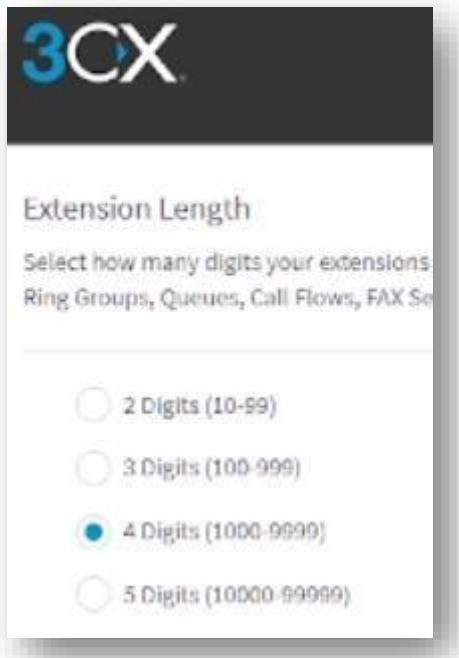
Une fois que cela est fait, on attend que la configuration se face.

Please wait...

Creating FQDN and certificates...

Waiting for the activation server to start processing your FQDN...

Après cela on nous demande de choisir le nombre de digit pour le pbx, attention cela n'est pas changeable par la suite. Il s'agit des numéros en interne.



Une fois cela fait on change la langue pour français.



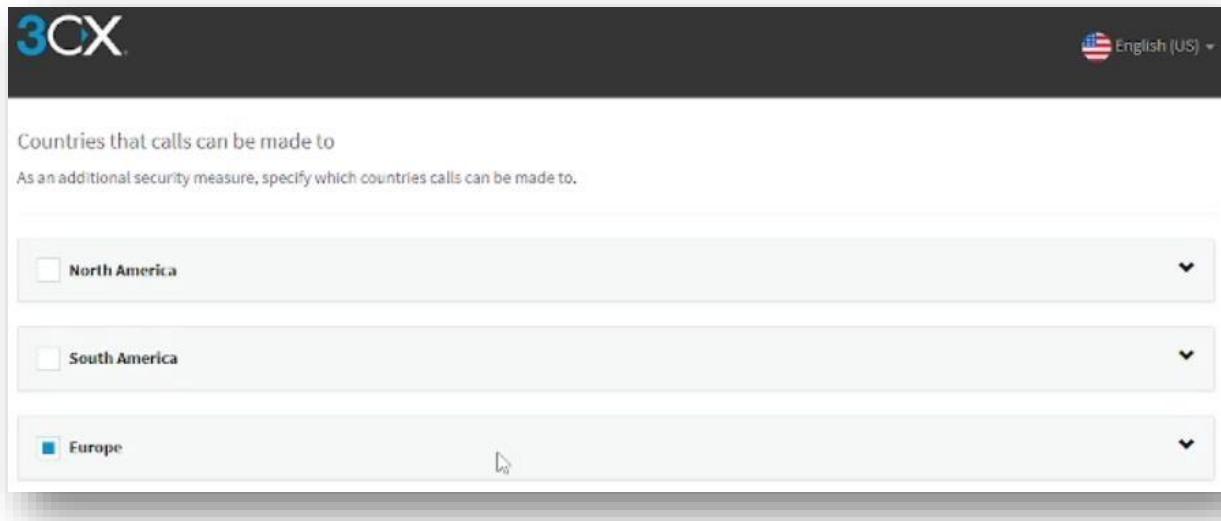
On crée la première extension, elle ne sera pas utilisé, uniquement pour les paramètres et test.

The screenshot shows the 'System Owner Extension' creation form. The fields filled are:

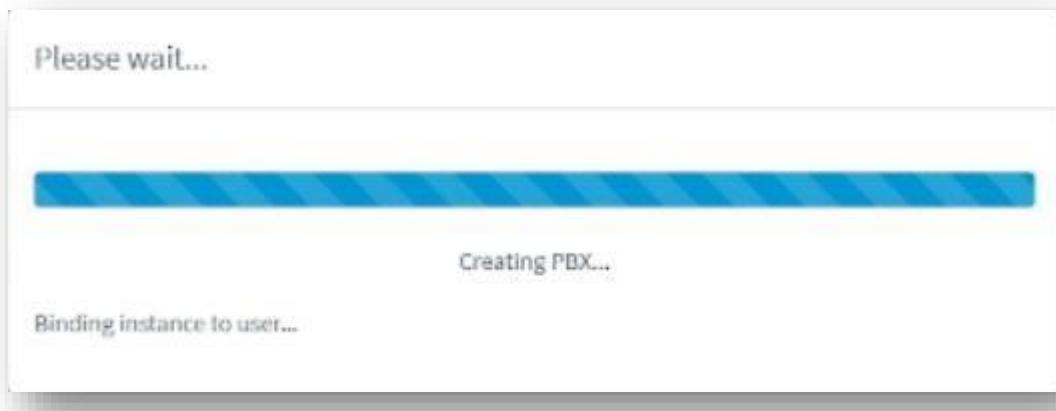
- Extension Number: 1000
- First Name: admin
- Last Name: admin
- Email Address: admin@test.fr
- Voicemail Number: 9999

At the bottom right, there are 'Prev' and 'Next' buttons.

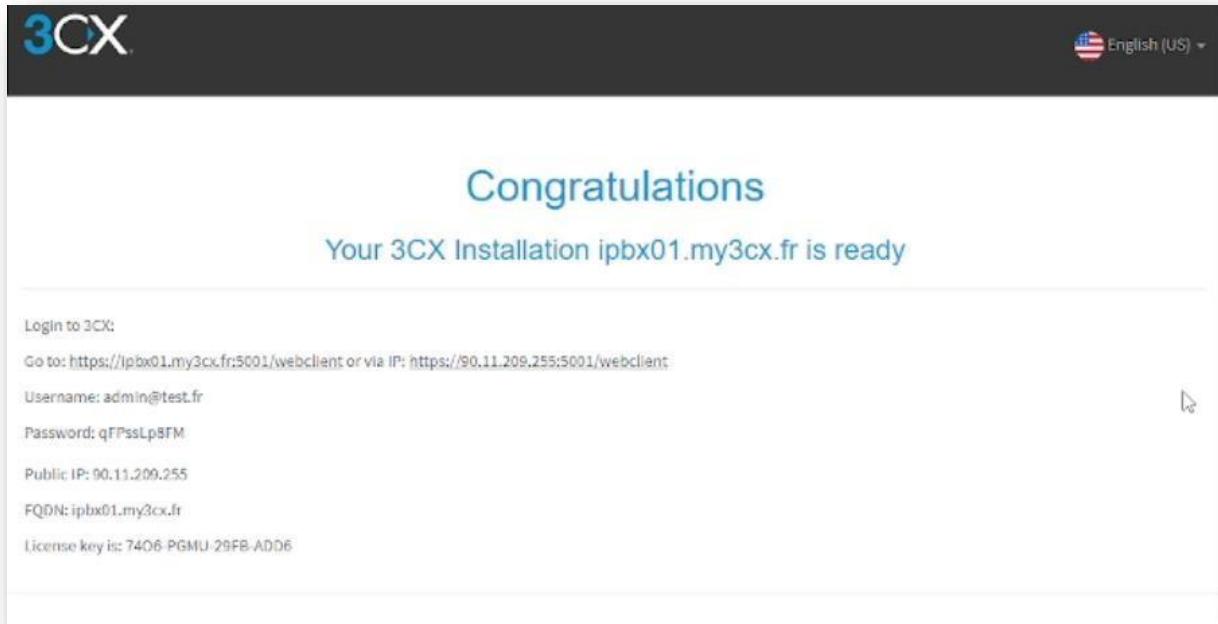
On choisit la région et la langue de messagerie



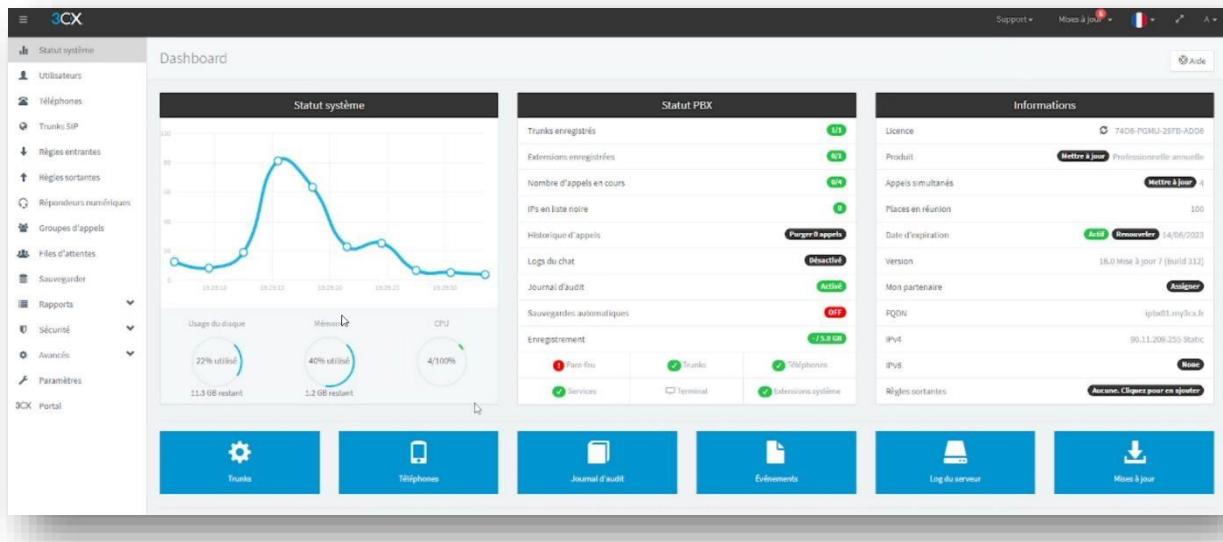
On clique sur **next** et on patiente que le pbx se mette en place.



L'installation est finie ! nous pouvons maintenant nous connecter au vrai panel de gestion.



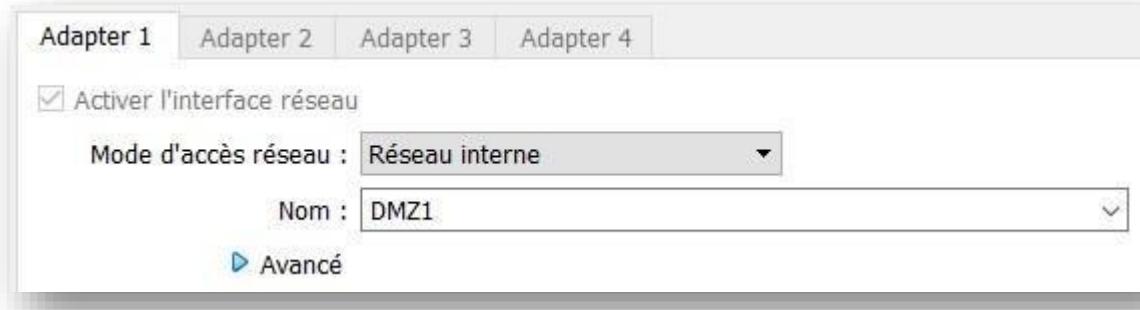
Voici le panel final de 3cx.



Serveur WEB (Application eBrigade) – Ubuntu (LAMP)

Environnement virtuel

Ubuntu 20.04. Le serveur web est placé dans une DMZ.



Configuration réseau final

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.200.4/29
      gateway4: 192.168.200.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
    enp0s8:
      dhcp4: true
version: 2
```

Installation LAMP

- L'installation des paquets apache, mysql et PHP sont nécessaires au fonctionnement de l'application eBrigade.

```
root@srvweb:~# sudo apt install apache2 php libapache2-mod-php mysql-server php-mysql,
```

- Après avoir installé les différents paquets, vérifiez si les différents services sont bien lancés

```
root@srvweb:/var/www# systemctl status apache2
● apache2.service - The Apache HTTP Server
```

```
root@srvweb:/var/www# systemctl status mysql
● mysql.service - MySQL Community Server
```

```
root@srvweb:/var/www# php --version
PHP 7.4.3 (cli) (built: Mar 2 2022 15:36:52) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.3, Copyright (c), by Zend Technologies
```

- Supprimer le dossier html qui se trouve par défaut dans /var/www, nous n'en avons pas besoin. Nous remplacerons le dossier html par les différents fichiers/dossiers de notre application eBrigade

```
root@srvweb:/var/www# rm -r html
```

Installation eBrigade

- Le logiciel est téléchargeable sur [ce lien](#)
- Une fois téléchargé, envoyez le dossier archivé sur votre serveur Ubuntu. Ici, nous l'avons fait via SSH. Pensez donc à installer/configurer l'accès SSH sur le serveur WEB.

```
C:\Users\Joé>scp Downloads\ebrigade-5.3.2.zip root@192.168.1.26:/home/srvweb
root@192.168.1.26's password:
ebrigade-5.3.2.zip                                              100%   33MB 109.5MB/s   00:00
```

- Notre dossier est bien arrivé sur notre serveur Ubuntu

```
root@srvweb:/home/srvweb# ls
ebrigade-5.3.2.zip
```

- Télécharger le paquet unzip pour pouvoir le dézipper

```
root@srvweb:/home/srvweb# apt install unzip
```

- Puis dézippez le dossier

```
root@srvweb:/home/srvweb# unzip ebrigade-5.3.2.zip -
```

- Résultat :

```
[root@srvweb ~]# ls ebrigade-5.3.2
```

- A présent nous allons déplacer les fichiers à l'intérieur du dossier dans /var/www

```
root@srvweb:/home/srvweb/ebrigade-5.3.2# cp -a . /var/www/
```

- Vérifions le contenu de notre dossier /var/www/

```
horaires.php                                upd_type_garde.php
iCalcreator.class.php                      upd_type_materiel.php
identification.php                          upd_type_vehicule.php
          upd_vehicule.php
import_api.php                            upgrade.php
index_d.php                               upload.php
index.html                                user-data
index.php                                 user_info.php
indispo_choice.php                        vcard_class.php
indispo_display.php                       vcard.php
indispo_list_xls.php                      vehicule_load.php
indispo.php                               vehicule.php
indispo_save.php                          vehicule_xls.php
indispo_status.php                        victimes.php
ins_company.php                          virements_extract.php
ins_groupe.php                           virements.php
ins_materiel.php                         webfonts
ins_personnel.php                        wizard.php
ins_poste.php                            zipcode.php
root@srvweb:~/var/www#
```

- Nous allons rapidement modifier notre virtualhost car nous avons supprimé le dossier html dans var. Nous allons devoir modifier le fichier suivant :

```
vim /etc/apache2/sites-available/000-default.conf
```

- Puis modifier la ligne « **DocumentRoot** » comme-ci-dessous

```
ServerAdmin webmaster@localhost
DocumentRoot /var/www/
```

- A ce stade nous n'avons toujours pas créé la BDD de eBrigade, nous allons donc le faire :

```
root@srvweb:~# mysql
```

- Puis renseignez la commande suivante

```
mysql> CREATE DATABASE `ebrigade` DEFAULT CHARACTER SET latin1 COLLATE latin1_general_cs;
Query OK, 1 row affected (0,01 sec)
```

- Nous allons maintenant créer notre utilisateur ebrigade pour la base de données et lui attribuer les droits nécessaires

```
mysql> CREATE USER 'ebrigade'@'localhost' IDENTIFIED BY 'ebrigade';
Query OK, 0 rows affected (0,01 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'ebrigade'@'localhost';
Query OK, 0 rows affected (0,02 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,01 sec)
```

ID : ebrigade MDP : ebrigade

- Pour se connecter à l'interface web. Renseignez dans le navigateur les identifiants comme-ci joint (à adapter).

Configuration Base de données

Paramètres de connexion à la base de données

Server Name **i** localhost

User **i** ebrigade

Password **i**

Database name **i** ebrigade

Valider

- L'erreur suivante peut apparaître :

Impossible d'écrire le fichier ./conf/sql.php.

Vérifier les permissions sur le filesystem

[Retour](#)

- Solution (accorder les droits nécessaires au dossier www) :

```
root@srvweb:/var# sudo chmod -R 777 www/
```

- Lors de votre prochaine tentative de connexion, l'erreur suivante peut apparaître :

```
ERROR 1419 (HY000): You do not have the SUPER privilege and  
binary logging is enabled (you *might* want to use the less safe  
log_bin_trust_function_creators variable)
```

- Pour la régler, renseignez la commande suivante (connexion en root à mysql) :

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

- Puis la commande suivante :

```
set global log_bin_trust_function_creators=1;
```

- Vous pouvez à présent vous connecter.



- Choisissez un mot de passe pour le compte Admin (**Azerty123**)



A light gray rectangular form with rounded corners. At the top left, it says "Modifier le mot de passe pour Admin ADMIN". Inside, there's a light blue callout box containing the text "Veuillez choisir un mot de passe personnel.". Below this are two input fields: "Nouveau mot de passe" followed by a redacted password and "Confirmation" followed by another redacted password. At the bottom left of the form is a light blue callout box containing the text "Pour plus de sécurité, mettez aussi des caractères spéciaux!". At the bottom right is a green rectangular button with white text that reads "Sauvegarder".

- Le mot de passe a bien été changé :



Pré-Configuration eBrigade

- Après l'installation, vous serez invité à renseigner plusieurs éléments :

A configuration form for eBrigade. It includes fields for organization type, short name, long name, web address, email, and a personalized application name.

Configuration eBrigade

Type d'organisation *

Service d'incendie et Secours i

Nom court de votre organisation *

SECUCIV i

Nom long de votre organisation *

SECURITE CIVILE i

Adresse Web *

http://192.168.200.4 i

Votre adresse email *

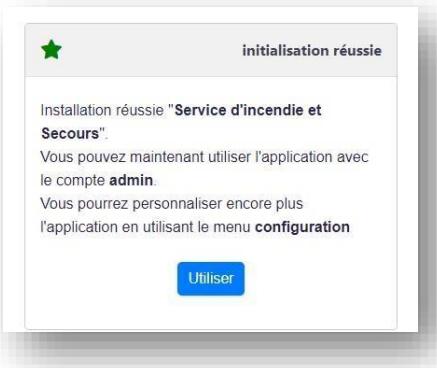
jonnedoue@gmail.com i

Nom personnalisé de l'application *

eBrigade i

Tous sauf le premier pourront être modifiés ultérieurement

- L'installation est terminée.



- Vous pouvez à présent commencer à utiliser eBrigade.

/!\ Informations importantes – eBrigade /!\

A ce stade, nous avons placé le serveur WEB dans notre DMZ (192.168.200.0/29) en modifiant la configuration réseau de celui-ci (jusqu'à présent, il était bridgé pour faciliter sa configuration).

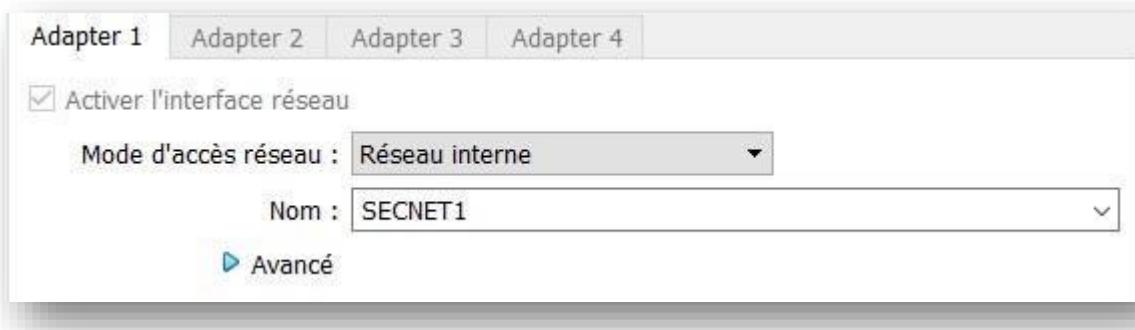
Des règles devront gérer le flux DMZ -> LAN (le bloquer) et le flux LAN -> DMZ / WAN -> DMZ (l'autoriser).

Se référer à la partie : [création des règles pare-feu](#)

Serveur de monitoring – Zabbix

Environnement virtuel Ubuntu

20.04.



[Configuration réseau final](#)

```
# This is the network config written by 'subiquity'  
network:  
    ethernets:  
        enp0s3:  
            dhcp4: no  
            addresses:  
                - 192.168.100.5/24  
            gateway4: 192.168.100.254  
            nameservers:  
                addresses: [8.8.8.8, 1.1.1.1]  
    version: 2
```

Installation Zabbix

Vous pouvez retrouver les différents paquets Zabbix pour les différents OS en suivant ce lien, l'agent utilisé pour la remontée d'informations de serveurs est aussi disponible à travers ce lien :
https://www.zabbix.com/download?zabbix=6.0&os_distribution=ubuntu&os_version=20.04_focal&db=mysql&ws=apache

Installation du répertoire Zabbix

- Tapez la commande suivante : wget

https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.01+ubuntu20.04_all.deb

- Puis la commande suivante permettant d'installer :

dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb

- Puis la commande :

apt update

Installation de Zabbix Server / Agent Zabbix... :

- Tapez la commande afin d'installation : apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbixagent

- Puis redémarrez le service Apache :

systemctl reload apache2

Ouverture des ports nécessaires au fonctionnement de Zabbix :

```
ufw allow 10050/tcp
```

```
ufw allow 443/tcp ufw
```

```
allow 80/tcp
```

A présent nous allons créer la BDD :

```
# mysql -uroot -p
* renseignez un mot de passe * mysql> create database zabbix character set
utf8mb4 collate utf8mb4_bin; mysql>
create user zabbix@localhost identified by 'joe0110';

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

- Puis tapez la commande suivante pour la peupler :

```
zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

- A présent nous devons configurer le MDP de l'utilisateur de la BDD dans les fichiers de configuration de Zabbix :

```
root@srvzabbix:/etc# vim /etc/zabbix/zabbix_server.conf
```

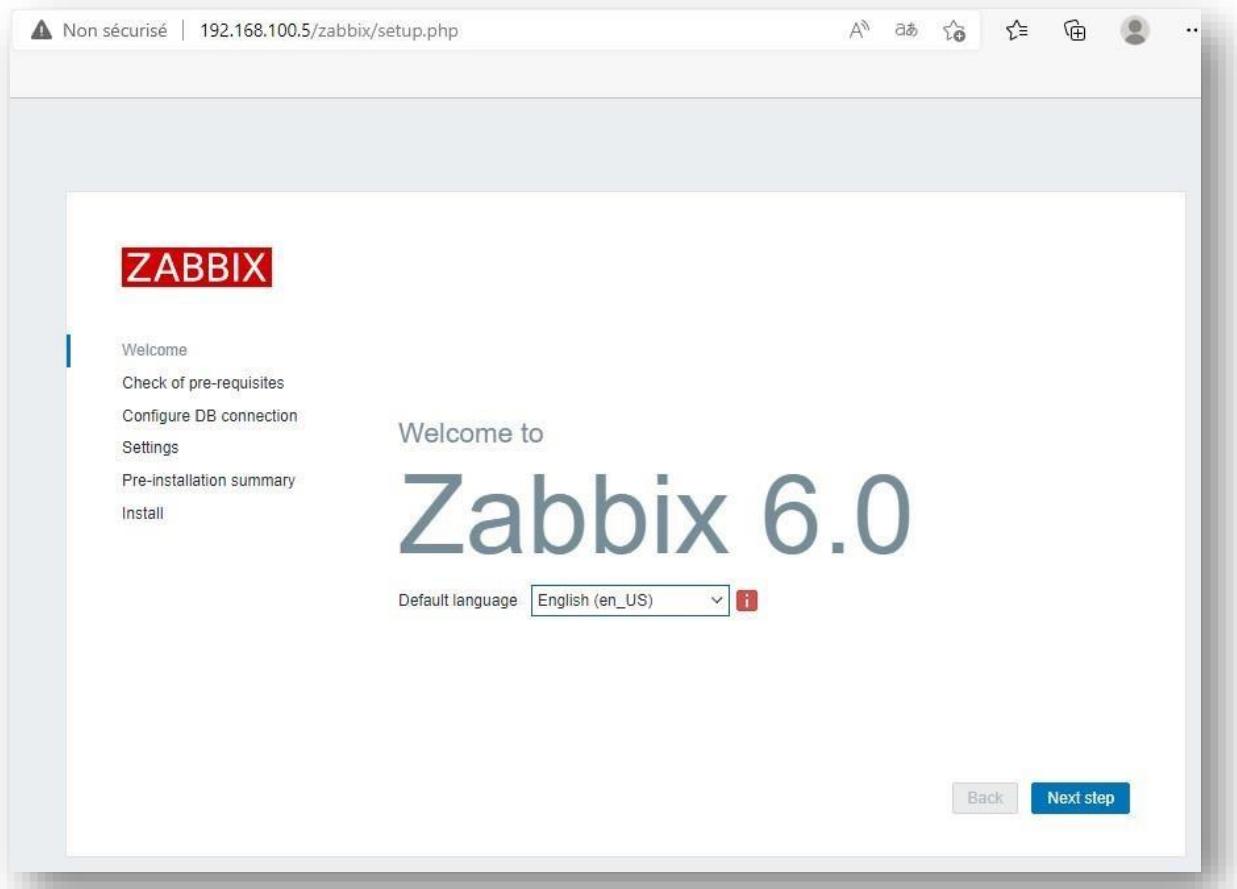
```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=
DBPassword=joe0110
```

- Redémarrage de Zabbix... systemctl restart zabbix-server zabbix-agent apache2

- ...Et activation du démarrage automatique lors des prochains redémarrages du serveur
`systemctl enable zabbix-server zabbix-agent apache2`

L'installation est terminée, nous pouvons accéder à l'interface de Zabbix en tapant `adresse_ip/zabbix` :



- *Configuration basique*

Sélectionnez la langue, nous laisserons en Anglais



- Configuration de la connexion à la BDD

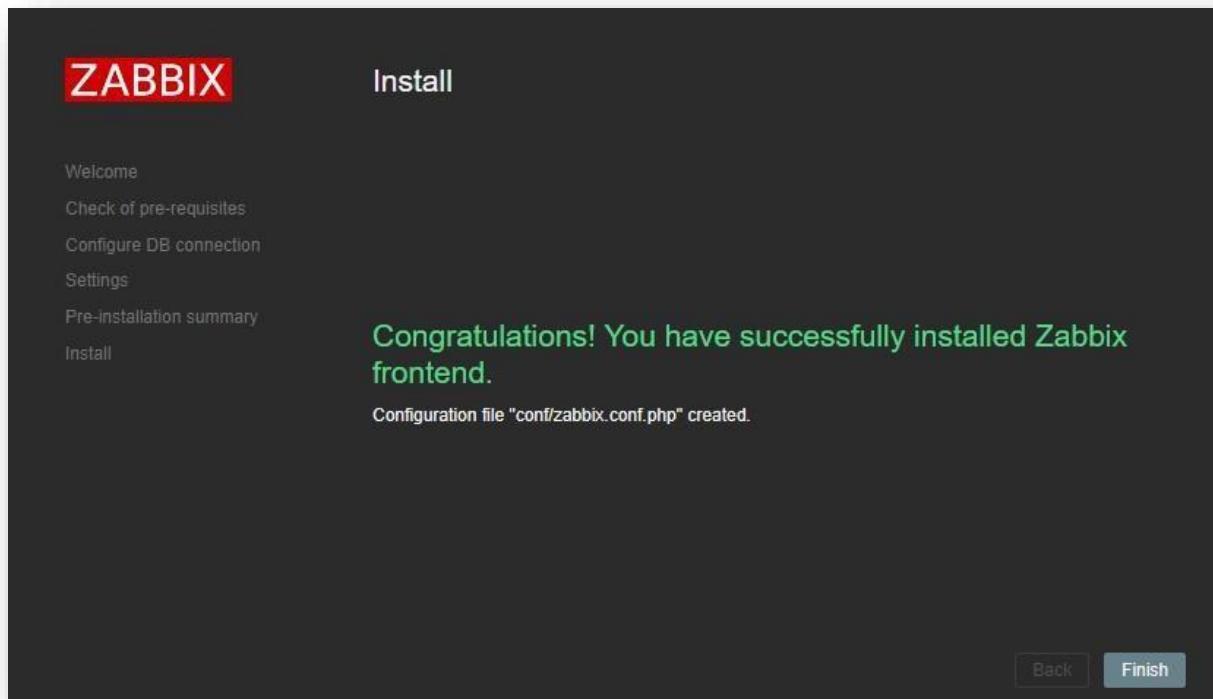
- Sélectionnez le nom du serveur ainsi que la timezone, nous pouvons également changer le thème.

The screenshot shows the Zabbix Settings configuration page. At the top, it says "ZABBIX" and "Settings". On the left, there's a sidebar with links: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary, and Install. The main area has three input fields: "Zabbix server name" set to "zabbix", "Default time zone" set to "(UTC+02:00) Europe/Paris", and "Default theme" set to "Dark". At the bottom right are "Back" and "Next step" buttons.

- Récapitulatif :

The screenshot shows the Zabbix Pre-installation summary configuration page. At the top, it says "ZABBIX" and "Pre-installation summary". Below that, a message says: "Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters." The main area lists configuration parameters with their values: Database type MySQL, Database server localhost, Database port default, Database name zabbix, Database user zabbix, Database password ***** (redacted), Database TLS encryption false, and Zabbix server name zabbix. At the bottom right are "Back" and "Next step" buttons.

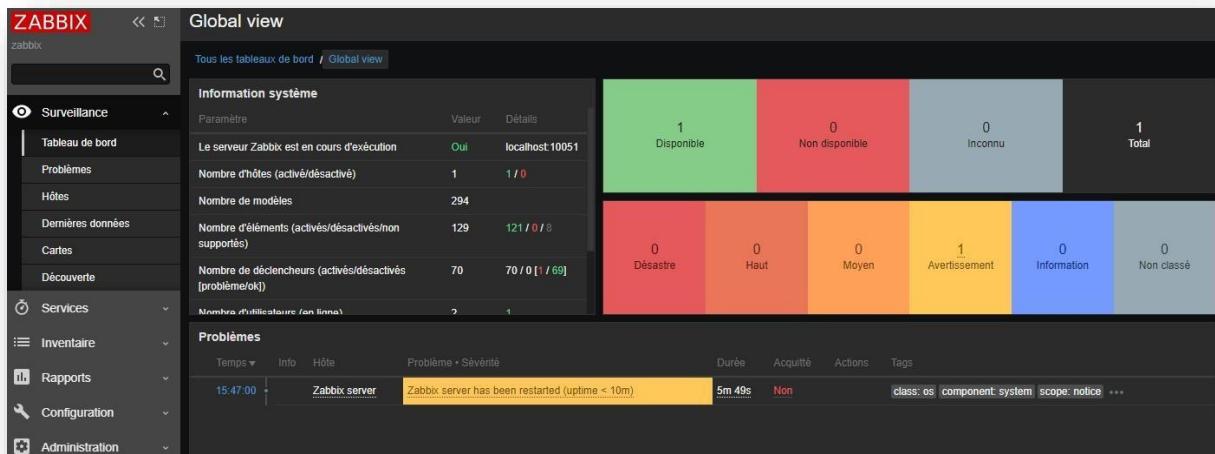
- Voilà ! L'installation et la configuration de base est terminée



- Pour vous connecter à l'interface web de Zabbix, rentrez les informations suivantes : ID : Admin / MDP : zabbix

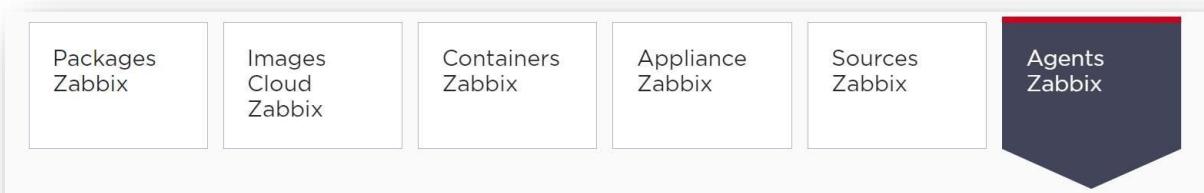


- Nous voilà connecté, la langue peut être modifiée dans les paramètres utilisateurs > profil > langue.



Déploiement de l'agent Zabbix (Windows)

- Nous allons déployer l'agent Zabbix sur notre serveur Windows Server 2019. Rendez-vous sur [ce site](#), puis télécharger l'agent correspondant à votre OS, ici nous choisirons Windows.



Téléchargez et installez les agents Zabbix précompilés

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

Show legacy downloads

OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	MATÉRIEL	VERSION DE ZABBIX	CHIFFREMENT	FORMAT
Windows	Any	amd64	6.0 LTS	OpenSSL	MSI
Linux		i386	5.4	No encryption	Archive
macOS			5.2		
AIX			5.0 LTS		

- Réalisez l'installation



- Dans « **Host Name** » renseignez un nom pour votre serveur Windows, dans « **Zabbix server IP** » renseignez l'adresse IP de votre serveur Zabbix. Le port par défaut est 10050. Ces paramètres pourront être modifiés ultérieurement dans les fichiers de configuration de l'agent Zabbix.



- Finalisez l'installation



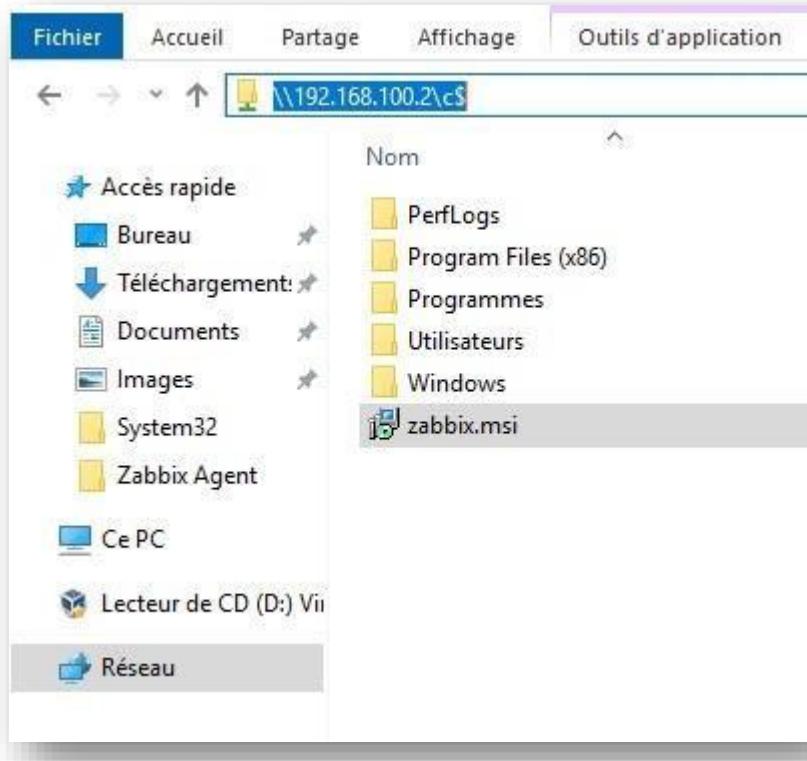


- On peut voir que le service Zabbix est bien en cours d'exécution

wuauserv	103b	Windows Update	en cours d'exé...	net
Zabbix Agent	3964	Zabbix Agent	En cours d'exé...	

Déploiement de l'agent Zabbix (Windows CORE)

- Sur votre serveur principal avec interface graphique, déposez l'installateur de l'agent Zabbix à la racine du disque C:\ de votre serveur CORE



- Sur votre serveur Core, lancez powershell.

```
PS C:\Users\Administrateur.SECU-CIV> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur.SECU-CIV>
```

- Puis lancez la commande suivante pour installer l'agent Zabbix

```
PS C:\Users\Administrateur.SECU-CIV> msieexec.exe /I C:\zabbix.msi
```

- La fenêtre de configuration de Zabbix s'ouvrira, le reste de la configuration s'effectue de la même manière que celle effectuée sur le serveur GUI.

Déploiement de l'agent Zabbix (Debian) /

Ubuntu)

- Tapez la commande apt install zabbix-agent

```
root@srvtel:/home/srvtel# apt install zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  zabbix-agent
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 578 ko dans les archives.
Après cette opération, 1 214 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 zabbix-agent amd64 1:5.0.8+dfsg-1
578 kB]
578 ko réceptionnés en 0s (1 860 ko/s)
Sélection du paquet zabbix-agent précédemment désélectionné.
(Lecture de la base de données... 65937 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../zabbix-agent_1%3a5.0.8+dfsg-1_amd64.deb ...
Dépaquetage de zabbix-agent (1:5.0.8+dfsg-1) ...
Paramétrage de zabbix-agent (1:5.0.8+dfsg-1) ...

Creating config file /etc/zabbix/zabbix_agentd.conf with new version
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
```

- Une fois l'installation terminée, rendez-vous dans les fichiers de configuration de l'agent Zabbix

```
root@srvtel:/home/srvtel# vim /etc/zabbix/zabbix_agentd.conf
```

- Modifiez le serveur, renseignez l'IP de celui de Zabbix

```
# Server=
Server=192.168.100.5
```

- Modifiez également le nom d'hôte du serveur de téléphonie, puis enregistrez le fichier

```
# Hostname=
Hostname=SRVTEL
```

- Tapez la commande suivante pour le démarrage automatique de l'agent : `systemctl enable --now zabbix-agent`

```
root@srvtel:/home/srvtel# systemctl enable --now zabbix-agent
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
```

- Vous n'avez plus qu'à créer un hôte sur Zabbix

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte: SRVTEL

Nom visible: SRVTEL

Modèles: Linux by Zabbix agent Sélectionner

taper ici pour rechercher

* Groupes: Machines LAN Sélectionner

taper ici pour rechercher

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	192.168.100.4		IP	DNS	10050

Ajouter

Description

Ajouter

- Résultat :

	Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité
<input type="checkbox"/>	SRVTEL	Éléments 42	Déclencheurs 14	Graphiques 8	Découverte 3	Web 192.168.100.4:10050			Linux by Zabbix agent	Activé	ZBX

- Si l'erreur suivante apparaît, pensez à ouvrir le port 10050 sur votre pare-feu



Sur DEBIAN (/Ubuntu) :

- D'abord, installez ufw, tapez la commande : sudo apt install ufw
- Puis activer le pare-feu : sudo ufw enable
- Pour vérifier le statut, tapez : sudo ufw status
- A ce stade, vous devriez avoir ce résultat

```
root@srvtel:/home/srvtel# sudo ufw status
Status: active
```

- Ajoutez les règles suivantes

```
root@srvtel:/home/srvtel# sudo ufw allow 10050/tcp
Rule added
Rule added (v6)
root@srvtel:/home/srvtel# sudo ufw allow 10050/udp
Rule added
Rule added (v6)
```

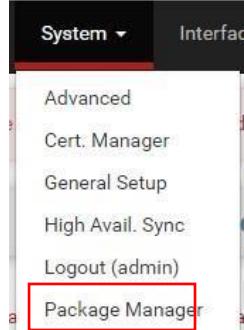
- Pour voir les différentes règles, tapez :

```
root@srvtel:/home/srvtel# sudo ufw status
Status: active

To                         Action      From
--                         --         --
10050/tcp                  ALLOW       Anywhere
10050/udp                  ALLOW       Anywhere
10050/tcp (v6)              ALLOW       Anywhere (v6)
10050/udp (v6)              ALLOW       Anywhere (v6)
```

Déploiement de l'agent Zabbix (Pfsense)

- Rendez-vous dans « **Packet Manager** »



- Puis cliquez sur « **Available Packages** »



- Cherchez « **zabbix-agent6** » puis cliquez sur « **+ Install** »



- Rendez-vous dans « **Services** » puis « **Zabbix Agent 6** »



- Les paramètres à renseigner sont les suivants : « **Server** » - **Serveur Zabbix** ; « **Server Active** » - **Serveur Zabbix** ; « **Hostname** » - Nom de votre routeur

Zabbix Agent Settings	
Enable	<input checked="" type="checkbox"/> Enable Zabbix Agent service.
Server	192.168.100.5 List of comma delimited IP addresses (or hostnames) of ZABBIX servers.
Server Active	192.168.100.5 List of comma delimited IP:port (or hostname:port) pairs of Zabbix servers for active checks.
Hostname	RTE02 Unique, case sensitive hostname. Required for active checks and must match host OS name.

- A présent, ajoutons notre routeur sur Zabbix

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte: RTE02
 Nom visible: RTE02
 Modèles: FreeBSD by Zabbix agent Sélectionner
 taper ici pour rechercher
 * Groupes: Machines LAN Sélectionner
 taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	
Agent		192.168.100.252		IP	DNS	10050

- Notre routeur a bien été ajouté



Création d'un groupe d'hôtes

Nous placerons tous nos serveurs dans un groupe d'hôtes que nous allons créer. •

Dans « Configuration », cliquez sur « Groupes d'hôtes »

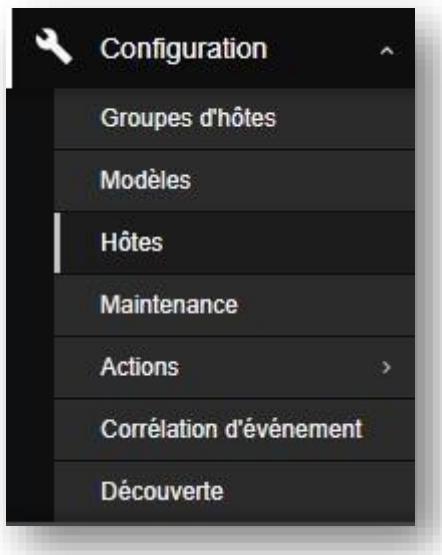


- Donnez un nom à votre groupe

* Nom du groupe: Machines LAN
 Ajouter Annuler

Création d'un hôte sur Zabbix

- Pour créer un hôte afin de la monitorer, rendez-vous dans « Configuration » puis « Hôtes »



- En haut à droite, cliquez sur « Créeer un hôte »



Dans « **Nom de l'hôte** » renseignez un nom pour votre hôte, dans « **Modèles** » choisissez un modèle correspondant à votre hôte, il y a un nombre important de modèles prédéfinis dans Zabbix. Dans « **Groupes** » renseignez le groupe que nous avons créé précédemment. Dans « **Interfaces** » ajoutez en une de type « **Agent** » puis renseignez dans « **Adresse IP** » l'adresse IP du serveur que vous souhaitez monitorer. Le port par défaut peut également être modifié.

-

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

Nom de l'hôte: SRVW01
Nom visible: SRVW01
Modèles: Windows by Zabbix agent Sélectionner
Groupes: Machines LAN Sélectionner
Interfaces: Type: adresse IP Nom DNS: Connexion à: IP Port: 10050 Défaut
Agent: 192.168.100.1 IP DNS
Ajouter
Description: Ajouter

- Cliquez ensuite sur « **Ajouter** », une fois créé celui-ci devrait apparaître dans les hôtes

Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface
SRVW01	Éléments 41	Déclencheurs 16	Graphiques 6	Découverte 4	Web 192.168.100.1:10050	

- On peut voir la disponibilité du serveur un peu plus à droite. Si c'est vert, cela signifie que disponibilité est fonctionnelle. Nous pouvons à présent récupérer des informations sur le serveur.



Monitoring d'un serveur Windows

- Rendons-nous dans « **Surveillance** » puis « **Hôtes** »



- Ici, nous avons un aperçu des différents hôtes, cliquons sur « **Dernières données** » du serveur SRVW01

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
SRVW01	192.168.100.1:10050	ZBX	class: os target: windows	Activé	Dernières données	Problèmes	Graphiques 6
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données	Problèmes	Graphiques 25

- Si nous cliquons par exemple sur « **CPU** » nous pouvons voir différentes informations sur le CPU de notre serveur Windows

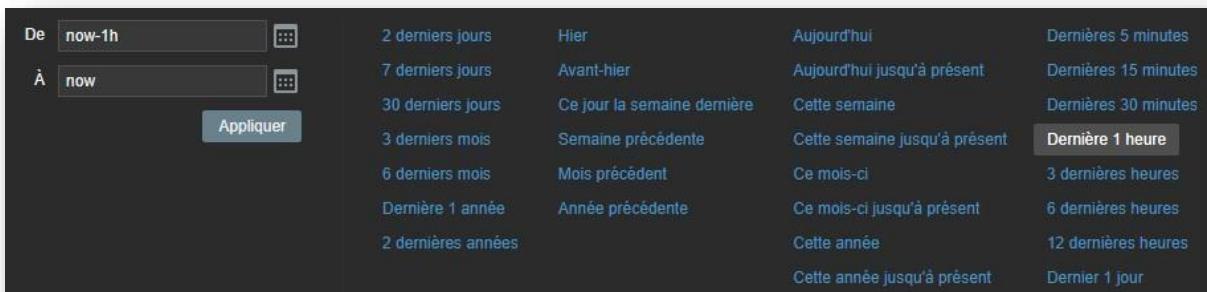
VALEURS DU TAG						
component: application +1 cpu 8 memory +12 network +9 os +3 raw +1 storage +4 system +7						
description: Ethernet +9						
interface: Intel(R) PRO/1000 MT Desktop Adapter +9						
DATA						
Avec données 33 Sans données 8						
Hôte	Nom		Dernière vérification	Dernière valeur	Changer	Tags
SRVW01	Context switches per second ?		6s	154.1575	-11.4244	component: cpu
SRVW01	CPU DPC time ?		10s	0 %		component: cpu
SRVW01	CPU interrupt time ?		9s	0 %		component: cpu
SRVW01	CPU privileged time ?		8s	0 %		component: cpu
SRVW01	CPU queue length ?		5s	1	+1	component: cpu
SRVW01	CPU user time ?		7s	0 %		component: cpu
SRVW01	CPU utilization ?		2s	0.2469 %	-0.2549 %	component: cpu
SRVW01	Number of cores ?		51s	1		component: cpu

Nous pouvons également faire de la métrologie, retournons dans « **Surveillance** » puis « **Hôtes** » puis cliquez sur « **Graphiques** » au lieu de « **Dernières données** » pour le serveur SRVW01.

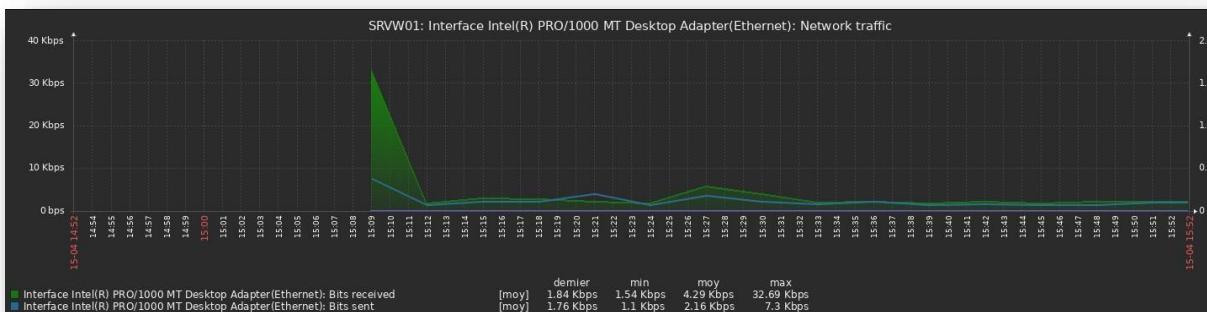
Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
SRVW01	192.168.100.1:10050	ZBX	class: os target: windows	Activé	Dernières données	Problèmes	Graphiques 6

•

- Nous pouvons régler, en haut de la page, les dates où nous souhaitons récupérer des informations sur le serveur



- Puis en dessous, différents graphiques sont disponibles. Par exemple nous pouvons voir l'impact de ce serveur sur le réseau.

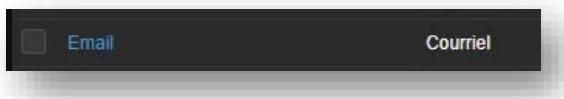


Envoyer d'un courriel en cas de dysfonctionnement d'un hôte

- Sur Zabbix, dans « **Administration** » cliquez sur « **Types de média** »



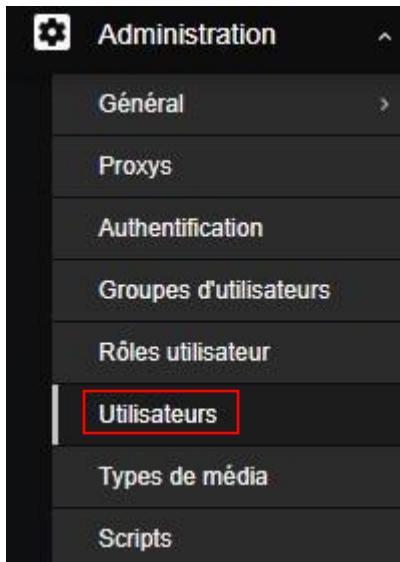
- Sélectionnez « Email »



- Renseignez les différents éléments comme ci-joint. Le but ici est de renseigner les informations du serveur de messagerie et de l'utilisateur qui recevra un courriel en cas de panne. Cliquez sur « Actualiser » une fois que la configuration est terminée.

* Nom: Email
 Type: Courriel
 * serveur SMTP: 192.168.100.1
 Port du serveur SMTP: 25
 * SMTP helo: secu-civ.lan
 * adresse SMTP: Administrateur@secu-civ.lan
 Sécurité de la connexion: Aucun
 Authentification: Aucun
 Nom d'utilisateur: Administrateur@secu-civ.l
 Mot de passe: Joe0110
 Format du message: HTML
 Description:
 Activé:
 Actualiser | Clone | Supprimer | Annuler

A présent, dans « Administration », cliquez sur « Utilisateurs »



- Sélectionnez l'utilisateur « **Admin** »

<input type="checkbox"/>	Nom d'utilisateur ▲	Prénom	Nom de famille	Rôle utilisateur
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super admin role

- Cliquez sur « **Média** »



- Renseignez les paramètres comme ci-joint. Nous pouvons choisir la sévérité nécessaire pour l'envoi d'un mail. Finalement, cliquez sur « **Ajouter** »

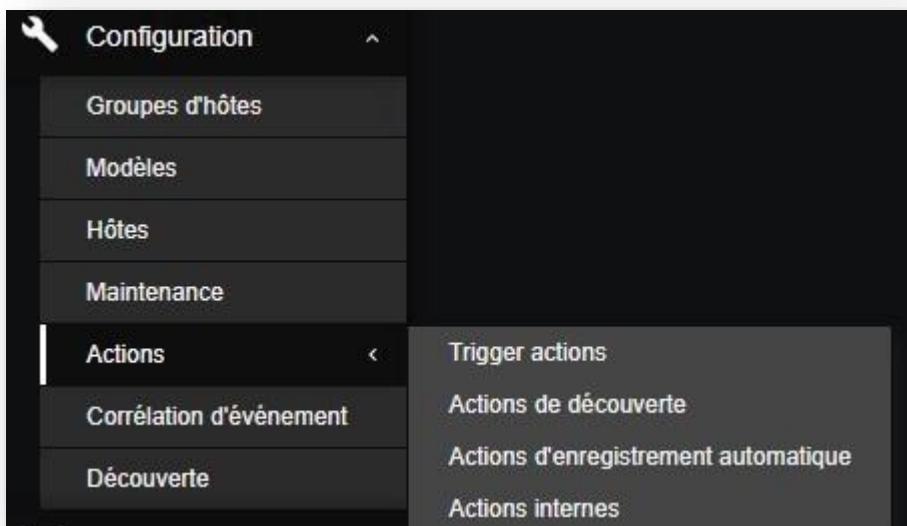
Média

Type	Email	<input type="button" value="▼"/>
* Envoyer	Administrateur@secu-civ.lan	<input type="button" value="Supprimer"/>
<input type="button" value="Ajouter"/>		
* Lorsque actif	1-7,00:00-24:00	
Utiliser si sévérité	<input type="checkbox"/> Non classé <input type="checkbox"/> Information <input type="checkbox"/> Avertissement <input checked="" type="checkbox"/> Moyen <input checked="" type="checkbox"/> Haut <input checked="" type="checkbox"/> Désastre	
Activé	<input type="checkbox"/>	
<input type="button" value="Ajouter"/> <input type="button" value="Annuler"/>		

- Cliquez sur « **Actualiser** » afin de valider les paramètres

Média	Type	Envoyer	Lorsque actif	Utiliser si sévérité	État	Action
Email	Administrateur@secu-civ.lan	1-7,00:00-24:00	<input type="checkbox"/> N <input type="checkbox"/> I <input type="checkbox"/> A <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> H <input checked="" type="checkbox"/> D	Activé	<input type="button" value="Édition"/>	<input type="button" value="Supprimer"/>
<input type="button" value="Ajouter"/>						
	<input type="button" value="Actualiser"/>	<input type="button" value="Supprimer"/>	<input type="button" value="Annuler"/>			

- A présent, nous allons configurer une action pour savoir quand le courriel doit être envoyé.
Dans « Configuration » > « Actions », cliquez sur « Trigger actions »



- Cliquez sur « Crée une action » en haut à droite

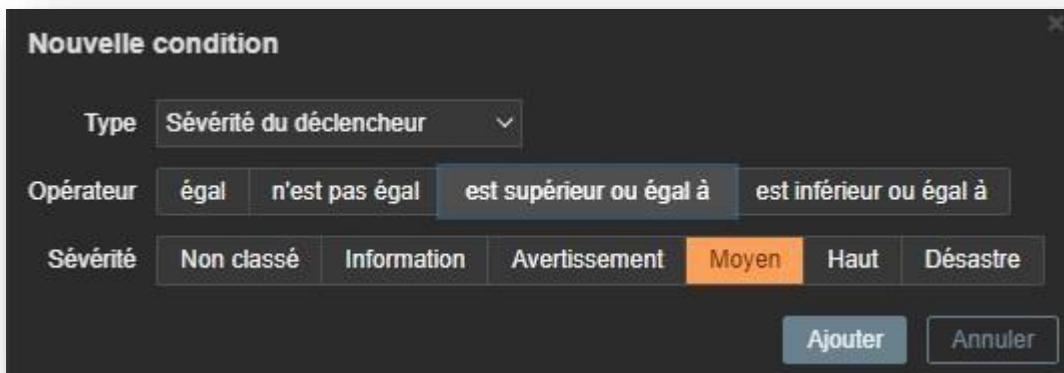


- Donnez un nom à votre action puis cliquez sur « Ajouter » dans « Conditions »

This screenshot shows a configuration dialog for adding a condition. The top section has a field labeled 'Nom' containing 'Alerte'. Below it is a table with columns 'Conditions', 'Étiquette', 'Nom', and 'Action'. The 'Conditions' column contains a row with 'Ajouter' and a plus sign icon. The 'Nom' column is empty. The 'Action' column is also empty. At the bottom, there is a checkbox labeled 'Activé' with a checked status. A note below the checkbox states: 'Au moins une opération doit exister.' (At least one operation must exist.) At the very bottom are two buttons: 'Ajouter' (in blue) and 'Annuler'.

- Dans type nous allons choisir « **Sévérité du déclencheur** » puis dans opérateur « **est supérieur ou égal à** » est dans « **Sévérité** » « **Moyen** ». Puis cliquez sur « **Ajouter** »

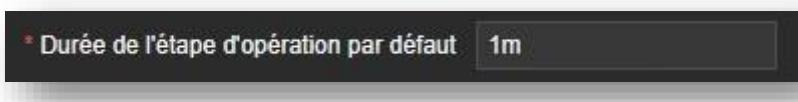
La condition d'envoi de courriel sera la suivante : la sévérité doit être supérieur ou égal à moyen



- A présent cliquez sur « **Opérations** ». Nous allons définir ce qui doit être fait lorsque la condition est respectée



- Mettez « **1m** » au lieu de « **1h** » cela permet de définir la durée d'attente avant que l'opération soit effectuée



- Dans « **Opérations** » cliquez sur « **Ajouter** », puis renseignez les paramètres comme ci-joint. Enfin, cliquez sur « **Add** »

Détails de l'opération

Opération Envoi message

Étapes - (0 - indéfiniment)

Durée de l'étape (0 - utiliser les paramètres par défaut de l'action)

* Au moins un utilisateur ou un groupe d'utilisateurs doit être sélectionné.

Envoyer aux groupes d'utilisateurs	Groupe d'utilisateurs	Action
	Ajouter	

Envoyer aux utilisateurs	Utilisateur	Action
	Admin (Zabbix Administrator)	Supprimer
	Ajouter	

Envoyer uniquement à

Message personnalisé

Conditions	Etiquette	Nom	Action
	Ajouter		

Add **Annuler**

- Enfin, cliquez sur « Ajouter »

* Durée de l'étape d'opération par défaut

Opérations	Détails	Démarrer dans	Durée	Action
1 Envoyer le message aux utilisateurs: Admin (Zabbix Administrator) via Email	Immédiatement	Défaut	Edition Supprimer	
Ajouter				

Opérations de récupération	Détails	Action
	Ajouter	

Opérations de mise à jour	Détails	Action
	Ajouter	

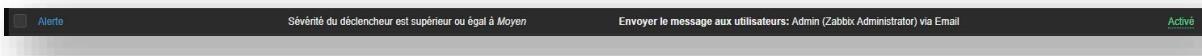
Suspendre les opérations des problèmes supprimés

Notifier les escalades annulées

* Au moins une opération doit exister.

Ajouter **Annuler**

- Notre action a été créé



Test d'intégration de l'envoi du courriel

- Sur notre serveur web, coupons le service apache2

```
root@srvweb:/home/srvweb# systemctl stop apache2
root@srvweb:/home/srvweb# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Sat 2022-04-16 20:52:25 UTC; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 637 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 1038 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
 Main PID: 767 (code=exited, status=0/SUCCESS)

avril 16 20:52:06 srvweb systemd[1]: Starting The Apache HTTP Server...
avril 16 20:52:07 srvweb apachectl[701]: AH00558: apache2: Could not reliably determine the
avril 16 20:52:07 srvweb systemd[1]: Started The Apache HTTP Server.
avril 16 20:52:25 srvweb systemd[1]: Stopping The Apache HTTP Server...
avril 16 20:52:25 srvweb apachectl[1040]: AH00558: apache2: Could not reliably determine the
avril 16 20:52:25 srvweb systemd[1]: apache2.service: Succeeded.
avril 16 20:52:25 srvweb systemd[1]: Stopped The Apache HTTP Server.
lines 1-15/15 (END)
```

- Nous avons bien reçu un courriel nous informant du problème

