Projet ECKHO

Table des matières

Présentation du projet

Le projet ECKHO consiste à concevoir et déployer une infrastructure informatique complète incluant :

- Un domaine Active Directory,
- Des services réseau (DNS, DHCP),
- Un pare-feu pfSense,
- Un serveur Web (WordPress),
- Un serveur mail,
- Un réseau Wi-Fi Invités isolé,
- Un outil de supervision (Centreon),
- Un serveur de fichiers centralisé.

L’objectif est d’obtenir une infrastructure sécurisée, segmentée et supervisée.

Adressage IP SALAUN TRAVELS

Serveurs (LAN — 10.5.0.0/16)

VM	Rôle	IP	Masque	VLAN
DC1	Contrôleur de domaine principal	10.5.10.0	/16	LAN
DC2	Contrôleur de domaine secondaire	10.5.20.0	/16	LAN
Serveur-mail	Messagerie centralisée	10.5.40.0	/16	LAN
SerFich	Serveur de fichiers	10.5.50.0	/16	LAN
BACKUP	Sauvegarde centralisée	10.5.10.5	/8	LAN
PfSense	Pare-feu / Routeur	10.5.30.1	/16	LAN

DMZ (VLAN 50 — 10.9.0.0/16)

VM	Rôle	IP	Masque	VLAN
DMZ	Passerelle DMZ	10.6.60.1	/24	DMZ
Web	Serveur Web WordPress	10.6.60.10	/24	DMZ

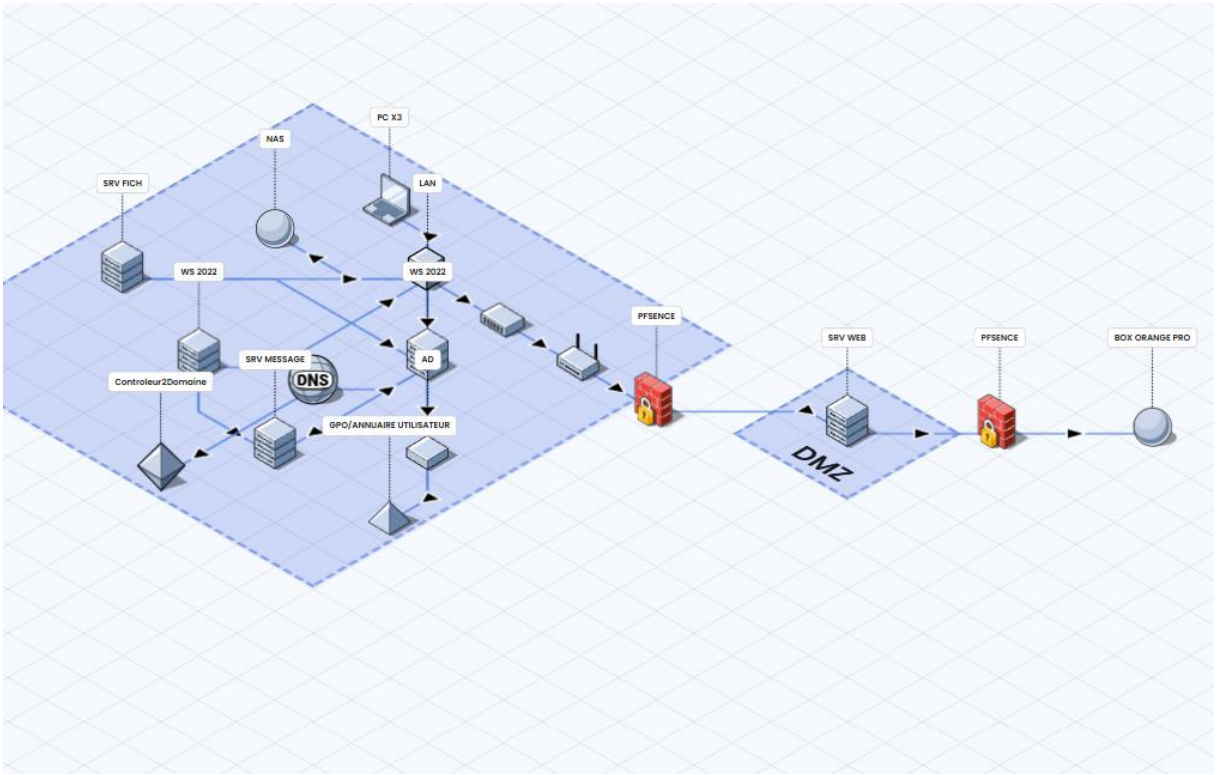
Postes clients

VM	Rôle	IP	VLAN
Client2	Poste utilisateur siège	DHCP (10.7.x.x)	Siège (30)

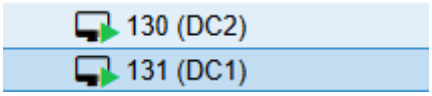
VLANs PfSense

VLAN	Nom	Gateway	Réseau
LAN	Serveurs	10.5.30.1	10.5.0.0/16
20	WiFi Invité	10.6.0.1	10.6.0.0/16
30	Siège	10.7.0.1	10.7.0.0/16
40	Agences	10.8.0.1	10.8.0.0/16
50	DMZ	10.9.0.1	10.9.0.0/16
60	WiFi Interne	10.10.0.1	10.10.0.0/16

Schéma d’architecture réseau.

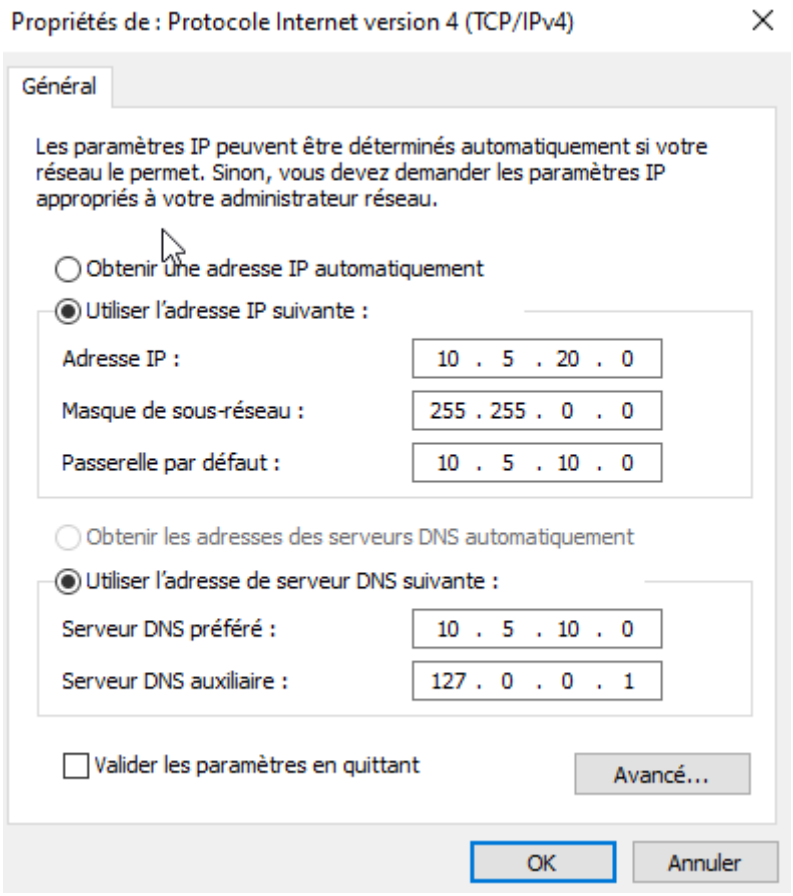


Création des serveurs Active Directory

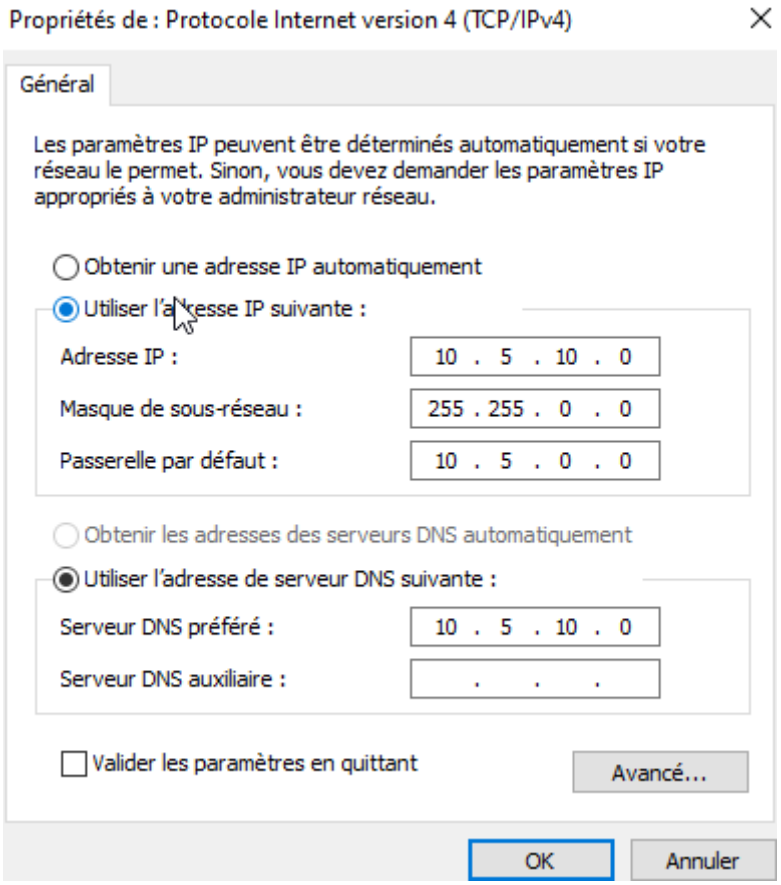


Création des active directory dans Proxmox.

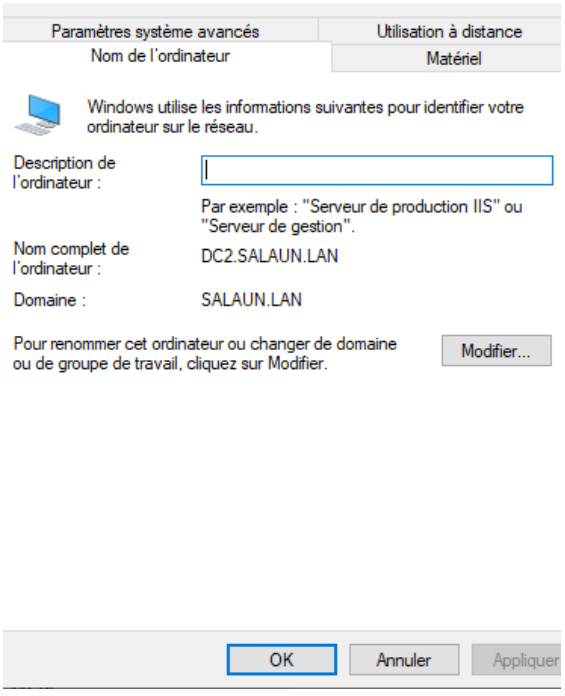
Paramétrage IP de DC2 :

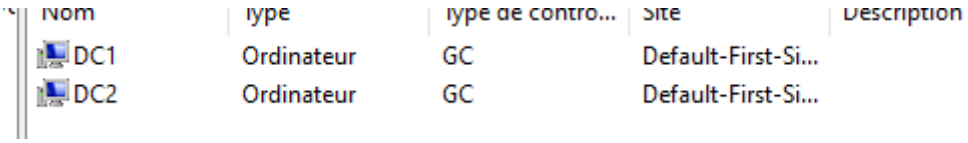


Paramétrage IP de DC1 :

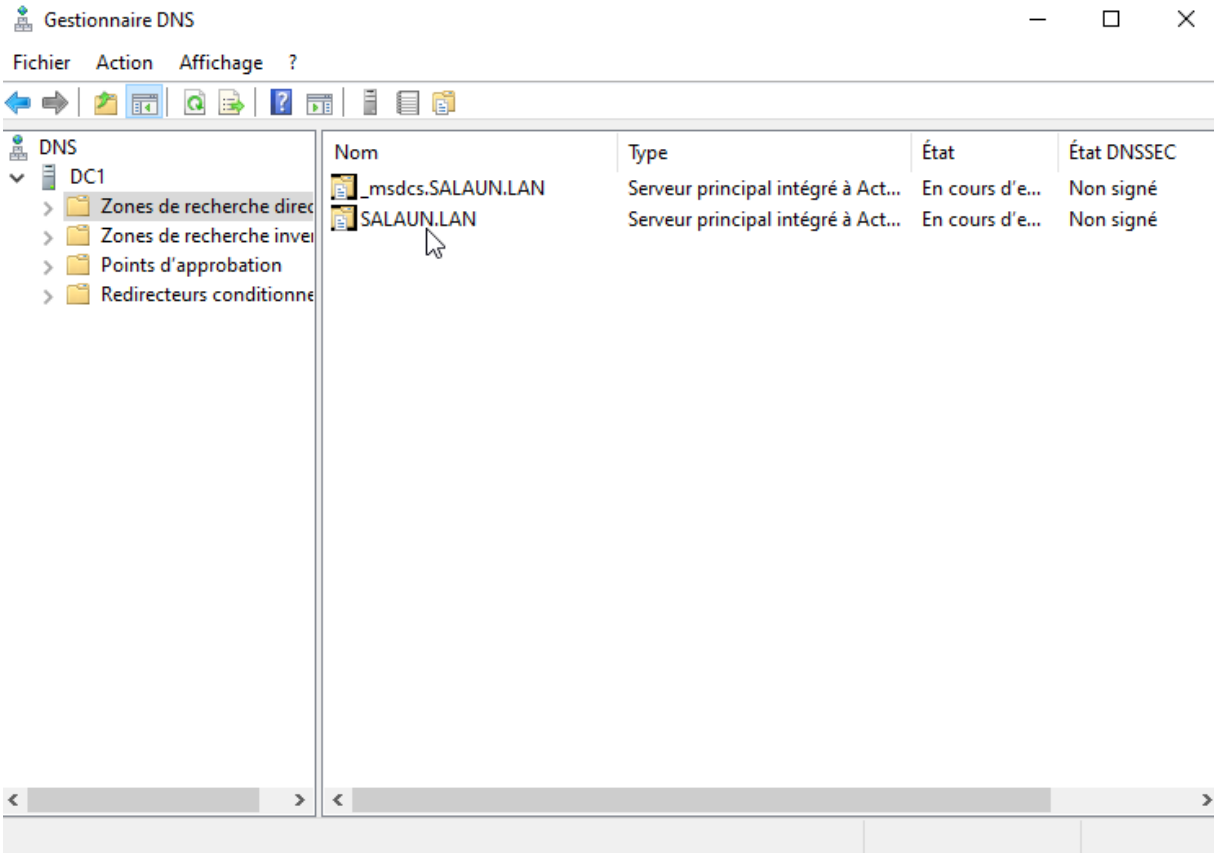


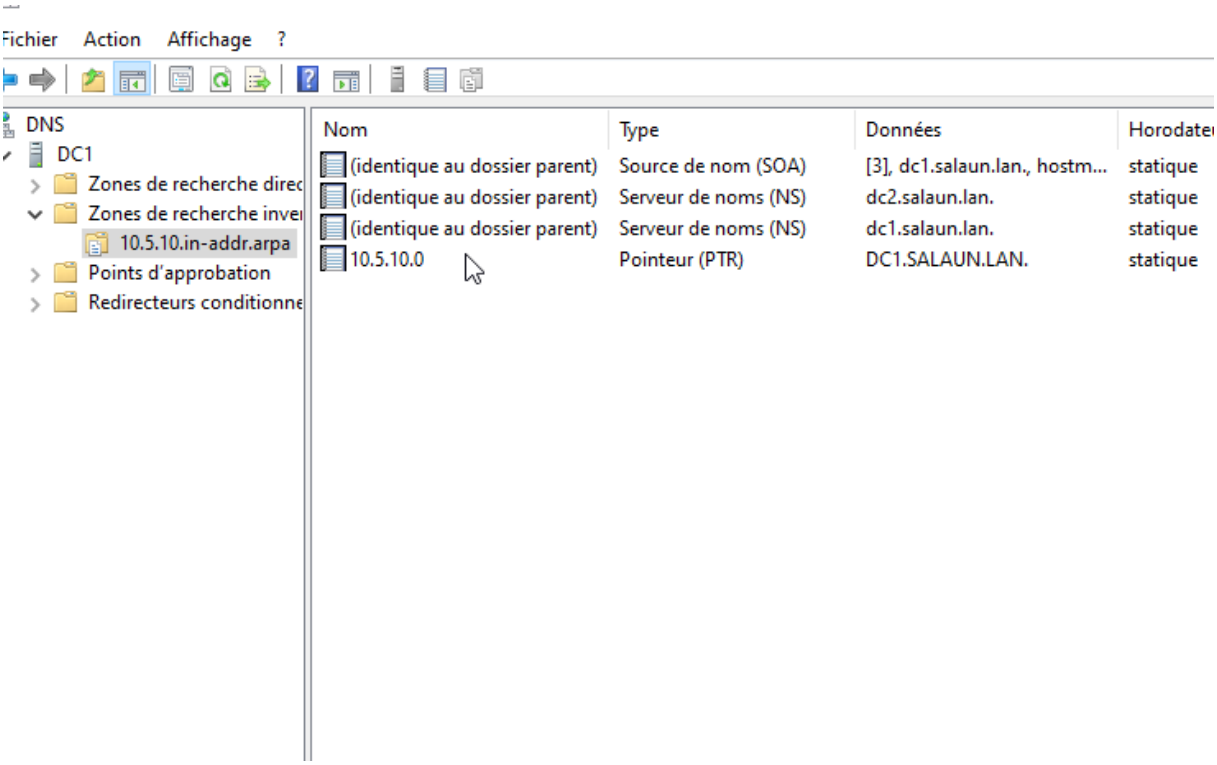
Nous rejoignons le domaine avec DC2 dans notre cas salaun.lan :

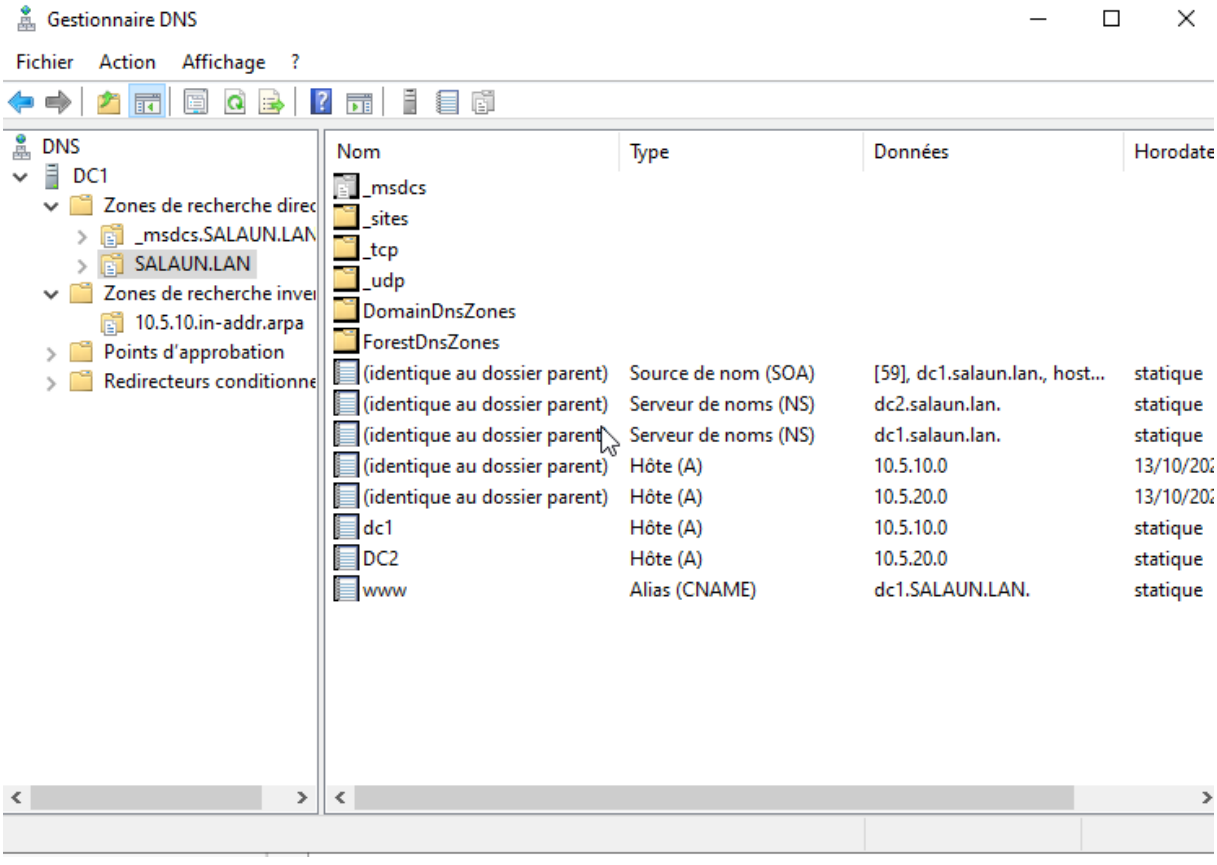




Nous pouvons donc maintenant configurer le DNS :



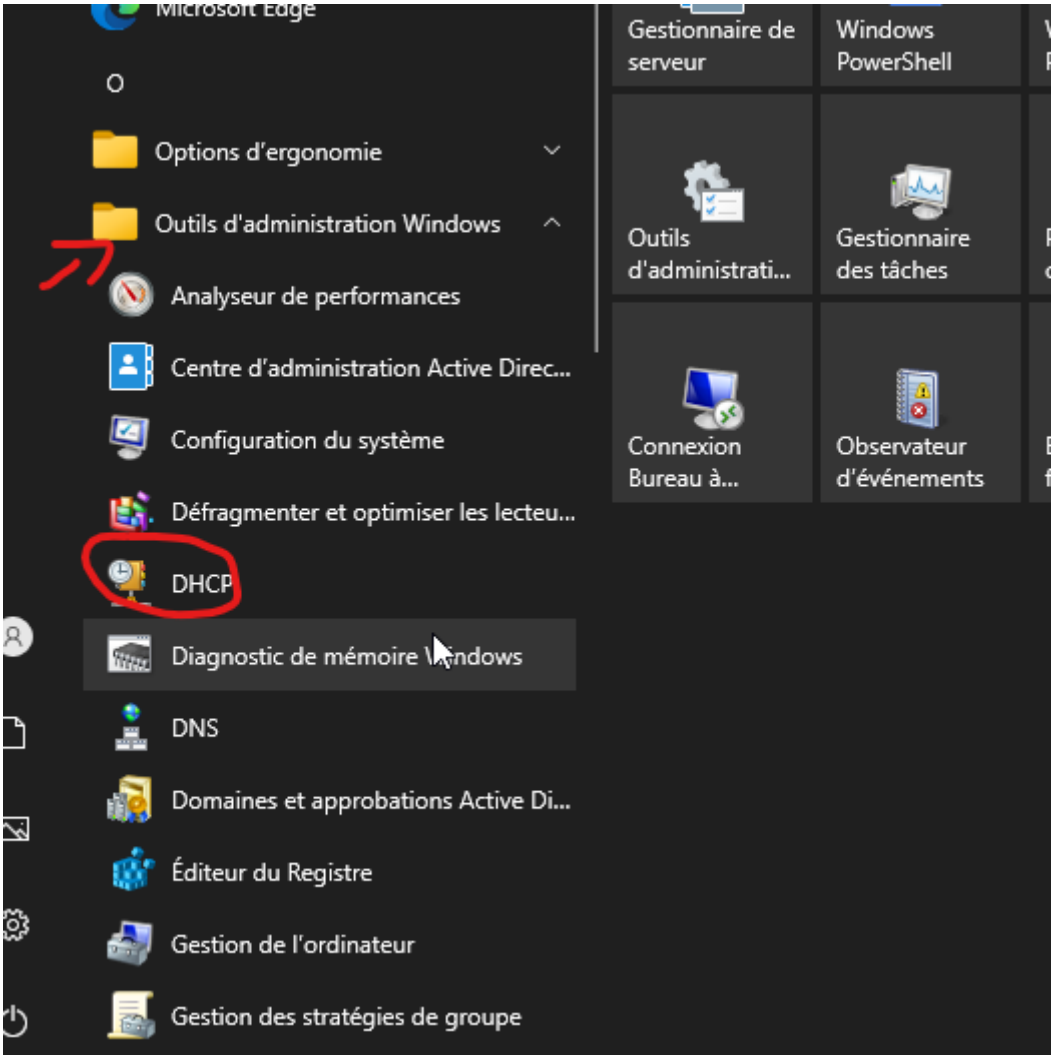

Fichier Action Affichage ?
DNS
DC1
Zones de recherche direc
Zones de recherche inver
10.5.10.in-addr.arpa
Points d'approbation
Redirecteurs conditionne
Nom
Type
Données
Horodate
(identique au dossier parent)
Source de nom (SOA)
[3], dc1.salaun.lan., hostm...
statique
(identique au dossier parent)
Serveur de noms (NS)
dc2.salaun.lan.
statique
(identique au dossier parent)
Serveur de noms (NS)
dc1.salaun.lan.
statique
10.5.10.0
Pointeur (PTR)
DC1.SALAUN.LAN.
statique


Gestionnaire DNS
Fichier Action Affichage ?
DNS
DC1
Zones de recherche direc
_msdcs.SALAUN.LAN
SALAUN.LAN
Zones de recherche inver
10.5.10.in-addr.arpa
Points d'approbation
Redirecteurs conditionne
Nom
Type
Données
Horodate
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(identique au dossier parent)
Source de nom (SOA)
[59], dc1.salaun.lan., host...
statique
(identique au dossier parent)
Serveur de noms (NS)
dc2.salaun.lan.
statique
(identique au dossier parent)
Serveur de noms (NS)
dc1.salaun.lan.
statique
(identique au dossier parent)
Hôte (A)
10.5.10.0
13/10/202
(identique au dossier parent)
Hôte (A)
10.5.20.0
13/10/202
dc1
Hôte (A)
10.5.10.0
statique
DC2
Hôte (A)
10.5.20.0
statique
www
Alias (CNAME)
dc1.SALAUN.LAN.
statique

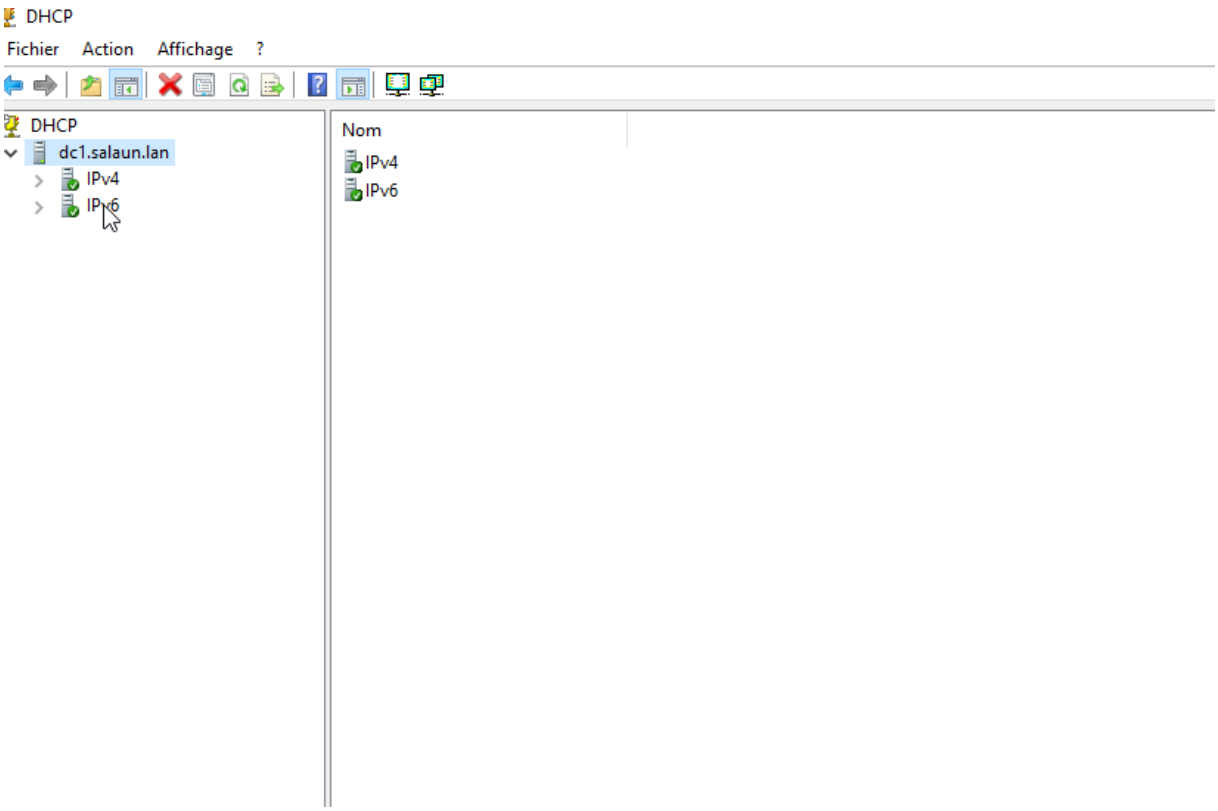
Configuration du DHCP :

On active le DHCP depuis l'assistant d'ajout de rôles et de fonctionnalités.

Dans « Outils d'administration Windows » cliquez sur DHCP.

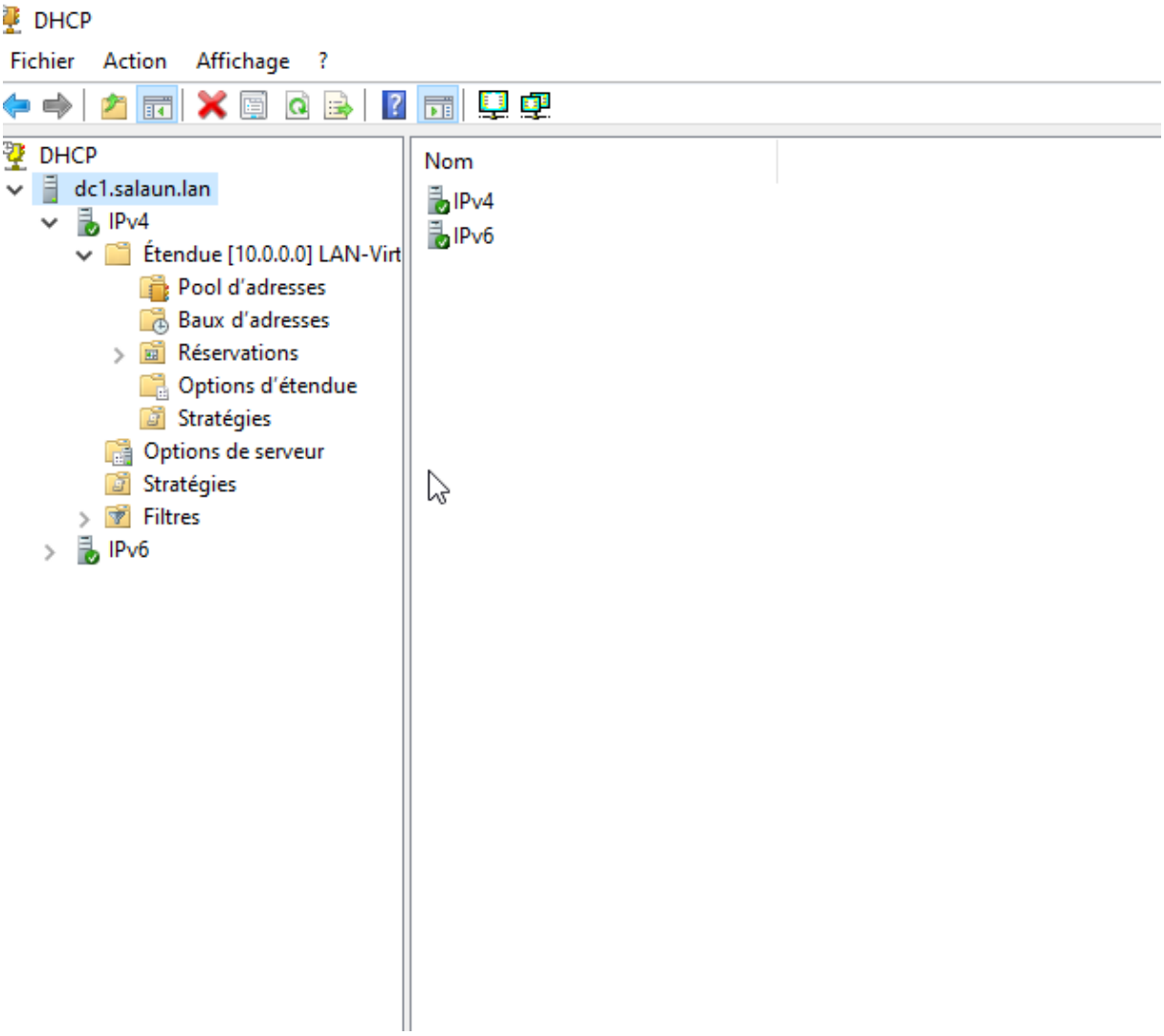


Vous arriverez sur cette page :

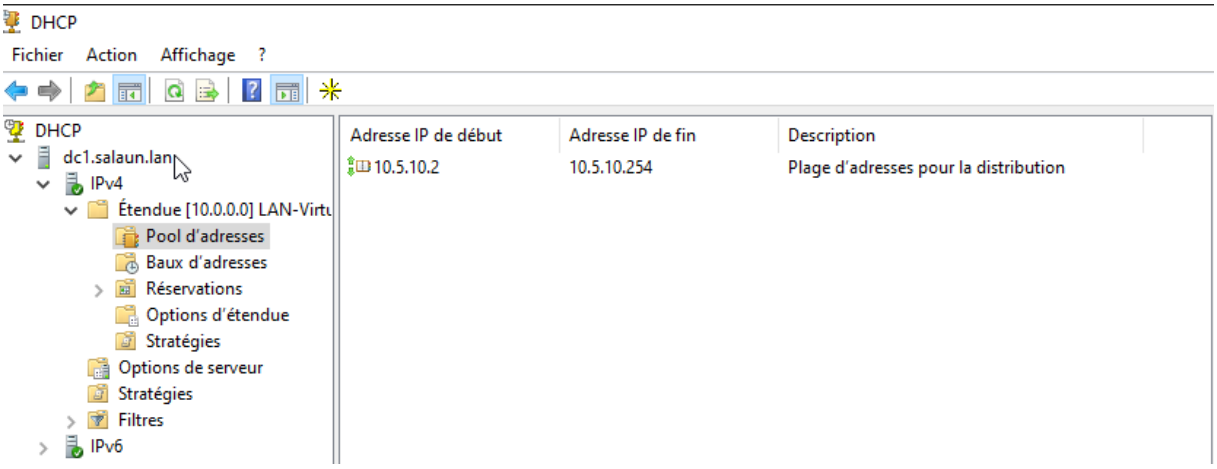


En effectuant un clic droit sur IPv4 puis « nouvelle étendue » et suivre les différentes étapes.

Vous devriez obtenir ce résultat :

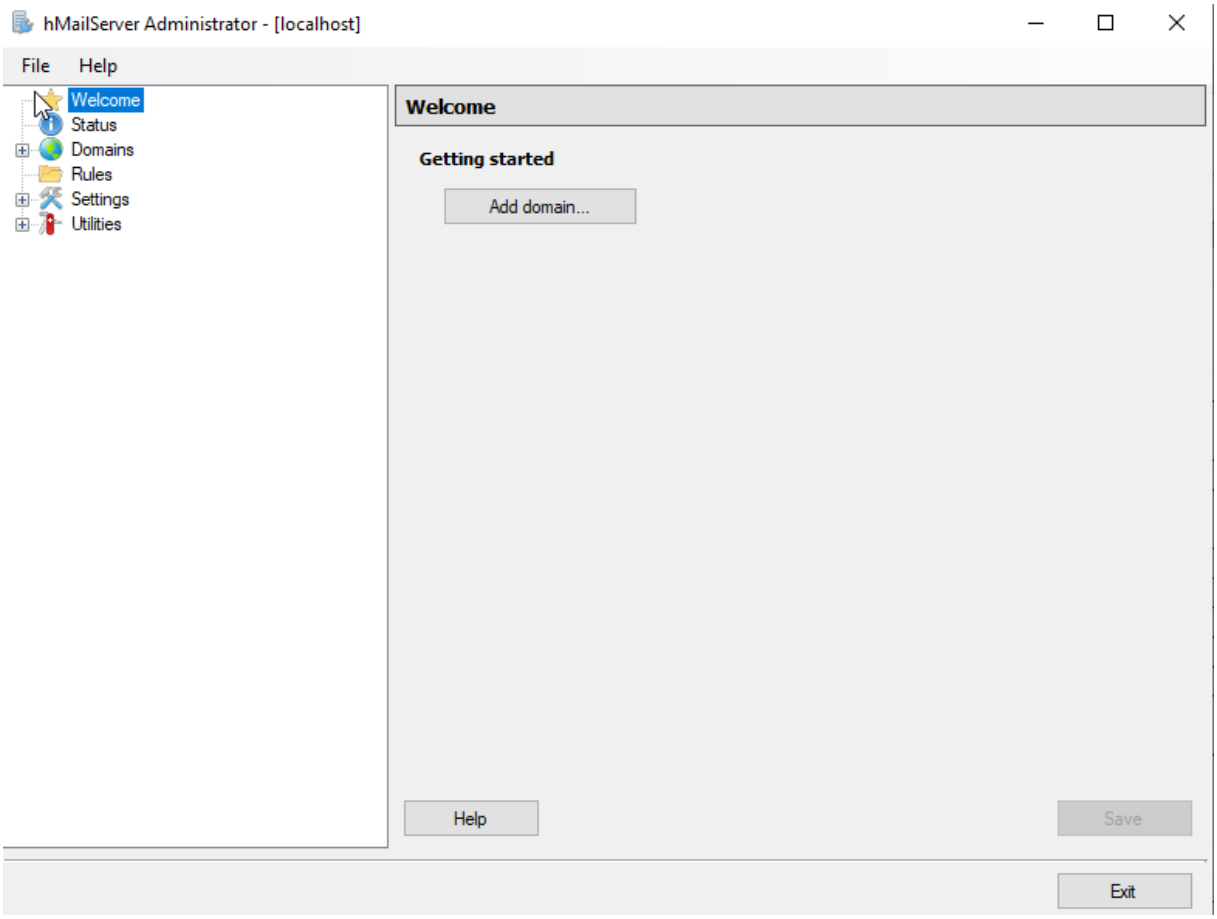


Une fois sur cette page allez dans pool d'adresses pour pouvoir ajouter notre etendue d'adresses que les diffrents clients recevrons :



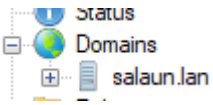
Configuration du serveur mail

Installation de hMailServer

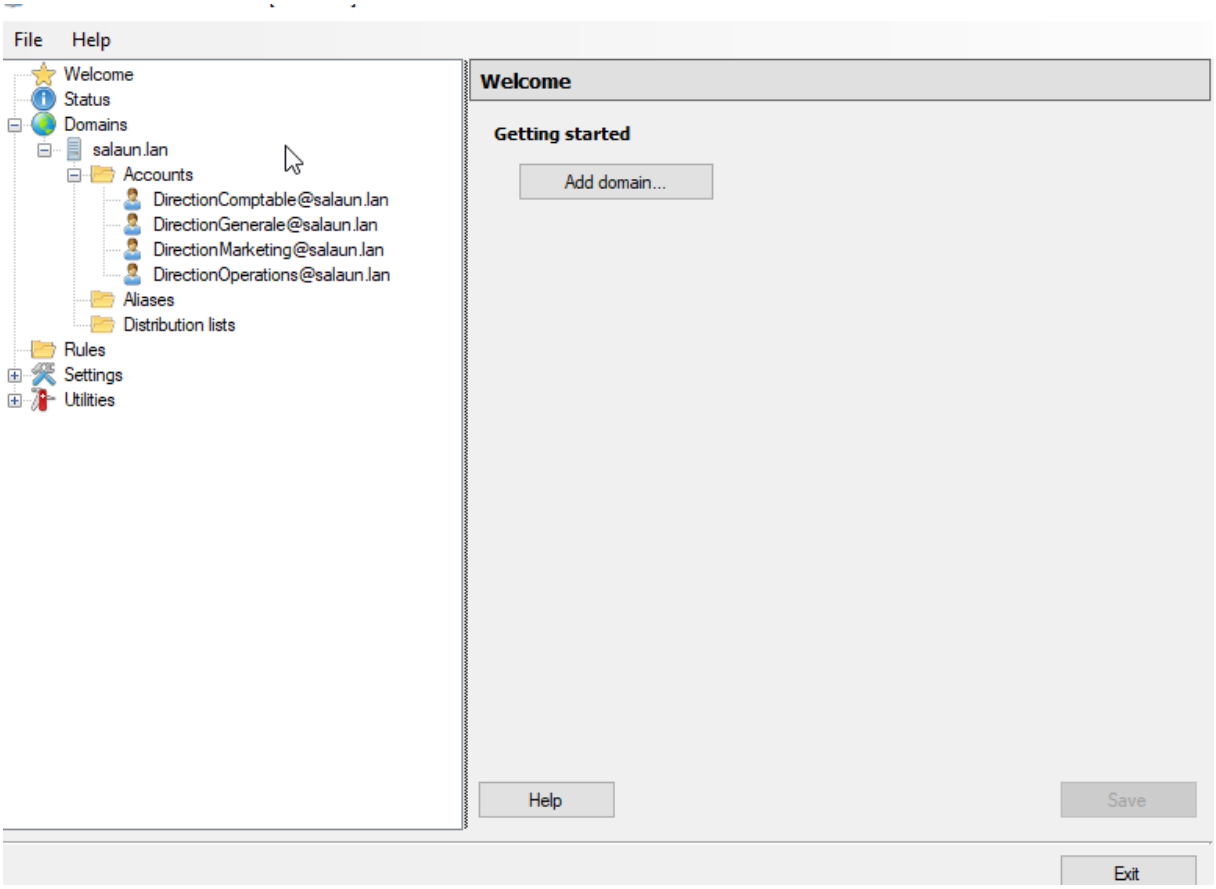


Après l'installation on arrive sur cette page et on ajoute un domaine.

Dans notre cas salaun.lan

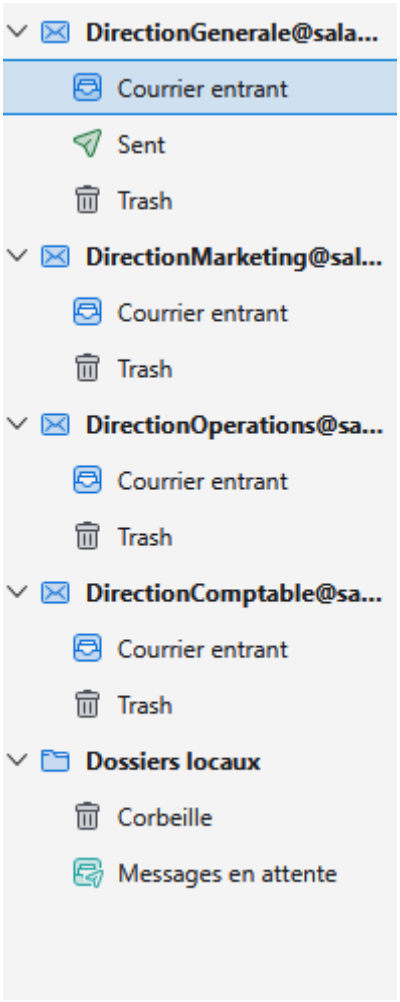


Puis dans « Accounts » nous ajoutons les comptes.



Nous choisissons un client mail ici Mozilla Thunderbird

Dans « Paramètres des comptes nous ajoutons les comptes déjà renseigner dans hMailServer »



Serveur Web

Mise en place d'une machine Debian 12.

|-> Ip fixe : 10.5.60.0

```
root@Web:/etc/apache2/sites-available# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0@if451: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:0d:ed:9b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.5.60.0/24 brd 10.5.60.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe0d:ed9b/64 scope link
       valid_lft forever preferred_lft forever
root@Web:/etc/apache2/sites-available#
```

Installation de MariaDB, Apache2, et MySQL.

|->apt install apache2 -y

|->apt install mariadb-server -y

|-> sudo apt install php php-mysql php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip libapache2-mod-php -y

Création base de données Wordpress

|->CREATE DATABASE wordpress_db;

CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'MDP';

GRANT ALL PRIVILEGES ON wordpress_db.* TO 'wordpress_user'@'localhost';

FLUSH PRIVILEGES;

EXIT;

Installation de Wordpress/ droits / déplacement des fichiers au bon endroit.

|->wget https://wordpress.org/latest.tar.gz tar -xvzf latest.tar.gz sudo mv wordpress /var/www/html/ sudo chown -R www-data:www-data /var/www/html/wordpress sudo chmod -R 755 /var/www/html/wordpress

Configuration Apache

|->nano /etc/apache2/sites-available/wordpress.conf

Y ajouter :

```
<VirtualHost *:80>
    ServerAdmin admin@example.com
    DocumentRoot /var/www/html/wordpress
    ServerName votre-domaine.com

    <Directory /var/www/html/wordpress/>
        Options FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Activation du site et du module rewrite

|->a2ensite wordpress.conf

|->a2enmod rewrite

|->systemctl restart apache2

Accès site

http://10.5.60.10

Erreur a éviter en créent le serveur WordPress éviter de mettre une adresse ip de réseau comme 10.5.60.0 le zero a la fin signifie adresse de réseau il faut mettre une adresse de machine comme exemple :10.5.60.10 . car le pfsence bloque l'accès avec l'adresse 10.5.60.0

Pourquoi pfSense bloquait l'accès avec 10.5.60.0

10.5.60.0 = adresse réseau

Dans un réseau /16, .0 identifie tout le réseau, pas une machine.

Une machine ne peut pas utiliser cette IP.

NAT / Redirection pfSense

pfSense doit savoir vers quelle machine envoyer le trafic WAN.

Avec .0, il ne sait pas quelle machine réelle doit recevoir le paquet.

Résultat : la redirection ne fonctionne pas → site inaccessible.

Passerelle .1

.1 est généralement pfSense lui-même, donc pas utilisable par le serveur.

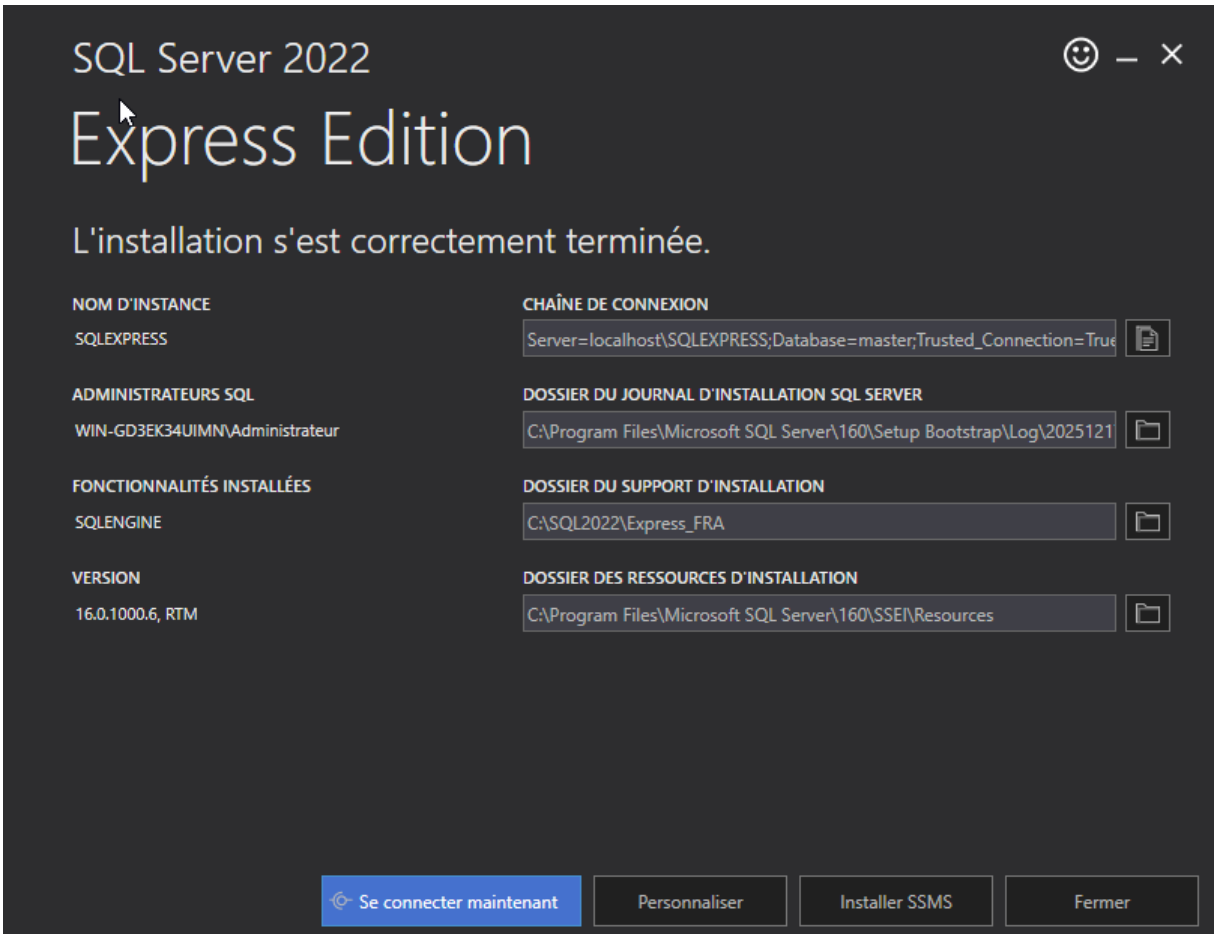
Solution : donner au serveur une IP valide comme 10.5.60.10

PfSense peut maintenant rediriger correctement le trafic WAN → serveur → WordPress accessible.

Mot de passe des utilisateurs

Nom	Prenom	Role	MDP
PODER	VALY	Compta fournisseur	3cz3LDgJt
PHILON	VALERIE	Compta fournisseur frais généraux	6Co?zLxrDs
AUTRET	FRANCK	Directeur de réseau	H@!6bCP!gm
MARCHAND	FREDERIC	Directeur	L5JVOrW
COURSIER	STEFAN	Informatique	SdxWW23
DEMAY	ROSELINE	Compta clients	o@6a84Nxk$
ALIX	PASCALE	Compta générale	SRsKRE6@Lg
JEAGLE	MARIE	Commercial	t4pSr9M$gs
BERTHEL	ANAIS	Accueil	T5i5?NiH$3
PENPENY	HUGUES	Administrateur réseaux et systemes	Sz!ecygP4o
LEMEN	MANON	Exploitation	7Xdi?rdBdy
PERRON	AURELIE	Formalités	hm46d@GfTf
COLLET	AUDE	Gestion des produits Autocar France et etrangers	9Bp$HDCMt4
JUSTAL	JULIE	Gestion des voyages	QdT!rNtb9S
ROCHEFORT	ISABELLE	Maquettiste	bx&NGTF43R
PANIS	OLIVIER	Pilote amateur	zBK6QpTe3
LOEB	SEBASTIEN	Pilote pro	DimAqFK8$L
GUINARD	PATRICIA	Prod	9D!i@zGFMX
THOUROUDE	ERIC	Production avion	PfRdYj&q7E

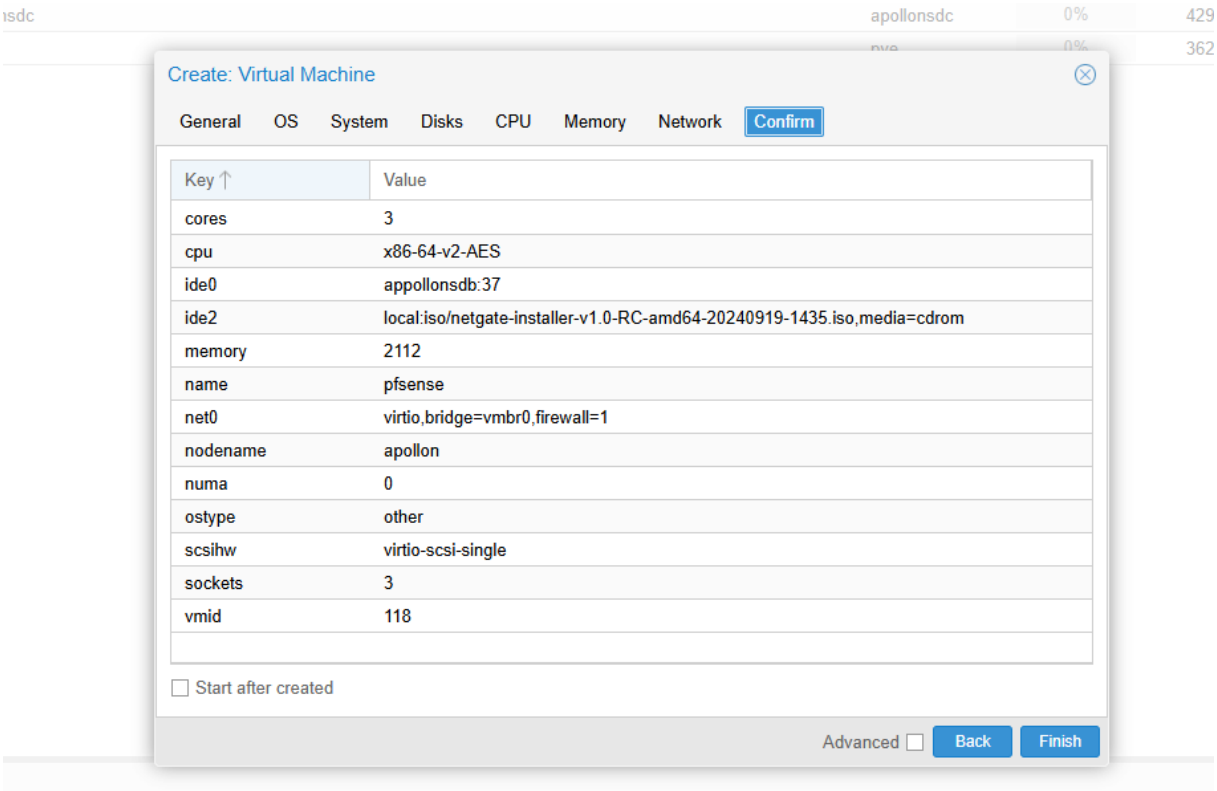
ROLLAND	ANGELIQUE	Qualité	$kXrph?K4$
LEBEC	FLORENCE	Responsable Agence	h&bRToxax7
SALAUN	HUGO	Service web	t4$JpN8x7s!
PAULI	PHILIPPE	Transport	$p7jtaKz6x



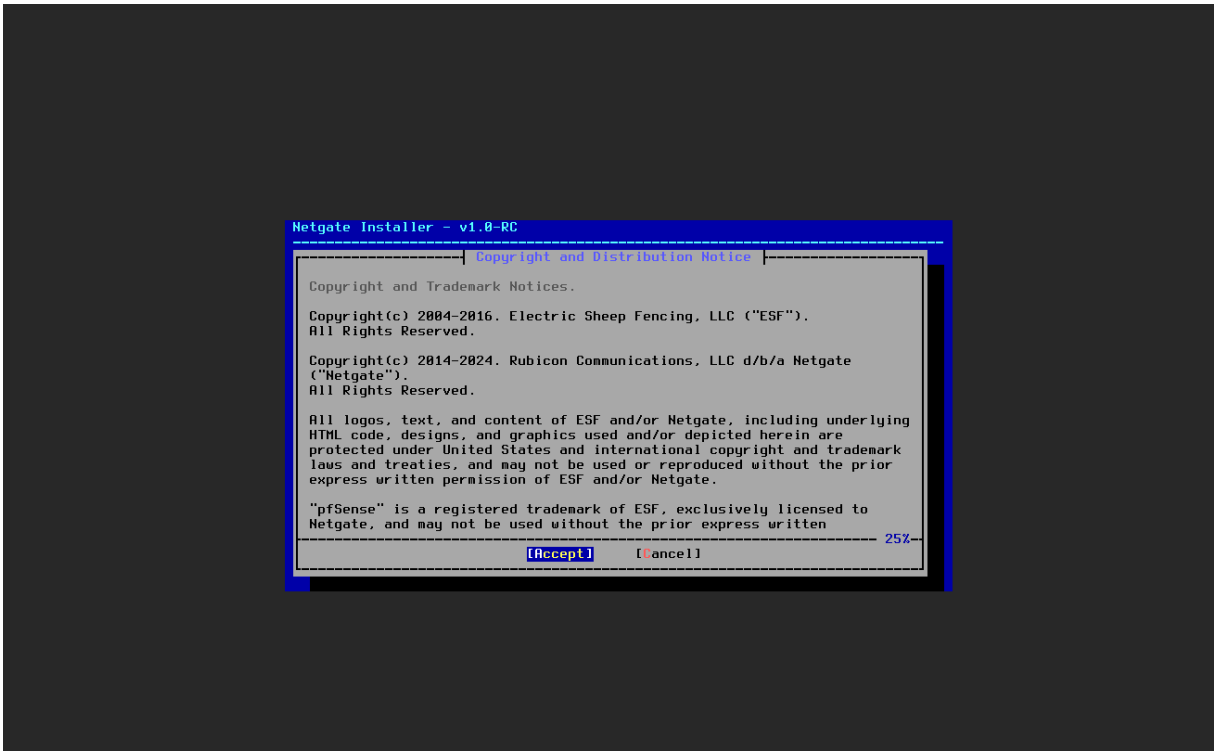
AP4 : Perfectionnement et ajout sur l'infrastructure réseau de Salaun.

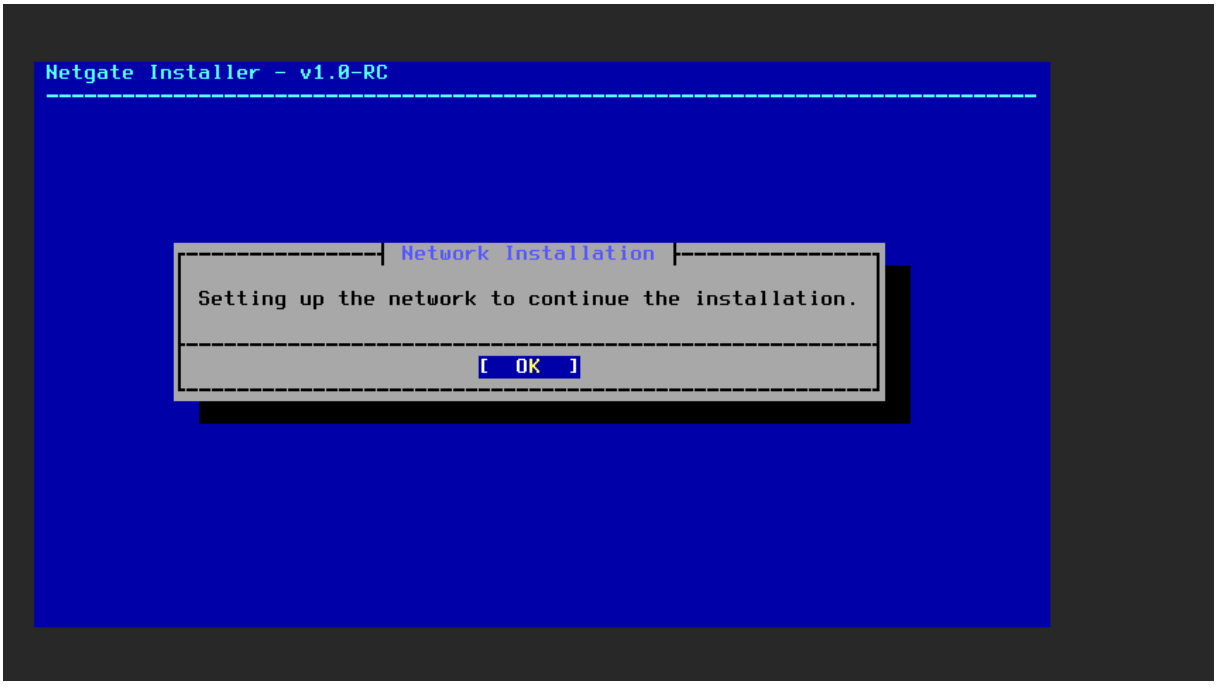
Configuration Pfsense

Création et installation de Pfsense



Voici une capture de la configuration de la machine virtuelle. Si tous les paramètres sont corrects, cliquer sur Finish pour lancer la création de la machine virtuelle.





Acceptation des licences (Copyright and Distribution Notice)

Lorsque l'installateur PfSense démarre, la première fenêtre affichée contient les informations de copyright et de licences d'utilisation.

Cet écran rappelle que PfSense et ses composants sont protégés par les droits d'auteur et que leur utilisation est soumise aux conditions de Netgate.

Action à effectuer :

1. Lire les informations affichées.
2. Sélectionner l'option Accepte à l'aide des flèches du clavier.
3. Valider avec Entrée pour poursuivre l'installation.

Initialisation du réseau (Network Installation)

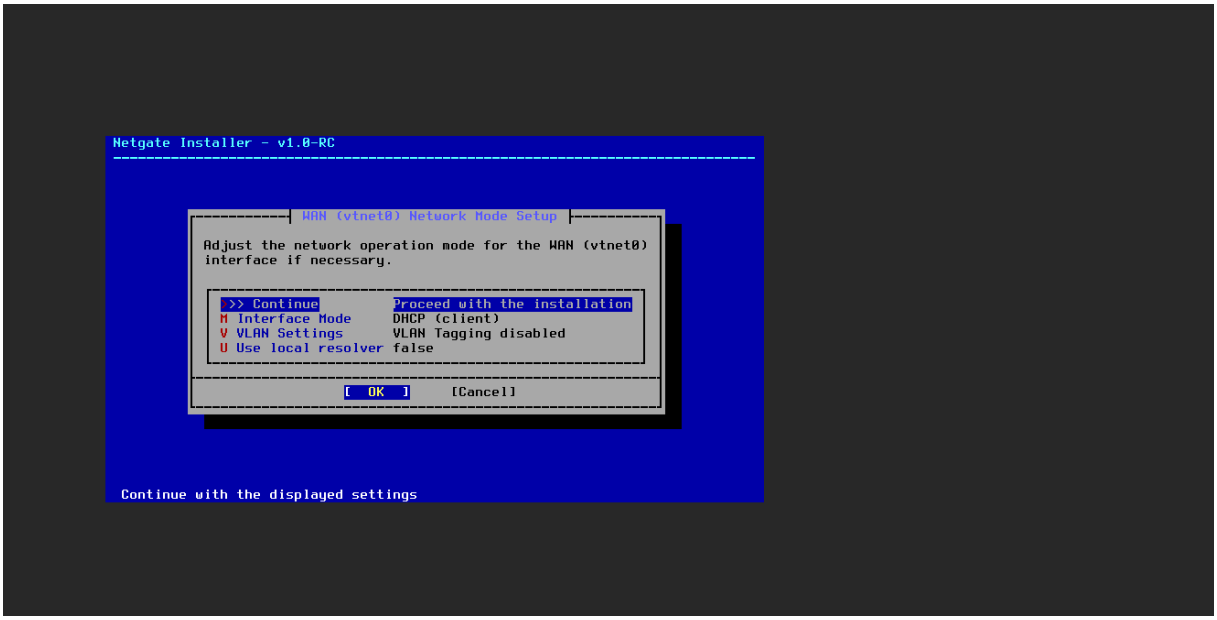
Après avoir accepté les licences, une fenêtre intitulée "Network Installation" apparaît. Cette fenêtre informe que PfSense procède à la configuration réseau minimale nécessaire pour continuer l'installation.

Le message affiché est :
"Setting up the network to continue the installation."

Action à effectuer :

- Appuyer sur Entrée pour valider l'option OK.

Une fois cette étape validée, l'installateur passe automatiquement à la configuration suivante.



Configuration du mode réseau WAN (vtnet0)

Après l'initialisation du réseau, l'installateur affiche la fenêtre « WAN (vtnet0) Network Mode Setup ».
Cette étape permet de choisir le mode de fonctionnement de l'interface WAN de PfSense (ici vtnet0) avant de poursuivre l'installation.

La fenêtre présente plusieurs paramètres configurés par défaut :

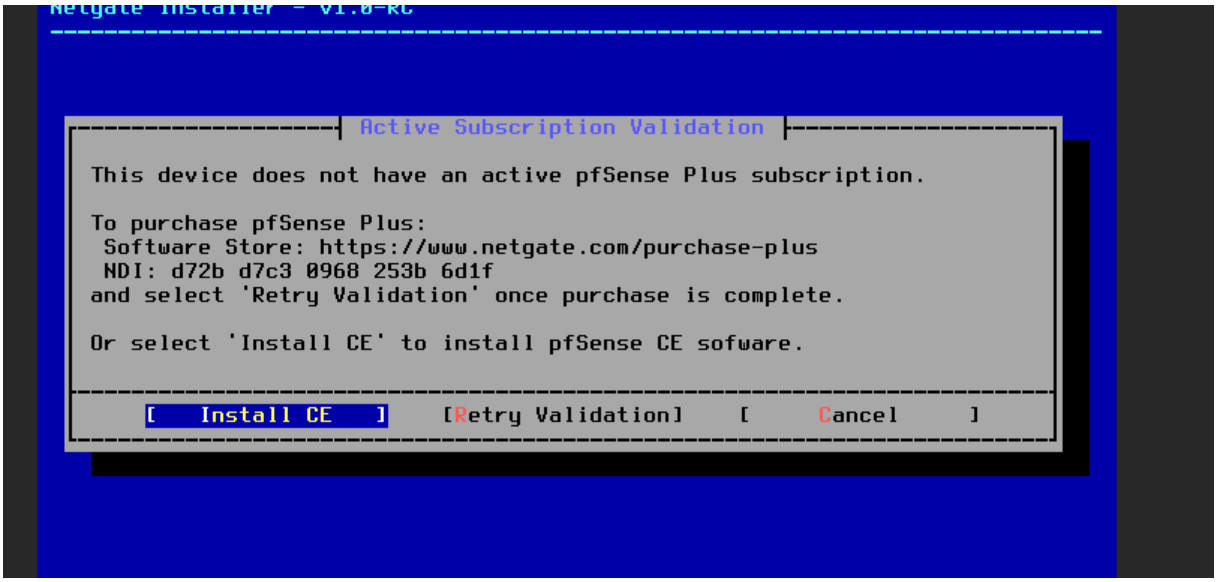
Paramètres affichés :

- Continue : Proceed with the installation
  → Permet de continuer vers la prochaine étape.
- Interface Mode : DHCP (client)
  → L'interface WAN sera configurée en DHCP, c'est-à-dire qu'elle recevra automatiquement une adresse IP du réseau amont.
- VLAN Settings : VLAN Tagging disabled
  → Aucun VLAN n'est activé sur l'interface WAN.
- Use local resolver : false
  → Le résolveur DNS local n'est pas utilisé pendant l'installation.

Action à effectuer :

1. Laisser les paramètres par défaut (sauf cas particulier de configuration réseau spécifique).
2. Sélectionner Continue si ce n'est pas déjà le cas.
3. Valider avec la touche Entrée.
4. Puis choisir OK pour continuer.

L'installation passe ensuite à la configuration suivante.



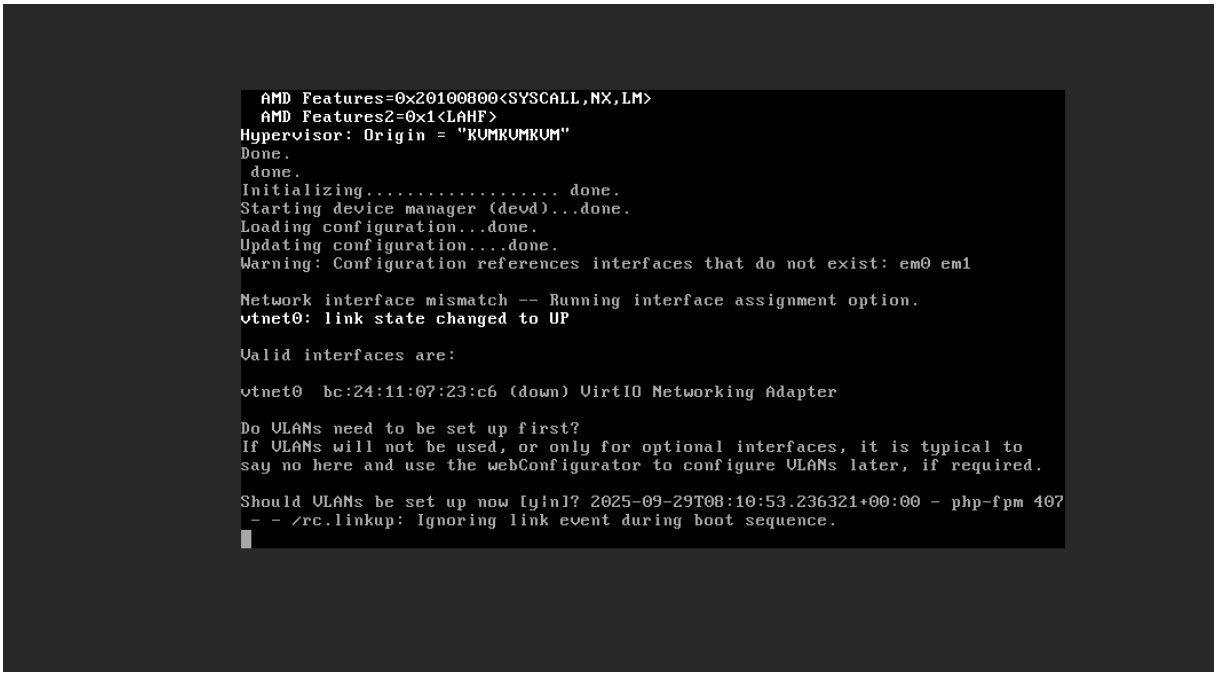
Choisir la version de pfSense à installer

L'installateur indique qu'aucune licence PfSense Plus n'est active sur la machine.
Pour continuer gratuitement, il faut installer la version pfSense CE (Community Edition).

Action à faire :

- Sélectionner Install CE
- Valider avec Entrée

Cela lance l'installation de la version gratuite et open-source de pfSense.



Configuration des VLANs au premier démarrage

Au premier démarrage, PfSense détecte les interfaces réseau et demande si des VLANs doivent être configurés maintenant.

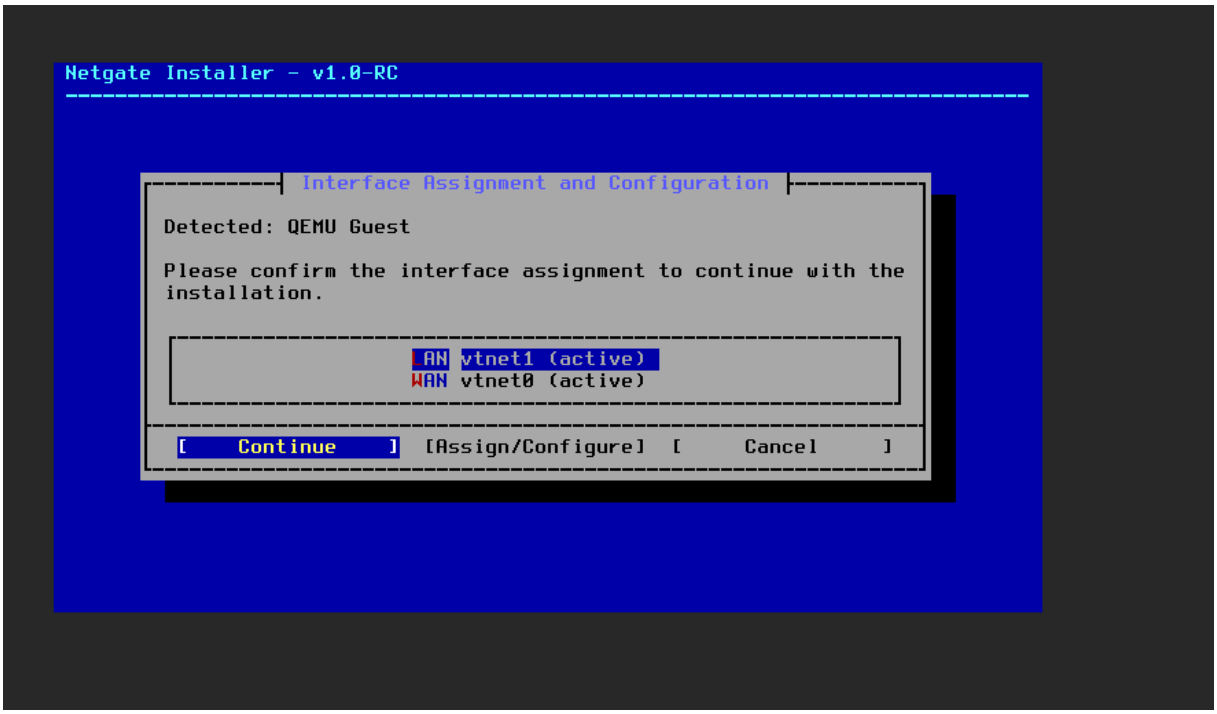
L'écran indique les interfaces disponibles (ex : vtnet0) et pose la question :

"Should VLANs be set up now [y/n]?"

Action à faire :

- Taper n (non)
- Valider avec Entrée

Les VLANs pourront être configurés plus tard via l'interface web si nécessaire.



Confirmation des interfaces réseau

L'installateur affiche les interfaces détectées pour PfSense :

- LAN : vtnet1 (active)
- WAN : vtnet0 (active)

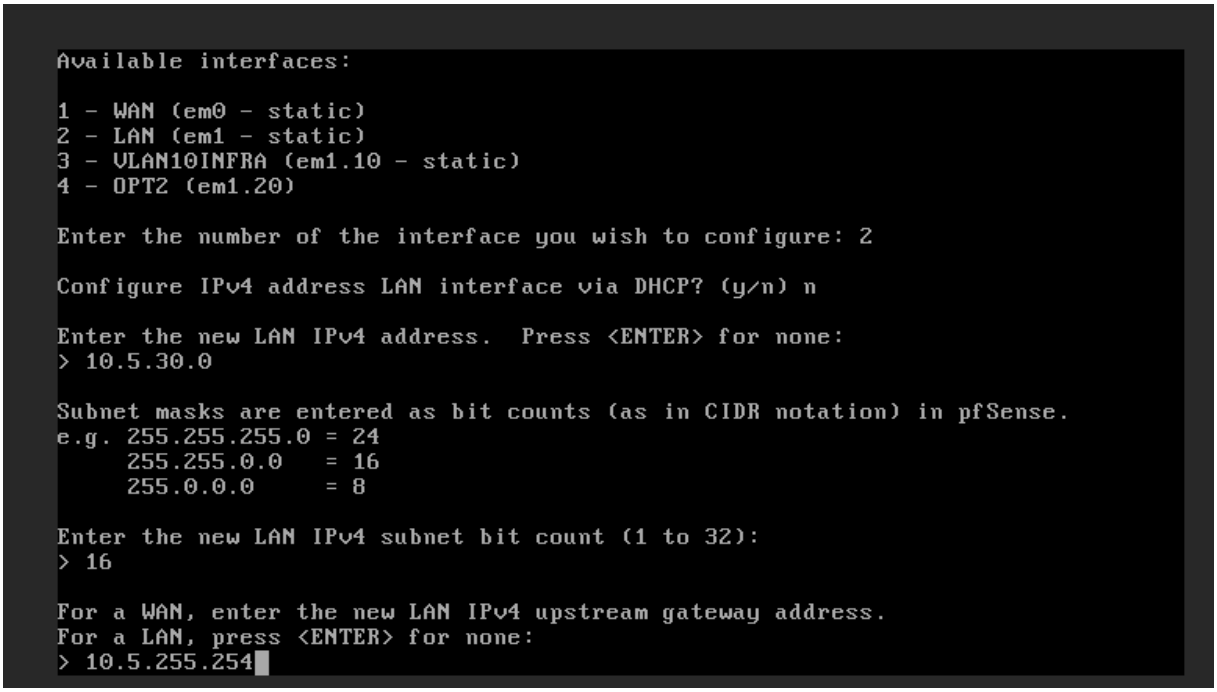
Il s'agit des bonnes interfaces détectées automatiquement.

Action à faire :

- Laisser les interfaces telles quelles

- Sélectionner Continue
- Valider avec Entrée

Cela confirme l'affectation des interfaces et poursuit l'installation

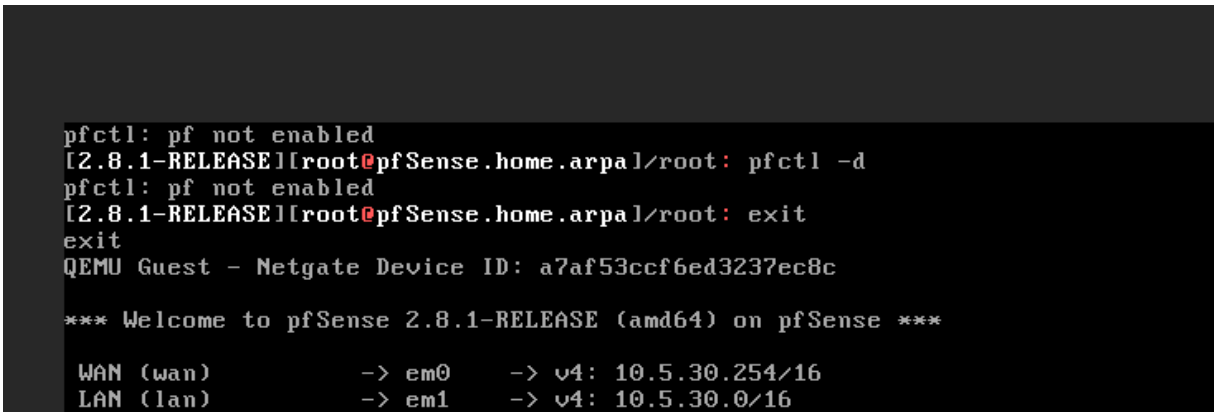


Configuration de l'adresse LAN

Dans cette étape, PfSense demande de configurer l'interface LAN manuellement.

Actions réalisées dans la capture :

1. Choix de l'interface à configurer :
   → Saisie : 2 (interface LAN)
2. Adresse LAN via DHCP
   → Réponse : n (configuration manuelle)
3. Nouvelle adresse IPv4 LAN
   → Saisie : 10.5.30.0
4. Masque de sous-réseau (CIDR)
   → Saisie : 16
   (équivalent à 255.255.0.0)
5. Gateway IPv4 pour le LAN :
   → Rien à mettre → appuyer sur Entrée
   (le LAN n'a pas de passerelle)



Fin de l'installation et affichage des interfaces

PfSense a terminé son installation et affiche maintenant un résumé des interfaces réseau configurées.

Informations visibles :

- WAN (em0) → IPv4 : 10.5.30.254/16
- LAN (em1) → IPv4 : 10.5.30.1/16

Cela confirme que pfSense est installé et que les interfaces sont opérationnelles.

Prochaine étape :

Vous pouvez maintenant accéder à l'interface web de pfSense via :

https://10.5.30.1

Problème : Impossible d'accéder à l'interface pfSense / pas d'accès Internet

Après l'installation de pfSense, nous avons constaté deux problèmes :

- Impossible d'accéder à l'interface web de pfSense
- Les machines du réseau ne pouvaient pas naviguer sur Internet

Ces problèmes étaient causés par le pare-feu pfSense, qui bloquait le trafic par défaut sur certaines interfaces.

Solution temporaire : Désactivation du pare-feu

Pour vérifier l'origine du problème, nous avons désactivé temporairement le pare-feu PfSense.

Une fois le pare-feu désactivé :

- L'accès à l'interface web de pfSense a immédiatement fonctionné
- L'accès Internet a été rétabli

Cela confirme que le blocage provenait des règles du pare-feu.

Conclusion

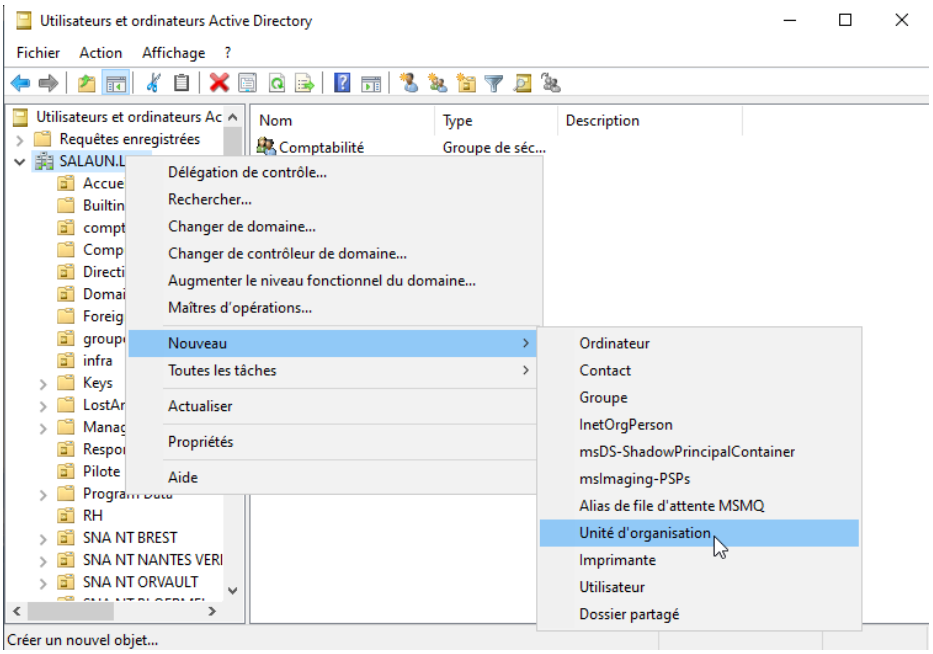
La désactivation du pare-feu a permis d'identifier l'origine du problème.
Ensuite, des règles de pare-feu adaptées devront être configurées pour permettre :

- L'accès à l'interface web depuis le LAN
- Le trafic Internet sortant
- Le routage entre réseaux si nécessaire

Ajout d'utilisateur

Création de l'Unité d'Organisation

Une unité d'organisation (UO) est un conteneur logique qui sert à organiser les objets du réseau.



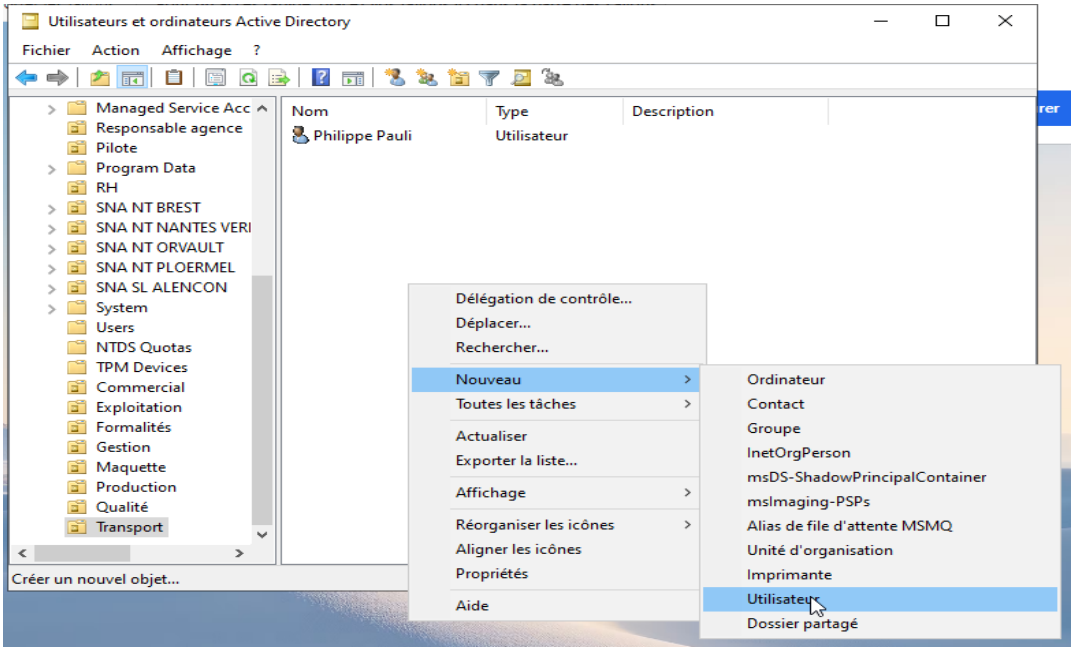
Dans Utilisateur et ordinateurs Active Directory effectuer :

-Un clic droit sur votre domaine.

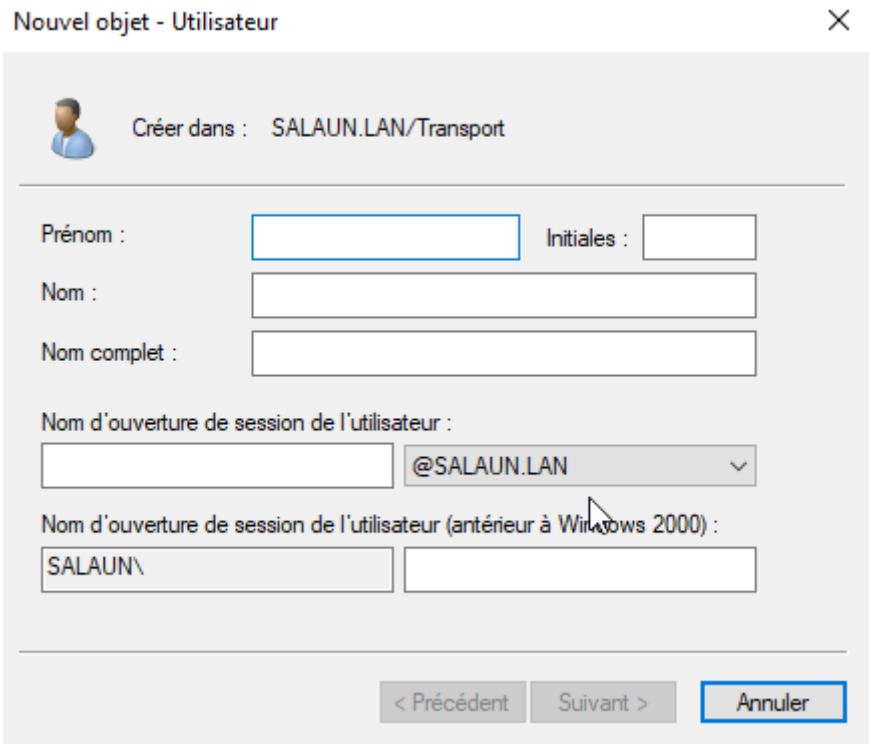
-Positionner sa souris sur nouveau et attendre que le menu déroulant apparaisse.

-Puis choisir Unité d'organisation.

Création de l’utilisateurs



Dans votre UO faire le même cheminement que pour crée une UO mais dans ce cas la vous allez choisir Utilisateur



Vous arriverez donc sur cette page :

-Rensignez donc le prénom, le nom et le nom d'ouverture de session.

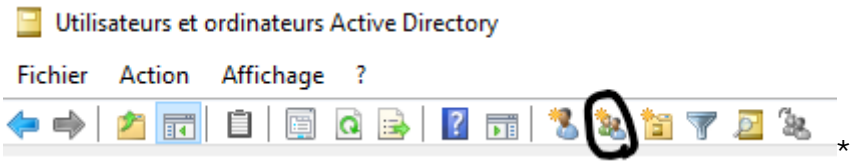
-Puis cliquez sur Suivant.

Une page va donc apparaitre :

-Rensignez le mot de passe de cette session puis effectuer les paramètres de votre choix en cochant ou décochant les carrés à gauche des informations.*

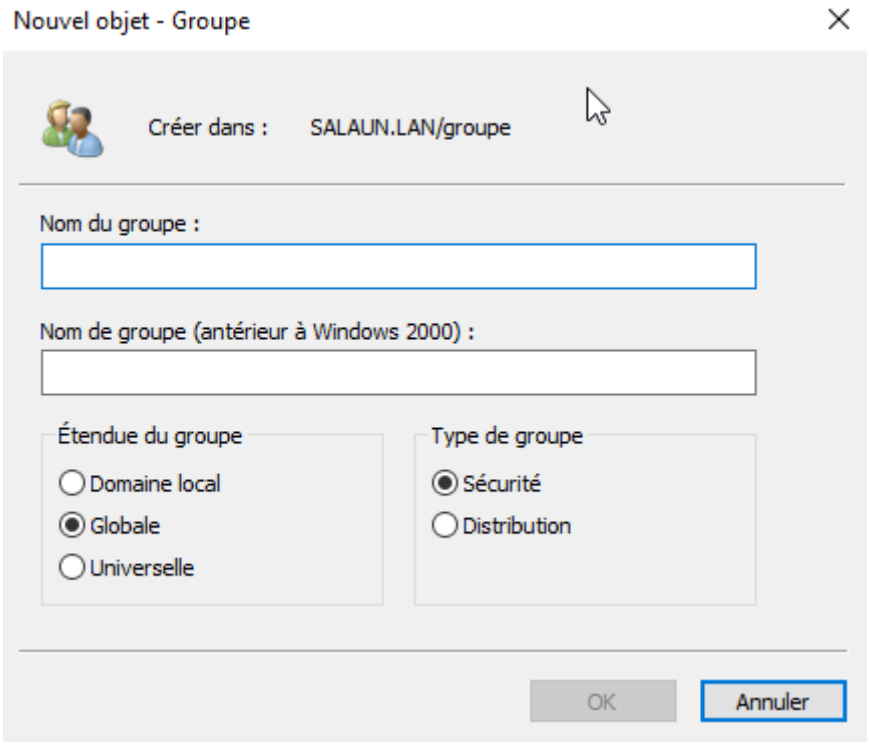
Votre utilisateur est Maintenant créé

Crée un groupe

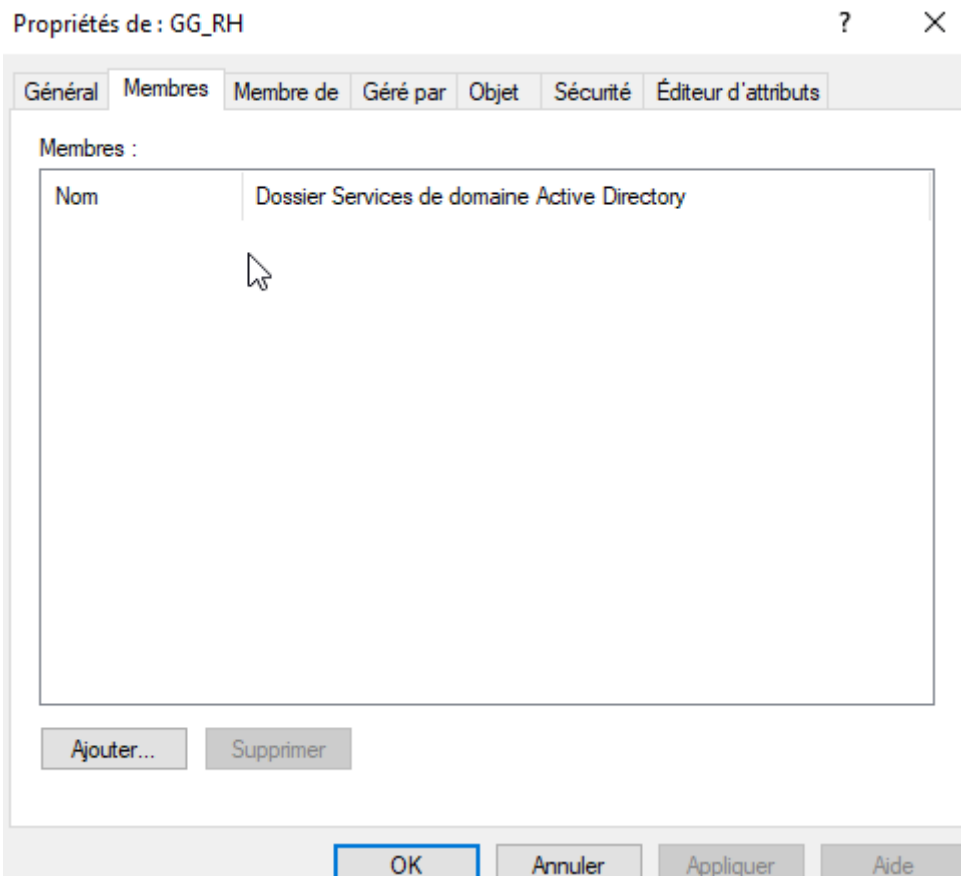


-Sélectionner ce bouton pour crée un groupe.

Vous arriverez sur cette page.

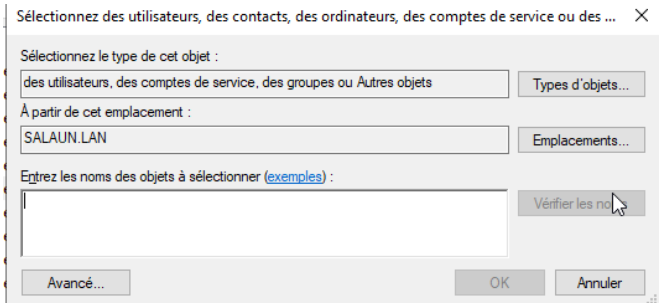


Après avoir crée le groupe vous pouvez effectuer un double clic sur le groupe crée pour arriver sur cette page.



Cette page permet d'ajouter des membres au groupe.

-Cliquer donc sur ajouter.

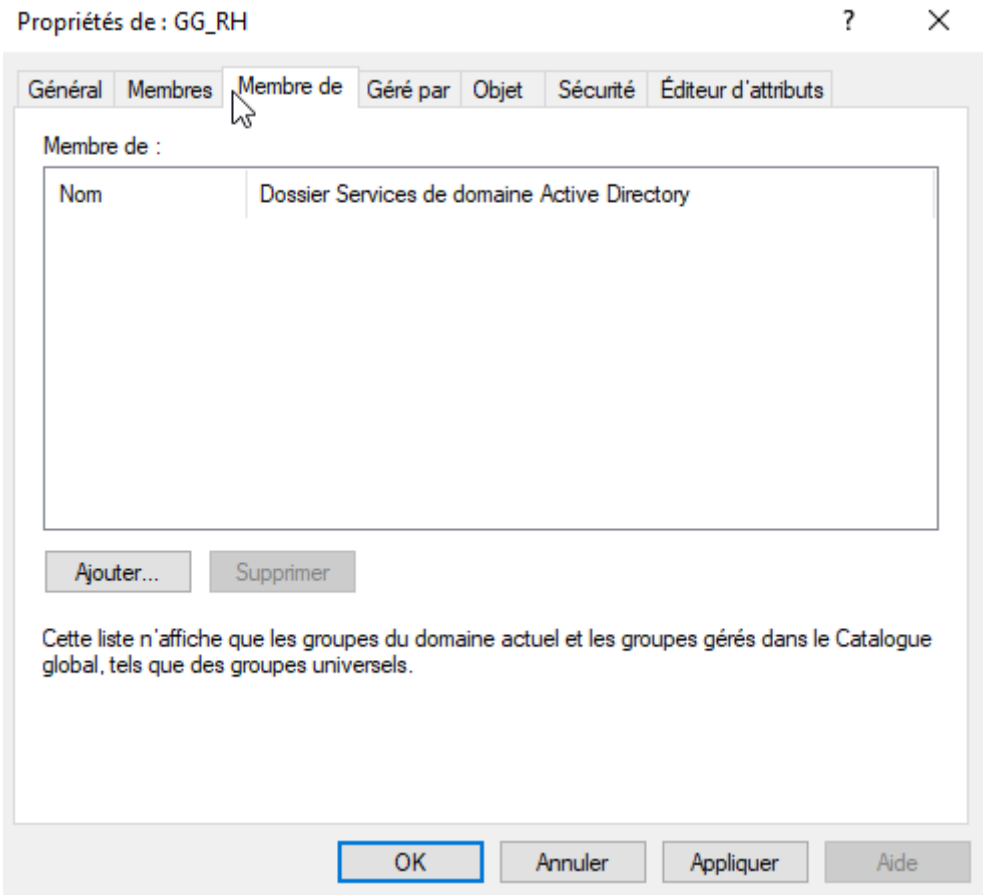


-Entrer le nom du compte a ajouter puis cliquer sur « Vérifier les noms » puis sur ok (vous pouvez ajouter plusieurs utilisateurs a la fois).

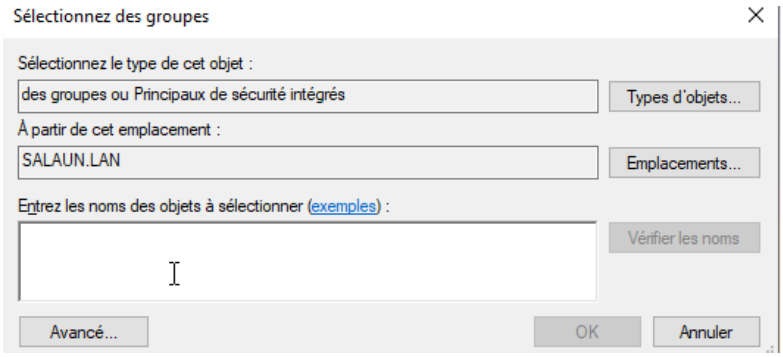
-Une fois ajouter l'utilisateur apparaitra dans la liste des membres.

Mettre de droits au groupe.

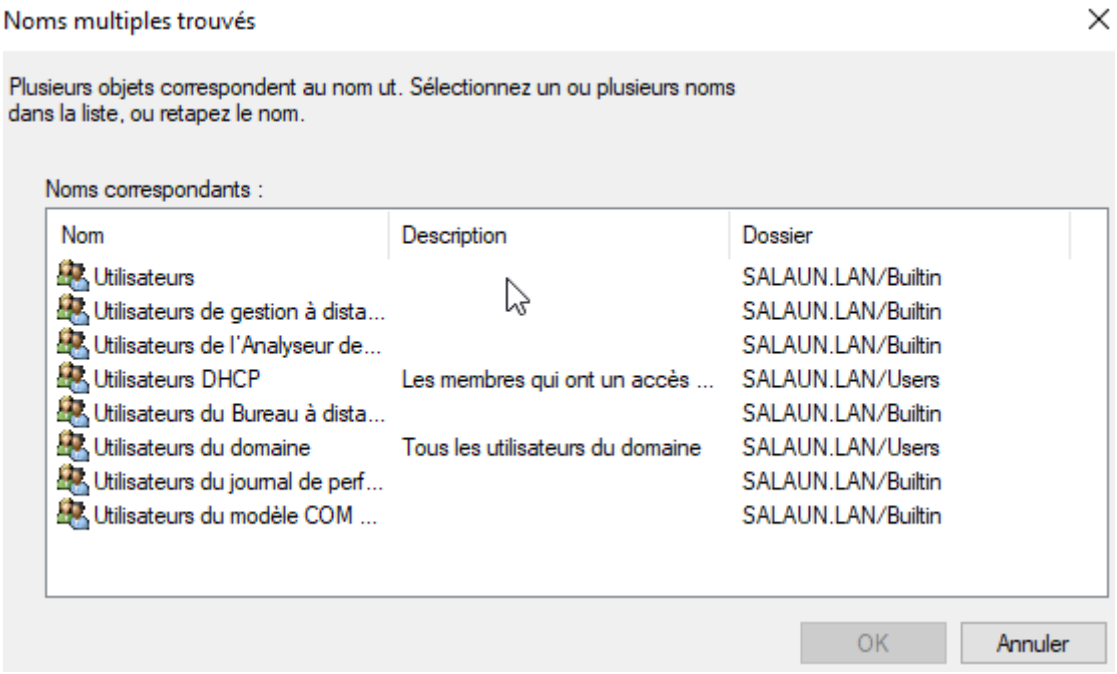
Toujours dans le même onglet, mais nous allons sélectionner « Membre de »



-Nous allons cliquer sur « ajouter ». Cette page apparaitra.



Dans cette page vous aller choisir le rôle des utilisateurs présents dans le groupe (dans notre cas « utilisateurs »



Sélectionner le premier choix puis « Ok » « Ok » et enfin « appliquer » et « ok ».

Réseau Wi-Fi Invités

Mettre en place un réseau Wi-Fi Invités isolé du réseau interne, avec :

- attribution automatique d'adresse IP par DHCP pfSense,
- Portail captif avec acceptation des CGU (Option A),
- accès Internet uniquement (blocage des réseaux privés internes),
- gestion par segmentation (VLAN + sous-réseau dédié).

Le Captive Portal pfSense force les utilisateurs à passer par une page web d'acceptation/connexion avant d'accéder au réseau, selon le mode choisi.

1) Pré-requis (réseau & Wi-Fi)

1.1 Matériel / VM

- pfSense avec 2 interfaces : WAN (em0) et LAN (em1) → OK.
- Switch/Point d'accès Wi-Fi capable de tagger un SSID sur un VLAN.

1.2 VLAN

- VLAN Invités : VLAN 20
- Le port switch vers l'AP doit transporter ce VLAN (trunk/tagged).
- Le SSID "Invités" doit être associé au VLAN 20.

---

2) Plan d'adressage (Portail captif)

2.1 Réseau invités

- Sous-réseau : 10.6.20.0/24
- Passerelle (pfSense GUEST) : 10.6.20.1
- DHCP : 10.6.20.50 → 10.6.20.200
- DNS : 10.6.20.1 (pfSense

Remarque : le Captive Portal s'applique sur une interface non-WAN (LAN/VLAN) ayant une IP.

---

3) Création du VLAN "Invités" sur pfSense (em1)

Étape 3.1 — Créer le VLAN

1. Aller dans Interfaces → Assignments
2. Onglet VLANs
3. Cliquer Add
4. Renseigner :
    - Parent interface : em1 (LAN)
    - VLAN Tag : 20
    - Description : VLAN_GUEST
5. Save

Étape 3.2 — Assigner le VLAN comme interface OPT

1. Revenir sur Interface Assignments
2. Dans la liste des ports disponibles, sélectionner VLAN 20 on em1
3. Ajouter bouton “Add” ou apparition d’OPT1 après sélection
4. Tu obtiens OPT1

Étape 3.3 — Configurer l’interface OPT1 (GUEST)

1. Aller dans Interfaces → OPT1
2. Cocher Enable
3. Description : GUEST ou INVITES
4. IPv4 Configuration Type : *Static IPv4*
5. IPv4 Address : 10.6.20.1/24
6. Save puis Apply Changes

---

4) DHCP sur pfSense (réseau invités)

1. Aller dans Services → DHCP Server → GUEST
2. Cocher Enable DHCP server on GUEST
3. Configurer :
    - Range : 10.6.20.50 à 10.6.20.200
    - (Optionnel) Default lease time : ex 7200 sec (2h) ou 14400 sec (4h)
4. DNS :
    - Soit 10.6.20.1 (pfSense)
    - Soit DNS public (si tu ne veux pas que les invités utilisent le DNS interne)

À ce stade, un client invité doit déjà obtenir une IP en 10.6.20.x.

---

5) Règles Firewall (Invités = Internet uniquement)

5.1 Pourquoi bloquer RFC1918 ?

Pour empêcher l’accès aux réseaux internes privés, on bloque les plages RFC1918 :

- 10.0.0.0/8
- 172.16.0.0/12

- 192.168.0.0/16

C’est parfait dans ton cas : ton LAN est en 10.5.x.x, donc il est inclus dans 10.0.0.0/8 → les invités ne pourront pas toucher ton SI.

5.2 Créer un alias RFC1918

1. Firewall → Aliases
2. Add
3. Type : Network(s)
4. Name : RFC1918
5. Ajouter :
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
6. Save

5.3 Créer les règles sur l’interface GUEST

Aller dans Firewall → Rules → GUEST et mettre dans cet ordre :

Règle 1 — Autoriser DNS (si DNS = pfSense)

- Action : Pass
- Protocol : TCP/UDP
- Source : GUEST net
- Destination : This Firewall (GUEST address) (donc 10.6.20.1)
- Port : 53
- Description : “DNS invités vers pfSense”

Règle 2 — Bloquer accès aux réseaux internes (RFC1918)

- Action : Block
- Source : GUEST net
- Destination : RFC1918
- Description : “Blocage réseaux privés (RFC1918)”

Règle 3 — Autoriser Internet

- Action : Pass
- Protocol : Any (ou TCP 80/443 + UDP 123)
- Source : GUEST net
- Destination : any
- Description : “Accès Internet invités”
- Résultat : les invités ont Internet mais ne peuvent pas joindre 10.5.x.x ni aucun réseau privé RFC1918.

4) Page captive “click-through” : simple OU personnalisée

Installation outil de monitoring

Nous avons choisi Centreon pour sa facilité de prise en main et nous le trouvons cohérent avec le projet.

Services actifs

-Centengine

-Cbd (broker)

-Apache2

-Mariadb

Installation via Debian

Etape 1 : Installation

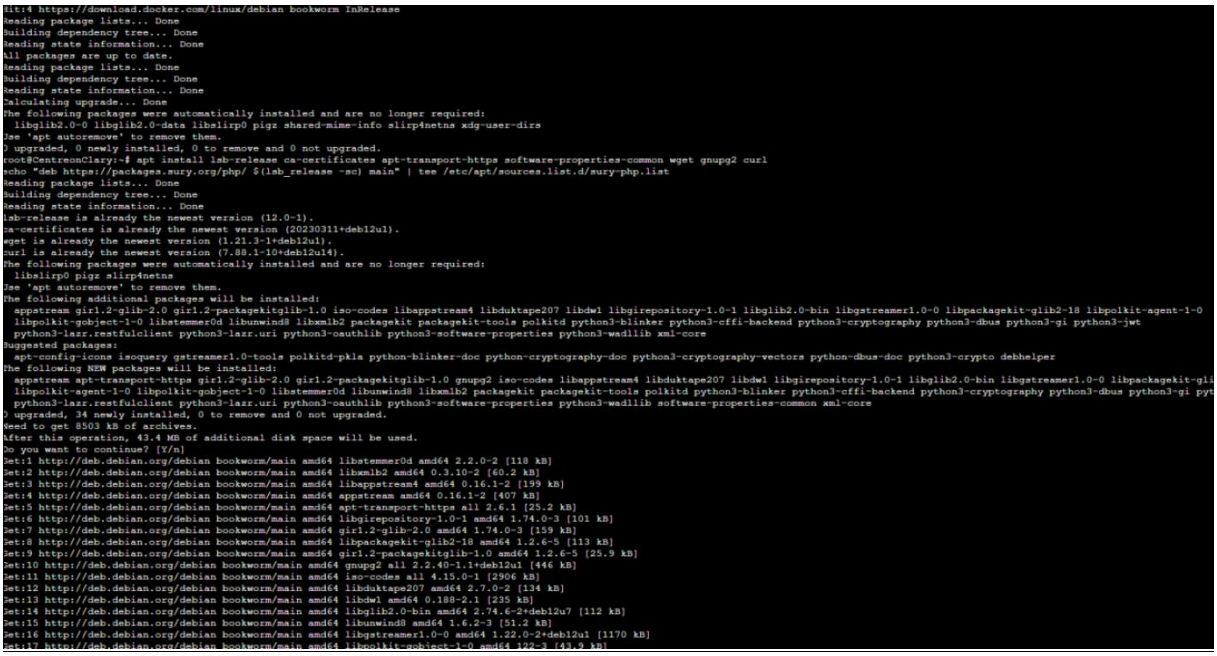
apt update && apt upgrade

apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl

echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/sury-php.list

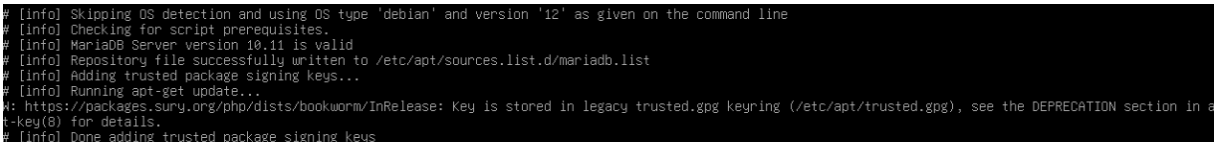
wget -O- https://packages.sury.org/php/apt.gpg | gpg --dearmor | tee /etc/apt/trusted.gpg.d/php.gpg > /dev/null 2>&1

apt update



Installation de la base de données :

curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | bash -s -- --os-type=debian --os-version=12 --mariadb-server-version="mariadb-10.11"

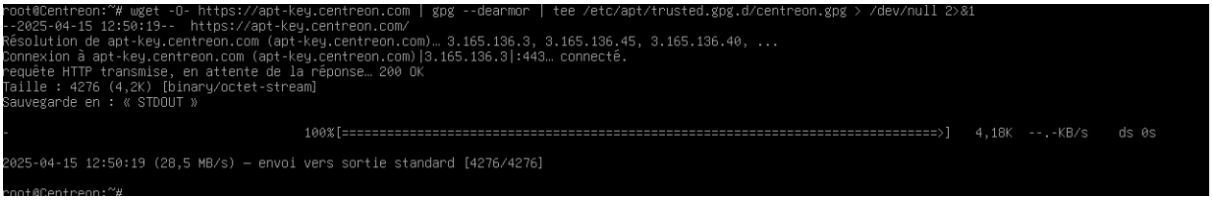


Installation des dépôts :

echo "deb https://packages.centreon.com/apt-standard-24.10-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon.list

echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list

wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1



apt update && apt install -y centreon-mariadb centreon

systemctl daemon-reload

systemctl restart mariadb

Étape 2 : Configuration

Lancement de Centreon au démarrage

systemctl enable php8.2-fpm apache2 centreon cbd centengine gorgoned centreontrapd snmpd snmptrapd mariadb

systemctl restart mariadb apache2

Sécurisation de la base de données :

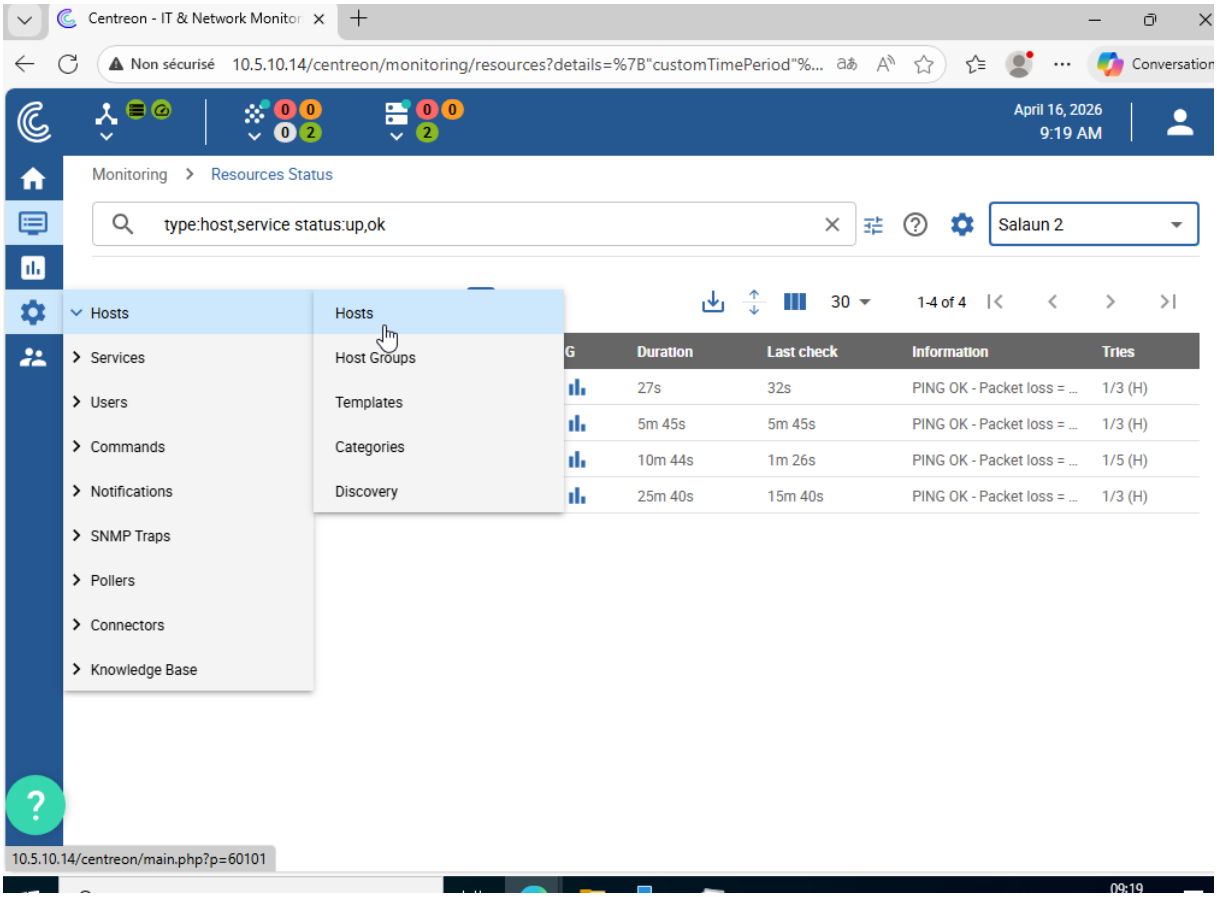
mariadb-secure-installation

Étape 3 : Interface web

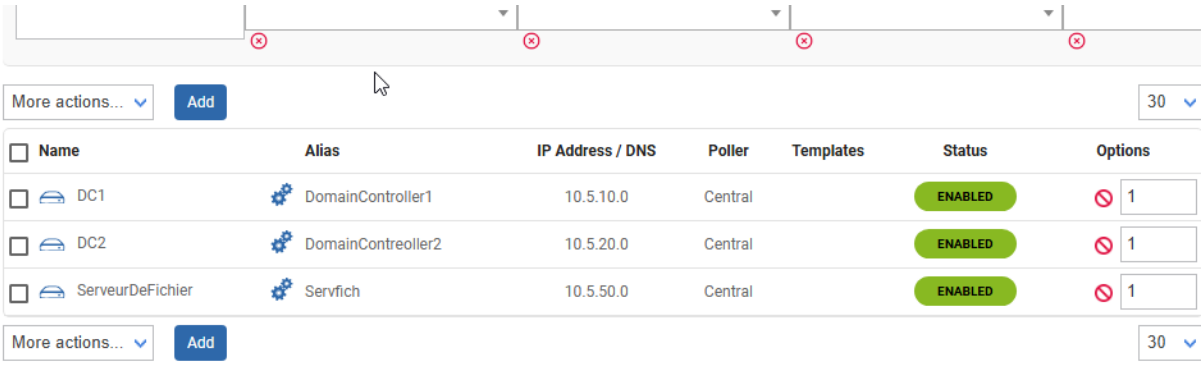
http://10.5.10.14

Ajout d’un serveur

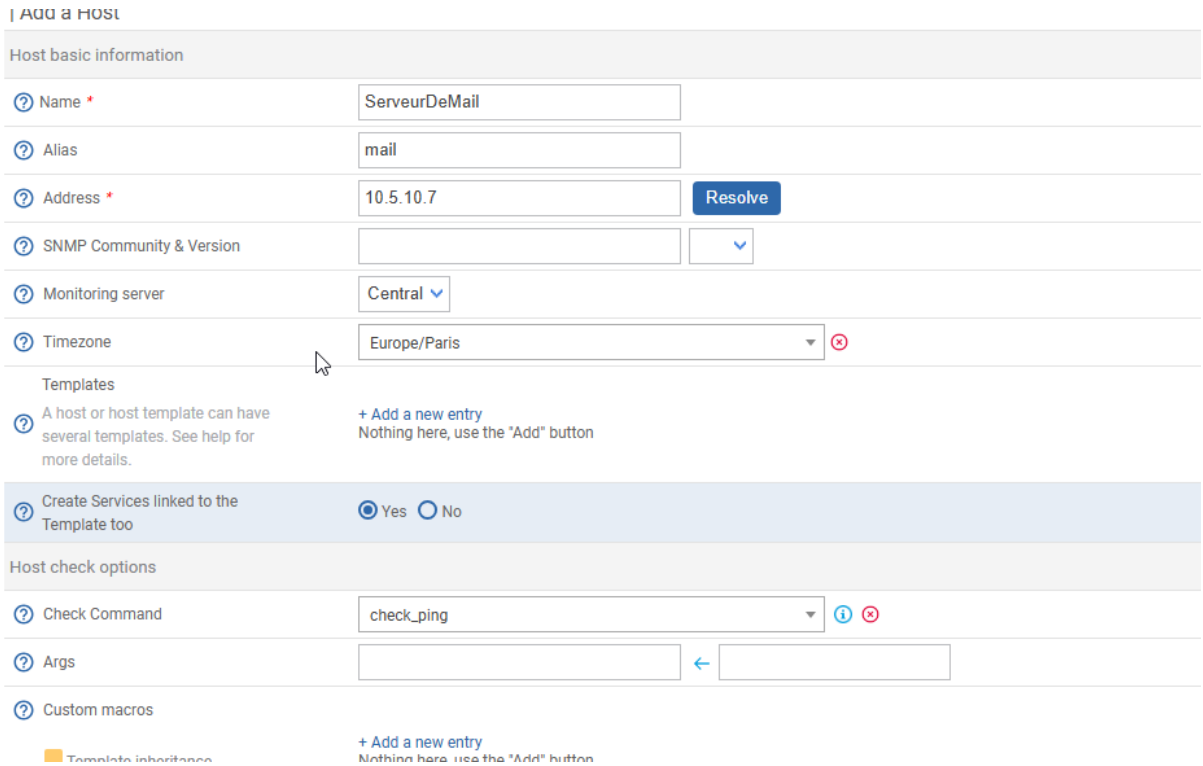
Une fois sur centreon il faut se rendre sur la roulette puis Hosts et encore une fois Hosts.

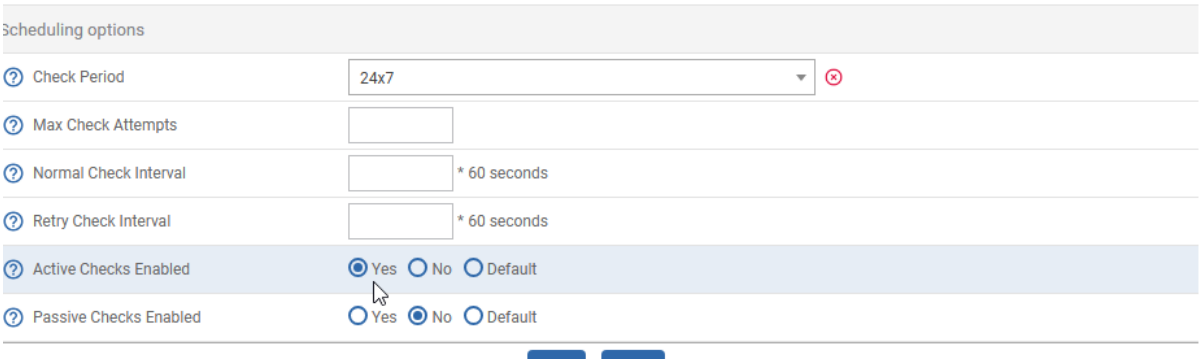


Une fois sur la page cliquer sur add.

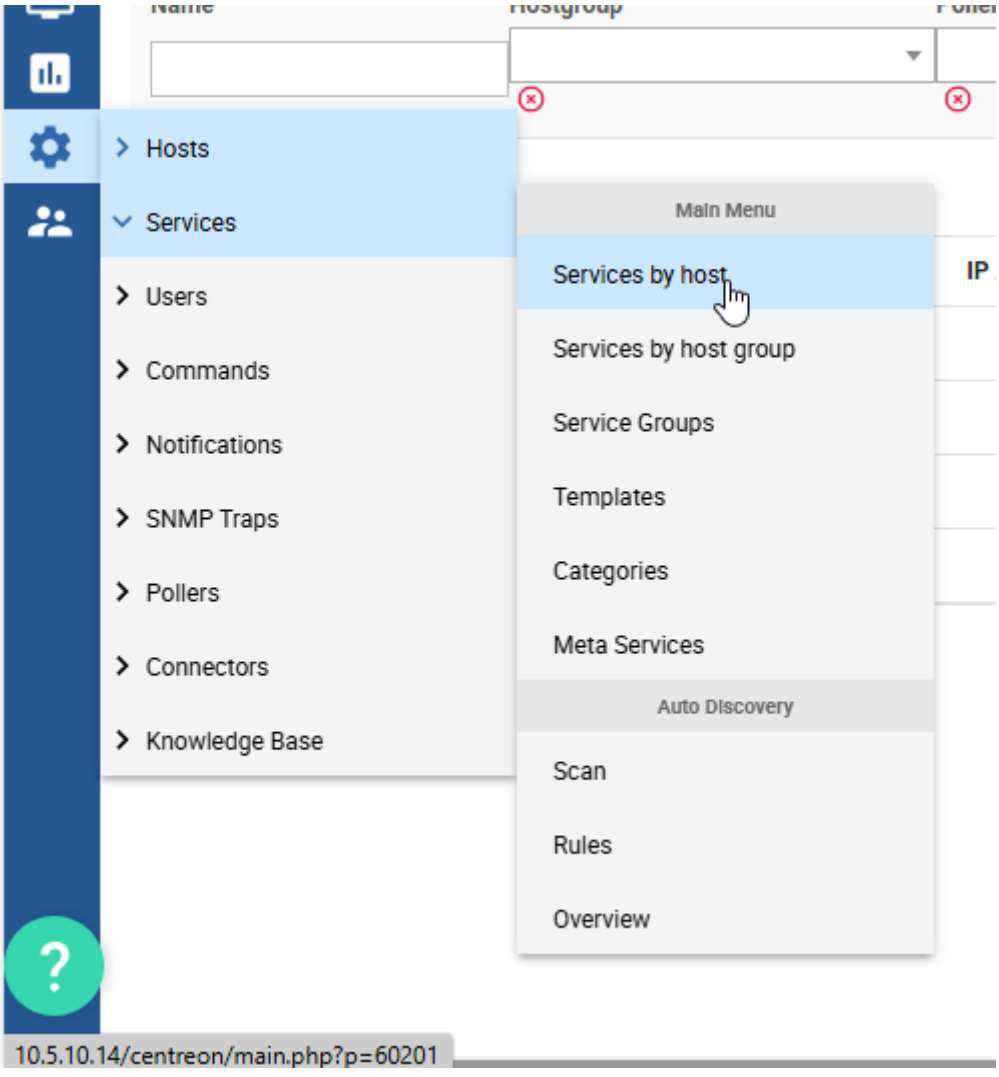


Après avoir cliqué sur add. Renseigner les différentes informations demander. Puis Save.

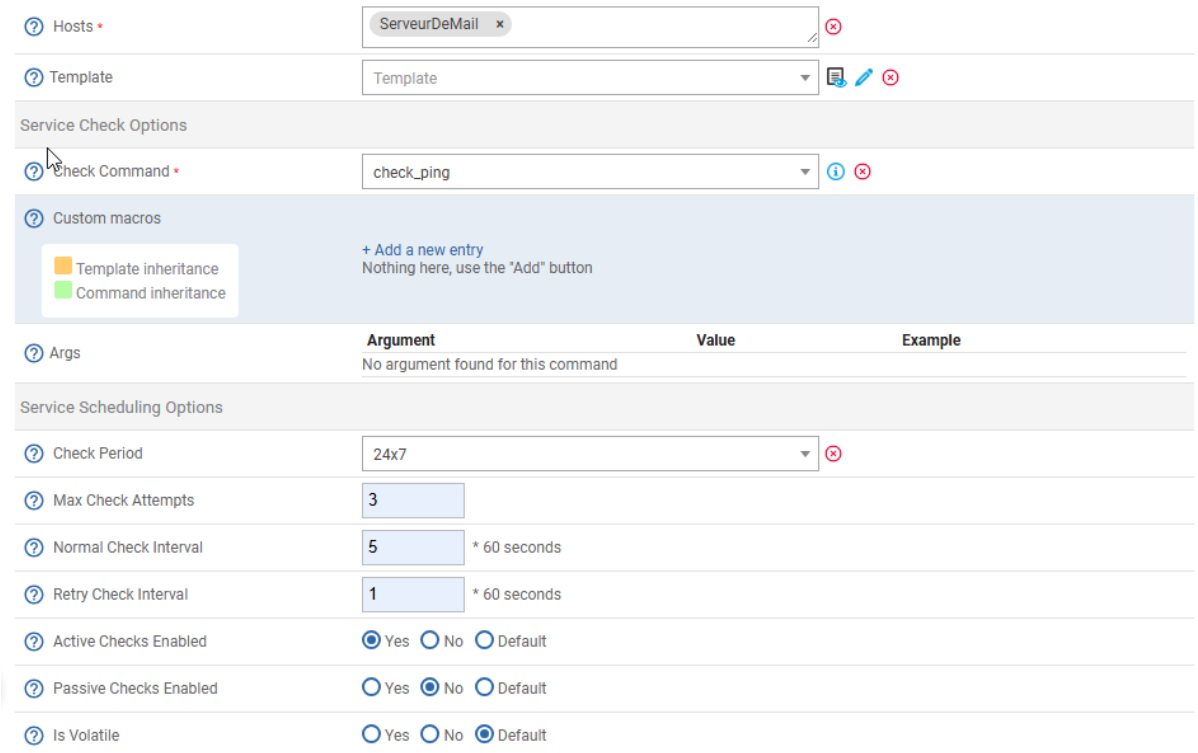




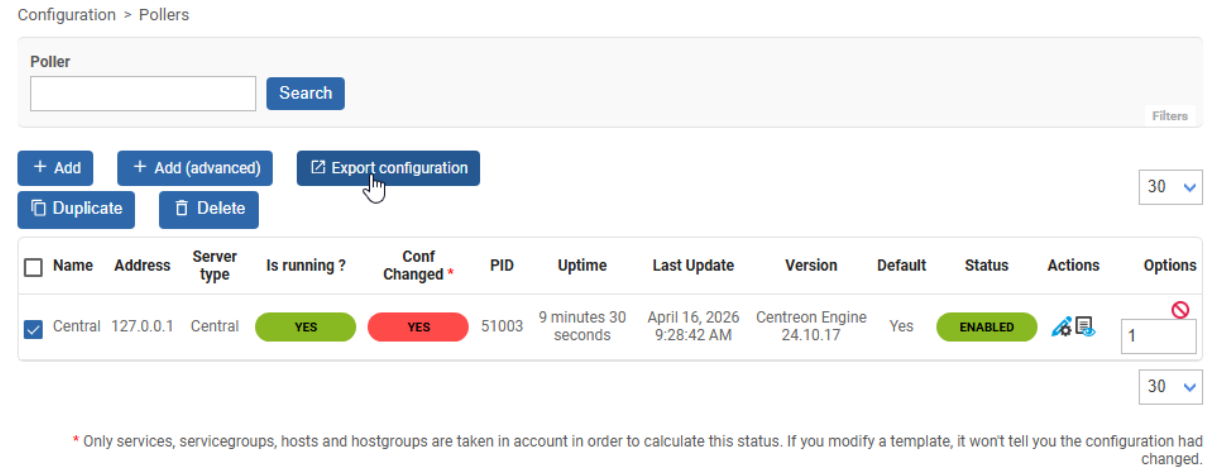
Une fois l'host crée nous allons faire de même dans les services by host.



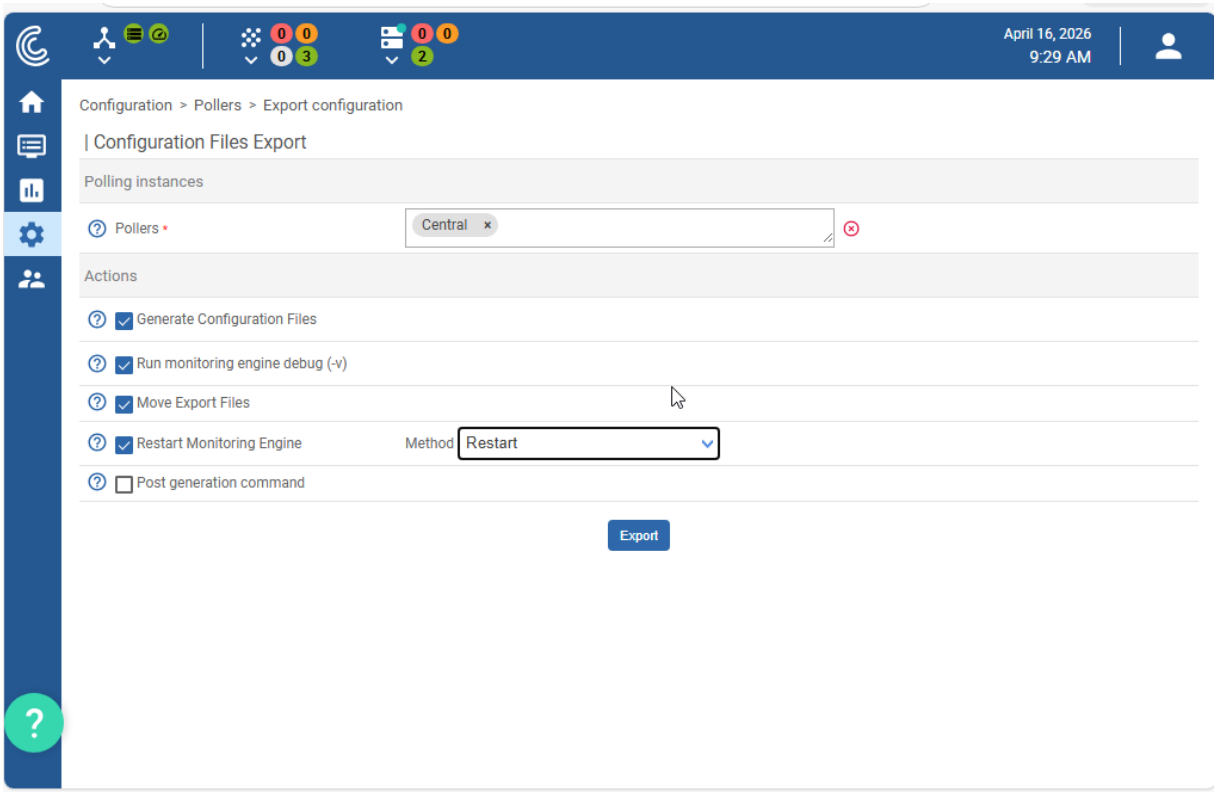
Une fois sur la page cliquer sur add et remplir de la même manière.



Une fois ces deux choses faites se rendre dans Pollers pour pouvoir enregistrer la configuration. Selectionner votre serveur et cliquer sur export configuration.



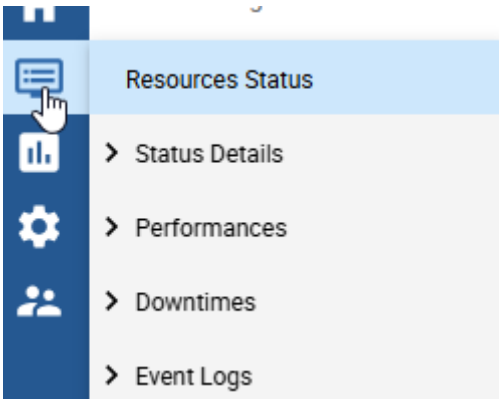
Sectionner les mêmes paramètres que sur l'image ci-dessous. Puis cliquer sur Export.



Une fois tout cela terminer se rendre sur le serveur ssh centreon pour redémarrer les différents services avec ces commandes dans cet ordre.

```
root@Centreon:~# systemctl restart cbd
root@Centreon:~# systemctl restart centengine
root@Centreon:~#
```

Après avoir terminer tout cela le serveur devrait apparaitre. Dans Ressources Status.



Serveur de fichier

Un disque de données dédié a été ajouté à la machine virtuelle via Proxmox afin de séparer le système d'exploitation des données utilisateurs.
Le volume D:\DATA est utilisé pour le stockage des fichiers partagés, facilitant la maintenance, la sauvegarde et la sécurité.

. Architecture mise en place

Élément	Valeur
Système	Windows Server
Rôle	Serveur de fichiers
Domaine	SALAUN.LAN
Serveur	SERFICH
Partage principal	\\SERFICH\Dossier-de-partage
Volume données	E:\DATA

Organisation des données

Les données sont stockées sur un disque dédié (E:), distinct du système d'exploitation.

Arborescence du volume

Plain Text

E:\DATA

├—dossier-de-partage

├— adminSYS

├— COMMERCIAL

├— Commun

├— Comptabilite

├— Direction

├— PRODUCTION

├— QUALITE

Groupes Active Directory utilisés

Les accès aux dossiers sont contrôlés par des groupes de sécurité globaux.

Exemples de groupes

Dossier	Groupe AD
Commun	GG_Tous
Comptabilite	GG_Compta
RH	GG_RH
Direction	GG_Direction
Commercial	GG_Commercial
Production	GG_Production
Qualité	GG_Qualite
Transport	GG_Transport
Admin système	GG_AdminSYS

Les utilisateurs sont ajoutés aux groupes correspondant à leur service.

Sauvegarde Centralisée

1. Présentation

Dans le cadre du projet, une solution de sauvegarde centralisée a été mise en place via Proxmox Backup Server (PBS) 4.2. Elle permet de sauvegarder automatiquement toutes les VMs de l'infrastructure SALAUN .

---

2. Caractéristiques techniques

Élément	Détail
Solution	Proxmox Backup Server 4.2

Élément	Détail
Hostname	pbs.SALAUN.LAN
IP du serveur	10.5.10.5/8
Gateway	10.5.30.1
DNS	10.5.10.0
Port d'administration	8007 (HTTPS)
Filesystem	ext4
Disque système	/dev/sda
Datastore	backup-store
Chemin du datastore	/mnt/datastore/backup-store
Compression	ZSTD
Mode de sauvegarde	Snapshot
GC Schedule	Daily
Prune Schedule	Daily
Fréquence	Toutes les nuits à 00h00
Périmètre	Toutes les VMs

---

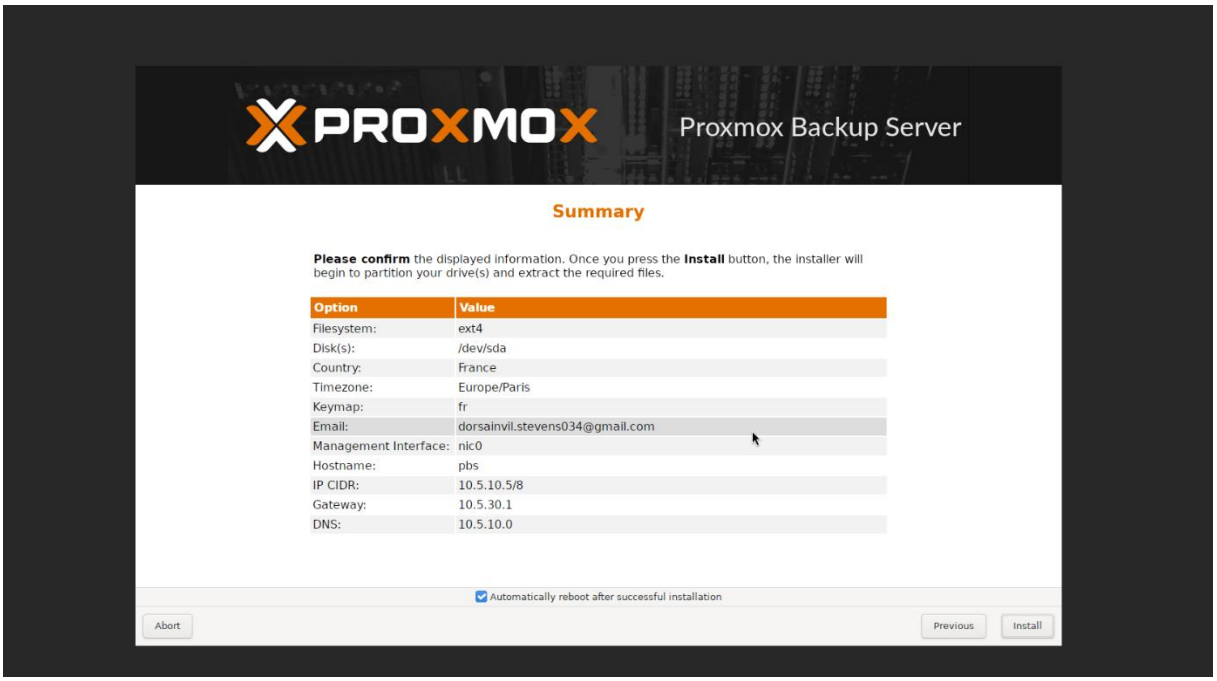
3. Étapes d'installation

Étape 1 — Boot sur l'ISO Démarrage sur l'ISO PBS 4.2, sélection de Install Proxmox Backup Server (Graphical).

Étape 2 — Configuration réseau

- Hostname : pbs.SALAUN.LAN
- IP : 10.5.10.5/8
- Gateway : 10.5.30.1

- DNS : 10.5.10.0



Étape 3 — Configuration du stockage Création d'un Directory sur le 2ème disque puis d'un Datastore backup-store dans /mnt/datastore/backup-store.

Étape 4 — Connexion à Proxmox sur l'interface https://10.5.10.5 :8007 Ajout du stockage PBS dans Datacenter → Storage → Add → Proxmox Backup Server avec le fingerprint SSL du certificat.

Étape 5 — Job de sauvegarde Création d'un job automatique dans Datacenter → Backup planifié à 00h00 chaque nuit pour toutes les VMs.

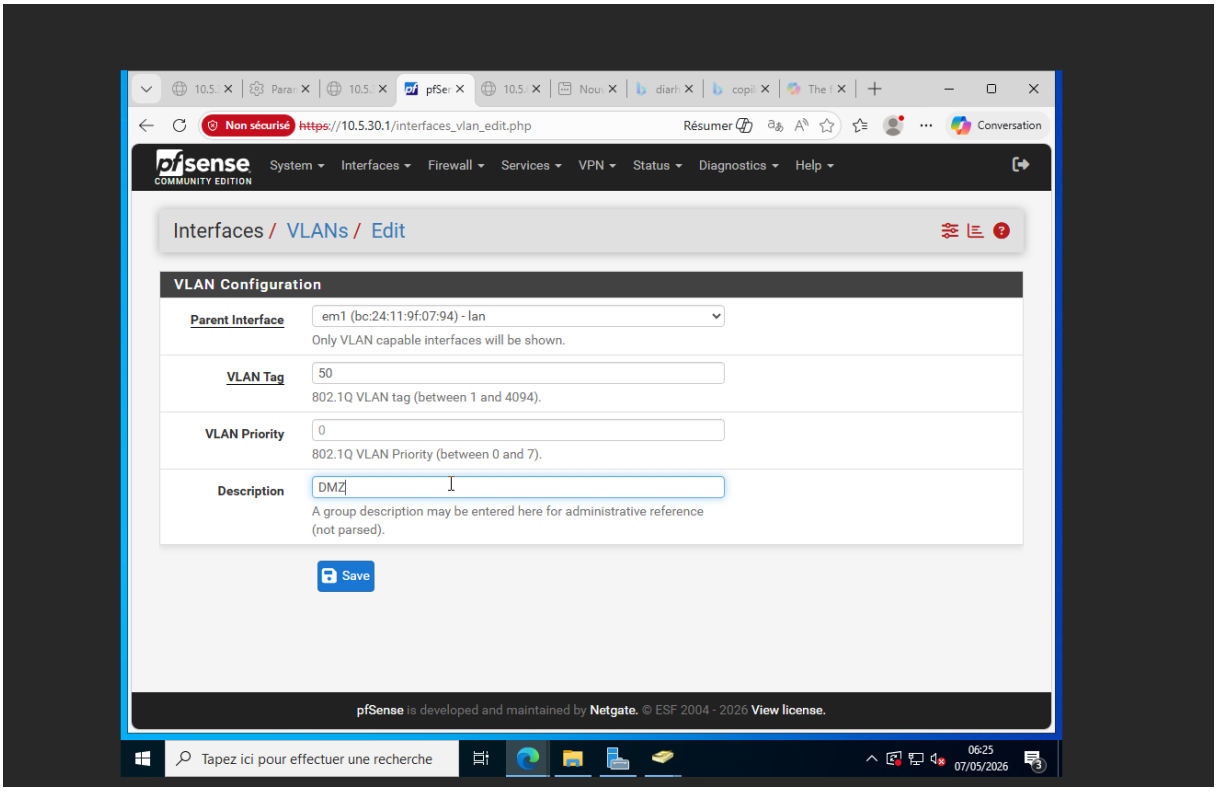
---

4. Procédure de restauration

1. Se connecter à Proxmox (https://10.5.40.100:8006)
2. Sélectionner la VM → Backup
3. Choisir le point de restauration
4. Cliquer sur Restore

Interface web https://10.5.10.5 :8007

DMZ



Étape 1 : Créer le VLAN 50

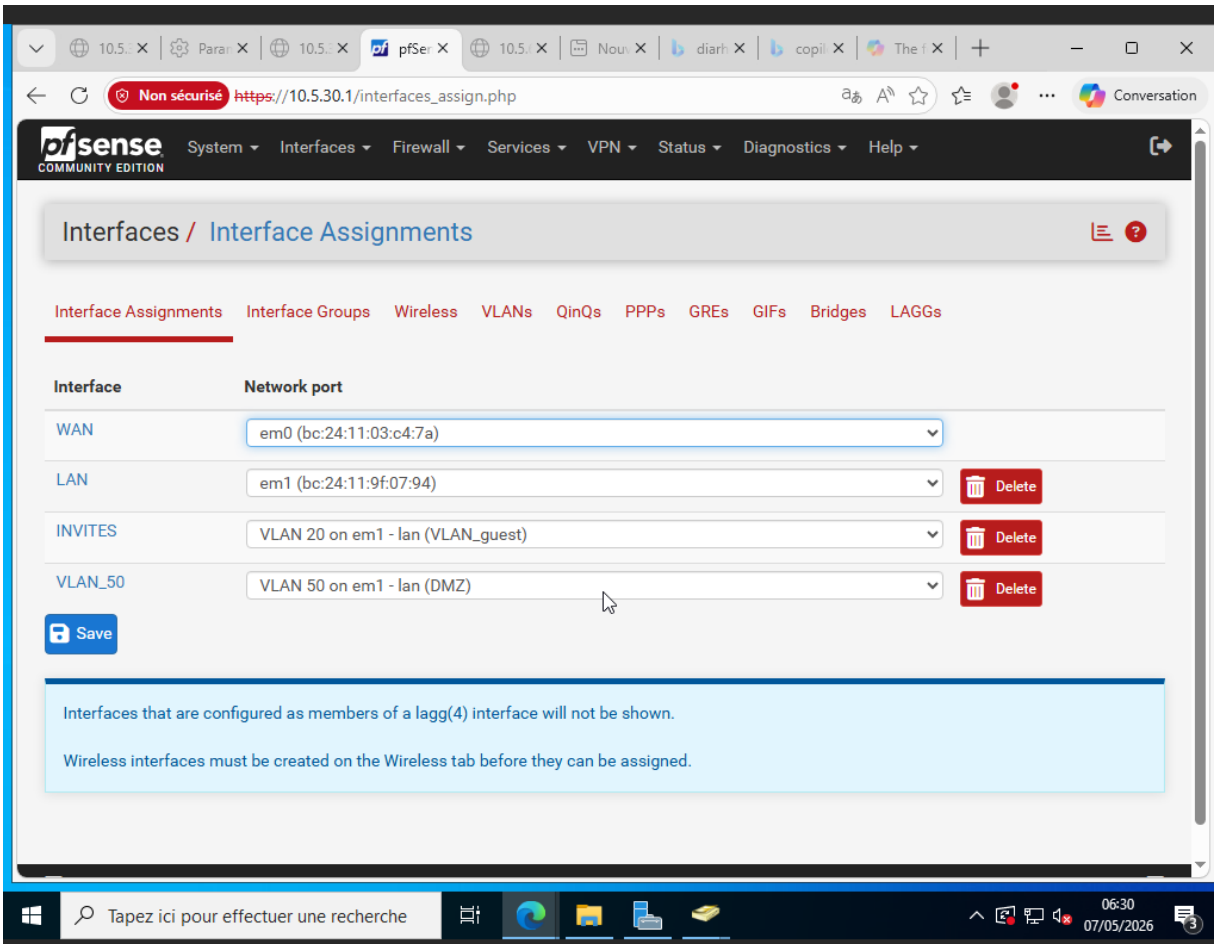
1. Accède à pfSense → Interfaces → Assignments → onglet VLANs
2. Clique Add
3. Remplis :

    Parent Interface : em1

    VLAN Tag : 50

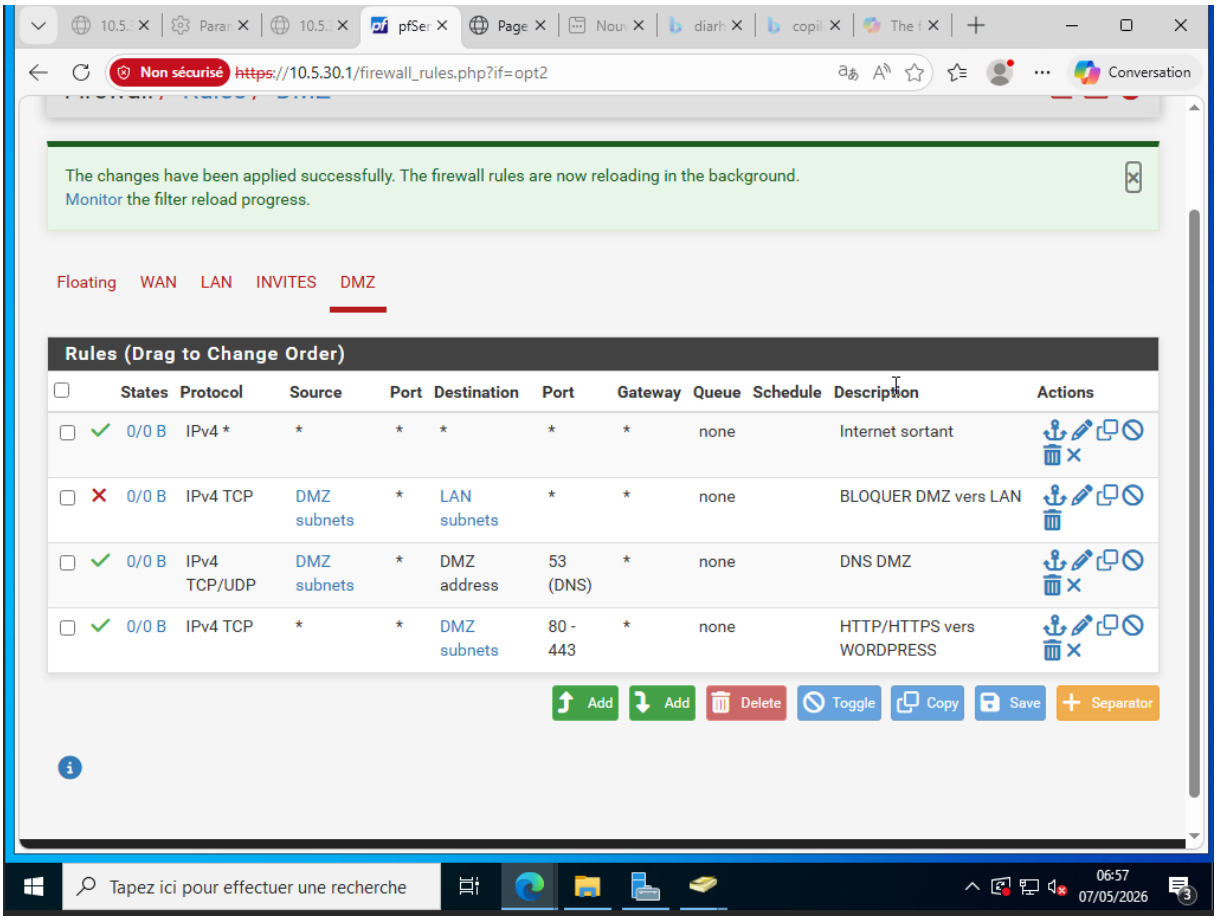
    Description : DMZ

4. Save



Étape 2 : Assigner comme interface

1. Dans Interfaces → Assignments, onglet Interface Assignments
2. Dans la dropdown, sélectionne "VLAN 50 on em1"
3. Clique Add
4. Save



Étape 4 : Créer les règles firewall DMZ

Va dans pfSense → Firewall → Rules → DMZ

Ajoute ces 4 règles (dans cet ordre) :

Règle 1 - HTTP/HTTPS (Internet → DMZ)

Action: Pass

Protocol: TCP

Source: any

Destination: DMZ net

Destination Port: 80, 443

Description: "HTTP/HTTPS vers WordPress"

Règle 2 - Bloquer accès LAN (DMZ → LAN)

Action: Block

Source: DMZ net

Destination: LAN net

Description: "Bloquer DMZ vers LAN"

Règle 3 - DNS (DMZ → pfSense)

Action: Pass

Protocol: TCP/UDP

Source: DMZ net

Destination: This Firewall (DMZ address)

Port: 53

Description: "DNS DMZ"

Règle 4 - Internet sortant (DMZ → WAN)

Action: Pass

Protocol: Any

Source: DMZ net

Destination: any

Description: "Internet sortant DMZ"

Segmentation Réseau — VLANS

Pour sécuriser et isoler les différents services de SALAUN TRAVELS, nous avons mis en place des VLANs sur PfSense.

Plan d'adressage

VLAN	Nom	Réseau	Gateway
LAN	Serveurs	10.5.0.0/16	10.5.30.1
20	WiFi Invité	10.6.0.0/24	10.6.0.1
30	Siège	10.7.0.0/24	10.7.0.1
40	Agences	10.8.0.0/24	10.8.0.1
50	DMZ	10.9.0.0/24	10.9.0.1

VLAN	Nom	Réseau	Gateway
60	WiFi Interne	10.10.0.0/24	10.10.0.1

Ce qu'on a fait

On a créé les VLANs sur l'interface em1 de PfSense, assigné chaque interface, configuré les IPs et activé le DHCP sur chaque VLAN avec le DNS pointant vers le DC1 (10.5.10.0). Des règles firewall ont été ajoutées pour autoriser le trafic sur chaque VLAN.

Le WiFi invité et la DMZ sont isolés du reste du réseau interne.