

# PROJET FIN DE FORMATION



## INFRA-PME

NOM : Illyes ZERGA- Alexandre LEGRAND- Anthony DERAEDT - David MOBOLE KIPONGO - Geoffrey DUYTSCHAEVER - Hatim EL HARRAK - Thomas DEMANGHON

Date : 22/09/2025-02/10/2025



**GESTION  
PROJET  
INFORMATIQUE**

# Table des Matières



01	Résumé Exécutif	P . 03
02	Contexte et Cahier des Charges	P . 04
03	Architecture Technique	P . 06
04	Services Déployés	P . 09
05	Gestion du Stockage et Sauvegardes	P . 12
06	Sécurisation de l'Infrastructure	P . 13
07	Exploitation	P . 15
08	Contribution de l'Équipe	P . 16
09	Bilan et Perspectives	P . 17
10	Conclusion	P . 18
11	Annexes Techniques	P . 19

# Résumé Exécutif

Dans le cadre de l'ouverture de la société PME Sport & Loisirs, spécialisée dans la vente d'articles de sport, nous avons mené un projet visant à doter l'entreprise d'une infrastructure informatique moderne, fiable et sécurisée.

Dès le départ, notre objectif a été clair : fournir aux 38 collaborateurs, qu'ils soient au siège, en déplacement ou en télétravail, un environnement de travail performant, simple d'utilisation et sécurisé.

L'équipe projet a conçu et mis en place une infrastructure virtualisée intégrant l'ensemble des services indispensables à leur activité :

- Un système centralisé de gestion des utilisateurs et des accès, garantissant simplicité et sécurité.
- Des outils collaboratifs (messagerie, téléphonie, intranet, partage documentaire) pour fluidifier la communication et le travail en équipe.
- Un dispositif de supervision et de sauvegarde assurant la continuité d'activité et la résilience face aux incidents.
- Une sécurité renforcée, reposant sur un pare-feu dédié et une segmentation du réseau, afin de protéger nos données et celles de nos clients.

# Contexte et Cahier des Charges

## Contexte de l'Entreprise

PME Sport & Loisirs est une société en cours d'ouverture, composée de 38 employés.

Elle est spécialisée dans la vente d'articles de sport et s'appuie sur :

- Un siège social regroupant la direction et l'administration.
- Une équipe de vente sur site et en magasin.
- Des commerciaux nomades et employés en télétravail nécessitant un accès distant sécurisé.

Dès son lancement, l'entreprise doit disposer d'une infrastructure informatique robuste, capable de soutenir sa croissance et de garantir la continuité de service.

## Besoins Exprimés

- Centralisation de la gestion des utilisateurs et des ressources (Active Directory, GPO).
- Services collaboratifs fiables : messagerie, téléphonie interne, partage documentaire, intranet.
- Sécurité renforcée : segmentation réseau, firewall, supervision, sauvegardes régulières.
- Accessibilité pour tous : connexion sécurisée pour les salariés en mobilité et en télétravail.
- Évolutivité : infrastructure conçue pour supporter des extensions futures (cloud, PRA avancé, SIEM).

## Contraintes Techniques et Matérielles

- Pas de nouvelles machines physiques → l'infrastructure doit être déployée sur les ressources fournie par l'entreprise.
- Matériel disponible :
  - 2 serveurs Dell PowerEdge R620.
  - 1 Switch L3.
  - 1 pare-feu pfSense.
  - 1 SAN iSCSI pour stockage et sauvegardes.
  - Virtualisation via VMware ESXi et vCenter.

# Objectifs Pédagogiques et Opérationnels

## **Objectifs pédagogiques :**

- Mettre en pratique les compétences acquises (réseau, systèmes, sécurité, virtualisation).
- Travailler en mode projet, avec une répartition claire des rôles.
- Produire une documentation professionnelle exploitable par un client/DSI.

## **Objectifs opérationnels :**

- Concevoir et déployer une infrastructure fiable, sécurisée et prête à l'emploi.
- Répondre aux besoins métiers de la PME dès son ouverture.
- Garantir la productivité des collaborateurs et la sécurité des données.

# Architecture Technique

## Schéma Global de l'Infrastructure

L'architecture repose sur une infrastructure virtualisée garantissant sécurité, performance et évolutivité.

Elle est composée de :

1

Deux serveurs physiques  
Dell PowerEdge R620  
hébergeant l'hyperviseur  
VMware ESXi.

2

Un vCenter pour la gestion  
centralisée des machines  
virtuelles et des ressources.

3

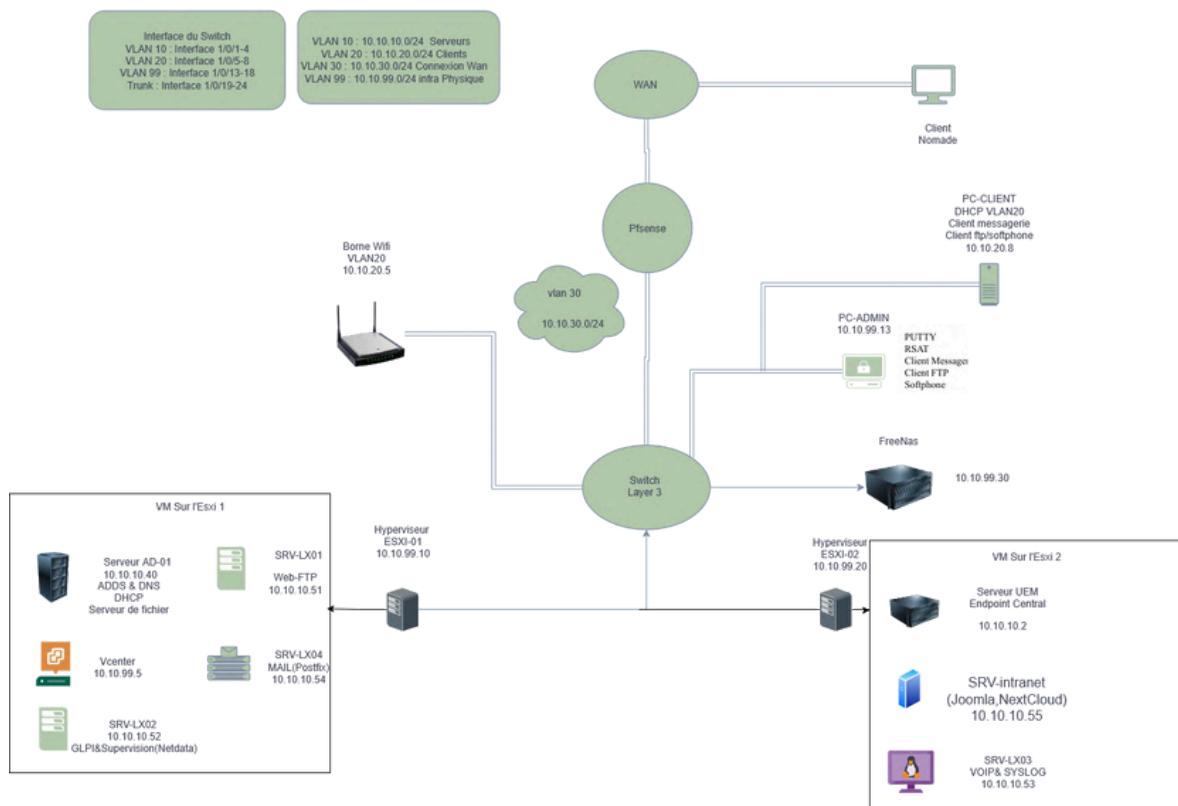
Un SAN iSCSI pour le  
stockage des données, les  
sauvegardes et les  
snapshots.

4

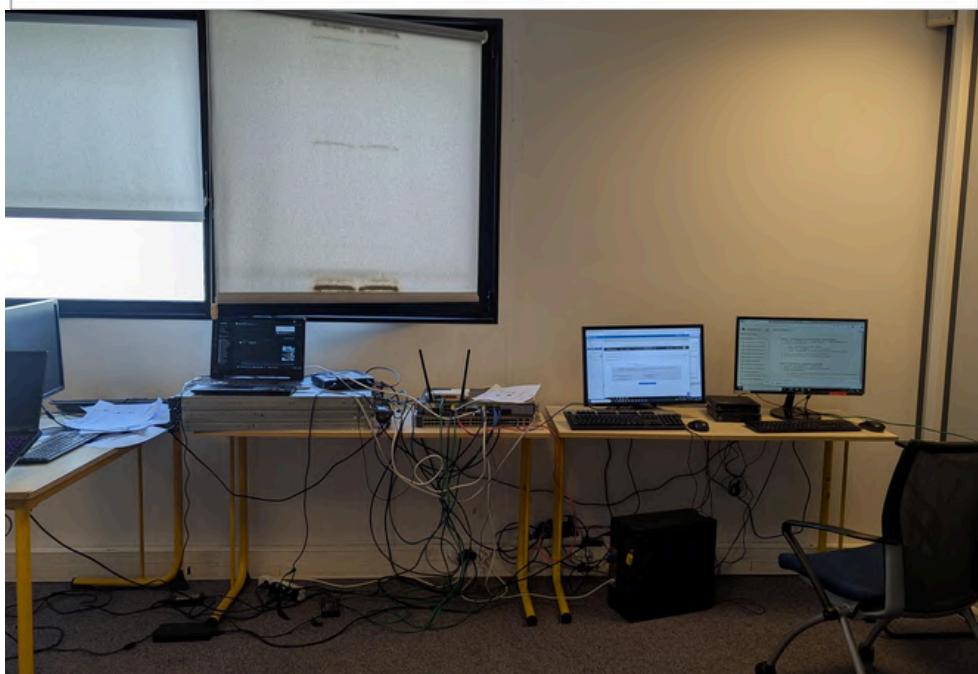
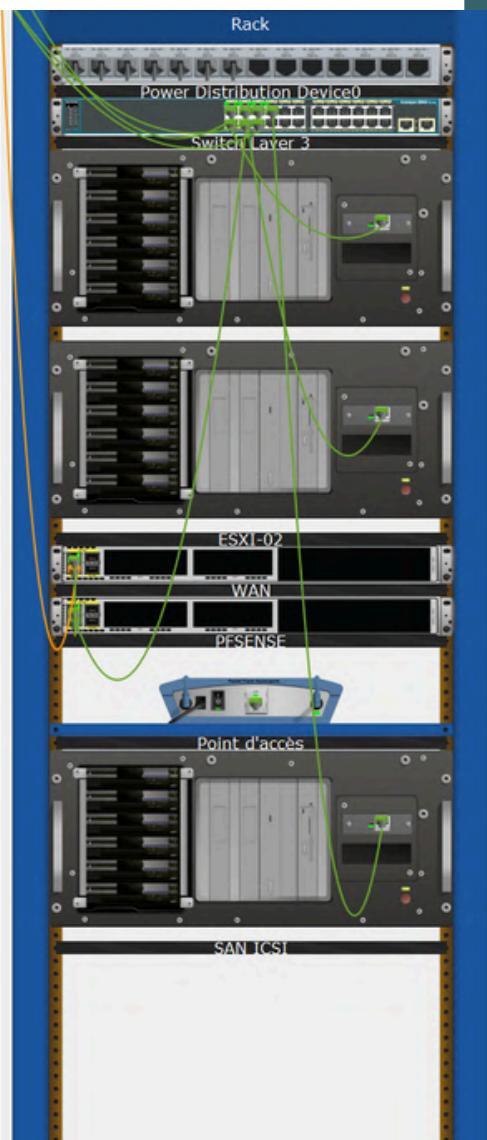
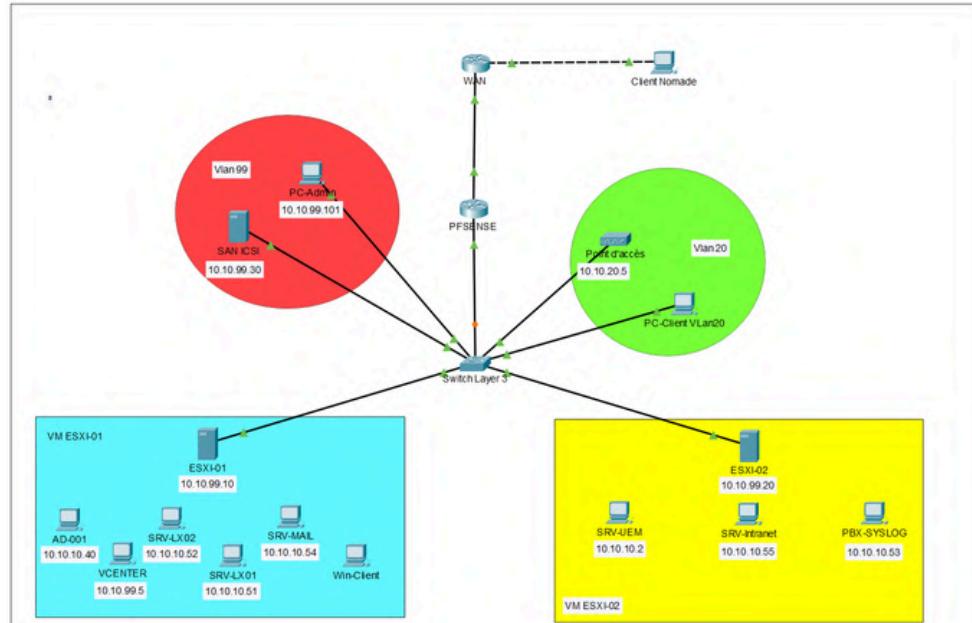
Un Switch L3 pour la  
segmentation du réseau et la  
inter-connectivité des  
équipements.

5

Un pare-feu pfSense en  
frontal, pour le routage inter-  
VLAN et protégeant  
l'infrastructure et gérant les  
accès Internet/VPN.



# Plan Logique et Physique



## Réseau et Vlans

La segmentation réseau a été conçue pour séparer les flux selon leur usage et renforcer la sécurité.

VLAN	Nom	Usage	Plage IP
10	Serveurs	AD, GLPI, Messagerie, Web, VoIP, Intranet	10.10.10.0/24
20	Clients	Postes utilisateurs (filaire + Wi-Fi)	10.10.20.0/24
30	WAN	Accès Internet	10.10.30.0/24
99	Infra	Hyperviseurs ESXi, SAN, vCenter	10.10.99.0/24

## Virtualisation (ESXi + vCenter)

- L'ensemble des services est déployé dans des machines virtuelles (VMs) hébergées sous VMware ESXi.
- Le vCenter permet une administration centralisée, avec les avantages suivants :
- Haute disponibilité : possibilité de répartir et déplacer les VMs entre hôtes.
- Flexibilité : création et restauration rapide de VMs.
- Gestion simplifiée : interface unique pour superviser l'infrastructure.

# Service déployés



## Active Directory, DNS et DHCP

⌚ Objectif : centraliser la gestion des utilisateurs, des postes et des ressources.

⚙ Description : déploiement d'Active Directory avec intégration DNS et DHCP. GPO mises en place pour appliquer des politiques de sécurité et uniformiser la configuration des postes.

💡 Valeur pour l'entreprise : simplicité de gestion, sécurité renforcée, authentification unique (SSO) pour tous les collaborateurs.



## Serveur de Fichiers

⌚ Objectif : offrir un espace centralisé pour le stockage et le partage des données.

⚙ Description : configuration d'un serveur dédié aux partages, avec gestion fine des droits par groupes d'utilisateurs.

💡 Valeur pour l'entreprise : accès rapide et sécurisé aux documents, réduction des risques liés au stockage local non contrôlé.



## Messagerie (Postfix + RainLoop)

⌚ Objectif : fournir une solution de communication interne et externe.

⚙ Description : installation d'un serveur Postfix/Dovecot pour l'envoi/réception, couplé à RainLoop comme webmail simple et moderne. Connexions sécurisées via TLS/SSL.

💡 Valeur pour l'entreprise : fluidité des échanges, accès aux mails depuis n'importe où, compatibilité avec smartphones et clients de messagerie.



## Téléphonie VoIP (FreePBX)

⌚ Objectif : centraliser la gestion des utilisateurs, des postes et des ressources.

⚙️ Description : déploiement d'Active Directory avec intégration DNS et DHCP. GPO mises en place pour appliquer des politiques de sécurité et uniformiser la configuration des postes.

💡 Valeur pour l'entreprise : simplicité de gestion, sécurité renforcée, authentification unique (SSO) pour tous les collaborateurs.

## GLPI (Gestion IT)



⌚ Objectif : gérer le parc informatique et les demandes utilisateurs.

⚙️ Description : mise en place de GLPI pour l'inventaire des équipements, la gestion des tickets et des réservations de ressources.

💡 Valeur pour l'entreprise : meilleur suivi des actifs, traçabilité des demandes, amélioration du support IT.



## Supervision (NetData + Syslog)

⌚ Objectif : superviser l'infrastructure et centraliser les événements.

⚙️ Description : NetData déployé pour surveiller serveurs et équipements, avec alertes configurées. Syslog pour regrouper les logs système et sécurité.

💡 Valeur pour l'entreprise : détection proactive des incidents, diagnostic rapide, continuité de service renforcée.



## Intranet Joomla & Nextcloud

🎯 Objectif : améliorer la collaboration et le partage d'informations.

⚙️ Description : intranet Joomla pour la communication interne (actualités, documents) et Nextcloud pour le partage et la synchronisation des fichiers.

💡 Valeur pour l'entreprise : meilleure communication interne, accès distant sécurisé pour les nomades et télétravailleurs.

## UEM (ManageEngine)



🎯 Objectif : administrer la flotte mobile de l'entreprise.

⚙️ Description : installation d'un solution UEM pour gérer smartphones et tablettes, appliquer des politiques de sécurité et effacer les données à distance si besoin.

💡 Valeur pour l'entreprise : protection accrue des données, gestion simplifiée des appareils, conformité avec les bonnes pratiques de sécurité.

# Gestion du Stockage et Sauvegardes

## San iSCSI

1

- Objectif : protéger les données contre les pertes, erreurs humaines ou incidents matériels.
- Description :
  - Sauvegardes quotidiennes et hebdomadaires planifiées sur le SAN.
  - Conservation de plusieurs versions pour revenir en arrière en cas de corruption.
  - Intégration avec snapshots VMware pour optimiser les sauvegardes.
- Valeur : sécurisation des données critiques et garantie de reprise rapide après incident.

## Politique de Sauvegarde

2

- Objectif : protéger les données contre les pertes, erreurs humaines ou incidents matériels.
- Description :
  - Sauvegardes quotidiennes et hebdomadaires planifiées sur le SAN.
  - Conservation de plusieurs versions pour revenir en arrière en cas de corruption.
  - Intégration avec snapshots VMware pour optimiser les sauvegardes.
- Valeur : sécurisation des données critiques et garantie de reprise rapide après incident.

## Snapshots et Restauration

3

- Objectif : permettre un retour rapide en cas de panne ou de mauvaise manipulation.
- Description :
  - Snapshots réguliers des VMs critiques (AD, GLPI, Messagerie, VoIP).
  - Procédures de restauration testées.
  - Restauration avant une mise à jour majeure ou une modification sensible.
- Valeur : réduction du temps d'interruption et sécurisation des évolutions.

# Sécurisation de l'Infrastructure

## 1. Sécurité Réseau

- Objectif : protéger l'infrastructure contre les menaces externes et internes.
- Description :
  - Segmentation par VLANs (Serveurs, Clients, WAN, Infra).
  - Pare-feu pfSense en frontal : filtrage des flux, NAT, VPN pour télétravail/nomades.
  - Règles spécifiques pour limiter les accès.
- Valeur : isolation des flux critiques, meilleure maîtrise de la surface d'attaque.

## 2. Sécurité des Hyperviseurs et Serveurs

- Objectif : sécuriser la base de l'infrastructure virtuelle.
- Description :
  - Authentification intégrée à l'AD pour vCenter et services critiques.
  - Certificats SSL/TLS pour sécuriser les interfaces d'administration.
  - Durcissement systèmes (patches réguliers, services inutiles désactivés).
  - GPO pour uniformiser la sécurité des postes clients.
- Valeur : réduction du risque d'intrusion et homogénéité des configurations.

## 3. Sécurité des Services

- Objectif : protéger les applications critiques et communications.
- Description :
  - Messagerie : TLS/SSL, authentification sécurisée, futur antispam.
  - VoIP : chiffrement SRTP, restrictions internes.
  - FTP : bascule vers FTPS.
  - Nextcloud & Joomla : accès HTTPS obligatoire, MFA en option.
- Valeur : communication et collaboration sécurisées, conformité aux bonnes pratiques.

## 4. PRA / PCI (Plan de Reprise et de Continuité)

- Objectif : garantir la continuité d'activité en cas d'incident majeur.
- Description :
  - Sauvegardes centralisées sur SAN iSCSI.
  - Snapshots réguliers des VMs critiques.
  - Procédures de restauration testées.
- Valeur : reprise rapide après incident, réduction des pertes de données.

## 5. Supervision et Logs

- Objectif : détecter rapidement incidents et anomalies.
- Description :
  - NetData : surveillance proactive (CPU, RAM, réseau, services).
  - Syslog : centralisation des journaux système et sécurité.
  - Alertes configurées pour notifications en temps réel.
- Valeur : détection préventive, diagnostic accéléré, amélioration de la disponibilité.

## 6. Perspectives d'Amélioration

- Déploiement futur d'un SIEM (Wazuh) pour détection avancée.
- Mise en place d'un antispam renforcé.
- Installation de la sauvegarde 3-2-1.
- Création de nouvelles GPO pour les utilisateurs du domaine.

# Exploitation

## Checklists d'Administration

01



Pour garantir la stabilité et la sécurité de l'infrastructure, des checklists d'exploitation ont été définies :

- Quotidien :
  - Vérification de la supervision NetData (alertes, performances).
  - Contrôle de la messagerie (file d'attente Postfix, disponibilité RainLoop).
  - Suivi de l'utilisation CPU/RAM sur les serveurs critiques.
- Hebdomadaire :
  - Vérification des sauvegardes SAN (logs, tests de restauration).
  - Contrôle de l'espace disque sur serveurs et SAN.
  - Analyse des journaux Syslog pour détection d'anomalies.
- Mensuel :
  - Tests de restauration de snapshots.
  - Application des mises à jour systèmes et correctifs de sécurité.
  - Vérification de la cohérence des GPO et des comptes utilisateurs.

## Procédures d'Incident

02



- Perte d'AD / DNS → restauration rapide depuis snapshots.
- Incident messagerie → vérification Postfix/Dovecot, bascule sur sauvegarde.
- Panne VoIP → test VM FreePBX, reconfiguration via fichiers de backup.
- Intrusion / alerte sécurité → isolement VLAN concerné, analyse Syslog et NetData, escalade vers équipe sécurité.

# Contributions de l'Équipe

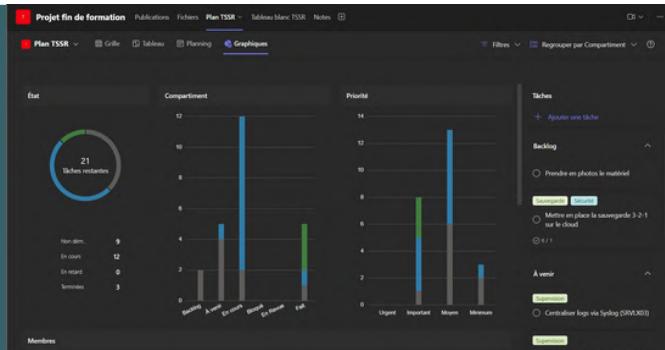
Le projet a été mené en équipe, chaque membre ayant pris en charge des responsabilités précises.

Cette répartition a permis une progression équilibrée et une montée en compétences collective.

Membre	Rôle	Contribution Clé
Illyes	Chef de Projet	Gestion d'équipe et équipement
Alexandre	Technicien	vCenter - Serveur Mail
Anthony	Technicien	ADDS - vCenter
David	Technicien	Serveur VOIP/Syslog
Geoffrey	Technicien	Serveur Intranet
Hatim	Technicien	Serveur UEM
Thomas	Technicien	Documentation - Serveur Mail

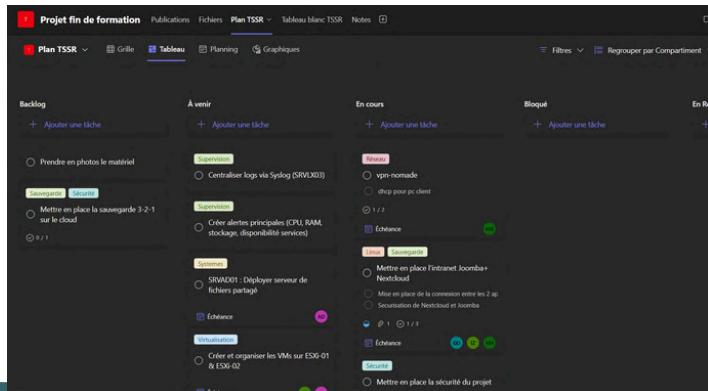
## Temps et Organisation

- ~45 heures de travail collectif, réparties sur deux semaines.
- Sessions de travail en groupe pour les jalons clés (mise en place VLANs, AD, messagerie).
- Utilisation d'outils collaboratifs (Teams) pour le suivi et le partage.



The screenshot shows a table of tasks with the following columns:

Nom de la tâche	Affectation	Date de début	Date d'échéance	Compartiment	Progression	Priorité	Deuxes
Définir la planification et les rôles du groupe	Illyes ZERGA	22/9/2025	22/9/2025	Fait	Terminées	Moyen	Opérations
Architecture réseau	Hatim EL HARI	22/9/2025	22/9/2025	Fait	Terminées	Important	Réseau
Installer SWAN001 (AD/VOIP/DCP/Windows)	Anthony DEP	22/9/2025	22/9/2025	Fait	Terminées	Important	Systèmes
Rédiger rapport final		22/9/2025	2/10/2025	En cours	En cours	Important	+
Créer VLAN 10/20/30/99 et configurer inter-VLAN		22/9/2025	22/9/2025	Fait	Terminées	Important	Réseau
Déployer vCenter Appliance + VLAN 99				Fait	En cours	Important	Supervision
Configurer détecteurs SAN (ESX-01 & -02)				Fait	Terminées	Moyen	Linux
SRVX03 : installer VoIP (freepbx + Syslog)				En cours	En cours	Moyen	Linux
SRVX04 : installer serveur mail (Postfix)				En cours	En cours	Moyen	Linux
SRVX05 : installer CMS web (HTWK/HTPS + FIPS)	Thomas DEMP	22/9/2025	22/9/2025	En cours	En cours	Moyen	Supervision
SRVX06 : installer GUI + Nfdatas (supervision)	Geoffrey DUY	23/9/2025	23/9/2025	En cours	En cours	Moyen	Supervision
Créer et organiser les VMs sur ESX-01 & ESX-02				À venir	Non demandé	Minimum	+
SRVAD01 : Déployer serveur de fichiers partagé				À venir	Non demandé	Moyen	Systèmes
SRVAD02 : Déployer serveur de fichiers partagé	Anthony DEP			À venir	Non demandé	Moyen	Systèmes



# Bilan & Perspectives

## Difficultés Rencontrées

1. Configuration du routage inter-Vlan sur le Switch.
2. Difficulté liée aux services utilisant le même port.
3. Obstacles à la mise en œuvre du serveur UEM.

## Solutions Apportées

1. Mettre en place le routage inter-Vlan sur le pfSense.
2. Implémentation de l'enregistrement DNS via l'ADDS et production des certificats par pfSense.
3. Déploiement d'EndPoint Manager pour rendre l'installation d'un serveur UEM plus aisée.

## Points Forts du Projet

1. Collaboration d'équipe qui s'est dans l'ensemble bien passée.
2. L'esprit d'équipe perdure, même face aux problèmes liés aux outils et matériels.
3. Capacité à suggérer des idées novatrices pour enrichir le projet.

## Pistes d'Amélioration et Perspectives

1. Infrastructures limitées et équipements à moderniser.
2. Optimisation de la gestion du temps en période de crise.

# Conclusion



Nous tenons à remercier chaleureusement la PME Sport & Loisirs pour sa confiance tout au long de ce projet.

Notre équipe a travaillé avec rigueur et collaboration afin de concevoir et mettre en œuvre une infrastructure moderne, performante et sécurisée, répondant aux besoins exprimés et anticipant la croissance future de l'entreprise.

L'ensemble des services prévus (gestion centralisée des utilisateurs, messagerie, téléphonie, supervision, intranet, stockage et sauvegardes) est désormais opérationnel. L'infrastructure est pleinement fonctionnelle et permet dès à présent aux collaborateurs d'exercer leurs activités dans un environnement fiable et sécurisé.

Nous sommes conscients que certains éléments restent à finaliser ou à renforcer, notamment :

- la mise en place complète des stratégies de groupe (GPO) dans l'Active Directory,
- l'optimisation des règles de sécurité avancées (antispam, SIEM),
- Mise en place de la sauvegarde 3-2-1
- Compléter la checklist administration

Ces éléments font déjà partie de notre plan de suivi, et seront intégrés dans les plus brefs délais afin de compléter et renforcer l'infrastructure déployée.

En conclusion, ce projet a été une opportunité d'appliquer nos compétences techniques et organisationnelles dans un cadre professionnel réaliste. Nous sommes fiers d'avoir livré une solution robuste et évolutive à la PME Sport & Loisirs, et restons engagés à accompagner l'entreprise dans ses évolutions futures.



**GESTION  
PROJET  
INFORMATIQUE**

# Annexes technique

01	Installation de VCAS	P . 20
02	Mise en place de VMotion	P . 27
03	Configuration TP-Link	P . 30
04	Configuration Règle / Certificat pfSense	P . 33
05	Configuration Switch Cisco L3	P . 39
06	Configuration Server ADDS	P . 41
07	Configuration Serveur WEB	P . 44
08	Installation / Configuration GLPI - NetData	P . 52
09	Installation Joomla / NextCloud	P . 58
10	Mise en place Syslog / FreePBX	P . 64
11	UEM – ManageEngine Endpoint Central	P . 72
11	Installation et Configuration FreeNas	P . 75
11	Configuration OpenVPN	P . 80

# Installation de VCAS - Déploiement de L'OVA - Alexandre / Anthony

Pré-requis :

- Image ISO ou OVA de VCAS (6.7.0)
- Accès à un hôte ESXi ou vSphere Client : ESXI-01 ; EXSI-02
- Informations réseau disponibles (IP, masque, passerelle, DNS, FQDN)
- Comptes et permissions nécessaires

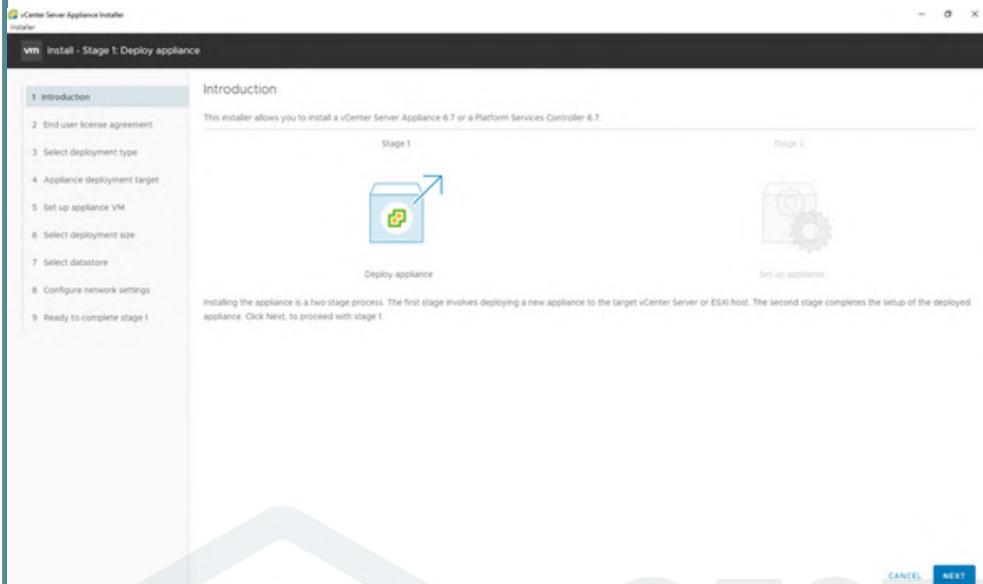
## 1. Lancement de l'installateur

Ouverture de l'ISO et le lancement de l'installateur via monter le disque.

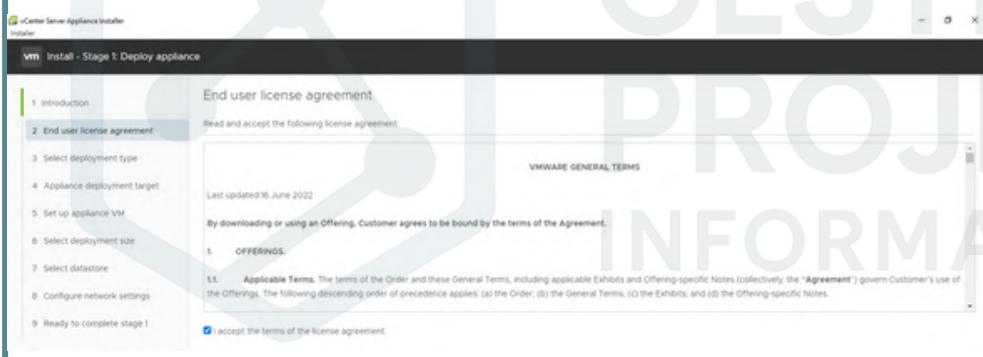
dbschema	25/09/2022 00:22	File folder	
migration-assistant	25/09/2022 00:22	File folder	
umds	25/09/2022 00:22	File folder	
vcsa	25/09/2022 00:22	File folder	
vcsa-cli-installer	25/09/2022 00:22	File folder	
<b>vcsa-ui-installer</b>	<b>25/09/2022 00:22</b>	<b>File folder</b>	
readme.txt	24/09/2022 23:36	Text Document	
readme-de.txt	24/09/2022 23:36	Text Document	
readme-es.txt	24/09/2022 23:36	Text Document	
readme-fr.txt	24/09/2022 23:36	Text Document	
readme-ja.txt	24/09/2022 23:36	Text Document	
readme-ko.txt	24/09/2022 23:36	Text Document	
readme-zh-CN.txt	24/09/2022 23:36	Text Document	
readme-zh-TW.txt	24/09/2022 23:36	Text Document	
locales	25/09/2022 00:22	File folder	
resources	25/09/2022 00:22	File folder	
swifshader	25/09/2022 00:22	File folder	
chrome_100_percent.pak	15/09/2022 13:53	PAK File	146 kB
chrome_200_percent.pak	15/09/2022 13:53	PAK File	215 kB
d3dcompiler_47.dll	15/09/2022 13:53	Application extens...	3 628 kB
ffmpeg.dll	15/09/2022 13:53	Application extens...	2 567 kB
icudtl.dat	15/09/2022 13:53	DAT File	10 044 kB
<b>installer.exe</b>	<b>15/09/2022 13:53</b>	<b>Application</b>	<b>125 394 kB</b>
libEGL.dll	15/09/2022 13:53	Application extens...	387 kB
libGLESv2.dll	15/09/2022 13:53	Application extens...	6 157 kB
LICENSE	15/09/2022 13:53	File	2 kB
LICENSES.chromium.html	15/09/2022 13:53	Microsoft Edge H...	5 428 kB
resources.pak	15/09/2022 13:53	PAK File	4 994 kB
snapshot_blob.bin	15/09/2022 13:53	BIN File	280 kB
v8_context_snapshot.bin	15/09/2022 13:53	BIN File	593 kB
version	15/09/2022 13:53	File	1 kB
vk_swifshader.dll	15/09/2022 13:53	Application extens...	4 033 kB
vk_swifshader_icd.json	15/09/2022 13:53	JSON File	1 kB
vulkan-1.dll	15/09/2022 13:53	Application extens...	762 kB

## 2. Sélection du type d'installation

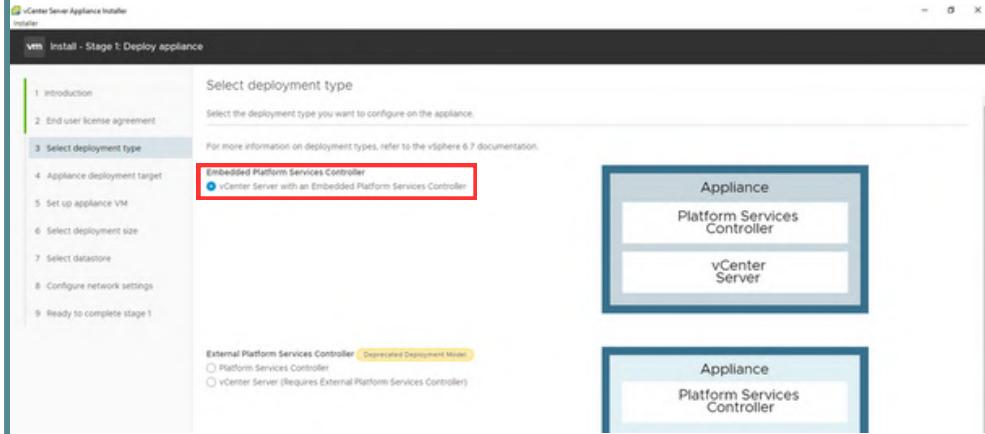
Choix : Nouveau vCenter Server Appliance puis “next”.



Confirmer les engagements utilisateurs puis “next”.

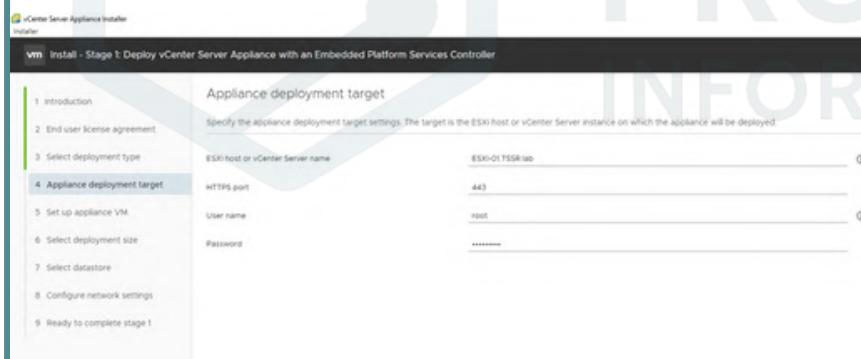


### 3. Sélection du type d'installation



### 4. Ciblage de l'hôte ESXI

- Adresse IP / login de l'hôte cible
- Acceptation du certificat SSL
- Mot de passe administrateur de l'EXSI



## 5. Paramètres de la VM VCENTER

- Nom de la machine virtuelle
- Mot de passe administrateur

Set up vCenter Server VM

Specify the VM settings for the vCenter Server to be deployed.

VM name: VCSCA

Set root password:

Confirm root password:

Configure network settings

Configure network settings for this appliance

Network: VLAN99

IPv4: static

FQDN (optional): 10.10.99.5

Subnet mask or prefix length: 255.255.255.0

Default gateway: 10.10.99.254

DNS servers: 10.10.10.40

Common Ports:

HTTP: 80

HTTPS: 443

## 6. Paramètres de la VM

- Nom de la machine virtuelle
- Mot de passe administrateur
- Taille de déploiement (Tiny, Small, Medium, Large)

vmw Install - Stage 1: Deploy vCenter Server

Select deployment size

Select the deployment size for this vCenter Server.

For more information on deployment sizes, refer to the vSphere 8.0 documentation.

Deployment size: Tiny

Storage size: Default

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	14	579	10	100
Small	4	21	694	100	1000
Medium	8	30	908	400	4000
Large	16	39	1358	1000	10000
X-Large	24	58	2263	2000	35000

## 7. Sélection du Datastore

- Sélectionner le bon DataStore (iSCSI-Data)

The screenshot shows the 'vCenter Server Installer' interface for 'Stage 1: Deploy vCenter Server'. The left sidebar lists steps 1 through 8, with step 6 ('Select datastore') currently selected. The main panel is titled 'Select datastore' and contains the instruction 'Select the storage location for this vCenter Server'. A checkbox 'Show only compatible datastores' is checked. Below it is a table with columns: Name, Type, Capacity, Free, Provisioned, and Thin Provisioning. A single item is listed in the table. At the bottom, there is a checkbox 'Enable Thin Disk Mode' which is also checked.

## 8. Configuration Réseau

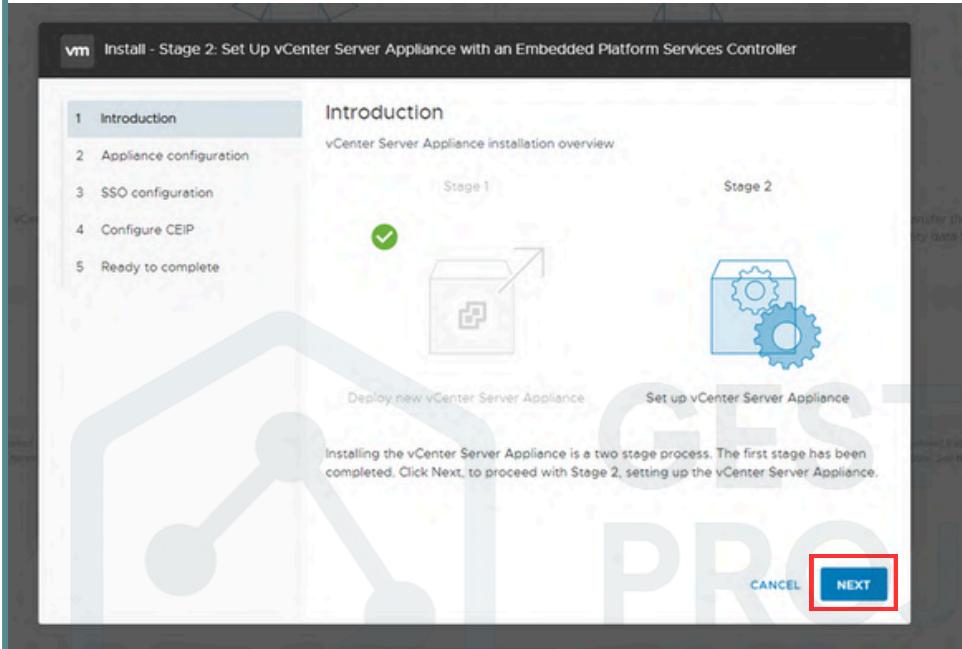
- Ip Statique
- Masque
- Passerelle
- DNS
- FQDN

The screenshot shows the 'vCenter Server Installer' interface for 'Stage 1: Deploy vCenter Server'. The left sidebar lists steps 1 through 8, with step 8 ('Ready to complete stage 1') currently selected. The main panel is titled 'Ready to complete stage 1' and contains a summary of deployment settings. It includes sections for 'Deployment Details' (Target ESXi host: VCSE), 'Datastore Details' (Datastore, Disk mode: Default), and 'Network Details' (Network: VM Network, IP settings: IPv4, static, IP address: 192.168.1.10, Subnet mask or prefix length: 255.255.255.0, Default gateway: 192.168.1.1, DNS servers: 8.8.8.8, HTTP Port: 80, HTTPS Port: 443).

# Installation de VCAS - Configuration de l'Appliance - Alexandre / Anthony

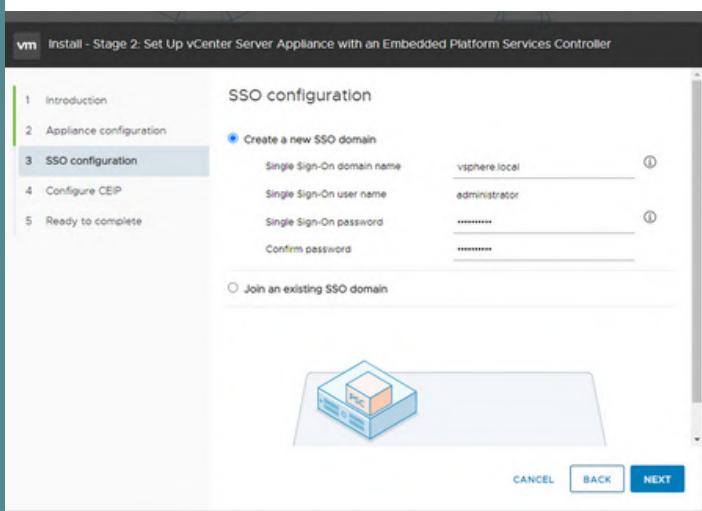
## 1. Accès à l'assistant de configuration

- Introduction à la phase 2 :



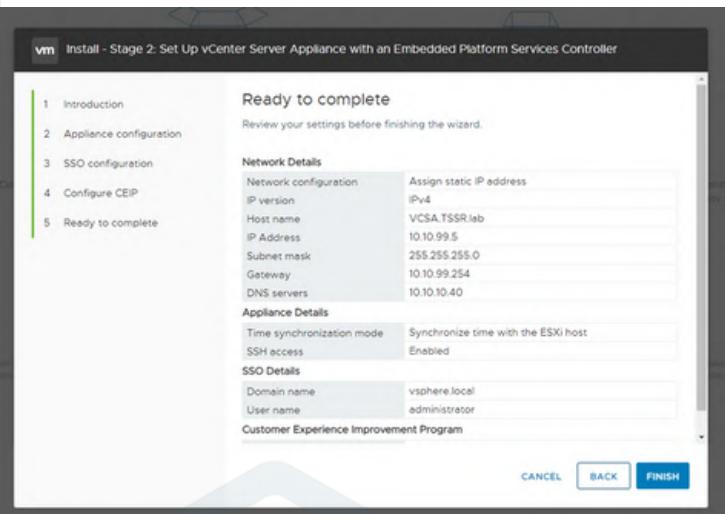
## 2. Configuration du SSO

- Domaine SSO (par défaut : vsphere.local)
- Mot de passe administrateur
- Intégration éventuelle à Active Directory



### 3. Finalisation

- Validation des paramètres
- Redémarrage éventuel de l'appliance



#### Accès à l'interface vSphere

- URL d'accès : [https://<FQDN\\_vccenter>/ui](https://<FQDN_vccenter>/ui)
- Connexion avec administrator@vsphere.local

The screenshot shows the VMware website with a blue header. Below it, a section titled 'Démarrage' contains a message about the obsolescence of the Flash-based vSphere Web Client and a recommendation to use the modern HTML5-based vSphere Client. It features two large buttons: 'LANCER VSPPHERE CLIENT (HTML5)' in blue and 'LANCER VSPPHERE WEB CLIENT (FLEX)' in white with red text. A note next to the second button says 'Obsolète'. Below these buttons, there's a 'Documentation' section with links to the 'Centre de documentation VMware vSphere' and 'Mises à jour des fonctionnalités de vSphere Client (HTML5)'.

# Mise en place de vMotion - Alexandre

Pré-requis :

- Un vCenter Server installé et opérationnel.
- Deux hôtes ESXi configurés et intégrés dans vCenter.
- Un datastore partagé entre les hôtes (NFS, iSCSI, SAN).
- Un réseau VMkernel dédié pour le trafic vMotion.
- Licence vSphere adaptée (Enterprise Plus).

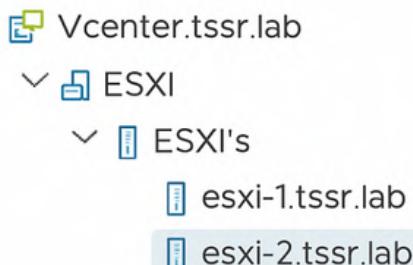
## 1. Configuration du réseau vMotion

- Créer un port VMkernel dédié au vMotion.
- Définir une IP statique sur chaque hôte ESXi.
- Activer l'option "vMotion traffic" sur l'adaptateur réseau.



## 2. Activation du service vMotion

- Dans vSphere Client, aller dans ESXi → Configure → VMkernel adapters.
- Sélectionner l'adaptateur → cocher vMotion traffic.
- Sauvegarder la configuration.



### 3. Test de migration à chaud

- Faire un clic droit sur une VM → Migrate.
- Choisir Change compute resource only.
- Sélectionner l'hôte ESXi cible et valider.

Win-client - Migrer

✓ 1 Sélectionner un type de...  
✓ 2 Sélectionner une ressourc...  
**3 Sélectionner un stockage**  
5 Sélectionner les réseaux  
6 Prêt à terminer

Sélectionner un stockage  
Sélectionnez le stockage de destination pour la migration de la machine virtuelle.

Origine de la machine virtuelle ⓘ

Sélectionner un format de disque virtuel :  Même format que la source  Configurer par disque

Stratégie de stockage VM :  Conserver les règles de stockage VM existantes

Nom	Capacité	Provisionné	Libre	Type	Cluster
datastore1 (1)	550,75 Go	387,93 Go	454,82 Go	VMFS 6	
san-iscsi	279,75 Go	313,06 Go	245,25 Go	VMFS 6	

Compatibilité

Win-client  
esxi-01.tssr.lab  
⚠ "Périphérique" « CD/DVD drive 1 » utilise un support « [datastore1] Win10\_22H2\_French\_x64vt.iso », qui n'est pas accessible.

Win-client - Migrer

✓ 1 Sélectionner un type de...  
✓ 2 Sélectionner une ressourc...  
✓ 3 Sélectionner un stockage  
**5 Sélectionner les réseaux**  
6 Prêt à terminer

Sélectionner les réseaux  
Sélectionnez les réseaux de destination pour la migration de la machine virtuelle.

Origine de la machine virtuelle ⓘ

Migrez une mise en réseau VM en sélectionnant un nouveau réseau de destination pour tous les adaptateurs réseau VM attachés au même réseau source.

Réseau source	Utilisé par	Réseau de destination
VLAN10	1 VM / 1 Adaptateurs réseau	VLAN10

Compatibilité

Win-client  
esxi-01.tssr.lab  
⚠ "Périphérique" « CD/DVD drive 1 » utilise un support « [datastore1] Win10\_22H2\_French\_x64vt.iso », qui n'est pas accessible.

Win-client - Migrer

✓ 1 Sélectionner un type de...  
✓ 2 Sélectionner une ressourc...  
✓ 3 Sélectionner un stockage  
✓ 5 Sélectionner les réseaux  
**6 Prêt à terminer**

Prett à terminer  
Vérifiez que les informations sont correctes et cliquez sur Terminer pour commencer la migration.

Origine de la machine virtuelle ⓘ

Type de migration	Modifier la ressource de calcul et le stockage
Machine virtuelle	Win-client
Cluster	ESXi's
Hôte	esxi-01.tssr.lab
Stockage	datastore1 (1)
Format de disque	Même format que la source
Réseaux	Aucune réaffectation réseau

## 4. Vérification finale

- Suivre la tâche dans Recent Tasks du vCenter.
- Vérifier que la VM a bien basculé sur le nouvel hôte sans interruption de service.

The screenshot shows the VMware vSphere interface with two windows side-by-side:

**Left Window (VM Details):**

- Summary Tab:** Shows the VM is "Hors tension".
  - Guest OS: Microsoft Windows 10 (64-bit)
  - Compatibility: ESXi 6.7 et versions ultérieures (VM version 14)
  - VMware Tools: Non exécuté, non installé
- Actions Tab:** Includes "Lancer la console Web" and "Lancer Remote Console".
- Associated Objects:** Lists Cluster (EXSi's), Host (esxi-02.tssr.lab), Networks (VLAN10), and Storage (datastore1).
- Recent Tasks:** Shows a task named "Replacer la machine virtuelle" initiated by "VSPIHERE.LOCAL\Administr..." with a status of 31%.

**Right Window (VM Details):**

- Summary Tab:** Shows the VM is "Hors tension".
  - Guest OS: Microsoft Windows 10 (64-bit)
  - Compatibility: ESXi 6.7 et versions ultérieures (VM version 14)
  - VMware Tools: Non exécuté, non installé
- Actions Tab:** Includes "Lancer la console Web" and "Lancer Remote Console".
- Associated Objects:** Lists Cluster (EXSi's), Host (esxi-01.tssr.lab), Networks (VLAN10), and Storage (datastore1).
- Recent Tasks:** Shows a task named "Replacer la machine virtuelle" initiated by "VSPIHERE.LOCAL\Administr..." with a status of "Terminée".

A large watermark reading "GESTION PROJET INFORMATIQUE" is overlaid across the bottom of the interface.

# Configuration TP-Link TL-WR841N en Point d'Accès - Hatim / Alexandre

## Pré-requis

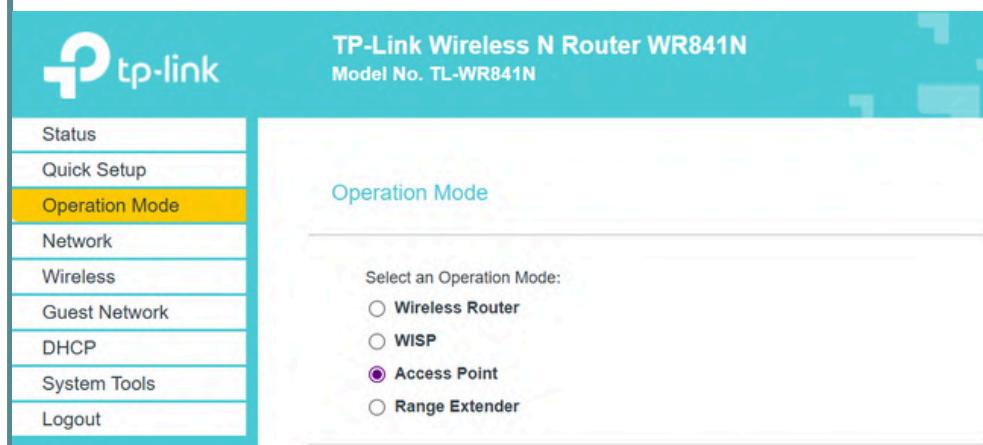
- Modèle : TP-Link TL-WR841N
- Accès à un PC relié en câble au port LAN du TP-Link
- Identifiants par défaut : admin / admin
- VLAN20 configuré sur le réseau

## 1. Préparation

- Brancher le PC sur un port LAN du TL-WR841N.
- Accéder à l'interface web via 192.168.0.1 ou 192.168.1.1.
- Se connecter avec les identifiants par défaut.

## 2. Mise en mode Point d'Accès

- Menu : System Tools → Operation Mode
- Choisir : Access Point
- Le routeur redémarre automatiquement.
- Cela désactive NAT, DHCP et le port WAN.



### 3. Configuration réseau

- Définir une IP fixe : 10.10.20.20
- Masque : 255.255.255.0
- Passerelle : 10.10.20.1 (routeur VLAN20)
- DHCP : déjà désactivé (mode AP).

#### LAN Settings

LAN Type: **Static IP**

Note: The IP parameters can be set to Smart IP(DHCP) (In this situation the device will automatically assign an IP address as you need).

MAC Address: E4:C3:2A:4E:7A:84  
IP Address: **10.10.20.5**  
Subnet Mask: **255.255.255.0**

### 4. Configuration Wi-Fi

- Menu : Wireless Settings
- SSID : WiFi\_VLAN20 (au choix)
- Sécurité : WPA2-PSK (AES)
- Mot de passe : fort

**TP-Link Wireless N Router WR841N**  
Model No. TL-WR841N

**Wireless Settings**

Status Quick Setup Operation Mode Network **Wireless** - Basic Settings - WPS - Wireless Security - Wireless MAC Filtering - Wireless Advanced - Wireless Statistics - Throughput Monitor - Wireless Security - Wireless MAC Filtering - Wireless Advanced - Wireless Statistics - Throughput Monitor Guest Network DHCP Custom Tools

Wireless:  Enable  Disable  
Wireless Network Name: CEO-ALEX  
Mode: 11bgn mixed  
Channel Width: Auto  
Channel: Auto  
 Enable SSID Broadcast

Disable wireless security  
 WPA/WPA2 - Personal (Recommended)  
Version: WPA2-PSK  
Encryption: AES  
Wireless Password: 123456789  
Group Key Update Period: 0

WPA/WPA2 - Enterprise

## 5. Branchement physique

- Connecter un câble du LAN (jaune) du TP-Link vers un port du switch.
- Configurer le port du switch en Access VLAN20 (untagged VLAN20).

## 5. Branchement physique

- Un client connecté au Wi-Fi doit obtenir une IP en 10.10.20.x.
- Tests ping :
  - 10.10.20.20 (AP)
  - 10.10.20.1 (gateway)
  - Une adresse Internet



GESTION  
PROJET  
INFORMATIQUE

# Configuration des Règles et des Certificats sur pfSense - Hatim

Pré-requis :

- Un pare-feu pfSense installé et opérationnel.
- Interfaces réseau déjà configurées :
  - VLAN 10 – Serveurs (10.10.10.0/24)
  - VLAN 20 – Clients (10.10.20.0/24)
  - VLAN 30 – Transit (10.10.30.0/24)
  - VLAN 99 – Infrastructure (10.10.99.0/24)
- Règles NAT déjà en place pour la sortie Internet.
- Accès administrateur à l'interface web pfSense.

## Configuration des règles pfSense - Hatim

### 1. Vlan 10 - Serveurs (10.10.10.0/24)

Objectif : permettre la communication entre serveurs, supervision et mises à jour.

- Autoriser communications internes (serveur ↔ serveur).
- Autoriser AD/DNS/LDAP vers SRV-AD01 (10.10.10.40).
- Autoriser Syslog (514 UDP) vers SRV-LX03.
- Autoriser SNMP (161/162 UDP) vers SRV-LX02 (supervision).
- Autoriser HTTP/HTTPS (80/443 TCP) pour mises à jour OS.
- Blocage par défaut → pas d'accès inutile vers clients ou Internet.

The screenshot shows the pfSense interface under Firewall / Rules / VLAN10. It displays a list of port rules with the following details:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓ 0/0 B	IPv4 TCP	VLAN10 net	*	*	HTTP	*	none	none	Autoriser MAJ systèmes (apt/yum/windows update)
✓ 0/0 B	IPv4 UDP	VLAN10 net	*	10.10.10.52	161 - 162	*	none	none	supervision snmp
✓ 0/0 B	IPv4 UDP	VLAN10 net	*	10.10.10.53	514 (Syslog)	*	none	none	syslog
✓ 0/0 B	IPv4 TCP/ UDP	VLAN10 net	*	10.10.10.40	AD	*	none	none	Autoriser services AD/DNS internes
✓ 0/0 B	IPv4 +	VLAN10 net	*	VLAN10 net	*	*	none	none	Autoriser communications internes serveurs
✓ 281/4.80 GiB	IPv4 *	*	*	*	*	*	none	none	
✗ 0/0 B	IPv4 *	VLAN10 net	*	*	*	*	none	none	Blocage par défaut VLAN10

## 2. Vlan 20 - Clients (10.10.20.0/24)

Objectif : donner aux postes clients l'accès aux services essentiels et à Internet.

- Autoriser DNS (53 TCP/UDP) → SRV-AD01 (10.10.10.40)
- Autoriser DHCP (67/68 UDP) → attribution IP
- Autoriser HTTP/HTTPS (80/443 TCP) → navigation Internet + intranet
- Autoriser Messagerie (25, 110, 995, 143, 993 TCP) → serveur mail (10.10.10.54)
- Autoriser VoIP (5060 UDP + 10000–20000 UDP) → serveur VoIP (10.10.10.53)
- Blocage par défaut → tout autre trafic refusé

The screenshot shows the Firewall configuration for VLAN20. It includes a table of aliases and a detailed view of the firewall rules.

**Aliases:**

Name	Values	Description	Actions
AD	53, 88, 389, 445, 125, 464, 636	dns/kerberos/ldap/rpc/ldb	<i>(Edit)</i> <i>(Delete)</i>
EX01	902, 443, 3260, 2049	Vmware/vcenter/scsi/nfs	<i>(Edit)</i> <i>(Delete)</i>
HTTP	80, 443	http	<i>(Edit)</i> <i>(Delete)</i>
JSP	22, 9399, 443	jsp	<i>(Edit)</i> <i>(Delete)</i>
mail_port	25, 110, 995, 143, 993	mail	<i>(Edit)</i> <i>(Delete)</i>
Voip	5060, 10000-20000	voip	<i>(Edit)</i> <i>(Delete)</i>

**Rules (Drag to Change Order):**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	IPv4 UDP	*	*	10.10.10.53	Voip	*	none	none	voip	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP	*	*	10.10.10.54	mail_port	*	none	none	mail	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP	VLAN20 net	*	*	443 (HTTPS)	*	none	none	https	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP	VLAN20 net	*	*	80 (HTTP)	*	none	none	http	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP/UDP	VLAN20 net	*	10.10.10.40	67-68	*	none	none	dhcp_vlan20	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP/UDP	*	*	10.10.10.40	53 (DNS)	*	none	none	dns	<i>(Edit)</i> <i>(Delete)</i>
✓ 243/444 GB	IPv4 *	*	*	*	*	*	*	*	*	<i>(Edit)</i> <i>(Delete)</i>
✗ 0/0 B	IPv4 *	VLAN20 net	*	*	*	*	*	*	Blocage par défaut VLAN20	<i>(Edit)</i> <i>(Delete)</i>

## 3. Vlan 30 - Clients (10.10.30.0/24)

Objectif : assurer le NAT et la sortie Internet.

- Autoriser VLAN20 → Internet (80/443).
- Autoriser VLAN10 → Internet (80/443) uniquement pour mises à jour.
- Autoriser PC-ADMIN (10.10.99.13) → Internet (80/443).
- Blocage par défaut → rien d'autre ne transite.

The screenshot shows the Firewall configuration for VLAN30. It includes a table of rules.

**Rules (Drag to Change Order):**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	*	*	*	LAN Address	443	*	*	*	Anti-Lockout Rule	<i>(Edit)</i>
✓ 0/0 B	*	*	*	80	*	*	*	*		
✓ 0/0 B	*	*	*	22	*	*	*	*		
✓ 0/0 B	IPv4 TCP	10.10.99.13	*	*	HTTP	*	none	none	PC-ADMIN → Internet	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP	VLAN10 net	*	*	HTTP	*	none	none		<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 TCP/UDP	VLAN20 net	*	*	HTTP	*	none	none	VLAN20 → Internet (Web)	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv4 *	LAN net	*	*	*	*	*	*	Default allow LAN to any rule	<i>(Edit)</i> <i>(Delete)</i>
✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	*	*	Default allow LAN IPv6 to any rule	<i>(Edit)</i> <i>(Delete)</i>
✗ 0/0 B	IPv4 *	LAN net	*	*	*	*	*	*	Blocage par défaut VLAN30	<i>(Edit)</i> <i>(Delete)</i>

## 4. Vlan 99 - Infrastructure(10.10.99.0/24)

Objectif : limiter l'accès aux hyperviseurs et au SAN à l'administrateur.

- Autoriser PC-ADMIN (10.10.99.13) → VLAN10 net (22 SSH, 3389 RDP, 443 HTTPS).
- Autoriser ESXi ↔ vCenter ↔ SAN (902, 443, 3260, 2049 TCP).
- Autoriser PC-ADMIN → Internet (80/443) pour téléchargements/MAJ.
- Blocage par défaut → pas d'accès pour les autres machines du VLAN99.

The screenshot shows two main sections of a firewall configuration interface:

**Firewall / Aliases / Ports**

Name	Values	Description	Actions
AD	53, 88, 389, 445, 135, 464, 636	dns/kerberos/ldap/rpc/smb	
EXCI	902, 443, 3260, 2049	Vmware,vcenter,jiscounfs	
HTTP	80, 443	http	
JSP	22, 3389, 443	jsp	
mail_port	25, 110, 995, 143, 993	mail	
Voip	5060, 10000-20000		

**Firewall / Rules / VLAN99**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	IPv4 TCP	10.10.99.13	*	*	HTTP	*	none		PC-ADMIN → Internet	
✓ 0/0 B	IPv4 TCP/UDP	VLAN99 net	*	VLAN99 net	EXCI	*	none		Comms VMware / SAN internes	
✓ 0/0 B	IPv4 TCP	10.10.99.13	*	VLAN10 net	JSP	*	none		PCadmin	
✓ 36/2.37 GiB	IPv4 *	*	*	*	*	*	*			
✗ 0/0 B	IPv4 *	*	*	*	*	*	*		Blocage par défaut VLAN99	

## 5. Wan - Internet

Objectif : bloquer toutes les entrées sauf VPN.

- Autoriser OpenVPN (1194 UDP) sur WAN address (accès nomades).
- Bloquer tout le reste.

The screenshot shows the Firewall / Rules / WAN section:

**Firewall / Rules / WAN**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 7/3.08 MiB	IPv4 *	*	*	*	*	*	none			
✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN wizard	
✗ 0/0 B	IPv4 *	*	*	*	*	*	none		Blocage par défaut WAN	

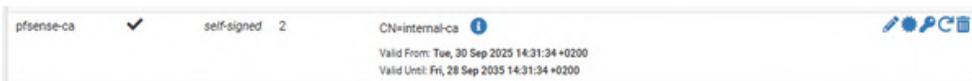
# Configuration des Certificats pfSense - Hatim

## 1. Crédation d'une autorité de certification

Dans pfSense, aller dans System > Cert. Manager > CAs.

Cliquer sur Add pour créer une nouvelle CA interne.

Enregistrer → La CA sera utilisée pour signer les certificats serveur et utilisateurs.



## 2. Crédation du certificat pour le serveur et export du certificat et de la clé

Aller dans System > Cert. Manager > Certificates.

Cliquer sur Add/Sign.

Lorsque que le certificat server est créé :

- Nous allons cliquer sur ces 2 icônes afin d'exporter le certificat et la clé respectivement :



### 3. Déployer certificat SSL PfSense-ca sur Debian (Apache)

Déplacer les fichiers dans les répertoires standards :

- sudo mv /root/PfSense-ca.crt /etc/ssl/certs/
- sudo mv /root/PfSense-ca.key /etc/ssl/private/

Il faut verrouiller les droits de la clé :

- sudo chmod 600 /etc/ssl/private/PfSense-ca.key
- sudo chown root:root /etc/ssl/private/PfSense-ca.key

Activer SSL dans Apache :

- sudo a2enmod ssl
- sudo a2enmod headers
- sudo a2ensite default-ssl.conf

Éditer /etc/apache2/sites-available/default-ssl.conf et configurer :

```
VirtuualHost *:443>
ServerAdmin webmaster@localhost
ServerName www.formation.local
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile    /etc/ssl/certs/PfSense-ca.crt
SSLCertificateKeyFile /etc/ssl/private/PfSense-ca.key
```

Redémarrage d'Apache :

- sudo apache2ctl configtest
- sudo systemctl reload apache2

## 4. Déployer le CA pfSense via GPO (Windows Server)

- Exporter le CA depuis pfSense :
- Attention : c'est bien le CA qu'il faut exporter, pas le certificat serveur.



- Le récupérer sur le SRV-AD et ensuite dans la gestion des stratégies de groupe on va créer ou modifier une GPO qui s'appliquera aux ordinateurs
- Naviguer dans :
  - Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Autorités de certification racines de confiance
  - Clic droit → Importer. puis suivez les étapes d'importation

Délivré à	Délivré par	Date d'expiration	Rôles prévus	Nom convivial
internal-ca	internal-ca	07/09/2035	< Tout >	< Aucun >

- Pour forcer la mise à jour des stratégies sur les PC clients du domaine :
  - gpupdate /force puis effectuer les enregistrements DNS dde votre serveur.
- Si le CA pfSense est bien installé via GPO, le certificat doit être reconnu comme valide (cadenas vert).

# Configuration Switch L3 Cisco - David / Hatim

Pré-requis :

- Un switch Cisco de niveau 3 (L3).
- Accès en console ou SSH au switch.
- Configuration de base réalisée :
- Nom du switch défini
- Accès administrateur (enable + mot de passe configuré)
- Service SSH activé
- Plan d'adressage IP validé (ex. : VLAN 10, 20, 30, 99).
- Câbles reliés entre le switch L3, le routeur/firewall (pfSense) et les machines de test.
- Logiciel Packet Tracer / GNS3 ou matériel physique prêt pour la configuration et les tests.

## 1. Configuration de Base

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-L3
SW-L3(config)#no ip domain-lookup
SW-L3(config)#enable secret Azerty1@
SW-L3(config)#username admin privilege 15 secret Azerty1@
SW-L3(config)#line console 0
SW-L3(config-line)# password Azerty1@
SW-L3(config-line)# login
SW-L3(config-line)# logging synchronous
SW-L3(config-line)#line vty 0 4
SW-L3(config-line)# password Azerty1@
SW-L3(config-line)# login
SW-L3(config-line)# transport input ssh
SW-L3(config-line)# logging synchronous
SW-L3(config-line)#ip domain-name projet.local
SW-L3(config)#crypto key generate rsa
The name for the keys will be: SW-L3.projet.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 43 seconds)

SW-L3(config)#
SW-L3(config)#
*Mar 1 00:14:34.009: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-L3(config)#ip ssh version 2
SW-L3(config)#[
```

## 2. Vlans

```
SW-L3(config)#vlan 10
SW-L3(config-vlan)# name SERVEURS
SW-L3(config-vlan)#vlan 20
SW-L3(config-vlan)# name CLIENTS
SW-L3(config-vlan)#vlan 30
SW-L3(config-vlan)# name TRANSIT
SW-L3(config-vlan)#vlan 99
SW-L3(config-vlan)# name INFRA
SW-L3(config-vlan)#[
```

### 3. Interfaces Range

```
!
interface GigabitEthernet1/0/1
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/0/3
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/0/4
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/0/5
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet1/0/6
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet1/0/7
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet1/0/8
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet1/0/9
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet1/0/10
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet1/0/13
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/14
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/15
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/16
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/17
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/18
switchport access vlan 99
switchport mode access
!
interface GigabitEthernet1/0/21
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/22
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/23
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

FORMATION  
JET  
INFORMATIQUE

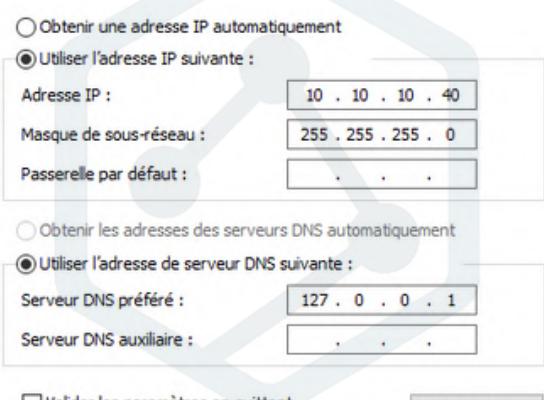
# Configuration du Server ADDS - Anthony

## Pré-requis

- Serveur Windows Server 2022 installé.
- Adresse IP fixe configurée.
- Mot de passe administrateur : Azerty1
- Rôle Active Directory Domain Services (ADDS) installé.

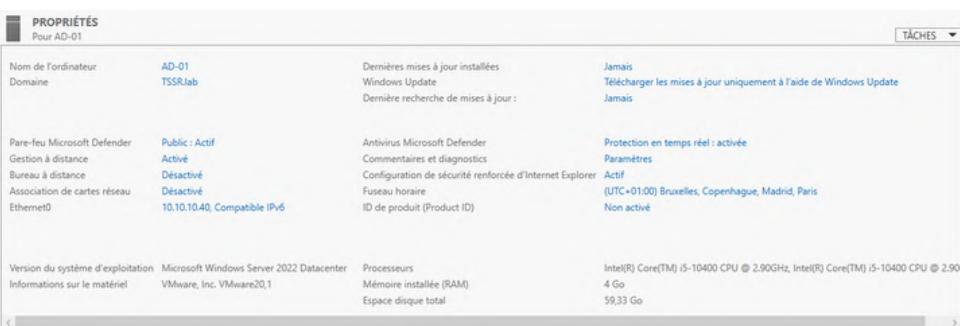
## 1. Configuration réseau

- Définir une IP statique adaptée au VLAN Serveurs.
- Configurer la passerelle et les DNS (pointant vers le futur contrôleur de domaine).
- Vérifier avec ipconfig/all et ping <IP passerelle>



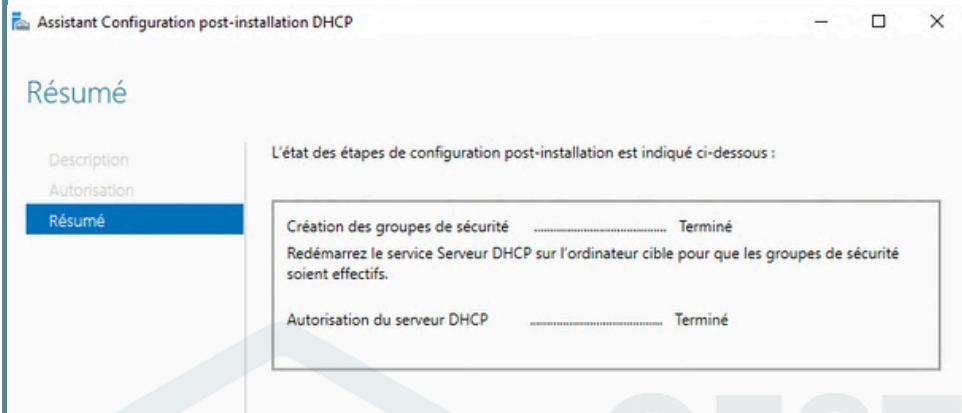
## 2. Installation du contrôleur de domaine

- Lancer l'assistant ADDS.
- Créer un nouveau domaine dans une nouvelle forêt.
- Définir le mot de passe DSRM.
- Redémarrer le serveur à la fin de l'installation.



### 3. Installation du rôle DHCP

- Ajouter le rôle DHCP via Server Manager.
- Définir une plage IP pour le VLAN Clients.
- Exclure les adresses réservées (imprimantes, serveurs fixes).
- Configurer les options DHCP (DNS, passerelle).
- Autoriser le serveur DHCP dans AD.



GESTION  
PROJET  
INFORMATIQUE

## 4. Validation finale

- Création d'un fichier csv avec les informations des utilisateurs à importer :

```

FirstLastName,LastName,SamAccountName,UserPrincipalName,OU,Unit,Role,Group,Department
Jean,Dupont,jdupont,jdupont@TSSR.lab,"OU=Sport Loisirs,DC=TSSR,DC=lab","Jdupont@TSSR.lab,Acerty@TSSR.lab,Directeur Général,Direction,geo
Pierre,Durand,pdurand,pdurand@TSSR.lab,"OU=Administratif,OU=Sport Loisirs,DC=TSSR,DC=lab","Jpdurand@TSSR.lab,Acerty@TSSR.lab,Assistant de Direction
Sophie,Leroy,leroy,leroy@TSSR.lab,"OU=Comptabilité,OU=Sport Loisirs,DC=TSSR,DC=lab","Sleroy@TSSR.lab,Acerty@TSSR.lab,Comptable,Admin
Elodie,Petit,petit@TSSR.lab,"OU=Ventes,OU=Sport Loisirs,DC=TSSR,DC=lab","Epetit@TSSR.lab,Acerty@TSSR.lab,Vendeur,Commercial
Thomas,Dubois,tdubois,tdubois@TSSR.lab,"OU=Chef de rayon,OU=Sport Loisirs,DC=TSSR,DC=lab","Tdubois@TSSR.lab,Acerty@TSSR.lab,Chef de Rayon,Ventes
Nicolas,Lambert,nlambert@TSSR.lab,"OU=Magasin,OU=Logistique,OU=Sport Loisirs,DC=TSSR,DC=lab","Nnlambert@TSSR.lab,Acerty@TSSR.lab,Magasinier
Julie,Rousseau,jrousseau,jrousseau@TSSR.lab,"OU=Support IT,OU=Sport Loisirs,DC=TSSR,DC=lab","Jrousseau@TSSR.lab,Acerty@TSSR.lab,Intervenant Logist
Audrey,lefeuvre,alefeuvre@TSSR.lab,"OU=Support IT,OU=Sport Loisirs,DC=TSSR,DC=lab","Alefrev@TSSR.lab,Acerty@TSSR.lab,Technicien Support IT,Grou
Charlotte,Girard,girard@TSSR.lab,"OU=RH,OU=Sport Loisirs,DC=TSSR,DC=lab","Cgirard@TSSR.lab,Acerty@TSSR.lab,Technicien RH
David,Blanc,dblanc@TSSR.lab,"OU=Comptabilité,OU=Administratif,OU=Sport Loisirs,DC=TSSR,DC=lab","Dblanc@TSSR.lab,Acerty@TSSR.lab,Comptable,Administrat
Florian,Bertrand,fbertrand,fbertrand@TSSR.lab,"OU=Ventes,OU=Sport Loisirs,DC=TSSR,DC=lab","Fbertrand@TSSR.lab,Acerty@TSSR.lab,Vendeur,Commercial
Garance,fournier,fournier@TSSR.lab,"OU=Chef de Rayon,OU=Ventes,OU=Sport Loisirs,DC=TSSR,DC=lab","Gfournier@TSSR.lab,Acerty@TSSR.lab,Chef de Ray
Inès,guillet,igUILLET@TSSR.lab,"OU=Livraison,OU=Logistique,OU=Sport Loisirs,DC=TSSR,DC=lab","Iguillet@TSSR.lab,Acerty@TSSR.lab,Livreur,Logistique
Noémie,Arousel,jrousset@TSSR.lab,"OU=Adm Système,IT,OU=Sport Loisirs,DC=TSSR,DC=lab","Jrousset@TSSR.lab,Acerty@TSSR.lab,Adm Système,IT,Groupe Admin
Laura,Noreau,lnoreau@TSSR.lab,"OU=Commerce,OU=Hommes,OU=Sport Loisirs,DC=TSSR,DC=lab","Lnoreau@TSSR.lab,Acerty@TSSR.lab,Commercial Homme
Mathieu,Chevallier,mchevallier@TSSR.lab,"OU=Techniciens,OU=Hommes,OU=Sport Loisirs,DC=TSSR,DC=lab","Mchevallier@TSSR.lab,Acerty@TSSR.lab,Technici
Oliver,Marchand,omarchand@TSSR.lab,"OU=Administratif,OU=Sport Loisirs,DC=TSSR,DC=lab","Omarchand@TSSR.lab,Acerty@TSSR.lab,Responsable RH
Pauline,dubois,pdubois@TSSR.lab,"OU=Support,OU=Administratif,OU=Sport Loisirs,DC=TSSR,DC=lab","Pdubois@TSSR.lab,Acerty@TSSR.lab,Technicien Support,
Romane,Martin,rmartin@TSSR.lab,"OU=Chef de Section,OU=Ventes,OU=Sport Loisirs,DC=TSSR,DC=lab","Rmartin@TSSR.lab,Acerty@TSSR.lab,Chef de Section,Ve
Simon,lefert,slefert,lefert@TSSR.lab,"OU=Magasin,OU=Logistique,OU=Sport Loisirs,DC=TSSR,DC=lab","Slefert@TSSR.lab,Acerty@TSSR.lab,Magasinier,Logistique,Gr

```

Création d'un fichier powershell pour importer utilisateurs dans leur OU respectifs :

```

# script-import-user - Bloc-notes
Fichier Edition Format Affichage Aide
# Chemin vers le fichier CSV
$csvPath = "C:\Users\Administrateur\Documents\Utilisateurs1.csv" # Modifiez le chemin si nécessaire

# Import des utilisateurs depuis le CSV
Import-Csv -Path $csvPath | ForEach-Object {
    # Création de l'utilisateur dans l'OU spécifiée
    New-ADUser -Name $_.FirstName -Lastname $_.LastName -SamAccountName $_.UserPrincipalName -UserPrincipalName $_.UserPrincipalName -GivenName $_.FirstName -Surname $_.LastName -Path $_.OU -EmailAddress $_.Email -Enabled $true -ChangePasswordAtLogon $true -Title $_.Title -Department $_.Department

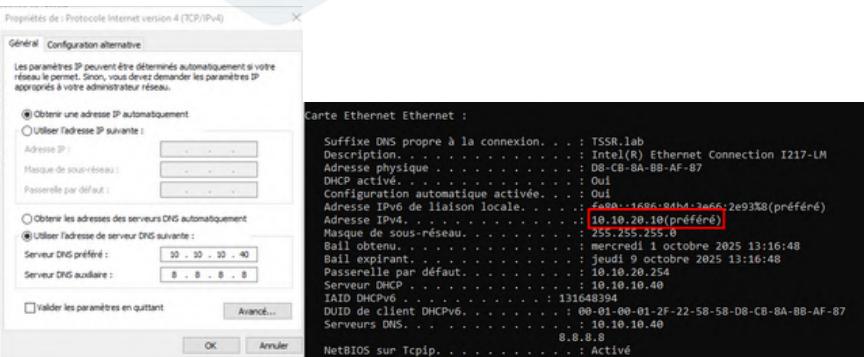
    # Ajout aux groupes spécifiés (séparés par des virgules dans le CSV)
    $groups = $_.Groups -split ","
    foreach ($group in $groups) {
        try {
            Add-ADGroupMember -Identity $group -Members $_.SamAccountName -ErrorAction Stop
            Write-Host "Utilisateur $($_.SamAccountName) ajouté au groupe $group" -ForegroundColor Green
        } catch {
            Write-Host "Erreur : Impossible d'ajouter $($_.SamAccountName) au groupe $group" -ForegroundColor Red
        }
    }
}

Write-Host "Import terminé avec succès !" -ForegroundColor Cyan

```

Sur un poste client :

- ipconfig /renew
- nslookup google.com



verifie dans l'onglet outil > Utilisateurs et ordinateurs Active Directory. Les utilisateurs ont bien été importé dans leur OU respectif :

Nom	Type
David Blanc	Utilisateur
Noémie Ler...	Utilisateur
Pierre Durand	Utilisateur

# Configuration du Server Web (Installation) - Thomas / Alexandre

## Pré-requis

- Serveur Debian 11 : SRV-MAIL (IP : 10.10.10.54)
- Postfix installé (SMTP)
- Dovecot installé (IMAP/POP3)
- Accès root ou sudo pour création d'utilisateurs
- Un poste client avec Thunderbird installé

## 1. Création d'un utilisateur mail

- Créer un nouvel utilisateur Linux qui servira pour la messagerie.
- Exemple :

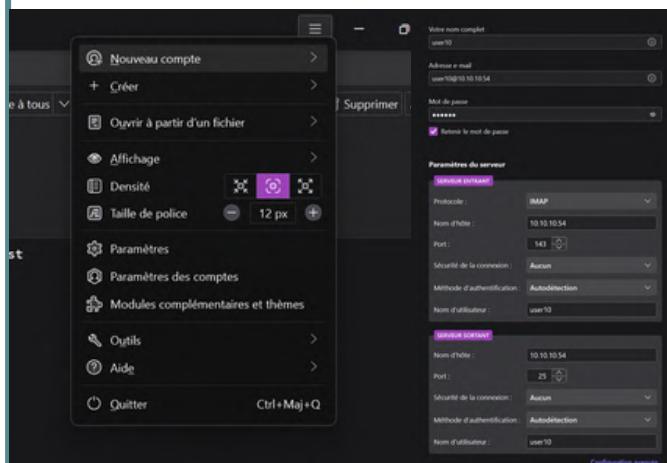
```
root@SRV-LX12:~# sudo adduser user10
Ajout de l'utilisateur « user10 » ...
Ajout du nouveau groupe « user10 » (1004) ...
Ajout du nouvel utilisateur « user10 » (1004) avec le groupe « user10 » (1004)
Création du répertoire personnel « /home/user10 » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe ne passe pas la vérification dans le dictionnaire
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour user10
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []: user10
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:

Cette information est-elle correcte ? [O/n]Ajout du nouvel utilisateur « user10 »
Ajout de l'utilisateur « user10 » au groupe « users » ...
```

GESTION  
PROJET  
INFORMATIQUE

## 2. Configuration du client Thunderbird

- Ouvrir Thunderbird sur le poste client.
- Ajouter un nouveau compte → adresse : user10@10.10.10.54
- Cliquer sur Continuer → l'autodétection échoue (normal).
- Cliquer sur Configuration manuelle / Paramètres manuels.



### 3. Sécurité Thunderbird

- Si un avertissement apparaît concernant le chiffrement :
- Cliquer sur Je comprends les risques
- Confirmer l'ajout du compte

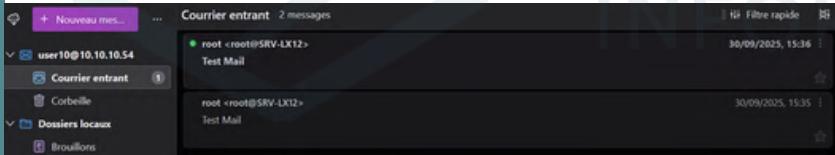


### 4. Test via SRV-MAIL

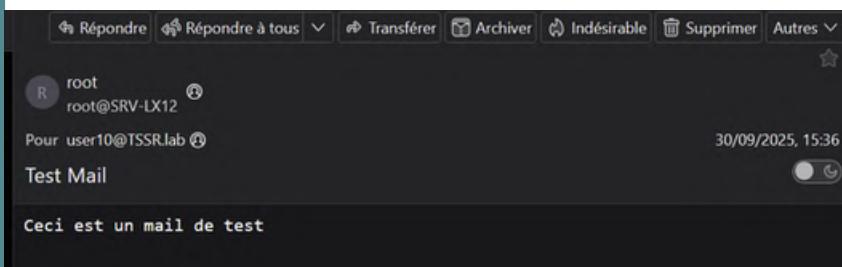
- Depuis Thunderbird → envoyer un mail à user10@10.10.10.54.

```
root@SRV-LX12:~# echo "Ceci est un mail de test" | mail -s "Test Mail" user10
```

- Vérifier que le mail est bien reçu dans la boîte de réception de user10.



- Vérifier aussi l'envoi depuis le serveur SRV-MAIL.



# Configuration du Server Web (Installation) - Geoffrey

Pré-requis :

- Serveur Linux avec IP statique configurée
- DNS configuré dans /etc/resolv.conf
- Accès SSH activé
- Droits administrateur

## 1. Installation d'Apache2

- Commande : apt install apache2 -y
- Activation du service : systemctl enable apache2
- Vérification via systemctl status apache2

```
root@SRV-Web-Ftp:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-09-22 11:55:38 CEST; 1min 2s ago
    Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2024 (apache2)
     Tasks: 55 (limit: 4597)
    Memory: 15.0M
       CPU: 56ms
      CGroup: /system.slice/apache2.service
              ├─2024 /usr/sbin/apache2 -k start
              ├─2086 /usr/sbin/apache2 -k start
              └─2087 /usr/sbin/apache2 -k start
sept. 22 11:55:37 SRV-Web-Ftp systemd[1]: Starting apache2.service - The Apache HTTP Server..
```

## 2. Installation de MatiaDB

- Commande : apt install mariadb-server mariadb-client -y
- Activation du service : systemctl enable mariadb
- Vérification via systemctl status mariadb

```
root@SRV-Web-Ftp:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-09-22 11:55:38 CEST; 1min 2s ago
    Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2024 (apache2)
     Tasks: 55 (limit: 4597)
    Memory: 15.0M
       CPU: 56ms
      CGroup: /system.slice/apache2.service
              ├─2024 /usr/sbin/apache2 -k start
              ├─2086 /usr/sbin/apache2 -k start
              └─2087 /usr/sbin/apache2 -k start
sept. 22 11:55:37 SRV-Web-Ftp systemd[1]: Starting apache2.service - The Apache HTTP Server..
```

### 3. Instalations PHP

- Commande : apt install php libapache2-mod-php php-mysql -y
- Vérification de la version : php -v

```
root@SRV-Web-Ftp:~# php -v
PHP 8.2.29 (cli) (built: Jul 3 2025 16:16:05) (NT
Copyright (c) The PHP Group
```

### 4. Installation FTP (vsftpd)

- Commande : apt install vsftpd -y

```
root@SRV-Web-Ftp:~# apt -y install vsftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires:
  linux-image-6.1.0-28-amd64 linux-image-6.1.0-9-amd64
Veuillez utiliser « apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

- Création des utilisateurs "geo" / "thomas"

```
Ajout de l'utilisateur « thomas » ...
Ajout du nouveau groupe « thomas » (1002) ...
Ajout du nouvel utilisateur « thomas » (1002) avec le groupe « thomas »
Création du répertoire personnel « /home/thomas » ...
root@SRV-Web-Ftp:~# adduser geo
Ajout de l'utilisateur « geo » ...
Ajout du nouveau groupe « geo » (1001) ...
Ajout du nouvel utilisateur « geo » (1001) avec le groupe « geo » (
Création du répertoire personnel « /home/geo » ...
```

- Ajout dans /etc/vsftpd.chroot\_list

```
GNU nano 7.2
# Utilisateurs autorisés à se connecter via vsftpd
geo
thomas
```

## 5. Activation du FTPS

- Génération certificat SSL :

```
root@SRV-Web-Ftp:~# cd /etc/ssl/private
root@SRV-Web-Ftp:/etc/ssl/private# openssl req -x509 -nodes -newkey rsa:2048 -keyout vsftpd.pem -out vsftpd.pem -days 365
```

- Modification du fichier /etc/vsftpd.conf

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=YES
ssl_ciphers=HIGH
ssl_tls1v1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

- Restriction des permissions sur fichier nouvellement créé au seul utilisateur propriétaire :

```
root@SRV-FTP:/etc/ssl/private# chmod 600 vsftpd.pem
```

- Modification du fichier de configuration de vsftpd afin qu'il tienne compte du certificat (/etc/vsftpd.conf)

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=YES
ssl_ciphers=HIGH
ssl_tls1v1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

- Redémarrage du service :
  - systemctl restart vsftpd

# Configuration du Server Web (Sécurisation) - Geoffrey

## 1. Pare-feu UFW

- installation et activation :

```
sudo apt install ufw -y
sudo ufw allow 22/tcp      # SSH
sudo ufw allow 80/tcp      # HTTP
sudo ufw allow 443/tcp     # HTTPS
sudo ufw enable
```

- Vérification du statut :

```
root@SRVLX01:~# ufw status
Status: active

To                         Action      From
--                         --         --
22/tcp                      ALLOW      Anywhere
80/tcp                      ALLOW      Anywhere
443/tcp                     ALLOW      Anywhere
22/tcp (v6)                 ALLOW      Anywhere (v6)
80/tcp (v6)                 ALLOW      Anywhere (v6)
443/tcp (v6)                ALLOW      Anywhere (v6)
```

GESTION  
PROJET  
INFORMATIQUE

## 2. HTTPS avec Let's Encrypt

- Installation de Certbot :

```
root@SRVLX01:~# apt install certbot python3-certbot-apache -y  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
root@SRVLX01:~# sudo apt install openssl -y
```

- #### • Génération du certificat

- Activation du module SSL :

```
root@SRVLX01:~# sudo a2enmod ssl
```

- Création d'un vhost SSL

```
GNU nano 7.2                                         /etc/apache2/sites-available/tssr-ssl.conf
<VirtualHost *:443>
    ServerName tssr.lab

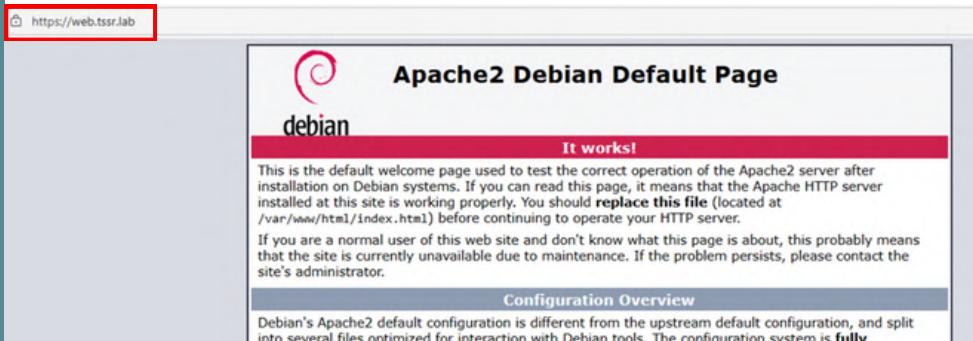
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/tssr.lab.crt
    SSLCertificateKeyFile /etc/ssl/private/tssr.lab.key

    <Directory /var/www/html>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

- Activation du site et recharge d'Apache :

- sudo a2ensite tssr-ssl.conf
  - systemctl reload



### 3. Masquer les informations serveur Apache

- Modification du fichier /etc/apache2/conf-available/security.conf :

```
GNU nano 7.2                               /etc/apache2/conf-available/security.conf *
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full
ServerTokens Prod
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature Off

#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of: On | Off | extended
TraceEnable Off
#TraceEnable On
```

### 4. Sécurisation du FTP (vsftpd)

- Modification du fichier /etc/vsftpd.conf :

```
listen=YES
listen_ipv6=NO
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES

ssl_enable=YES
rsa_cert_file=/etc/ssl/private/vsftpd.pem
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
```

# Installation et configuration GLPI + Netdata - Geoffrey

## Pré-requis

- Serveur Linux (Debian/Ubuntu) avec IP statique.
- Stack LAMP installée (Linux, Apache, MariaDB, PHP).
- Accès root ou sudo.

## GLPI

### 1. Installation de GLPI

Télécharger la dernière version de GLPI :

```
root@SRV-LX12:~# wget https://github.com/glpi-project/glpi/releases/download/10.0.20/glpi-10.0.20.tgz  
root@SRV-LX12:~# tar -xvzf glpi-10.0.20.tgz
```

### 2. Configuration initiale GLPI

Accès via navigateur : <http://10.10.10.52/glpi/install/install.php>

- Étapes :
- Sélection de la langue.
- Connexion à la base SQL (10.10.10.52, user glpi\_user, mdp Azerty1).
- Initialisation base → message Connexion réussie.

The screenshots illustrate the six-step setup process:

- Step 1: Selectionnez votre langue** (Select your language). The user has chosen "Français".
- Step 2: Configuration de la connexion à la base de données** (Database connection configuration). The user has entered "10.10.10.52" for the MySQL server, "glpi\_user" for the database user, and "Azerty1" for the password. The "Continuer >" button is visible.
- Step 3: Initialisation de la base de données** (Database initialization). A success message states "OK - La base a bien été initialisée".
- Step 4: Configuration de la connexion à la base de données** (Database connection configuration). The user has entered "localhost" for the MySQL server, "glpi\_user" for the database user, and "Azerty1" for the password. The "Continuer >" button is visible.
- Step 5: Configuration de la connexion à la base de données** (Database connection configuration). This step is identical to Step 4, showing the same input fields and "Continuer >" button.
- Step 6: L'installation est terminée** (Installation is completed). It lists the default administrator and technician credentials:
  - glpi/glpi pour le compte administrateur
  - tech/tech pour le compte technicien
  - normal/normal pour le compte normal
  - post-only/postonly pour le compte postonly

### 3. Création d'un super-admin

- Aller dans Administration → Utilisateurs → Ajouter utilisateur.
- Créer un compte admin personnalisé (ex. toto/toto).
- Associer le rôle Super-Admin.

The screenshot shows the GLPI administration interface. On the left, there's a sidebar with various menu items like Parc, Assistance, Gestion, Outils, Administration, Utilisateurs (which is selected and highlighted in red), and Groups. The main area has a title bar with 'Accueil / Administration / Utilisateurs' and a 'Ajouter' button. Below this is a search bar with 'Actions' and a 'Ajouter utilisateur...' button, which is also highlighted in red. The main content area shows a form for creating a new user 'admin'. The fields filled in are:

Identifiant	admin	1
Nom de famille	toto	
Prénom	toto	
Mot de passe	*****	
Confirmation mot de passe	*****	
Fuseau horaire	L'utilisation des fuseaux horaires n'a pas été "php bin/console database:enable_timezone"	
Actif	Oui	
Valide depuis		
Téléphone		
Téléphone mobile		
Téléphone 2		
Matricule		
Titre	----- i +	
Habilitation		
Profil	Super-Admin	2

### 4. Inventaire automatique GLPI Agent

- Télécharger l'agent : lien GitHub officiel
- Déployer sur les postes clients (Windows/Linux).
- L'agent remonte automatiquement les infos matérielles/logiciels dans GLPI.
- Activer l'inventaire dans GLPI (Administration → Inventaire).

### 6. Sécurisation de GLPI

Restriction des droits MySQL :

- Donner uniquement les droits nécessaires à l'utilisateur GLPI.

```
root@SRV-LX12:~# rm -rf /var/www/html/glpi/install
```

# Netdata - Geoffrey

## 1. Installation de Netdata

```
root@SRV-LX12:~# apt install netdata
root@SRV-LX12:~# systemctl start netdata && sudo systemctl enable netdata
root@SRV-LX12:~# systemctl status netdata
● netdata.service - netdata - real-time performance monitoring
  Loaded: loaded (/lib/systemd/system/netdata.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-09-29 09:03:17 CEST; 1h 33min ago
    Docs: man:netdata(7)
           file:///usr/share/doc/netdata/html/index.html
           https://github.com/netdata/netdata
      Main PID: 608 (netdata)
        Tasks: 50 (limit: 2260)
       Memory: 122.0M
          CPU: 56.533s
         CGroup: /system.slice/netdata.service
                   ├─ 608 /usr/sbin/netdata -D
                   ├─ 702 /usr/sbin/netdata --special-spawn-server
                   ├─ 1025 /usr/lib/netdata/plugins.d/apps.plugin 1
                   ├─ 1029 /usr/lib/netdata/plugins.d/nfacct.plugin 1
                   └─ 76412 bash /usr/lib/netdata/plugins.d/tc-qos-helper.sh 1
```

- Le service est actif et écoute par défaut sur le port 19999.
- Vérification :

```
root@SRV-LX12:~# netstat -tunlp | grep 19999
tcp        0      0 127.0.0.1:19999          0.0.0.0:*
                                              LISTEN      608/netdata
```

## 2. Configuration du service

- Éditer le fichier /etc/netdata/netdata.conf :

```
GNU nano 7.2                                         /etc/netdata/netdata.conf
# NetData Configuration

# The current full configuration can be retrieved from the running
# server at the URL
#
#   http://localhost:19999/netdata.conf
#
# for example:
#
#   wget -O /etc/netdata/netdata.conf http://localhost:19999/netdata.conf
#

[global]
  run as user = netdata
  web files owner = root
  web files group = root
  # Netdata is not designed to be exposed to potentially hostile
  # networks. See https://github.com/netdata/netdata/issues/164
  bind socket to IP = 10.10.10.52
```

- Puis redémarrer le service :

```
root@SRV-LX12:~# systemctl restart netdata
```

### 3. Intégration avec Apache (reverse proxy)

- Créer le fichier /etc/apache2/sites-available/netdata.conf \*:

```
GNU nano 7.2                               /etc/apache2/sites-available/netdata.conf *
```

```
<VirtualHost *:80>
    ServerName tssr.lab
    RewriteEngine On
    ProxyRequests Off
    ProxyPreserveHost On

    <Proxy *>
        Require all granted
    </Proxy>

    ProxyPass "/" "http://10.10.10.52:19999/" connectiontimeout=5 timeout=30 keepalive=on
    ProxyPassReverse "/" "http://10.10.10.52:19999/"

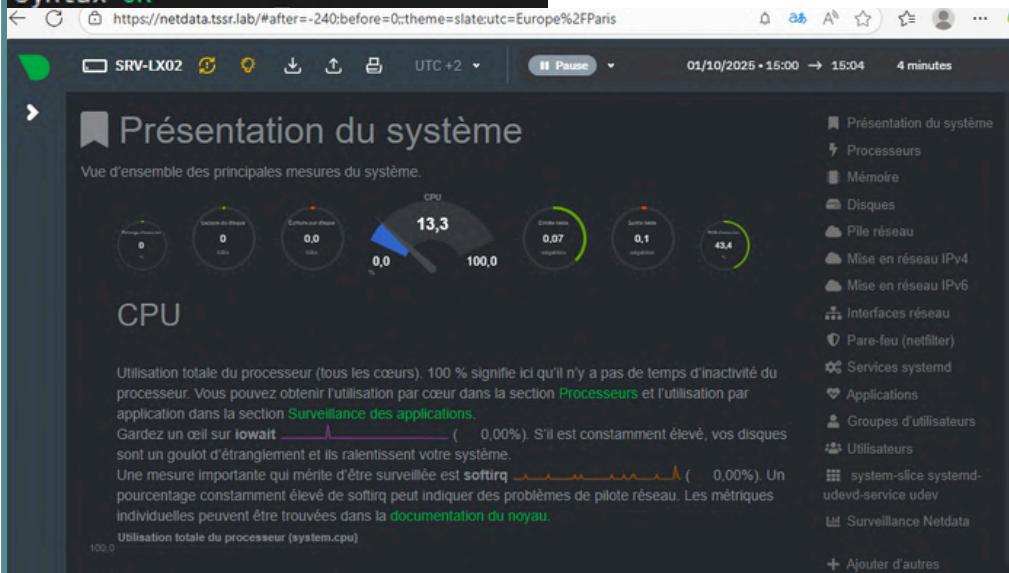
</VirtualHost>
```

- Activez la configuration Apache et les modules proxy :

```
root@SRV-LX12:~# a2ensite netdata.conf
a2enmod proxy
a2enmod proxy_http
a2enmod rewrite
Enabling site netdata.
To activate the new configuration, you need to run:
    systemctl reload apache2
Enabling module proxy.
To activate the new configuration, you need to run:
    systemctl restart apache2
Considering dependency proxy for proxy_http:
Module proxy already enabled
Enabling module proxy_http.
To activate the new configuration, you need to run:
    systemctl restart apache2
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
```

- Vérification la syntaxe de la configuration d'Apache2.

```
root@SRV-LX12:~# apachectl -t
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using SRV-LX12. You probably need to run apachectl under a
Syntax OK
```



## 4. Sécurisation HTTPS

- Installer Certbot et générer un certificat SSL :

```
root@SRV-LX12:~# apt install -y certbot python3-certbot-apache
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
root@SRV-LX12:~# certbot --apache -d glpi.tssr.lab
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel):
Invalid email address: .

If you really want to skip this, you can run the client with
--register-unsafely-without-email but you will then be unable to receive notice
about impending expiration or revocation of your certificates or problems with
your Certbot installation that will lead to failure to renew.

Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): degon77537@bitmens.com
```

- Redirection automatique HTTP → HTTPS activée.
- Accès désormais via : https://monitor.tssr.lab

## 5. Restriction d'accès (LAN uniquement)

- Dans /etc/netdata/netdata.conf :

```
GNU nano 7.2                                         /etc/netdata/netdata.conf
# NetData Configuration

# The current full configuration can be retrieved from the running
# server at the URL
#
#   http://localhost:19999/netdata.conf
#
# for example:
#
#   wget -O /etc/netdata/netdata.conf http://localhost:19999/netdata.conf
#
[global]
  run as user = netdata
  web files owner = root
  web files group = root
  # Netdata is not designed to be exposed to potentially hostile
  # networks. See https://github.com/netdata/netdata/issues/164
  bind socket to IP = 10.10.10.52
[web]
  bind to = 10.10.10.0/24
```

- Redémarrer :

```
root@SRV-LX12:~# systemctl restart netdata
```

## 6. Sécurisation du serveur Linux

Activation et configuration du pare-feu UFW :

- Autoriser uniquement les ports nécessaires (SSH, HTTPS, Netdata LAN).
- Vérifier l'état du pare-feu et la numérotation des règles.

```
root@SRV-LX12:~# ufw allow 22/tcp # SSH
ufw allow 443/tcp # HTTPS GLPI
ufw allow from 10.10.10.0/24 to any port 19999 proto tcp # Netdata LAN
ufw enable
ufw status verbose
Skipping adding existing rule
Skipping adding existing rule (v6)
Skipping adding existing rule
Skipping adding existing rule (v6)
Rules updated
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active
root@SRV-LX12:~# ufw status numbered
Status: active

      To          Action    From
      --          ----
[ 1] 19999/tcp    ALLOW IN  Anywhere
[ 2] 22/tcp       ALLOW IN  Anywhere
[ 3] 443/tcp      ALLOW IN  Anywhere
[ 4] 19999/tcp    ALLOW IN  10.10.10.0/24
[ 5] 19999/tcp (v6) ALLOW IN  Anywhere (v6)
[ 6] 22/tcp (v6)  ALLOW IN  Anywhere (v6)
[ 7] 443/tcp (v6) ALLOW IN  Anywhere (v6)
```

Installation et activation de Fail2ban :

- Installation du paquet.
- Activation du service au démarrage.
- Protection automatique contre les tentatives de connexion SSH/Apache répétées.

```
root@SRV-LX12:~# apt install -y fail2ban
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
root@SRV-LX12:~# systemctl enable --now fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
```

# Installation de Joomla et Nextcloud - Hatim / Geoffrey

## Pré-requis

- Serveur Debian 12 (IP : 10.10.10.55).
- VLAN :
  - VLAN 10 : Serveurs (Nextcloud/Joomla).
  - VLAN 20 : Clients.
  - VLAN 30 : Internet (WAN).
  - VLAN 99 : Infrastructure (ESXi, vCenter, SAN).
- DNS ou fichiers hosts configurés pour cloud.tssr.lab et intranet.tssr.lab.
- Accès root.

## 1. Installation de la stack LAMP

- Installer Apache, MariaDB et PHP :
  - apt install -y apache2 mariadb-server libapache2-mod-php \
  - php php-mysql php-xml php-mbstring php-curl php-zip php-gd php-intl
- Activer et démarrer :
  - systemctl enable apache2 mariadb
  - systemctl start apache2 mariadb
- Tester via : <http://10.10.10.55> (Apache2 Debian Default Page).



## 2. Configuration MariaDB

- Sécuriser l'installation :
  - mysql\_secure\_installation
- Créer base et utilisateur pour Joomla :
  - mysql -u root -p

```
MariaDB [(none)]> CREATE DATABASE joomla_db CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'illyes'@'localhost' IDENTIFIED BY 'Azerty1@';
CREATE DATABASE nextcloud_db CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE USER 'alexandre'@'localhost' IDENTIFIED BY 'Azerty1@';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON joomla_db.* TO 'illyes'@'localhost';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]>
MariaDB [(none)]> CREATE DATABASE nextcloud_db CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'alexandre'@'localhost' IDENTIFIED BY 'Azerty1@';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'alexandre'@'localhost';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]>
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> EXIT;
Bye

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database      |
+-----+
| information_schema |
| joomla_db      |
| mysql          |
| nextcloud_db    |
| performance_schema |
| sys            |
+-----+
6 rows in set (0,000 sec)

MariaDB [(none)]>
MariaDB [(none)]> SELECT User, Host FROM mysql.user;
+-----+-----+
| User   | Host    |
+-----+-----+
| alexandre | localhost |
| illyes    | localhost |
| mariadb.sys | localhost |
| mysql     | localhost |
| root      | localhost |
+-----+-----+
5 rows in set (0,001 sec)
```

### 3. Installation de Joomla

- Télécharger et déployer :
  - cd /var/www/
  - wget https://downloads.joomla.org/cms/joomla5/5-1-1/Joomla\_5-1-1-Stable-Full\_Package.zip
  - unzip Joomla\_5-1-1-Stable-Full\_Package.zip -d joomla
  - chown -R www-data:www-data /var/www/joomla
- Crée un VirtualHost Apache :
  - nano /etc/apache2/sites-available/joomla.conf

```
GNU nano 7.2
<VirtualHost *:80>
    ServerName intranet.tssr.lab
    DocumentRoot /var/www/joomla
    <Directory /var/www/joomla>
        AllowOverride All
        Require all granted
    </Directory>
    Alias /joomla /var/www/joomla
</VirtualHost>
```

- Désactiver le site par défaut et activer Joomla :
  - a2dissite 000-default.conf
  - systemctl reload apache2
- Activer le site et reload Apache :
  - a2ensite joomla.conf
  - a2enmod rewrite
  - systemctl reload apache2
- Lancer l'installateur web :
  - Langue : Français.
  - Nom du site : Intranet PME.
  - Super-Utilisateur : admin / mot de passe fort.
  - Base : joomla\_db, user joomla\_user.
- Connexion à l'administration : http://intranet.tssr.lab/administrator.

The screenshot shows the Joomla 5.1.1 installation process at the 'Informations de connexion' (Connection Information) step. The form fields are as follows:

- Choix de la langue d'installation:** French (fr-FR) | French (fr-FR)
- Choix du nom du site:** Saisissez le nom de ce site \* Veuillez remplir ce champ. Intranet PME
- Informations de connexion:**
  - Saisissez le nom/prénom du 'Super Utilisateur' principal \* Administrateur Intranet
  - Saisissez un nom d'utilisateur pour ce compte 'Super Utilisateur' \* admin
  - Saisissez un mot de passe pour ce compte 'Super Utilisateur' \* Azerty12345@
  - Mot de passe accepté Saisissez au minimum 12 caractères
  - Saisissez une adresse e-mail pour ce compte 'Super Utilisateur' \* admin@tssr.lab
- Configuration de la base de données:**
  - Sélectionnez le type de base de données à utiliser \* MySQL
  - Entrez le nom d'hôte, généralement "localhost" ou un nom fourni par votre hébergeur. \* localhost
  - Veuillez saisir le nom d'utilisateur de la base de données que vous avez créé ou un nom d'utilisateur fourni par votre hébergeur. \* iHys
  - Veuillez saisir le mot de passe de la base de données que vous avez créé ou un mot de passe fourni par votre hébergeur. \* Azerty1@
  - Saisissez le nom de la base de données \* joomla\_db
  - Saisissez un préfixe de table ou utilisez celui généré aléatoirement \* adwks\_
  - Si vous utilisez une base de données existante avec des tables ayant le même préfixe, Joomla renommera les tables existantes en leur ajoutant le préfixe "bak\_".
  - Cryptage de la connexion \* Par défaut (contrôlé par le serveur)

**Buttons:**

- Configuration des données de connexion > (highlighted with a red box)
- Configuration de la connexion à la base de données >
- Installer Joomla >

## 4. Installation de Nextcloud

- Télécharger et déployer :
  - cd /var/www/
  - wget https://download.nextcloud.com/server/releases/nextcloud-29.0.1.zip
  - unzip nextcloud-29.0.1.zip -d nextcloud
  - chown -R www-data:www-data /var/www/nextcloud
- Créer un VirtualHost
  - nano /etc/apache2/sites-available/nextcloud.conf

```
GNU nano 1.2
<VirtualHost *:80>
    ServerName cloud.tssr.lab
    DocumentRoot /var/www/nextcloud

    <Directory /var/www/nextcloud>
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

- Activer Nextcloud et modules Apache nécessaires :
  - a2ensite nextcloud.conf
  - a2enmod rewrite headers env dir mime
  - systemctl reload apache2

## 5. Séparation Joomla et Nextcloud (Apache)

- Pour éviter les conflits entre Joomla et Nextcloud :
  - Utiliser ServerAlias pour différencier (cloud.tssr.lab, intranet.tssr.lab).
  - Renommer nextcloud.conf en 001-nextcloud.conf pour qu'il soit chargé en priorité.
- Résultat attendu :
  - http://10.10.10.55 → Nextcloud.
  - http://10.10.10.55/joomla → Joomla.
  - http://cloud.tssr.lab → Nextcloud.
  - http://intranet.tssr.lab → Joomla.

## 6. Sécurisation

- Le serveur Debian hébergeant Joomla et Nextcloud est situé dans le VLAN 10 (Serveurs).
- VLAN 20 : Clients (postes utilisateurs).
- VLAN 30 : Internet (WAN).
- VLAN 99 : Infrastructure (ESXi, vCenter, SAN, etc.).
- Objectif : rendre Nextcloud accessible uniquement depuis VLAN 10 et VLAN 20, jamais directement depuis VLAN 30.
- Modification du fichier /var/www/nextcloud/config/config.php pour n'autoriser que :
  - cloud.tssr.lab
  - 10.10.10.55

```
CONFIG = array (
    'instanceid' => 'ocm4v0wuw8ca',
    'passwordsalt' => 'TfiSYApf35x+GoHfFspaPzRhP6qXo0',
    'secret' => 'nrzhes2mbHio1dbBnfocju/RGD99KjoIaLDv3ib+BESnfE',
    'trusted_domains' => [
        array (
            0 => 'cloud.tssr.lab',
            1 => '10.10.10.55',
        ),
        'datadirectory' => '/var/www/nextcloud/data',
        'dbtype' => 'mysql',
        'version' => '29.0.1.1',
        'overwrite.cli.url' => 'http://10.10.10.55',
        'dbname' => 'nextcloud_db',
        'dbhost' => 'localhost',
        'dbport' => '',
        'dbtableprefix' => 'oc_',
        'mysql.utf8mb4' => true,
        'dbuser' => 'alexandre',
        'dbpassword' => 'Azerty1@',
        'installed' => true
    ],
)
```

- Installation de Certbot :
  - apt install -y certbot python3-certbot-apache
- Génération certificat SSL (Let's Encrypt) :
  - certbot --apache -d cloud.tssr.lab
- Accès sécurisé : https://cloud.tssr.lab.
- Redirection automatique HTTP → HTTPS.

- Mise en place d'une tâche cron pour Nextcloud :

```
# m h dom mon dow   command
*/5 * * * * php -f /var/www/nextcloud/cron.php
```

- Ajout d'en-têtes de sécurité dans le VirtualHost :

```
<VirtualHost *:80>
    ServerName cloud.tssr.lab
    DocumentRoot /var/www/nextcloud

    <Directory /var/www/nextcloud>
        AllowOverride All
        Require all granted
    </Directory>

    <IfModule mod_headers.c>
        Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
        Header always set X-Content-Type-Options "nosniff"
        Header always set X-Frame-Options "SAMEORIGIN"
        Header always set Referrer-Policy "no-referrer"
    </IfModule>
```

## 7. Synchronisation de Nextcloud avec Joomla

- Installation du plugin mini orange sur Joomla

The screenshot shows the Nextcloud administration interface under the "Administration" tab. In the sidebar, "Sécurité" is selected. On the main page, there is a section titled "Clients OAuth 2.0" with a sub-section "intranet". It displays a client entry for "intranet" with the following details:

- Nom: intranet
- URI de redirection: https://intranet.tssr.lab/api/index.php/v1/miniorangeoauth
- Identifiant du client: FLUE6jXtpKvvi3Vco173JPAPdyMdsp7qnKpWZJVdFLKrceO1aRuS53aqb3kpzAP
- Clé secrète: \*\*\*\*

Below this, there is a button "Ajouter un client" and a search bar.

- On renseigne le nom du client (intranet) et l'url de redirection (<https://intranet.tssr.lab/api/index.php/v1/miniorangeoauth>).
- Une fois validée, est généré automatiquement un id client et une clé secrète
  - Id client :  
FLUE6jXtpKvvi3Vco173JPAPdyMdsp7qnKpWZJVdFLKrceO1aRuS53aqb3kpzAP
  - Clé secrète :  
uWQTZUak5ZeEuYnfC02oqQ2Z2G7Js2e4pJEgAgrusurml1xg7R6fLWdKEq6Vs  
z59
- On revient dans la configuration de Oauth :

The screenshot shows the Joomla! OAuth Client configuration interface. The left sidebar shows the "Components" menu with "miniorange OAuth Client" selected. The main panel shows the "Configure OAuth" step 2 (client ID & Secret) configuration. The "Client ID" field contains "FLUE6jXtpKvvi3Vco173JPAPdyMdsp7qnKpWZJVdFLKrceO1aRuS53aqb3kpzAP" and the "Client Secret" field contains "uWQTZUak5ZeEuYnfC02oqQ2Z2G7Js2e4pJEgAgrusurml1xg7R6fLWdKEq6Vs  
z59". Below this, the "Test Configuration" button is highlighted, and a modal window titled "TEST SUCCESSFUL" is displayed, showing a large green checkmark icon.

### ATTRIBUTES RECEIVED:

ATTRIBUTE NAME	ATTRIBUTE VALUE
ocs.meta.status	ok

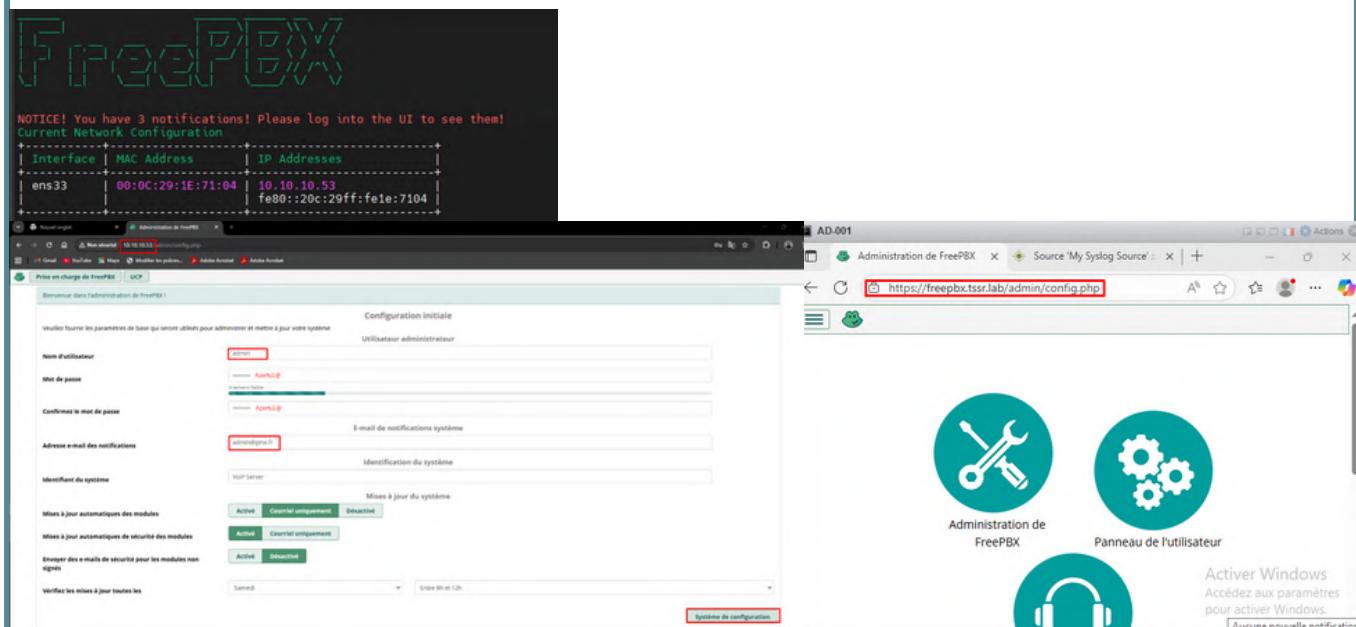
# Mise en place de Syslog et FreePBX - David

## Pré-requis

- Serveur Debian 12 (IP : 10.10.10.53, hostname pbx.local).
- Rôles :
- FreePBX 17 pour la VoIP.
- LogAnalyzer pour la collecte/visualisation Syslog.
- Accès root.

## 1. Installation et configuration FreePBX

- Mise à jour + hostname :
  - sudo timedatectl set-ntp true
  - sudo apt update && sudo apt -y full-upgrade
  - sudo reboot
  - sudo hostnamectl set-hostname pbx.local
  - echo "10.10.10.53 pbx.local pbx" | sudo tee -a /etc/hosts
  - sudo apt -y install git curl ca-certificates
  - apt -y install git
- Installation FreePBX 17 (script officiel Debian 12) :  
Le script officiel “GNU GPL Install Script” installe FreePBX 17 sur Debian 12. Exécuté sur un Debian propre (pas de LAMP pré-installé).
  - cd ~
  - git clone https://github.com/FreePBX/sng\_freespbx\_debian\_install
  - cd sng\_freespbx\_debian\_install
  - sudo ./sng\_freespbx\_debian\_install.sh
- Connexion web : http://10.10.10.53/ (admin / azerty1@).



## 2. Préparation Apache et Reverse Proxy

- Ajouter les ports backend 8081/8443 :
  - echo -e "Listen 8081\n<IfModule ssl\_module>\nListen 8443\n</IfModule>" | sudo tee -a /etc/apache2/ports.conf
- Activer les modules nécessaires.
  - sudo a2enmod proxy proxy\_http proxy\_html headers rewrite ssl
  - sudo apache2ctl configtest && sudo systemctl reload apache2

```
root@SRV-LX12:~# # Ajouter les ports backend pour LogAnalyzer
echo -e "Listen 8081\n<IfModule ssl_module>\nListen 8443\n</IfModule>" | sudo tee -a /etc/apache2/ports.conf

# Activer les modules nécessaires
sudo a2enmod proxy proxy_http proxy_html headers rewrite ssl
sudo apache2ctl configtest && sudo systemctl reload apache2
```

- Vérifier la configuration :

```
Listen 8081
<IfModule ssl_module>
  Listen 8443
</IfModule>
Enabling module proxy.
Considering dependency proxy for proxy_http:
Module proxy already enabled
Enabling module proxy_http.
Considering dependency proxy for proxy_html:
Module proxy already enabled
Considering dependency xml2enc for proxy_html:
Enabling module xml2enc.
Enabling module proxy_html.
Enabling module headers.
Module rewrite already enabled
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
To activate the new configuration, you need to run:
  systemctl restart apache2
Syntax OK
root@SRV-LX12:~#
```

### 3. Installation de LogAnalyzer

- Télécharger et déployer LogAnalyzer 4.1.13 :
  - cd /tmp
  - rm -f loganalyzer-\*.tar.gz
  - wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
  - Attention de vérifier que c'est bien une archive gzip et non HTML
- Extraction et déploiement :
  - tar -xzf loganalyzer-4.1.13.tar.gz
  - sudo mkdir -p /var/www/html/loganalyzer
  - sudo cp -r loganalyzer-4.1.13/src/\* /var/www/html/loganalyzer/
  - sudo cp loganalyzer-4.1.13/contrib/configure.sh /var/www/html/loganalyzer/
  - sudo chown -R www-data:www-data /var/www/html/loganalyzer

```
root@pbx:~# cd /tmp
rm -f loganalyzer-*.tar.gz
# Lien direct (officiel) vers l'archive 4.1.13
wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
# Vérifie que c'est bien une archive gzip, pas du HTML
file loganalyzer-4.1.13.tar.gz

# Extraction + déploiement
tar -xzf loganalyzer-4.1.13.tar.gz
sudo mkdir -p /var/www/html/loganalyzer
sudo cp -r loganalyzer-4.1.13/src/* /var/www/html/loganalyzer/
sudo cp loganalyzer-4.1.13/contrib/configure.sh /var/www/html/loganalyzer/
sudo chown -R www-data:www-data /var/www/html/loganalyzer
--2025-09-26 12:53:38--  https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
Résolution de download.adiscon.com (download.adiscon.com). 95.217.26.43, 2a01:4f9:01f:8033::1
Connexion à download.adiscon.com (download.adiscon.com)|95.217.26.43|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 5030126 (4,8M) [application/x-gzip]
Sauvegarde en : < loganalyzer-4.1.13.tar.gz >
loganalyzer-4.1.13.tar.gz 100%[=====] 4,80M 6,57MB/s   ds 0,7s
2025-09-26 12:53:39 (6,57 MB/s) - < loganalyzer-4.1.13.tar.gz > sauvegardé [5030126/5030126]
loganalyzer-4.1.13.tar.gz: gzip compressed data, from Unix, original size modulo 2^32 11294720
```

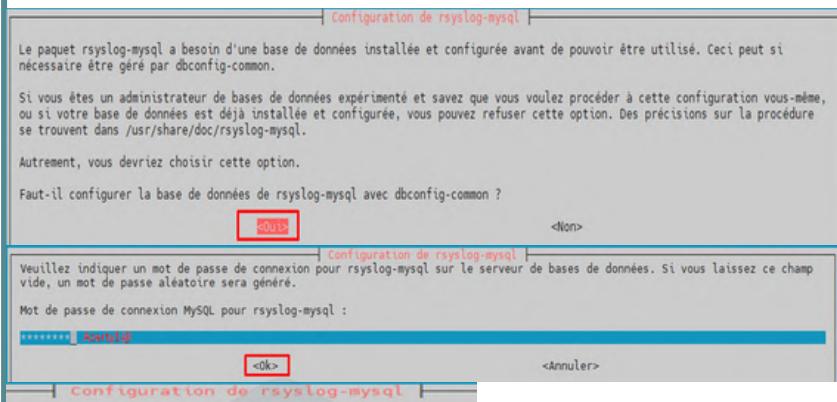
## 4. Configuration du vHost backend (8081/8443)

- Configuration Apache pour héberger LogAnalyzer sur ports backend 8081 (HTTP) et 8443 (HTTPS) et générer un certificat pour sécuriser l'accès.

## • Dernière Vérification :

## 5. Base de données Syslog

- Installation de rsyslog-mysql, création base Syslog et utilisateur rsyslog avec droits (rsyslog / azerty1@).
  - sudo apt update
  - sudo apt -y install rsyslog-mysql



- Schéma MySQL :

```
CREATE TABLE IF NOT EXISTS SystemEventsProperties (
    ID          INT UNSIGNED NOT NULL AUTO_INCREMENT,
    SystemEventID INT UNSIGNED NOT NULL,
    ParamName   VARCHAR(255) NULL,
    ParamValue   TEXT NULL,
    PRIMARY KEY (ID),
    KEY idx_SystemEventID (SystemEventID),
    CONSTRAINT fk_SystemEventsProperties_SystemEventID
        FOREIGN KEY (SystemEventID) REFERENCES SystemEvents(ID) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
SQL

sudo mysql Syslog < /tmp/rsyslog_createDB.sql
mysql -e "SHOW TABLES FROM Syslog;"
```

Tables_in_Syslog		
SystemEvents		
SystemEventsProperties		

```
mysql -e "SHOW TABLES FROM Syslog;"|grep stemEvents
+-----+
| stemEvents |
+-----+
root@pbx:/tmp#
```

```
root@pbx:/tmp# sudo mysql -e "
CREATE USER IF NOT EXISTS 'rsyslog'@'localhost' IDENTIFIED BY 'azerty1@';
CREATE USER IF NOT EXISTS 'rsyslog'@'127.0.0.1' IDENTIFIED BY 'azerty1@';
GRANT ALL ON Syslog.* TO 'rsyslog'@'localhost';
GRANT ALL ON Syslog.* TO 'rsyslog'@'127.0.0.1';
FLUSH PRIVILEGES;
"
# vérif
mysql -e "SELECT User,Host,plugin FROM mysql.user WHERE User='rsyslog';"
```

User	Host	plugin
rsyslog	localhost	mysql_native_password
rsyslog	127.0.0.1	mysql_native_password

```
root@pbx:/tmp#
```

- Test de bout en bout :

```
root@pbx:/tmp# logger -p local5.notice "TEST-ASTERISK->SQL"
sleep 1
mysql -e "SELECT ReceivedAt,FromHost,SysLogTag,LEFT(Message,80) AS Msg \
FROM Syslog.SystemEvents ORDER BY ID DESC LIMIT 3;"
```

ReceivedAt	FromHost	SysLogTag	Msg
2025-09-26 14:10:00	pbx	root:	TEST-ASTERISK->SQL
2025-09-26 14:09:08	pbx	rsyslogd:	(origin software="rsyslogd" swVersion="8.2302.0" x-pid="182370" x-info="https://imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from system
2025-09-26 14:09:08	pbx	rsyslogd:	

GESTION  
PROJET  
INFORMATIQUE

## 6. Publication de LogAnalyser dans FreePBX

- Configuration reverse-proxy dans vhosts FreePBX pour publier LogAnalyzer sur l'URL "/loganalyzer". Permet l'accès via port 443.

The screenshot shows four terminal windows side-by-side, each displaying an Apache configuration file (HTTPD.conf) with specific sections highlighted by red boxes:

- /etc/apache2/sites-available/default-ssl.conf**: Contains configurations for port 443, including a virtual host for "freepbx.tssr.lab" and SSL settings.
- /etc/apache2/sites-available/000-default.conf**: Contains configurations for port 8001, including a virtual host for "rsyslog.tssr.lab" and a directory block for "/var/www/html/loganalyzer".
- /etc/apache2/sites-available/freepbx.conf**: Contains configurations for port 8081, including a virtual host for "rsyslog.tssr.lab" and a directory block for "/var/www/html/loganalyzer".
- /etc/apache2/sites-available/logs-8081.conf**: Contains configurations for port 8081, identical to the /etc/apache2/sites-available/freepbx.conf file.

- Activation modules proxy :

```
root@pbx:/tmp# sudo a2enmod proxy proxy_http proxy_html headers rewrite
sudo apache2ctl configtest && sudo systemctl reload apache2
Module proxy already enabled
Considering dependency proxy for proxy_http:
Module proxy already enabled
Module proxy_http already enabled
Considering dependency proxy for proxy_html:
Module proxy already enabled
Considering dependency xml2enc for proxy_html:
Module xml2enc already enabled
Module proxy_html already enabled
Module headers already enabled
Module rewrite already enabled
Syntax OK
```

- Vérification de l'accès attendu :



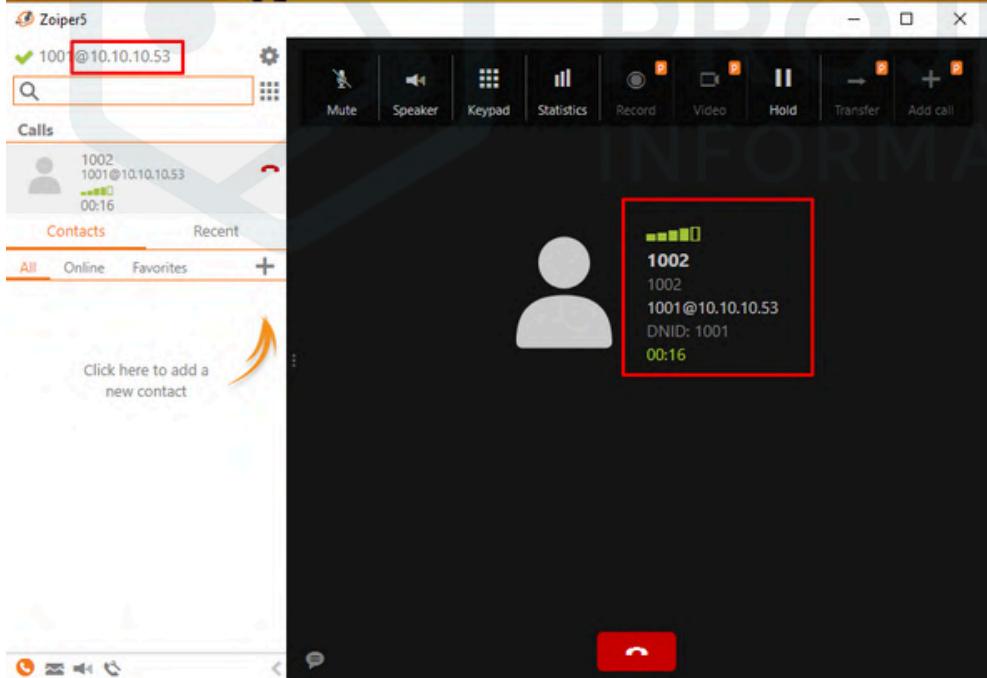
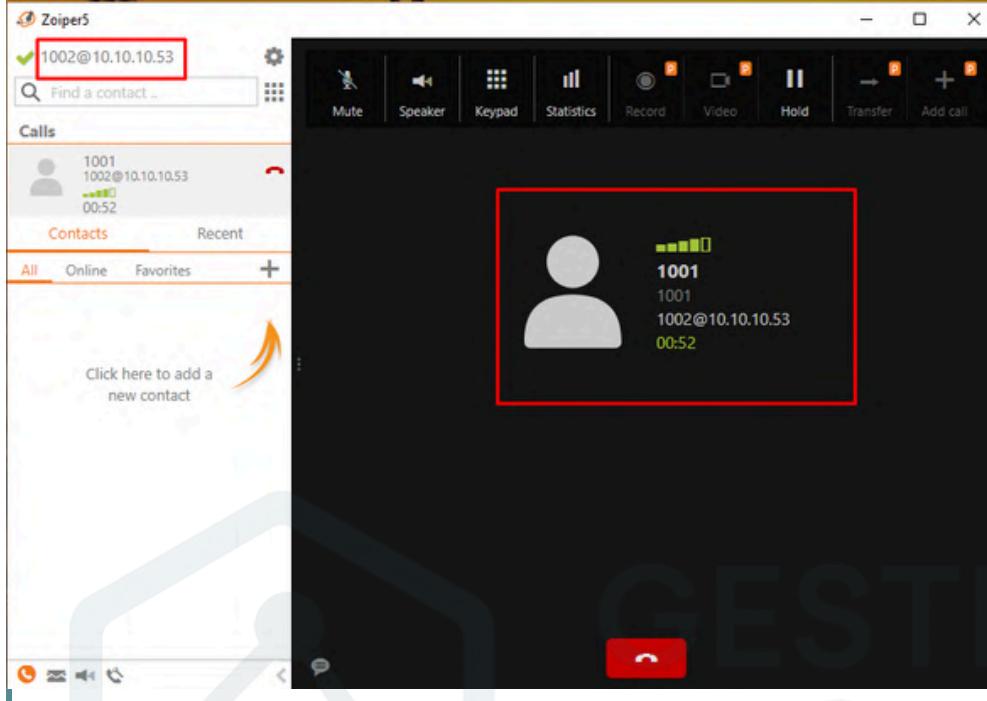
- Retirer la page Apache par défaut :

```
root@pbx:/tmp# sudo test -f /var/www/html/index.html && sudo mv /var/www/html/index.html /var/www/html/index.html.bak
sudo a2enmod rewrite
sudo sed -i '$a<Directory /var/www/>#<Directory /var/www/>\n    AllowOverride All#\n</Directory>' /etc/apache2/apache2.conf
sudo apache2ctl configtest && sudo systemctl reload apache2
Module rewrite already enabled
Syntax OK
```

- Vérification que FreePBX répond toujours
  - Connexion sur <http://10.10.10.53/admin> → Validation de l'admin.
  - Passage en HTTPS : <https://10.10.10.53/>.

## 7. Test validation FreePBX

- Tests effectués sur 2 postes clients du domaine :



## 7. Finalisation de LogAnalyzer

- Création du fichier config.php, un fichier vide où on y ajuste les droits (temporaires pour l'installation) :
  - sudo touch /var/www/html/loganalyzer/config.php
  - sudo chown www-data:www-data /var/www/html/loganalyzer/config.php
  - sudo chmod 666 /var/www/html/loganalyzer/config.php
- Vérification du propriétaire du dossier, où on s'assure que le répertoire complet appartient à l'utilisateur Apache :
  - sudo chown -R www-data:www-data /var/www/html/loganalyzer
- Accès aux logs par LogAnalyzer, création d'un fichier dédié :
  - echo 'local5.\* /var/log/asterisk-syslog.log' | sudo tee /etc/rsyslog.d/10-asterisk-file.conf
  - sudo touch /var/log/asterisk-syslog.log
  - sudo chown asterisk:asterisk /var/log/asterisk-syslog.log
  - sudo chmod 644 /var/log/asterisk-syslog.log
  - sudo systemctl restart rsyslog
- On termine l'installation via l'interface web

The screenshot shows the Adiscon LogAnalyzer interface. At the top, there is a form titled "Créer un compte utilisateur" (Create a user account) with fields for "Nom d'utilisateur" (admin), "Mot de passe" (Azerty1@), and "Répéter le mot de passe" (Azerty1@). Below this is a progress bar labeled "Progression de l'installation :" which is mostly green, with a red box highlighting the "Suivant" (Next) button. The main dashboard below the progress bar displays the title "Adiscon LogAnalyzer Version 4.1.13". It includes a navigation menu with links like "Search", "Show Events", "Statistics", "Reports", "Help", and "Admin Center". The "Admin Center" link is underlined, indicating it is the active section. The dashboard also shows a search bar with the query "facility:local0 severity:info" and a table titled "Recent syslog messages" with columns: Date, Facility, Severity, Host, Syslogtag, ProcessID, Message type, and Message. The table contains several entries from the "crontab" process on the "pbx" host, all of which are "Syslog" type messages at the "info" level.

# UEM – ManageEngine Endpoint Central - Hatim / Geoffrey

## Pré-requis

- Serveur Debian/Windows avec accès Internet pour télécharger Endpoint Central.
- Domaine tssr.lab déjà configuré (Active Directory opérationnel).
- Accès administrateur au domaine et aux machines clientes.
- Poste client disponible pour installer et tester l'agent.

## 1. Installation et accès à Endpoint Central

- Télécharger l'application depuis le site officiel de ManageEngine.
- Suivre l'assistant d'installation sur le serveur choisi.
- Lancer l'interface web de gestion après installation.

The screenshot shows two windows of the ManageEngine Endpoint Central Setup wizard. The left window is titled 'ManageEngine Endpoint Central Setup' and displays the 'Bienvenue dans le programme d'installation de ManageEngine Endpoint Central' screen. It contains a brief description of the installation process and a large blue background graphic. The right window is titled 'ManageEngine Endpoint Central Setup' and displays the 'Panneau de sélection des ports' screen. It asks for server port details, with 'Port HTTP' set to 8020 and 'Port HTTPS' set to 8383. Both windows have standard Windows-style navigation buttons ('Précédent', 'Suivant', 'Annuler' or 'Cancel').

The screenshot shows the 'Endpoint Central' web interface. At the top, there's a banner with the message 'Bienvenue chez Endpoint Central !'. Below it, a callout box says 'Nouvel appareil intégré !' and 'The computer "svr-uem" has been successfully onboarded.' A 'Voir les détails de l'appareil' button is shown. The main dashboard includes sections for 'Alertes' (11), 'Informations' (11), and 'Le référentiel de logiciels n'a pas encore été configuré'. It also shows 'Packages non publiés dans SSP' (0) and 'Packages dans SSP qui ne sont pas utilisés' (0). On the right, there's a detailed view of a device named 'svr-uem' under the 'Ordinateurs' tab, showing its status as 'Installé avec succès' on '25.05.2020 01:55 PM' by 'svr-uem'. The interface is clean with a dark header and light-colored cards for different sections.

## 2. Déploiement de l'agent sur une machine cliente

- Depuis la console Endpoint Central, accéder à l'onglet Ordinateurs.
- Lancer l'option Ajouter des ordinateurs.

The screenshot shows the Endpoint Central dashboard. The left sidebar has sections like 'Résumé', 'Domaine', 'Bureaux distants', and 'Ordinateurs'. The main area displays a message about domain password expiration and a warning about unsupported operating systems. Below is a table of computers with columns for name, domain, status, last contact, version, remarks, processor architecture, location, and user. A red box highlights the 'Ajouter des ordinateurs' button.

- Les OU du domaine tssr.lab apparaissent, avec la liste des machines associées.
- Sélectionner la machine cible (exemple : client-nomade).
- Déployer l'agent sur ce poste.
- Une fois l'agent installé, vérifier que l'état affiché est Installé avec succès.

This screenshot shows the 'Ajouter des ordinateurs' dialog. It has tabs for 'Domaines' (selected) and 'Sélectionné (0)'. On the left is a tree view of the domain structure under 'tssr'. A red box highlights the 'tssr' node. To the right is a table titled 'Masquer les ordinateurs gérés' showing computer objects from various domains like AD-01, PEX, SRV-INTRANET, and SRV-LX02. The table includes columns for name, type, and status. At the bottom are 'Suivant' and 'Annuler' buttons.

### 3. Création de packages logiciels

- Depuis la console Endpoint Central, aller dans l'onglet Déploiement logiciel.
- Choisir Créer un package → sélectionner Windows comme plateforme.
- Renseigner l'application à installer : Mozilla Firefox.
- Activer l'option Mettre automatiquement à jour à la dernière version pour que Firefox reste toujours à jour.
- Enregistrer le package.

The screenshot displays the Endpoint Central interface, specifically the 'Déploiement logiciel' (Deployment Software) section. On the left, a sidebar shows navigation options like 'Création de package', 'Déploiement', 'Rapports', and 'Paramètres'. The main area shows a list of packages under 'Packages non publiés dans SSP'. A new package is being created for 'Google Chrome (x64) (141.0.7390.54, 141.0.7390.55)'. The configuration screen includes fields for 'Nom du package' (set to 'Google Chrome (x64) (141.0.7390.54, 141.0.7390.55)'), 'Emplacement de téléchargement' (set to 'googlechromestandaloneenterprise64.msi'), and 'Taille du téléchargement' (set to '131 MB'). Below this, the 'Cible' (Target) configuration is shown, with a summary table and detailed tabs for 'Résumé', 'Détails de la configuration', 'État d'exécution', and 'Détails de la réplication'. The 'État d'exécution' tab shows a green circle indicating success ('Réussi') and a legend for execution status: En att... (yellow), Réussi (green), En cours (blue), Échec (red), Non ap... (dark blue), Nouvell... (orange), and En cou... (dark red). The 'Résumé' tab provides a detailed view of the configuration parameters.

# Installation et configuration FreeNas - Alexandre / Anthony

## Pré-requis

- ISO FreeNAS disponible.
- Une VM dédiée sur ESXi avec au moins :
  - 2 vCPU, 4 Go RAM.
  - Un disque système + un disque de données (ex. 400 GiB).
- Réseau configuré (IP fixe pour FreeNAS).

## 1. Installation de FreeNAS

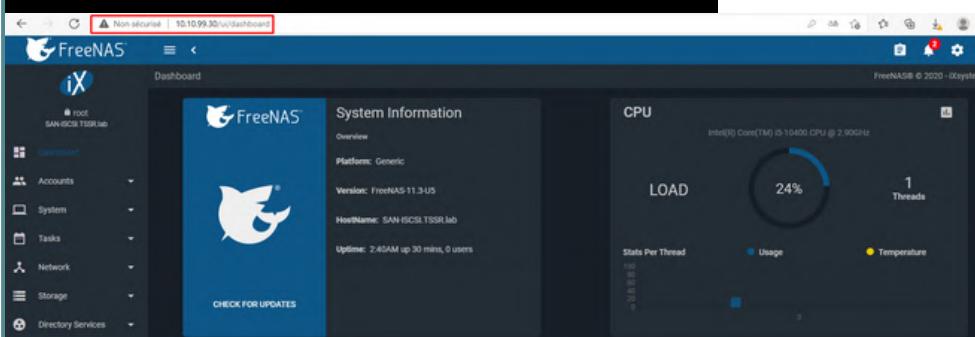
- Créer une VM sur VMware ESXi.
- Monter l'ISO FreeNAS et l'installer.
- Définir une adresse IP statique pour FreeNAS.
- Accéder à l'interface web via navigateur :

```
FreeBSD/amd64 (SAN-ISCSI.TSSR.lab) (ttyv0)

Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:
http://10.10.99.30
https://10.10.99.30

Enter an option from 1-11: ■
```



### 3. Configuration du réseau et ajout disque

- Définir le hostname et le domaine (tssr.lan).
- Passerelle : 10.10.99.254, DNS : 10.10.10.40.
- Importer le disque de données (400 GiB) dans FreeNAS.

The screenshot shows the FreeNAS configuration interface. At the top, there's a list of network settings:

- Hostname: SAN-ISCSI
- Domain: TSSR.lab
- Additional Domains:

  - IPv4 Default Gateway: 10.10.99.254
  - IPv6 Default Gateway:

    - Nameserver 1: 10.10.10.40
    - Nameserver 2
    - Nameserver 3

- HTTP Proxy
- Enable netwait feature

Below these is a "Host name database" section with a "SAVE" button.

At the bottom, there's a "Disk" configuration section for a new volume:

- Volume name: pool-esa\data
- Comments
- Size for this vvol\*: 280.00 GiB
- Force size
- Sync: Inherit (standard)
- Compression level\*: Inherit (gzip)
- ZFS Deduplication\*: Inherit (off)

At the bottom right are "SAVE" and "CANCEL" buttons.

GESTION  
PROJET  
INFORMATIQUE

## 4. Partage iSCSI dans FreeNAS

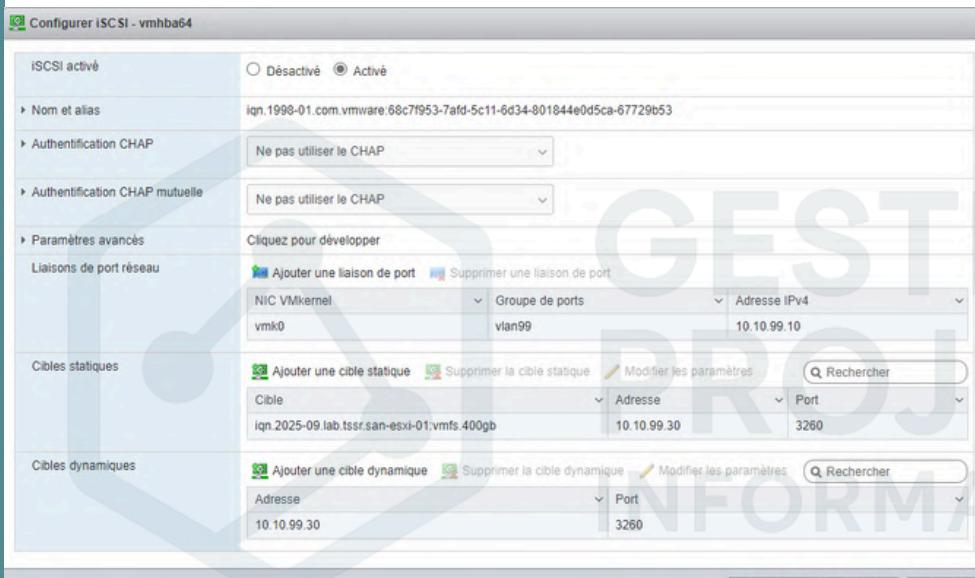
- Aller dans Sharing → Block Shares (iSCSI).
- Étapes principales :
- Disks : définir les disques utilisables (ex. 400 GiB).
- Portals : définir l'IP et le port (3260).
- Initiators : limiter l'accès au réseau 10.10.99.0/24.
- Targets : créer une cible iSCSI.
- Extents : créer un LUN basé sur le disque.
- Associated Targets : associer extent ↔ target.

The screenshot shows the FreeNAS web interface with the following sections visible:

- Disks**: A table showing a single disk entry: ada0 (400 GiB).
- Portals**: A table showing one portal: 1 (IP: 10.10.99.30:3260, Description: portal1, Auth Method: NONE).
- Initiators**: A table showing one initiator group: 1 (Network: 10.10.99.0/24).
- Targets**: A table showing one target: iqn.2025-09.lab.tsrr.san-esxi-01:vmfs.400gb.
- Extents**: A table showing one extent: vmfs\_400gb (Serial: 000c295e6063000, NAA: 0x6589fc000000be238bbfb2f3, Enabled: yes).
- Associated Targets**: A table showing one association: iqn.2025-09.lab.tsrr.san-esxi-01:vmfs.400gb (LUN ID: 0, Extent: vmfs\_400gb).

## 5. Intégration iSCSI dans ESXi

- Dans l'interface ESXi → Storage → Adapters.
- Ajouter un adaptateur iSCSI logiciel.
- Renseigner :
  - IQN de la cible.
  - Adresse IP FreeNAS (10.10.99.30).
  - Port par défaut : 3260.
- L'adaptateur iSCSI virtuel (ex. vmhba64) sert de pont entre ESXi et le stockage FreeNAS.
- Sauvegarder, puis rescanner les périphériques.
- Le disque FreeNAS apparaît comme périphérique disponible.



Nom	État	Type	Capacité	Profondeur de file	Fournisseur
Local TSSTcorp CD-ROM (mpx:vmhba0 C0 T4 L0)	Normale	CDROM	Inconnue	S/0	TSSTcorp
Local DELL Disk (naa:fb2a720d4604002d554c7506936679)	Normale	Disque	558.38 Go	64	DELL
FreeNAS iSCSI Disk (naa:6549cfc000000e2j88beb2f958c1)	Normale, Degrade	Disque (SSD)	280 Go	128	FreeNAS

## 6. Création du Datastore VMFS

- Une fois le disque iSCSI détecté par ESXi :
- Aller dans Storage → Datastores → New Datastore.
- Sélectionner le disque iSCSI découvert.
- Choisir le format VMFS6.
- Nommer le datastore (ex. SAN-VMFS).
- Finaliser l'assistant.

Le datastore est maintenant disponible pour héberger des VMs.

## 7. Validation finale

- Créer une VM de test sur le datastore iSCSI.
- Vérifier que la création du disque virtuel se fait correctement.
- Lancer la VM pour s'assurer que le stockage est fonctionnel.
- Vérifier également les logs FreeNAS et ESXi en cas de problème.

# Configuration OpenVPN - Hatim

## Pré-requis

- pfSense installé et fonctionnel.
- Accès administrateur à l'interface web.
- Interface WAN disponible (IP publique ou NAT).
- Certificats nécessaires :
  - Autorité de Certification (CA).
  - Certificat serveur.

## 1. Paramétrage du serveur OpenVPN

- Lancer l'assistant OpenVPN – Remote Access (SSL/TLS).
- Étapes principales :
  - Création d'une CA interne.
  - Génération d'un certificat serveur signé par la CA.
- Définition des paramètres :
  - Interface : WAN
  - Port : 1194/UDP
  - Chiffrement : AES-256
  - Réseau tunnel : 10.10.30.0/24
  - Accès au LAN activé.
- Les règles firewall sont créées automatiquement.

Paramètres clients avancés

Domaine DNS par défaut

Renseigner un nom de domaine par défaut aux clients.

Domaine DNS par défaut

tssr.lab

Activer le Serveur DNS

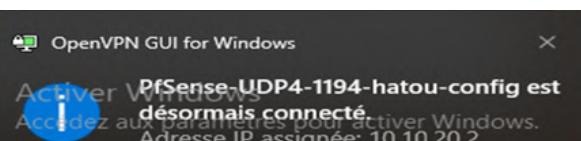
Fournir une liste de serveur DNS pour les clients. Les adresses peuvent être en IPv4 ou IPv6.

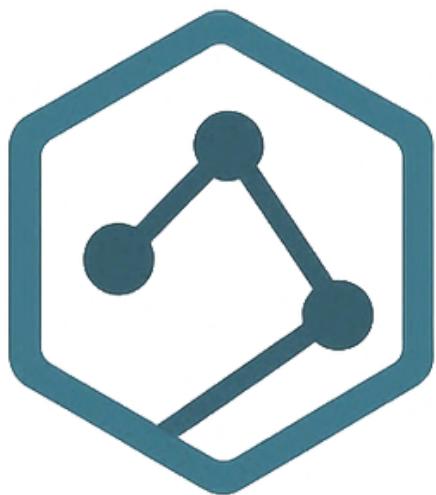
Serveur DNS 1

10.10.10.40

Propriétés utilisateur

Défini par	USER
Désactivé	<input type="checkbox"/> Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur	hatou
Mot de passe	*****
Nom complet	hatou
Nom complet de l'utilisateur, à des fins administratives uniquement	
Date d'expiration	Laissez vide si le compte ne doit pas expiration, sinon entrez la date d'expiration sous la forme MM.JJ/AAAA
Paramètres personnalisa	<input type="checkbox"/> Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.
Appartenance à un groupe	admin
Pas un membre de	Member of
<a href="#">Déplacer vers la liste "Membre de"</a>	<a href="#">Déplacer vers la liste "Non membre de"</a>
Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.	
Nom	AC
hatou	phase 1 openvpn





**GESTION  
PROJET  
INFORMATIQUE**