

**E5**

**Documentation technique situation professionnel 2**

Sommaire

[Sommaire 2](#_Toc132789405)

[Documentation technique & mode d’emploi Active Directory redondé-Windows Server 2019 3](#_Toc132789406)

[1. Active Directory redondé - Windows Server 2019 3](#_Toc132789407)

[*Installation de Windows Server 2019* 4](#_Toc132789408)

[*ADDS : Installation / Configuration / DNS(GUI)* 8](#_Toc132789409)

[*ADDS : configuration / installation / DNS :* 12](#_Toc132789410)

[*Installation DHCP* 19](#_Toc132789411)

[2. Routeur & Pare-feu – Pfsense 20](#_Toc132789412)

[*Installation PfSense* 21](#_Toc132789413)

[*Configuration PfSense* 25](#_Toc132789414)

[*CARP – Pfsync – XML – RPC / IP virtuelle configuration / redondance* 28](#_Toc132789415)

[*Mise en place des règles de Pare-feu* 36](#_Toc132789416)

[*OpenVPN / PfSense – VPN RW* 37](#_Toc132789417)

[3. OpenVPN 43](#_Toc132789418)

[4. Messagerie – hMailServer & Thunderbird (Serveur&Client) 46](#_Toc132789419)

[*Configuration de hMailServer* 49](#_Toc132789420)

[5. Téléphonie – PBX & Linphone 54](#_Toc132789421)

[6. Serveur de monitoring – Zabbix 59](#_Toc132789422)

[7. Serveur WEB (eBrigade) / LAMP 84](#_Toc132789423)

[*Installation LAMP* 84](#_Toc132789424)

[*Installation eBrigade* 84](#_Toc132789425)

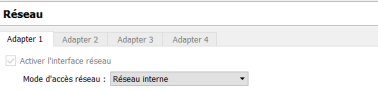
# 

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

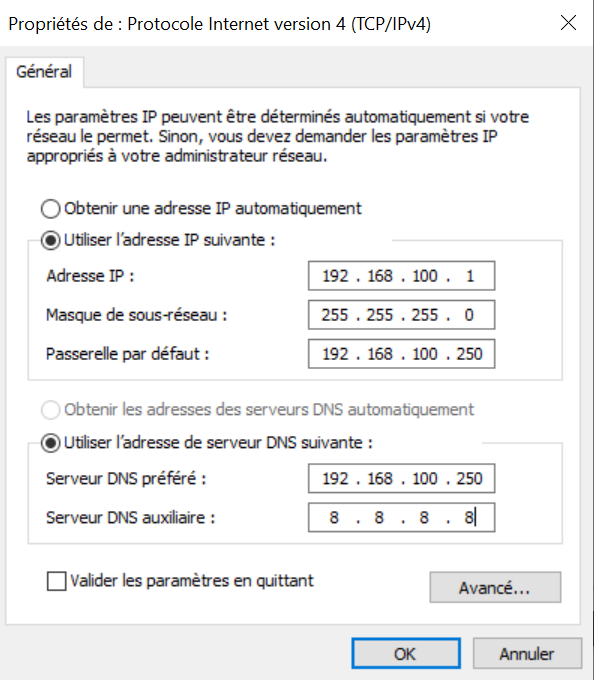
# Active Directory redondé - Windows Server 2019

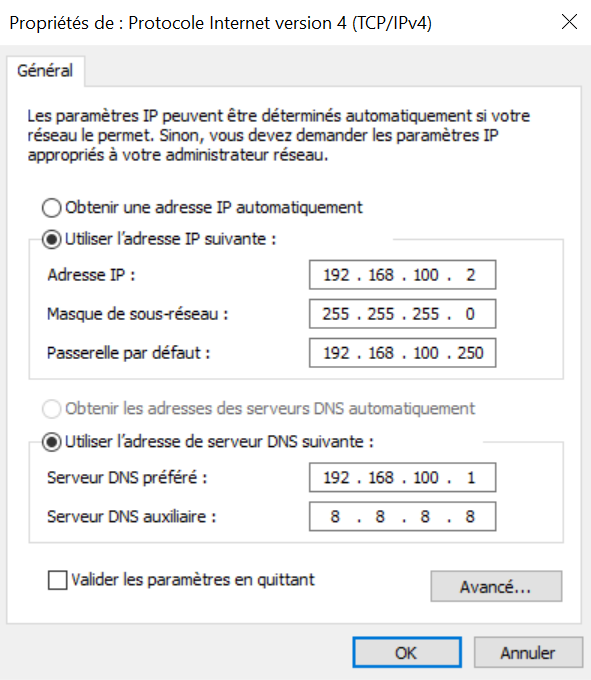
Deux VM Windows Server (1 Windows Server GUI / 1 Windows Server CORE)

Interface réseau :

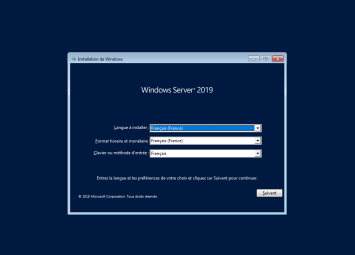


Configuration réseau des deux VM :  
  
SRVWIN01 :

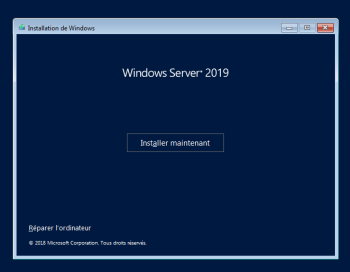


SRVWIN02 :   


# *Installation de Windows Server 2019*



Sélectionnez installer maintenant :



Prenez Windows Server 2019 Standard Evaluation :

Une image contenant texte

Description générée automatiquement

Faites suivant :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

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 » :

Une image contenant texte

Description générée automatiquement

Tapez 6 puis entrer :

Une image contenant texte

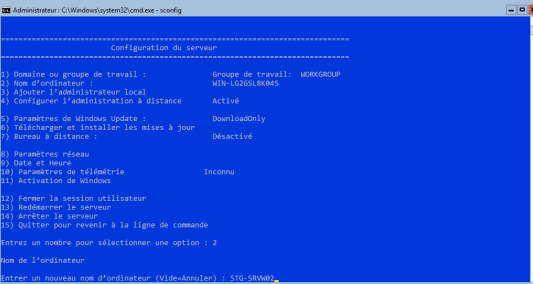
Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Faire de même pour le second serveur :



# *ADDS : Installation / Configuration / DNS(GUI)*

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

Une image contenant texte

Description générée automatiquement

Sélectionner le serveur :

Une image contenant texte

Description générée automatiquement

Rôle « AD DS » :

Une image contenant texte

Description générée automatiquement

Installer :

Une image contenant texte

Description générée automatiquement

Patientez le temps de l’installation :

Une image contenant texte

Description générée automatiquement

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

Ajouter une nouvelle forêt :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Faites suivant plusieurs fois :

Une image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquement

# *ADDS : configuration / installation / DNS :*

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

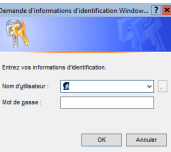
Une image contenant texte

Description générée automatiquement

Ajouter le serveur Core dans le domaine :



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



Rebootez le serveur :



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



« Ajouter d’autres serveurs à régler » :

Une image contenant texte

Description générée automatiquement

Sélectionner le second serveur puis faites « ok » :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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 :

Une image contenant texte

Description générée automatiquement

« Sélection du serveur », sélectionner le serveur CORE :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquement

Une fois terminée, promouvoir le contrôleur de domaine :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Faites suivant et renseignez le mot de passe demandé   
Dans « option supplémentaire » cliquez sur « tout contrôleur de domaine et sélectionner le serveur principal GUI :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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 créer l’UO « Strasbourg » sur notre serveur principal, on peut voir qu’il apparait aussi sur le serveur secondaire : (voir images ci-dessous)

Une image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquement

# *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 :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Faites terminer la configuration DHCP :

Une image contenant texte

Description générée automatiquement

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 :

Une image contenant texte

Description générée automatiquement

# Routeur & Pare-feu – Pfsense

3 interfaces réseaux requises : WAN, LAN, DMZ :

Voici les IP de nos 2 routeurs :

Routeur 1 : 

Routeur 2 : 

# Installation PfSense

Entrer :

Une image contenant texte

Description générée automatiquement

Sélectionner Install et faites entrer :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Auto (UFS) :

Une image contenant texte

Description générée automatiquement

Faites « No » :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Une fois reboot, vous devrez attendre sur cette page :

Une image contenant texte

Description générée automatiquement

Et arriver sur celle là : Une image contenant texte

Description générée automatiquement

# *Configuration PfSense*

Entrer option 1 :

em0 = wan  
em1 = lan  
em2 = dmz

Une image contenant texte

Description générée automatiquement

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

Description générée automatiquement

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



Masque de sous réseau : 24

Une image contenant texte

Description générée automatiquement

Entrer :



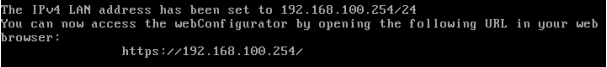
Entrer à nouveau :



Faites « n » pour les deux prochaines étapes :

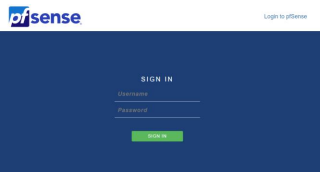
 

Depuis notre client windows 10, nous pouvons maintenant accéder à la page web :   
Attention, pensez à mettre votre VM client dans le même réseau local sinon cela ne fonctionnera pas :



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

Entrer le Login : admin   
Et le mot de passe : pfsense



Next :

Une image contenant texte

Description générée automatiquement

Renseignez les informations demandés :

Une image contenant texte

Description générée automatiquement

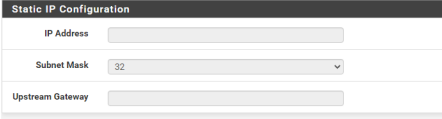
Timezone :

Une image contenant texte

Description générée automatiquement

Wan en DHCP et masque 32 :

Une image contenant table

Description générée automatiquement 

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

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Vous pouvez modifier votre identifiant admin de pfsense :

Une image contenant Site web

Description générée automatiquement

Faites « reload »

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Cliquez sur « Add » :

Une image contenant texte

Description générée automatiquement

Faire une IP virtuelle identique sur les deux routeurs : Une image contenant texte

Description générée automatiquement

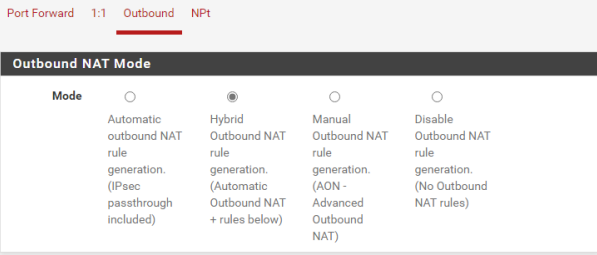
Voilà ce que ça donne une fois créée : Une image contenant texte

Description générée automatiquement

Ensuite nous allons aller dans Firewall -> NAT :

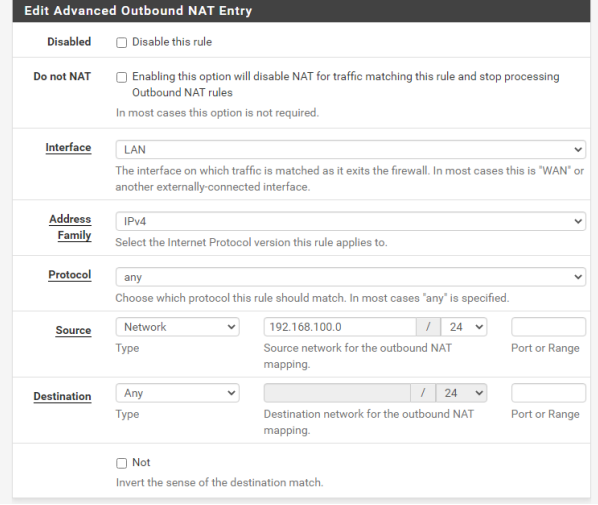
Une image contenant texte

Description générée automatiquement

Sélectionner « Hybrid Outbound NAT » puis « save » : 

« Add » pour créer une nouvelle règle : Une image contenant texte

Description générée automatiquement

Suivez les indications sur l’image ci-dessous : 

Une image contenant texte

Description générée automatiquement

Voici ce que vous devez obtenir :

Une image contenant Site web

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Rentrer votre ID and PASSWORD de Pfsense : Une image contenant texte

Description générée automatiquement

Sélectionner toutes les cases si cela n’est pas fait : Une image contenant texte

Description générée automatiquement

Faites « Save » et votre configuration est terminée.   
  
Maintenant sur le routeur secondaire : System -> High Avail Sync

Une image contenant texte

Description générée automatiquement

Sélectionner la case puis LAN puis mettez l’adresse IP du routeur principal : Une image contenant texte

Description générée automatiquement

La seconde configuration est terminée.

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

Une image contenant texte

Description générée automatiquement

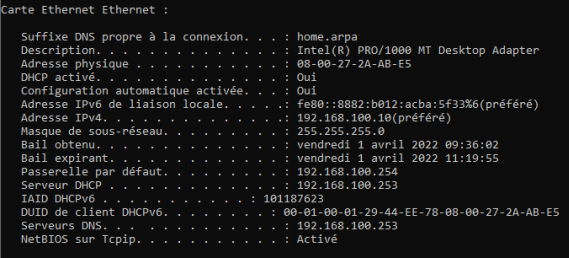
Vous aurez juste à l’activer si ce n’est pas déjà fait et dans la « Gateway », vous mettrez l’IP du LAN.

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

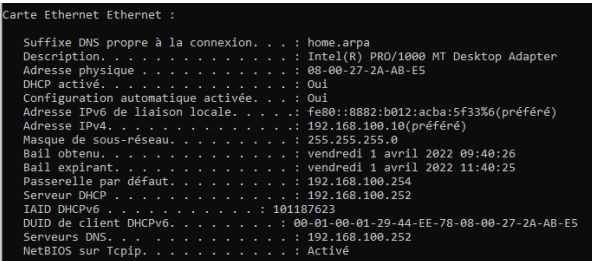
La passerelle est bien notre IP virtuelle lorsque nous faisons un ipconfig /all sur notre réseau LAN :



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 :



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

Une image contenant texte

Description générée automatiquement

Dans CARP nous pouvons distinguer le statu t de chacun de nos routeurs

Routeur 1 : Routeur 2 :

Une image contenant texte

Description générée automatiquement Une image contenant texte, Site web

Description générée automatiquement

Nous avons terminé avec notre IPV LAN et nous avons aussi créer des IPV pour notre WAN et notre DMZ.

# *Mise en place des règles de Pare-feu*

Règles LAN :

Autorisation LAN->DMZ & Autorisation Zabbix & Autorisation ICMP

Une image contenant texte, capture d’écran, intérieur

Description générée automatiquement

Règles WAN :

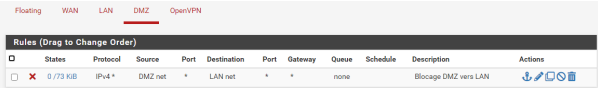
Destination vers DMZ

Une image contenant texte

Description générée automatiquement

Règles DMZ :

Blocage des flux de la DMZ vers le LAN



# *OpenVPN / PfSense – VPN RW*

Nous allons commencer par la liaison LDAP :

System->User Manager :

Une image contenant texte

Description générée automatiquement

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 :

Une image contenant table

Description générée automatiquement

Passons au serveur VPN

Allez dans VPN->OpenVPN

Une image contenant texte

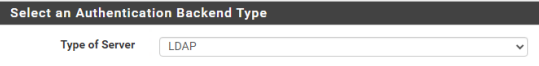
Description générée automatiquement

Sélectionner « Wizards » :

Une image contenant logo

Description générée automatiquement

Choisir « LDAP » :



Prendre le serveur LDAP que nous avons configuré :

Une image contenant texte

Description générée automatiquement

Configuration du CA :

Une image contenant texte

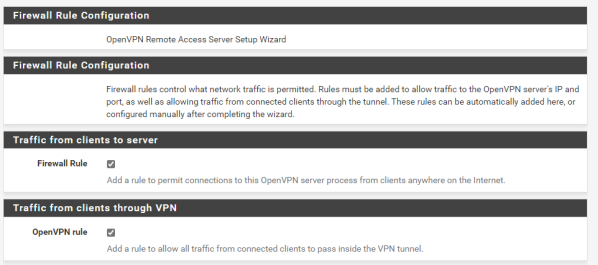
Description générée automatiquement Une image contenant texte

Description générée automatiquement Une image contenant texte

Description générée automatiquement

A la suite de ces indications, mettre l’adresse du VPN et celle du réseau LAN que nous voulons atteindre : Une image contenant texte

Description générée automatiquement

Cocher les deux cases : 

Une fois cette étape terminée, la configuration est aboutie.

Voici les différentes règles que nous venons de créer

OpenVPN :



WAN :



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

Une image contenant texte

Description générée automatiquement

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

Une encoche verte apparait à gauche quand il est bien installé :

Une image contenant texte

Description générée automatiquement

Dans VPN -> OpenVPN -> Client Export

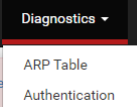
Selectionner « Archive » dans « Bundled Configurations »

Une image contenant texte

Description générée automatiquement

Récupérer le dossier.

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



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

Une image contenant texte

Description générée automatiquement

# OpenVPN

Sur notre client, on va télécharger OpenVPN Connect :

Une image contenant texte, Site web

Description générée automatiquement

Vous vous souvenez de l’archive que nous avons récupérée ? Ehh bien nous allons l’utiliser pour cette étape :

File -> Browse



Mon fichier :



Ensuite renseigner les informations nécessaires :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Nous en avons terminé avec Open VPN et PfSense.

# Messagerie – hMailServer & Thunderbird (Serveur&Client)

Nous allons installer hMailServer sur le serveur 1.

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

Une image contenant texte

Description générée automatiquement

Accepter et « Next » :

Une image contenant texte

Description générée automatiquement

Tout sélectionner et faire « Next »

Laisser l’option déjà sélectionnée :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

Lancer hmail en admin :

Une image contenant texte

Description générée automatiquement

# *Configuration de hMailServer*

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

Une image contenant texte

Description générée automatiquement

Sélectionnez « Add domain » :   
  
Une image contenant texte

Description générée automatiquement

Mettez votre nom de domaine :



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 :

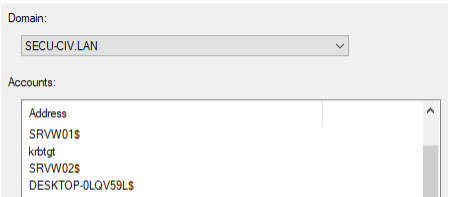


Dans le domaine que nous venons de créer, nous allons faire un clic droit sur « Accounts » et « Add AD account » :

Une image contenant texte

Description générée automatiquement

Sélectionner le domaine et l’utilisateur dans cette partie :



Et une fois sélectionner il doit être ajouter avec succès.

La prochaine étape et l’installation de Thunderbird et ça configuration :

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

Installer en standard :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

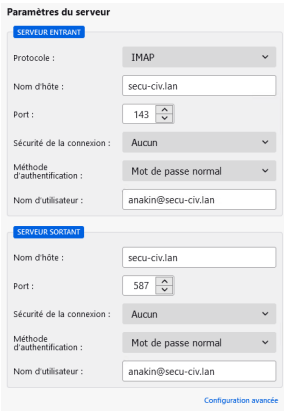
Une fois installé, lancez Thunderbird et connectez vous avec l’utilisateurs que vous avez créé sur votre hMailServer

Une image contenant texte

Description générée automatiquement

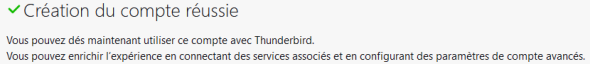
Cliquez sur configuration manuelle :

Appliquez les différents paramètres ci-dessous :



Si tout est opérationnel, ce message doit apparaitre après avoir appuyé sur « retester »  
  
Une image contenant texte

Description générée automatiquement



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

Faites un mail, envoyez le et vérifiez que vous ave bien réceptionné le mail   
Si vous l’avez, alors c’est gagner !

# Téléphonie – PBX & Linphone

Renseignez la commande suivante pour télécharger FusionPBX :



Installez le avec cette commande :



Sauvegarder ces informations :

Une image contenant texte

Description générée automatiquement

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

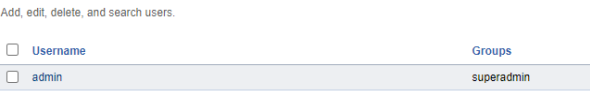


Une image contenant Site web

Description générée automatiquement

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 :



« Save » quand le mot de passe est changé :



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

Settings -> Domains

Une image contenant texte

Description générée automatiquement

Ajoutez un domaine et mettez la bonne IP de votre serveur

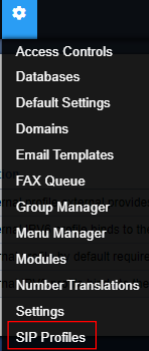
Une fois cela fait, votre domaine sera créé.

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

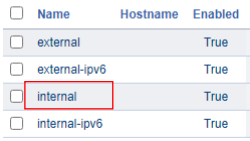
Une image contenant texte

Description générée automatiquement

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 :



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 : 

Faites un restart du premier et du troisième :



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



Lorsque c’est fait, vous devriez voir apparaitre 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.

Une image contenant texte

Description générée automatiquement

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 créer 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.

1. 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&d](https://www.zabbix.com/download?zabbix=6.0&os_distribution=ubuntu&os_version=20.04_focal&db=mysql&ws=apache) [b=mysql&ws=apache](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 :

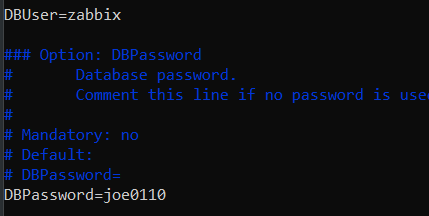
# mysql -uroot -p

\* 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

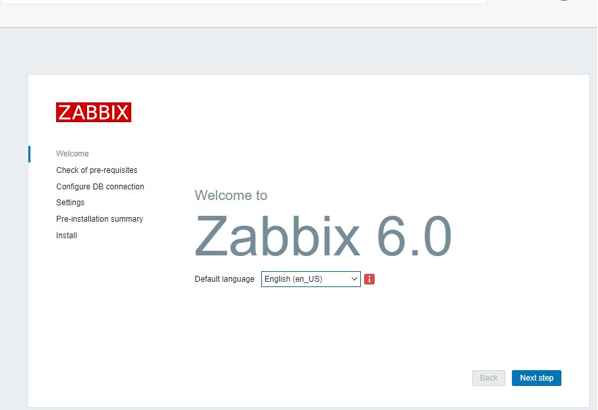
• A présent nous devons configurer le MDP de l’utilisateur de la BDD dans les fichiers de configuration de Zabbix :

• 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 :

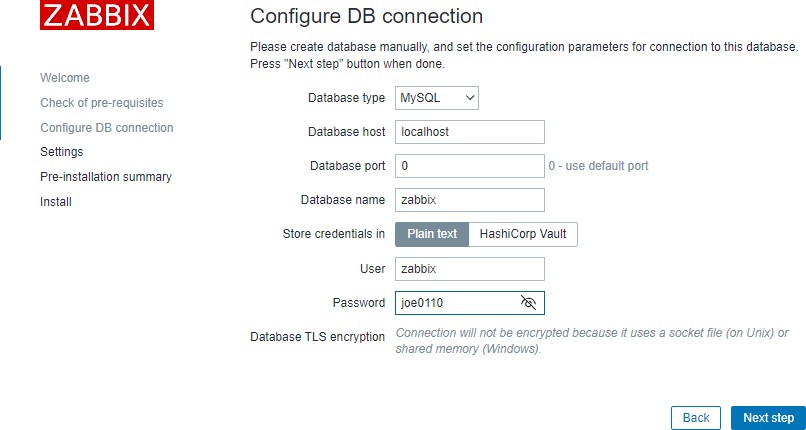


***Configuration :***

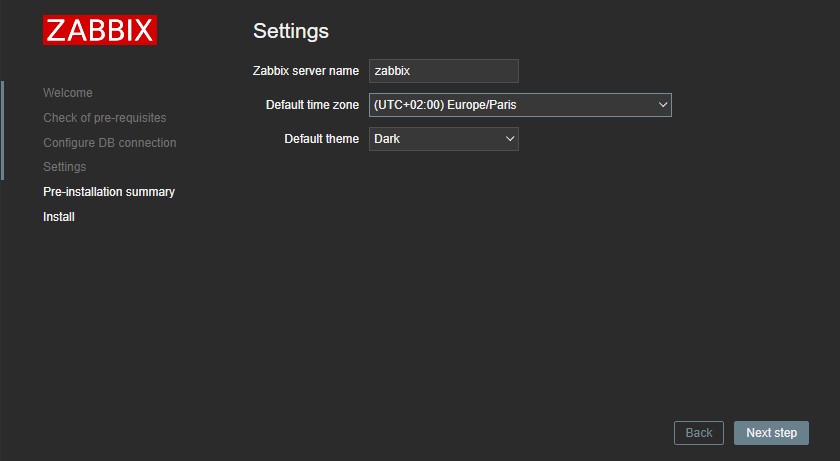
• Sélectionnez la langue, nous laisserons en Anglais

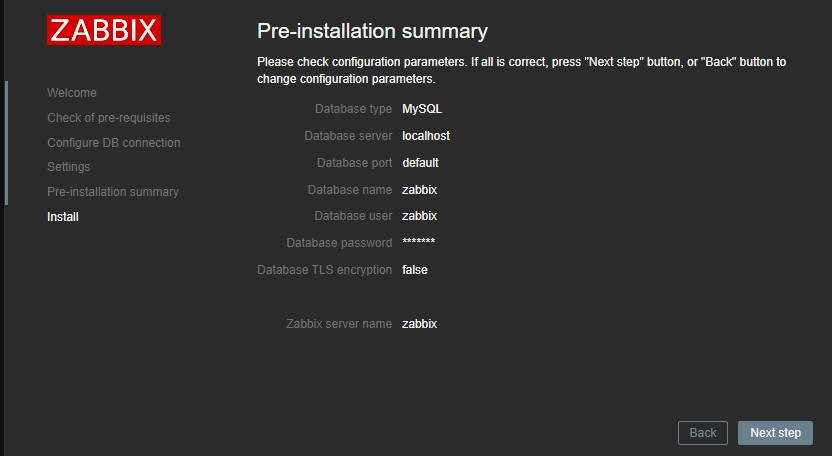


• Configuration de la connexion à la BDD

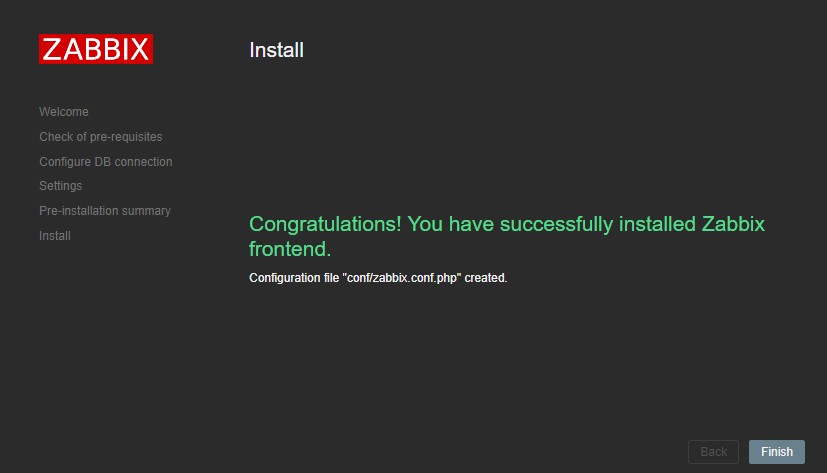


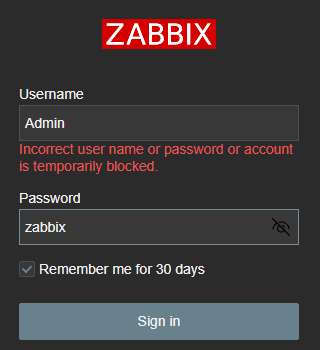
• Sélectionnez le nom du serveur ainsi que la timezone, nous pouvons également changer le thème.

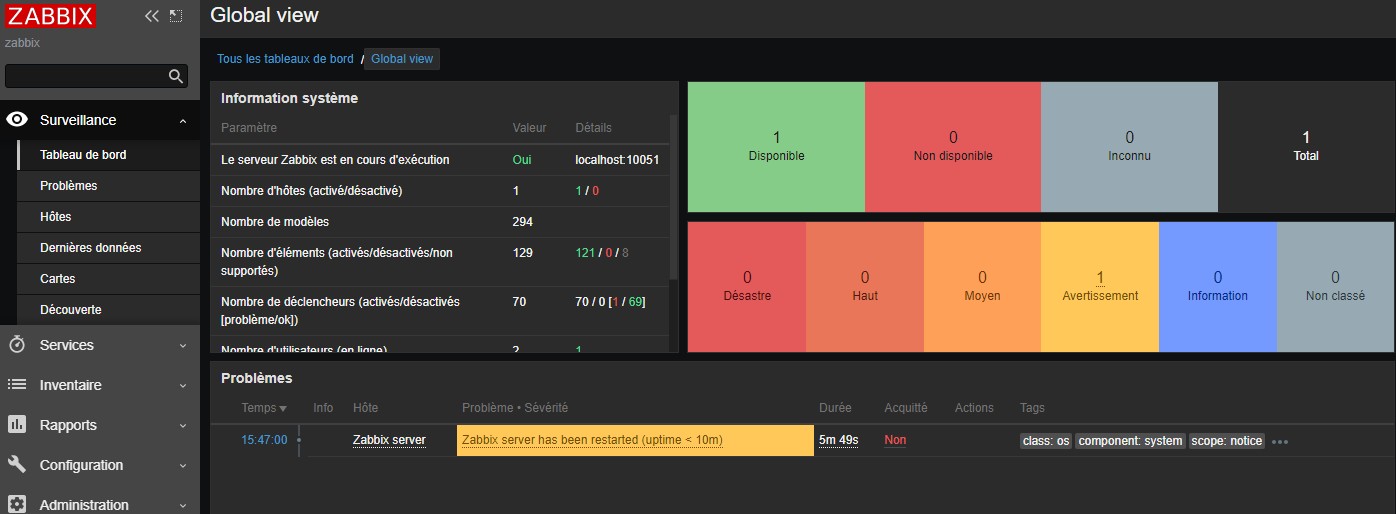


• Récapitulatif :

• 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

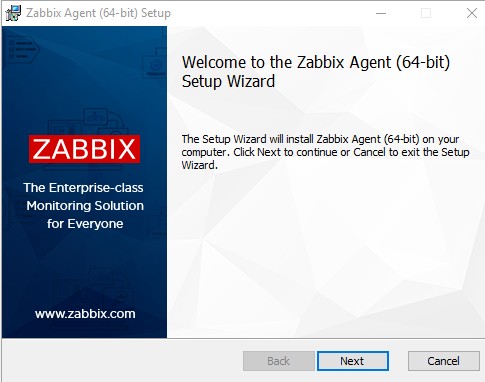
• Nous voilà connecté, la langue peut être modifié dans les paramètres utilisateurs > profil > langue.

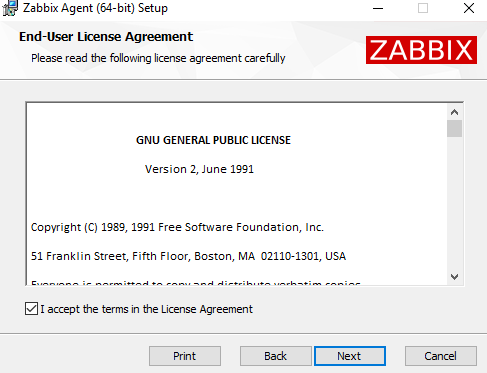
***Déploiement de l’agent Zabbix (Windows) :***

Une image contenant table

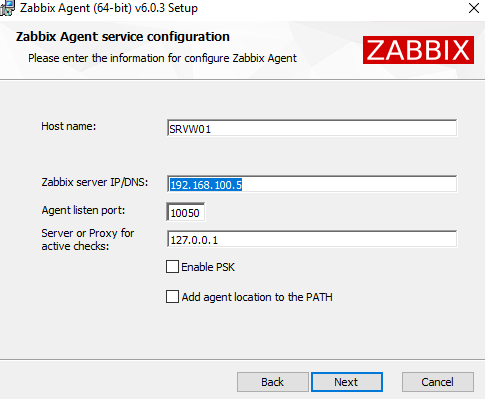
Description générée automatiquementNous allons déployer l’agent Zabbix sur notre serveur Windows Server 2019. Rendez-vous sur [https://www.zabbix.com/fr/download\_agents,](https://www.zabbix.com/fr/download_agents) puis télécharger l’agent correspondant à votre OS, ici nous choisirons Windows.

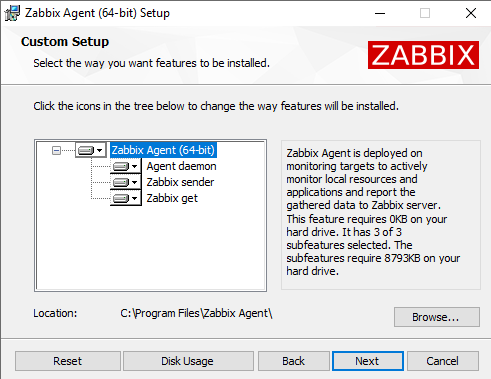
• Réalisez l’installation

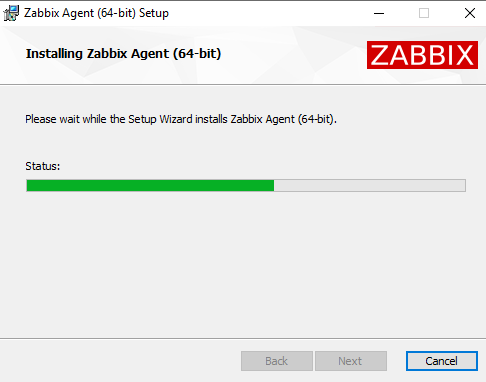
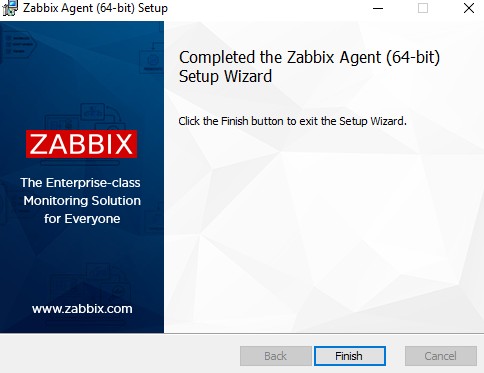




• Dans « Host name » renseignez un nom pour votre serveur Windows, dans « Zabbix server IP » renseignez l’adresse IP de votre serveur Zabbix. Le port par défaut est 10050. Ces paramètres pourront être modifiés ultérieurement dans les fichiers de configuration de l’agent Zabbix.





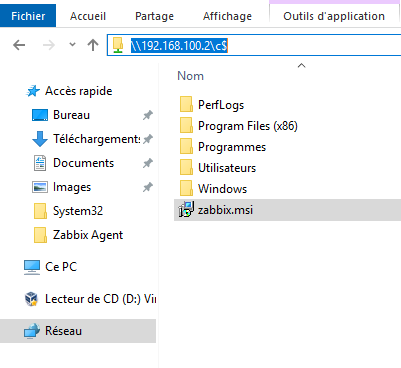


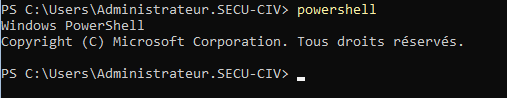
* On peut voir que le service Zabbix est bien en cours d’exécution



***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.

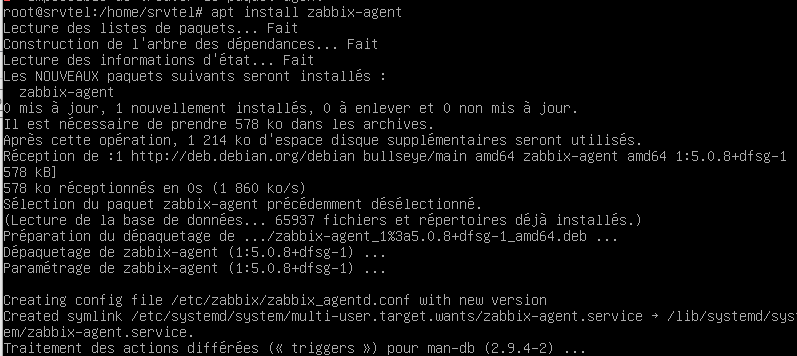
• Puis lancez la commande suivante pour installer l’agent Zabbix

* 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



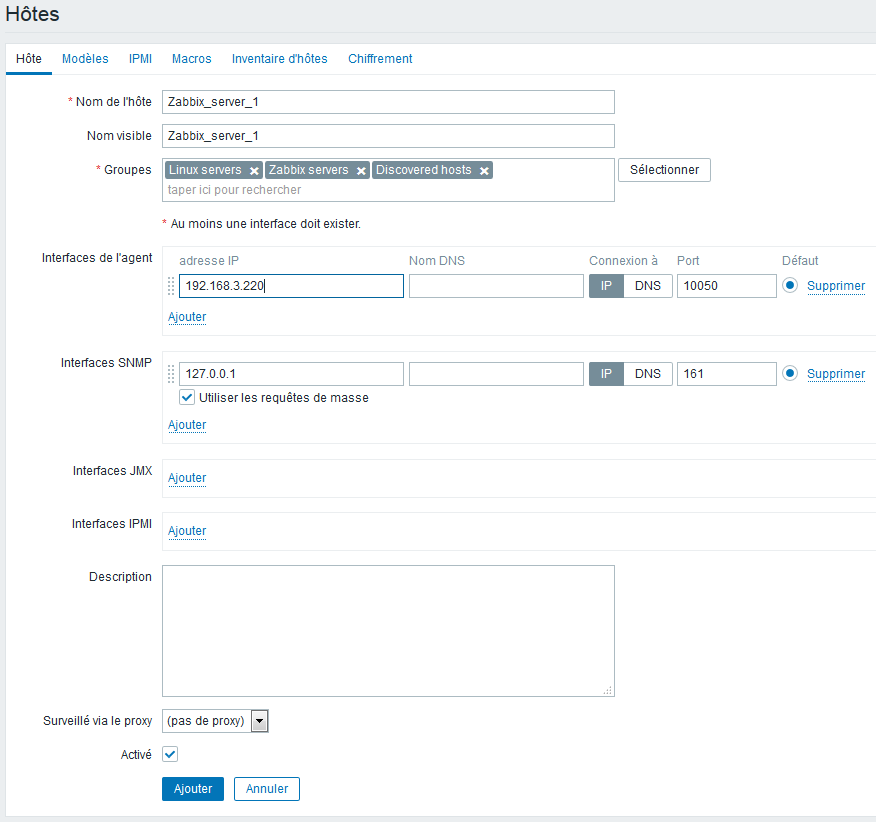
• Une fois l’installation terminée, rendez-vous dans les fichiers de configuration de l’agent Zabbix

• 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

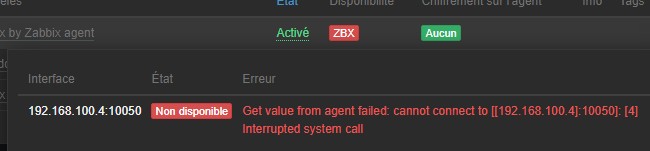
• Vous n’avez plus qu’à créer un hôte sur Zabbix



* + Résultat :



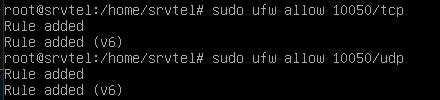
* + Si l’erreur suivante apparaît, pensez à ouvrir le port 10050 sur votre pare-feu

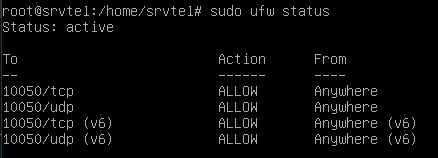


Sur DEBIAN (/Ubuntu) :

* + 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

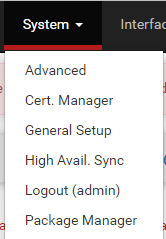


* + Ajoutez les règles suivantes
  + Pour voir les différentes règles, tapez :



***Déploiement de l’agent Zabbix (Pfsense)***

* + Rendez-vous dans « Packet Manager »



* + Puis cliquez sur « Available Packages »

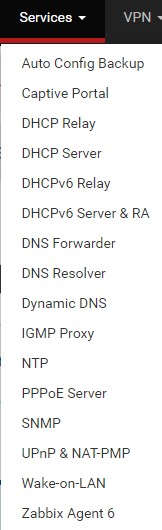


* + Cherchez « zabbix-agent6 » puis cliquez sur « + Install »

Une image contenant texte

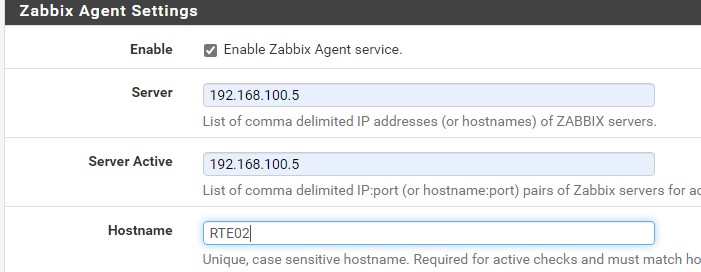
Description générée automatiquement

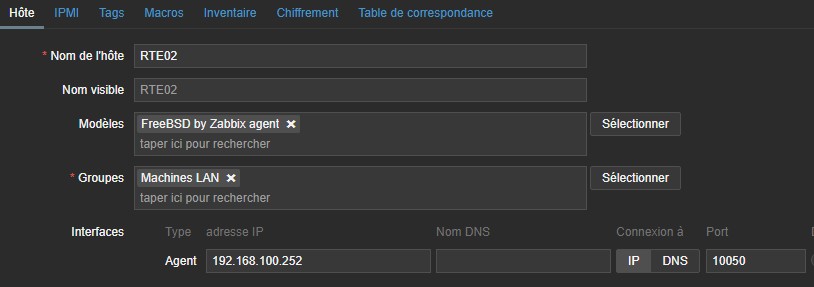
* + Rendez-vous dans « Services » puis « Zabbix Agent 6 »



* + Les paramètres à renseigner sont les suivants : « Server » - Serveur Zabbix ; « Server Active »

- Serveur Zabbix ; « Hostname » - Nom de votre routeur

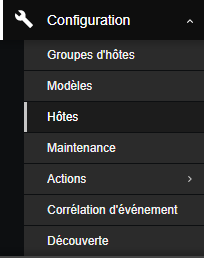


* + A présent, ajoutons notre routeur sur Zabbix
  + Notre routeur a bien été ajouté



***Création d’un groupe d’hôtes :***

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

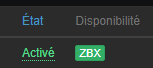


• En haut à droite, cliquez sur « Créer un hôte »

• 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.



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

• 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 serveurt.

***Monitoring d’un serveur Windows :***

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

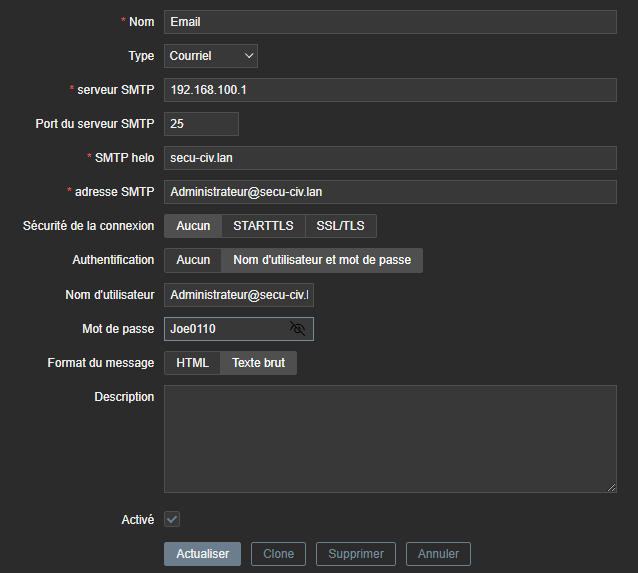
Ensuite nous avons accès aux différentes informations du serveur.

***Envoi d’un courriel en cas de dysfonctionnement d’un hôte :***

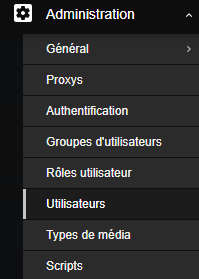
• Sur Zabbix, dans « Administration » cliquez sur « Types de média »



• Sélectionnez « Email »

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

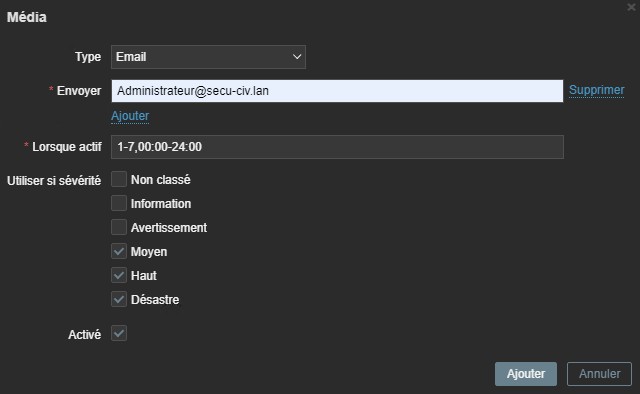
• A présent, dans « Administration », cliquez sur « Utilisateurs »



Une image contenant Site web

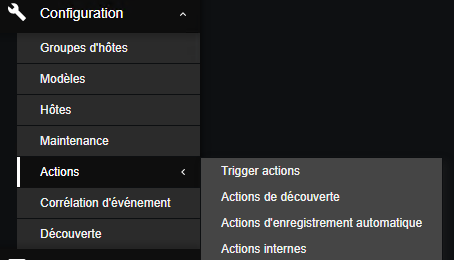
Description générée automatiquement• Sélectionnez l’utilisateur « Admin »

• 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 »

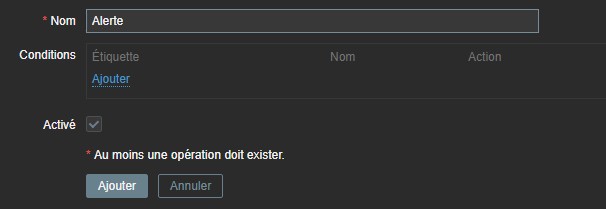
Une image contenant texte

Description générée automatiquement• Cliquez sur « Actualiser » afin de valider les paramètres

• 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 »

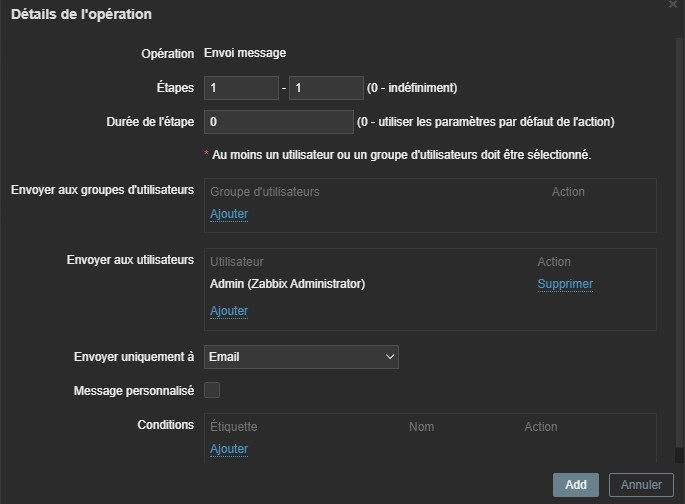
Une image contenant Site web

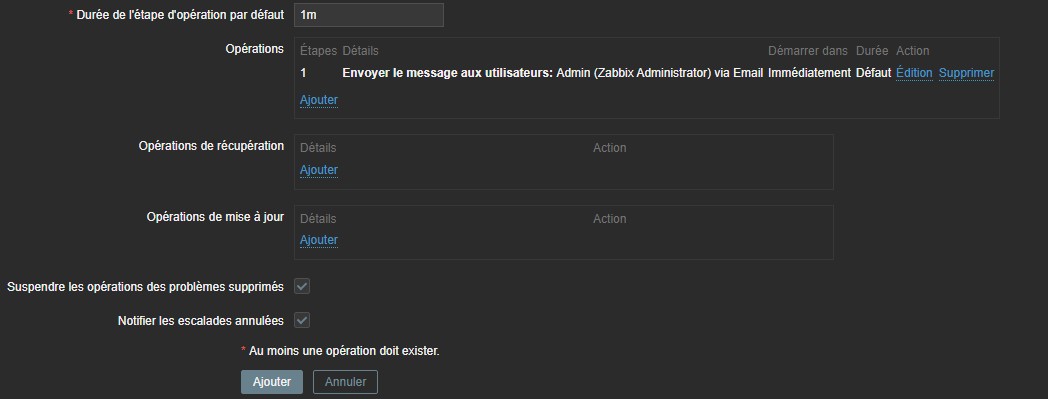
Description générée automatiquementLa condition d’envoi de courriel sera la suivante : la sévérité doit être supérieur ou égal à moyen

  
• 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 »

  
• Notre action a été créé

# Serveur WEB (eBrigade) / LAMP

# *Installation LAMP*



# *Installation eBrigade*

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

Envoyer le fichier vers le serveur Ubuntu



Commande pour dézipper :



Affichage une fois dézippé :



Création de la Base de données de eBrigade :



Tapez cette commande :



Création utilisateur eBrigade :

Une image contenant texte

Description générée automatiquement

Renseignez un identifiant et un mot de passe.

Maintenant nous allons nous connecter à l’interface web :

Une image contenant texte

Description générée automatiquement

Si ça fonctionne vous aurez cette image :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement Une image contenant texte

Description générée automatiquement

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

