


RAPPORT

DE CLÔTURE DE PROJET ET DOCUMENTATION TECHNIQUE

| | | |
|------------------------------|--|-----------------|
| Nom du projet | Sécurité Civil [AP4] | Date du rapport |
| Personne en charge du projet | HEUSSER Nathan RACLOT Emilien GOURDIN Thomas | |
| BTS SIO |  | 21/04/2024 |



SOMMAIRE :

1. Introduction et Contexte du Projet

- Présentation du contexte et de la sécurité civile en France
- Description des Centres Opérationnels Départementaux et de leur importance
- Présentation du groupe

2. Objectifs du Projet

- Description détaillée des objectifs du projet
- Les enjeux informatiques pour le Centre Opérationnel Départemental
- Les enjeux des SIC à distance

3. Analyse des Besoins

- Expression détaillée des besoins initiaux
 - Les défis rencontrés et les ajustements nécessaires
 - Comparaison des besoins initiaux avec les fonctionnalités finales implémentées
- 4. Solution Technique Déployée**
 - Présentation de la solution de haute disponibilité pour les routeurs et l'accès Internet
 - Configuration des serveurs Active Directory et du serveur de messagerie
 - Mise en place de la supervision et du monitoring
 - Établissement de la connexion VPN et de la DMZ pour eBrigade
 - 5. Évaluation de la Solution**
 - Tests et validation de la solution technique
 - 6. Documentation Technique**
 - Manuel d'installation et de configuration détaillé
 - Procédures de maintenance et de surveillance
 - 7. Retours d'Expérience et Bonnes Pratiques**
 - Enseignements tirés du projet
 - Bonnes pratiques
 - Erreurs
 - 8. Conclusion**
 - Synthèse des résultats par rapport aux objectifs
 - 9. Annexes**
 - Copies d'écrans, diagrammes réseaux, scripts de configuration

1 : Introduction et Contexte du Projet

- Présentation du contexte et de la sécurité civile en France

Le projet de sécurité civile visait à optimiser la **résilience informatique** des Centres Opérationnels Départementaux en proposant une solution technique **autonome et redondée**, notamment en redondant l'accès Internet. Le projet impliquait également la mise en œuvre d'une **messagerie électronique**, la **supervision des serveurs et équipements critiques**, et l'établissement d'une **connexion OpenVPN Road Warrior** pour diffuser des applications à distance. De plus, il était nécessaire de mettre en place le logiciel open source **eBrigade**.

Pour la **clôture de ce projet**, le rapport doit **synthétiser toutes les phases**, des caractéristiques initiales du projet aux résultats finaux, y compris **les écarts** par rapport aux **objectifs** prévus. Il convient également de **documenter les**

meilleures pratiques qui ont émergé tout au long du projet ainsi que **les erreurs à ne pas répéter** pour des projets futurs, et de faciliter le transfert des connaissances accumulées.

La **documentation technique complète** du projet doit fonctionner comme un manuel d'utilisation, détaillant chaque étape de la mise en œuvre de la solution.

- Description des Centres Opérationnels Départementaux et de leur importance
-

Les **Centres Opérationnels Départementaux** (COD), parfois nommés Centres de Commandement Départementaux, sont des structures clés au sein des dispositifs de sécurité civile en France. Ils sont l'épine dorsale des **opérations de secours** et jouent un **rôle crucial dans la coordination des interventions d'urgence** et la gestion des crises au niveau départemental.

- Présentation du groupe
-



Emilien Raclot

Chef de Projet



Heusser Nathan

Administrateur
Système



Gourdin Thomas

Technicien

Emilien Raclot (Chef de Projet) :

- **Coordination générale du projet.**
- **Planification des tâches et gestion des délais.**
- **Communication avec le client et suivi des besoins.**
- **Gestion des ressources humaines et matérielles.**
- **Supervision de l'avancement des travaux et résolution des problèmes.**

Heusser Nathan (Administrateur Systeme) :

- **Configuration et déploiement des serveurs Active Directory.**

- **Installation et configuration du serveur de messagerie électronique.**
- **Mise en place du serveur de supervision et de monitoring.**
- **Configuration du serveur VPN Road Warrior.**
- **Déploiement du serveur Web eBrigade dans la DMZ.**

Gourdin Thomas (Technicien) :

- **Assistance à la configuration des serveurs Active Directory.**
- **Support pour l'installation et la configuration du serveur de messagerie électronique.**
- **Aide à la mise en place du serveur de supervision et de monitoring.**
- **Collaboration à la configuration du serveur VPN Road Warrior.**
- **Contribution au déploiement du serveur Web eBrigade dans la DMZ.**

2 : Objectifs du Projet

- Description détaillée des objectifs du projet
-
- **Optimiser la résilience informatique des Centres Opérationnels Départementaux** : en proposant une solution technique autonome et redondante, notamment en redondant l'accès Internet.
 - **Connexion sécurisée OpenVPN Road Warrior** : Mise en place d'un accès sécurisé et distant aux ressources du réseau pour les agents sur le terrain, permettant une coordination en temps réel pendant les interventions.
 - **Déploiement de la messagerie électronique** : Installation d'un serveur de messagerie pour faciliter la communication interne et externe, essentielle pour le partage rapide d'informations en situation d'urgence.
 - **Supervision des infrastructures critiques** : Utilisation d'outils de monitoring pour surveiller en continu l'état des serveurs et des équipements essentiels, avec des alertes immédiates en cas de défaillance.
 - **Implémentation du logiciel eBrigade** : Déploiement de cette solution open source pour la gestion des effectifs, des interventions, et la production de rapports d'activité, améliorant ainsi la gestion des opérations et la coordination des équipes.
- Les enjeux informatiques pour le Centre Opérationnel Départemental
-
- **Fiabilité des Systèmes** : Garantir la robustesse et la résilience des infrastructures informatiques pour assurer une disponibilité constante en situations d'urgence.

- **Sécurité des Données** : Protéger les informations sensibles contre les cyberattaques grâce à des mesures de cybersécurité avancées.
 - **Continuité Opérationnelle** : Mettre en place des solutions de redondance et de récupération après sinistre pour maintenir les opérations sans interruption.
 - **Intégration Technologique** : Assurer l'interopérabilité entre différents systèmes et technologies pour optimiser la gestion des interventions.
 - **Compétences Techniques** : Former le personnel à l'utilisation efficace des outils technologiques pour améliorer la réactivité et l'efficacité des réponses.
- Les enjeux des SIC à distance
-

- **Accessibilité sécurisée** : Assurer un accès distant sécurisé aux systèmes d'information via le VPN même en 4G ...
- **Intégrité des données** : Maintenir la fiabilité et l'intégrité des données transmises à distance.
- **Latence et bande passante** : Optimiser la performance des réseaux pour réduire la latence.
- **Interopérabilité** : Garantir la compatibilité des systèmes à distance avec divers équipements et logiciels utilisés.
- **Gestion des identités et des accès** : Contrôler strictement l'accès aux informations sensibles.
- **Formation et support technique** : Fournir une formation continue et un support technique efficace pour les utilisateurs distants

3 : Analyse des Besoins

- Expression détaillée des besoins initiaux
-

- **Accès aux outils en situation de crise**, même en l'absence d'Internet.
- **Utilisation du logiciel eBrigade** pour la gestion du personnel, des interventions et des rapports.
- **Supervision en temps réel des serveurs et équipements critiques**, avec alerte en cas de dysfonctionnement.
- **Autonomie et sécurité des accès et des données**, avec une installation locale des serveurs et services.
- **Haute disponibilité des systèmes** : Maintenir une opérabilité constante des systèmes

- Les défis rencontrés et les ajustements nécessaires
-

- **Défis** : Rencontres de problèmes de compatibilité entre les systèmes existants et les nouvelles solutions, problèmes de sécurité des données lors de l'accès à distance.
- **Ajustements** : Mise à niveau des infrastructures réseau existantes, renforcement des protocoles de sécurité, et intégration de solutions de redondance pour améliorer la résilience des systèmes.
 - Comparaison des besoins initiaux avec les fonctionnalités finales implémentées

- **Accès sécurisé à distance** : Implémentation réussie d'une solution VPN robuste qui assure un accès sécurisé et crypté pour les agents, surpassant les attentes initiales en termes de sécurité des données.
- **Haute disponibilité des systèmes** : Les systèmes de redondance et de basculement automatique installés assurent une disponibilité quasi totale, même en cas de panne majeure, ce qui correspond aux besoins initiaux.
- **Communication efficace** : Installation d'un système de messagerie .

4 : Solution Proposée et Déployée

- Architecture Matérielle et Infrastructure Réseau pour l'entreprise

1. Serveurs :

- **PCSpecialist** : Serveurs robustes utilisés pour héberger les services critiques tels que Active Directory, le serveur de messagerie Zimbra, et le système de surveillance WAZUH.

2. Routeurs Redondés :

- **Netgate 8200 MAX HA pfSense+ Security Gateway** : Deux unités configurées en haute disponibilité (HA) pour assurer la continuité du service en cas de défaillance d'une unité.

3. Switches :

- **Aruba 2530 48 ports POE+** : Switches gérables fournissant la connectivité réseau aux serveurs, routeurs, et autres périphériques réseau, supportant Power over Ethernet (PoE) pour alimenter des dispositifs tels que des caméras de sécurité ou des points d'accès sans fil.

4. Onduleur :

- **APC Back-UPS Pro 1500VA** : Protection contre les interruptions de courant, garantissant une alimentation électrique ininterrompue pour les équipements critiques.

5. Infrastructure Réseau :

- Câbles RJ45 CAT 7 SFTP : Câbles de catégorie 7 avec blindage pour une meilleure protection contre les interférences, garantissant une transmission de données à haute vitesse et fiable.
- Émetteurs-récepteurs SFP+ 10GBase-SR : Modules pour connectivité fibre optique permettant des liaisons à très haut débit jusqu'à 10 Gbps, utilisés pour connecter les switches aux serveurs et au stockage en réseau.
- Fibre Orange pro et SFR pro : Connexions internet professionnelles à très haut débit de deux fournisseurs différents, assurant redondance et haute disponibilité de l'accès à internet.

6. Licences CA :

- 5 licences CA : Certificats d'autorité de certification utilisés pour sécuriser les communications entre les différents composants du réseau via SSL/TLS.
- Présentation de la solution de haute disponibilité pour les routeurs et l'accès Internet

-
- **Configuration des routeurs** : Installation de deux routeurs **pfSense** en configuration redondante utilisant le protocole CARP (Common Address Redundancy Protocol) pour garantir qu'en cas de défaillance d'un routeur, l'autre prendra immédiatement le relais WAN, LAN, VLANs ...



- Configuration des serveurs Active Directory et du serveur de messagerie

-
- **Serveurs Active Directory** : Déploiement de deux serveurs **Active Directory** en configuration de redondance pour la gestion des identités et des politiques de sécurité à travers l'organisation AD & DNS redondés.
 - **Serveur de messagerie** : Installation d'un serveur de messagerie robuste "**Zimbra Collaboration Suite**" intégré à Active Directory pour un contrôle d'accès basé sur les rôles et une gestion facilitée des comptes utilisateurs.





- Mise en place de la supervision et du monitoring
-

- Outils de supervision : Implémentation de **WAZUH**, pour la surveillance réseau pour contrôler en temps réel l'état de santé des infrastructures IT, avec des alertes proactives en cas de défaillance détectée.

wazuh.

- Établissement de la connexion VPN et de la DMZ pour eBrigade
-

- Connexion VPN Road Warrior : Configuration d'une solution **OPEN VPN** via pfSense qui permet aux agents de terrain d'accéder de manière sécurisée aux ressources internes du réseau, même lorsqu'ils sont en déplacement ou en intervention.
- DMZ pour eBrigade : Mise en œuvre d'une zone démilitarisée (DMZ) sur le VLAN 40 pour héberger l'application **eBrigade**, assurant son accessibilité externe sécurisée tout en protégeant le reste du réseau interne.



5 : Evaluation de la Solution

- Tests et validation de la solution technique
-

- **Tests de basculement des routeurs** : Des simulations de défaillance ont été réalisées pour vérifier la capacité de basculement automatique entre les deux routeurs pfSense. Ces tests ont confirmé que le second routeur prend le relais sans interruption du service, validant ainsi la redondance et la résilience de la solution réseau.

```

Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : scivil.local
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : BC-24-11-DA-5A-83
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::5533:da4:4db0:ac15%9(préféré)
Adresse IPv4. . . . . : 192.168.2.100(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : dimanche 21 avril 2024 16:13:48
Bail expirant. . . . . : dimanche 21 avril 2024 18:13:49
Passerelle par défaut. . . . . : 192.168.2.1
Serveur DHCP . . . . . : 192.168.2.2
IAID DHCPv6 . . . . . : 230433809
DUID de client DHCPv6. . . . . : 00-01-00-01-2D-AC-00-85-BC-24-11-DA-5A-83
Serveurs DNS. . . . . : 192.168.10.10
                        192.168.10.11
  
```

Désactivation du Routeur Principal :

```

Microsoft Windows [version 10.0.19045.4291]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping google.com -t

Envoi d'une requête 'ping' sur google.com [216.58.215.46] avec 32 octets de données :
Réponse de 216.58.215.46 : octets=32 temps=12 ms TTL=248
Réponse de 216.58.215.46 : octets=32 temps=12 ms TTL=248
Réponse de 216.58.215.46 : octets=32 temps=12 ms TTL=248
  
```

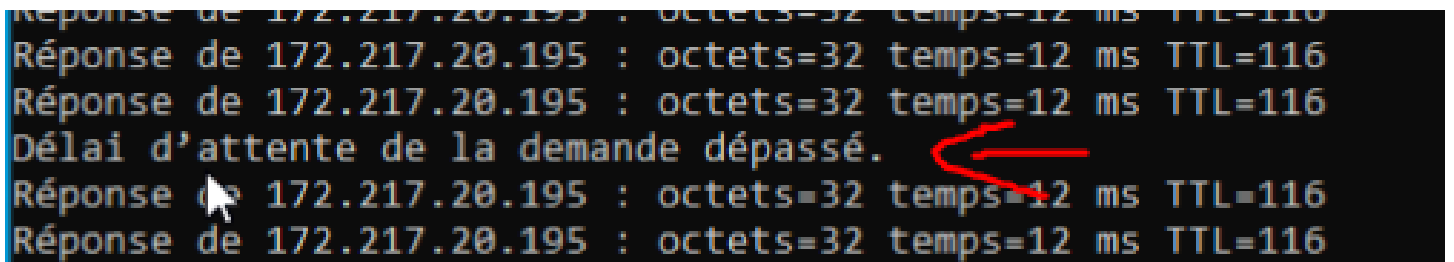
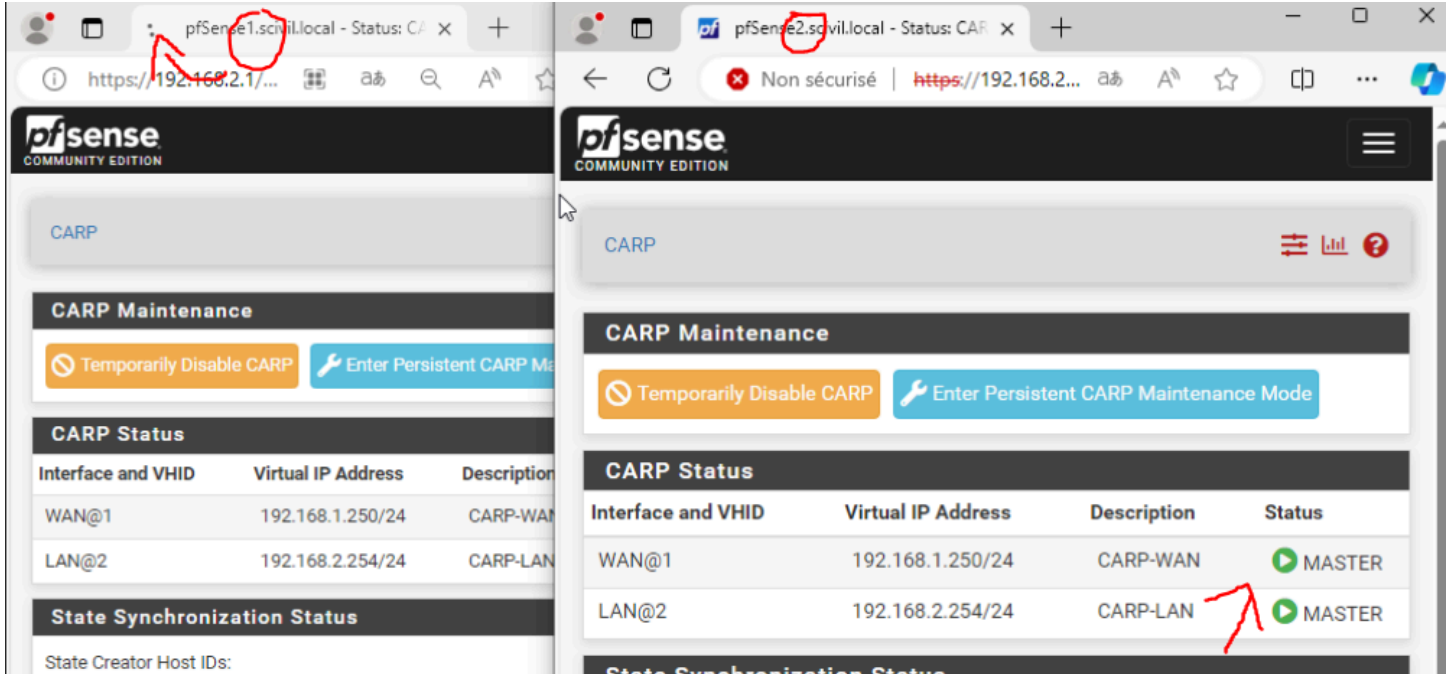
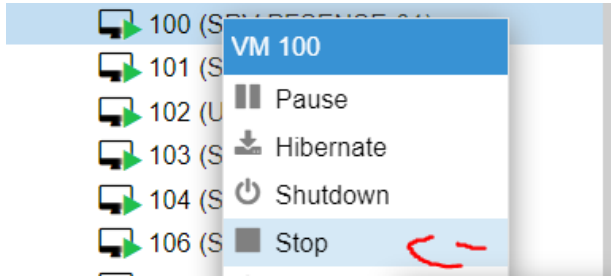
The image shows two side-by-side screenshots of the pfSense web interface, specifically the CARP (Common Address Redundancy Protocol) configuration page. Both screenshots show the 'CARP Maintenance' section with buttons for 'Temporarily Disable CARP' and 'Enter Persistent CARP Maintenance Mode'. Below this is the 'CARP Status' table.

| Interface and VHID | Virtual IP Address | Description | Status |
|--------------------|--------------------|-------------|--------|
| WAN@1 | 192.168.1.250/24 | CARP-WAN | MASTER |
| LAN@2 | 192.168.2.254/24 | CARP-LAN | MASTER |

In the right screenshot, the status has changed:

| Interface and VHID | Virtual IP Address | Description | Status |
|--------------------|--------------------|-------------|--------|
| @1 | 192.168.1.250/24 | CARP-WAN | BACKUP |
| @2 | 192.168.2.254/24 | CARP-LAN | BACKUP |

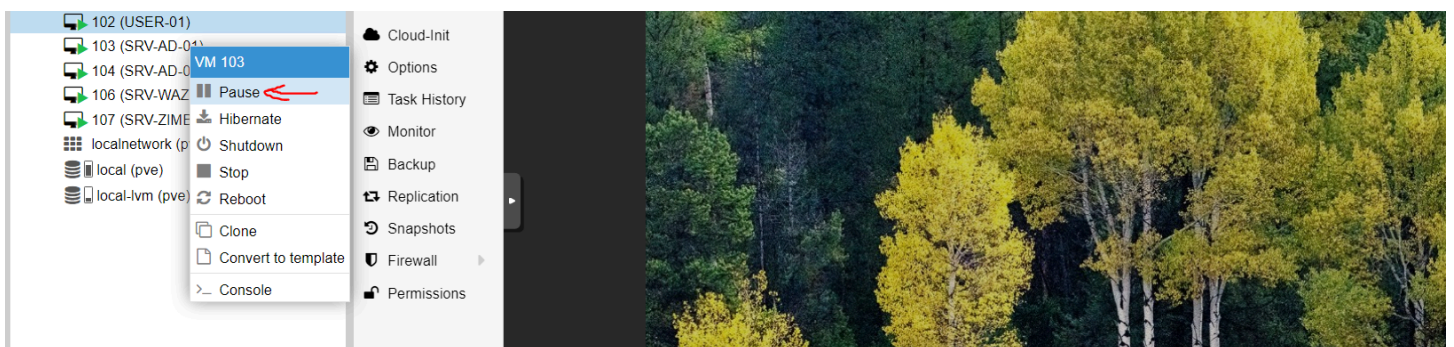
Red arrows in the original image point to the status changes in the CARP Status table.

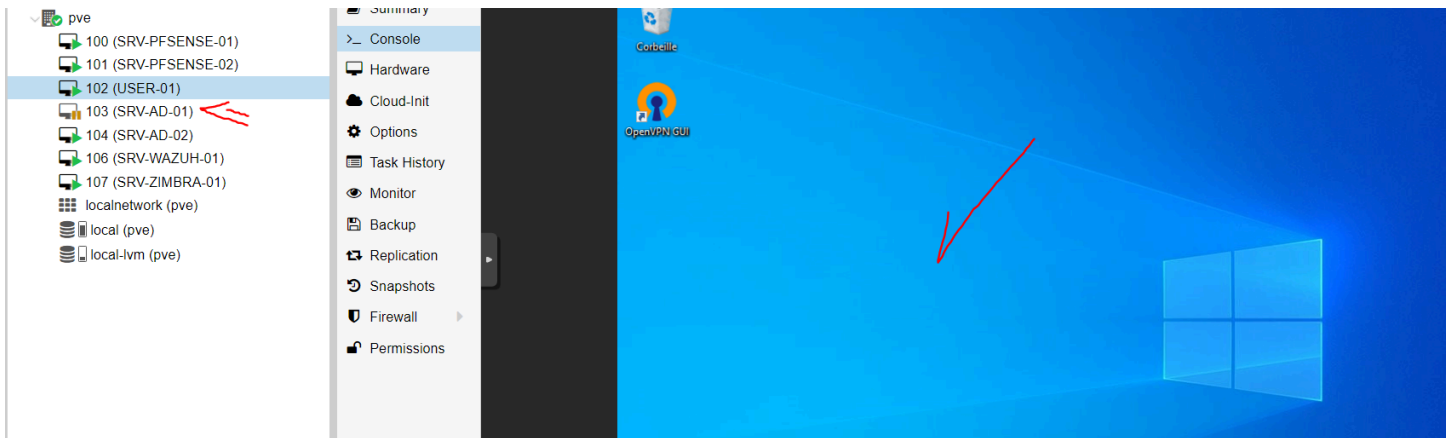
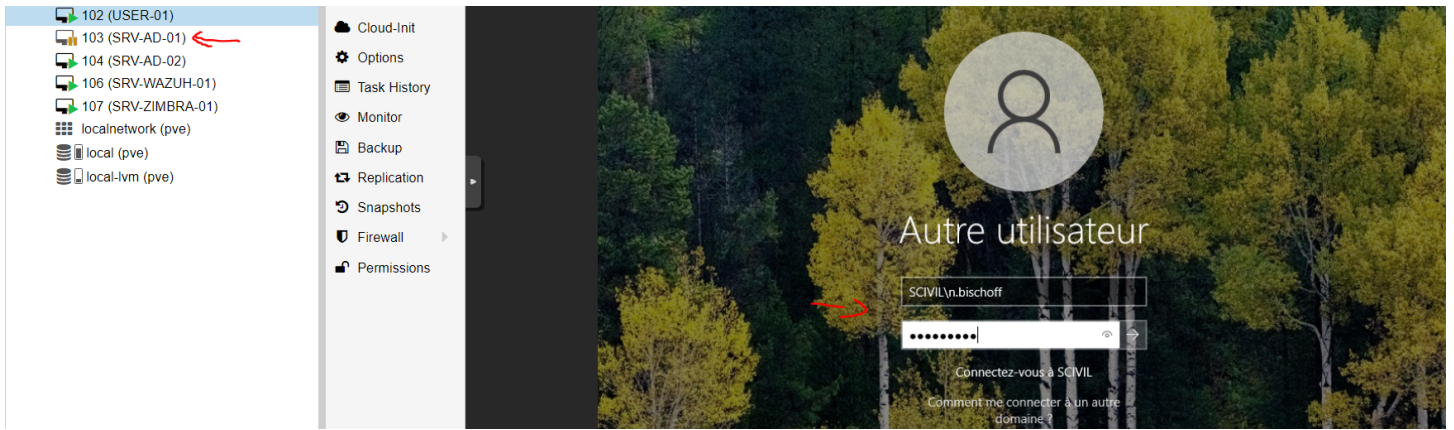


Notre routeur a bien pris le relai sur notre machine.

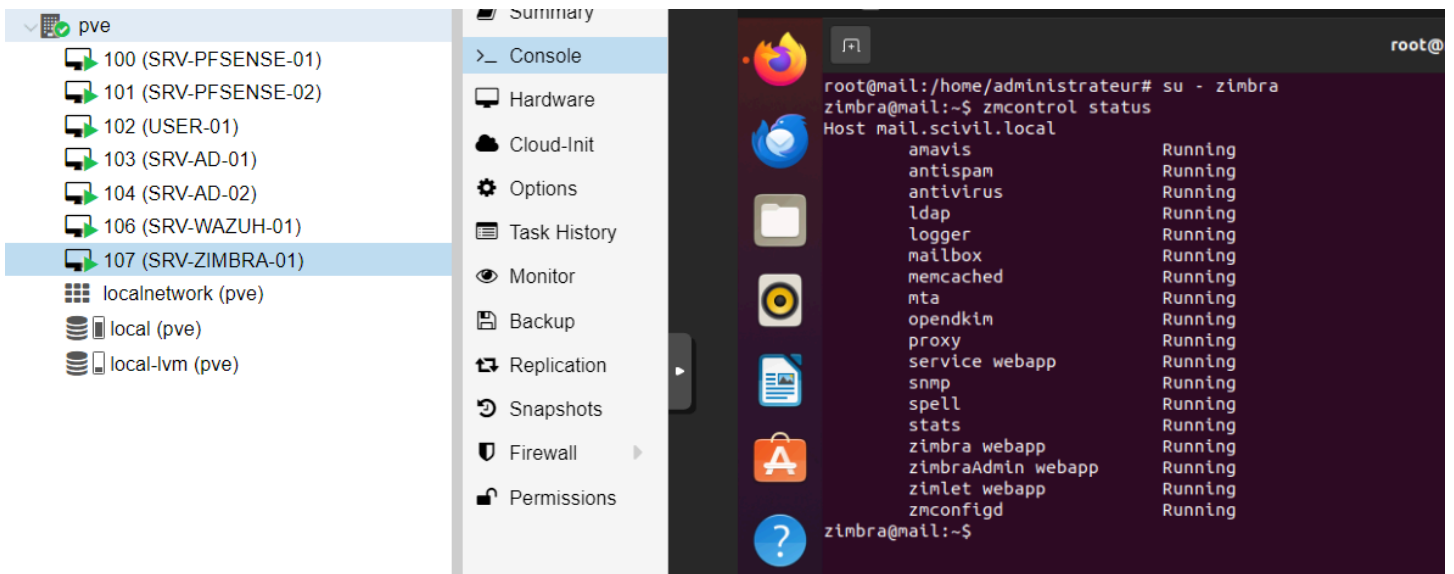
- Validation des serveurs Active Directory :

Tests de synchronisation et d'authentification pour assurer que la redondance des serveurs Active Directory fonctionne correctement :

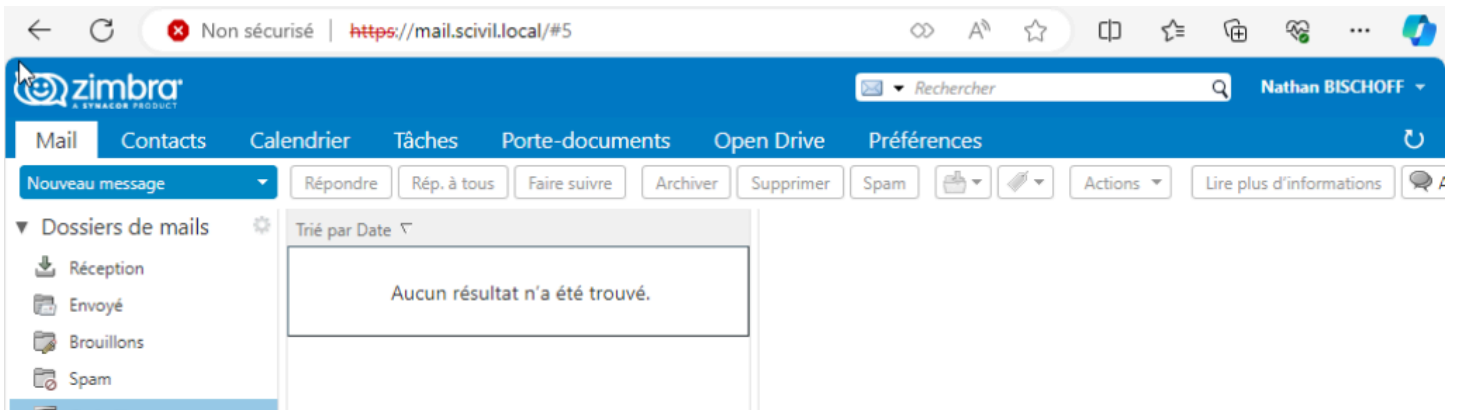
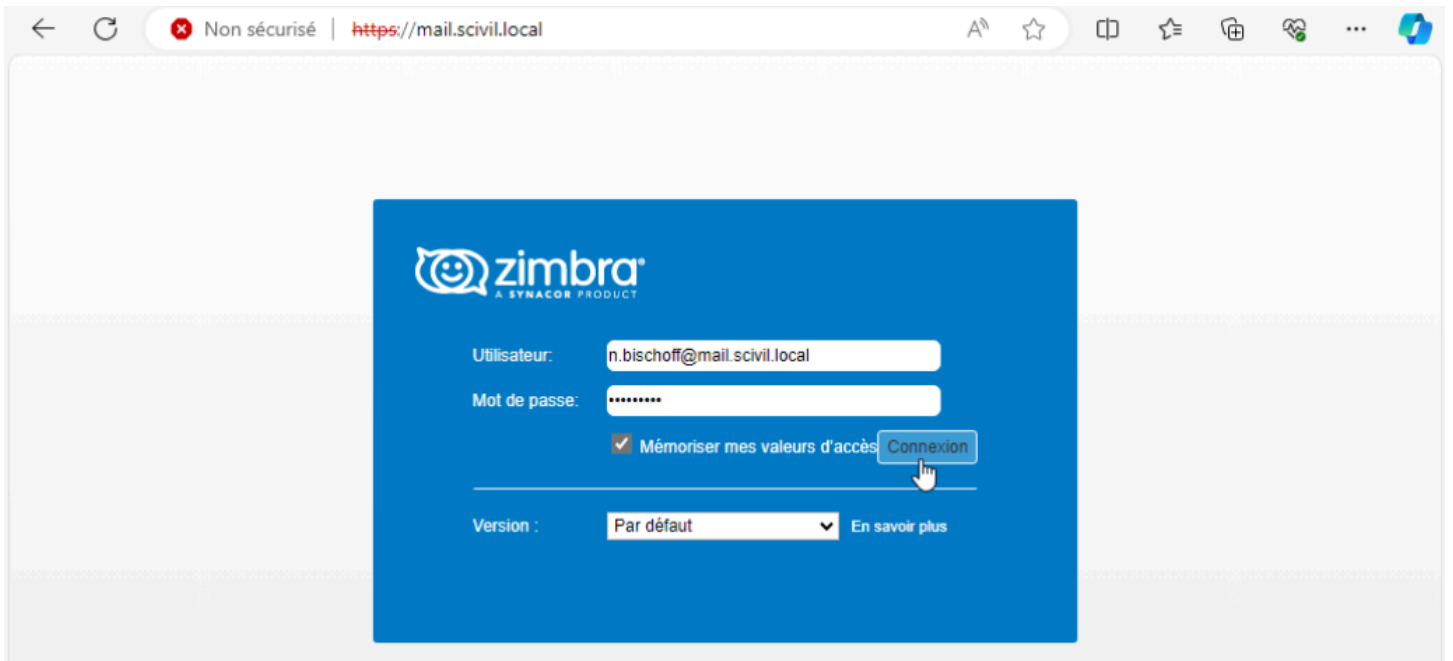




• Serveur de messagerie Zimbra :



Accès depuis un Utilisateur : <https://mail.scivil.local>

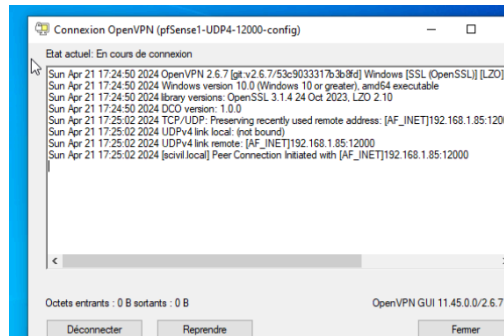
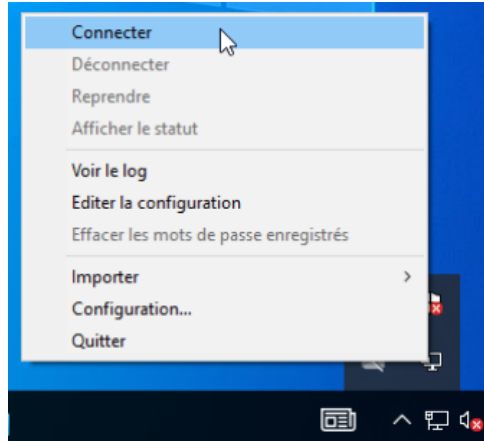


• Accès à Wazuh avec l'agent installé sur les différents matériels :

| ID | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status | Actions |
|-----|-------------------|---------------|----------|--|--------------|---------|--------|---------|
| 001 | mail.scivil.local | 192.168.20.3 | default | Ubuntu 20.04.6 LTS | node01 | v4.7.3 | active | |
| 002 | AD01 | 192.168.10.10 | default | Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587 | node01 | v4.7.3 | active | |
| 003 | AD02 | 192.168.10.11 | default | Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587 | node01 | v4.7.3 | active | |

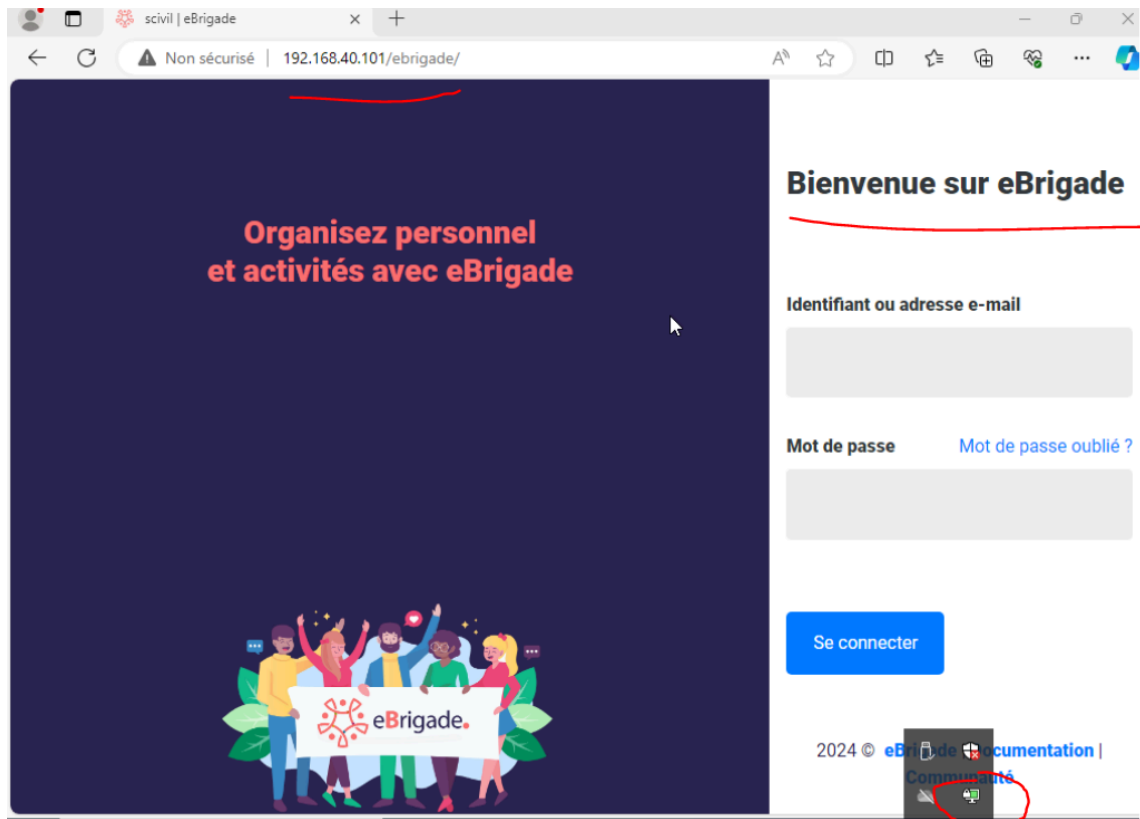
- **Accès à E-BRIGADE depuis une connexion OPEN VPN d'un Utilisateur EXTERNE :**

| | | | |
|-----------|----------|--------|---------|
| Bridge: | vmbr0 | Model: | |
| VLAN Tag: | Bridge ↑ | Active | Comment |
| Firewall: | vmbr0 | Yes | WAN |



OpenVPN GUI
Connecté à: pfSense1-UDP4-12000-confi
Connecté depuis: 21/04/2024 17:26
Adresse IP assignée: 10.0.8.2





6 : Evaluation de la Solution

- Manuel d'installation et de configuration détaillé

Installation des Routeurs pfSense



Préparation de l'environnement :

Étape 1 : Installation des Instances pfSense

- Créez deux VMs pfSense dans Proxmox avec la configuration système minimale requise ainsi que 3 Carte réseaux vubr0, vubr1, vubr2 (LAN WAN et CARP .)
- Installez pfSense sur chaque VM en suivant l'assistant d'installation standard.
- Attribuez les interfaces sur chaque VM pfSense. Assurez-vous que chaque VM a une interface pour le WAN et une pour le LAN.

PROXMOX Virtual Environment 8.1.4 Search Documentation Create VM Create CT root@pam

Server View Datacenter

Datacenter

- pve
 - localnetwork (pve)
 - local (pve)
 - local-lvm (pve)

Search

Summary

Notes

Cluster

Ceph

Options

Storage

Backup

Replication

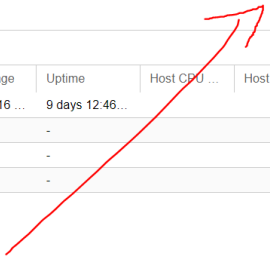
Permissions

- Users
- API Tokens
- Two Factor
- Groups
- Pools
- Roles
- Realms
- HA

| Type ↑ | Description | Disk usage... | Memory us... | CPU usage | Uptime | Host CPU ... | Host Mem... | Tags |
|---------|--------------------|---------------|--------------|----------------|-----------------|--------------|-------------|------|
| node | pve | 18.8 % | 4.8 % | 0.1% of 16 ... | 9 days 12.46... | | | |
| sdn | localnetwork (pve) | | | | | | | |
| storage | local (pve) | 18.8 % | | | | | | |
| storage | local-lvm (pve) | 0.0 % | | | | | | |

Tasks Cluster log

| Start Time ↓ | End Time | Node | User name | Description | Status |
|--------------|----------|------|-----------|-------------|--------|
|--------------|----------|------|-----------|-------------|--------|



Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 100

Name: SRV-PFSENSE-01

Help Advanced Back **Next**

Create: Virtual Machine



General **OS** System Disks CPU Memory Network Confirm

Use CD/DVD disc image file (iso)

Guest OS:

Storage: local

Type: Linux

ISO image: |

Version: 6.x - 2.6 Kernel

Use physical C

Name

For...

Size

Do not use any

debian-12.5.0-amd64-netinst.iso

iso

659.55 MB

pfSense-CE-2.7.2-RELEASE-amd64.iso

iso

874.67 MB

w_server_2022.iso

iso

5.06 GB

Windows_10.iso

iso

4.92 GB

Advanced

Back

Next

Create: Virtual Machine



General

OS

System

Disks

CPU

Memory

Network

Confirm

| Key ↑ | Value |
|----------|--|
| cores | 1 |
| cpu | x86-64-v2-AES |
| ide2 | local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom |
| memory | 2048 |
| name | SRV-PFSENSE-01 |
| net0 | virtio,bridge=vibr0,firewall=1 |
| nodename | pve |
| numa | 0 |
| ostype | l26 |
| scsi0 | local-lvm:32,iotthread=on |
| scsihw | virtio-scsi-single |
| sockets | 1 |
| vmid | 100 |

Start after created

Advanced

Back

Finish



100 (SRV-PFSENSE-01)


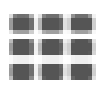




Hardware









| Bridge ↑ | Active | Comment |
|----------|--------|---------|
| vmbr0 | Yes | |
| vmbr1 | Yes | |
| vmbr2 | Yes | |



 pve






-  100 (SRV-PFSENSE-0)
-  localnetwork (
-  local (pve)
-  local-lvm (pve)




VM 100

-  Start
-  Shutdown
-  Stop
-  Reboot

-  Clone
-  Convert to template

-  Console

- 
 pve
- 
 100 (SRV-PFSENSE-0)
-  101 (SRV-PFSENSE-0)

-  Summary
-  Console
-  Hardware

Guest not running

 Start Now

pfSense Installer

-----| Copyright and distribution notice |-----

Copyright and Trademark Notices.

Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.

Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are

----- 26%-----

[Accept]

pfSense Installer

Welcome

Welcome to pfSense!

- Install**
- Rescue Shell
- Recover config.xml
- Install pfSense**
- Launch a shell for rescue operations
- Recover config.xml from a previous install

< **DK** >

<Cancel>

pfSense Installer

Partitioning

How would you like to partition your disk?

- Auto (ZFS)**
- Auto (UFS)
- Manual
- Shell
- Guided Root-on-ZFS**
- Guided UFS Disk Setup
- Manual Disk Setup (experts)
- Open a shell and partition by hand

< **DK** >

<Cancel>

To use ZFS with less than 8GB RAM, see <https://wiki.freebsd.org/ZFSTuningGuide>

ZFS Configuration

Configure Options:

| | |
|---------------------|---------------------------|
| >>> Install | Proceed with Installation |
| T Pool Type/Disks: | stripe: 0 disks |
| - Rescan Devices | * |
| - Disk Info | * |
| N Pool Name | pfSense |
| 4 Force 4K Sectors? | YES |
| E Encrypt Disks? | NO |
| P Partition Scheme | GPT (BIOS) |
| S Swap Size | 1g |
| M Mirror Swap? | NO |
| W Encrypt Swap? | NO |

<Select> <Cancel>

---[Use alphanumeric characters, punctuation, TAB or ENTER]---

Create ZFS boot pool with displayed options

ZFS Configuration

Select Virtual Device type:

| | |
|--------|---------------------------------|
| stripe | Stripe - No Redundancy |
| mirror | Mirror - n-Way Mirroring |
| raid10 | RAID 1+0 - n x 2-Way Mirrors |
| raidz1 | RAID-Z1 - Single Redundant RAID |
| raidz2 | RAID-Z2 - Double Redundant RAID |
| raidz3 | RAID-Z3 - Triple Redundant RAID |

<DK> <Cancel>

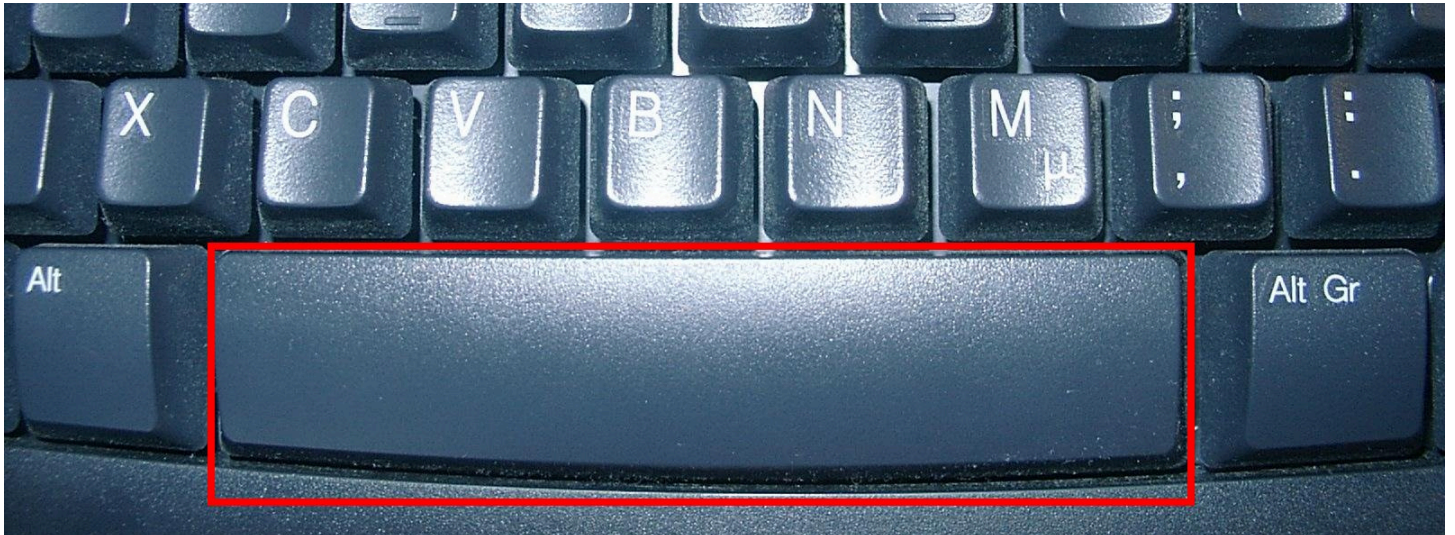
---[Use alphanumeric characters, TAB or ENTER]---

pfSense Installer

ZFS Configuration

[*] da0 QEMU QEMU HARDDISK

< OK > < Back >



pfSense Installer

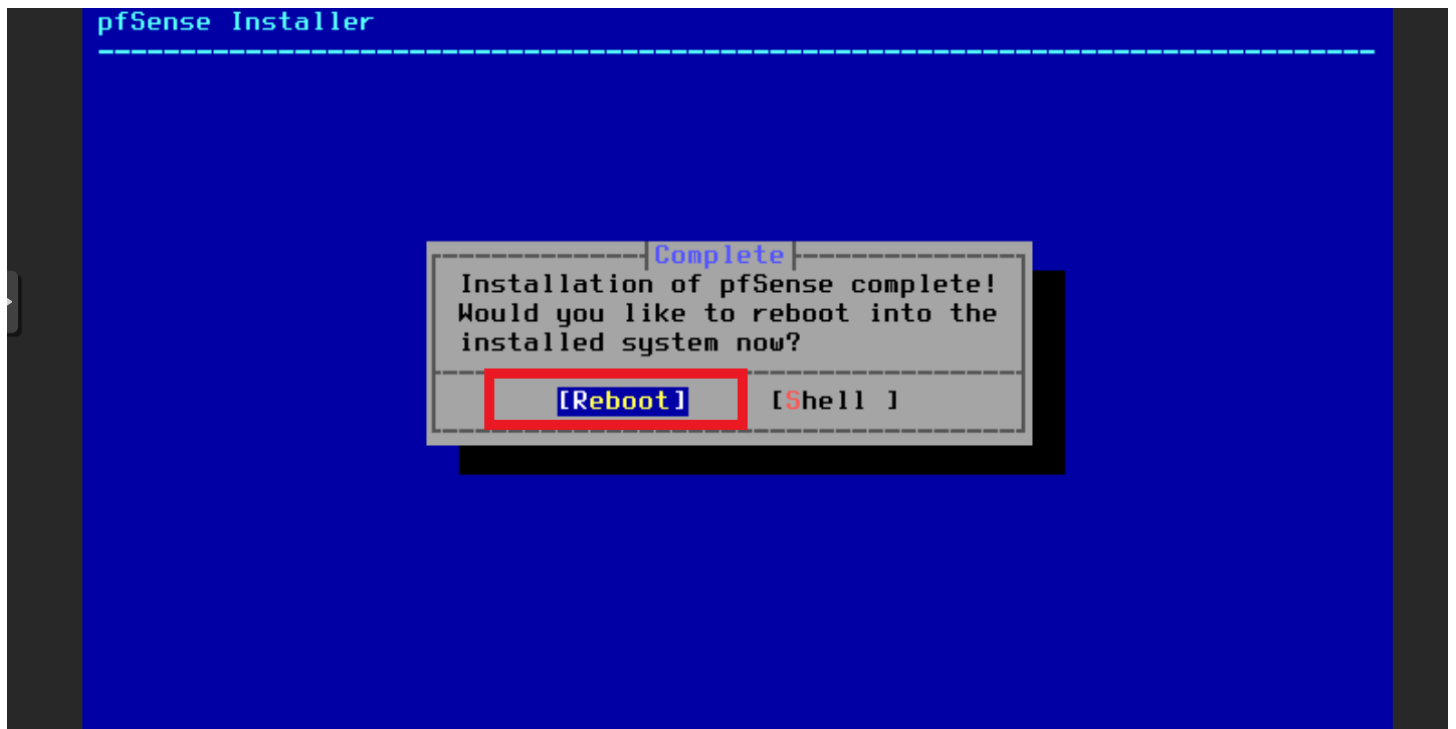
ZFS Configuration

Last Chance! Are you sure you want to destroy the current contents of the following disks:

da0

< YES > < NO >

[PRESS ARROW, TAB or ENTER]



- > Même manipulation sur la vm copier pour la redondance

Configurez le WAN sur chaque instance pfSense.

- Pour pfSense Principal (Master), utilisez une adresse IP telle que 192.168.1.64/24.
- Pour pfSense Secondaire (Backup), utilisez une adresse IP telle que 192.168.1.79/24.

Configurez le LAN sur chaque instance pfSense.

- Pour pfSense Principal, utilisez une adresse IP telle que 192.168.2.1/24.
- Pour pfSense Secondaire, utilisez une adresse IP telle que 192.168.2.2/24.

On configure l'interface LAN (Le WAN est automatiquement configuré)

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.85/24
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

Enter an option: 2

Available interfaces:

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

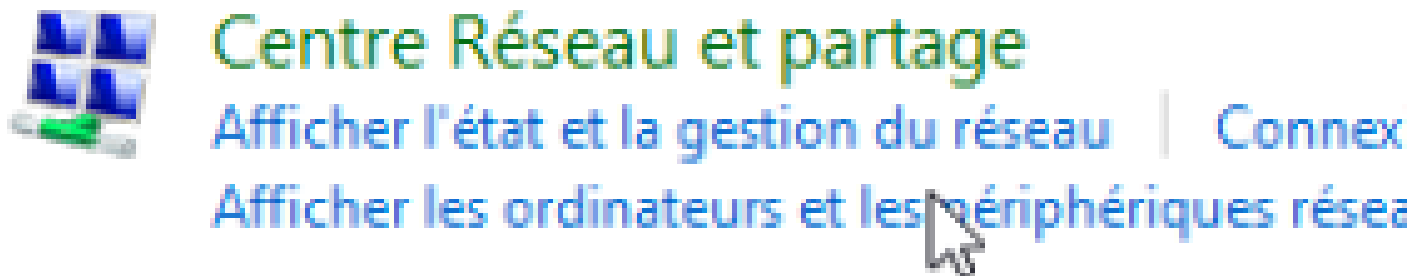
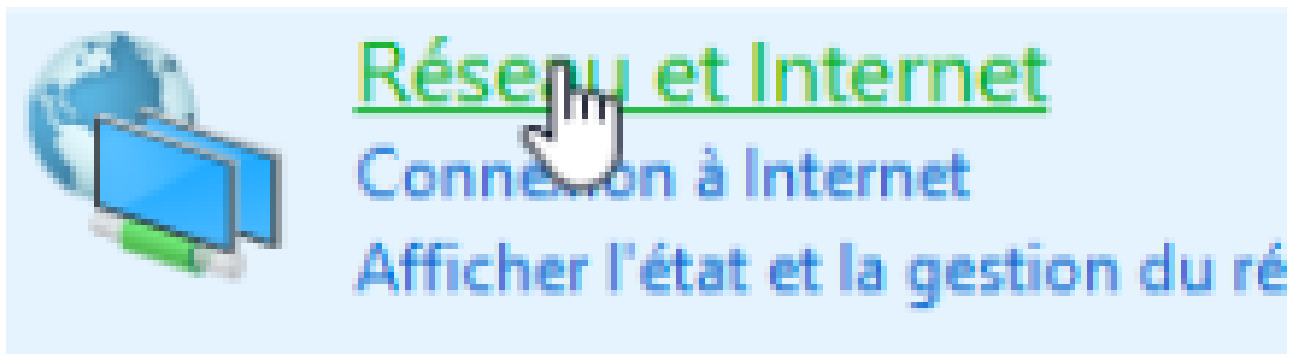
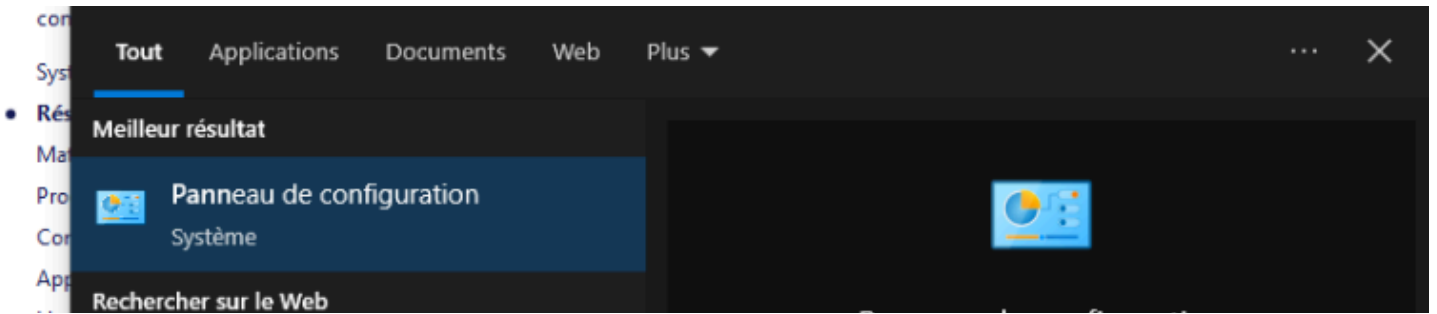
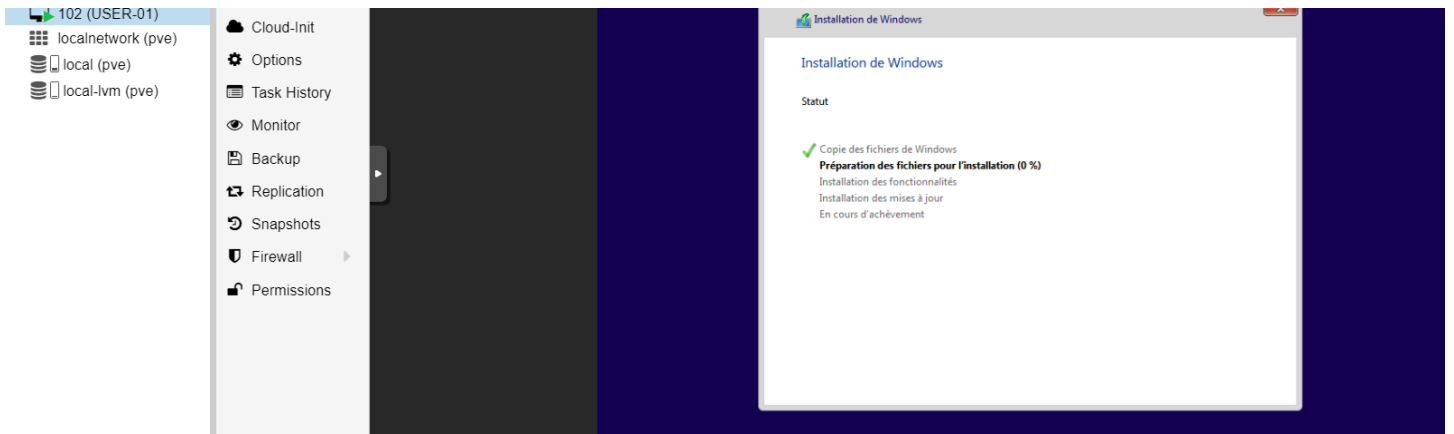
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

```
Configure IPv4 address LAN
Enter the new LAN IPv4 address
> 192.168.2.1
```

```
Subnet masks are entered as bit count
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
> 24
```

Pour accéder à l'interface web , nous allons créer une VM Utilisateur Windows 10 avec une IP dans le même réseau que le pfSense :



ATTACHER VOS RESEAUX ACTIFS

Réseau non identifié
Réseau public

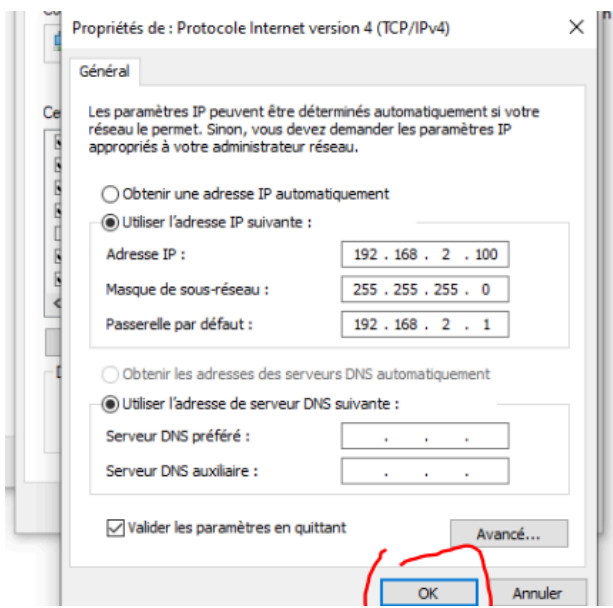
Type d'accès :
Connexions :

Pas d'accès réseau
Ethernet

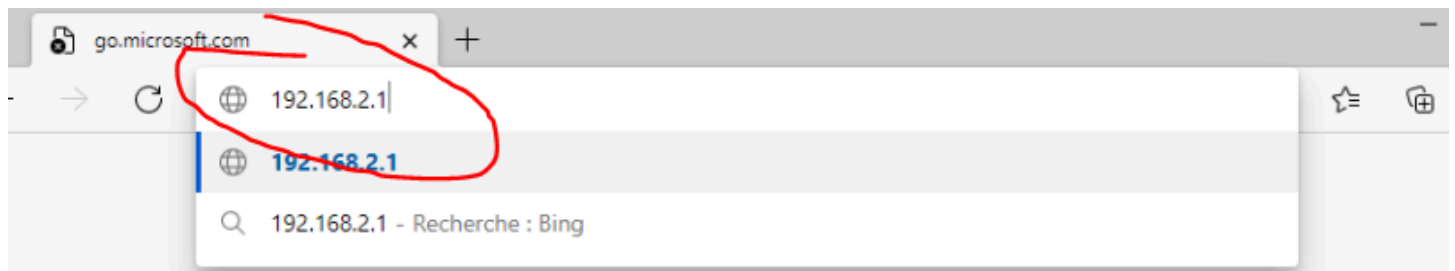
Modifier vos paramètres réseau



Manificateur de paquets UoS
Protocole Internet version 4 (TCP/IPv4)



On va ensuite sur un navigateur web et dans l'url de la page on tape l'up LAN que l'on as choisis, ici 192.168.2.1 :





Login to pfSense

SIGN IN

admin

pfSense



SIGN IN



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Netgate® Global Support is available 24/7 ?

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

» Next

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

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

Secondary DNS Server

Override DNS

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

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

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

Secondary DNS Server

Override DNS

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

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / [pfSense Setup](#) / Time Server Information 

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

**Time server
hostname**

Enter the hostname (FQDN) of the time server.

Timezone



>> Next

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / [pfSense Setup](#) / [Configure WAN Interface](#) ?

Step 4 of 9

Configure WAN Interface

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

SelectedType

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address

Subnet Mask

Upstream Gateway

DHCP client configuration

DHCP Hostname

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

PPPoE
Username

PPPoE
Password

Show PPPoE
password

Reveal password characters

PPPoE
Service name

Hint: this field can usually be left empty

PPPoE Dial on
demand

Enable Dial-On-Demand mode

This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPPoE Idle
timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

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.

[»» Next](#)

→ Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. **Comme mon infra est ici virtuelle, je vais obligatoirement faire communiquer des réseaux privés, je n'utilise pas réellement une adresse publique.** Il est donc **nécessaire dans le cadre d'un labo de décocher ces 2 cases** sinon vous pourrez avoir des petits couacs.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface 

Step 5 of 9

Configure LAN Interface

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

LAN IP Address

192.168.3.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

24 

>> Next

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Set Admin WebGUI Password 

Step 6 of 9

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

.....

>> Next

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Set Admin WebGUI Password 

Step 6 of 9

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

>> Next

Wizard / pfSense Setup / Reload configuration 

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Reload in progress

A reload is now in progress. Please wait.

The wizard will redirect to the next step once the reload is completed.

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- [Learn more about Netgate's product line, services, and pfSense software from our website](#)
- [To learn about Netgate appliances and other offers, visit our store](#)
- [Become part of the pfSense community. Visit our forum](#)
- [Subscribe to our newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

System Information

| | |
|--------------------|---|
| Name | pfSense.localdomain |
| User | admin@192.168.3.100 (Local Database) |
| System | VMware Virtual Machine Netgate Device ID: a86f287011fe9e1cd7a2 |
| BIOS | Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020 |
| Version | 2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Mon Aug 14 16:37:26 CEST 2023 |
| CPU Type | 13th Gen Intel(R) Core(TM) i5-13400 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No |
| Hardware crypto | Inactive |
| Kernel PTI | Disabled |
| MDS Mitigation | Inactive |
| Uptime | 00 Hour 20 Minutes 57 Seconds |
| Current date/time | Mon Aug 14 16:57:26 CEST 2023 |
| DNS server(s) | <ul style="list-style-type: none"> 127.0.0.1 10.0.0.2 |
| Last config change | Mon Aug 14 16:54:36 CEST 2023 |
| State table size | 0% (12/96000) Show states |
| MBUF Usage | 0% (3556/1000000) |
| Load average | 0.19, 0.24, 0.23 |
| CPU usage | 1% |
| Memory usage | 27% of 960 MiB |
| SWAP usage | 0% of 1023 MiB |

Netgate Services And Support

Contract type: **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

| Interface | Status | Speed | MAC |
|-----------|--------|-------------------------|-------------|
| WAN | ↑ | 1000baseT <full-duplex> | 10.128.0.1 |
| LAN | ↑ | 1000baseT <full-duplex> | 192.168.3.1 |

Disks

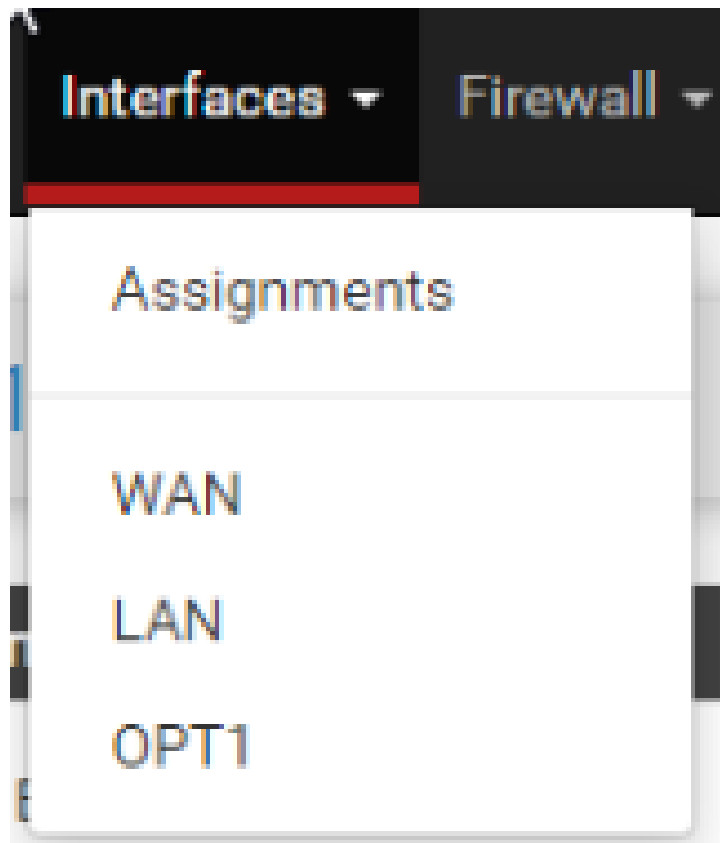
| Mount | Used | Size | Usage |
|-------|------|------|-----------------|
| > / | 1.3G | 18G | 8% of 18G (ufs) |

Available Widgets

| | | | |
|---|--------------------------------------|--------------------------------------|--------------------------------------|
| + Captive Portal Status | + CARP Status | + Dynamic DNS Status | + Firewall Logs |
| + Interface Statistics | + Gateways | + GEOM Mirror Status | + Installed Packages |
| + OpenVPN | + Interfaces | + IPsec | + NTP Status |
| + Services Status | + Picture | + RSS | + S.M.A.R.T. Status |
| + Wake-on-Lan | + System Information | + Thermal Sensors | + Traffic Graphs |

Other dashboard settings are available from the [General Setup](#) page.

On configure la redondance en configurant la troisième carte réseau :



General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

Sur le deuxième PF SENSE on synchronise bien la réception de la configuration :

The screenshot shows the pfSense web interface for High Availability settings. The browser address bar indicates the URL is https://192.168.2.2/system_hasync.php. The page title is "System / High Availability".

State Synchronization Settings (pfsync)

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

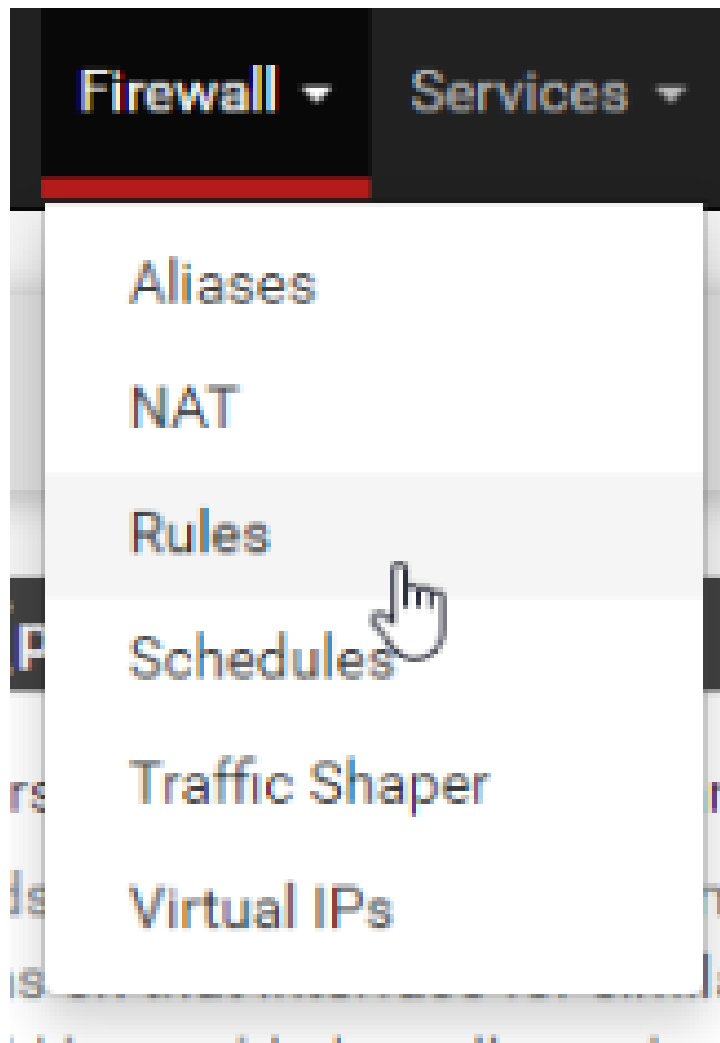
Synchronize Interface
If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.

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

Configuration Synchronization Settings (XMLRPC Sync)

Mais pour qu'elle réceptionne on doit juste dans le par feu l'autoriser :





Sur le CARP1 :

| Rules (Drag to Change Order) | | | | | | | | | | | | |
|------------------------------|-------------------------------------|------------------|--------------------------|------|------------------|----------------|---------|-------|----------|----------------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/0 B TCP/UDP | IPv4 CARP1 address | * | CARP1 net | 443 (HTTPS) | * | none | | SYNCHRONISATION CONFIGURATION | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0/0 B PFSYNC | IPv4 CARP1 net | * | CARP1 address | * | * | none | | | <input type="checkbox"/> | <input type="checkbox"/> |

Buttons:

Ensuite on éteint le PF SENSE 1 et on voit bien que le PF SENSE 2 prend le relai et que la configuration firewall ... est dupliqué

CARP Maintenance**CARP Status**

| Interface and VHID | Virtual IP Address | Description | Status |
|--------------------|--------------------|-------------|--|
| WAN@1 | 192.168.1.250/24 | CARP-WAN |  MASTER |
| LAN@2 | 192.168.2.254/24 | CARP-LAN |  MASTER |

State Synchronization Status

State Creator Host IDs:

- 84feff3
- f56655ac (This node)

On ajoute les VLANS

The changes have been applied successfully.

General ConfigurationEnable Enable interface**Description**

VLAN_ADMIN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

The MAC address of a VLAN interface must be set on its parent interface

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstance

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above, minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Active Windows
Accédez aux paramètres pour ac
Windows.

Interface Assignments Interface Groups Wireless **VLANs** QinQs PPPs GREs GIFs Bridges LAGGs

VLAN Interfaces

| Interface | VLAN tag | Priority | Description | Actions |
|-----------|----------|----------|---------------|---------|
| em1 (lan) | 10 | | vlan_admin | |
| em1 (lan) | 20 | | vlan_serveurs | |
| em1 (lan) | 30 | | vlan_dmz | |
| em1 (lan) | 40 | | vlan_vpn | |

Add

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks Blocks traffic from IP addresses that are reserved for private networks (RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the source address of any packets received. This option should be turned on for WAN interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local addresses. Note: The update of the bogon list is performed in the background. For more information, see System > Advanced, Firewall & NAT settings.

Save

Active Windows
Accédez aux paramètres pour activer Windows.

On voit que la redondance fonctionne en coupant le pfsense 1 et on voit que l'autre passe en Maître et non en backup

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / DHCP Server / VLAN_SERVEURS

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

LAN CARP1 VLAN_ADMIN VLAN_SERVEURS VLAN_DMZ VLAN_VPN

General DHCP Options

| | |
|-----------------------|---|
| DHCP Backend | ISC DHCP |
| Enable | <input checked="" type="checkbox"/> Enable DHCP server on VLAN_SERVEURS interface |
| BOOTP | <input type="checkbox"/> Ignore BOOTP queries |
| Deny Unknown Clients | <input type="text" value="Allow all clients"/> When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range. |
| Ignore Denied Clients | <input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small> |

ps://192.168.2.1/services_dhcp.php

Configuration des Serveurs Active Directory



1. Installation de Windows Server :
 - Installation et configuration des rôles AD DS (Active Directory Domain Services).
 - Configuration du DNS et du DHCP au sein de l'Active Directory.
2. Synchronisation et redondance :
 - Mise en place de la réplication entre les deux serveurs AD.
 - Tests de failover pour garantir la continuité du service.



Configuration du système d'exploitation Microsoft Server

Microsoft

Langue à installer: Français (France)

Format horaire et monétaire: Français (France)

Clavier ou méthode d'entrée: Français

Entrez la langue et les préférences de votre choix et cliquez sur Suivant pour continuer.

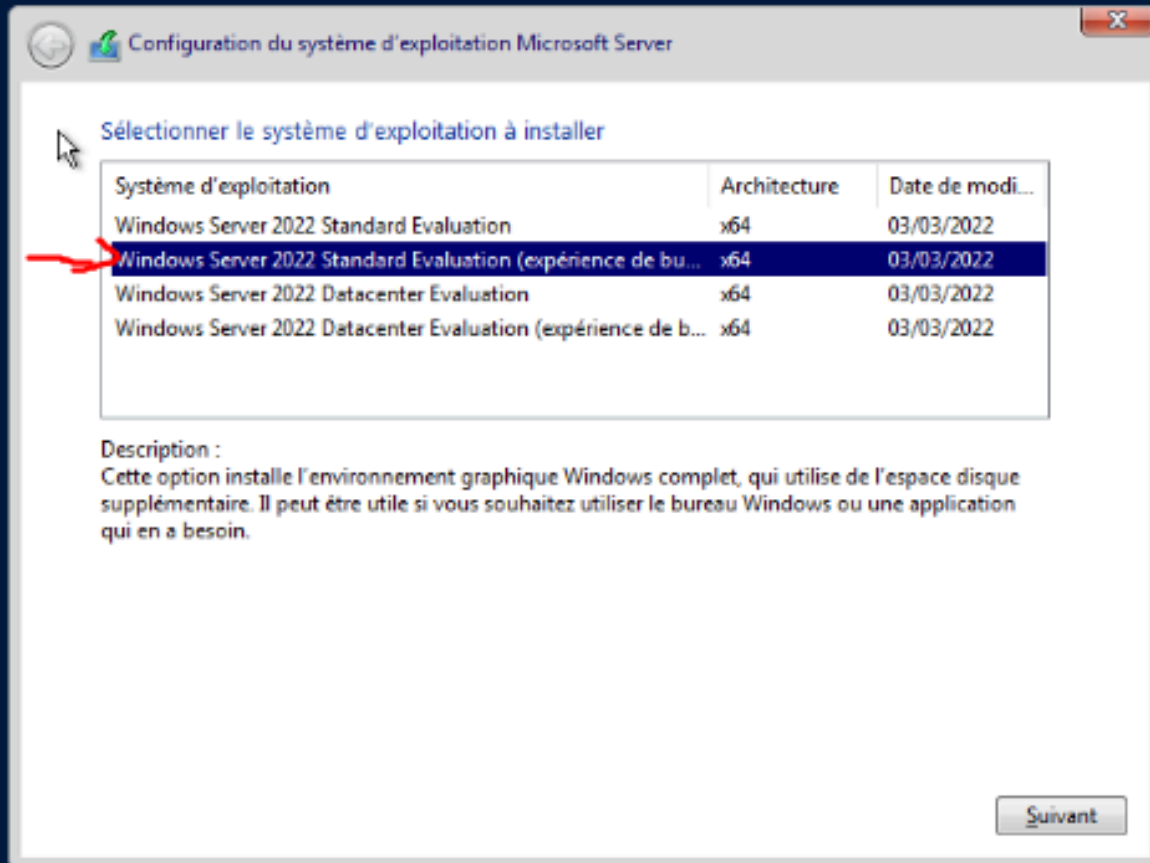
© Microsoft Corporation. Tous droits réservés.

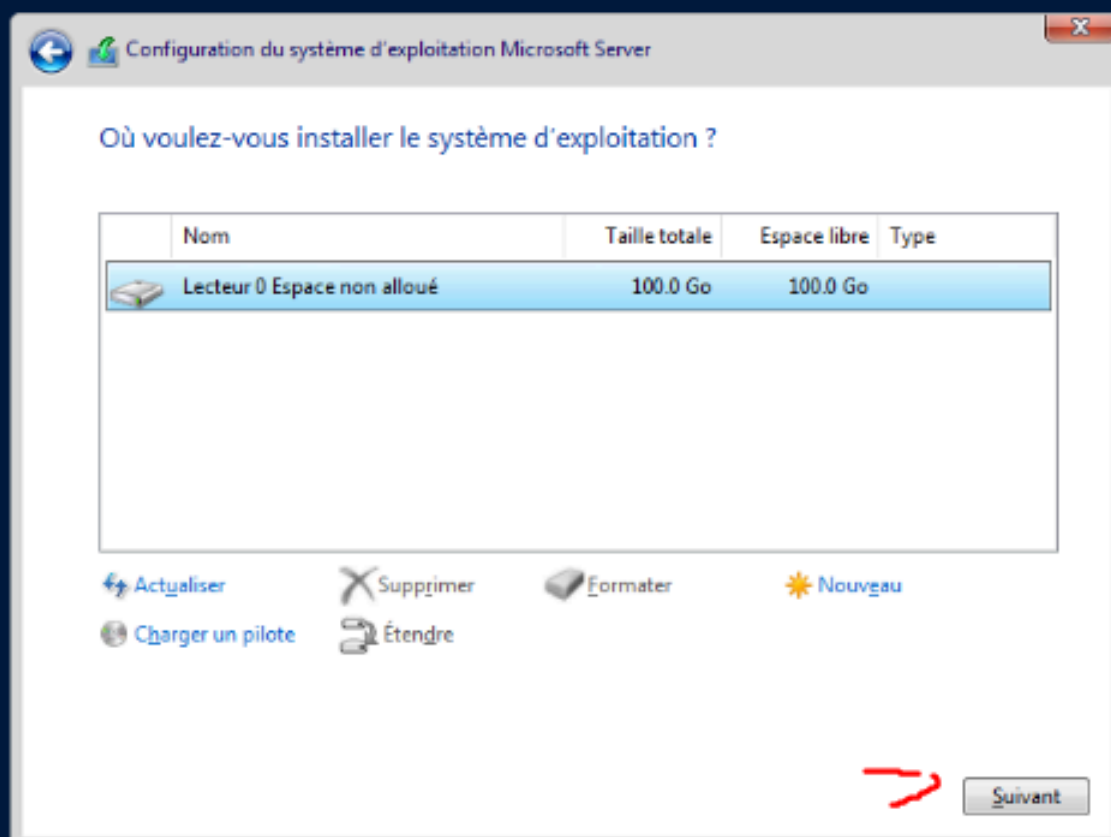
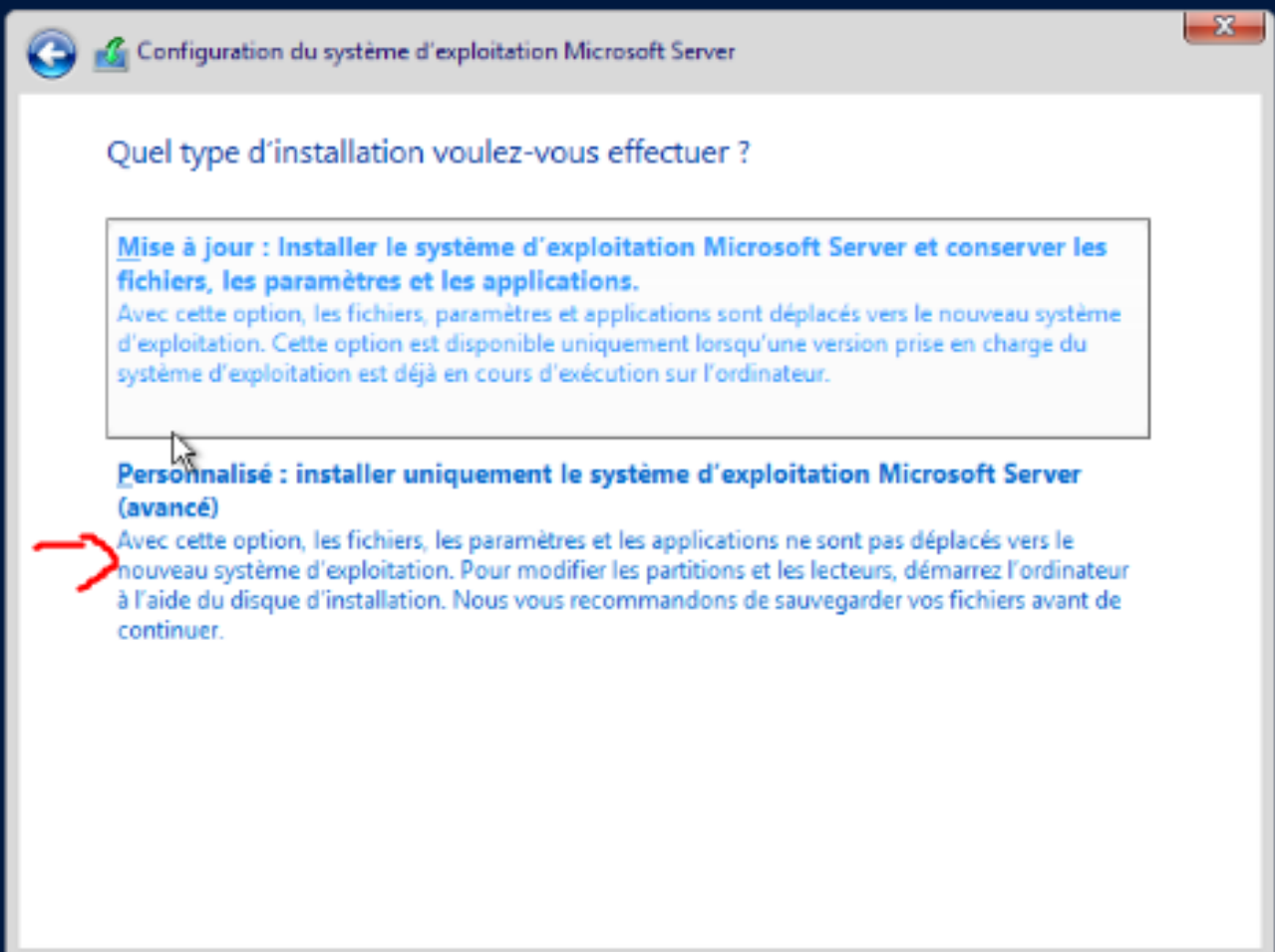
Suivant



Installer maintenant

Démarrage du programme d'installation





Installation du système d'exploitation Microsoft Server

Statut

✓ Copie en cours des fichiers du système d'exploitation Microsoft Server

Préparation des fichiers pour l'installation (0 %)

Installation des fonctionnalités

Installation des mises à jour

En cours d'achèvement

- Tableau de bord
- Serveur local**
- Tous les serveurs
- Services de fichiers et d...

PROPRIÉTÉS

Pour WIN-IRQFQMLNNSJ

| | | | |
|-----------------------------------|---|---|--------------------------------------|
| Nom de l'ordinateur | WIN-IRQFQMLNNSJ | Dernières mises à jour installées | |
| Groupe de travail | WORKGROUP | Windows Update | |
| | | Dernière recherche de mises à jour : | |
| | | Jamais | |
| Pare-feu Microsoft Defender | Privé : Actif | Antivirus Microsoft Defender | Protection en temps réel : activée |
| Gestion à distance | Activé | Commentaires et diagnostics | Paramètres |
| Bureau à distance | Désactivé | Configuration de sécurité renforcée d'Internet Explorer | Actif |
| Association de cartes réseau | Désactivé | Fuseau horaire | (UTC+01:00) Bruxelles, Copenhague, N |
| Ethernet | 192.168.10.11, Compatible IPv6 | ID de produit (Product ID) | 00454-40000-00001-AA807 (activé) |
| Version du système d'exploitation | Microsoft Windows Server 2022 Standard Evaluation | Processeurs | QEMU Virtual CPU version 2.5+, QEM |
| Informations sur le matériel | QEMU Standard PC (Q35 + ICH9, 2009) | Mémoire installée (RAM) | 7,96 Go |
| | | Espace disque total | 99,33 Go |

ÉVÉNEMENTS

Tous les événements | 8 au total

TÂCHES ▾

- Ajouter des rôles et fonctionnalités**
- Supprimer des rôles et fonctionnalités
- Ajouter des serveurs
- Créer un groupe de serveurs
- Propriétés du Gestionnaire de serveur

Gestionnaire de serveur

Gestionnaire de serveur > Serveur local

Tableau de bord

Serveur local

Tous les serveurs

Services de fichiers et d.

PROPRIÉTÉS
Pour WIN-IROFQMLNNSJ

| Nom de l'ordinateur | Groupes de travail | Dernières mises à jour installées |
|---------------------|--------------------|-----------------------------------|
| WIN-IROFQMLNNSJ | WORKGROUP | Windows Update |

Assistent Ajout de rôles et de fonctionnalités

Avant de commencer

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
Démarrer l'Assistant de Suppression de rôles et de fonctionnalités

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

Ignorer cette page par défaut

< Précédent Suivant > Installer Annuler

Microsoft-Windows-CertificateServicesClient-CertEnroll Application 14/04/2024 16:07:45

Assistent Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SERVEUR DE DESTINATION
WIN-IROFQMLNNSJ

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

- Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
- Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Tableau de bord

Serveur local

Tous les serveurs

Services de fichiers et d...

PROPRIÉTÉS
Pour WIN-IRQFQMLNNSJ

Nom de l'ordinateur: WIN-IRQFQMLNNSJ
Groupe de travail: WORKGROUP

Dernières mises à jour installées: Windows Update

Assistent Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SEVEUR DE DESTINATION
WIN-IRQFQMLNNSJ

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

| Nom | Adresse IP | Système d'exploitation |
|-----------------|----------------|---|
| WIN-IRQFQMLNNSJ | 192.168.20.101 | Microsoft Windows Server 2022 Standard Evaluation |

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Assistent Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SEVEUR DE DESTINATION
WIN-IRQFQMLNNSJ

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

AD DS

Confirmation

Résultats

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

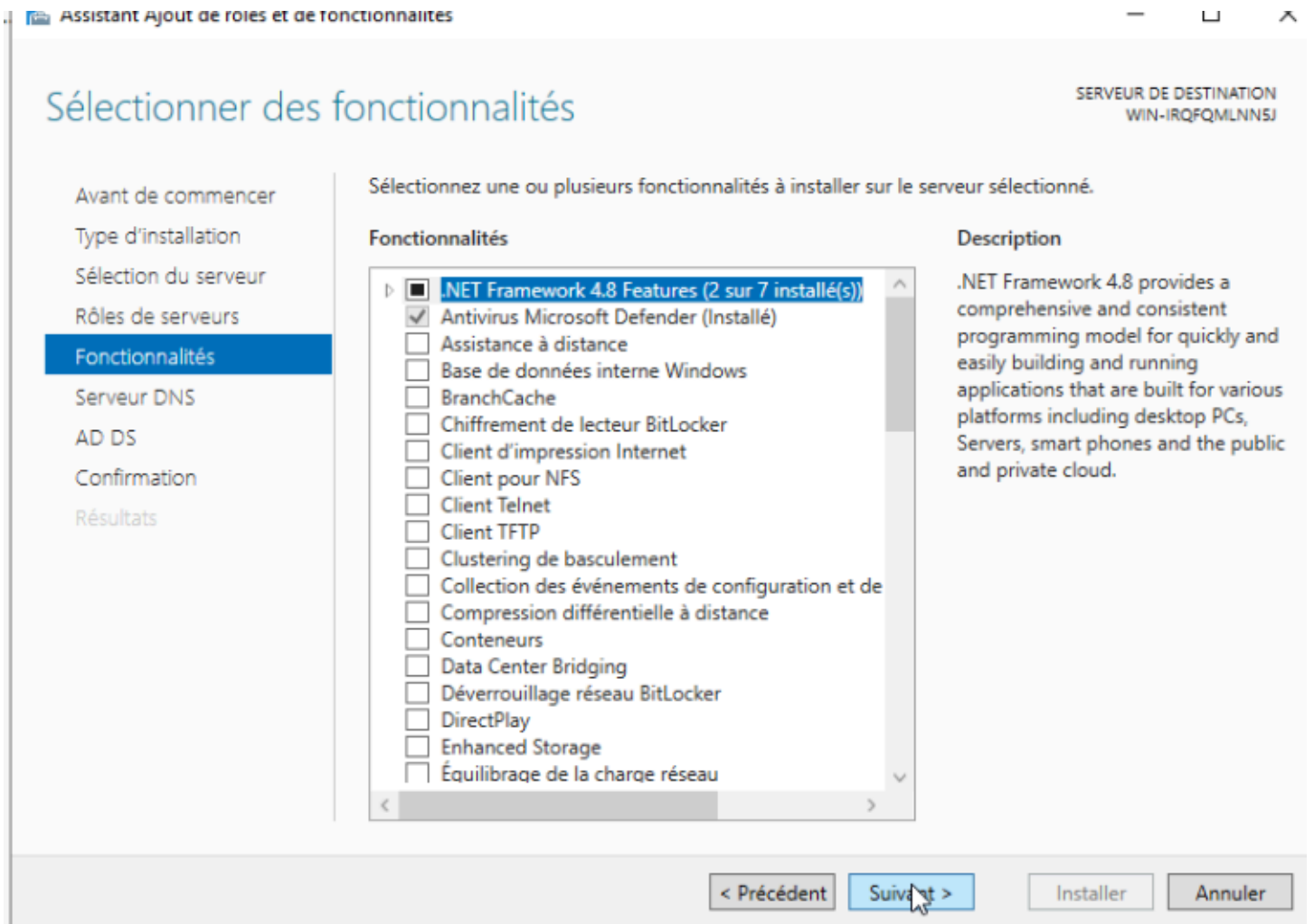
Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Hyper-V
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (1 sur 12 installés)
- Services de stratégie et d'accès réseau
- Services WSUS (Windows Server Update Services)

Description

Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.

< Précédent Suivant > Installer Annuler



PfSense : configurer un VPN-SSL client-to-site avec OpenVPN :

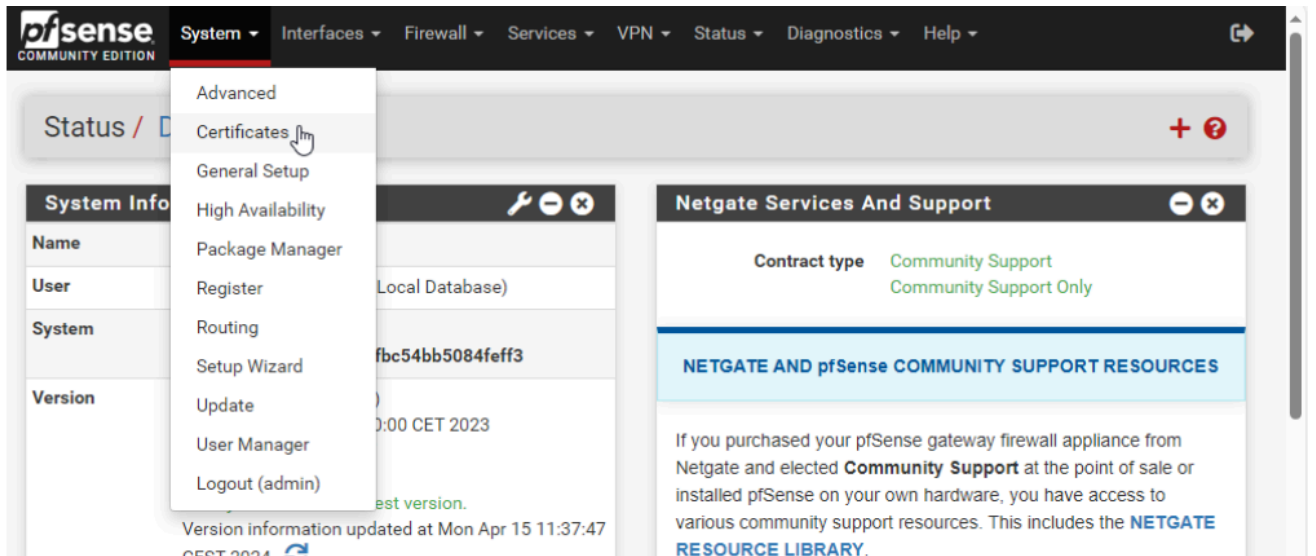


Configuration des VPNs et de la DMZ pour sécuriser l'accès à l'application eBrigade.

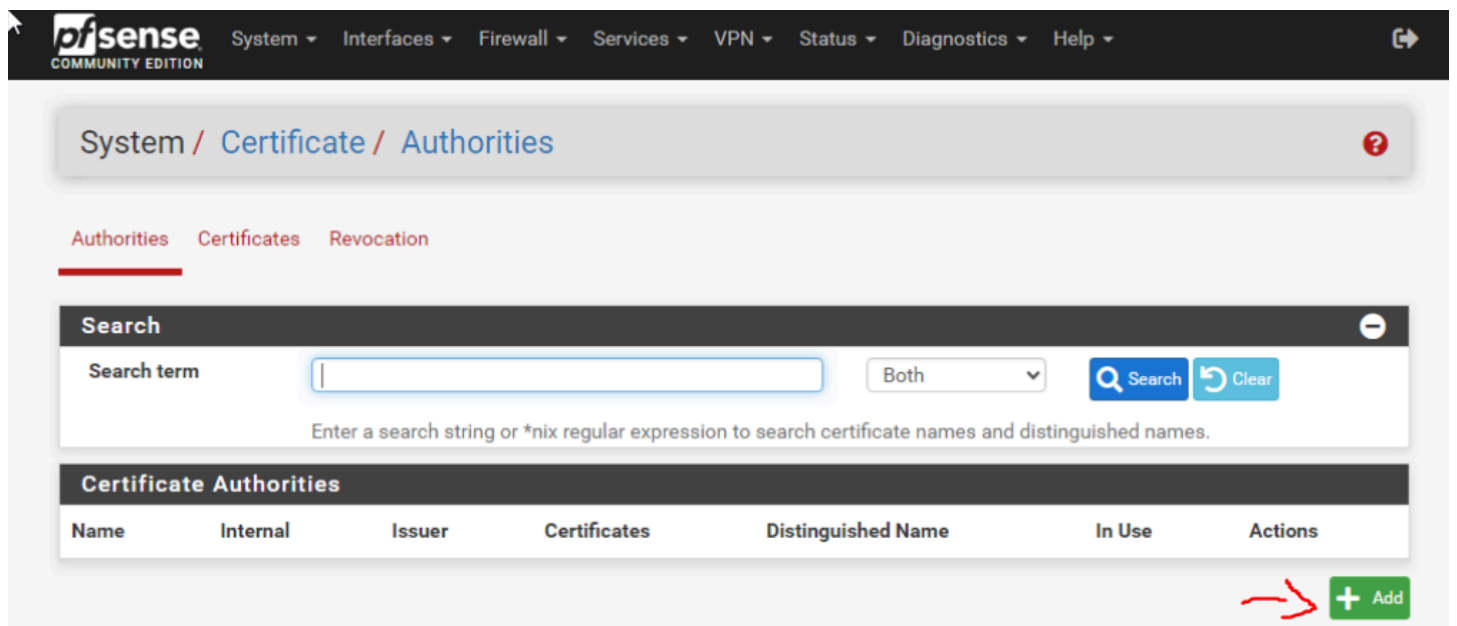
Créer l'autorité de certification

Pour créer l'autorité de certification sur pfSense vous devez accéder au menu :

System > Certificates / Cert Manager



Dans l'onglet "Authorities", cliquez sur le bouton "Add".



Create / Edit CA

Descriptive name

The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
 When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type

The length to use when generating a new RSA key, in bits.
 The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

Internal Certificate Authority

Key type

The length to use when generating a new RSA key, in bits.
 The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

The digest method used when the CA is signed.
 The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days)

Common Name

The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

| Name | Internal | Issuer | Certificates | Distinguished Name | In Use | Actions |
|--------------------|----------|-------------|--------------|--|--------|---------|
| SV-CONNECT-OPENVPN | ✓ | self-signed | 0 | CN=scivil.connect Valid From: Mon, 15 Apr 2024 13:12:17 +0200 Valid Until: Thu, 13 Apr 2034 13:12:17 +0200 | | |

Créer le certificat Serveur :

Authorities **Certificates** Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|-----------------|--|-----------------|---------|
| GUI default (661a44838b6fb) Server Certificate CA: No Server: Yes | self- signed | O=pfSense GUI default Self-Signed Certificate, CN=pfSense- 661a44838b6fb Valid From: Sat, 13 Apr 2024 10:38:27 +0200 Valid Until: Fri, 16 May 2025 10:38:27 +0200 | webConfigurator | |

Cliquer une nouvelle fois sur Add/Sign & Choisissez la méthode “**Create an Internal Certificate**” puisqu’il s’agit d’une création, donnez-lui un nom (VPN-SSL-REMOTE-ACCESS) et sélectionnez l’autorité de certification au niveau du paramètre “**Certificate authority**”.

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Internal Certificate

Certificate authority SV-CONNECT-OPENVPN

Key type RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256

Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le “Common Name” correspond là aussi au nom intégré dans le certificat, **si vous souhaitez établir une connexion VPN basée sur un nom de domaine**, il est préférable d’indiquer cette valeur ici.

Common Name

The following certificate subject components are optional and may be left blank.











Choisissez bien le **type de certificat (Certificate Type)** suivant : **Server Certificate**.

Certificate Type Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrict the signed certificate.

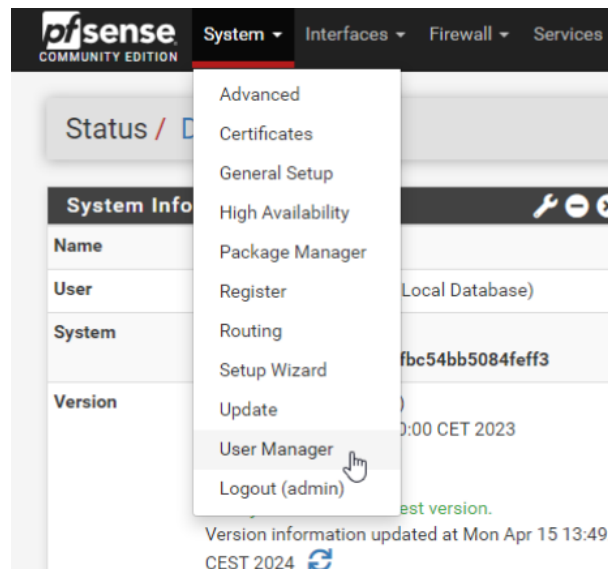



Il apparait bien dans la liste des certificats :


| Name | Issuer | Distinguished Name | In Use | Actions |
|---|--------------------|---|-----------------|---|
| GUI default (661a44838b6fb) Server Certificate CA: No Server: Yes | self-signed | O=pfSense GUI default Self-Signed Certificate, CN=pfSense-661a44838b6fb ⓘ Valid From: Sat, 13 Apr 2024 10:38:27 +0200 Valid Until: Fri, 16 May 2025 10:38:27 +0200 | webConfigurator |      |
| VPN-SSL-REMOTE-ACCESS Server Certificate CA: No Server: Yes | CA-CONNECT-OPENVPN | CN=scivil.local ⓘ Valid From: Mon, 15 Apr 2024 13:20:58 +0200 Valid Until: Thu, 13 Apr 2034 13:20:58 +0200 | |      |

Créer les utilisateurs locaux :

Je vais créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN.



| Users | | | | | |
|--------------------------------|----------------------|--------|--------|---|--|
| Username | Full name | Status | Groups | Actions | |
| <input type="checkbox"/> admin | System Administrator | ✓ | admins |  | |

[+ Add](#) 

User Properties

Defined by: USER

Disabled: This user cannot login

Username: vpn.scivil

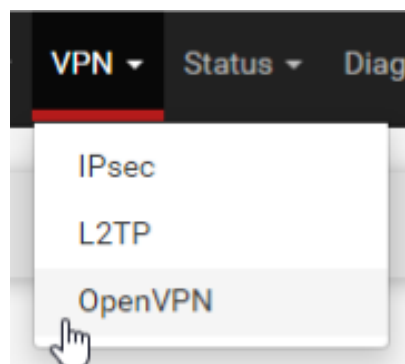
Password: [masked]

Certificate Click to create a user certificate

On peut sauvegarder et aller voir dans Certificates > Certificates que le certificat est apparu pour notre utilisateur :

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|-----------------------|---|-----------------|---------|
| GUI default (661a44838b6fb) Server Certificate CA: No Server: Yes | self-signed | O=pfSense GUI default Self-Signed Certificate, CN=pfSense-661a44838b6fb Valid From: Sat, 13 Apr 2024 10:38:27 +0200 Valid Until: Fri, 16 May 2025 10:38:27 +0200 | webConfigurator | |
| Certificat-OpenVpn Server Certificate CA: No Server: Yes | CA-SCIVIL- OPENVPN | ST=Alsace, O=SECURITE-CIVIL, L=Mulhouse, CN=scivil.local, C=FR Valid From: Mon, 15 Apr 2024 13:49:05 +0200 Valid Until: Thu, 13 Apr 2034 13:49:05 +0200 | | |
| Certificat-VPN-SCIVIL User Certificate CA: No Server: No | CA-SCIVIL- OPENVPN | ST=Alsace, O=SECURITE-CIVIL, L=Mulhouse, CN=vpn.scivil, C=FR Valid From: Mon, 15 Apr 2024 13:53:11 +0200 Valid Until: Thu, 13 Apr 2034 13:53:11 +0200 | User Cert | |

On va ensuite dans notre interface VPN



VPN / OpenVPN / Servers [Icons]

Servers Clients Client Specific Overrides Wizards

| OpenVPN Servers | | | | | |
|-----------------|-----------------|----------------|---------------|-------------|---------|
| Interface | Protocol / Port | Tunnel Network | Mode / Crypto | Description | Actions |

+ Add

VPN / OpenVPN / Servers / Edit [Icons]

Servers Clients Client Specific Overrides Wizards

General Information

Description
A description of this VPN for administrative reference.

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode Peer to Peer (SSL/TLS) ←

Device mode

- Peer to Peer (SSL/TLS)
- Peer to Peer (Shared Key)
- Remote Access (SSL/TLS)
- Remote Access (User Auth)
- Remote Access (SSL/TLS + User Auth)

most common and compatible mode across all platforms.

Endpoint Configuration

Protocol UDP on IPv4 only

On met notre certificat server :

Peer Certificate Revocation list

OCSP Check

Server certificate Certificat-OpenVpn (Server: Yes, CA: CA-SCIVIL-OPENV) ▾

==== Server Certificates ====

GUI default (661a44838b6fb) (Server: Yes, In Use)

Certificat-OpenVpn (Server: Yes, CA: CA-SCIVIL-OPENVPN)

==== Non-Server Certificates ====

Certificat-VPN-SCIVIL (Server: NO, CA: CA-SCIVIL-OPENVPN, In Use)

On choisit ensuite l'ip du tunnel VPN (Je prend un VLAN dans mon cas mais vous pouvez très bien mettre 10.10.10.0/24 par exemple) :

Tunnel Settings

IPv4 Tunnel
Network

This is the IPv4 virtual network or network type alias with a single entry used for server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The address is assigned to the server virtual interface. The remaining usable addresses will be

Je vous conseil d'activer cette option pour plus de facilité de connexion :

Client Settings

Dynamic IP

Allow connected clients to retain their connections if their IP address changes.

Advanced Client Settings

DNS Default Domain

Provide a default domain name to clients

DNS Default Domain

On peu ajouter les DNS de l'entreprise pour faire de la résolution

DNS Server enable

Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

DNS Server 2

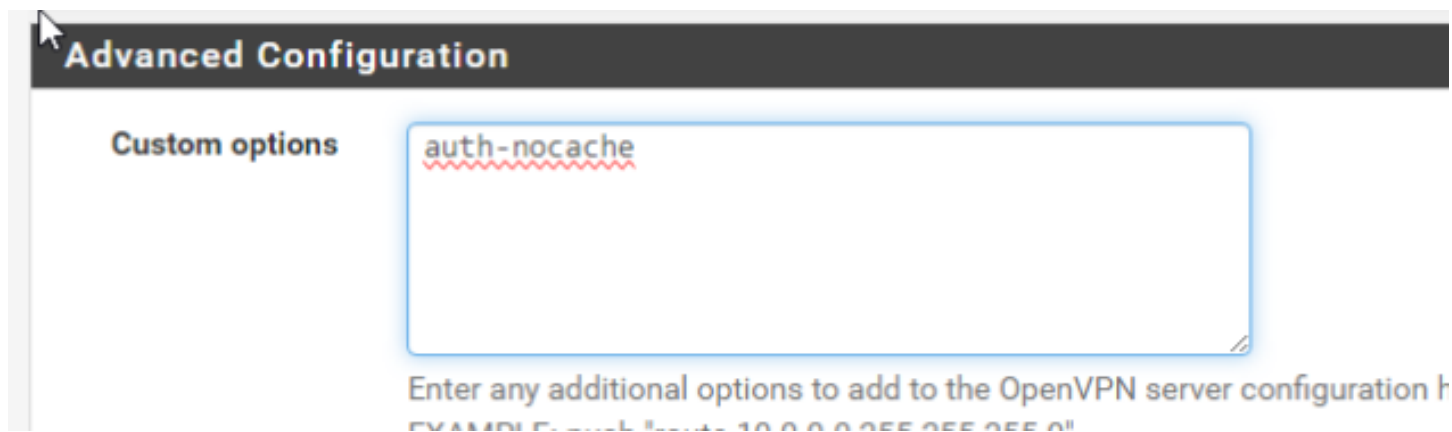
On active l'option en dessous pour que obliger le PC Client à se connecter via ses dns et non via le DNS local de notre utilisateur :

Block Outside DNS

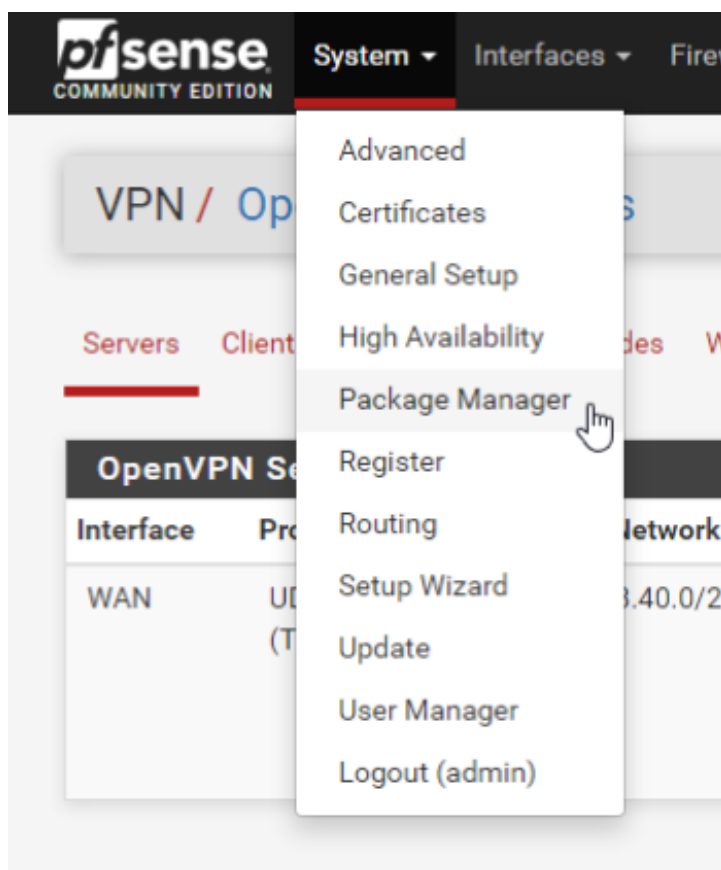
Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

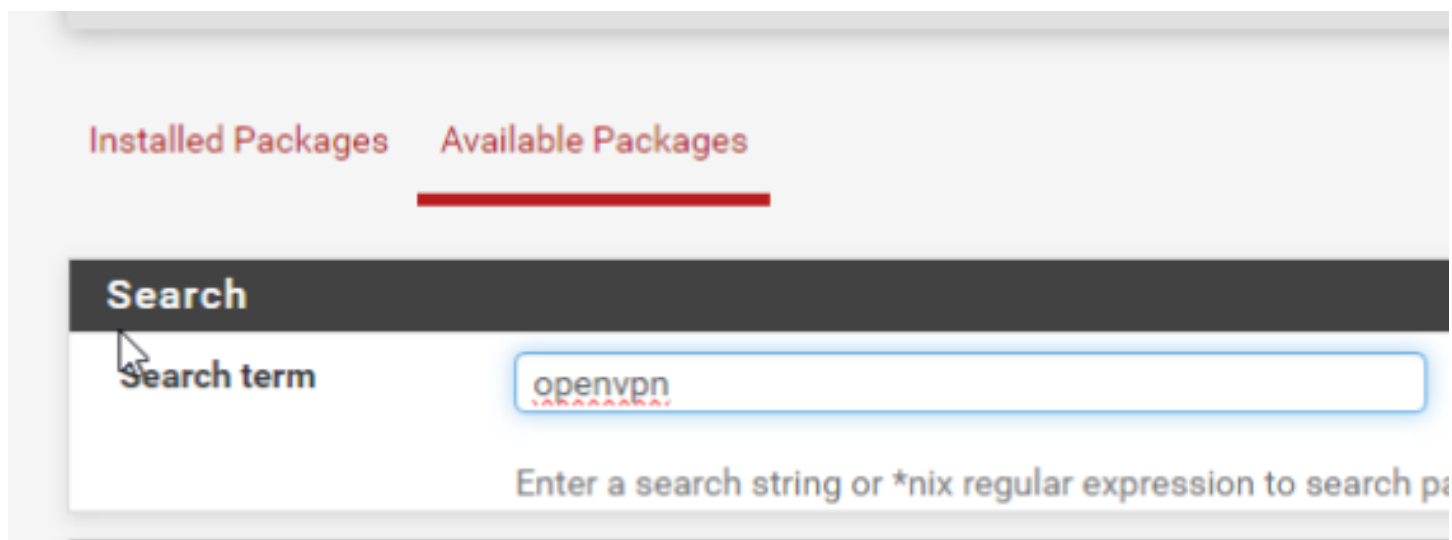
Si nous voulons une connexion plus sécurisé nous pouvons activer l'option ci-dessous afin de ne pas enregistrer les identifiants en cache :



Save et il faut se diriger ici :



On cherche les paquets Openvpn :







Installed Packages Available Packages

Search

Search term: Both

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

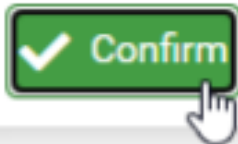
Packages

| Name | Version | Description | |
|-----------------------|---------|---|---|
| openvpn-client-export | 1.9.2 | Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01 |  |
| WireGuard | 0.2.1 | WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry. |  |

Activer Windows

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-op



System / Package Manager / Package Installer

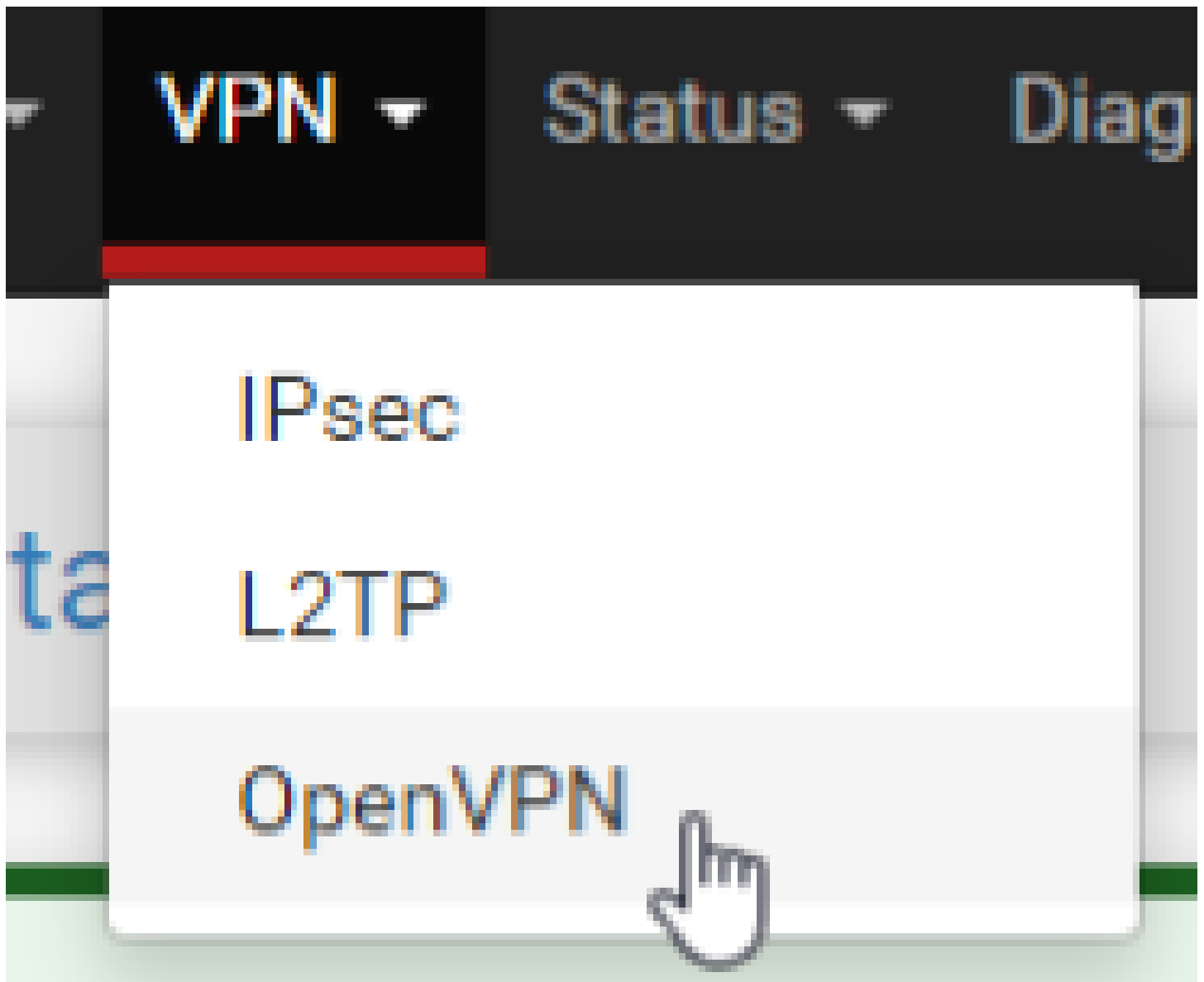
pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ..... done
Saving updated package information...
done.
```

Ok , on retourne dans la partie VPN :



Servers Clients Client Specific Overrides Wizards Client Export

| OpenVPN Servers | | | | | |
|-----------------|----------------------|-----------------|--|-------------|---------|
| Interface | Protocol / Port | Tunnel Network | Mode / Crypto | Description | Actions |
| WAN | UDP4 / 1194 (TUN) | 192.168.40.0/24 | Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-128-CBC Digest: SHA256 D-H Params: 2048 bits | | |

[+ Add](#)

Comme nous avons au préalable mis un nom de domaine , on choisit hostname dans la résolution du hostname :

OpenVPN Server

Remote Access Server

Client Connection Behavior

Host Name Resolution

Verify Server CN



Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers

Save as default

Pour installer la config :

OpenVPN Clients

| User | Certificate Name | Export |
|------------|-----------------------|--|
| vpn.scivil | Certificat-VPN-SCIVIL | <ul style="list-style-type: none">- Inline Configurations:<ul style="list-style-type: none"><input type="button" value="Most Clients"/><input type="button" value="Android"/><input type="button" value="OpenVPN Connect (iOS/Android)"/>- Bundled Configurations:<ul style="list-style-type: none"><input checked="" type="button" value="Archive"/><input type="button" value="Config File Only"/>- Current Windows Installers (2.6.7-1x001):<ul style="list-style-type: none"><input type="button" value="64-bit"/><input type="button" value="32-bit"/>- Previous Windows Installers (2.5.9-1x601):<ul style="list-style-type: none"><input type="button" value="64-bit"/><input type="button" value="32-bit"/>- Legacy Windows Installers (2.4.12-1x601):<ul style="list-style-type: none"><input type="button" value="10/2016/2019"/><input type="button" value="7/8/8.1/2012r2"/>- Viscosity (Mac OS X and Windows):<ul style="list-style-type: none"><input type="button" value="Viscosity Bundle"/><input type="button" value="Viscosity Inline Config"/> |

Only OpenVPN-compatible user certificates are shown



Pour installer directement l'exe :

- Current Windows Installers (2.6.7-1x001):

Maintenant il faut qu'on configure les règles du Pare-Feu pour les connexions VPN :








- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs


Floating **WAN** LAN CARP1 VLAN_ADMIN VLAN_SERVEURS VLAN_DMZ VLAN_VPN OpenVPN

Rules (Drag to Change Order)

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------|----------|--------|------|-------------|------|---------|-------|----------|-------------|---------|
|--------|----------|--------|------|-------------|------|---------|-------|----------|-------------|---------|

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

 Add  Add  Delete  Toggle  Copy  Save  Separator



pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

Source Invert match Any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match WAN address Destination Address /

Destination Port Range (other) 1194 (other) 1194
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Floating WAN LAN CARP1 VLAN_ADMIN VLAN_SERVEURS VLAN_DMZ VLAN_VPN OpenVPN

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------|----------------------|--------|------|----------------|-------------------|---------|-------|----------|--------------------------|---------|
| <input type="checkbox"/> | ✓ | 0/0 B IPv4 UDP | * | * | WAN address | 1194 (OpenVPN) | * | none | | Accès distant OpenVPN | |

↑ Add ↓ Add 🗑 Delete 🔄 Toggle 📄 Copy 💾 Save + Separator

Firewall **Services**

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Floating WAN LAN CARP1 VLAN_ADMIN VLAN_SERVEURS VLAN_DMZ VLAN_VPN OpenVPN

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--|--------|----------|--------|------|-------------|------|---------|-------|----------|-------------|---------|
| <p>No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.</p> | | | | | | | | | | | |

↑ Add ↓ Add 🗑 Delete 🔄 Toggle 📄 Copy 💾 Save + Separator

ici il faut déclarer les règles firewall pour l'accès au ressources internes de l'entreprise.

ici , les règles pour que any , les gens du wan peuvent se connecter au serveur e-brigade donc serveur WEB

Floating WAN LAN CARP1 VLAN_ADMIN VLAN_SERVEURS VLAN_DMZ VLAN_VPN **OpenVPN**

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------|----------|--------------|------|-------------|------------------|-------------|-------|----------|-------------|---------|
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 TCP/UDP | * | * | VLAN_DMZ address | 443 (HTTPS) | * | none | | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 TCP/UDP | * | * | VLAN_DMZ subnets | 80 (HTTP) | * | none | | |

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Sur le poste Client :

On se connecte à notre pfsense 192.168.2.1 et on exporte la config

Non sécurisé | https://192.168.2.1/vpn_openvpn_server.php

System Interfaces Firewall Services **VPN** Status Diagnostics Help

VPN / OpenVPN / Servers

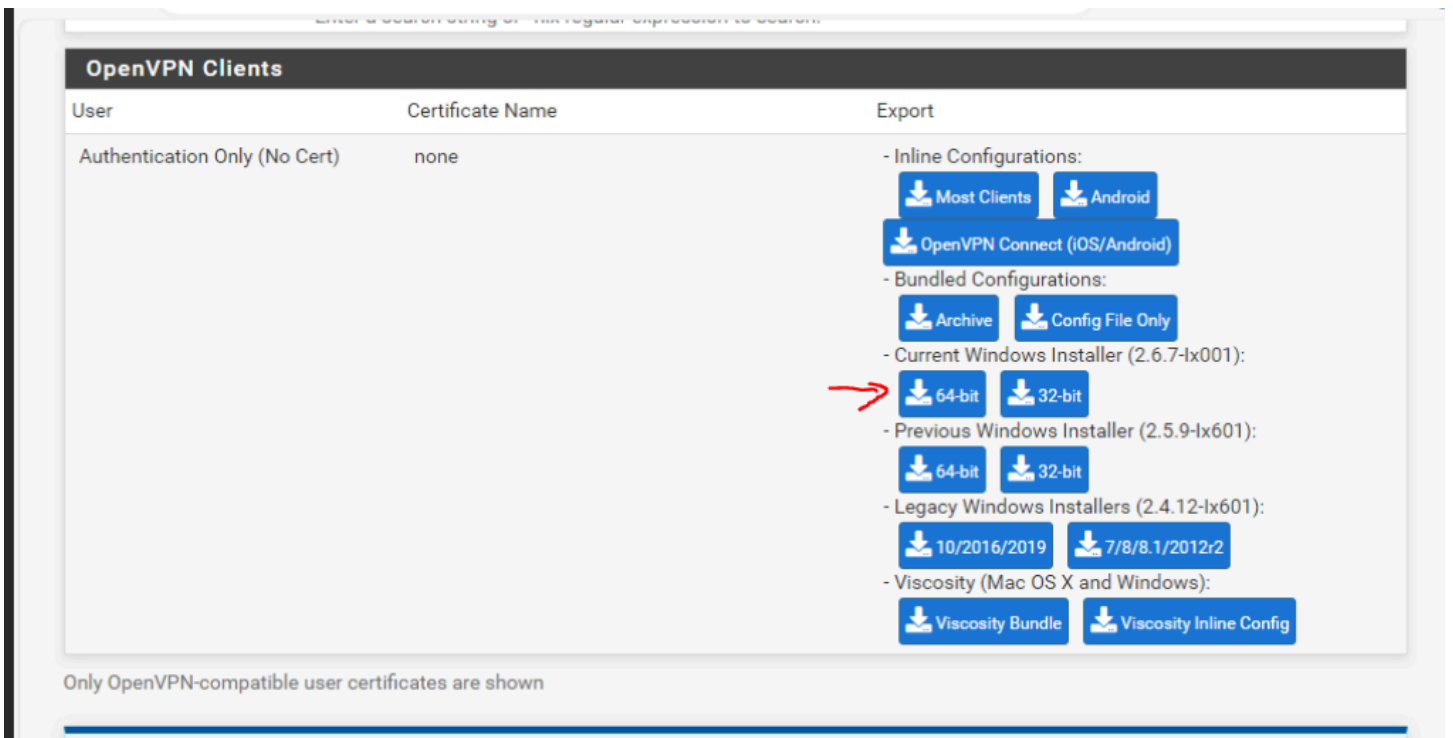
Servers Clients Client Specific Overrides Wizards Client Export

OpenVPN Servers

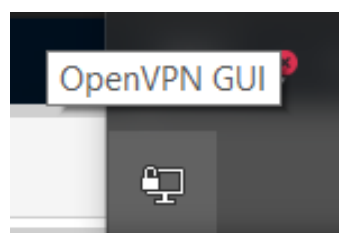
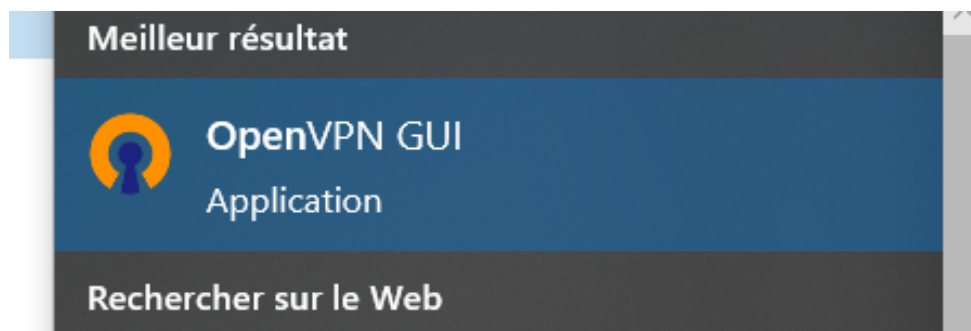
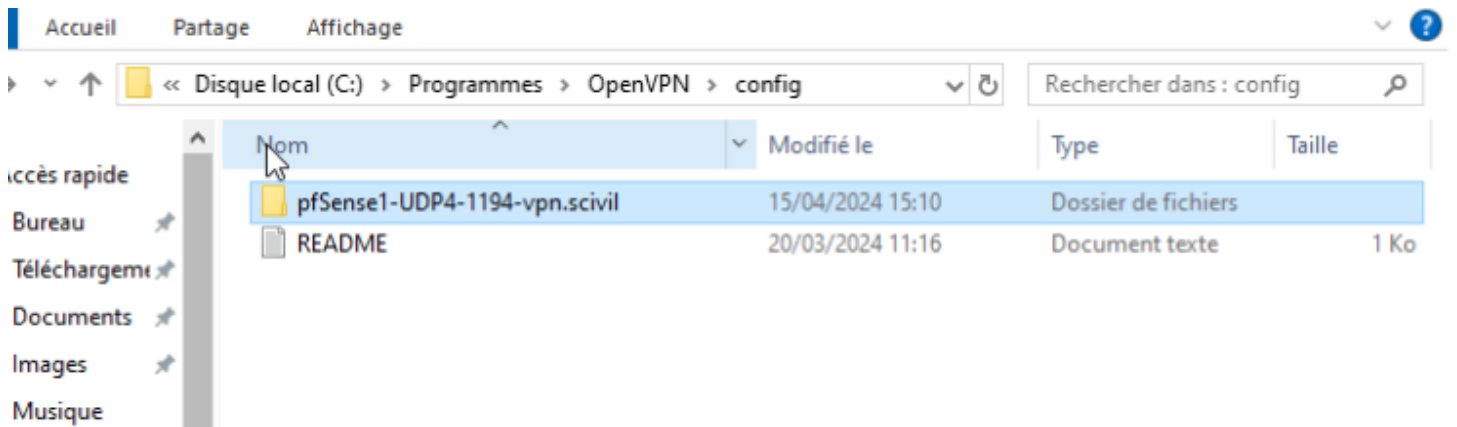
| Interface | Protocol / Port | Tunnel Network | Mode / Crypto | Description | Actions |
|-----------|--------------------|----------------|--|------------------------|---------|
| WAN | UDP4 / 12000 (TUN) | 10.0.8.0/24 | Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits | Accès distant OPEN VPN | |

+ Add

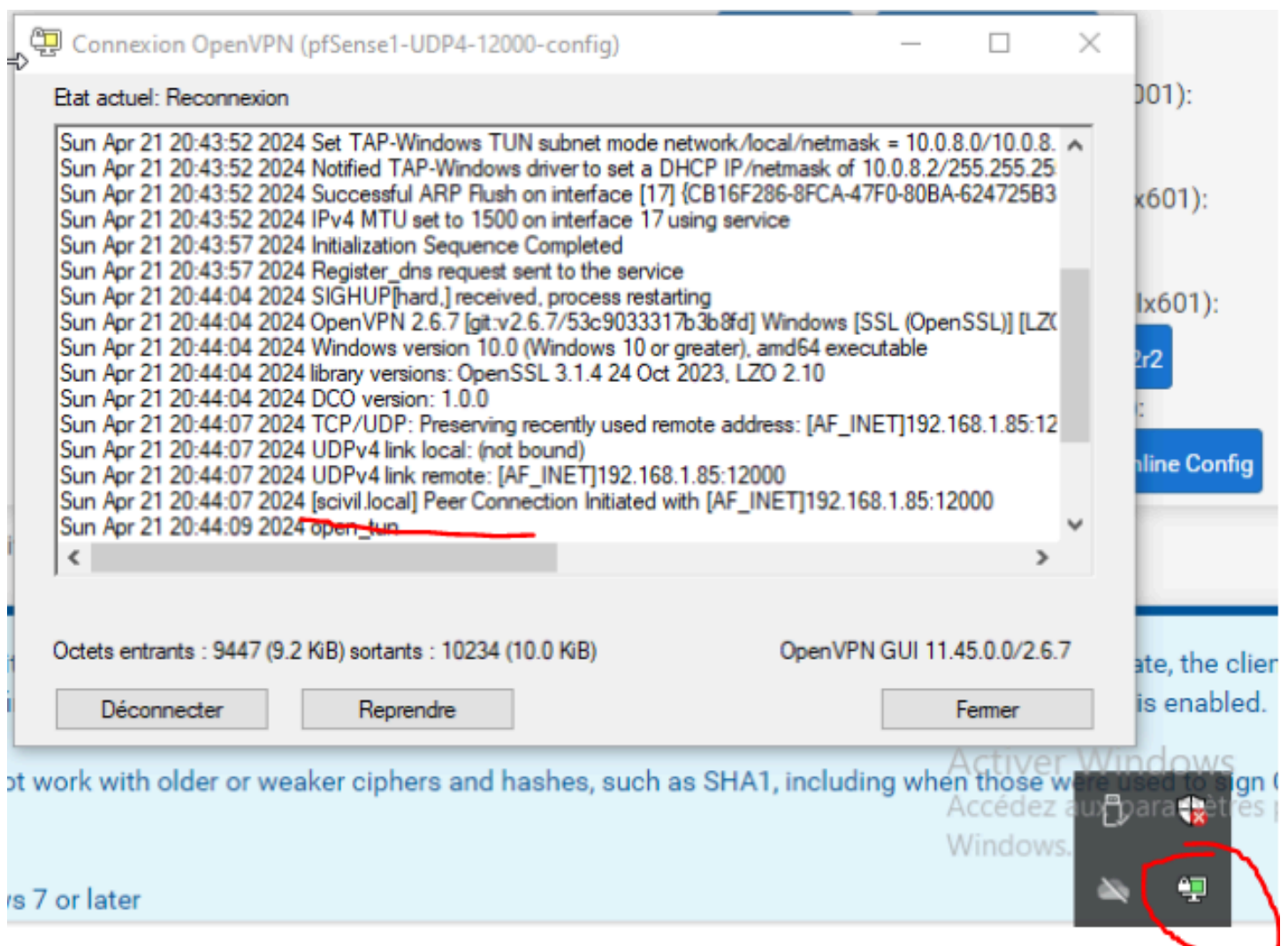
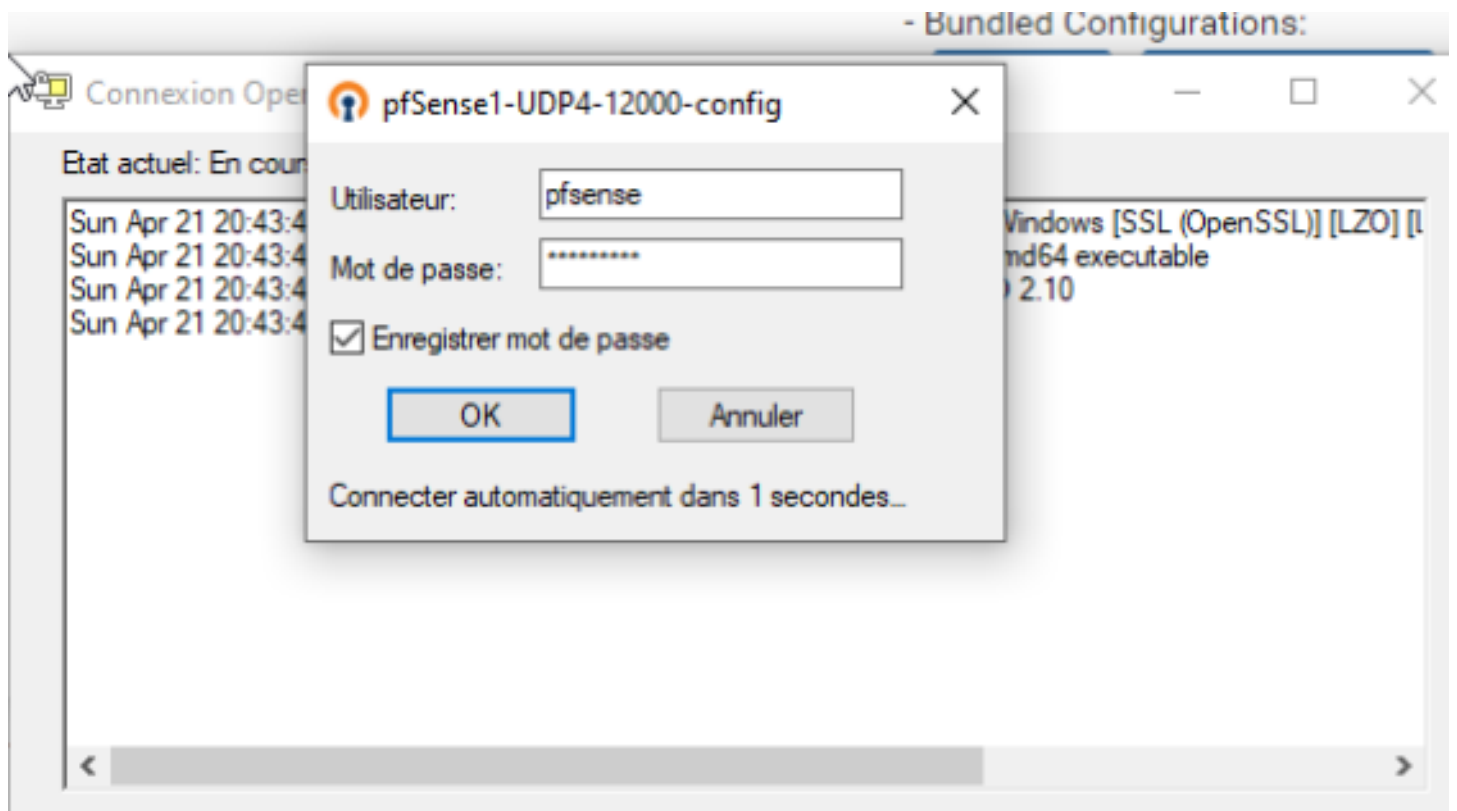
On descend plus bas dans Client Export pour retrouver :



On télécharge et on a juste a lancer l'installateur télécharger et cela installera Open VPN avec la configuration requise .



On fait cliquer droit > connecter , puis on rentre les identifiants



Mise en place du logiciel E-BRIGADE



eBrigade étant désormais en SaaS, on ne trouve plus de fichiers sources à jour. Il faut donc utiliser une ancienne version, qui ne supporte pas les dernières version PHP

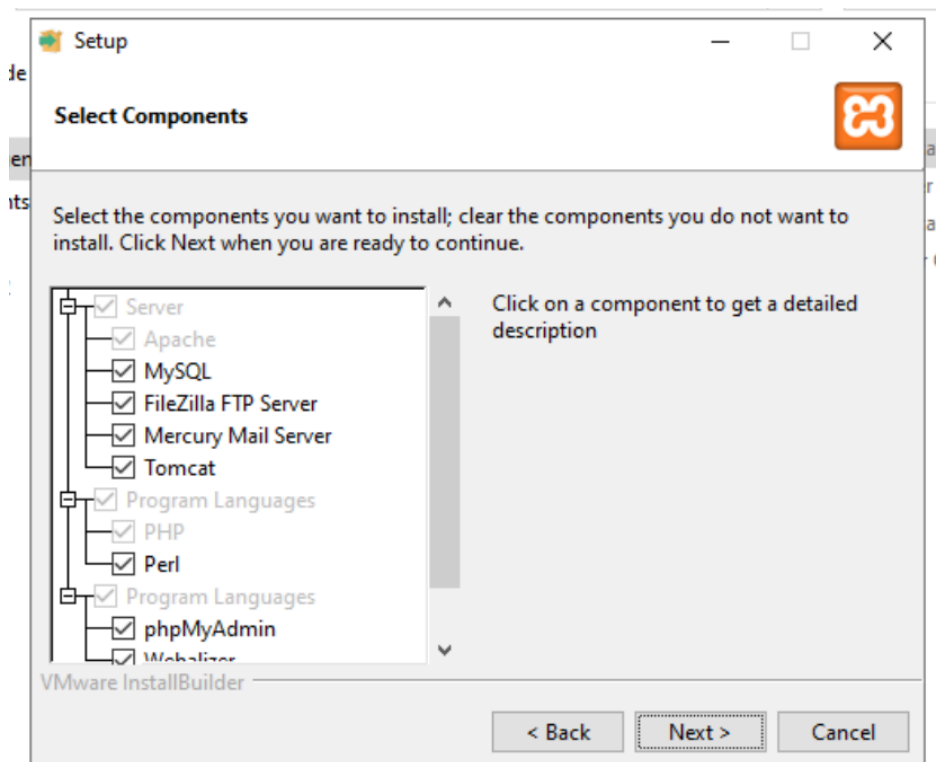
Dans notre installation, nous mettons directement eBrigade sur le Windows server à l'aide de xampp. Nous voulons donc installer une ancienne version de xampp avec nativement php 7

Nous mettrons l'application sur une base de données MySQL incluse avec xampp.

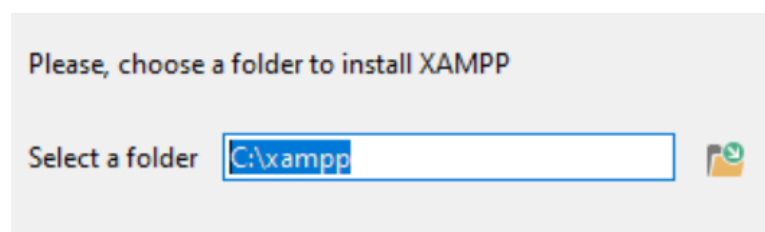
On télécharge xampp et eBrigade

- Lien de xampp:
<https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/7.4.33/>
 - On passe via sourceforge afin de pouvoir sélectionner une version antérieure de xampp
- Lien de eBridage : fourni par le formateur

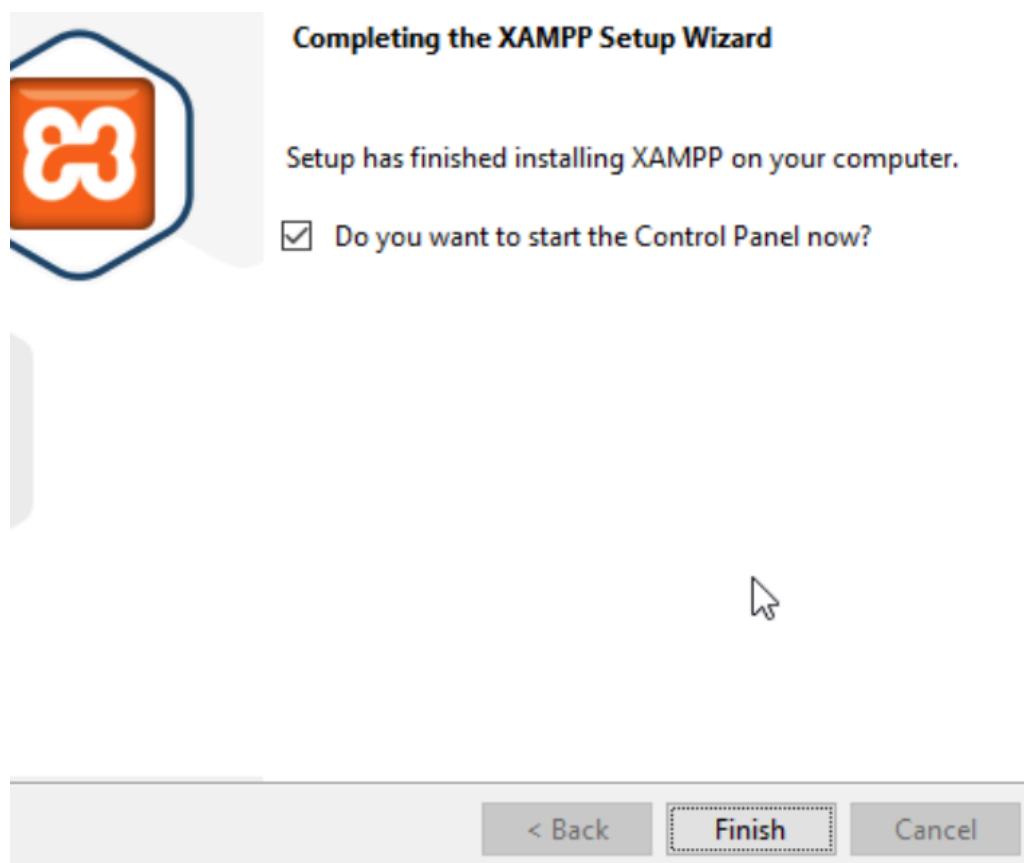
On exécute l'installateur xampp et on suit les étapes



On vérifie que tous les services que l'on souhaite sont installés.

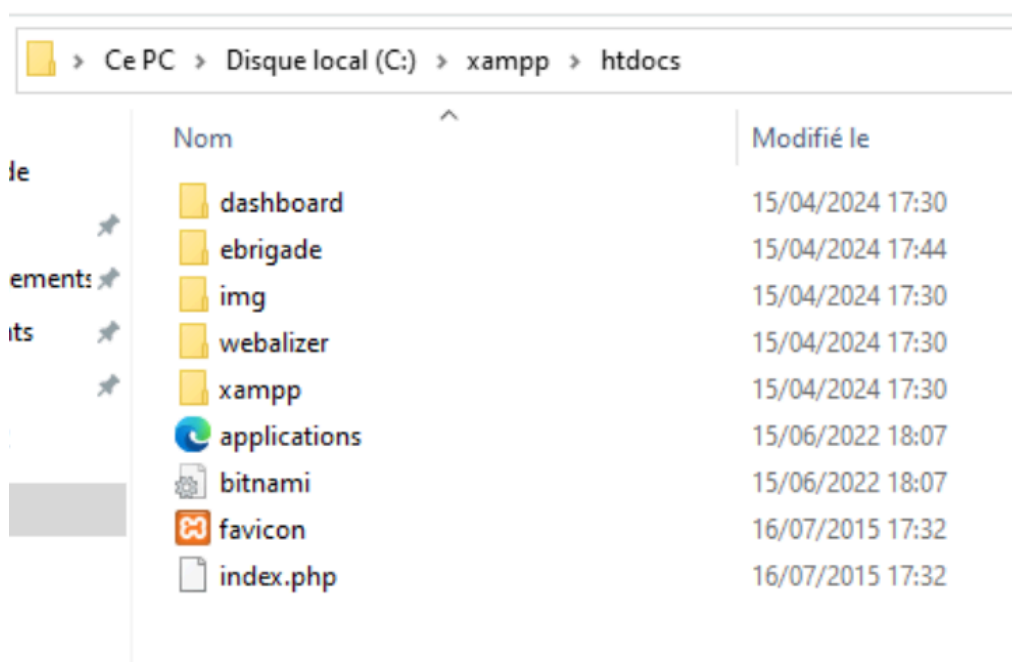


Si on a créé un second disque pour le service, on vient modifier le dossier d'installation



A la fin on lance directement l'application

On veut désormais importer eBrigade



Dans le dossier d'installation de xampp puis "htdocs" on vient glisser le dossier contenant les sources du logiciel.

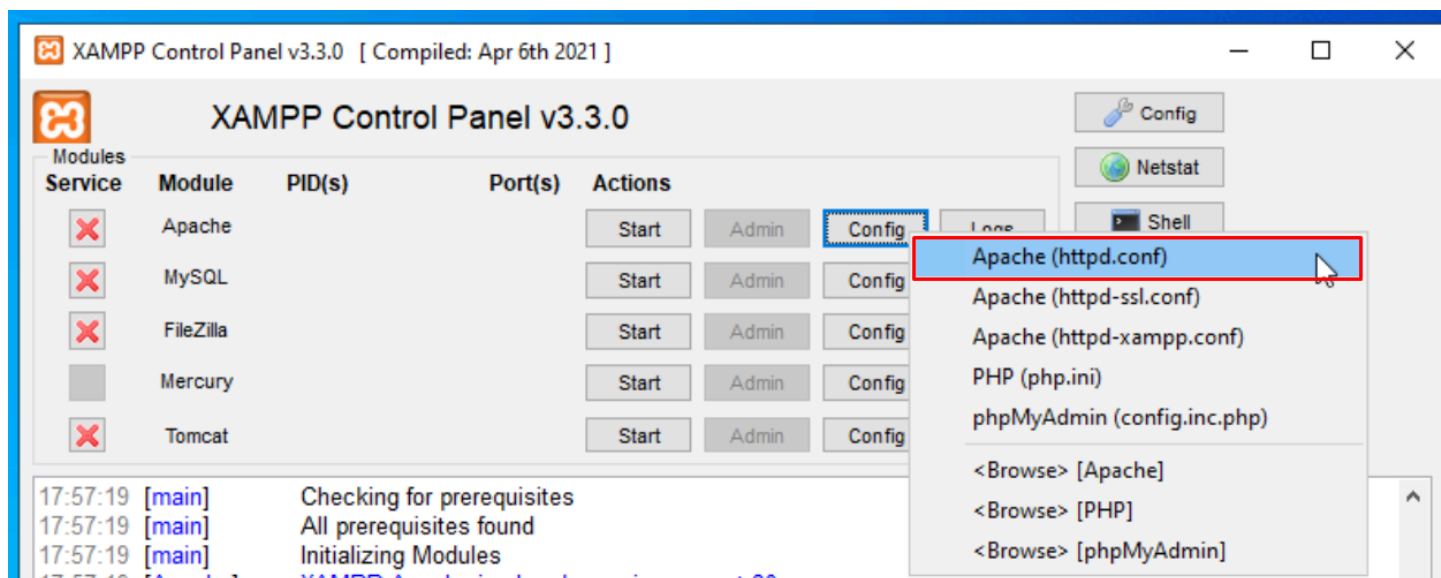
| Service | Module | PID(s) | Port(s) | Actions |
|-------------------------------------|-----------|--------|---------|-------------------------|
| <input checked="" type="checkbox"/> | Apache | | | Start Admin Config Logs |
| <input checked="" type="checkbox"/> | MySQL | | | Start Admin Config Logs |
| <input checked="" type="checkbox"/> | FileZilla | | | Start Admin Config Logs |
| <input type="checkbox"/> | Mercury | | | Start Admin Config Logs |
| <input checked="" type="checkbox"/> | Tomcat | | | Start Admin Config Logs |

```
17:43:22 [main] Initializing Control Panel
17:43:22 [main] Windows Version: 64-bit
17:43:22 [main] XAMPP Version: 7.4.33
17:43:22 [main] Control Panel Version: 3.3.0 [ Compiled: Apr 6th 2021 ]
17:43:22 [main] Running with Administrator rights - good!
17:43:22 [main] XAMPP Installation Directory: "c:\xampp\"
17:43:22 [main] Checking for prerequisites
17:43:24 [main] All prerequisites found
17:43:24 [main] Initializing Modules
17:43:24 [main] Starting Check-Timer
17:43:24 [main] Control Panel Ready
```

On peut désormais lancer Xampp et vérifier la version de PHP.

Modifier l'IP utilisée

Dans notre AP, nous voulons mettre eBrigade dans une DMZ afin de gérer les droits d'accès. Pour cela nous allons modifier la configuration d'Apache et de MySQL afin de les changer de vLAN et ne pas prendre l'ip par défaut du serveur Windows.

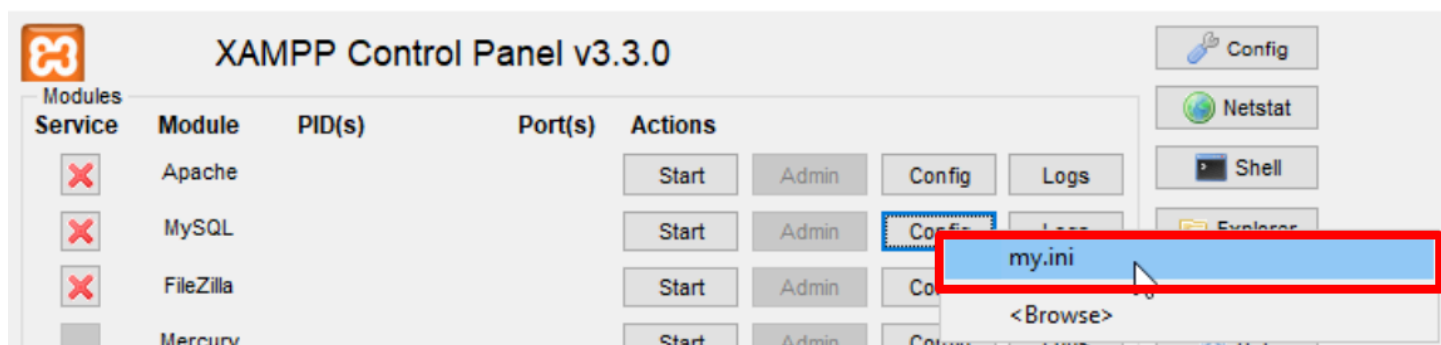


Dans xampp nous pouvons éditer cela via “config” puis “httpd.conf”

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
Listen 192.168.40.2:80
#Listen 80
```

Voici la ligne concernée, il suffit de retirer le # devant afin d’activer l’option, et de mettre l’IP de notre vLAN puis d’enregistrer. On peut également modifier le port, mais ici on laisse le port HTTP par défaut (80)

Nous venons faire la même chose pour le MySQL, puisqu’il doit lui aussi être sur le même vLAN



Dans xampp nous pouvons éditer cela via “config” puis “my.ini”

```
# Change here for bind listening  
bind-address="192.168.40.2"  
# bind-address = ::1 # for ipv6
```

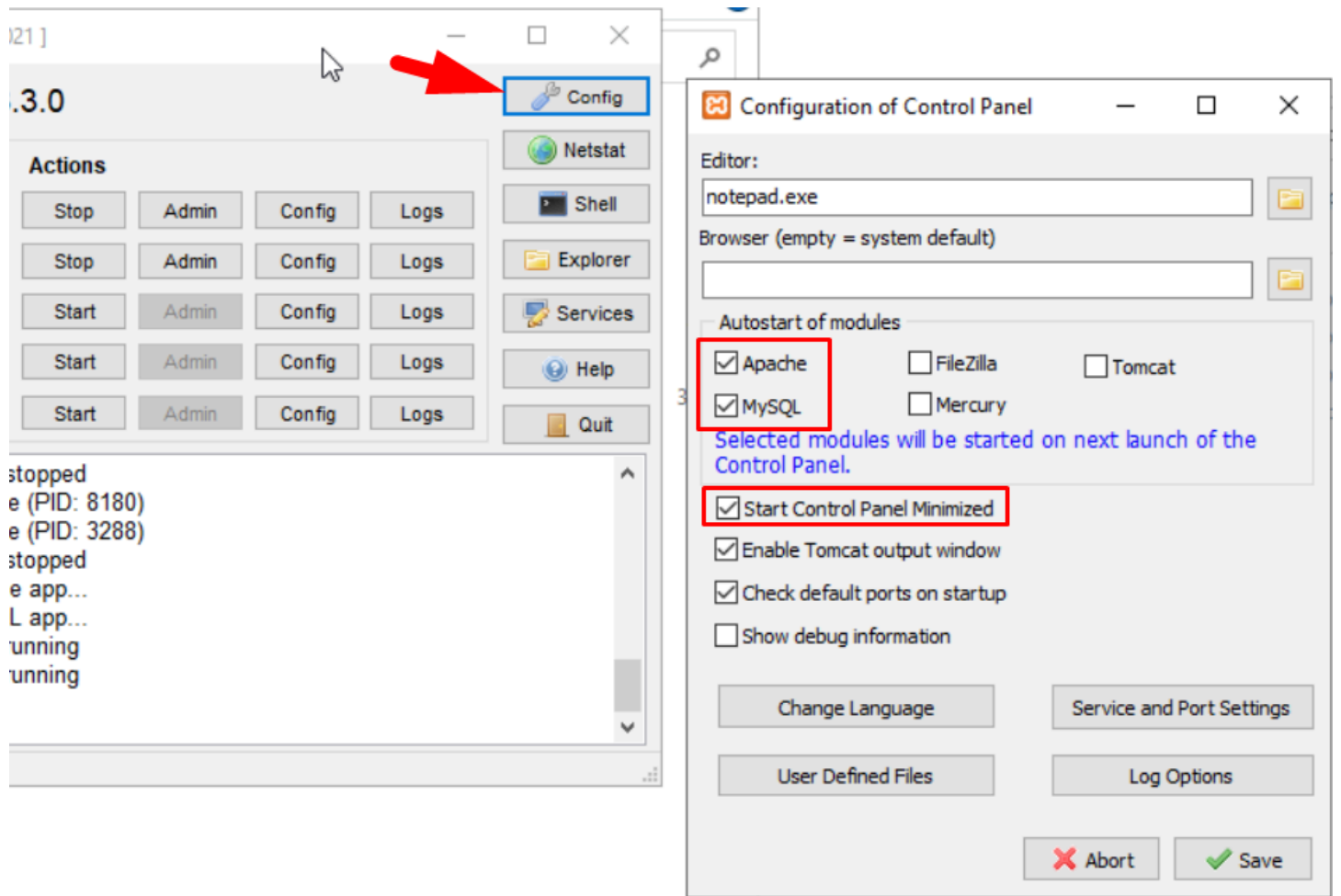
Voici la ligne concernée, il suffit de retirer le # devant afin d'activer l'option, et de mettre l'IP de notre vLAN puis d'enregistrer.

| Modules | | | | |
|-------------------------------------|--------|--------------|---------|---------|
| Service | Module | PID(s) | Port(s) | Actions |
| <input checked="" type="checkbox"/> | Apache | 3512 2116 | 80, 443 | Stop |
| <input checked="" type="checkbox"/> | MySQL | 580 | 3306 | Stop |

Tout est bon, on peut lancer le module Apache et MySQL

Lancer xampp dès le lancement du serveur

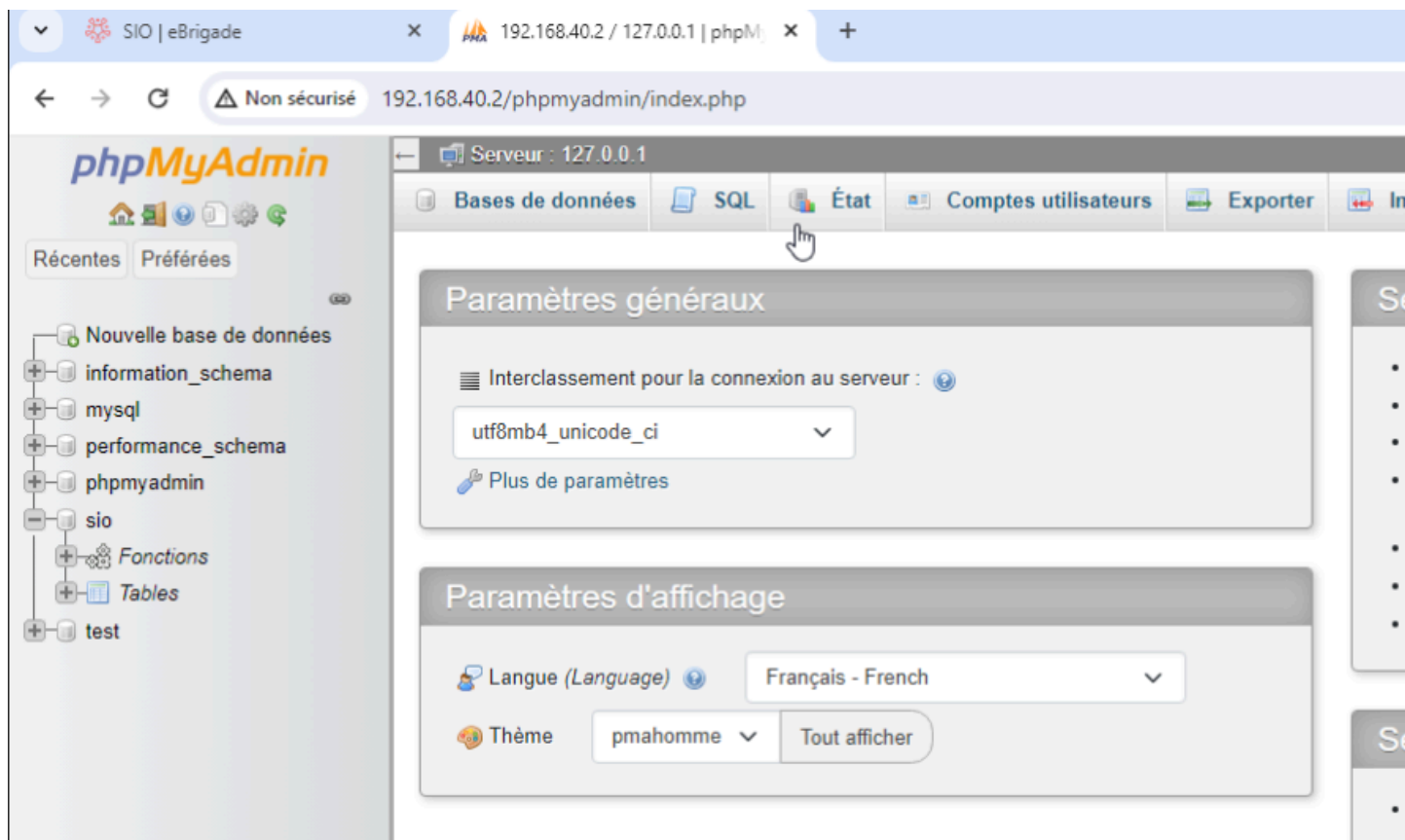
Par défaut, xampp ne se lancera pas au démarrage de la machine, nous venons donc régler ce soucis



Nous allons dans config puis cochons les options Apache/MySQL

Créer la base de données

Pour se faire, nous nous connectons au site de phpmyadmin, qui est donc l'IP de notre vLAN, pour nous c'est 192.168.40.2/phpmyadmin



Page d'accueil de phpmyadmin

← → ↻ Non sécurisé 192.168.40.2/phpmyadmin/index.php?route=/server/privileges&viewing_m...

phpMyAdmin

Recentes Préférées

Nouvelle base de données
+ information_schema
+ mysql
+ performance_schema
+ phpmyadmin
- sio
 + Fonctions
 + Tables
+ test

Serveur : 127.0.0.1

Bases de données SQL État Comptes utilisateur

| | Nom d'utilisateur | Nom d'hôte | Mot de passe | Privilèges globaux |
|--------------------------|-------------------|------------|--------------|--------------------|
| <input type="checkbox"/> | N'importe quel | % | Non | USAGE |
| <input type="checkbox"/> | pma | localhost | Non | USAGE |
| <input type="checkbox"/> | root | % | Non | ALL PRIVILEGES |
| <input type="checkbox"/> | root | 127.0.0.1 | Non | ALL PRIVILEGES |
| <input type="checkbox"/> | root | ::1 | Non | ALL PRIVILEGES |
| <input type="checkbox"/> | root | localhost | Non | ALL PRIVILEGES |
| <input type="checkbox"/> | sio | % | Oui | ALL PRIVILEGES |

↑ Tout cocher Avec la sélection : Exporter

Nouvel utilisateur

Révoquer tous les privilèges actifs de ces utilisateurs, puis effacer les utili

On va dans comptes utilisateurs puis "ajouter un compte utilisateur"

The image shows a web form for creating a user. The fields are as follows:

- Nom d'utilisateur : Saisir une valeur (dropdown) | ebrigade (text input)
- Nom d'hôte : Tout hôte (dropdown) | % (text input)
- Mot de passe : Saisir une valeur (dropdown) | (password input) | Force : [Progress bar] Bon
- Saisir à nouveau : (password input)
- Extension d'authentification : Authentification MySQL native (dropdown)
- Générer un mot de passe: [Générer] (button) | [Empty text input]

Below the form, there is a section titled "Base de données pour ce compte d'utilisateur" with two options:

- Créer une base portant son nom et donner à cet utilisateur tous les privilèges sur cette base. (This option is highlighted with a red box in the image)
- Accorder tous les privilèges à un nom passe-partout (utilisateur_%).

On précise bien qu'on autorise l'accès depuis tout hôte pour ne pas avoir de soucis en connexion externe. Puis on vient créé une table au même nom que l'utilisateur

Configurer eBrigade

On peut désormais commencer la configuration de eBrigade en se rendant sur l'url du dossier, pour nous : 192.168.40.2/ebrigade



Configuration Base de données

Paramètres de connexion à la base de données

Server Name ⓘ 192.168.40.2

User ⓘ sio

Password ⓘ

Database name ⓘ sio

Valider



On vient compléter les nom du serveur qui sera l'IP de la base de donnée, ainsi que le nom d'utilisateur et le mot de passe créé précédemment


 **initialisation réussie**

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](#)

Pas d'embuche, l'installation est correcte

Modifier le mot de passe pour Admin ADMIN

Veuillez choisir un mot de passe personnel.

Nouveau mot de passe

Confirmation

Bon Mot de passe!

Sauvegarder

On rentre le mot de passe du compte d'administration, on ne met pas le même mot que la base de donnée pour éviter les risques.

Configuration eBrigade

Type d'organisation *
Service d'incendie et Secours

Nom court de votre organisation *
SIO

Nom long de votre organisation *
SIO

Adresse Web *
http://192.168.40.2

Votre adresse email *
mimile5252@gmail.com

Nom personnalisé de l'application *
eBrigade

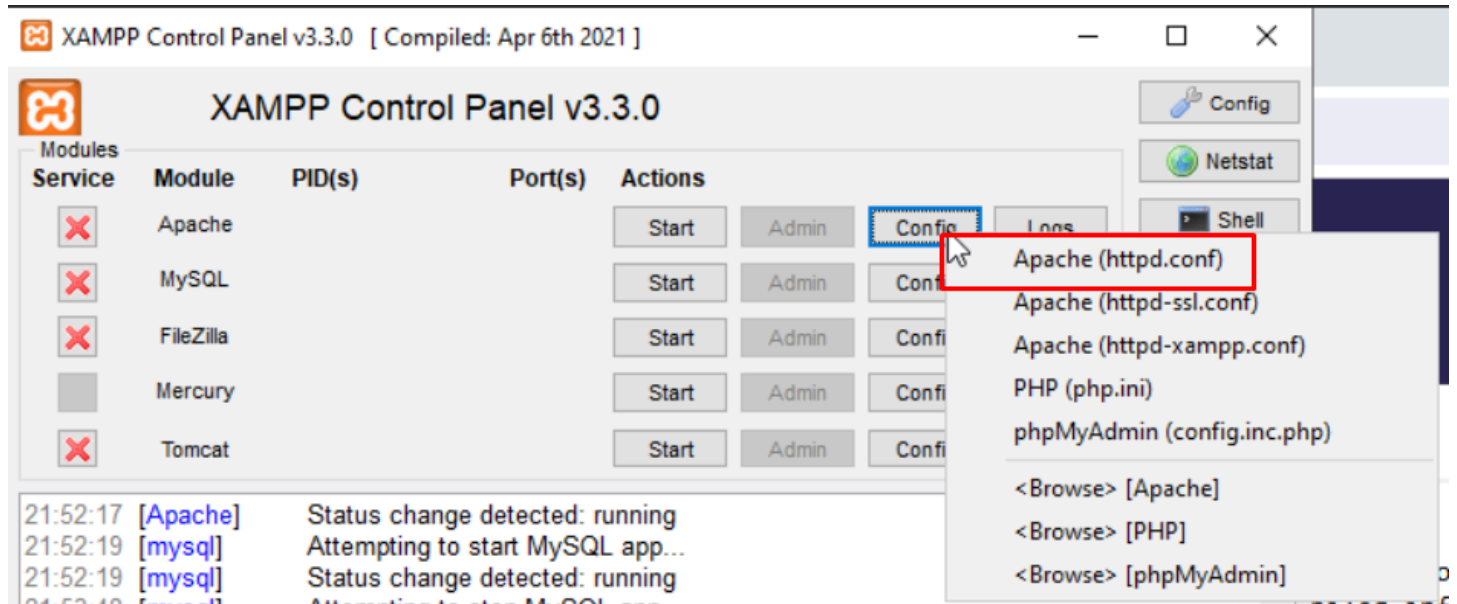
Valider

Et la dernière étape on remplit les informations sur l'organisation.

Rendre le site accessible depuis l'extérieur

Par défaut le xampp n'est accessible qu'en localhost, donc les autres postes que le notre ne peuvent pas y accéder. Dans le cadre de notre AP tous les postes doivent pouvoir y accéder, puis on restreindra avec le VLAN.

Pour se faire on va modifier la config apache pour modifier l'accès à ce dossier

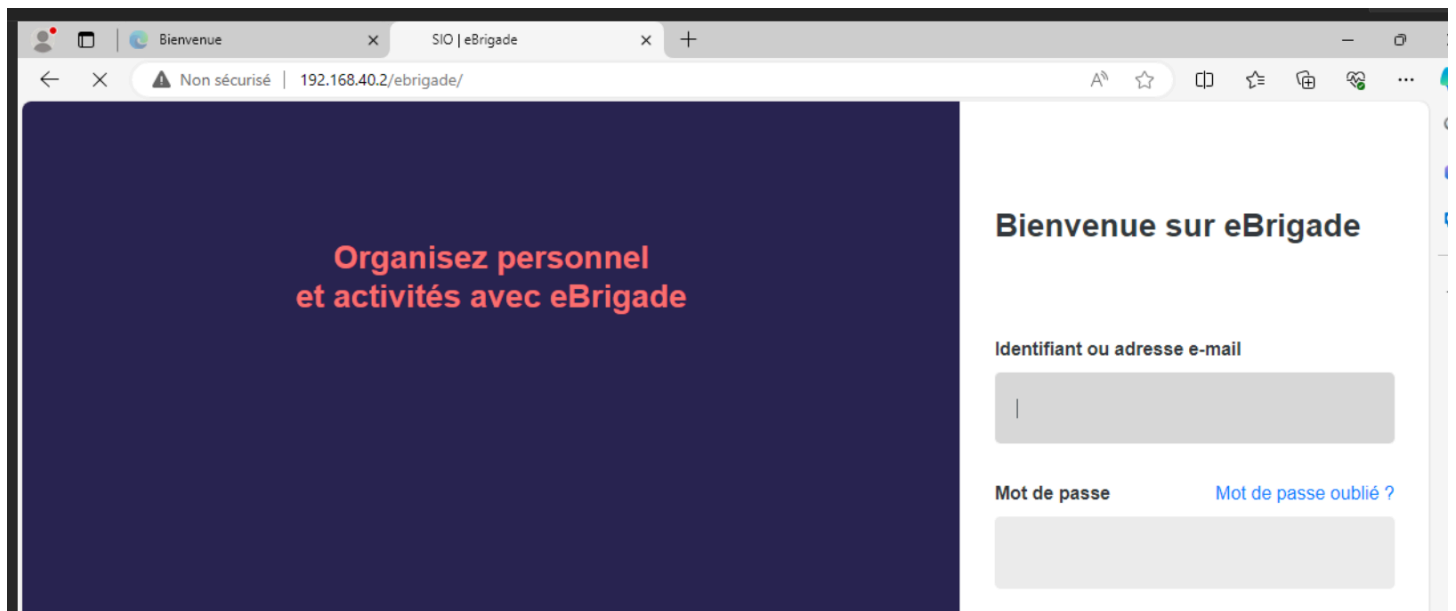


On retourne dans la configuration de Apache

```
<Directory "C:/xampp/htdocs/ebrigade">  
Options Indexes FollowSymLinks  
AllowOverride All  
Require all granted  
</Directory>
```

Chercher la ligne <Directory> et modifier comme ceci, cela donnera tous les droits d'accès depuis l'extérieur mais pour ebrigade uniquement.

Nous nous connectons ensuite sur un poste client, et nous avons bien accès à eBrigade :



Installation du Serveur de Messagerie Zimbra



1. Préparation du serveur :

- Installation de l'OS et configuration de l'adresse IP statique. (Ubuntu 20.04 ici)
- Mise à jour des systèmes et installation des dépendances nécessaires.

2. Installation de Zimbra :

- Téléchargement et installation de Zimbra Collaboration Suite.
- Configuration des services de messagerie pour synchronisation avec l'ad
- DNS Dans l'ad

ZIMBRA (mail) :

Pour installer Zimbra Collaboration Suite sur votre système Ubuntu (20.04 ici car pour l'open source prend en charge que cette version au maximum) , tout en intégrant votre domaine Active Directory , suivez ces étapes détaillées, en ajustant les configurations pour s'adapter à votre réseau / VLAN et à l'adresse IP de votre VM Zimbra dans le domaine (ici scivil.local) :

ATTENTION : Ne pas crée d'utilisateur ou ne donner pas le nom de la vm " ZIMBRA " car lors de l'installation , Zimbra crée cette utilisateur automatiquement pour lui.

Préparation initiale du serveur

1 - Connexion en tant que superutilisateur :

sudo su

2 - Mise à jour du système

apt update && apt upgrade -y

```
root@zimbra:~# apt update && apt upgrade -y
Atteint :1 http://security.ubuntu.com/ubuntu focal-security InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu focal InRelease
Atteint :3 http://fr.archive.ubuntu.com/ubuntu focal-updates InRelease
Atteint :4 http://fr.archive.ubuntu.com/ubuntu focal-backports InRelease
```

3 - Configuration du nom d'hôte :

hostnamectl set-hostname mail.scivil.local

```
root@zimbra:~# hostnamectl set-hostname mail.scivil.local
root@zimbra:~#
```

4 - Edition du fichier hosts :

Ouvrez le fichier /etc/hosts avec un éditeur de texte comme nano : **nano /etc/hosts**

```
GNU nano 4.8 /etc/hosts
127.0.0.1    localhost
127.0.1.1    zimbra
# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

→ on ajoute 192.168.20.3 mail.scivil.local mail

```
GNU nano 4.8 /etc/hosts
127.0.0.1    localhost
127.0.1.1    zimbra
192.168.20.3 mail.scivil.local mail
# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
```

On CTRL + X et O et entrer pour enregistré .

5 - Configuration DNS avec Dnsmasq

Installation de Dnsmasq :


```
systemctl disable systemd-resolved
```

```
systemctl stop systemd-resolved
```

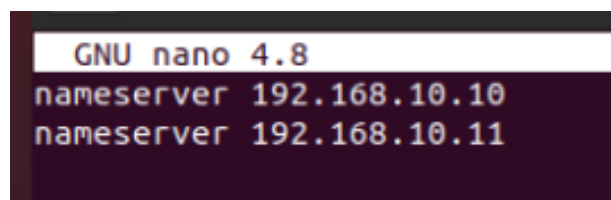
```
rm -f /etc/resolv.conf
```

```
nano /etc/resolv.conf
```

Dans le fichier resolv.conf, ajoutez :

```
nameserver 192.168.10.10
```

```
nameserver 192.168.10.11
```



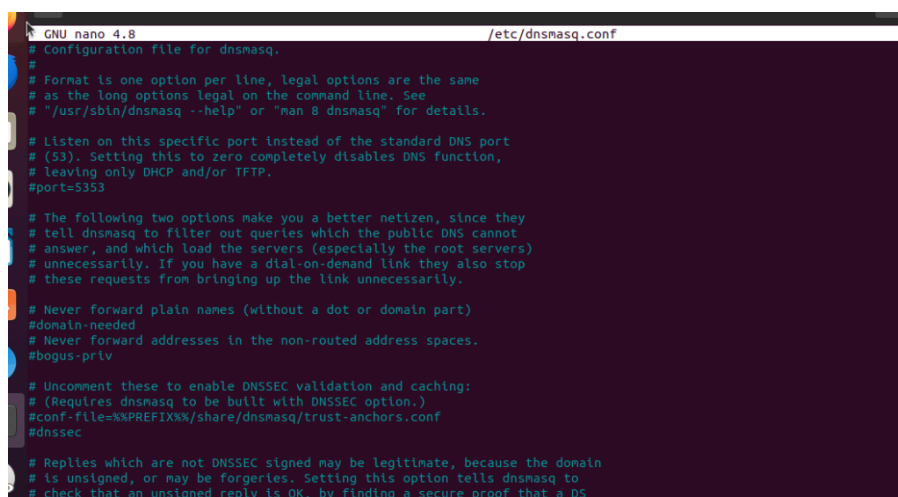
```
GNU nano 4.8
nameserver 192.168.10.10
nameserver 192.168.10.11
```

6 - Installation et configuration de Dnsmasq :

```
apt install dnsmasq -y
```

```
cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bak
```

```
nano /etc/dnsmasq.conf
```



```
GNU nano 4.8 /etc/dnsmasq.conf
# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.
#
# Listen on this specific port instead of the standard DNS port
# (53). Setting this to zero completely disables DNS function,
# leaving only DHCP and/or TFTP.
#port=5353
#
# The following two options make you a better netizen, since they
# tell dnsmasq to filter out queries which the public DNS cannot
# answer, and which load the servers (especially the root servers)
# unnecessarily. If you have a dial-on-demand link they also stop
# these requests from bringing up the link unnecessarily.
#domain-needed
# Never forward addresses in the non-routed address spaces.
#bogus-priv
#
# Uncomment these to enable DNSSEC validation and caching:
# (Requires dnsmasq to be built with DNSSEC option.)
#conf-file=%PREFIX%/share/dnsmasq/trust-anchors.conf
#dnssec
#
# Replies which are not DNSSEC signed may be legitimate, because the domain
# is unsigned, or may be forgeries. Setting this option tells dnsmasq to
# check that an unsigned reply is OK, by finding a secure proof that a DS
```

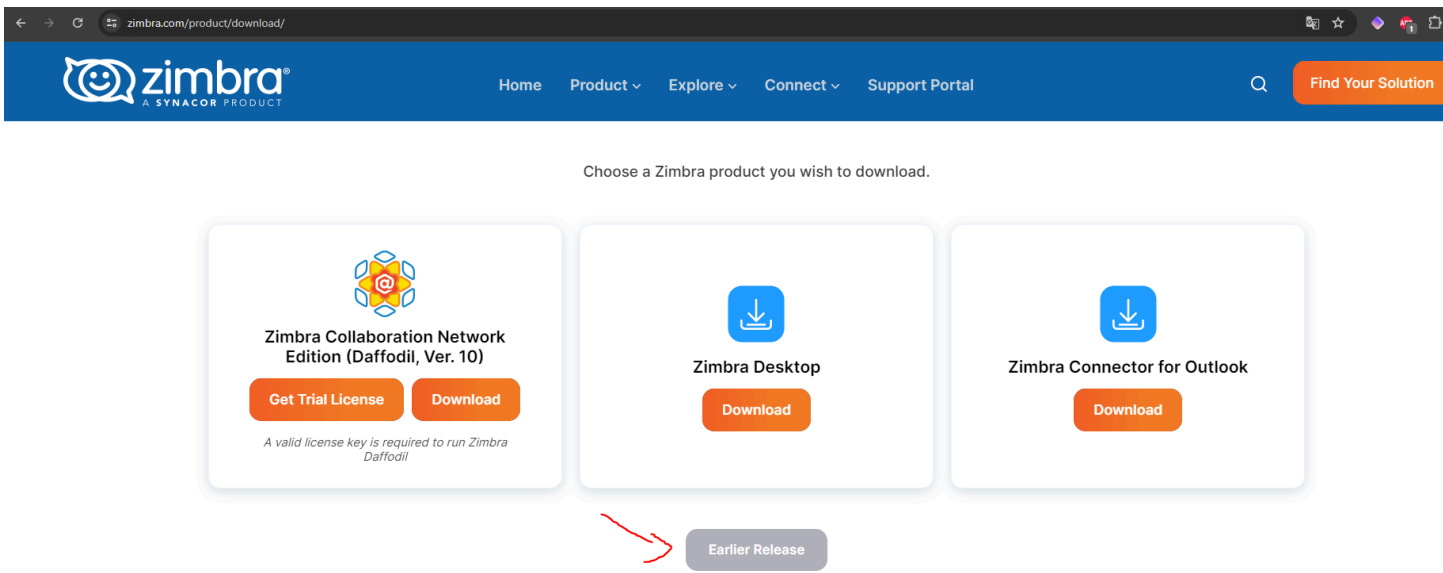
Ajoutez à la fin du fichier :

```
# If a DHCP client claims that its name is "wpad", ignore that.
# This fixes a security hole. see CERT Vulnerability VU#598349
#dhcp-name-match=set:wpad-ignore,wpad
#dhcp-ignore-names=tag:wpad-ignore
server=192.168.10.10
domain=scivil.local
mx-host=scivil.local, mail.scivil.local, 5
mx-host=mail.scivil.local, mail.scivil.local, 5
listen-address=127.0.0.1
```

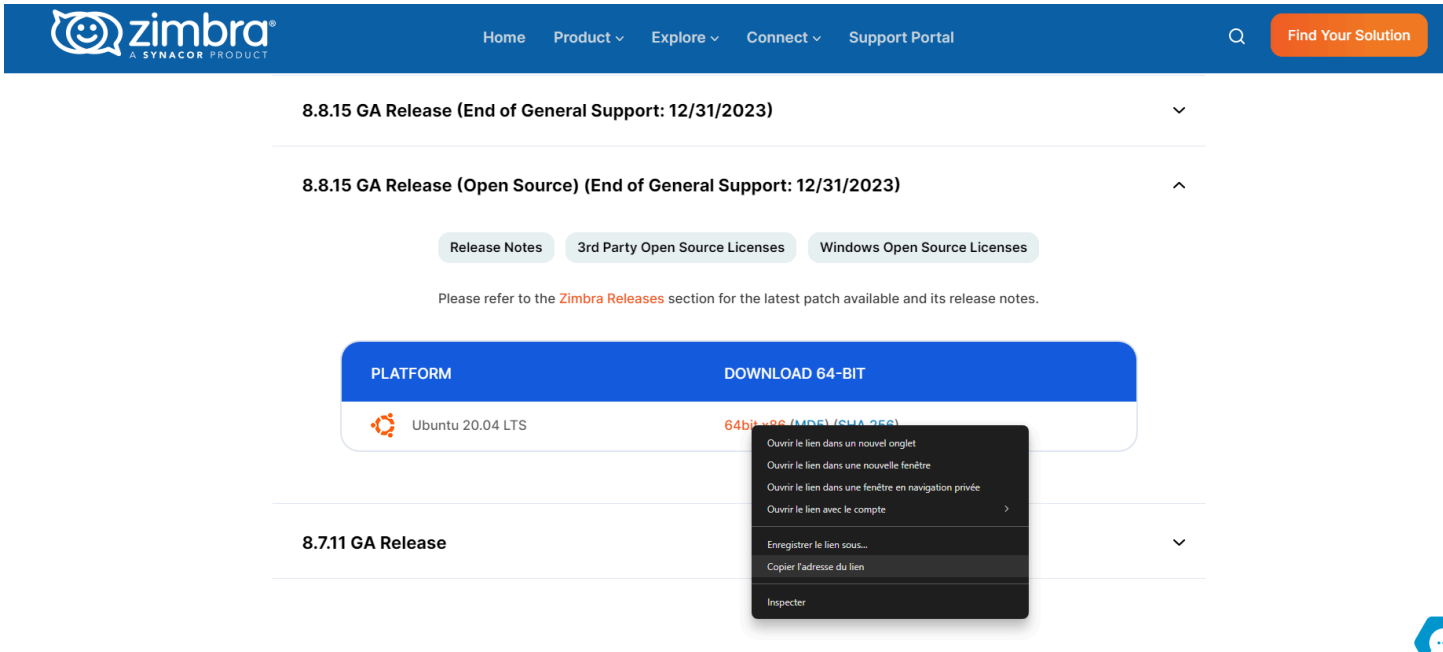
6- Installation de Zimbra

Téléchargement de Zimbra OSE : Aller sur le site officiel de ZIMBRA afin de trouver la version adapté , ici la version Ubuntu 20.04 Open Source

<https://www.zimbra.com/product/download/>



On clique droit sur la version et on copie le lien :



On se retrouve pour wget {le lien}

wget

https://files.zimbra.com/downloads/8.8.15_GA/zcs8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz

```
root@zimbra:~# wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
--2024-04-20 14:38:41-- https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
Résolution de files.zimbra.com (files.zimbra.com)... 18.66.115.55
Connexion à files.zimbra.com (files.zimbra.com)|18.66.115.55|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 246925287 (235M) [application/x-tar]
Enregistre : «zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz»

zcs-8.8.15_GA_4179.UBUNTU20_64.2 100%[=====>] 235,49M 35,5MB/s ds 6,7s
2024-04-20 14:38:51 (35,3 MB/s) - «zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz» enregistré [246925287/246925287]

root@zimbra:~# █
```

tar xvzf zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz

```
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-lmapi_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mta_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-admin-console-war_8.8.15.1624007059-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-docs_8.8.15.1552677786-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-proxy_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-spell_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-snmp_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-timezone-data_2.0.1.1618576642-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf-msgs_8.8.15.1556130968-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-war_8.8.15.1634917408-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-core-jar_8.8.15.1634917408-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-service_8.8.15.1634917408-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-logger_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf-msgs_8.8.15.1556130968-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-docs_8.8.15.1552677786-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-conf_8.8.15.1597662783-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf-rights_8.8.15.1487328490-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf-attrs_8.8.15.1571124020-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-war_8.8.15.1634917408-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-core_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-webclient-war_8.8.15.1635813854-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf-rights_8.8.15.1487328490-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-core-libs_8.8.15.1626439528-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-conf_8.8.15.1597662783-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-dnscache_8.8.15.GA.4179.UBUNTU20_64_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-service_8.8.15.1634917408-1.u20_amd64.deb
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-common-mbox-conf_8.8.15.1634917408-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/packages/zimbra-mbox-webclient-war_8.8.15.1635813854-1.u20_amd64.changes
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/.BUILD_PLATFORM
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/.BUILD_RELEASE_CANDIDATE
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/.BUILD_TYPE
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/data/
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/data/versions-init.sql
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/.BUILD_RELEASE_NO
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/readme_binary_en_US.txt
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/lib/
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/lib/jars/
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/.BUILD_NUM
zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954/install.sh
```

cd zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954

```
root@zimbra:~# cd zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954
root@zimbra:~/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954#
```

./install.sh

```
zimbra-core...NOT FOUND

-----
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
SYNACOR, INC. ("SYNACOR") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for this Zimbra Collaboration Suite Software:
https://www.zimbra.com/license/zimbra-public-eula-2-6.html
-----

Do you agree with the terms of the software license agreement? [N] Y

Use Zimbra's package repository [Y] Y

Warning: apt-key output should not be parsed (stdout is not a terminal)
Importing Zimbra GPG key

Configuring package repository
█
```

On met Y (yes) à tout sauf BETA :

```
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [Y] y
Install zimbra-proxy [Y] y
Install zimbra-drive [Y] y
Install zimbra-inapd (BETA - for evaluation only) [N] n
Install zimbra-chat [Y] y
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
zimbra-store package check complete.

Installing:
  zimbra-core
  zimbra-ldap
  zimbra-logger
  zimbra-mta
  zimbra-snmp
  zimbra-store
  zimbra-apache
  zimbra-spell
  zimbra-memcached
  zimbra-proxy
  zimbra-drive
  zimbra-patch
  zimbra-mta-patch
  zimbra-proxy-patch
  zimbra-chat

The system will be modified. Continue? [N] █
```

Dans le menu choisir l'interface correspondante et 4 pour configurer le Admin Password

Store configuration

```
1) status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@mail.scivil.local
** 4) Admin Password UNSET
5) Anti-virus quarantine user: virus-quarantine.g6g15caiw1@mail.scivil.local
6) Enable automated spam training: yes
7) Spam training user: spam._ls39ykvw@mail.scivil.local
8) Non-spam(Ham) training user: ham.ppxhh5mpa@mail.scivil.local
9) SMTP host: mail.scivil.local
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) Web server mode: https
13) IMAP server port: 7143
14) IMAP server SSL port: 7993
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://mail.scivil.local:7780/aspell.php
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@mail.scivil.local
22) Version update source email: admin@mail.scivil.local
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes
```

Select, or 'r' for previous menu [r] 4

Password for admin@mail.scivil.local (min 6 characters): [dtxR3Qe] Azerty52!

Store configuration

On valide & sauvegarde la configuration (press "a")

```
q) Quit
```

```
*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] yes
```

Il faudra patienter quelque minutes pour l'installation.

On se connecte à l'utilisateur zimbra avec une commande et on check le status des services de zimbra :

```
root@user01-Standard-PC-i440FX-PIIX-1996:~# su - zimbra
zimbra@mail:~$ zmcontrol status
Host mail.scivil.local
      amavis           Running
      antisppam        Running
      antivirrus       Running
      ldap             Running
      logger           Running
      mailbox          Running
      memcached        Running
      mta              Running
      opendkim         Running
      proxy            Running
      service webapp   Running
      snmp             Running
      spell            Running
      stats            Running
      zimbra webapp    Running
      zimbraAdmin webapp Running
      zimlet webapp    Running
      zmconfigd        Running
zimbra@mail:~$
```

ATTENTION : N'oublier pas de désactiver le par-feu :

```
sudo ufw disabe
```

OU ouvrir les ports nécessaires :

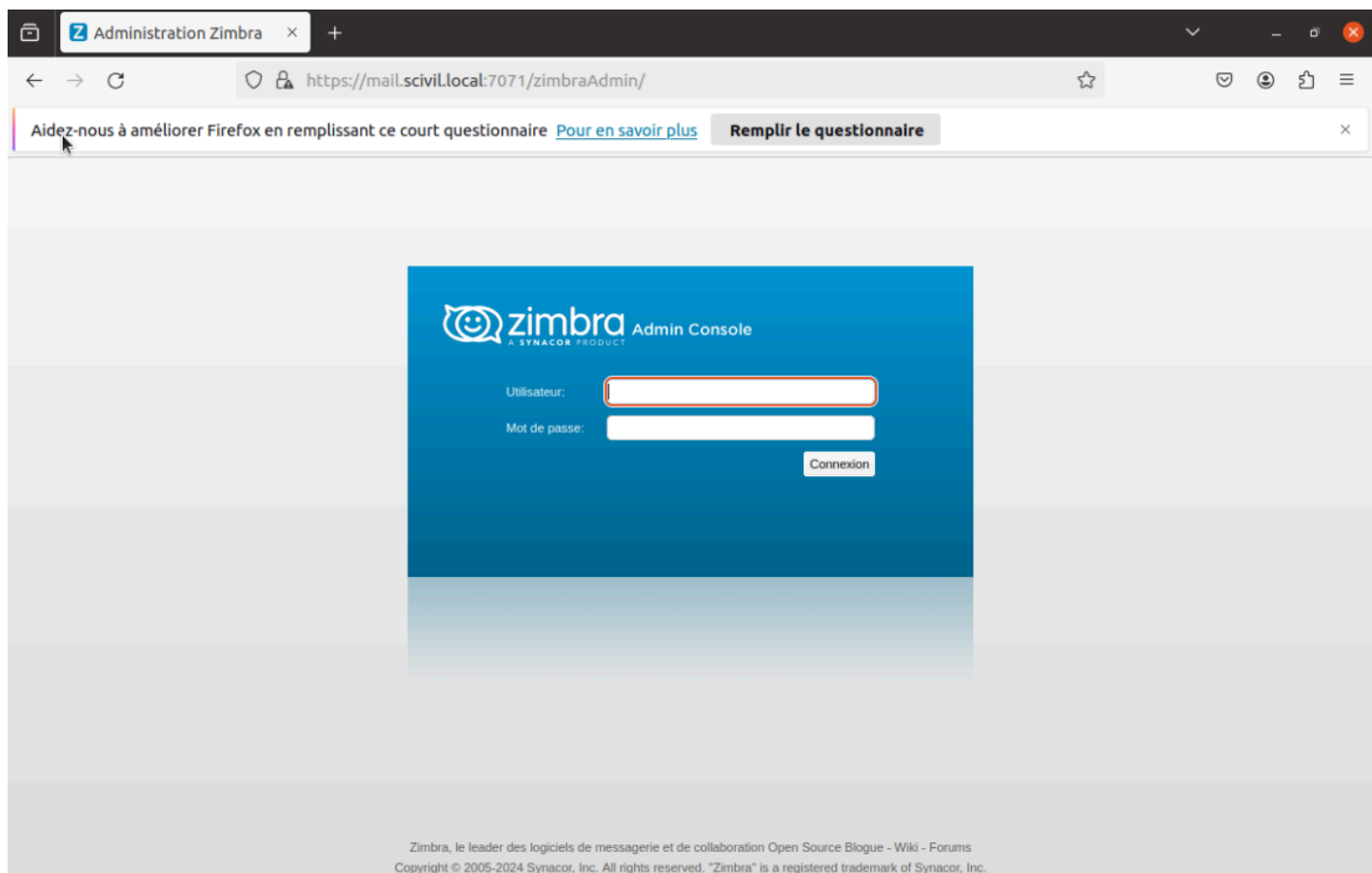
```
ufw allow 25,80,110,143,443,465,587,993,995,5222,5223,9071,7071/tcp
```

7- Accès à Zimbra :

Accédez à Zimbra via un navigateur à l'adresse :

<https://mail.scivil.local:7071> (adapté de votre coté)

Utilisez le nom d'utilisateur **admin** et le **mot de passe que vous avez configuré**.



Vous voilà avec votre serveur Zimbra correctement installé .

Une fois connecté à votre session administrateur nous pouvons ajouter l'active directory comme moyen d'authentification à Zimbra :



- Mode d'authentification
- Paramètres d'authentification
- Liaison LDAP
- Récapitulatif de la configuration de l'authentification
- Paramétrage de groupe externe
- Configuration du domaine terminée

Mode d'authentification de ce domaine

- Interne
Le mode d'authentification LDAP interne suppose que le schéma Zimbra est exécuté sur le serveur d'annuaire OpenLDAP.
- Active Directory externe
Le mécanisme d'authentification Active Directory tente de se connecter au serveur d'annuaire en utilisant les services d'annuaire Microsoft Active Directory pour l'authentification.
- LDAP externe
Le mécanisme d'authentification LDAP externe tente de se connecter au serveur d'annuaire en utilisant le nom d'utilisateur et le mot de passe fournis.



- Mode d'authentification
- Paramètres d'authentification
- Liaison LDAP
- Récapitulatif de la configuration de l'authentification
- Paramétrage de groupe externe
- Configuration du domaine terminée

Paramètres Active Directory

Domaine du serveur AD :*

Serveur AD

| | Nom du serveur AD :* | Port :* | Utiliser SSL : | |
|---------|----------------------|---------|--------------------------|-----------|
| ldap:// | 192.168.10.10 | 3268 | <input type="checkbox"/> | Supprimer |
| ldap:// | 192.168.10.11 | 3268 | <input type="checkbox"/> | Supprimer |

Ajouter une URL

Version Zimbra : 8.8.15_GA_4581.FOS Service : ✔ En cours

Aide pour la configuration de l'authentification (scivil.local)

Mode d'authentification
Paramètres d'authentification
Liaison LDAP
Récapitulatif de la configuration de l'authentification
Paramétrage de groupe externe
Configuration du domaine terminée

Utiliser un identifiant (DN)/ mot de passe pour associer un serveur externe :

Associer un identifiant (DN) :

Associer un mot de passe :

Confirmer l'association du mot de passe :

Aide Annuler Précédent Suivant Terminer

Version Zimbra : 8.8.15_GA_4581.FOS Service : ✔ En cours

Aide pour la configuration de l'authentification (scivil.local)

Mode d'authentification
Paramètres d'authentification
Liaison LDAP
Récapitulatif de la configuration de l'authentification
Paramétrage de groupe externe
Configuration du domaine terminée

Récapitulatif de la configuration de l'authentification

Mécanisme d'authentification : **Active Directory externe**

Domaine du serveur AD : scivil.local

URL LDAP : ldap://192.168.10.10:3268
ldap://192.168.10.11:3268

Veillez fournir un nom d'utilisateur et un mot de passe pour tester les paramètres d'authentification

Nom d'utilisateur :

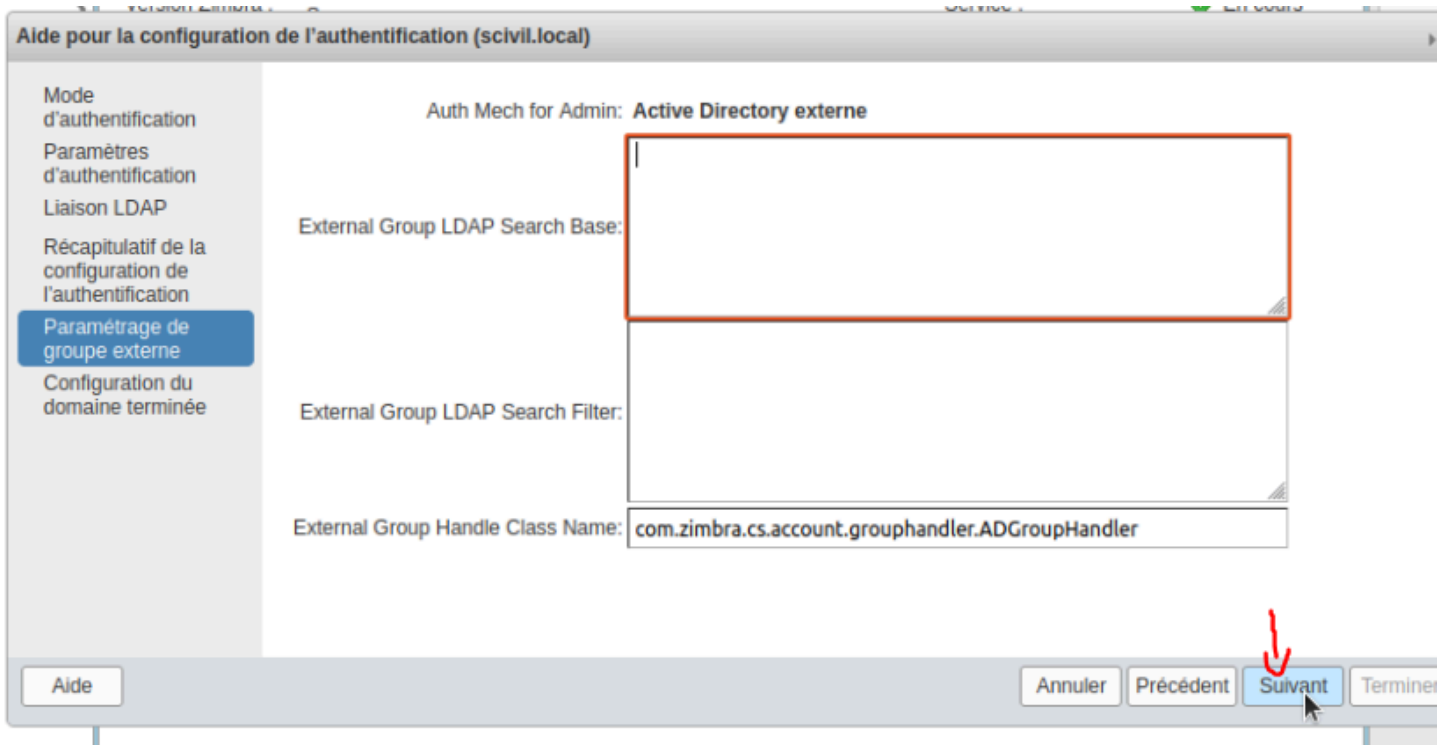
Mot de passe :

Tester

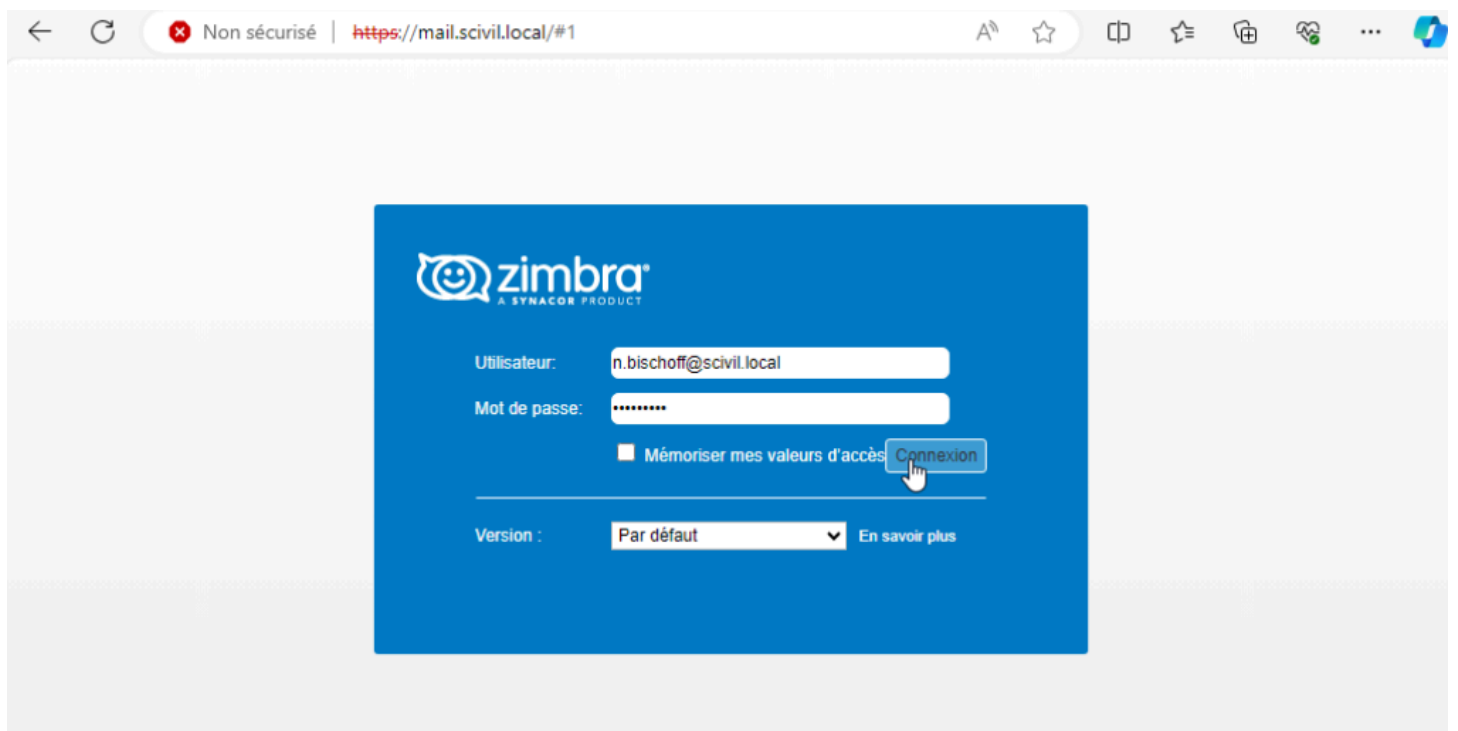
Le test d'authentification a réussi

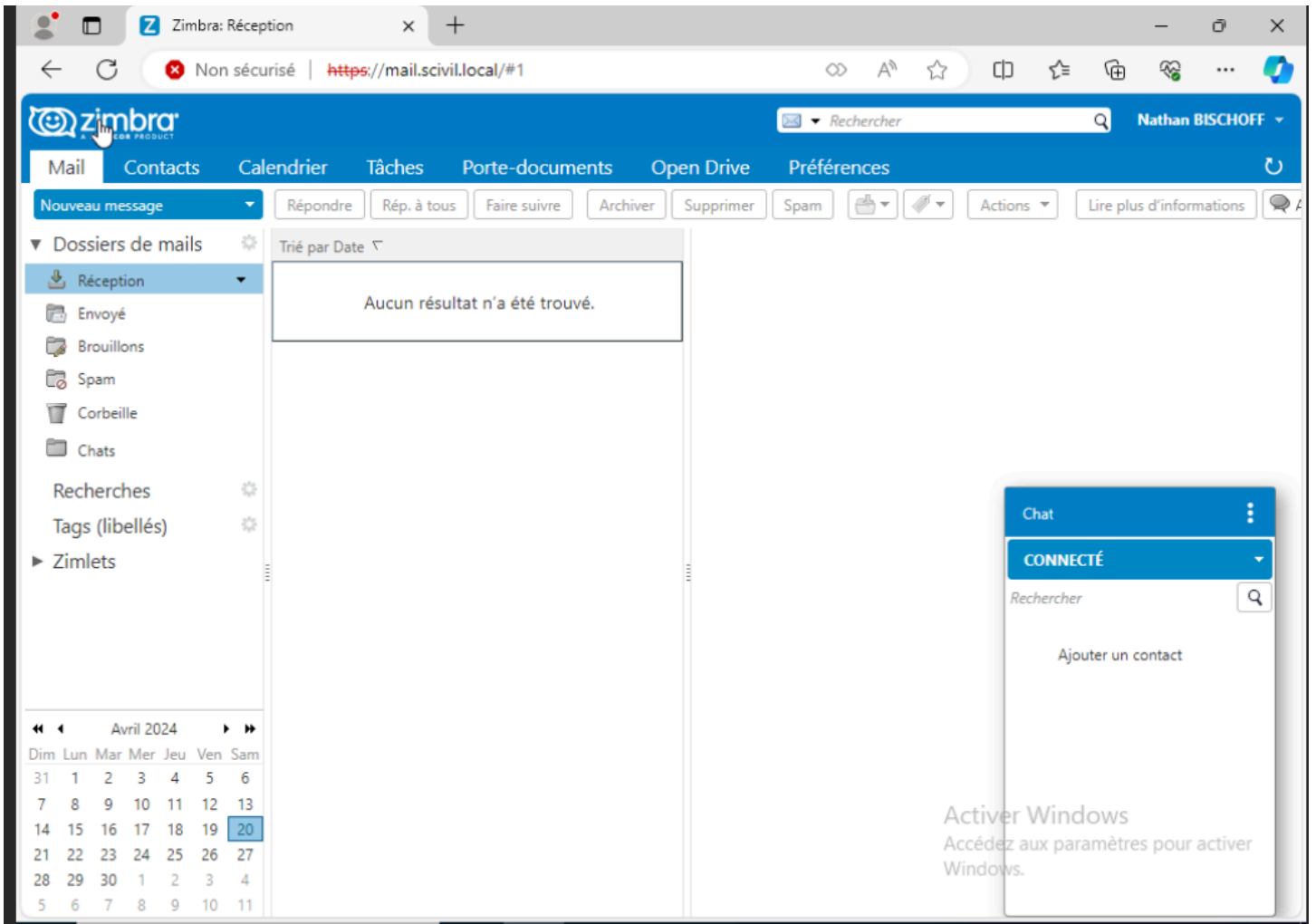
DN de liaison calculé : n.bischoff@scivil.local

Aide Annuler Précédent Suivant Terminer

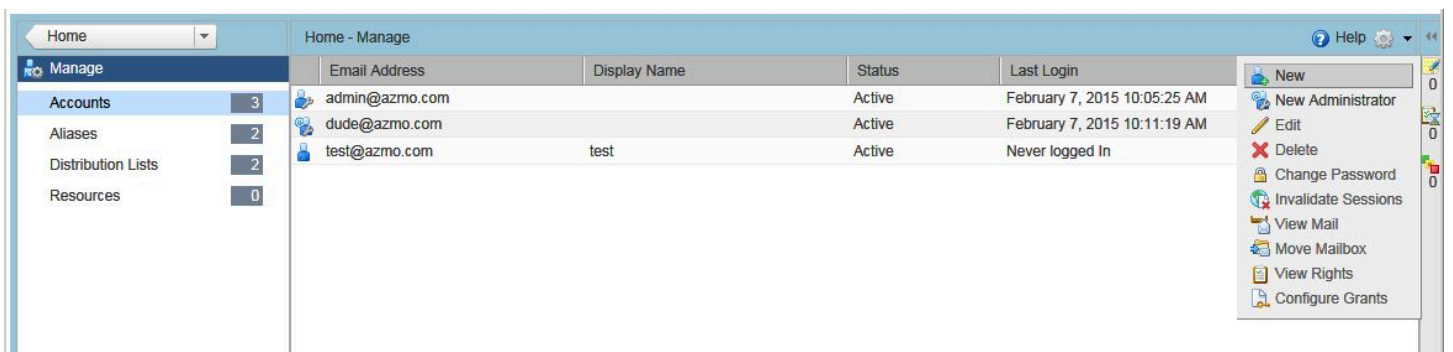


Terminé !





N'oubliez pas de créer l'utilisateur dans Manage > Account > New account sans mettre de mot de passe étant donné que c'est le rôle de l'AD :



New Account

General Information

Account Name

Account name: * @

First name:

Middle initial:

Last name: *

Display name: auto

Hide in GAL:

Account Setup

Status:

Class of Service: auto

Global Administrator

Administrator

Help Cancel Previous Next Finish

Aide pour la configuration de l'authentification (scvii.local)

Mode d'authentification

Paramètres d'authentification
Liaison LDAP
Récapitulatif de la configuration de l'authentification
Paramétrage de groupe externe
Configuration du domaine terminée

Mode d'authentification de ce domaine

Interne
Le mode d'authentification LDAP interne suppose que le schéma Zimbra est exécuté sur le serveur d'annuaire OpenLDAP.

Active Directory externe
Le mécanisme d'authentification Active Directory tente de se connecter au serveur d'annuaire en utilisant les services d'annuaire Microsoft Active Directory pour l'authentification.

LDAP externe
Le mécanisme d'authentification LDAP externe tente de se connecter au serveur d'annuaire en utilisant le nom d'utilisateur et le mot de passe fournis.

Aide Annuler Précédent Suivant Terminer

Aide pour la configuration de l'authentification (scivil.local)

Mode d'authentification

- Paramètres d'authentification
- Liaison LDAP
- Récapitulatif de la configuration de l'authentification
- Paramétrage de groupe externe
- Configuration du domaine terminée

Paramètres Active Directory

Domaine du serveur AD :*


Serveur AD

| | Nom du serveur AD :* | Port :* | Utiliser SSL : | |
|---------|--|-----------------------------------|--------------------------|--|
| ldap:// | <input type="text" value="192.168.10.10"/> | <input type="text" value="3268"/> | <input type="checkbox"/> | <input type="button" value="Supprimer"/> |
| ldap:// | <input type="text" value="192.168.10.11"/> | <input type="text" value="3268"/> | <input type="checkbox"/> | <input type="button" value="Supprimer"/> |

Administration Zimbra

https://mail.scivil.local:7071/zimbraAdmin/

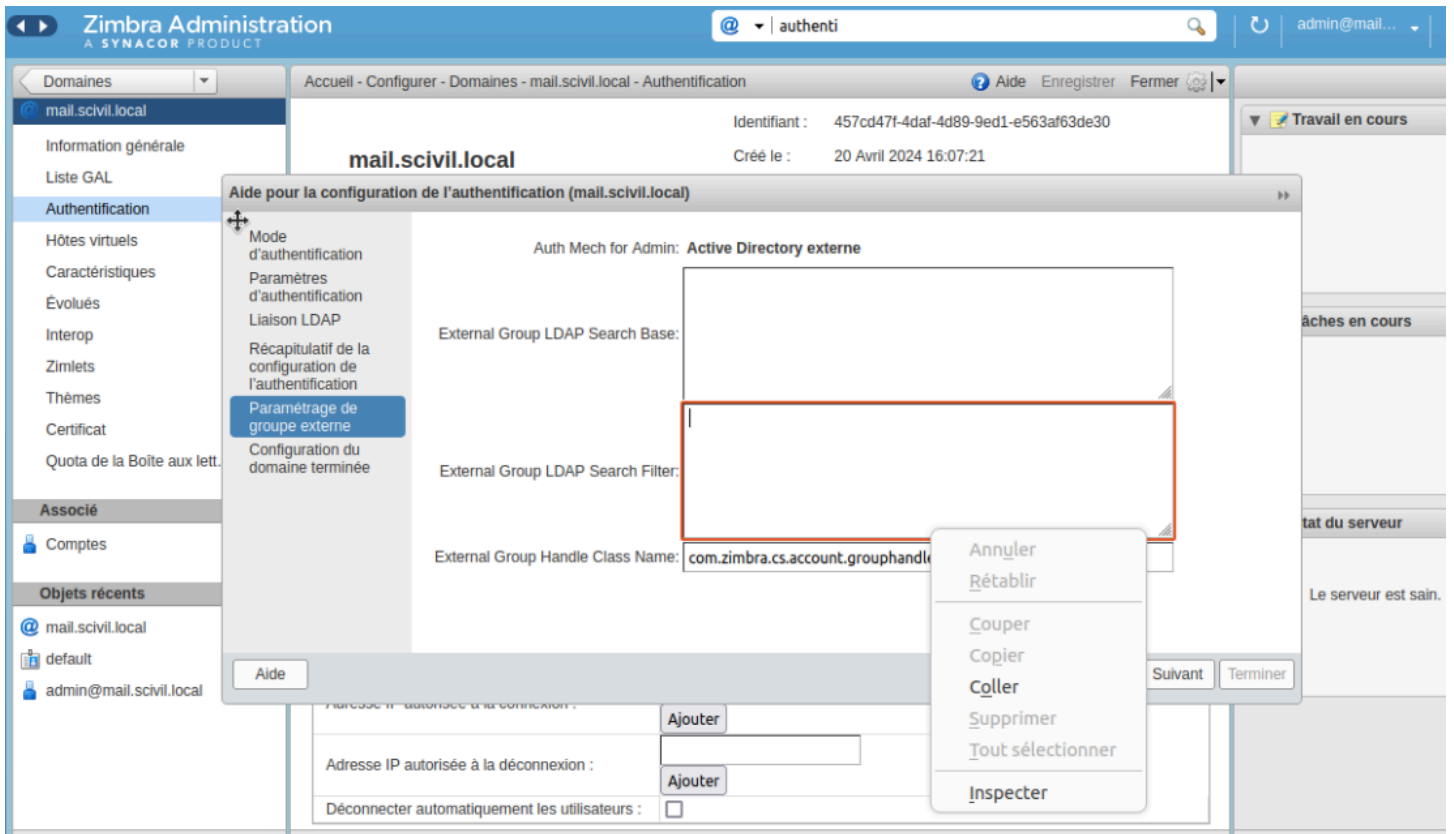
Aidez-nous à améliorer Firefox en remplissant ce court questionnaire [Pour en savoir plus](#)



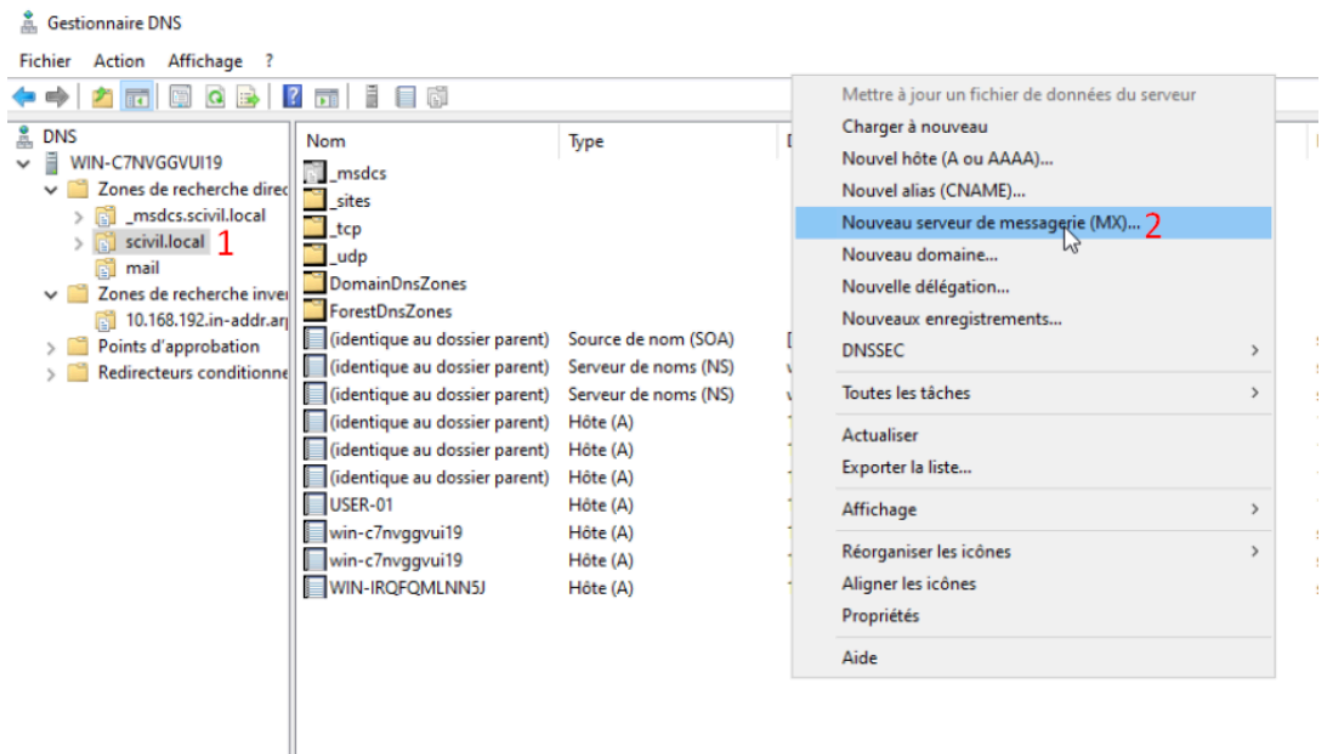
Utilisateur:

Mot de passe:

Zimbra, le leader des logiciels de messagerie et de collaboration Open Source Blogue - Wiki - Forums
Copyright © 2005-2024 Synacor, Inc. All rights reserved. "Zimbra" is a registered trademark of Synacor, Inc.



On configure la redirection DNS afin que cela s'applique



On crée une nouvelle redirection type messagerie donc MX

Serveur de messagerie (MX) Sécurité

On crée une nouvelle redirection type messagerie donc MX

Serveur de messagerie (MX) Sécurité

Hôte ou domaine enfant :

Par défaut, DNS utilise le nom de domaine parent lors de la création d'un serveur de courrier Exchange. Vous pouvez spécifier un nom d'hôte ou d'enfant n'importe lequel. Dans la plupart des déploiements, le champ ci-dessus est conservé vide.

Nom de domaine pleinement qualifié (FQDN) :

Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie :

Priorité du serveur de messagerie :

On met en hôte le nom mis précédemment, et l'IP du serveur de mail, donc notre linux

Voilà le serveur de mail ZIMBRA prêt.

Mise en place de la supervision et du monitoring avec WAZUH



Wazuh est une plateforme de sécurité gratuite et open source qui unifie la protection XDR et SIEM pour les terminaux et les charges de travail en cloud .

Wazuh propose une suite de sécurité open source avec des fonctionnalités clés :

Gestion des Logs : Collecte et normalise les logs de diverses sources.

Détection d'Intrusion (IDS) : Analyse les logs pour détecter des activités suspectes ou des attaques.

FIM (File Integrity Monitoring) : Surveille les modifications non autorisées des fichiers.

Gestion des Vulnérabilités : Identifie les vulnérabilités en analysant les logs.

Gestion des Configurations : Surveille les configurations système pour détecter des changements non autorisés.

Réponse aux Incidents : Déclenche des actions automatisées en réponse à des événements spécifiques.

Interface Web (Kibana App) : Fournit une interface visuelle et des tableaux de bord interactifs pour la gestion.

Extensibilité et Intégration : Peut être étendu avec des modules et s'intègre avec d'autres outils de sécurité.

Support Multi-Plateforme : Compatible avec divers systèmes d'exploitation, y compris Linux, Windows, macOS, etc.

SOMMAIRE :

Partie 1 : Installation de l'indexeur Wazuh .

Partie 2 : Installation des nœuds de l'indexeur .

Partie 3 : Initialisation du cluster .

Partie 4 : Installation des Agents .

Partie 5 : Configuration des Outils .

Partie 6 : Avis sur la solution .

Partie 7 : L'intérêt de cette solution open-source .

Partie 1 : Installation de l'indexeur Wazuh :

On initie la configuration de Wazuh & on crée les certificats SSL :

Téléchargement de l'assistant d'installation Wazuh et le fichier de configuration. :

```
apt-get install curl
```

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

```
curl -sO https://packages.wazuh.com/4.7/config.yml
```

On modifie le ./config.yml et on remplace les noms de nœuds et les valeurs IP par les noms et adresses IP qui correspondent :


```
GNU nano 6.2
nodes:
# Wazuh indexer nodes
indexer:
- name: node-1
  ip: "192.168.154.140"
#- name: node-2
# ip: "<indexer-node-ip>"
#- name: node-3
# ip: "<indexer-node-ip>"

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: wazuh-1
  ip: "192.168.154.140"
# node_type: master
#- name: wazuh-2
# ip: "<wazuh-manager-ip>"
# node_type: worker
#- name: wazuh-3
# ip: "<wazuh-manager-ip>"
# node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: "192.168.154.140"
```

Exécutez l'assistant avec la possibilité --generate-config-files :

```
bash wazuh-install.sh --generate-config-files
```

Partie 2 : Installation des nœuds de l'indexeur :

Téléchargez l'assistant d'installation Wazuh :

```
root@wazuh-virtual-machine:~# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
root@wazuh-virtual-machine:~#
```

Exécutez l'assistant avec l'option --wazuh-indexer :

```
bash wazuh-install.sh --wazuh-indexer node-1
```

```
18/01/2024 15:20:35 INFO: Initializing Wazuh indexer cluster
18/01/2024 15:20:37 INFO: Wazuh indexer cluster initialized
18/01/2024 15:20:37 INFO: --- Dependencies ---
18/01/2024 15:20:37 INFO: Removing gawk.
18/01/2024 15:20:41 INFO: Installation finished.
root@wazuh-virtual-machine:~#
```

Partie 3 : Initialisation du cluster :

```
bash wazuh-install.sh --start-cluster
```

On tape cette commande afin d'obtenir le mot de passe admin :

```
root@wazuh-virtual-machine:~# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin\'" -A 1
indexer_username: 'admin'
indexer_password: 'lHr6631JQxM1pAIm1HPbH3SzQG5d6iB.'
```

Après test on voit que le cluster marche correctement :

```
virtual-machine:~# curl -k -u admin:lHr6631JQxM1pAIm1HPbH3SzQG5d6iB. https://192.168.154.140:9200/_cat/nodes?v
heap.percent ram.percent cpu load_1m load_5m load_15m node.role node.roles cluster_manager
.140 12 92 5 0.20 0.36 0.30 dimr data,ingest,master,remote_cluster_client *
```

Partie 4 : Installer le serveur Wazuh à l'aide de l'assistant :

Téléchargez l'assistant d'installation Wazuh :

```
root@wazuh-virtual-machine:~# bash wazuh-install.sh --wazuh-server wazuh-1
18/01/2024 15:31:51 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.2
18/01/2024 15:31:51 INFO: Verbose logging redirected to /var/log/wazuh-install.log
```

Installation du tableau de bord Wazuh :

bash wazuh-install.sh --wazuh-dashboard dashboard

```
18/01/2024 15:36:38 INFO: You can access the web interface https://192.168.154.140:443
User: admin
Password: lHr6631JQxM1pAIm1HPbH3SzQG5d6iB.
```

On va maintenant regarder les mots de passes :

```
root@wazuh-virtual-machine:~# tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: 'lHr6631JQxM1pAIm1HPbH3SzQG5d6iB.'
```

```
# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: 'B640tPEDv4Mkc0cNFfhPl1xz?o5g4DKK'
```

```
# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
indexer_username: 'kibanaro'
indexer_password: 'eT*FA.6QfdGjMK7q55Xt+dHKL6CN96Lz'
```

```
# Filebeat user for CRUD operations on Wazuh indices
indexer_username: 'logstash'
indexer_password: 'SLm7tG+Au6L6HM.H2xk3kzMM?AuW5wXs'
```

```
# User with READ access to all indices
indexer_username: 'readall'
indexer_password: 'RtFZkwtT1f*Fl*KHutls9v7ilQprcPtJ'
```

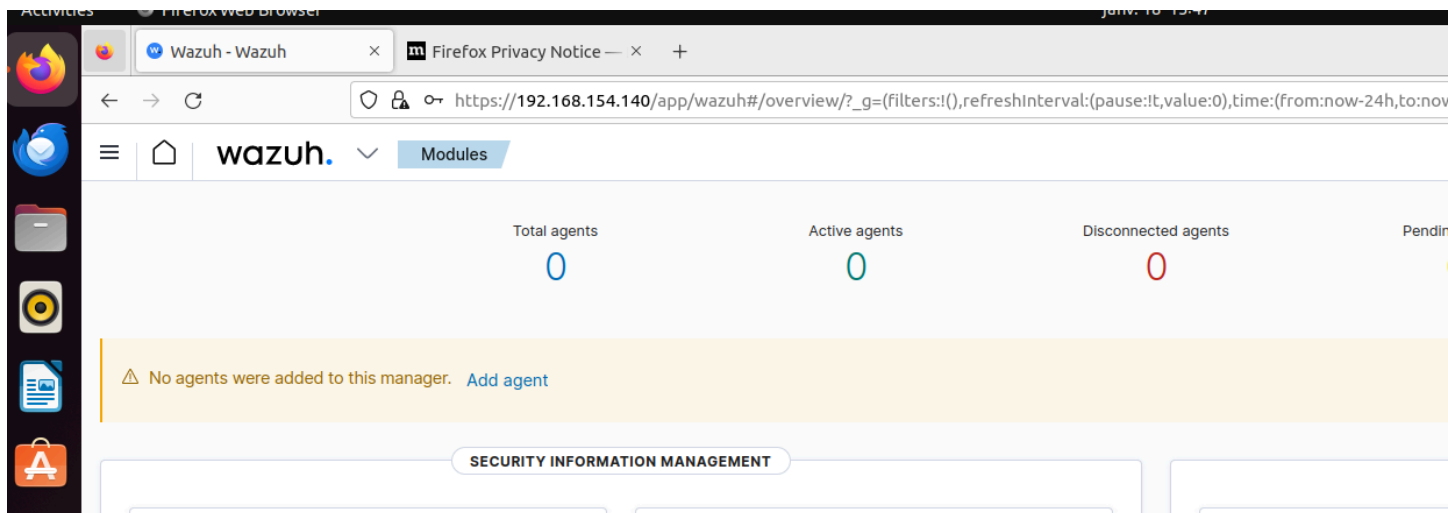
```
# User with permissions to perform snapshot and restore operations
indexer_username: 'snapshotrestore'
indexer_password: '2TLRRtqcIZsh0y9Wwi?4cp?*g3?FWk?J'
```

```
# Password for wazuh API user
api_username: 'wazuh'
api_password: 'ux9zPda?WhH*X+X0sfwCiJsTL+*VP410'
```

```
# Password for wazuh-wui API user
api_username: 'wazuh-wui'
api_password: 'rqnjrA0Jl4*0H55oD20RDh5U9MR*k*7B'
```

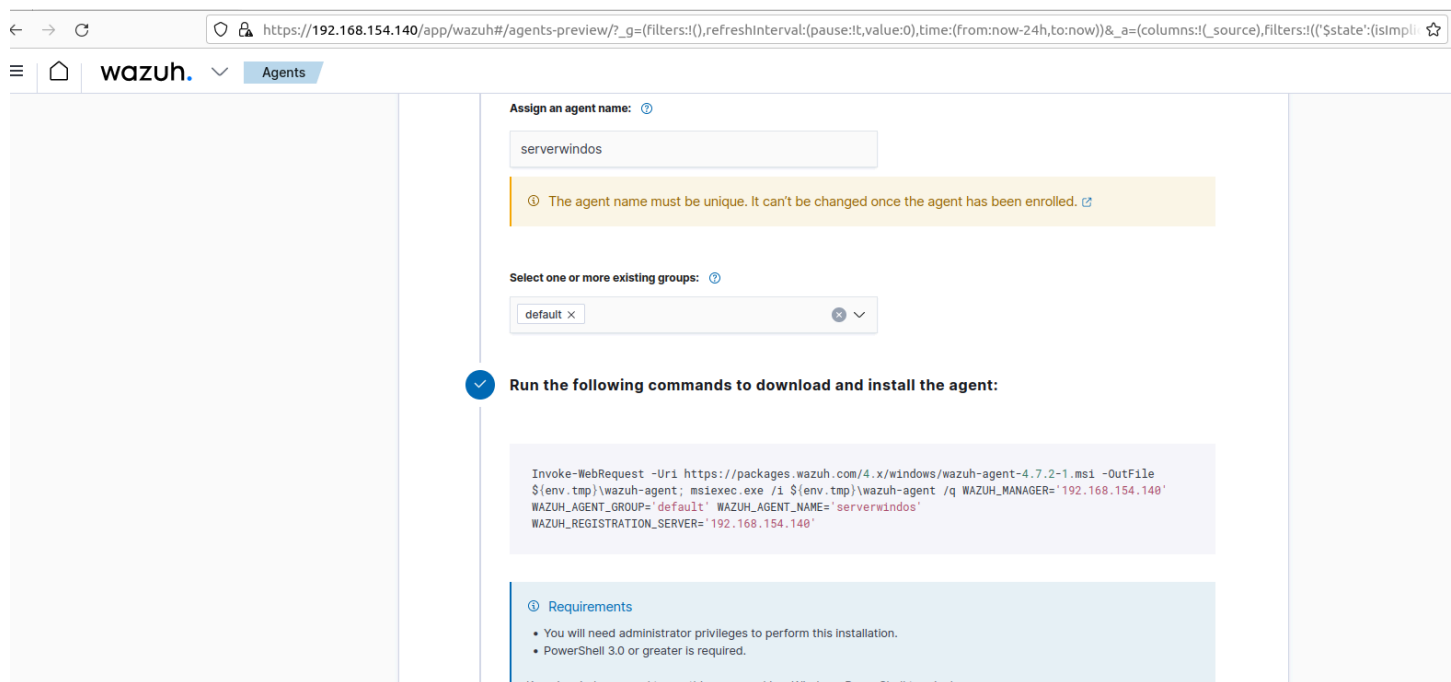
Pour maintenant accéder à l'interface web :

- URL: <https://192.168.154.140>
- Username: admin
- Password: VotreMotDePasse



installer l'agent Wazuh sur un Serveur Windows 10_2022 :

il faut installer l'agent sur notre serveur Windows avec la commande générée grâce aux infos qu'on donne sur le site :



Une fois la commande rentré on vérifie bien la présence du service :

```
PS C:\Users\User> Get-Service -Name wazuh

Status Name      DisplayName
-----
Running WazuhSvc   wazuh

PS C:\Users\User>
```

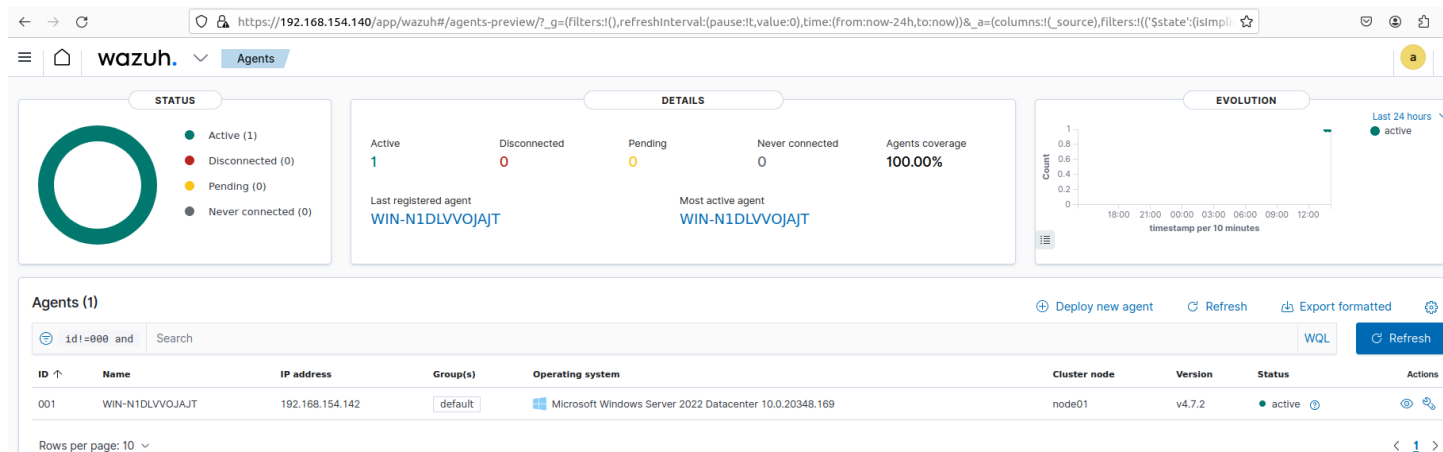
Running donc c'est ok .

On vérifie le statut de l'agent sur notre serveur Ubuntu :

```
available agents:  
ID: 001, Name: WIN-N1DLVVOJAJT, IP: any
```

On voit qu'il est bien présent et qu'il porte l'ID numéro 1.

On le voit ainsi aussi sur notre interface web :



Pour installer l'agent Wazuh sur un PC Windows 10 :

On se retrouve sur le panel agents sur notre interface web et on sélectionne déploiement nouvel agent :

[+ Deploy new agent](#)

On remplit encore une fois les bonnes infos pour récupérer la commande à mettre dans le PowerShell de notre PC Windows 10 :

```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -OutFile $(env:tmp)\wazuh-agent; msixec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER=192.168.154.140 WAZUH_AGENT_GROUP=default WAZUH_AGENT_NAME=pc01 WAZUH_REGISTRATION_SERVER=192.168.154.140
```

On le lance :

```
PS C:\Windows\system32> NET START WazuhSvc  
Le service Wazuh a démarré.  
PS C:\Windows\system32> Get-Service -Name WazuhSvc  
  
Status Name DisplayName  
-----  
Running WazuhSvc Wazuh
```

Le nouvel agent du PC Windows apparaît :

Agents (2)

| ID ↑ | Name | IP address | Group(s) | Operating system |
|------|-----------------|-----------------|----------|---|
| 001 | WIN-N1DLVVOJAJT | 192.168.154.142 | default | Microsoft Windows Server 2022 Datacenter 10.0.20348.169 |
| 002 | nathan | 192.168.154.136 | default | Microsoft Windows 10 Pro 10.0.19045.3930 |

Rows per page: 10 ▾

Partie 5 : Configuration des Outils :

Détection d’Intrusion (IDS) :

- **Explication** : La détection d’intrusion analyse les logs pour détecter des activités suspectes ou des attaques en temps réel, ce qui permet de prévenir les violations de sécurité.

Dans ce cas d’utilisation, nous montrons comment intégrer Suricata à Wazuh. Suricata peut fournir des informations supplémentaires sur la sécurité de votre réseau grâce à ses capacités d’inspection du trafic réseau.

Installation de Suricata sur le serveur Wazuh Ubuntu :

- Ajoutez le référentiel Suricata stable : `sudo add-apt-repository ppa:oisf/suricata-stable`.
- Mettez à jour les paquets : `sudo apt-get update`.
- Installez Suricata : `sudo apt-get install suricata -y`.

Téléchargement des règles :

- Téléchargez et extrayez les règles Emerging Threats Suricata :

```
root@wazuh-virtual-machine:/home/wazuh# cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left   Speed
31 4129k    31 1291k    0     0  499k      0  0:00:08  0:00:02  0:00:06  499k
```

On modifie la configuration de Suricata pour mettre la bonne IP & l’interface à surveiller :

`sudo nano /etc/suricata/suricata.yaml :`

`HOME_NET: "192.168.154.140"`

`EXTERNAL_NET: "any"`

`af-packet:`

`- interface: ens33`

`sudo systemctl restart suricata`

Ajout de la configuration au fichier ossec.conf de l'agent Wazuh :

```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
```

Émulation d'attaque :

```
root@wazuh-virtual-machine:/tmp# ping -c 20 192.168.154.140
PING 192.168.154.140 (192.168.154.140) 56(84) bytes of data.
64 bytes from 192.168.154.140: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 192.168.154.140: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 192.168.154.140: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 192.168.154.140: icmp_seq=4 ttl=64 time=0.036 ms
```

Il faudra alors voir dans Alerts si le Suricata détecte bien l'attaque.

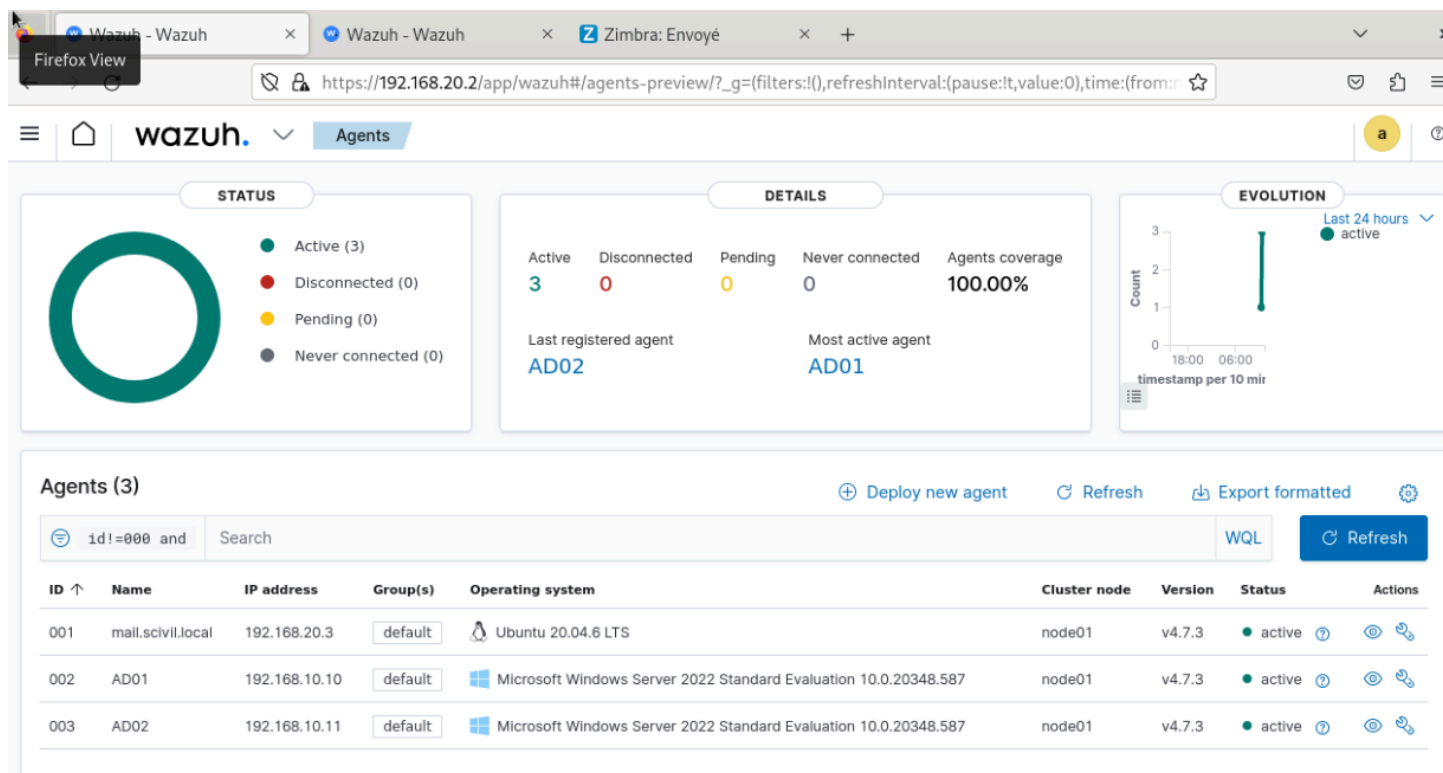
Gestion des Logs :

Sources d'un OSSEC.LOG

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  <localfile>
    <location>/var/ossec/logs/ossec.log</location>
    <log_format>syslog</log_format>
  </localfile>
</global>

<alerts>
```

Voilà Wazuh correctement installé .



7 – Retours d'Expérience et Bonnes Pratiques

● Retours d'Expérience

1. Haute Disponibilité des Routeurs pfSense :

- **Leçon apprise :** La configuration initiale du CARP est critique et nécessite une vérification rigoureuse des adresses IP et des priorités pour éviter les conflits.
- **Pratique recommandée :** Effectuer des tests réguliers de basculement pour s'assurer que les mécanismes de failover fonctionnent comme prévu en cas de défaillance d'un routeur.

2. Déploiement d'Active Directory :

- **Leçon apprise :** La synchronisation entre les serveurs Active Directory doit être constamment surveillée pour prévenir les erreurs de réplication qui peuvent causer des interruptions de service.
- **Pratique recommandée :** Mettre en place des alertes automatisées pour détecter les échecs de réplication et intervenir rapidement.

3. Installation et Configuration de Zimbra :

- **Leçon apprise :** La configuration des enregistrements DNS est cruciale pour le bon fonctionnement des services de messagerie et doit être effectuée avec précision.
- **Pratique recommandée :** Valider les configurations DNS via des outils externes avant de lancer le déploiement de Zimbra pour garantir l'acheminement correct des courriels.

4. Utilisation de WAZUH pour la Surveillance et le Monitoring :

- **Leçon apprise :** La complexité de configuration initiale peut retarder la mise en place effective de la surveillance.
- **Pratique recommandée :** Documenter en détail les étapes de configuration et de déploiement pour faciliter les futurs déploiements ou maintenances.

● Bonnes Pratiques

1. **Documentation Rigoureuse :**

- **Importance :** La documentation détaillée de chaque étape du processus d'installation et de configuration s'est avérée indispensable pour le transfert de connaissances et pour les opérations de maintenance.
- **Action :** Continuer à mettre à jour les documents techniques à mesure que le système évolue et que de nouvelles configurations sont implémentées.

2. **Tests Continus :**

- **Importance :** Les tests continus des systèmes pour vérifier leur performance et leur résilience ont permis de détecter des problèmes avant qu'ils ne deviennent critiques.
- **Action :** Établir un calendrier de tests réguliers et de simulations de pannes pour garantir la préparation et la réactivité des équipes techniques.

3. **Formation et Sensibilisation des Utilisateurs :**

- **Importance :** La formation des utilisateurs finaux sur les fonctionnalités des nouveaux systèmes et les procédures de sécurité a réduit significativement le nombre d'incidents liés à l'utilisateur.
- **Action :** Continuer les sessions de formation régulières et développer des guides utilisateur intuitifs pour accompagner les changements technologiques.

8 – Conclusion

● Conclusion

Ce projet visait à améliorer la résilience informatique et l'efficacité des Centres Opérationnels Départementaux en implémentant des solutions de haute disponibilité pour les routeurs et serveurs, en déployant des outils de communication et de collaboration modernes, et en mettant en place un système robuste de surveillance et de monitoring. Les objectifs principaux ont été largement atteints, avec la mise en œuvre réussie de :

- Une infrastructure réseau redondante qui a déjà prouvé sa capacité à gérer les défaillances sans interruption significative du service.
- Un système Active Directory bien configuré qui facilite la gestion des utilisateurs et améliore la sécurité.
- Un serveur de messagerie Zimbra qui a amélioré les communications internes et externes.
- Un système de surveillance avec WAZUH qui permet une réaction rapide face aux incidents de sécurité et aux défaillances du système.
- Un accès Open VPN ROADWARRIOR qui dans une DMZ qui donne accès au logiciel E-Brigade.

Les délais prévus ont été respectés et l'organisation du GANTT Project respecté.

HEUSSER NATHAN

<https://nathanheusser.fr>

RACLOT EMILIEN

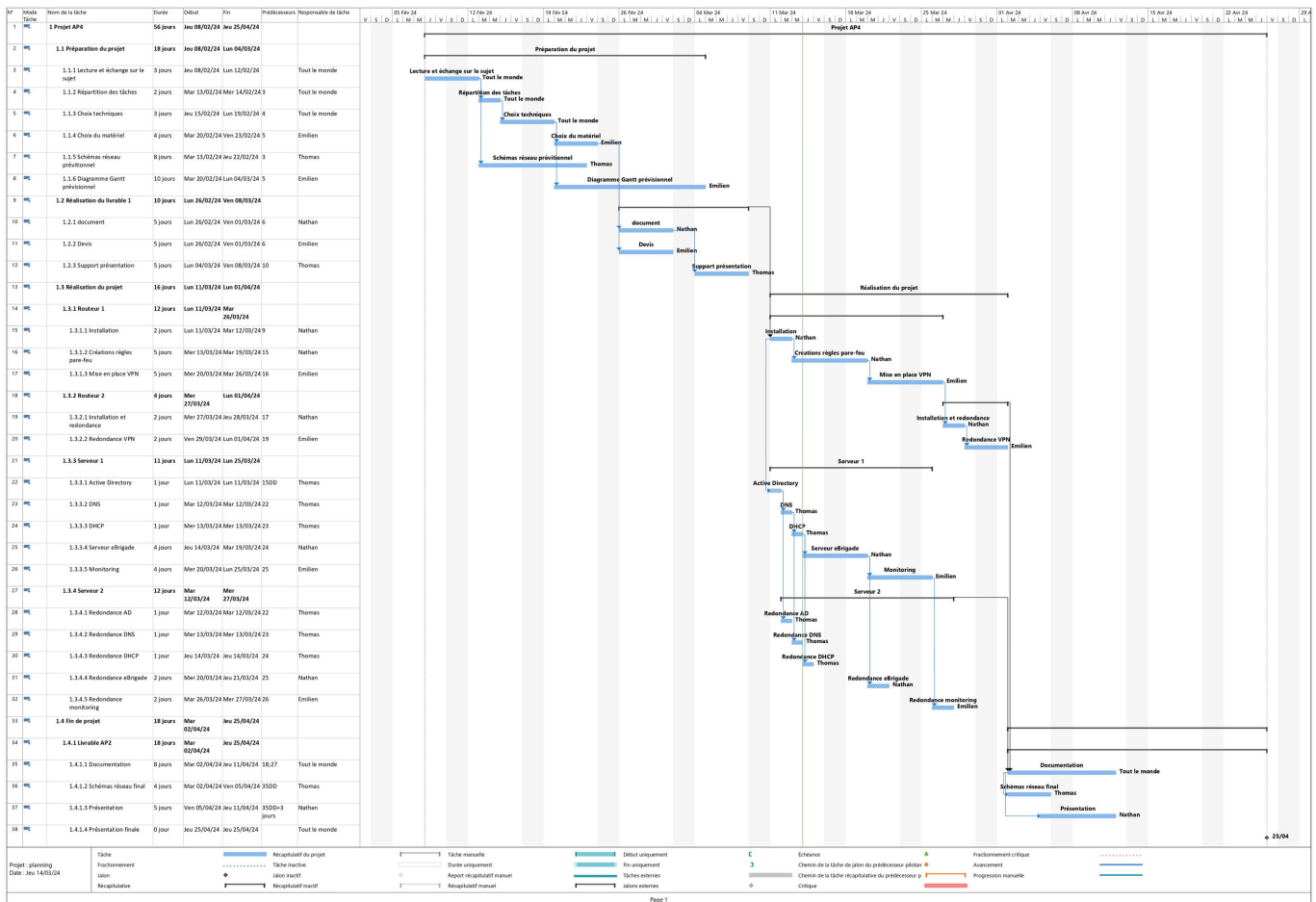
<https://emilienraclot.fr>

THOMAS GOURDIN

<https://thomasgourdin.fr>

9 – Annexes

Planning complet :



BUDGET

| Désignation | Référence | Quantité | Prix HT |
|-------------------------|---|----------|-----------|
| Serveur | Serveur PCSpecialist + 5 licences CAL | 2 | 9608,34 |
| Routeur redondé | Netgate 8200 MAX HA pfSense+ Security Gateway | 1 | 2938 |
| Switch | Aruba 2530 48 ports POE+ | 2 | 2734,66 |
| Onduleur | APC Back-UPS Pro 1500VA | 2 | 724,92 |
| Cordons RJ45 baie | Textorm Câble RJ45 CAT 7 SSTP 0.5m | 6 | 37,74 |
| Emetteur- récepteur | SFP+ 10GBase-SR Transceiver | 2 | 113,98 |
| Offre fibre dédiée | Orange pro (mensuel) | 1 | 55 |
| Offre fibre dédiée | SFR pro (mensuel) | 1 | 120 |
| Main d'œuvre (jours) | 1 technicien 1200€/j | 5 | 6000 |
| Total | | | 22 332.61 |

TABLEAU COMPARATIF DES SOLUTIONS ENVISAGÉES

| Option choisie | Raison | Alternative étudiée | Amélioration possible |
|--|--|--|---|
| Windows serveur | <ul style="list-style-type: none"> • Solution complète • Gère les postes et les serveurs • Facilité d'utilisation | <ul style="list-style-type: none"> • Linux : plus complexe d'utilisation • Chrome OS : moins complet que Windows | |
| Serveur sur mesure | <ul style="list-style-type: none"> • Avoir les composants de notre choix • Meilleur rapport performances/prix • Stockage raid 1 gen 3 | <ul style="list-style-type: none"> • Serveur préconfigurés : peu de choix, très cher • Stockage raid 5/raid 10/raid 01 : Inutile au vu de la faible utilisation du service, le raid 1 sera suffisant | <ul style="list-style-type: none"> • Garantie panne sur site • En cas de ralentissement : SSD nvme gen 5 |
| Double fibres avec opérateurs différents | <ul style="list-style-type: none"> • Si un des deux opérateur a un soucis, l'autre prend le relai • 8Gbps sur la fibre principale | <ul style="list-style-type: none"> • Box 4g : Moins fiable, débit plus faible • Deux fibres avec le même opérateur : risqué en cas de panne d'un opérateur | <ul style="list-style-type: none"> • Que les deux fibres aient une box 4g de secours qui switch automatiquement en cas de panne |
| Onduleurs 800W | <ul style="list-style-type: none"> • Peu tenir les équipement sur une bonne durée • Prix raisonnable | <ul style="list-style-type: none"> • Gros onduleur 5000W : prix excessivement cher | <ul style="list-style-type: none"> • Avoir un groupe électrogène en plus si les services sont amenés à se couper durant plusieurs heures |
| Routeurs | <ul style="list-style-type: none"> • Redondance facilitée • Modèle incluant PfSense+ | <ul style="list-style-type: none"> • Routeur avec d'autres types de pare-feu (type watchguard) : On connaît bien l'interface PfSense+ | <ul style="list-style-type: none"> • Meilleure interface |

| COMPOSANT | DESCRIPTION | VLAN ID | IP / PLAGE IP | NOTES SUPPLÉMENTAIRES |
|--|----------------------------------|---------|-------------------|--|
| CARP (IP VIRTUELLE) | IP PARTAGÉE ENTRE LES ROUTEURS | N/A | 192.168.2.10/24 | UTILISÉE POUR LA REDONDANCE DES ROUTEURS |
| VLAN 10 - ADMIN | ADMINISTRATION | 10 | 192.168.10.0 / 24 | INCLUT LES SERVEURS AD, DNS |
| SERVEUR AD PRINCIPAL | ACTIVE DIRECTORY, DNS | 10 | 192.168.10.10/24 | SERVEUR AD PRINCIPAL ET DNS |
| SERVEUR AD SECONDAIRE | ACTIVE DIRECTORY, DNS | 10 | 192.168.10.11/24 | REDONDANCE POUR AD ET DNS |
| VLAN 20 - SERVEURS | SERVEURS | 20 | 192.168.20.0/24 | ACCÈS AUX RESSOURCES INTERNES |
| VLAN 40 - DMZ | ZONE DÉMILITARISÉE POUR EBRIGADE | 40 | 192.168.40.0/24 | HÉBERGE L'APPLICATION EBRIGADE EN SÉCURITÉ |
| SERVEUR EBRIGADE SERVEUR AD PRINCIPAL | APPLICATION EBRIGADE | 40 | 192.168.40.1/24 | ACCESSIBLE DE L'EXTÉRIEUR MAIS ISOLÉ |
| SERVEUR DE MESSAGERIE | ZIMBRA COLLABORATION SUITE | 20 | 192.168.20.3 | SERVEUR DE MESSAGERIE POUR LE DOMAINE |
| SERVEUR DE MONITORING | WAZUH (SURVEILLANCE ET ALERTES) | 20 | 192.168.20.2 | SURVEILLANCE DES INFRASTRUCTURES IT |

routeur principal





```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.85/24
LAN (lan)      -> em1      -> v4: 192.168.2.1/24
CARP1 (opt1)   -> em2      -> v4: 192.168.3.1/24
VLAN_ADMIN (opt2) -> em1.10   -> v4: 192.168.10.1/24
VLAN_SERVEURS (opt3) -> em1.20   -> v4: 192.168.20.1/24
VLAN_DMZ (opt5) -> em1.40   -> v4: 192.168.40.1/24
```

routeur secondaire

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.86/24
LAN (lan)      -> em1      -> v4: 192.168.2.2/24
CARP2 (opt1)   -> em2      -> v4: 192.168.3.2/24
VLAN_ADMIN (opt2) -> em1.10   -> v4: 192.168.10.1/24
VLAN_SERVEURS (opt3) -> em1.20   -> v4: 192.168.20.1/24
VLAN_DMZ (opt5) -> em1.40   -> v4: 192.168.40.1/24
```

CARP

Firewall / Virtual IPs ?

| Virtual IP Address | Interface | Type | Description | Actions |
|----------------------------|-----------|------|-------------|---|
| 192.168.1.250/24 (vhid: 1) | WAN | CARP | CARP-WAN |   |
| 192.168.2.254/24 (vhid: 2) | LAN | CARP | CARP-LAN |   |

+ Add

Tableau des flux du pare-feu principal 1/2

| SOURCE | DESTINATION | PORT | DESCRIPTION |
|-------------|-------------|---------|---|
| LAN | INTERNET | 80, 443 | AUTORISER L'ACCÈS HTTP/HTTPS VERS INTERNET |
| LAN | INTERNET | 25 | AUTORISER L'ENVOI DE COURRIELS SORTANTS |
| INTERNET | LAN | 80, 443 | AUTORISER LES RÉPONSES HTTP/HTTPS DEPUIS INTERNET |
| INTERNET | LAN | 587 | AUTORISER LES COURRIELS ENTRANTS VIA SMTP |
| VPN CLIENTS | LAN | 3389 | AUTORISER L'ACCÈS RDP DEPUIS LES CLIENTS VPN |
| SERVEUR WEB | INTERNET | 80, 443 | AUTORISER L'ACCÈS HTTP/HTTPS AU SERVEUR WEB |

Tableau des flux du pare-feu principal 2/2

| | | | |
|--------------|--------------|----------|---|
| SERVEUR WEB | LAN | 443 | REQUÊTES HTTPS ENTRANTES AU SERVEUR |
| DMZ | LAN | 443 | AUTORISER L'ACCÈS HTTPS DEPUIS LA DMZ |
| LAN | DMZ | 80, 443 | AUTORISER L'ACCÈS HTTP/HTTPS VERS LA DMZ |
| DMZ | INTERNET | 80, 443 | AUTORISER L'ACCÈS HTTP/HTTPS DEPUIS LA DMZ |
| SERVEUR MAIL | INTERNET | 25, 587 | AUTORISER LES CONNEXIONS SMTP SORTANTES |
| INTERNET | SERVEUR MAIL | 25, 587 | AUTORISER LES COURRIELS ENTRANTS VIA SMTP |
| SUPERVISION | LAN | 161, 162 | AUTORISER LA SUPERVISION SNMP DEPUIS LE LAN |
| LAN | SUPERVISION | 161, 162 | AUTORISER LA SUPERVISION SNMP VERS LE LAN |

Schéma réseau complet

