



AP4

RAPPORT DE CLÔTURE DU PROJET

LIVRABLE 2

GROUPE 10
GOMES Julien
MULLER Gaétan

Durée du projet : 06/01/2023 au 15/04/2023

Date limite de remise : Samedi 15 avril 2023

Sommaire

Sommaire	2
1. Présentation et composition du groupe	4
2. Rappel des besoins et objectifs du projet.....	4
3. Solution choisie et tableau comparatif.....	5
4. Budget / Coût du projet.....	6
5. Diagramme de Gantt	7
6. Schéma réseau	8
7. Plan d'adressage réseau	10
8. Tableau des Flux	11
Documentation technique & mode d'emploi Active Directory redondé-Windows Server 2019	12
9. Active Directory redondé - Windows Server 2019.....	12
<i>Installation de Windows Server 2019</i>	13
<i>ADDS : Installation / Configuration / DNS(GUI)</i>	18
<i>ADDS : configuration / installation / DNS :</i>	21
<i>Installation DHCP</i>	28
10. Routeur & Pare-feu – Pfsense	29
<i>Installation PfSense</i>	30
<i>Configuration PfSense</i>	34
<i>CARP – Pfsync – XML – RPC / IP virtuelle configuration / redondance</i>	38
<i>Mise en place des règles de Pare-feu.....</i>	46
<i>OpenVPN / PfSense – VPN RW</i>	46
11. OpenVPN	53
12. Messagerie – hMailServer & Thunderbird (Serveur&Client)	56
<i>Configuration de hMailServer.....</i>	59
13. Téléphonie – PBX & Linphone	64
14. Serveur de monitoring – Zabbix	70
15. Serveur WEB (eBrigade) / LAMP.....	95
<i>Installation LAMP</i>	95
<i>Installation eBrigade</i>	95

1. Présentation et composition du groupe

Le groupe se compose de GOMES Julien (Administrateur systèmes et réseaux) et de MULLER Gaétan (Administrateur systèmes et réseaux).

GOMES Julien et MULLER Gaétan sont les personnes qui s'occuperont de ce projet. Vous pouvez nous contacter via Teams ou alors sur nos adresse mail professionnel respective :

-GOMES Julien : alss-sio-sisr21-gju@ccicampus.fr

-MULLER Gaétan : alss-sio-sisr21-mga@ccicampus.fr

2. Rappel des besoins et objectifs du projet

L'objectif du projet est de permettre aux Préfectures d'améliorer leur résilience informatique en cas de crise, d'optimiser leur système d'information ainsi que l'accès à leur système d'information de l'extérieur.

Les différents besoins pour ce projet sont :

- En préfecture :

- un réseau électrique ondulé
- Redondance des routeurs et liens WAN
- Accès aux ressources du serveur eBrigade en LAN et DMZ
- Messagerie électronique fonctionnelle uniquement en LAN/VPN RW
- Serveur VoIP et logiciels de téléphonie IP uniquement en LAN/VPN RW
- L'ensemble des postes de travail sont sur Windows 10 Pro x64
- Couplage avec l'annuaire Active Directory de l'établissement (à créer).
- La cible est de 10 utilisateurs en simultanés

En connexion à distance :

- Connexion à distance au réseau informatique de la Préfecture en mode « OpenVPN Road Warrior »
- Une fois la connexion VPN RW initialisée, il sera possible de :
- Envoi/Réception de courriers électroniques
- Appels sur téléphone IP via softphone
- L'accès et l'utilisation du logiciel eBrigade + accès en mode dégradé via DMZ

Objectifs attendus :

1. Mise en œuvre d'une haute disponibilité de routeurs et liaison Internet redondée (2 routeurs / 2 accès Internet)
2. Mise en œuvre de 2 serveurs Active Directory (Principal et Secondaire)
3. Mise en œuvre d'1 serveur de téléphonie IpBX et déploiement d'un client softphone
4. Mise en œuvre d'1 serveur de messagerie et déploiement d'un client de messagerie -> Utilisation des comptes de l'Active Directory
5. Mise en œuvre d'1 serveur de supervision et de monitoring
 - Supervision de la disponibilité des routeurs et serveurs
 - Monitoring et historique des indisponibilités des routeurs et serveurs
 - Alerte par mail aux administrateurs en cas de panne
6. Mise en œuvre d'une solution de VPN RW (Road Warrior)-> Utilisation des comptes de l'Active Directory
 - Lorsque la connexion VPN est établie, l'accès aux ressources et outils est possible sinon non (Téléphonie, Messagerie...)
7. Mise en œuvre d'une DMZ pour accéder au Serveur WEB E-Brigade (Avec règles de pare-feu adaptés)

3. Solution choisie et tableau comparatif

Besoin	Solution choisie argumentée	Comparaison avec une autre solution
Routeur/Pare-feu	Pfsense : <ul style="list-style-type: none">-Open Source-Fonctionnalité avancées-Interface utilisateur intuitive-support communautaire	OPNsense : <ul style="list-style-type: none">-Interface utilisateur moderne-Sécurité stricte par défaut-Support de plugin tierce
Redondance WAN	CARP/pfSync : <ul style="list-style-type: none">-Facilité de configuration-Evolutivité-fonctionnalité inclus dans pfsense	Safekit : <ul style="list-style-type: none">-Compatibilité-Facilité d'utilisation-Sécurité
VPN RW	OpenVPN : <ul style="list-style-type: none">-Flexibilité-Facilité d'utilisation-Comptabilité	OPNsense : <ul style="list-style-type: none">-Interface utilisateur moderne-Sécurité stricte par défaut-Support de plugin tierce

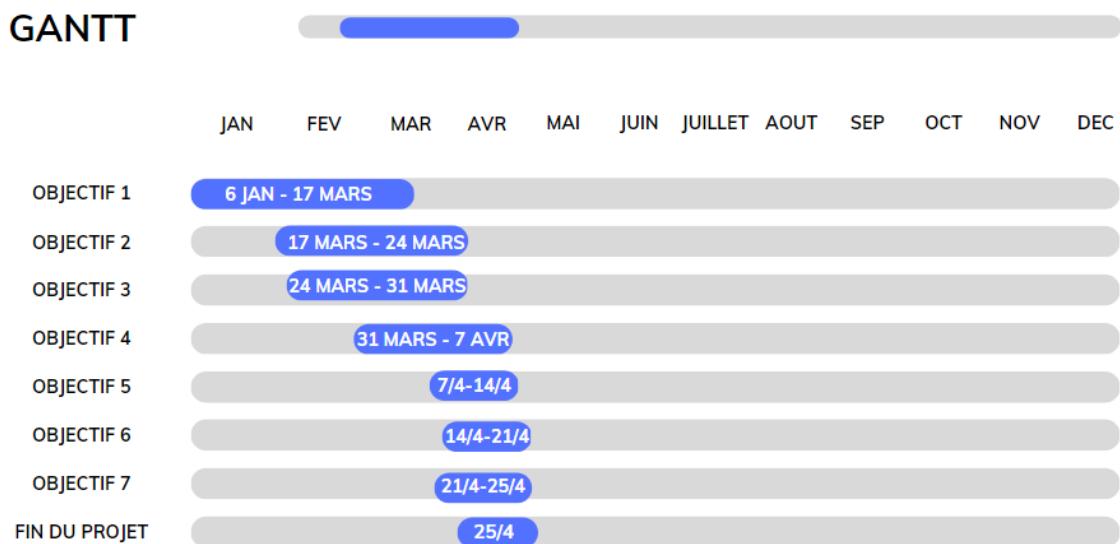
Supervision	Zabbix : -Surveillance complète -Flexibilité -Open Source	Nagios : -Open Source -Flexibilité -Extensibilité
AD DS	Windows Server 2019 Gui Active Directory : -Intégration avec les produits Microsoft -Facilité d'utilisation -Haute Disponibilité -Gestion de groupe	OpenLDAP : -Open source -Haute Performance -Interopérabilité
VOIP et Softphone	Asterisk : -Open Source -Flexibilité -Haute Qualité audio -Personnalisation	3CX : -Facilité d'utilisation -Haute qualité audio -Mobilité -Cout abordable
E-Brigade	Apache, Mysql, PHP : -Cout abordable -Flexibilité Sécurité	EasyPHP : -Open Source -Flexibilité -Sécurité
Messagerie	HmailServer : -Open source -Facilité d'installation -Gestion facile des utilisateurs -Surveillance et journalisation	Axigen : -Haute disponibilité -Gestion Facile -Flexibilité -Collaboration

4. Budget / Coût du projet

Quantité	Objets	Prix (euro)	Total (euro)
110	Heures de travail	45	4950
1	Licence CAL pour 5 utilisateurs	102,9	102,9
2	Licence windows server 2019 standard-licence-16coeur	783,09	1566,18
2	Dell PowerEdge R350-Montable sur rack-RAM 16 Go-Serveur AD	2264,25	4528,5
3	Dell PowerEdge R250-RAM 8Go-Serveur PfSense-VoIP-Asterisk_Ubuntu	1984,02	5952,06
2	Routeur sans fil Wifi Bi-Bande Asus RT-AX86U Noir	337,01	674,02
2	Cisco Catalyst 2960CX-8PC-L-commutateur-8 ports-Géré-Montable	1164,01	2328,02
12	Câble RJ45 Cat 6a	18,55	222,6
		Prix total	20 324,80 €

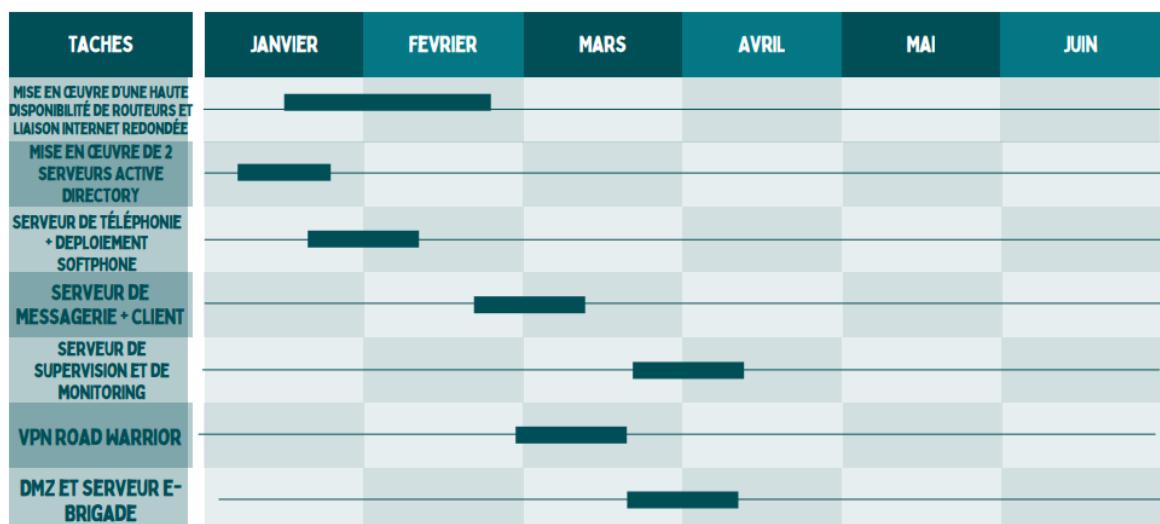
5. Diagramme de Gantt

Ancien diagramme de Gantt :



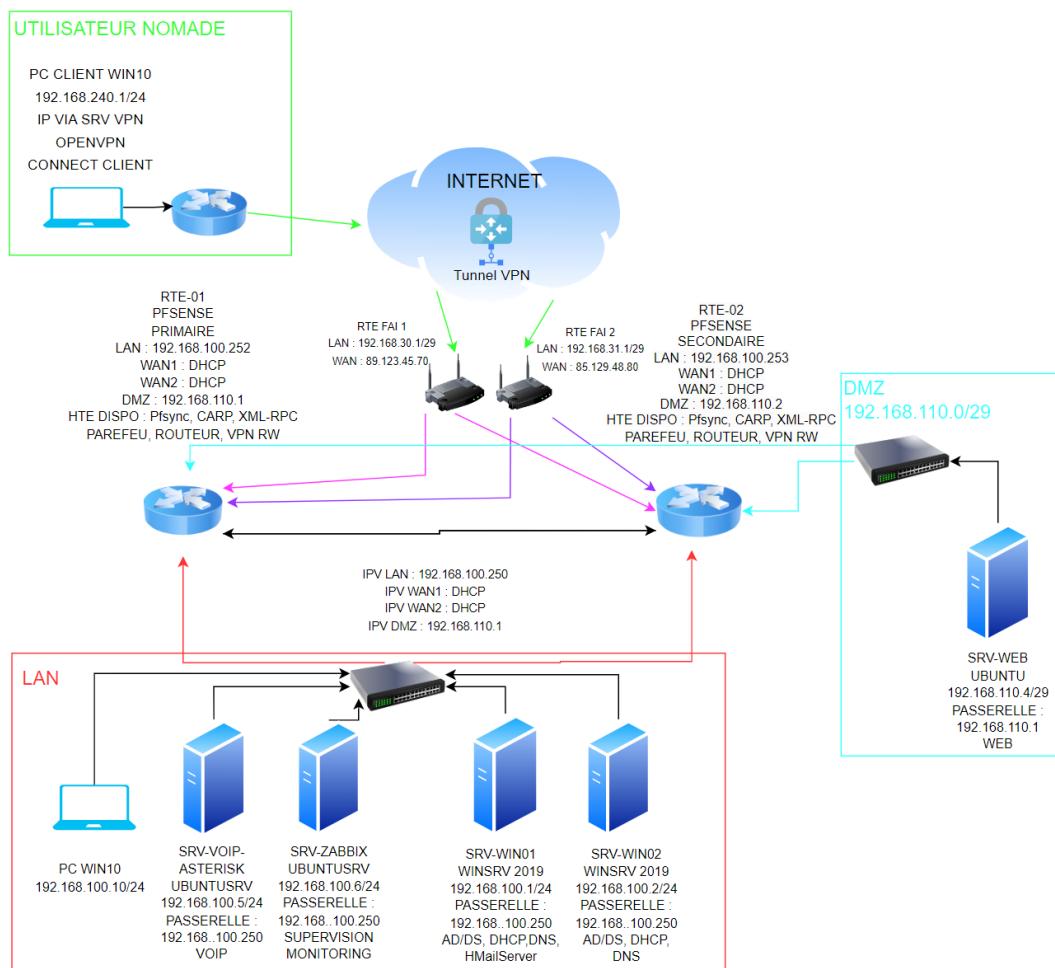
Nouveau diagramme de Gantt :

GANTT CHART

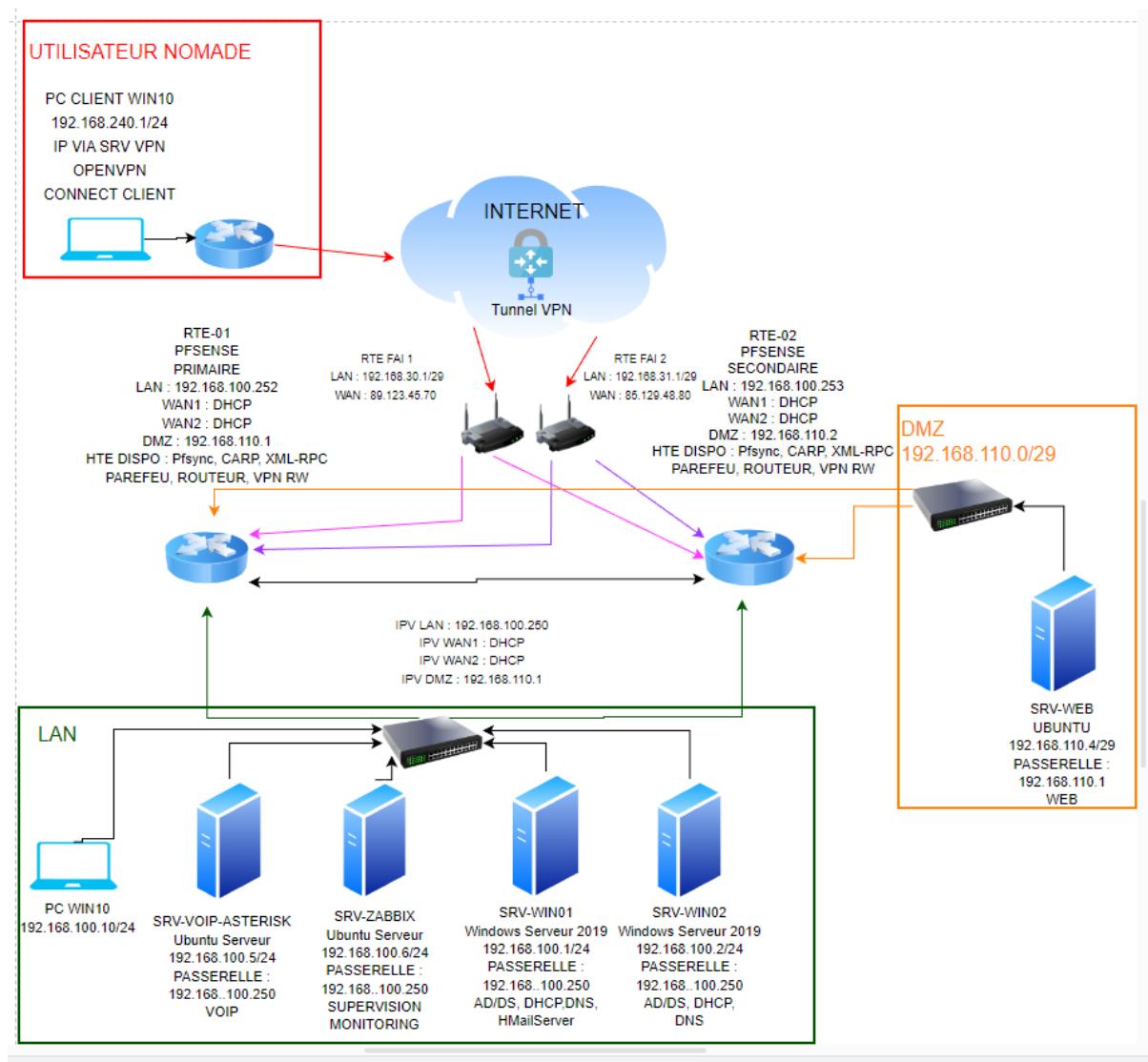


6. Schéma réseau

Ancien schéma réseau :



Nouveau schéma réseau :



7. Plan d'adressage réseau

Nom	Interface	Adresse IP	OS	Rôles
SRV-VOIP-Asterisk	VMNET1	Adresse : 192.168.100.5/24 Passerelle : 192.168.100.250	Ubuntu Server	Solution de VOIP et softphone Asterisk
SRV-ZABBIX	VMNET1	Adresse : 192.168.100.6/24 Passerelle : 192.168.100.250	Ubuntu Server	Zabbix (Supervision)
SRV-WIN01	VMNET1	Adresse : 192.168.100.1/24 Passerelle : 192.168.100.250	Windows Server 2019 Gui	AD/DS, DHCP, DNS, HmailServer
SRV-WIN02	VMNET1	Adresse : 192.168.100.2/24 Passerelle : 192.168.100.250	Windows Server 2019 Gui	AD/DS, DHCP, DNS
SRV-WEB	VMNET1	Adresse : 192.168.110.4/29 Passerelle : 192.168.110.1	Ubuntu Server	WEB
RTE-01	3 interfaces : -WAN (accès par pont) -LAN (réseau interne VMNET1) -DMZ (Réseau interne VMNET2)	Adresse WAN : DHCP Adresse LAN : 192.168.100.252 Adresse DMZ : 192.168.110.1	FreeBSD	Routeur, Pare-feu (pfSense), VPN RW (OpenVPN)
RTE-02	3 interfaces : -WAN (accès par pont) -LAN (réseau interne VMNET1) -DMZ (réseau interne VMNET2)	Adresse WAN : DHCP Adresse LAN : 192.168.100.253 Adresse DMZ : 192.168.110.2	FreeBSD	Routeur, Pare-feu (pfSense), VPN RW (OpenVPN)
PC-CLIENT-Nomade	VMNET1	Adresse : 192.168.240.1/24	WIN 10 PRO	Utilisateur Nomade

PC-Client-LAN	VMNET1	Adresse : 192.168.100.10/24	WIN 10 PRO	Utilisateur Fixe
---------------	--------	--------------------------------	------------	------------------

8. Tableau des Flux

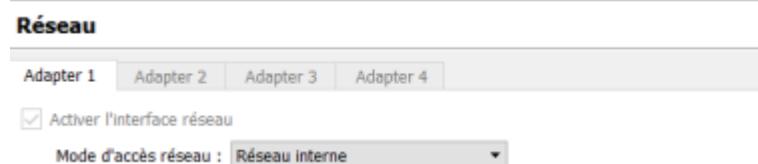
Service	Protocol	Port	Source	Destination	Description
VPN Site a Site	UDP	1194	Site distant	RTE-01/02	Autorise trafic VPN site a site
Site WEB	TCP	80	Any	SRV-WEB	Autorise trafic http vers SRV-WEB
Site WEB	TCP	443	Any	SRV-WEB	Autorise trafic https vers SRV-WEB
Audio	UDP	5004	Any	SRV-VOIP	Autorise le trafic Audio
Vidéo	TCP/UDP	5005	Any	SRV-VOIP	Autorise le trafic vidéo
Courriel	TCP	25	SRV-Messagerie	Any	Autorise trafic SMTP vers Any
Courriel	TCP	143	Any	SRV-Messagerie	Autorise le trafic IMAP vers SRV-MESSAGERIE

Documentation technique & mode d'emploi Active Directory redondé-Windows Server 2019

9. Active Directory redondé - Windows Server 2019

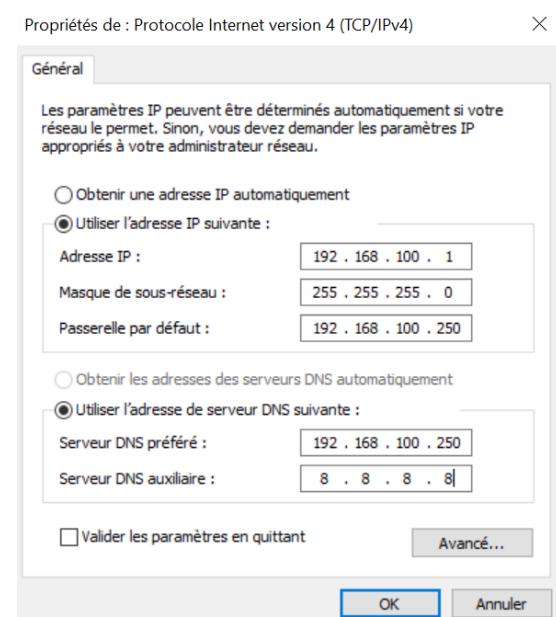
Deux VM Windows Server (1 Windows Server GUI / 1 Windows Server CORE)

Interface réseau :

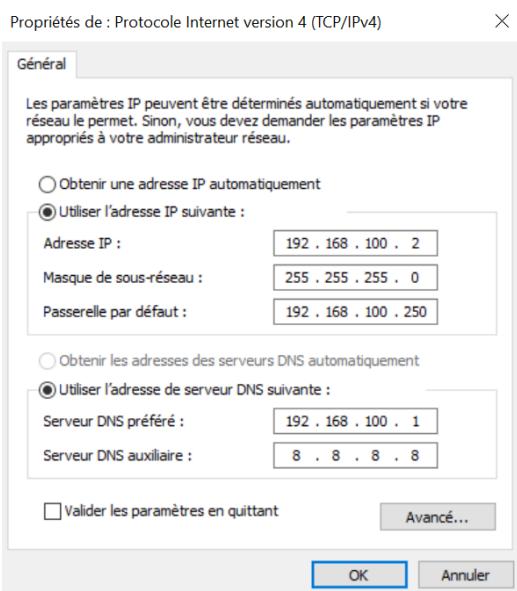


Configuration réseau des deux VM :

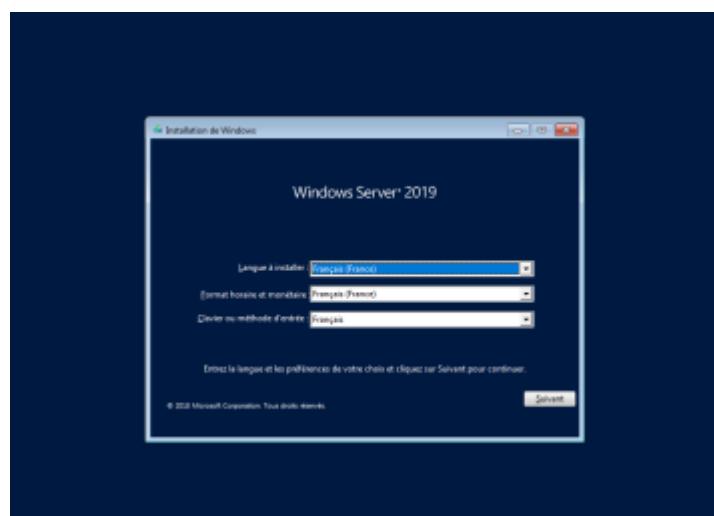
SRVWIN01 :



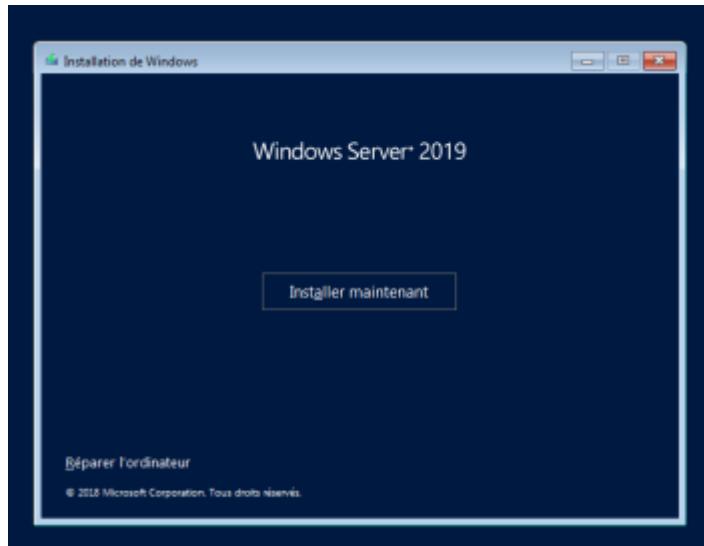
SRVWIN02 :



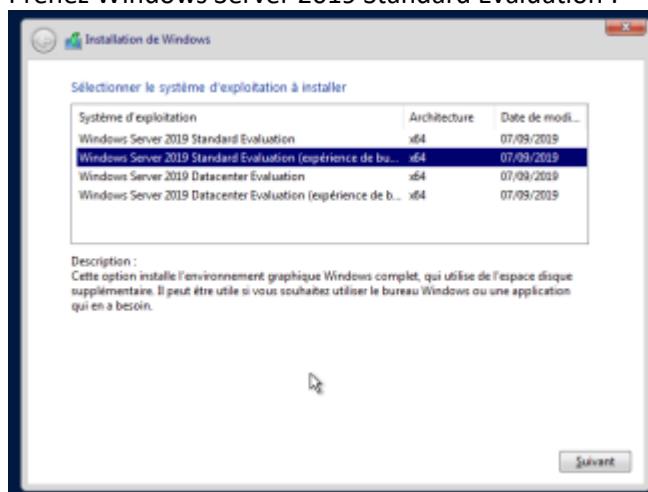
Installation de Windows Server 2019



Sélectionnez installer maintenant :



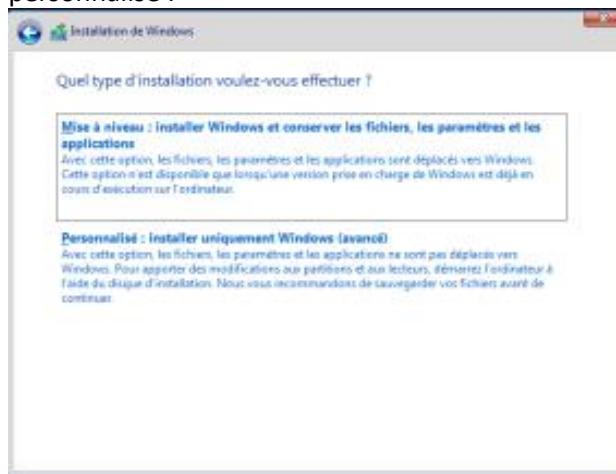
Prenez Windows Server 2019 Standard Evaluation :



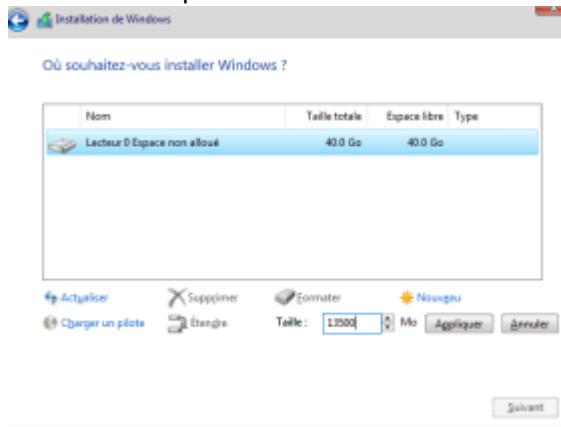
Faites suivant :

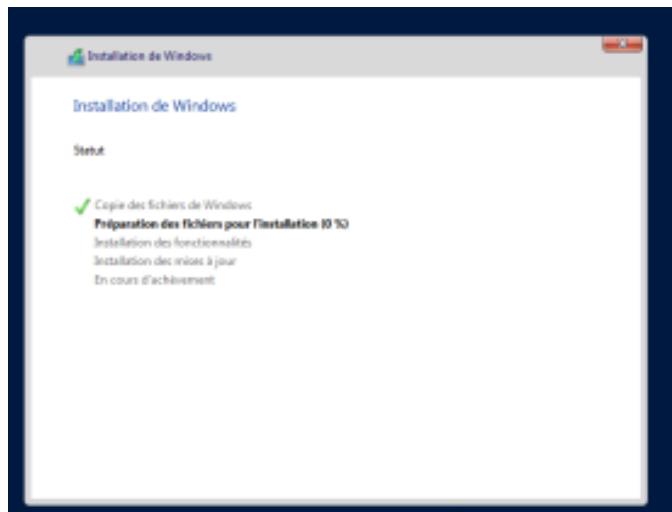


Si vous souhaitez conserver des fichiers, sélectionnez le premier et sinon je vous conseil de sélectionner le mode personnalisé :



Installer sur la partition non allouée et en faisant suivant, laissez l'installation se faire :





Une fois terminé redémarrez votre VM.

Une fois redémarré, nous allons commencer sur des bases propres donc nous allons faire la mise à jour du serveur et pour cela vous allez taper « sconfig » :

A screenshot of a Windows Command Prompt window. The title bar says "Administateur : C:\Windows\system32\cmd.exe". The command line shows "C:\Users\Administrateur>sconfig" being typed.

Tapez 6 puis entrer :

```
Administrator : 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 : ■
```

Faites T, patientez le temps que les mises à jour se recherchent et tapez T à nouveau :

```
Rechercher (T)outes les mises à jour ou uniquement les mises à jour (R)ecommandées ? T
Recherche de toutes les mises à jour applicables...
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 2022 et systèmes 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
```

Faire de même pour le second serveur :

```
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 Activé
4) Configurer l'administration à distance

5) Paramètres de Windows Update : DownloadOnly
6) Télécharger et installer les mises à jour Désactivé
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

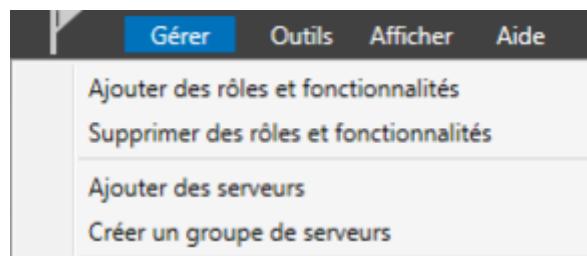
Entrez un nombre pour sélectionner une option : 2

Nom de l'ordinateur

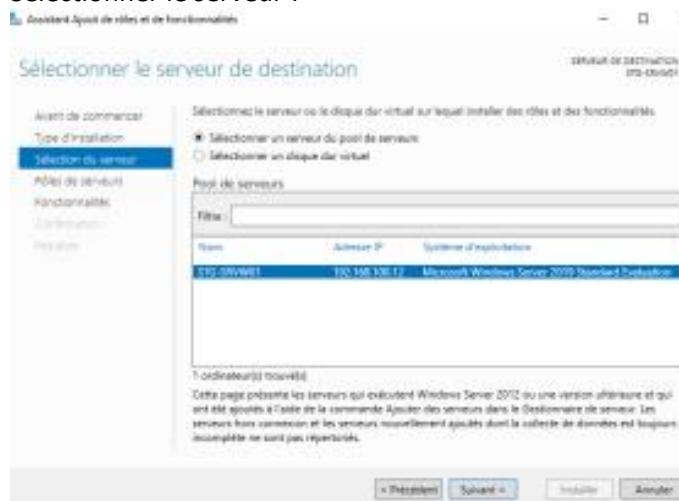
Entrez un nouveau nom d'ordinateur (Vide=Annuler) : STG-SRVWB2
```

ADDS : Installation / Configuration / DNS(GUI)

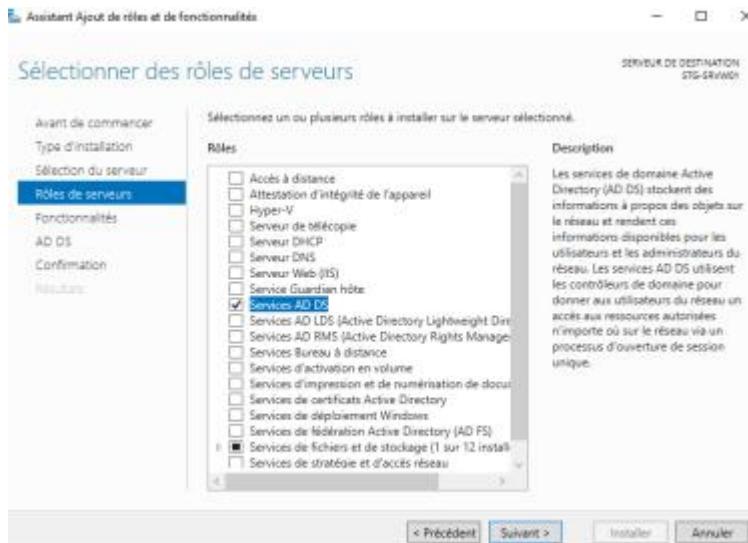
Sélectionner Gérer puis « ajouter des rôles et des fonctionnalités » :



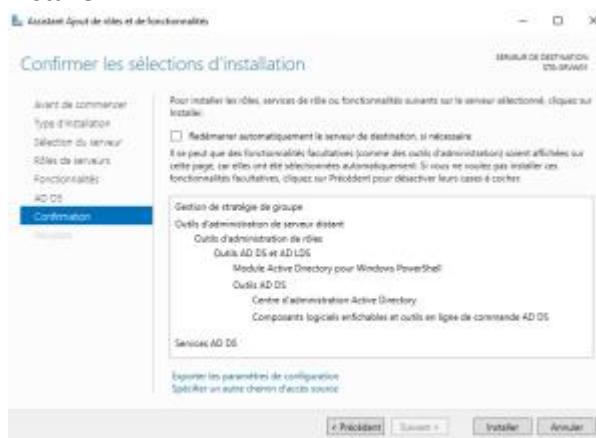
Sélectionner le serveur :



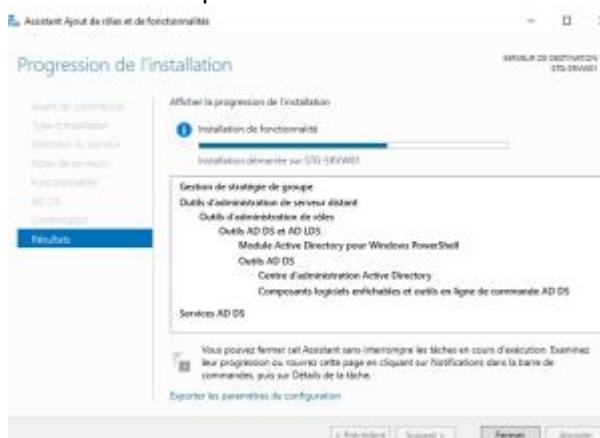
Rôle « AD DS » :



Installer :



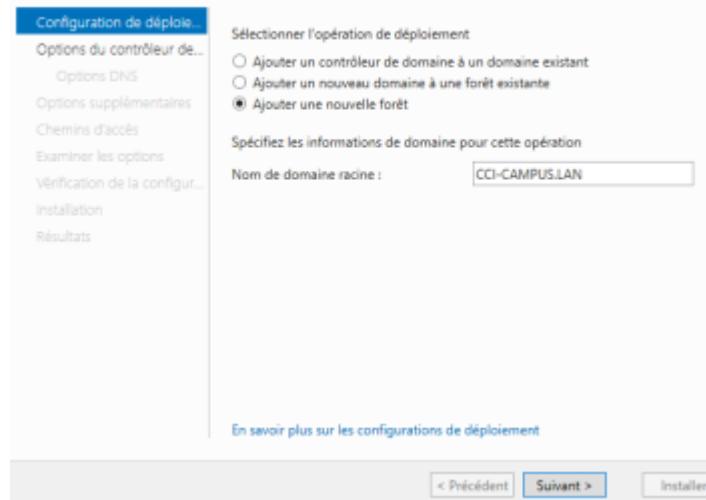
Patientez le temps de l'installation :



Une fois l'AD installé, on va configurer l'AD :

Ajouter une nouvelle forêt :

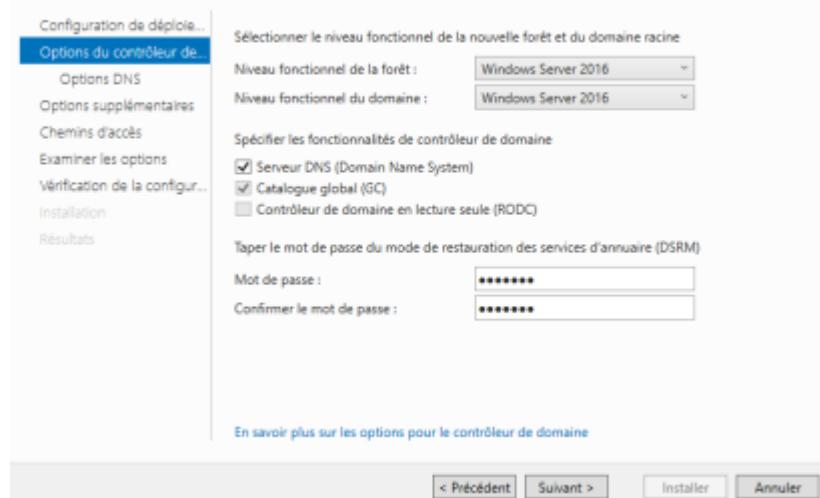
Configuration de déploiement



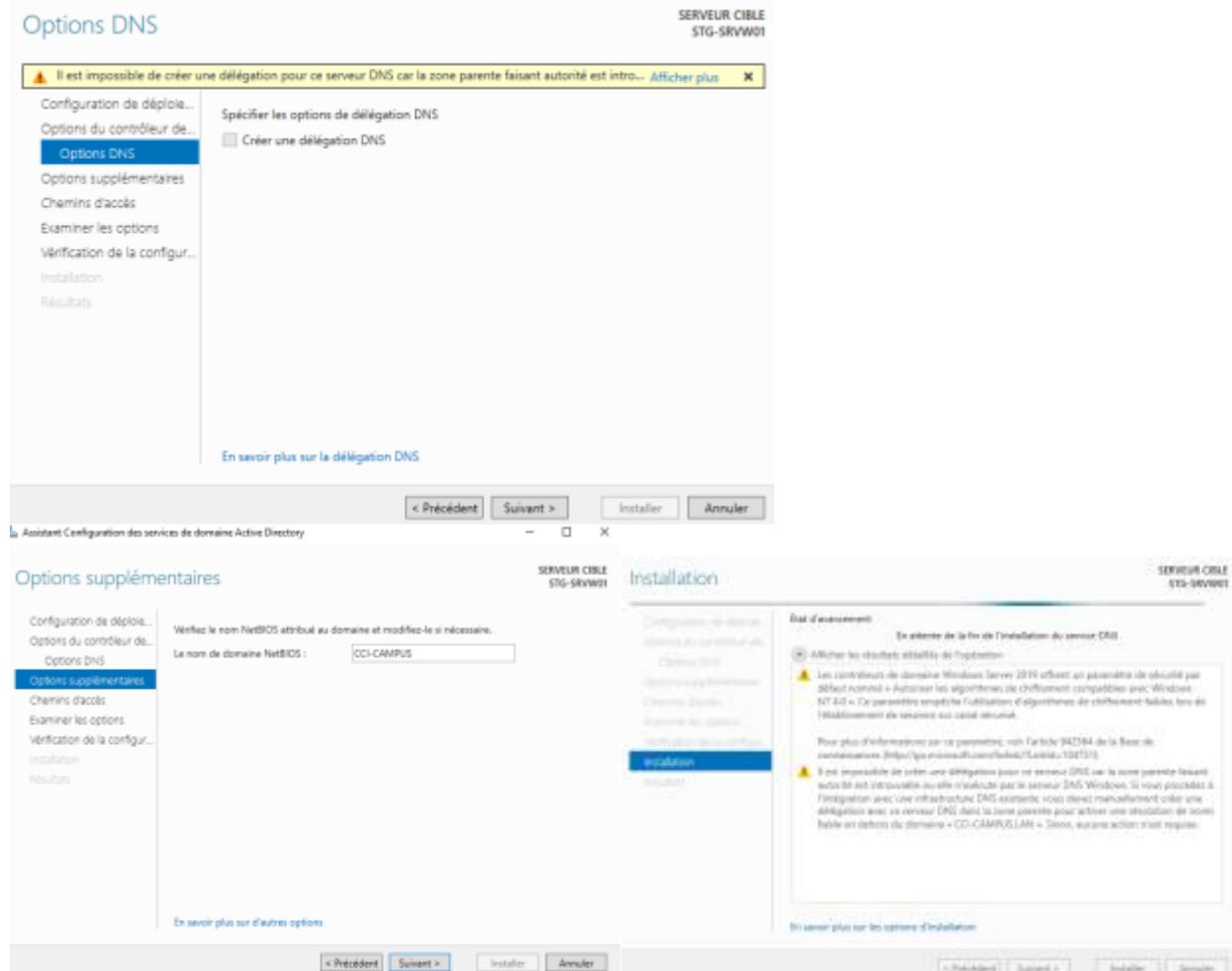
Prenez « Windows Server 2016 » et entrez un mot de passe :

Options du contrôleur de domaine

SERVEUR CIBLE
STG-SRVW01



Faites suivant plusieurs fois :



ADDS : configuration / installation / DNS :

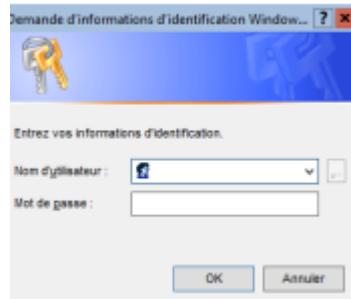
Modifier dans un premier temps le serveur DNS par l'IP du serveur principal (GUI) : (« sconfig »)



Ajouter le serveur Core dans le domaine :



Rentrer le nom d'utilisateur et le mot de passe :



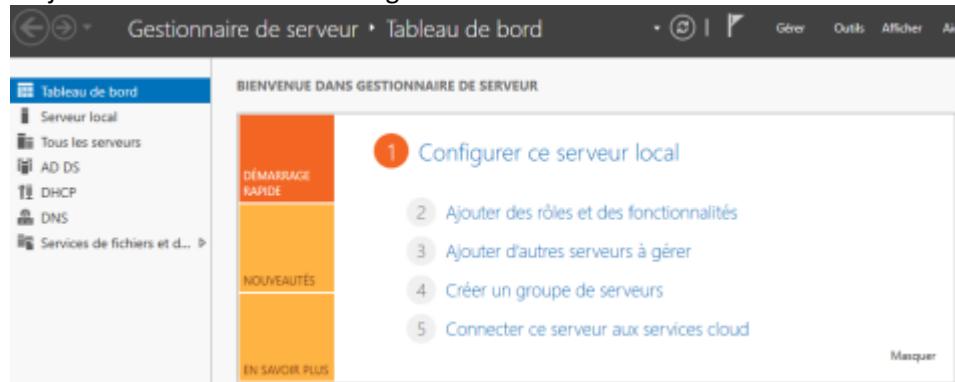
Rebootez le serveur :

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

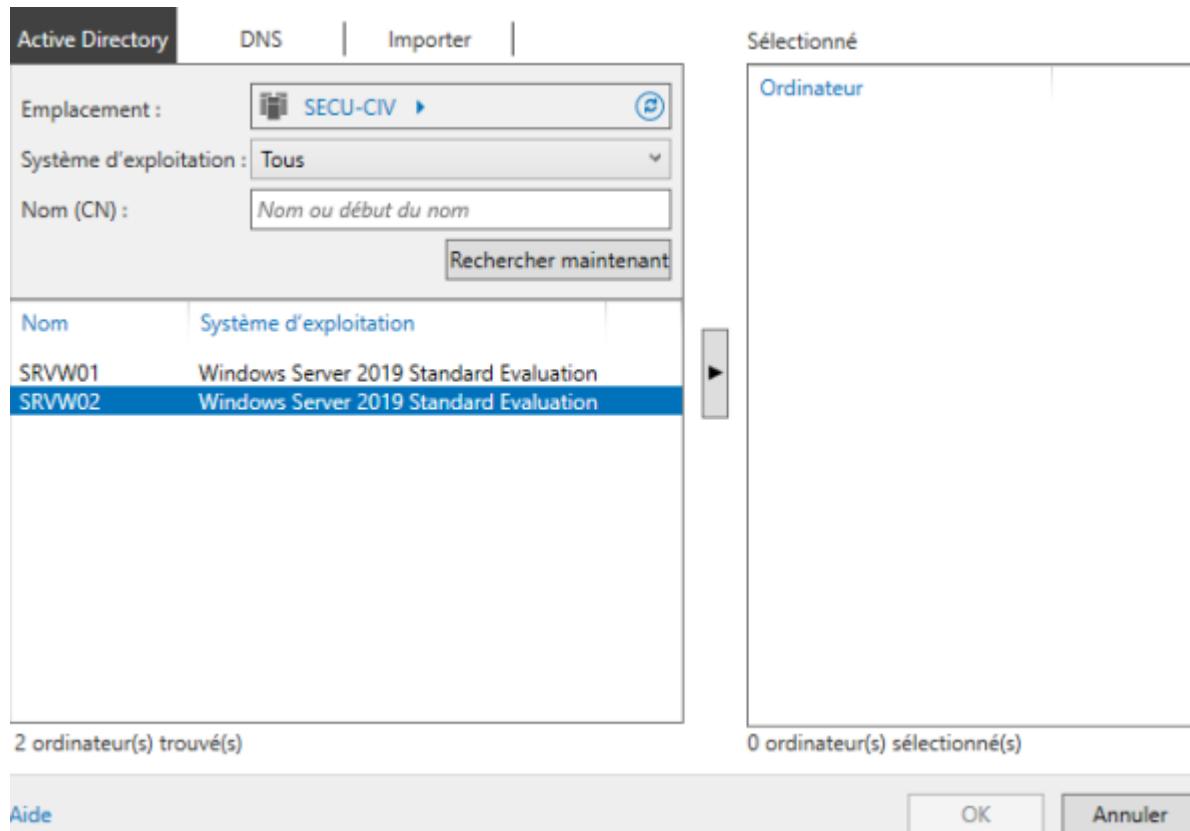
Pour ce qui est du serveur GUI, il doit apparaître dans le domaine et pour vérifier cela, dirigez-vous vers votre serveur principal et s'il apparaît, vous êtes sur la bonne voie :

Nom	Type
STG-SRVW02	Ordinateur

« Ajouter d'autres serveurs à régler » :



Sélectionner le second serveur puis faites « ok » :



Dans l'onglet « tous les serveurs », on peut voir nos deux serveurs :

The screenshot shows the "Tous les serveurs" (All Servers) page in the Server Manager. The left sidebar has a menu with "Tous les serveurs" selected. The main pane displays a table of servers with columns: Nom du serveur, Adresse IPv4, Facilité de gestion, and Dernière mise à jour. Two servers are listed: SRVW01 and SRVW02.

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour
SRVW01	192.168.100.1	En ligne - Compteurs de performances non démarré	01/04/2022 11:52:40
SRVW02	192.168.100.2	En ligne - Compteurs de performances non démarré	01/04/2022 11:55:31

Une fois cette partie réalisée, nous allons maintenant installer l'AD/DNS et promouvoir le serveur CORE en contrôleur de domaine : (manipulation faites à partir du serveur principal GUI)

Ajoutez des rôles et des fonctionnalités comme précédemment :



« Sélection du serveur », sélectionner le serveur CORE :

The screenshot shows the 'Selectionner le serveur de destination' (Select Server Destination) dialog. On the left, a sidebar lists steps: 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 'SERVEUR DE DESTINATION SRVW02.SECU-CIV.LAN'. It contains instructions: 'Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.' Below this are two radio buttons: '(.) Sélectionner un serveur du pool de serveurs' (selected) and '() Sélectionner un disque dur virtuel'. A 'Pool de serveurs' table follows, with a 'Filtre:' input field above it. The table has columns: Nom, Adresse IP, and Système d'exploitation. It lists two entries: 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).

Rôles AD DS puis faire suivant jusqu'à l'installation :

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
SRVW02.SECU-CIV.LAN

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

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

<input type="checkbox"/> Accès à distance	Description
<input type="checkbox"/> Attestation d'intégrité de l'appareil	Les services de domaine Active
<input type="checkbox"/> Hyper-V	Directory (AD DS) stockent des
<input type="checkbox"/> Serveur DHCP	informations à propos des objets sur
<input type="checkbox"/> Serveur DNS	le réseau et rendent ces
<input type="checkbox"/> Serveur Web (IIS)	informations disponibles pour les
<input type="checkbox"/> Service Guardian hôte	utilisateurs et les administrateurs du
<input checked="" type="checkbox"/> Services AD DS	réseau. Les services AD DS utilisent
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directo	les contrôleurs de domaine pour
<input type="checkbox"/> Services AD RMS (Active Directory Rights Manageme	donner aux utilisateurs du réseau un
<input type="checkbox"/> Services Bureau à distance	accès aux ressources autorisées
<input type="checkbox"/> Services d'activation en volume	n'importe où sur le réseau via un
<input type="checkbox"/> Services d'impression et de numérisation de documen	processus d'ouverture de session
<input type="checkbox"/> Services de certificats Active Directory	unique.
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (1 sur 12 installé(s))	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	
<input type="checkbox"/> Windows Deployment Services	

< >

< Précédent Suivant > Installer Annuler

Progression de l'installation

SERVEUR DE DESTINATION
SRVW02.SECU-CIV.LAN

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

Afficher la progression de l'installation.

1 Installation de fonctionnalité

Installation démarrée sur SRVW02.SECU-CIV.LAN

Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell

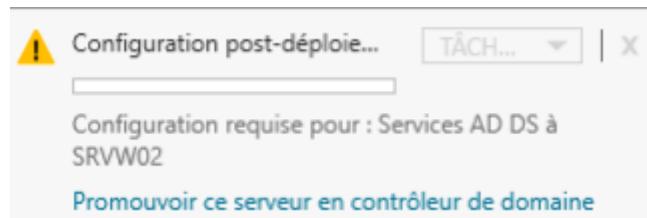
Services AD DS

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler

Une fois terminée, promouvoir le contrôleur de domaine :

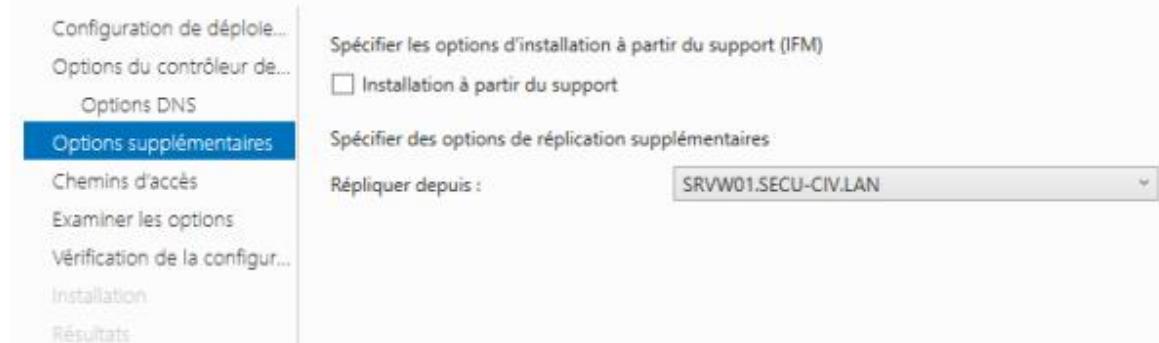


Dans configuration de déploiement, veuillez sélectionner la première option, rentrer votre nom de domaine et faites « modifier » :



Faites suivant et renseignez le mot de passe demandé

Dans « option supplémentaire » cliquez sur « tout contrôleur de domaine et sélectionner le serveur principal GUI :



Allez jusqu'au bout en cliquant sur suivant et faites « installer » :

Installation

SERVEUR CIBLE
SRVW02.SECU-CIV.LAN

Configuration de déploiement

Options du contrôleur de domaine

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configuration

Installation

Résultats

État d'avancement

Configuration du service Serveur DNS en cours sur cet ordinateur...

Afficher les résultats détaillés de l'opération

⚠️ Les contrôleurs de domaine Windows Server 2019 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

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

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

Sayez, nous venons de mettre le serveur secondaire en contrôleur de domaine donc notre AD/DNS de notre serveur principal est maintenant redondé dessus :

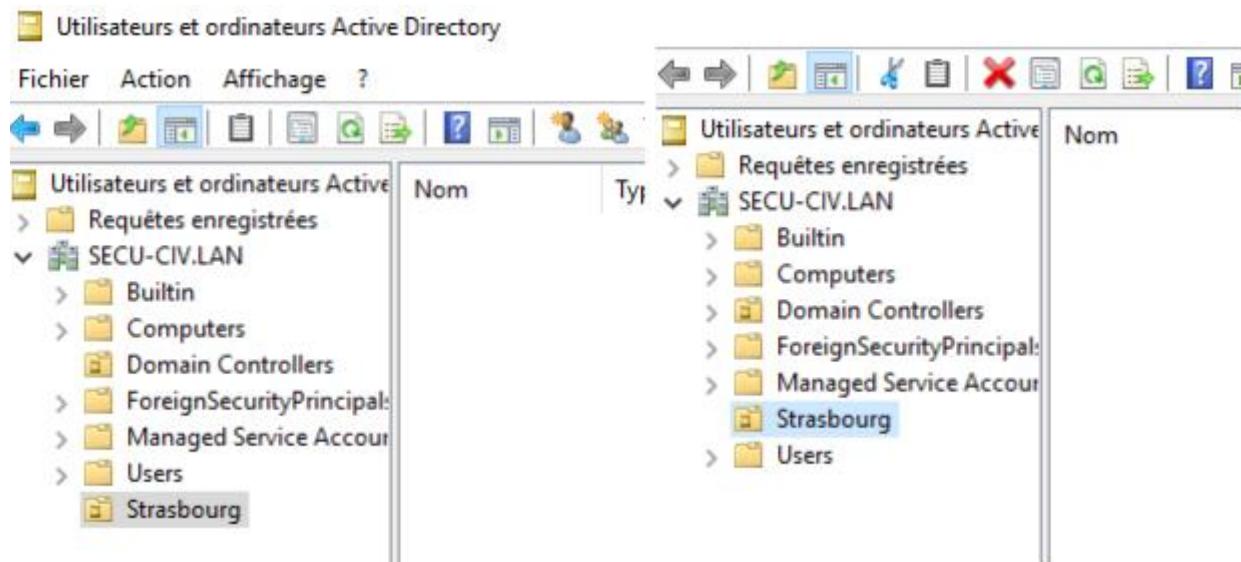
Quand on crée l'UO « Strasbourg » sur notre serveur principal, on peut voir qu'il apparaît aussi sur le serveur secondaire : (voir images ci-dessous)

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom Type Type de contrôleur Site Description

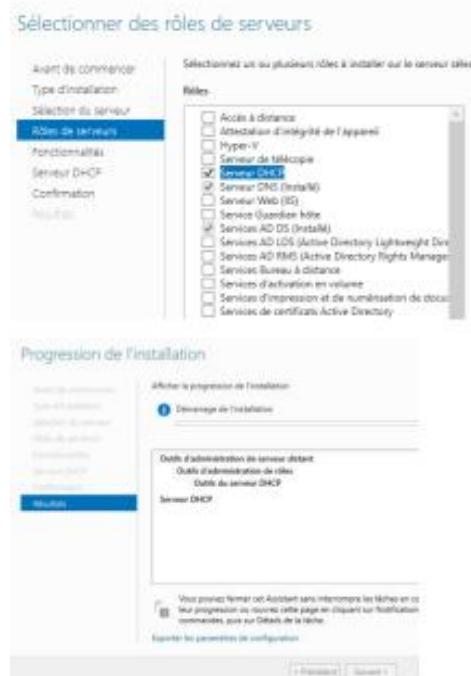
Nom	Type	Type de contrôleur	Site	Description
SRVW01	Ordinateur	GC	Default-First-Site	
SRVW02	Ordinateur	GC	Default-First-Site	



Installation DHCP

Une fois notre AD et notre DNS créé, nous allons passer à l'installation de notre DHCP :

Sélectionner le rôle « serveur DHCP » et installez le :



Faites terminer la configuration DHCP :



On peut à présent installer DHCP sur notre serveur CORE depuis le serveur GUI :

La seule étape que nous allons devoir réaliser en plus que celle d'avant est d'indiquer le bon nom de serveur :

Autorisation

Description Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

Autorisation

Résumé

Utiliser les informations d'identification de l'utilisateur suivant
Nom d'utilisateur : CCI-CAMPUS\Administrateur

Utiliser d'autres informations d'identification
Nom d'utilisateur : Spécifier...

Ignorer l'autorisation AD

< Précédent Suivant > Valider Annuler

10. Routeur & Pare-feu – PfSense

3 interfaces réseaux requises : WAN, LAN, DMZ :

Voici les IP de nos 2 routeurs :

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

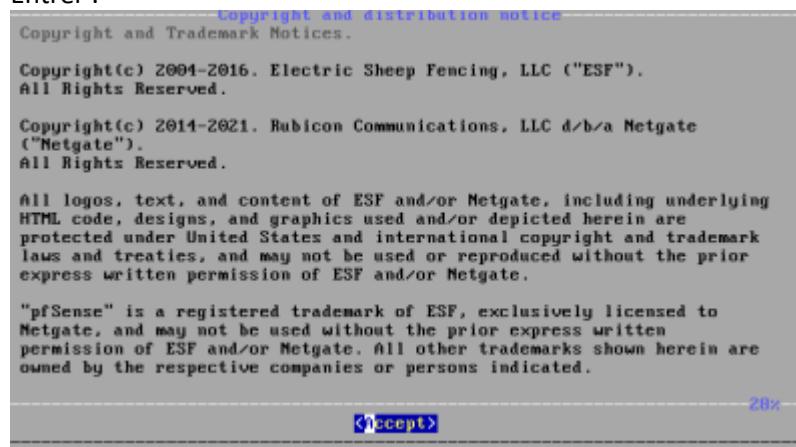
Routeur 1 :

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

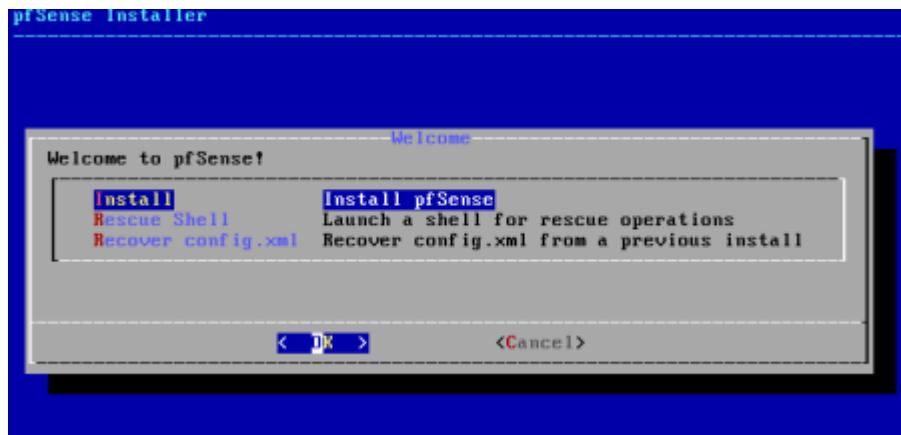
Routeur 2 :

Installation PfSense

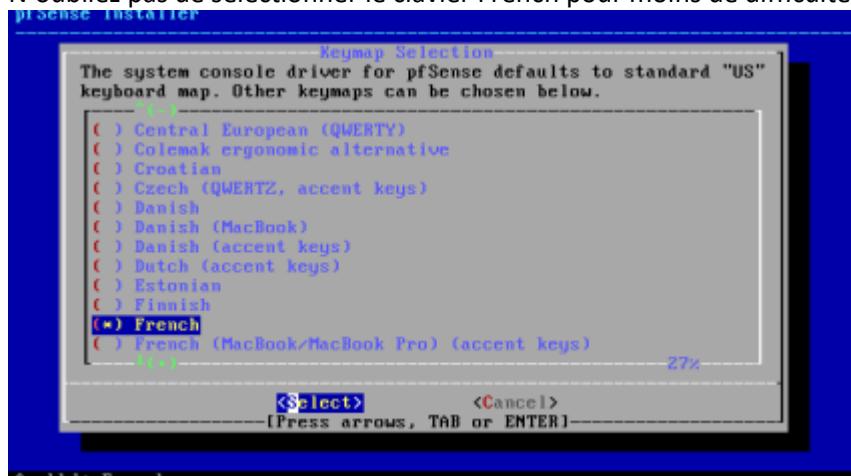
Entrer :



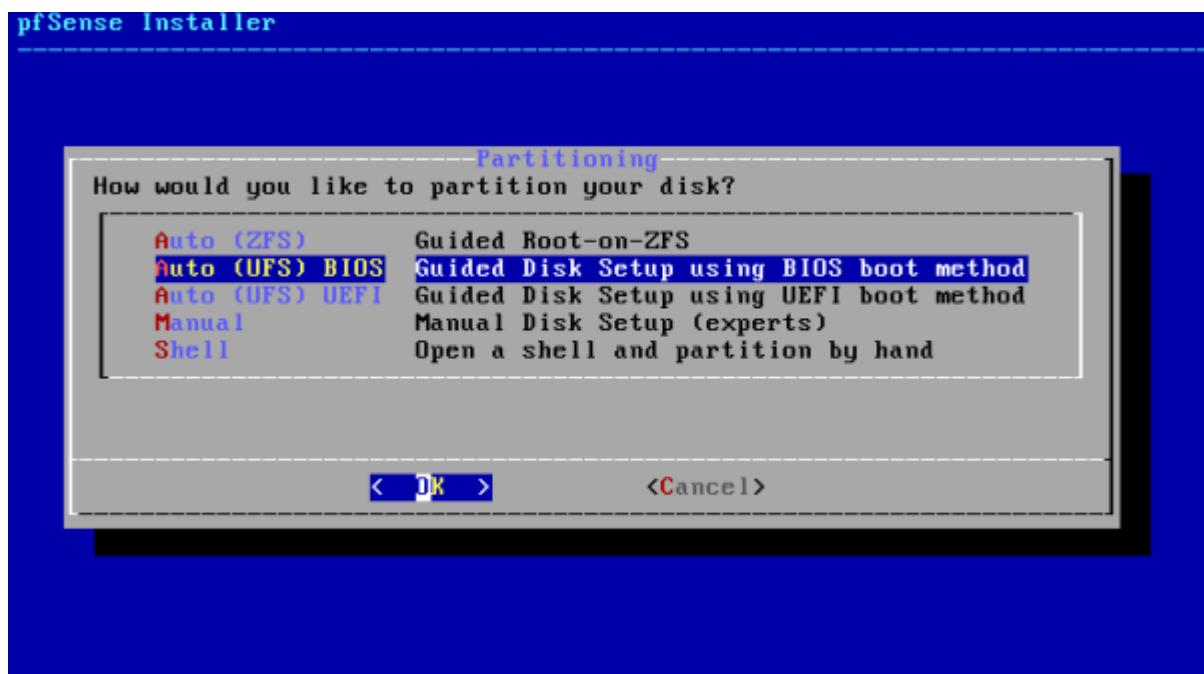
Sélectionner Install et faites entrer :



N'oubliez pas de sélectionner le clavier French pour moins de difficulté par la suite :



Auto (UFS) :



Faites « No » :



Faites reboot et si l'installation repart du début, veuillez expulser l'iso de votre machine virtuelle :



Une fois reboot, vous devrez attendre sur cette page :

```
.... 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 LAN interface...done.  
Configuring WAN interface...■
```

Et arriver sur celle là :

```
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
```

Configuration PfSense

Entrer option 1 :

```
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]? █
```

Une fois fait, tapez 2 dans les options. Cela va nous permettre de configurer les cartes de nos routeurs :

```
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█
```

Entrer l'adresse LAN pour commencer : (voir schéma réseau)

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

Masque de sous réseau : 24

```
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█
```

Entrer :

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

Entrer à nouveau :

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

Faites « n » pour les deux prochaines étapes :

```
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 █
```

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

Depuis notre client windows 10, nous pouvons maintenant accéder à la page web :

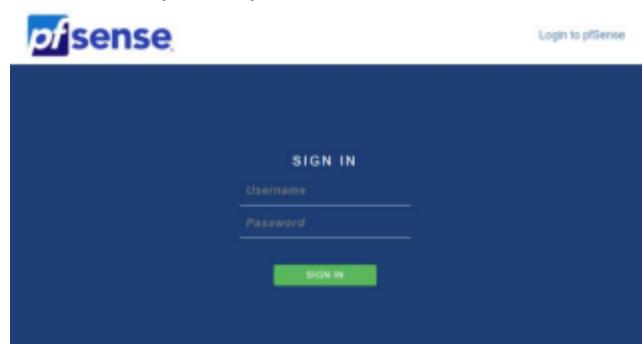
Attention, pensez à mettre votre VM client dans le même réseau local sinon cela ne fonctionnera pas :

```
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:
```

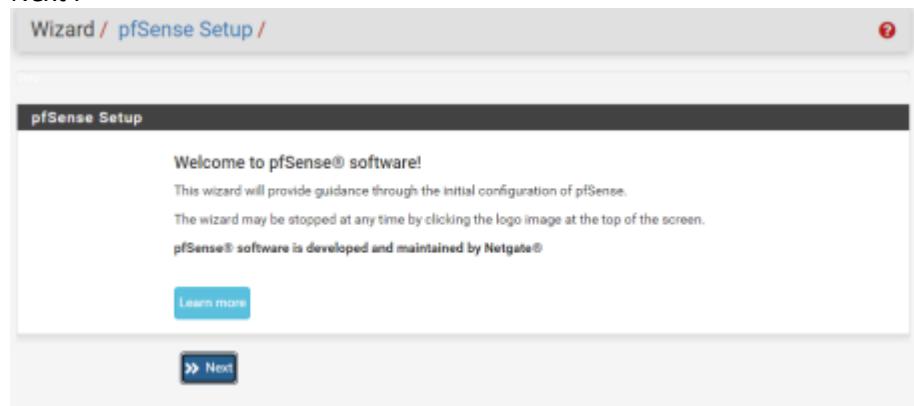
Dans notre VM client windows, voici la page sur laquelle nous devons atterrir lorsque nous rentrons l'adresse IP :

Entrer le Login : admin

Et le mot de passe : pfSense



Next :



Renseignez les informations demandés :

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
EXAMPLE: myserver

Domain: 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: [empty]

Secondary DNS Server: [empty]

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

[» Next](#)

Timezone :

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

Wan en DHCP et masque 32 :

Configure WAN Interface

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

Selected Type: DHCP

Static IP Configuration

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

Désactiver les deux options sinon le trafic sur l'interface wan va être bloqué puis next :

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.

Pour la configuration du LAN, il y a juste à faire next :

Configure LAN Interface

Vous pouvez modifier votre identifiant 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

Faites « reload »

Reload configuration

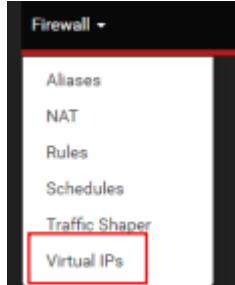
Click 'Reload' to reload pfSense with new changes.

>> Reload

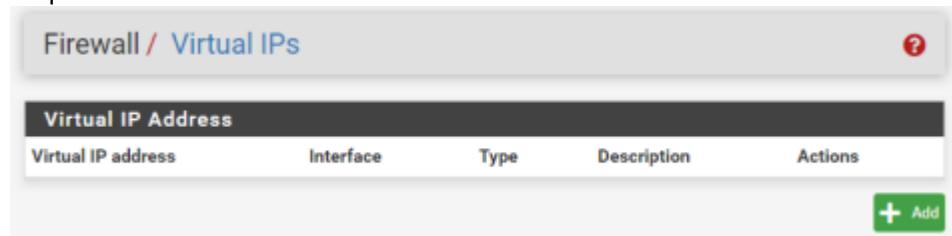
Nous venons de terminer la configuration de Pfsense de notre serveur principal.
Il faut réaliser la même chose en modifiant juste les IP.

CARP – Pfsync – XML – RPC / IP virtuelle configuration / redondance

Sur le routeur principal et secondaire : Firewall -> Virtual IPs



Cliquez sur « Add » :



Faire une IP virtuelle identique sur les deux routeurs :

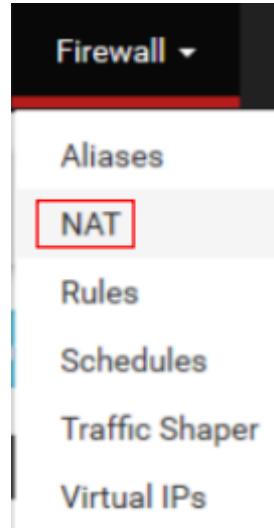
A detailed screenshot of the 'Edit Virtual IP' configuration form. The form has the following fields:

- Type:** Radio buttons for 'IP Alias' (unchecked), 'CARP' (checked), 'Proxy ARP' (unchecked), and 'Other' (unchecked).
- Interface:** A dropdown menu set to 'LAN'.
- Address type:** A dropdown menu set to 'Single address'.
- Address(es):** An input field containing '192.168.100.254' with a subnet mask of '/24'.
- Virtual IP:** Two input fields for the virtual IP address, both containing '.....'.
- Password:** A field labeled 'Enter the VHID group password.' followed by a 'Confirm' field.
- VHID Group:** A dropdown menu set to '1'.
- Advertising frequency:** Two dropdown menus for 'Base' (set to '1') and 'Skew' (set to '0'). A note below explains that the frequency determines the master machine.
- Description:** An input field containing 'IPV LAN'.

Voilà ce que ça donne une fois créée :

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

Ensuite nous allons aller dans Firewall -> NAT :



Sélectionner « Hybrid Outbound NAT » puis « save » :

Port Forward 1:1 Outbound NPt

Outbound NAT 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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disable Outbound NAT rule generation. (No Outbound NAT rules)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

« Add » pour créer une nouvelle règle :

Mappings									
	Source		Destination		NAT	NAT	Static		
<input type="checkbox"/>	Interface	Source	Port	Destination	Port	Address	Port	Port	Description Actions
								Add Add Delete Save	

Suivez les indications sur l'image ci-dessous :

Edit Advanced Outbound NAT Entry

Disabled Disable this rule

Do not NAT Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface 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.

Not
Invert the sense of the destination match.

Voici ce que vous devez obtenir :

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

Vous pouvez réaliser la même chose pour les deux autres interfaces tout en adaptant vos paramètres avec ceux requis.

Une fois que vous êtes arrivé à cette étape, nous allons synchroniser les deux routeurs et mettre en place de la haute disponibilité grâce à XML-RPC et Pfsync.

Allez sur votre serveur principal et aller dans System -> High Avail Sync

Sélectionner la case puis mettez « LAN » puis l'IP du serveur secondaire :

Rentrer votre ID and PASSWORD de Pfsense :

Remote System Username	<input type="text" value="admin"/>	Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	<input type="password" value="....."/>	<input type="password" value="....."/>	Confirm
Synchronize admin	<input type="checkbox"/> 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.		

Sélectionner toutes les cases si cela n'est pas fait :

Select options to sync

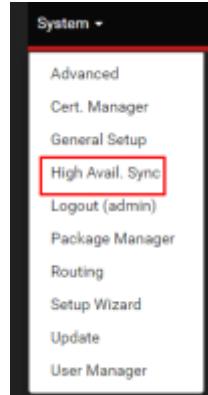
- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- 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

Faites « Save » et votre configuration est terminée.

Maintenant sur le routeur secondaire : System -> High Avail Sync



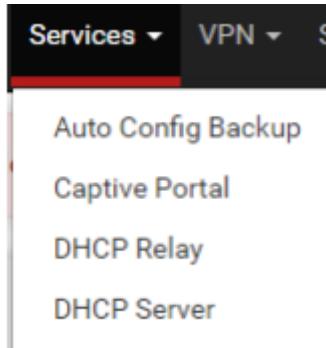
Sélectionner la case puis LAN puis mettez l'adresse IP du routeur principal :

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

La seconde configuration est terminée.

Maintenant nous allons faire le DHCP sur PfSense et mettre l'IPV par défaut :
Service -> DHCP Server :



Vous aurez juste à l'activer si ce n'est pas déjà fait et dans la « Gateway », vous mettrez l'IP du LAN.

Nous allons pouvoir à présent tester notre IP virtuelle : (192.168.100.254/24)

IP LAN RTE 1 : 192.168.100.253/24

IP LAN RTE 2 : 192.168.100.252/24

La passerelle est bien notre IP virtuelle lorsque nous faisons un ipconfig /all sur notre réseau LAN :

```
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
```

Maintenant si notre serveur principal tombe, il faut que le secondaire prenne le relais et nous allons donc réaliser un petit test pour prouver cela :

Ipconfig /release -> ipconfig /renew

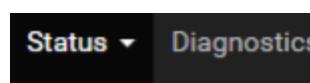
Une fois avoir fait ces deux étapes, refaire un ipconfig /all

On constate bien que c'est notre routeur secondaire qui a pris le relais :

```
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
```

Rendons-nous à nouveau dans PfSense et allons dans Status -> CARP



Captive Portal

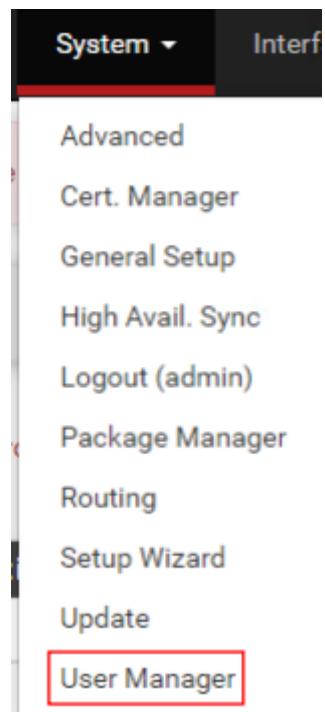
CARP (failover)

Dashboard

Dans CARP nous pouvons distinguer le statut de chacun de nos routeurs

Routeur 1 :

Routeur 2 :



Dirigez vous vers Authentification Servers et faites « Add » :



Une fois que vous êtes sur cette partie, suivez les instructions et entrer les paramètres en fonction de votre projet. Voici un exemple de mon projet :

Server Settings

- Descriptive name:** SECU-CIV.LAN
- Type:** LDAP

LDAP Server Settings

- Hostname or IP address:** 192.168.100.1
- Port value:** 389
- Transport:** Standard TCP
- Peer Certificate Authority:** Global Root CA List
- Protocol version:** 3
- Server Timeout:** 25

Search scope: Level
Entire Subtree

Base DN: DC=SECU-CIV,DC=LAN

Authentication containers: CN=Users,DC=SECU-CIV,DC=LAN

Extended query: Enable extended query

Bind anonymous: Use anonymous binds to resolve distinguished names

Bind credentials: Administrateur@SECU-CIV.LAN

User naming attribute: samAccountName

Group naming attribute: cn

Group member attribute: memberOf

RFC 2307 Groups: 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).

Group Object Class: posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication

Group DN: 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

UTF8 Encode: UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

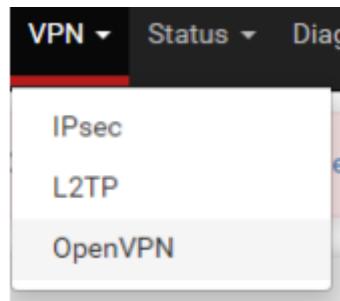
Username Alterations: Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.

Allow unauthenticated bind: 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.

Passons au serveur VPN

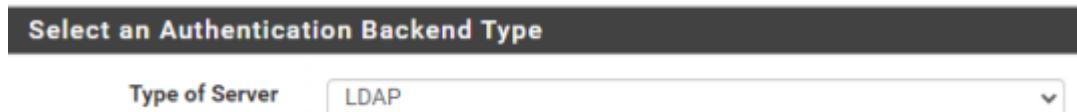
Allez dans VPN->OpenVPN



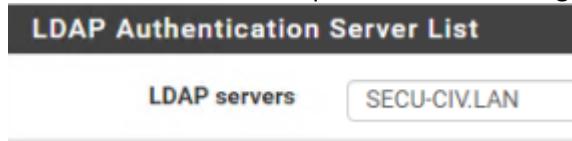
Sélectionner « Wizards » :



Choisir « LDAP » :



Prendre le serveur LDAP que nous avons configuré :



Configuration du CA :

A screenshot of a 'Create a New Certificate Authority (CA) Certificate' form. The fields include:

- Descriptive name:** openvpn
- Key length:** 2048 bit
- Lifetime:** 3650 days
- Country Code:** FR
- State or Province:** Alsace
- City:** Strasbourg

Below each field, there is a brief description of its purpose.

Create a New Server Certificate	
Descriptive name	openvpn_cert
A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."	
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	398
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
Country Code	FR
Two-letter ISO country code (e.g. US, AU, CA)	
State or Province	Alsace
Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).	
City	Strasbourg
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).	
General OpenVPN Server Information	
Interface	WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Protocol	UDP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Local Port	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	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.	

A la suite de ces indications, mettre l'adresse du VPN et celle du réseau LAN que nous voulons atteindre :

Tunnel Network	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	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.	

Cocher les deux cases :

The screenshot shows the 'Firewall Rule Configuration' step of the OpenVPN setup wizard. It includes sections for 'Traffic from clients to server' and 'Traffic from clients through VPN'. In the 'Traffic from clients to server' section, the 'Firewall Rule' checkbox is checked. In the 'Traffic from clients through VPN' section, the 'OpenVPN rule' checkbox is also checked.

Une fois cette étape terminée, la configuration est aboutie.
Voici les différentes règles que nous venons de créer

OpenVPN :

The screenshot shows the 'Rules (Drag to Change Order)' table. There are two entries:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4	*	*	*	*	*	none		OpenVPN VPN SSL OpenVPN wizard	

WAN :

The screenshot shows the 'WAN' rules table. There is one entry:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4	*	*	WAN address	1194	*	none		OpenVPN VPN SSL OpenVPN wizard	

Un outil nous sera indispensable pour la suite et nous allons le télécharger dans :
System -> Package Manager

The screenshot shows the 'System' menu with the 'Interfaces' tab selected. A red box highlights the 'Package Manager' option in the list of links.

- System ▾
- Interfaces
- Advanced
- Cert. Manager
- General Setup
- High Avail. Sync
- Logout (admin)
- Package Manager

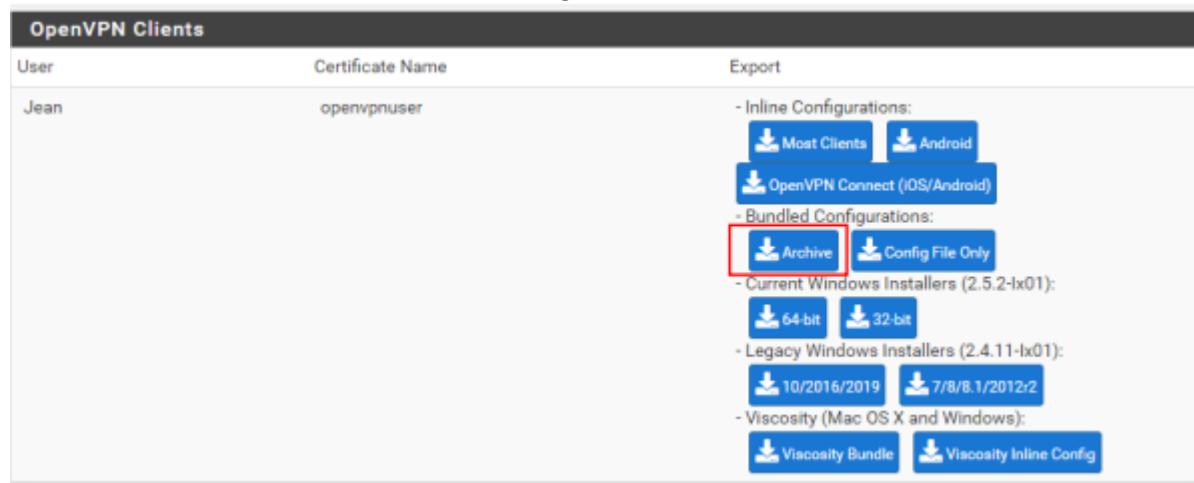
Télécharger openvpn-client-export -> Install -> Confirm

Une encoche verte apparaît à gauche quand il est bien 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

Dans VPN -> OpenVPN -> Client Export

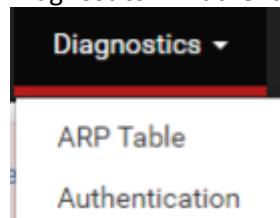
Selectionner « Archive » dans « Bundled Configurations »



The screenshot shows the 'OpenVPN Clients' configuration page. In the 'Export' section, there are several download options: 'Inline Configurations' (Mobile Clients, Android, OpenVPN Connect), 'Bundled Configurations' (Archive, Config File Only, both highlighted with a red box), 'Current Windows Installers' (64-bit, 32-bit), 'Legacy Windows Installers' (10/2016/2019, 7/8/8.1/2012/2), and 'Viscosity (Mac OS X and Windows)' (Viscosity Bundle, Viscosity Inline Config).

Récupérer le dossier.

On va maintenant faire un diagnostic de LDAP et on va se rendre dans
Diagnostics -> Authentification



The screenshot shows the 'Diagnostics' menu with a dropdown arrow. Below it, the 'Authentication' option is visible.

Si on renseigne les identifiants d'un des utilisateurs dans le domaine, un message vert de succès doit apparaître :



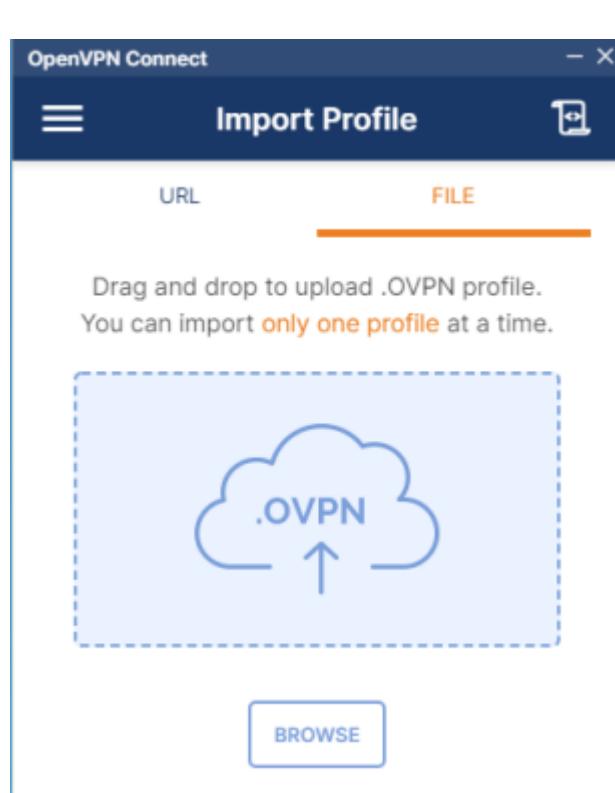
The screenshot shows a green message box containing the text: 'User Anakin authenticated successfully. This user is a member of groups:'

11. OpenVPN

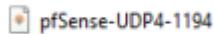
Sur notre client, on va télécharger OpenVPN Connect :



Vous vous souvenez de l'archive que nous avons récupérée ? Eh bien nous allons l'utiliser pour cette étape :
File -> Browse



Mon fichier :



Ensuite renseigner les informations nécessaires :

OpenVPN Connect - x

Access Server Profiles Configuration

IMPORT FROM SERVER IMPORT FROM FILE

You have no profiles yet.

Access Server Hostname _____

Title _____

Port (optional) _____

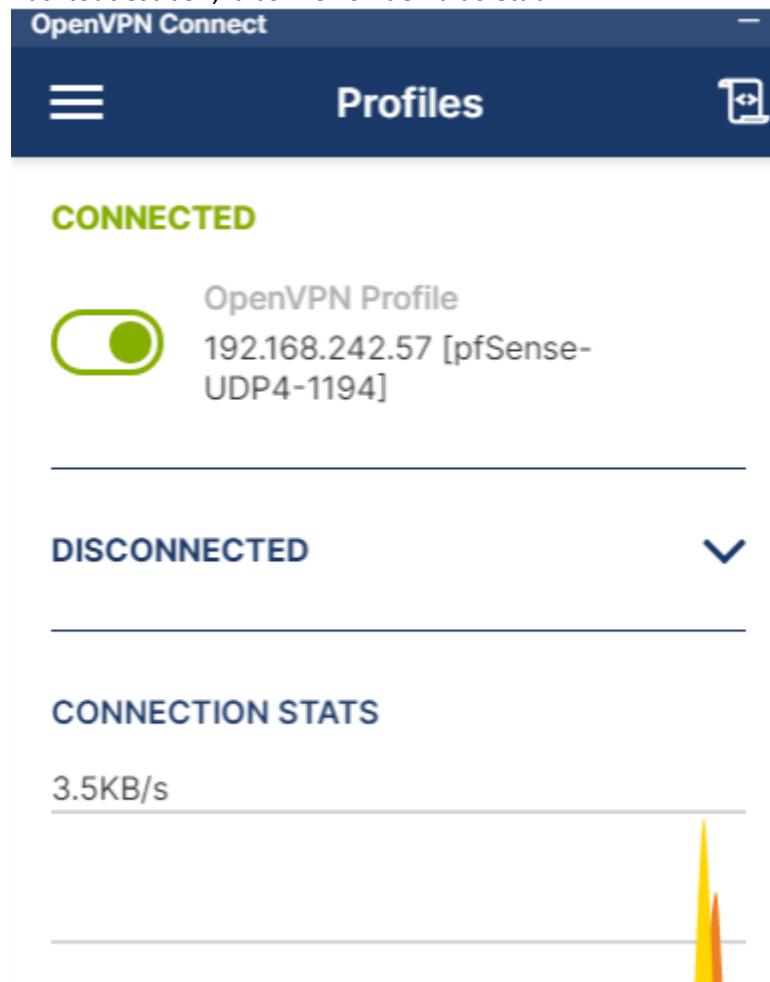
Username _____

Password _____ 

Import autologin profile ADD

[Get Access Server](#)

Et si tout est bon, la connexion devrait s'établir :

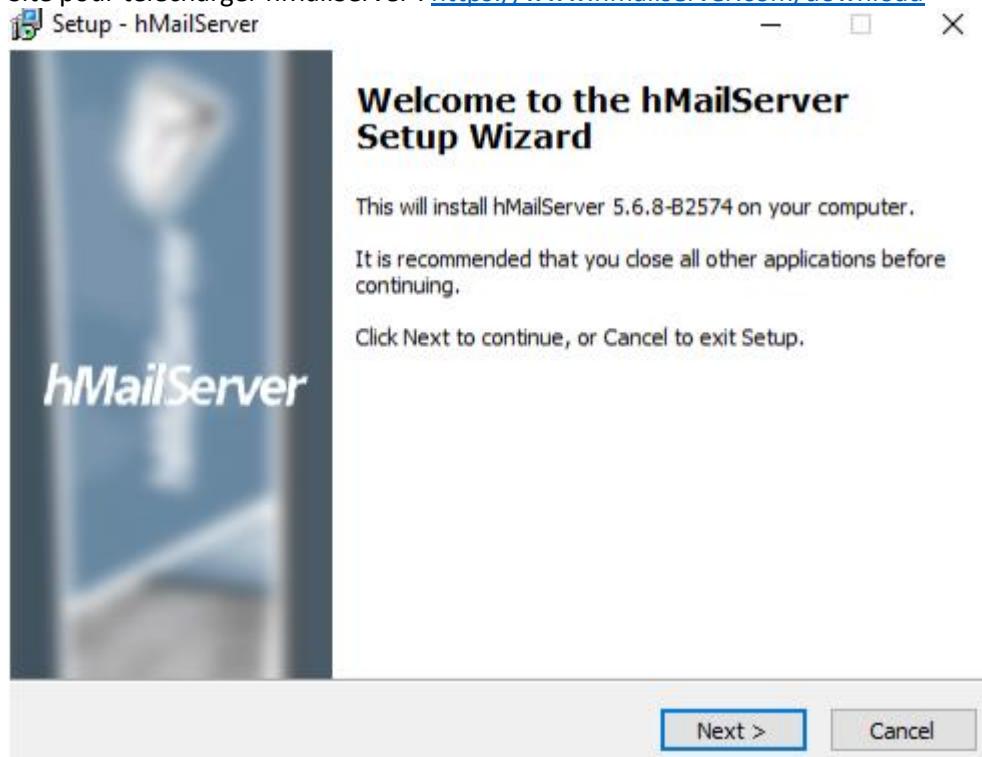


Nous en avons terminé avec Open VPN et PfSense.

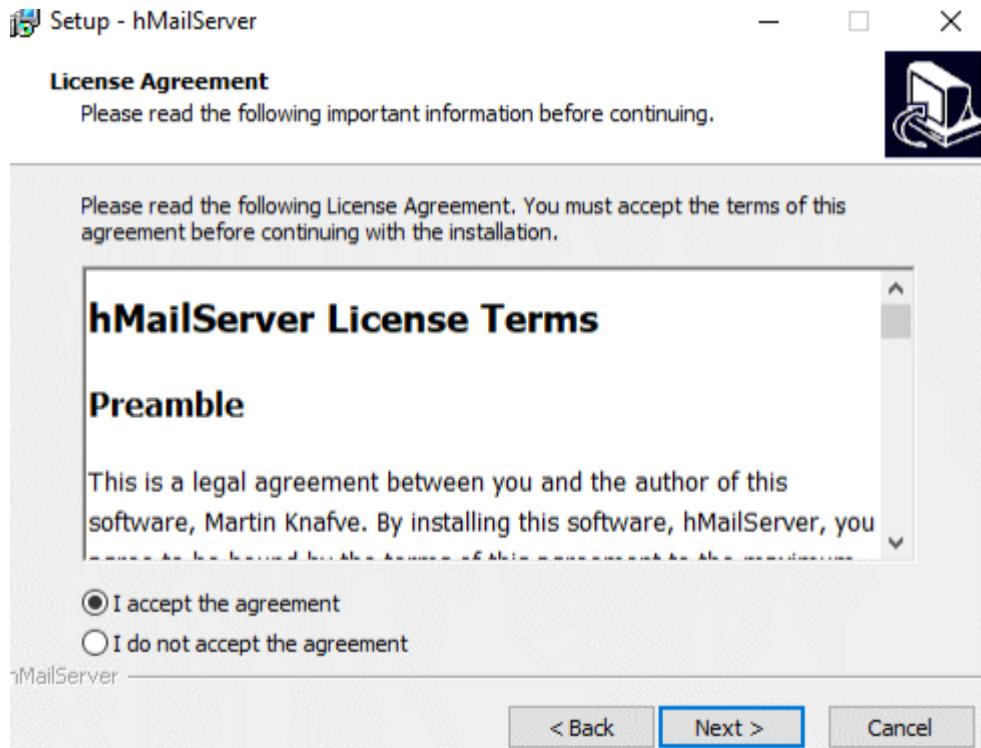
12. Messagerie – hMailServer & Thunderbird (Serveur&Client)

Nous allons installer hMailServer sur le serveur 1.

Site pour télécharger hMailServer : <https://www.hmailserver.com/download>

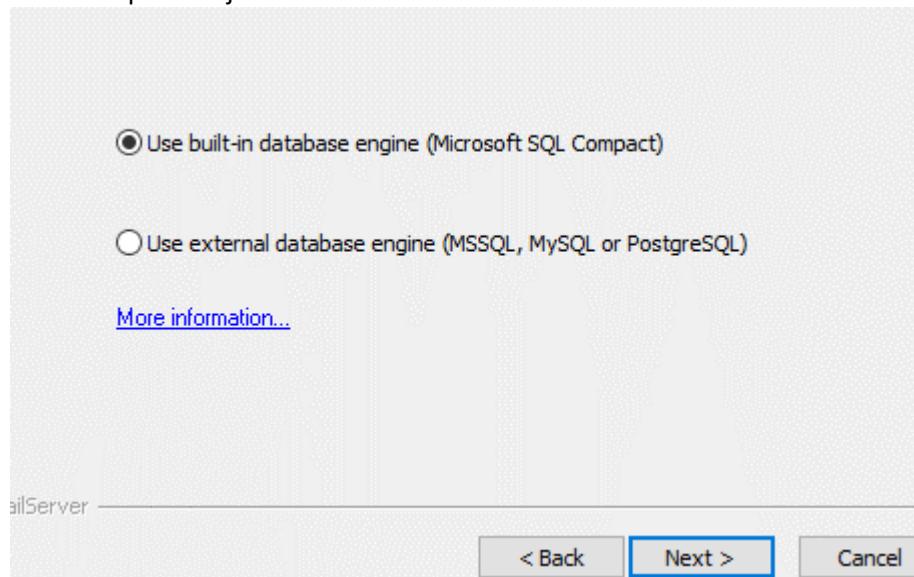


Accepter et « Next » :

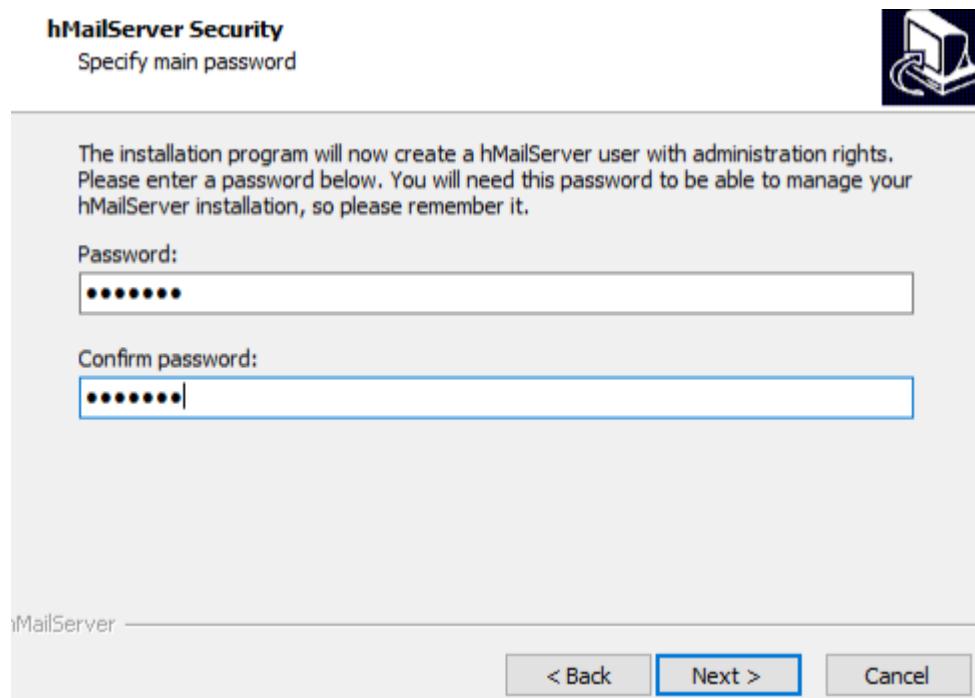


Tout sélectionner et faire « Next »

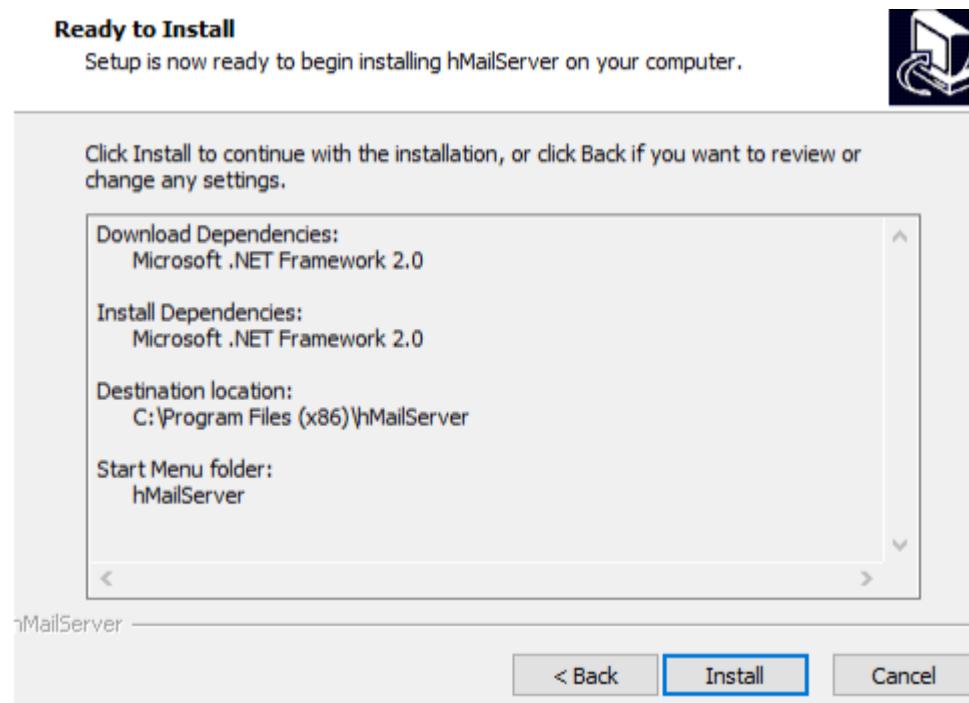
Laisser l'option déjà sélectionnée :



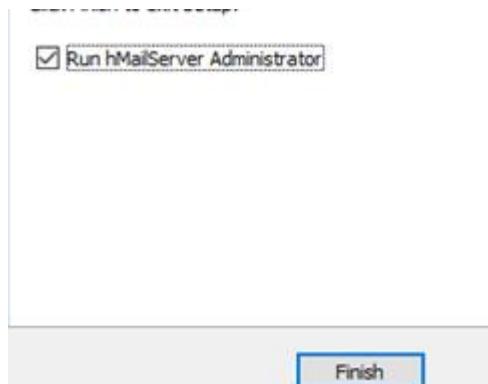
Choisir un mot de passe pour l'administrateur de hmail :



Faire « Next » et Install à l'étape suivante :

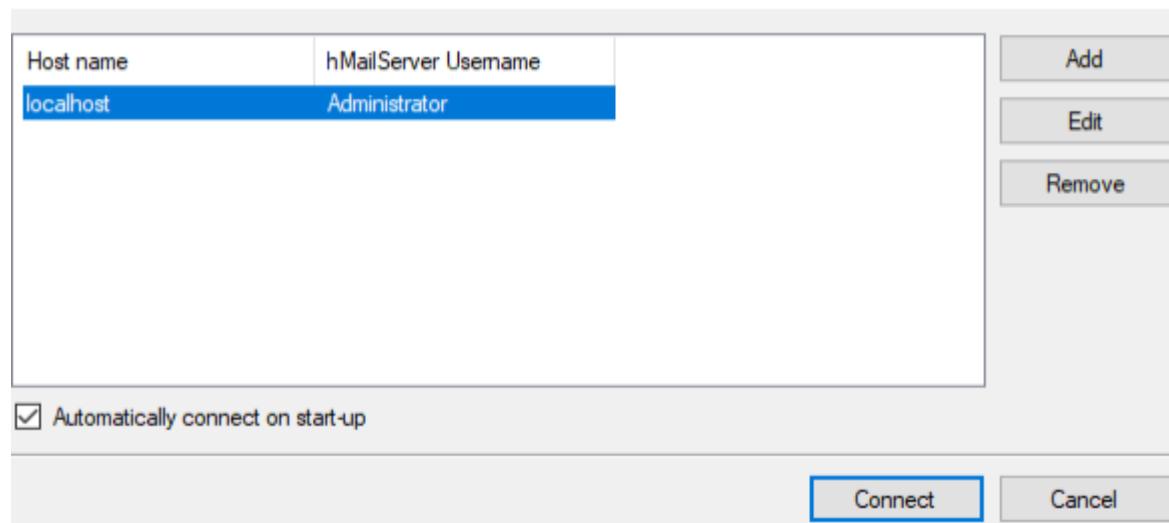


Lancer hmail en admin :

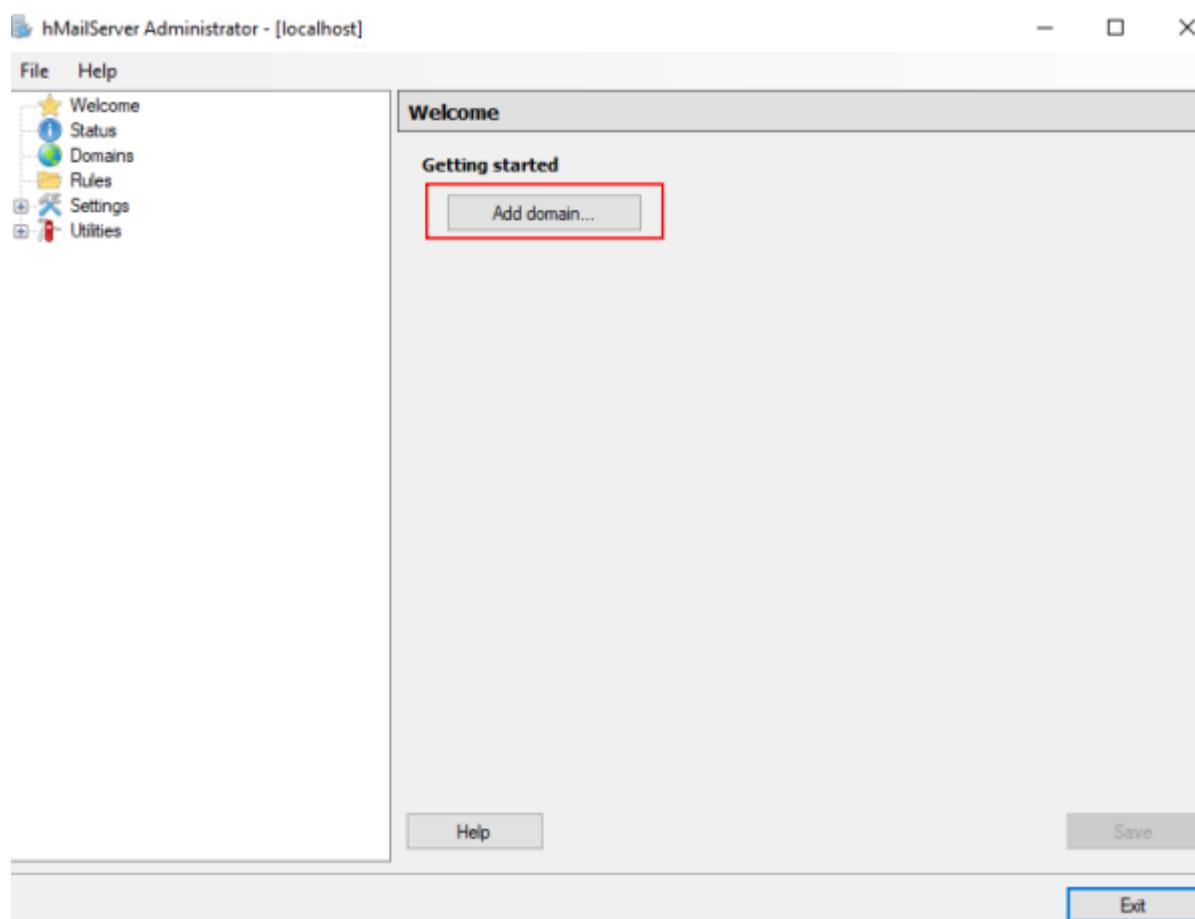


Configuration de hMailServer

Connectez vous avec l'identifiant et le mot de passe que vous venez de créer aux étapes précédentes :



Sélectionnez « Add domain » :



Mettez votre nom de domaine :

Domain

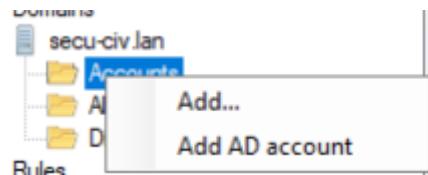
Enabled

Allez maintenant dans Settings -> Protocols -> SMTP -> Routes et mettez les informations que l'on vous demande en fonction toujours de votre projet.

Ajoutez le local host name dans Settings -> Protocols -> SMTP ->Delivery of e-mail :

Local host name

Dans le domaine que nous venons de créer, nous allons faire un clic droit sur « Accounts » et « Add AD account » :



Sélectionner le domaine et l'utilisateur dans cette partie :

Domain:

Accounts:

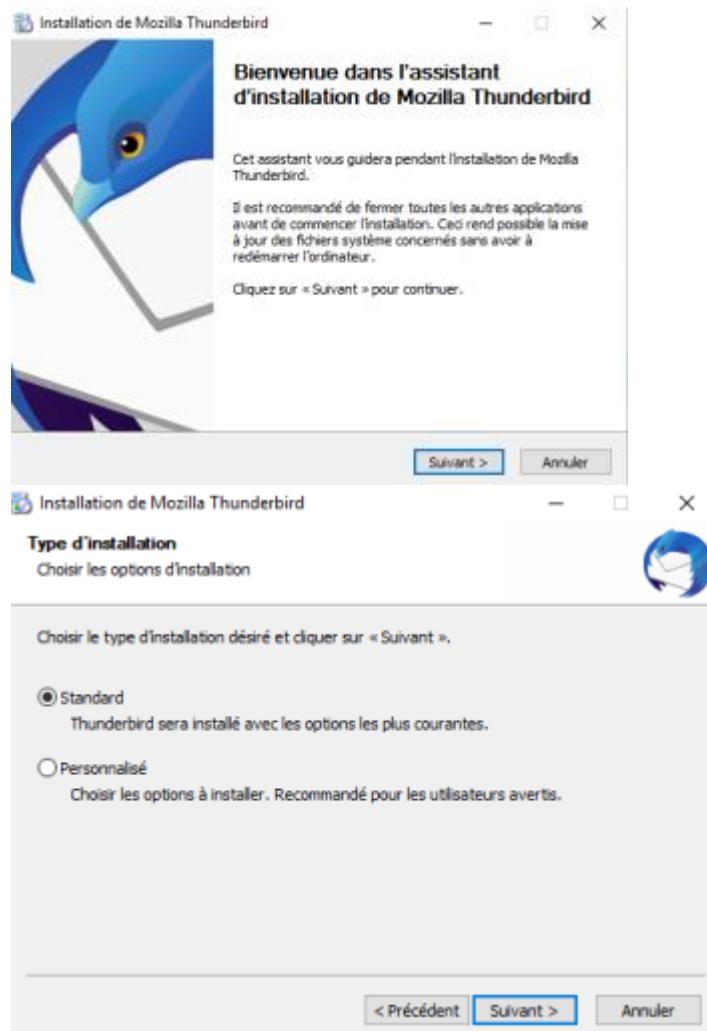
Address
SRVW01\$
krbtgt
SRVW02\$
DESKTOP-0LQV59L\$

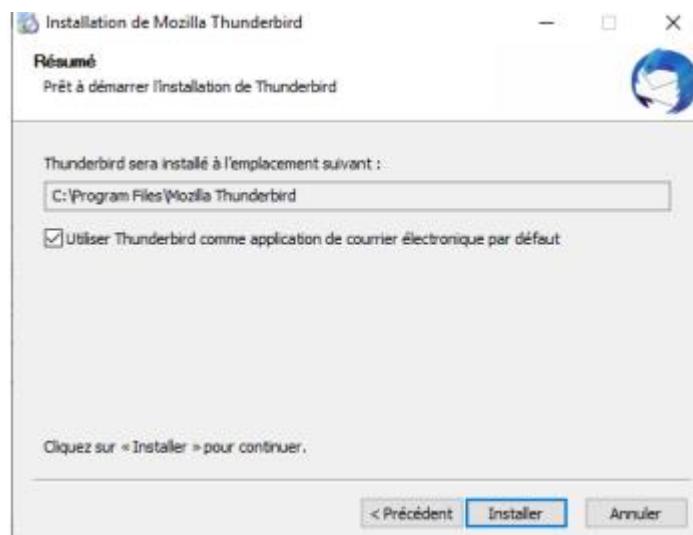
Et une fois sélectionner il doit être ajouter avec succès.

La prochaine étape est l'installation de Thunderbird et sa configuration :

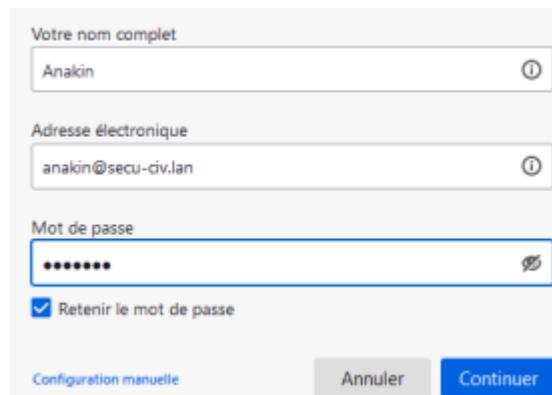
Comme pour hMailServer, nous allons aller sur ce lien pour le télécharger : <https://www.thunderbird.net/fr/>.

Installer en standard :





Une fois installé, lancez Thunderbird et connectez vous avec l'utilisateurs que vous avez créé sur votre hMailServer



Cliquez sur configuration manuelle :
Appliquez les différents paramètres 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 opérationnel, ce message doit apparaître après avoir appuyé sur « retester »

- ✓ Les paramètres suivants ont été trouvés en sondant le serveur donné :

✓ Crédit du compte réussie

Vous pouvez dès maintenant utiliser ce compte avec Thunderbird.

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

Rien de plus à dire que vous avez déjà parcouru un bon bout de chemin.

Faites un mail, envoyez-le et vérifiez que vous avez bien réceptionné le mail. Si vous l'avez, alors c'est gagné !

13. Téléphonie – PBX & Linphone

Renseignez la commande suivante pour télécharger FusionPBX :

```
wget -O - https://raw.githubusercontent.com/fusionpbx/fusionpbx-install.sh/master/debian/pre-install.sh | sh;
```

Installez le avec cette commande :

```
cd /usr/src/fusionpbx-install.sh/debian && ./install.sh
```

Sauvegarder ces informations :

```
Use a web browser to login.  
domain name: https://192.168.246.207  
username: admin  
password: 5Nu62c5mY1P00le8VmpKnJq6ezI
```

Aller sur le client et renseigner l'IP dans l'URL et l'identifiant ainsi que le mot de passe :



Pour ce qui est de la configuration, allez dans Account -> Users
Cela va nous permettre d'aller changer notre mot de passe qui est bien trop long.

Cliquez sur admin :

Add, edit, delete, and search users.

<input type="checkbox"/> Username	Groups
<input checked="" type="checkbox"/> admin	superadmin

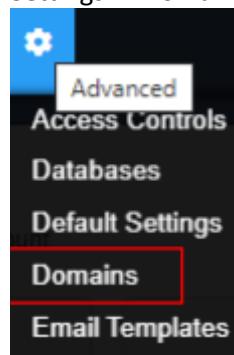
« Save » quand le mot de passe est changé :

dit user information and group membership.

Username	<input type="text" value="admin"/>
Password	<input type="password"/> Required: 12 Invalid Password Length (Number, Lowercase, Uppercase, Special)
Confirm Password	<input type="password"/> Green field borders indicate typed passwords match.
Email	<input type="text" value="alss-siosisr20-fjo@ccicamp"/>
Language	<input type="button" value="▼"/> Select the language.

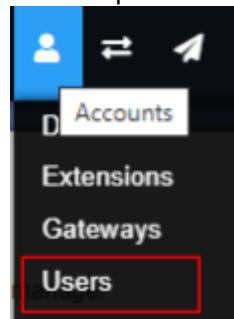
En cas d'erreur, nous allons ajouter un second domaine :

Settings -> Domains

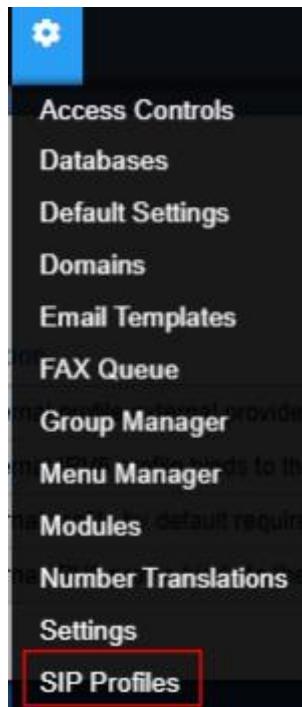


Ajoutez un domaine et mettez la bonne IP de votre serveur
Une fois cela fait, votre domaine sera créé.

Pour ce qui est des utilisateurs allez dans « Users » et changez le domaine par celui créé.



Pour ce qui est des profils SIP (intern/extern) : Settings -> SIP Profiles



Mettez votre IP que vous avez choisi et faites cela pour les deux :

	Name	Hostname	Enabled
<input type="checkbox"/>	external		True
<input type="checkbox"/>	external-ipv6		True
<input type="checkbox"/>	internal		True
<input type="checkbox"/>	internal-ipv6		True

Une fois fait redémarrer pour que tout s'initialise correctement.

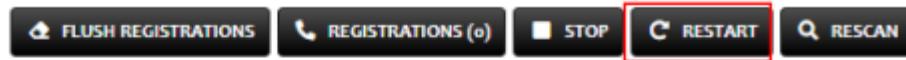
A coté de settings, on va cliquer sur l'onglet de stat :



Et aller dans : **SIP Status**

Faites un restart du premier et du troisième :

status profile external



status profile external-ipv6



status profile internal



status profile internal-ipv6



Retournez dans les utilisateurs et cette fois-ci, en cliquant sur le « + », créez un nouvel utilisateur et rentrez les paramètres dont vous avez besoin :

Username
Password
Confirm Password
Email
Language
Time Zone
Status
Contact
Groups
Domain
API Key
Enabled

Lorsque c'est fait, vous devriez voir apparaître votre utilisateur.
Et voilà nous en avons fini avec cette étape.

Passons dès à présent à l'installation de Linphone et de sa configuration

Voici le lien pour le télécharger : <https://www.linphone.org/technical-corner/linphone>

Une fois téléchargé et installé, lancez l'application.



Cliquez sur « Assistant de compte » puis « utiliser un compte SIP » :



Pour que votre nom fonctionne il va falloir créer une extension sur FusionPBX.
Une fois que vous avez créé votre utilisateur avec le nom associé, vous pourrez renseigner le nom d'utilisateur dans Linphone.

Une fois les informations correctement renseignées sur Linphone, vous devriez être connecté.

14. Serveur de monitoring – Zabbix

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_6.0-1+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 zabbix-agent
```

- 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 :

- Sélectionnez la langue, nous laisserons en Anglais



- Configuration de la connexion à la BDD

ZABBIX

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database.
Press "Next step" button when done.

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

Database type

Database host

Database port 0 - use default port

Database name

Store credentials in

User

Password 

Database TLS encryption *Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).*

[Back](#)

[Next step](#)

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

ZABBIX

Settings

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

Zabbix server name

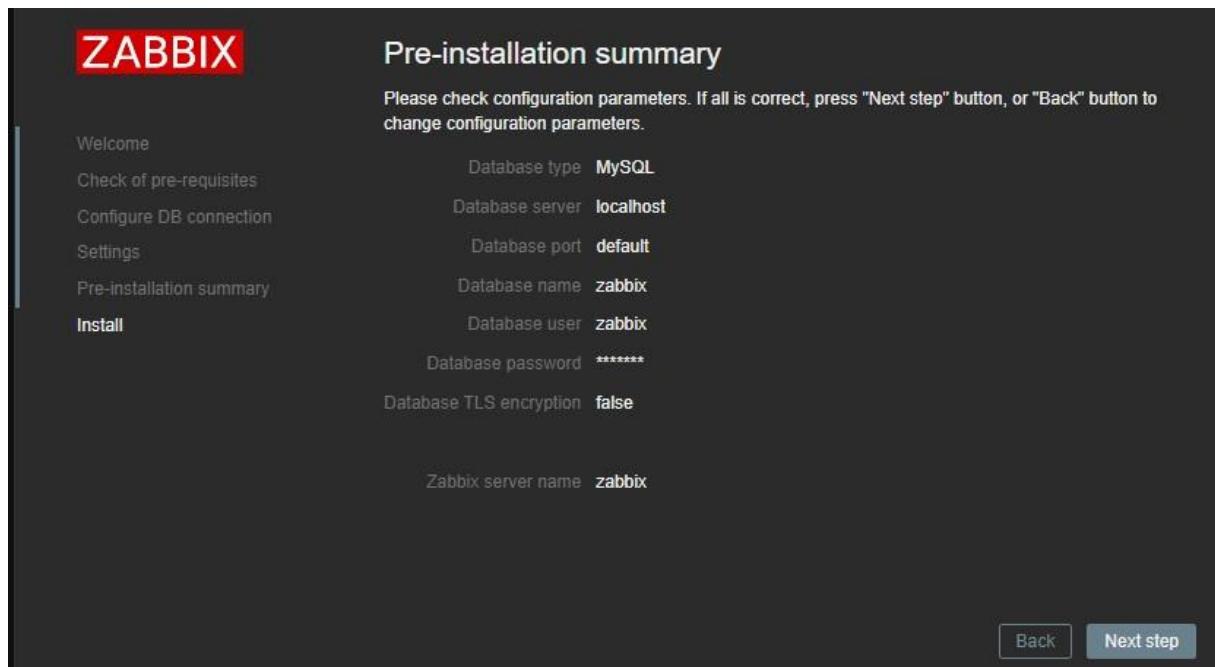
Default time zone

Default theme

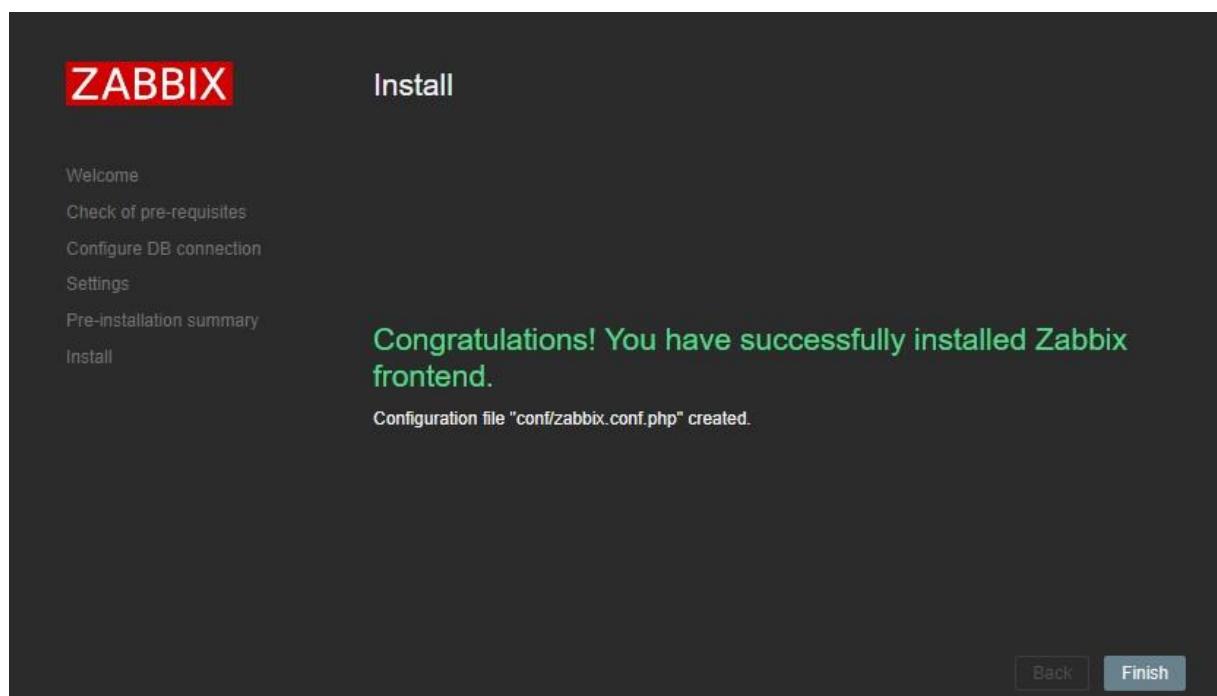
[Back](#)

[Next step](#)

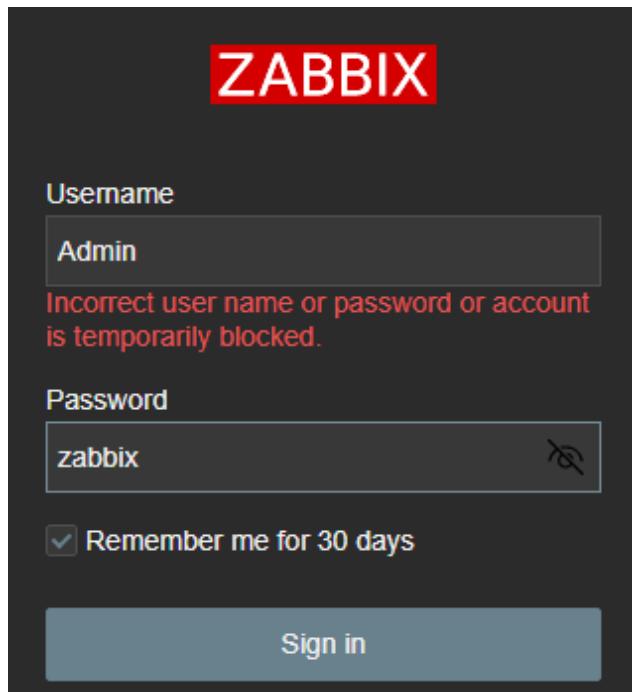
- Récapitulatif :



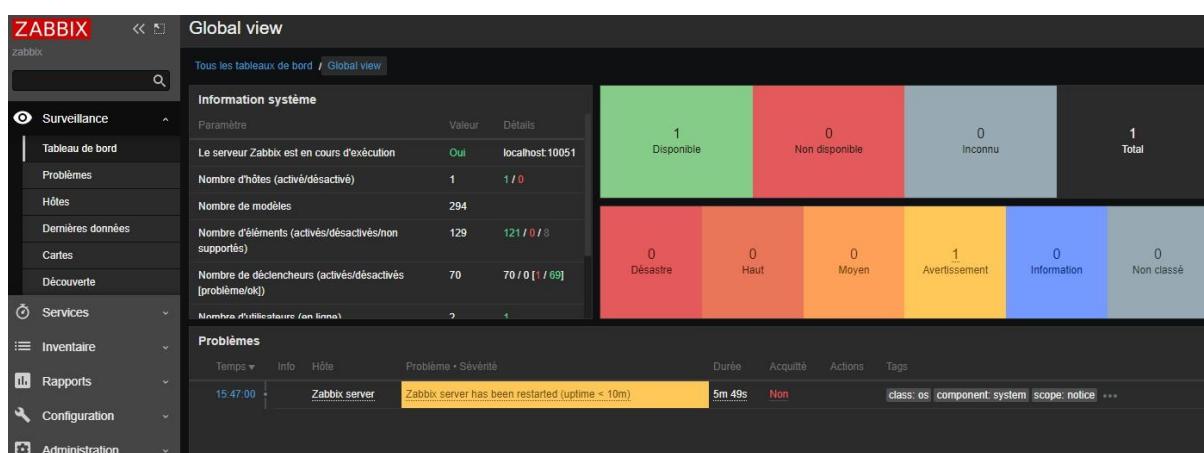
- Voilà ! L'installation et la configuration de base est terminée



- 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) :

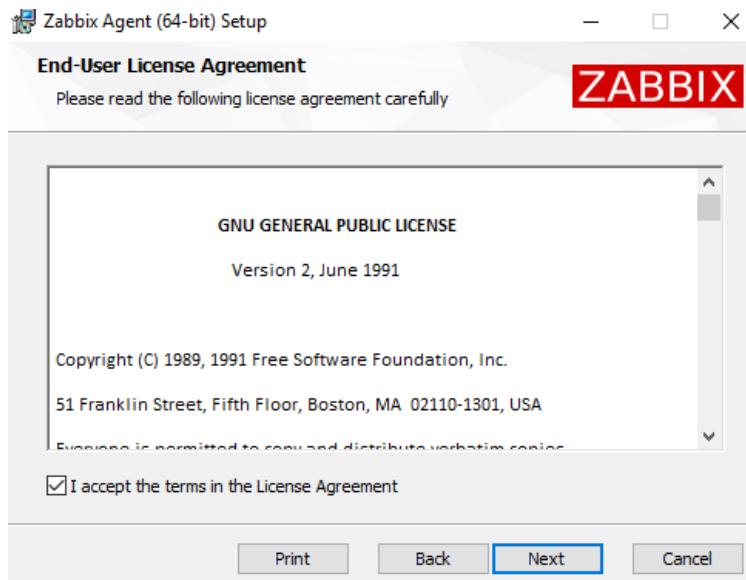
Nous allons déployer l'agent Zabbix sur notre serveur Windows Server 2019. Rendez-vous sur https://www.zabbix.com/fr/download_agents, puis télécharger l'agent correspondant à votre OS, ici nous choisissons Windows.

The screenshot shows a navigation menu with several options: 'Packages Zabbix', 'Images Cloud Zabbix', 'Containers Zabbix', 'Appliance Zabbix', 'Sources Zabbix', and 'Agents Zabbix'. The 'Agents Zabbix' option is highlighted with a dark blue background and a red border. Below the menu, there is a heading 'Téléchargez et installez les agents Zabbix précompilés' and a note 'For Agent DEBs and RPMs please visit [Zabbix packages](#)'. There is also a checkbox for 'Show legacy downloads' and a small circular icon with a dollar sign. A table below lists agent configurations for different operating systems:

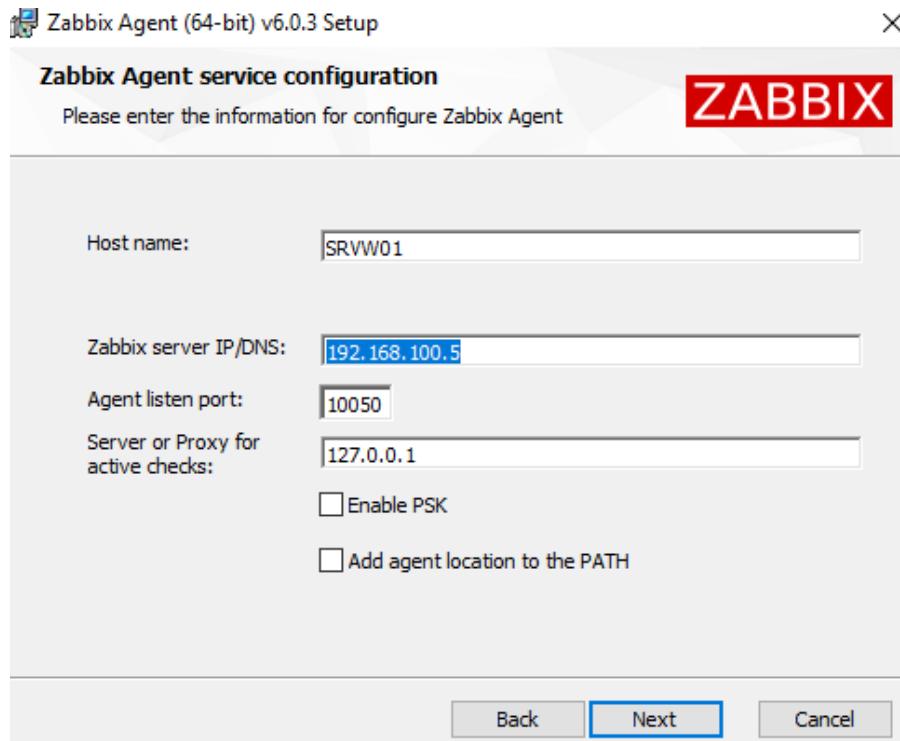
OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	MATÉRIEL	VERSION DE ZABBIX	CHIFFREMENT	FORMAT
Windows	Any	amd64	6.0 LTS	OpenSSL	MSI
Linux		i386	5.4	No encryption	Archive
macOS			5.2		
AIX			5.0 LTS		

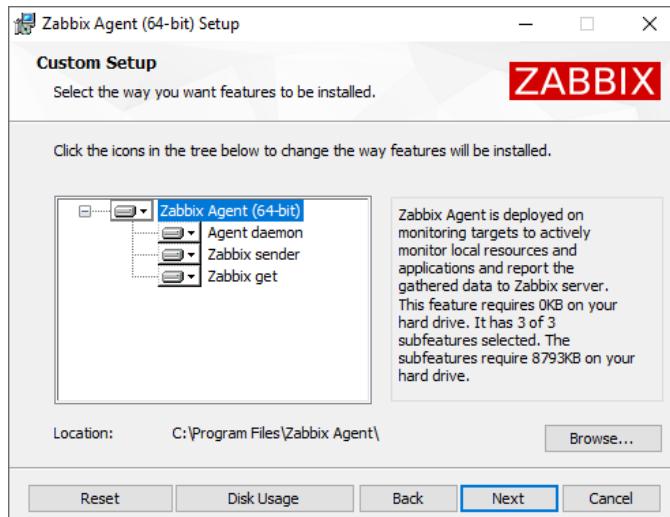
- Réalisez l'installation

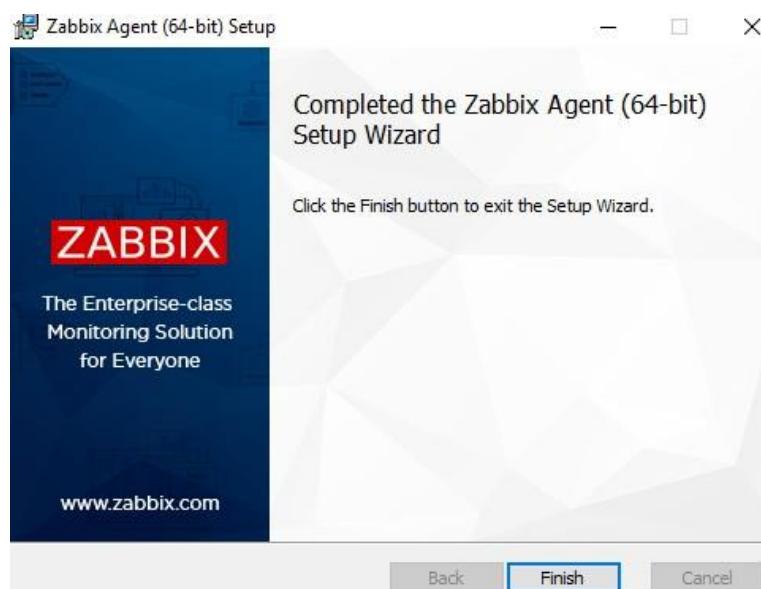
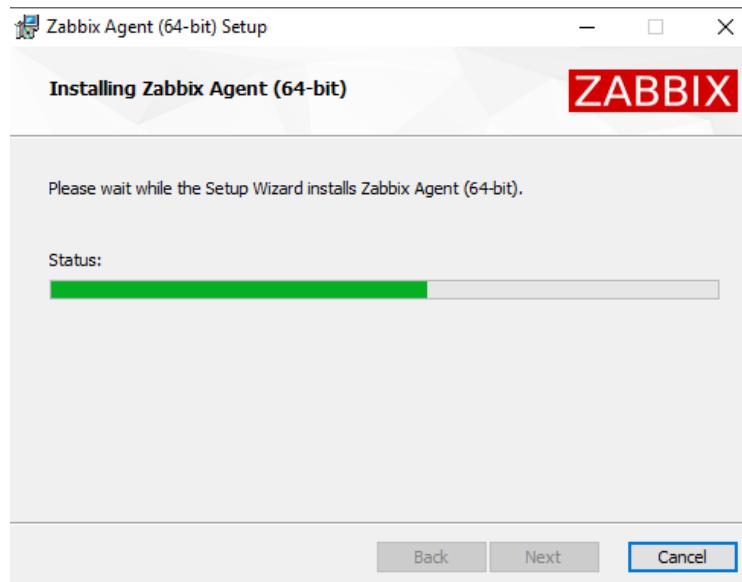




- Dans « Host name » renseignez un nom pour votre serveur Windows, dans « Zabbix server IP » renseignez l'adresse IP de votre serveur Zabbix. Le port par défaut est 10050. Ces paramètres pourront être modifiés ultérieurement dans les fichiers de configuration de l'agent Zabbix.





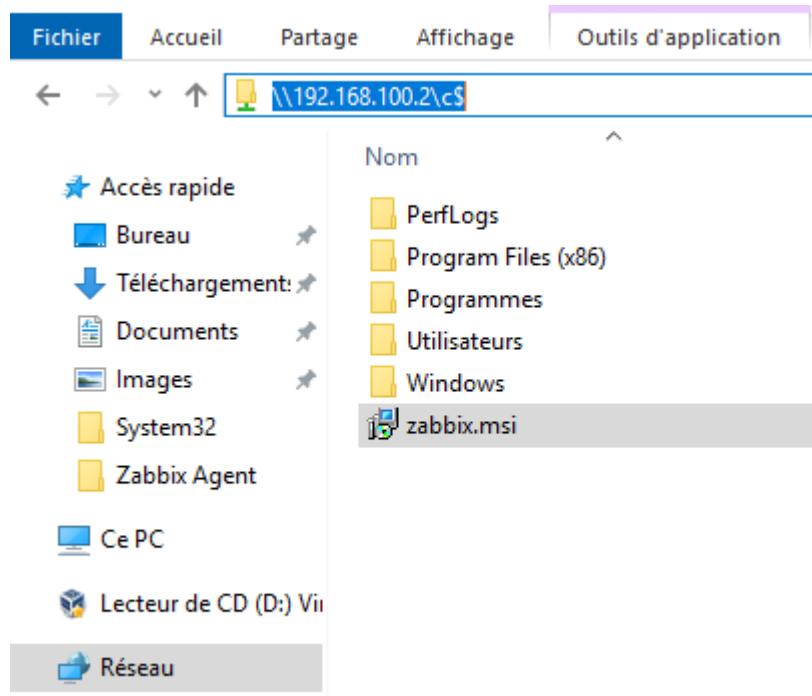


- On peut voir que le service Zabbix est bien en cours d'exécution

wuauserv	1030	Windows Update	En cours d'exéc...	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
- Modifiez également le nom d'hôte du serveur de téléphonie, puis enregistrez le fichier
- 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

Hôtes

Hôte Modèles IPMI Macros Inventaire d'hôtes Chiffrement

* Nom de l'hôte: Zabbix_server_1

Nom visible: Zabbix_server_1

* Groupes: Linux servers x, Zabbix servers x, Discovered hosts x, Sélectionner, taper ici pour rechercher

* Au moins une interface doit exister.

Interfaces de l'agent	adresse IP	Nom DNS	Connexion à	Port	Défaut
	192.168.3.220		IP	10050	<input checked="" type="radio"/> Supprimer
	Ajouter				

Interfaces SNMP	127.0.0.1		IP	161	<input checked="" type="radio"/> Supprimer
	Ajouter				

Interfaces JMX	Ajouter
----------------	---------

Interfaces IPMI	Ajouter
-----------------	---------

Description:

Surveillé via le proxy: (pas de proxy)

Activé:

Ajouter **Annuler**

- Résultat :

	Nom	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité
	SRVTTEL	Éléments 42	Déclencheurs 14	Graphiques 8	Découverte 3	Web	192.168.100.4:10050	Linux by Zabbix agent		Activé	

- 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)
```

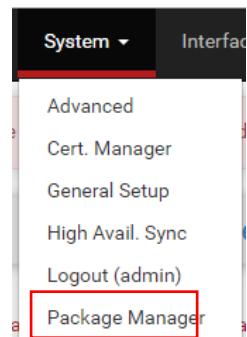
- Pour voir les différentes règles, tapez :

```
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)

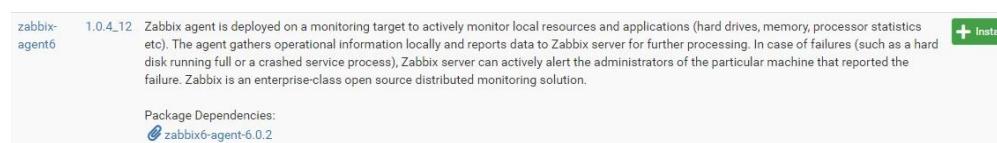
- Rendez-vous dans « Packet Manager »



- 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 hostnames defined in Zabbix.	

- A présent, ajoutons notre routeur sur Zabbix

The screenshot shows the 'Hôte' (Host) configuration page in Zabbix. The top navigation bar includes tabs for 'IPMI', 'Tags', 'Macros', 'Inventaire', 'Chiffrement', and 'Table de correspondance'. The main form fields are:

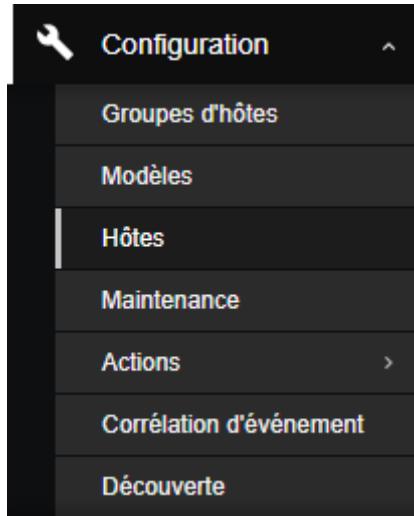
- Nom de l'hôte:** RTE02
- Nom visible:** RTE02
- Modèles:** FreeBSD by Zabbix agent (selected)
- Groupes:** Machines LAN (selected)
- Interfaces:** Agent (Type: adresse IP, IP: 192.168.100.252), Nom DNS, Connexion à, Port: 10050

- Notre routeur a bien été ajouté



Création d'un groupe d'hôtes :

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



- En haut à droite, cliquez sur « Créer 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 taper ici pour rechercher
* Groupes Machines LAN taper ici pour rechercher

Interfaces Type adresse IP Nom DNS Connexion à Port Défaut
Agent 192.168.100.1 10050

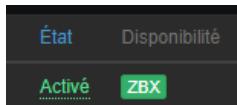
Ajouter

Description

- 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 »



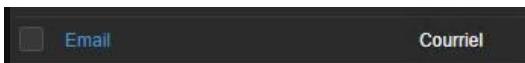
Ensuite nous avons accès aux différentes informations du serveur.

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

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



- Sélectionnez « Email »



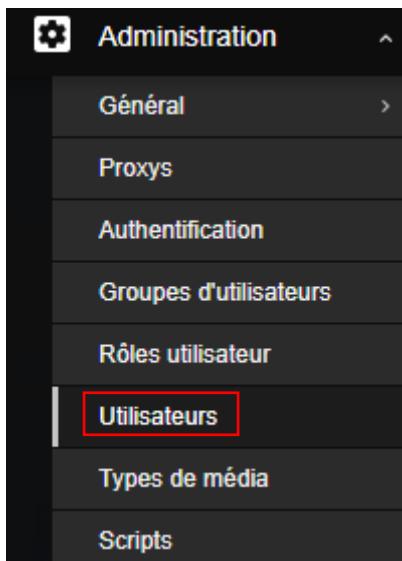
- Renseignez les différents éléments comme ci-joint. Le but ici est de renseigner les informations du serveur de messagerie et de l'utilisateur qui recevra un courriel en cas de panne. Cliquez sur « Actualiser » une fois que la configuration est terminée.

A screenshot of the Zabbix 'Email' configuration form. The fields filled out are:

- * 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.lan
- Mot de passe: Joe0110
- Format du message: HTML
- Description: (empty)
- Activé: checked

At the bottom are buttons for Actualiser, Clone, Supprimer, and Annuler.

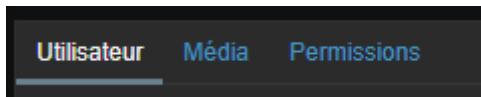
- A présent, dans « Administration », cliquez sur « Utilisateurs »



- 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 »

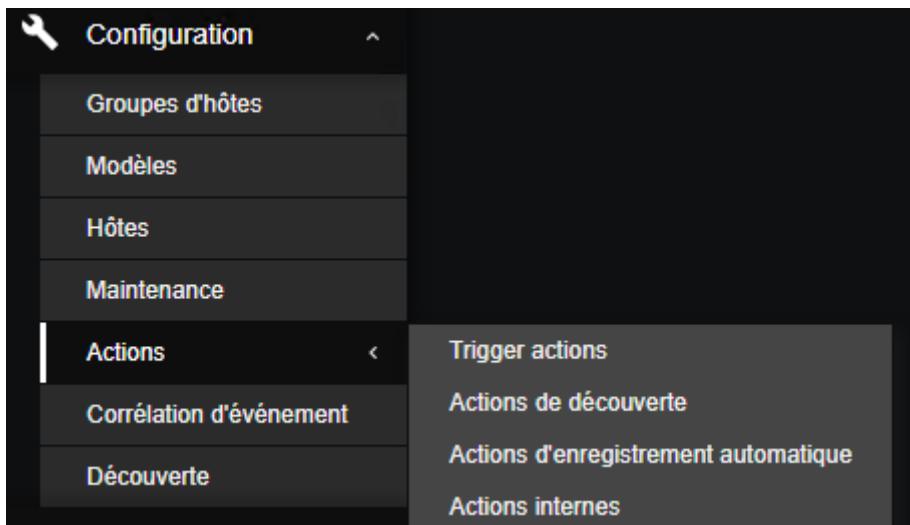
Média

Type	Email	<input type="button" value="Supprimer"/>
* Envoyer	Administrateur@secu-civ.lan	<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 checked="" type="checkbox"/>	
<input type="button" value="Ajouter"/> <input type="button" value="Annuler"/>		

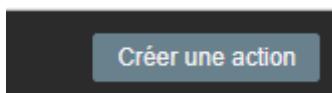
- Cliquez sur « Actualiser » afin de valider les paramètres

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"/>			

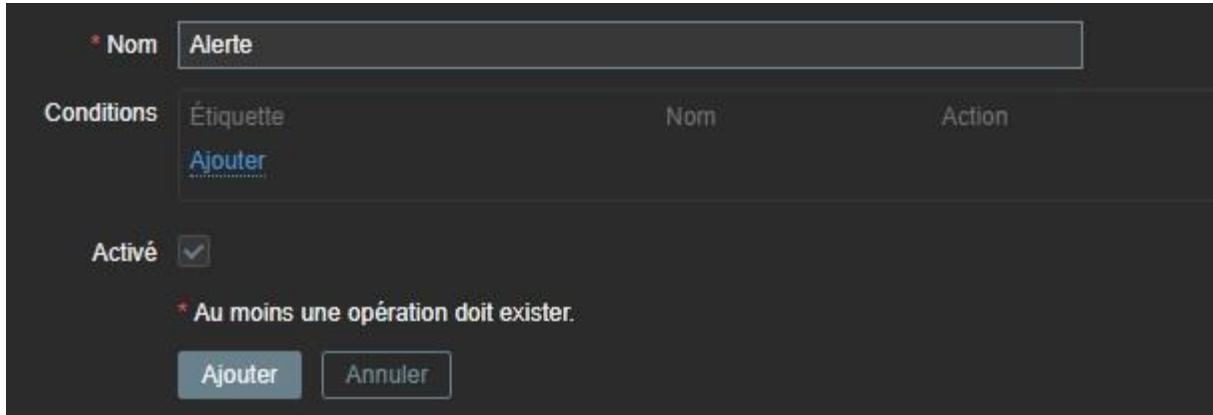
- A présent, nous allons configurer une action pour savoir quand le courriel doit être envoyé. Dans « Configuration » > « Actions », cliquez sur « Trigger actions »



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

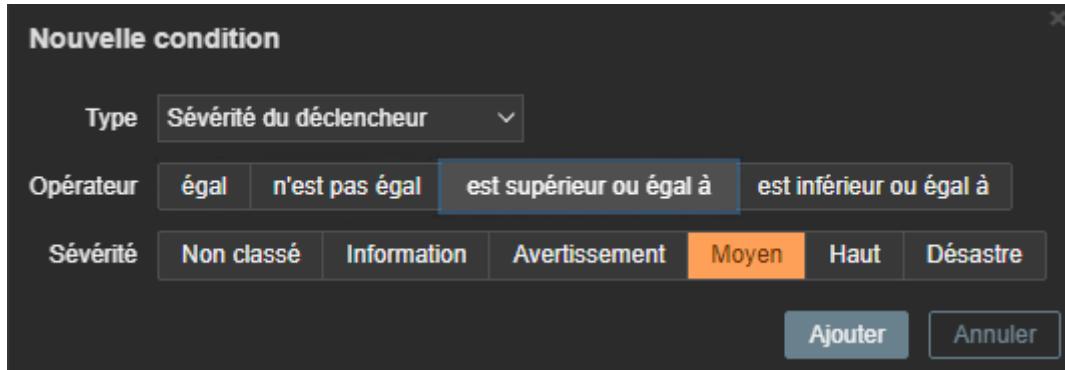


- Donnez un nom à votre action puis cliquez sur « Ajouter » dans « Conditions »

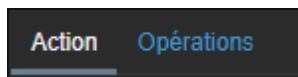


- Dans type nous allons choisir « Sévérité du déclencheur » puis dans opérateur « est supérieur ou égal à » est dans « Sévérité » « Moyen ». Puis cliquez sur « Ajouter »

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



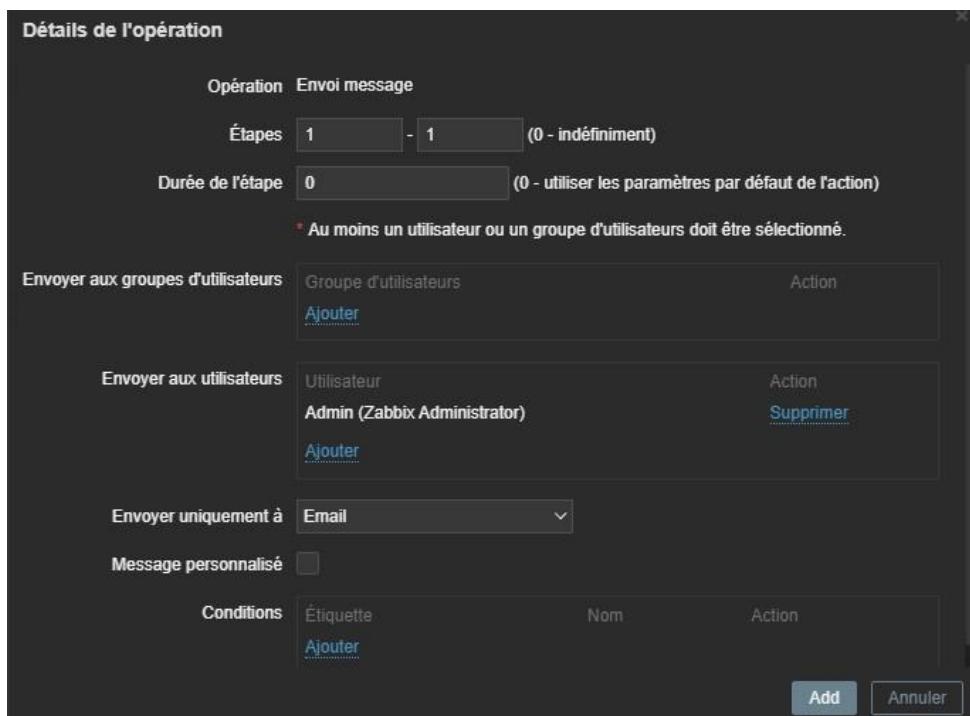
- A présent cliquez sur « Opérations ». Nous allons définir ce qui doit être fait lorsque la condition est respectée



- 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 »



- Enfin, cliquez sur « Ajouter »

Durée de l'étape d'opération par défaut: 1m

Opérations	Etapes	Détails	Démarrer dans	Durée	Action
	1	Envoyer le message aux utilisateurs: Admin (Zabbix Administrator) via Email	Immédiatement	Défault	Édition 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



15. Serveur WEB (eBrigade) / LAMP

Installation LAMP

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

Installation eBrigade

Téléchargement : <https://ebrigade.app/download.php>

Envoyer le fichier vers le serveur Ubuntu

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

Commande pour dézipper :

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

Affichage une fois dézippé :

```
ebrigade-5.3.2
```

Création de la Base de données de eBrigade :

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

Tapez cette commande :

```
mysql> CREATE DATABASE `ebrigade` DEFAULT CHARACTER SET latin1 COLLATE latin1_general_ci;
Query OK, 1 row affected (0,01 sec)
```

Création utilisateur eBrigade :

```
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)
```

Renseignez un identifiant et un mot de passe.

Maintenant nous allons nous connecter à l'interface web :

Paramètres de connexion à la base de données

Server Name 	localhost
User 	ebrigade
Password 	*****

Si ça fonctionne vous aurez cette image :



Schéma de base de données importé avec succès.

Vous pouvez maintenant choisir le mot de passe
pour le compte **admin**.

Choix mot de passe pour admin

Un mot de passe est demandé pour le compte admin (mettez celui que vous voulez) :

Modifier le mot de passe pour Admin ADMIN

Veuillez choisir un mot de passe personnel.

Nouveau mot de passe
Confirmation

Pour plus de sécurité, mettez aussi des caractères spéciaux!

Sauvegarder

★ changement réussi

le mot de passe a été configuré avec succès

Continuer

Renseignez ensuite les éléments demandés et une fois validé vous aurez à nouveau ce genre de message si c'est validé :



La procédure est à présent terminée !