INSTITUTION BEAUPEYRAT
- depuis 1634 -

DIRECTION GÉNÉRALE DES
FINANCES PUBLIQUES

# RAPPORT DE STAGE

Etudiante BTS SIO, SISR 2ème année

**KIBAMBA-WILFRIDE Vhann Danielle**

Janvier-Février 2026

Tuteur de Stage : ROSSO Martin

Enseignant Principal : SAUTOUR Florent

Organisme D'accueil : DSI SUD OUEST-ESI DE POITIERS

Ecole De Formation : Institut Beaupeyrat

# SOMMAIRE

# INTRODUCTION

Dans le cadre de ma formation en **BTS Services Informatiques aux Organisations (SIO)**, option **Solutions d'Infrastructure, Systèmes et Réseaux (SISR)**, j'ai effectué un stage au sein de la **Direction Générale des Finances Publiques (DGFIP)**, sur le site de **Poitiers**.
Ce stage s'inscrit dans le parcours de formation obligatoire et a pour objectif de me permettre de découvrir le fonctionnement d'un environnement informatique professionnel.

Ce stage s'est déroulé au sein d'une administration publique disposant d'un système d'information assez complexe et fortement sécurisé, en raison de la sensibilité des données traitées.
Intégrée à une équipe informatique, j'ai pu observer l'organisation de l'infrastructure, les méthodes de travail et les outils utilisés pour assurer la disponibilité, la sécurité et la continuité des services informatiques.

Les objectifs de ce stage étaient multiples :

- découvrir le fonctionnement d'une grande infrastructure informatique
- mettre en relation les notions vues en cours avec la réalité du milieu professionnel
- comprendre les enjeux de la sécurité des systèmes d'information
- observer le travail des exploitants système et des administrateurs
- développer des compétences techniques et professionnelles en lien avec l'option **SISR**.

# I. Présentation De L'entreprise :

## a) Présentation générale de la DGFIP :

La Direction Générale des Finances Publiques **(DGFIP)** est une administration dépendant du **Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique**.
Elle a pour mission principale la gestion des finances publiques de l'État, notamment la collecte des impôts, la gestion comptable et financière ainsi que le contrôle fiscal.
Le site de Poitiers joue un rôle important dans le fonctionnement du système d'information de la DGFIP et participe à l'administration et à la sécurisation des infrastructures informatiques.

## b) Présentation Du Site de Poitiers :

La DSI Sud-Ouest – ESI de Poitiers est un centre informatique de la DGFiP chargé de l'exploitation, de la maintenance et de la sécurité des systèmes informatiques. Il fait partie d'un réseau national d'ESI et joue un rôle essentiel dans la continuité des services informatiques de l'administration fiscale

Le site de Poitiers est structuré en **équipes spécialisées**, chacune ayant des missions bien définies, telles que l'exploitation des systèmes et d'applications.

Le site est subdivisé en 2 pôles : Pôle 1 et Pôle 2. J'ai réalisé mon stage au **pôle PTS (pôle technique des systèmes)** , plus précisément dans la **zone 4**, qui correspond à la **zone d'administration**.

# II. Outils De la DGFIP :

Le système d'information de la DGFiP repose sur une dualité technologique : l'utilisation de **logiciels propriétaires** pour les besoins transverses et d'**outils métiers internes** spécifiques à leur besoin .

## a) Sauvegarde Et Supervision :

- **Time Navigator** :
  Outil de **sauvegarde**, utilisé pour assurer la protection et la restauration des données.
- **SYNAPSE** :
  Outil interne de **supervision**, permettant de surveiller l'état des systèmes et des applications.
- **ISAC :**
  Solution de supervision, il se charge de surveiller les services.
- **Munin :**

  Système de monitoring pour les serveurs admin (VMU et VCA)

## b) Gestion D'Architecture :

- **WebPoit :**

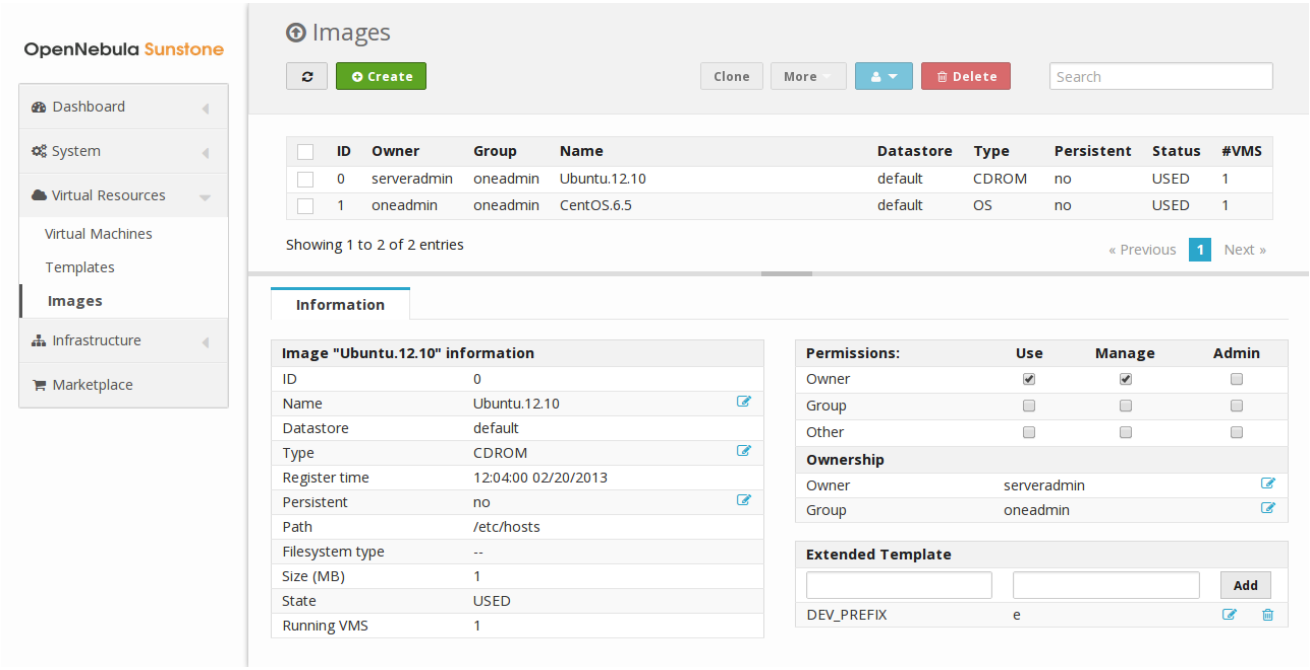
  Outil de zone 4 qui permet de faire l'inventaire des ; gérer les hosts du SPS (physiques ou virtuels) ; De recenser les informations réseau (Vlan, adresses IP …) , on y accède par une URL.
- **GESIP :**

  Gestionnaire des interventions programmées, propre à la DGFIP.
- **GLPI :**

  Outil propriétaire pour optimiser la gestion informatique
- **OMEGA :**

  Outil interne qui permet de modéliser Et de gérer l'Architecture.
- **Opennebula :**

  Orchestrateur, permet de gérer, automatiser et orchestrer des machines virtuelles sur plusieurs hyperviseurs depuis une interface centrale. elle transforme une infrastructure physique en un cloud managé Infrastructure as a Service (IaaS),




## C) Sécurité :

- **Bastion WALLIX** :

  Solution de cybersécurité spécialisée dans la gestion des accès privilégiés (PAM – *Privileged Access Management*). sert de **point de passage sécurisé** entre les utilisateurs (admins, prestataires…) et les serveurs.

- **Pare-Feu Fortinet :**

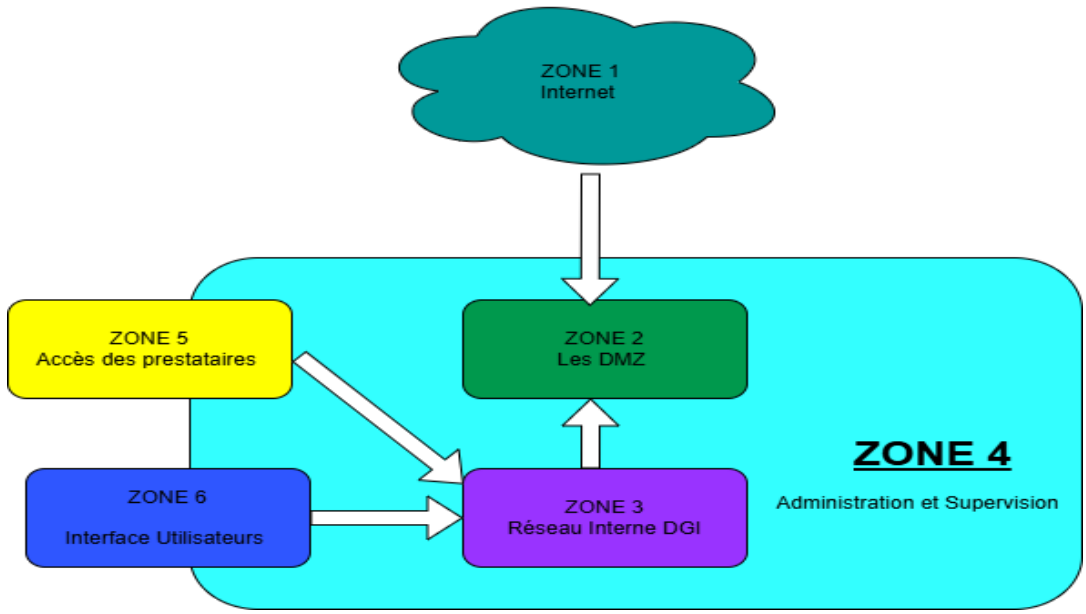
  contrôle, filtre et sécurise les flux réseau entrants et sortants d'un système ou d'un réseau.

# III. Présentation du système d'information :

## a) Vue d'ensemble de l'infrastructure :

La DSI Sud-Ouest – ESI de Poitiers est subdivisé en plusieurs zones , pour limiter les attaques, et sécuriser ses machines.

- Zone 1 : Internet
- Zone 2 : Les DMZ publiques
- Zones 3 : Le réseau Interne à la DGFIP, le LAN en quelque sorte.
- Zone 4 : Zone d'administration et de supervision (zone sécurisée)
- Zone 5 : L'accès des prestataires de services aux ressources internes.
- Zone 6 : Interface pour l'accès des utilisateurs nomades au réseau interne.




## b) **Présentation de L'environnement Technique** :

Lors de mon cinquième jour de stage, on m'a présenté l'environnement de virtualisation ainsi que l'infrastructure informatique de la DGFIP de Poitiers. Cette découverte m'a permis de mieux comprendre l'organisation des

accès administrateurs et les mesures de sécurité mises en place pour protéger les serveurs.

- **La console d'administration virtuelle : VCA**

Le **VCA** (Virtual Console Administration) est une console d'administration virtuelle. Elle est utilisée comme **poste de rebond**, c'est-à-dire un point de passage obligatoire avant d'accéder aux serveurs.

L'objectif d'une VCA est :

- d'éviter les connexions directes aux serveurs,
- de limiter les risques de manipulation ou d'erreur,
- de permettre le **travail à distance** de manière sécurisée,
- d'**importer des fichiers** sans intervenir directement sur les serveurs.

Les **exploitants système (ES)** utilisent donc le VCA pour administrer l'infrastructure sans **"s'amuser"** directement sur les serveurs de production.

- **Environnement de Virtualisation : Opennebula**

L'infrastructure repose sur un environnement de virtualisation dont l'orchestrateur **e**st Opennebula.
Opennebula permet de gérer :

- des machines virtuelles,
- les ressources (CPU, mémoire, stockage),
- et l'orchestration des environnements virtualisés.

Cet outil est utilisé pour centraliser et administrer les serveurs virtuels de manière sécurisée et organisée.

### c) <u>Sécurité / Gestion des accès :</u>

La DGFIP utilise un bastion d'administration WALLIX.
Ce bastion joue un rôle central dans la sécurité des accès administrateurs.

Il permet notamment :

- de contrôler les accès des administrateurs,
- de tracer et enregistrer les actions réalisées,
- de réaliser des inventaires des accès et des systèmes,
- de renforcer la sécurité globale de l'infrastructure.

Le bastion est donc un point de passage obligatoire avant toute action d'administration.

### d) Parcours de connexion d'un exploitant système :

Lorsqu'un exploitant système se connecte à l'infrastructure, il suit un **chemin sécurisé précis** :

1. Connexion à un **VPN nomade**.
2. Passage par l'un des pare-feux, qui filtrent et sécurisent la connexion.
3. Accès au **bastion WALLIX**.
4. Passage par la **console de rebond VCA**.
5. Accès à la **Zone 4**, qui correspond à la **zone d'administration**.

### e) Notions et Termes Abordés :

- **La matrice de flux (GMAF)**

L'infrastructure repose également sur une **matrice de flux**, qui définit les communications autorisées entre les différentes zones.

Il existe :

- des **flux standards** (ssh , http, https ...)
- des **flux non standards**,
- des **flux complémentaires**

## IV. Travaux réalisés :

## VCA DE STRASBOURG : Déploiement d'une VM & MIGRATION

Lors de cette semaine, j'ai effectué le **déploiement d'une nouvelle machine virtuelle**, appelée **VCA** au sein de la DGFIP. Ce déploiement avait pour objectif la mise à jour du système d'exploitation, en passant de **Ubuntu 20** à **Ubuntu 24.**

---

- **Procédure de déploiement**

La procédure de déploiement s'est déroulée en plusieurs étapes :

1. **Arrêt de la machine virtuelle existante**
   La machine a été arrêtée sur Opennebula, afin d'éviter tout **conflit de configuration réseau**.
2. **Extinction préalable de la VM**
   Cette étape permet de sécuriser l'opération avant le déploiement de la nouvelle instance.
3. **Utilisation du modèle Ubuntu 24**
   Un **modèle (template) Ubuntu 24** a été sélectionné pour créer la nouvelle VCA.
4. **Déploiement de la VCA**
   La nouvelle VCA a été **instanciée** à partir du modèle.
5. **Personnalisation de la VCA**
   La machine a été personnalisée en :
   - reprenant le **même nom** que l'ancienne
   - configurant les **droits d'accès**
6. **Vérification de la connectivité réseau**
   Une connexion au **pare-feu** a été effectuée afin de tester la **connectivité en SSH**.

## Ouverture des Flux :

Dans le cadre de cette mise en production, il a été nécessaire de **traduire une demande de flux réseau** en **règles de pare-feu**.

La procédure suivie est la suivante :

- analyse de la **demande de flux** (communications autorisées entre systèmes),
- création des **règles de pare-feu correspondantes**,
- application des règles **sans accès direct aux pare-feux**.

En effet, les règles ne sont pas configurées directement sur les pare-feux. Elles sont d'abord transmises à un outil appelé **Forti manager**, qui centralise la gestion et se charge de **déployer les règles sur l'ensemble des pare-feux concernés** par la mise à jour.

## Déployer et de Configurer une VM .

Je devais déployer et configurer la VM FMG (Forti Manager) depuis l'environnement KVM/Libvirt sur les hyperviseurs du PTS.

Un FortiManager, est un outil qui gère plusieurs Fortigate, il déploie les configurations. C'est l'outil central de gestion des Fortigates.

**Etapes Suivies :**

### 1. Introduction et Objectifs

- Produit : FortiManager (FMG).
- Rôle : Gestion centralisée et déploiement de configurations pour un parc de pare-feu FortiGate.
- Objectif du TP : Déployer l'Appliance virtuelle sur un cluster d'hyperviseurs KVM (PTS) via **virt-manager**

### 2. Préparation de l'environnement de travail

Avant le déploiement, une configuration du poste client a été nécessaire pour joindre les hyperviseurs.

### A. Résolution de noms (DNS Local)

Modification du fichier /etc/hosts pour mapper les noms des hyperviseurs (ptspgsh001 et ptspgsh002) à leurs adresses IP respectives sur l'interface **eno1** (interface dédiée au flux de virtualisation).

Les hyperviseurs ont 2 interfaces (idrac et en01), j'ai choisi les ip de l'interfaces eno1, parce que c'est plus adapté à la virtualisation.

**Commande :** sudo nano /etc/hosts Ajout des lignes : [IP_Hyperviseur] ptspgsh001 & ptspgsh002.

### B. Sécurisation des accès (SSH)

Génération d'une paire de clés SSH pour l'authentification sans mot de passe.

**Commande :** ssh-keygen -C 'Vhann'

Note : La clé publique a été poussée sur les 2 hyperviseurs par un administrateur PTS pour permettre la connexion distante via Libvirt.

car je ne dispose pas des droits nécessaires pour le faire. Après l'avoir fait, j'ai pu me connecter en SSH .

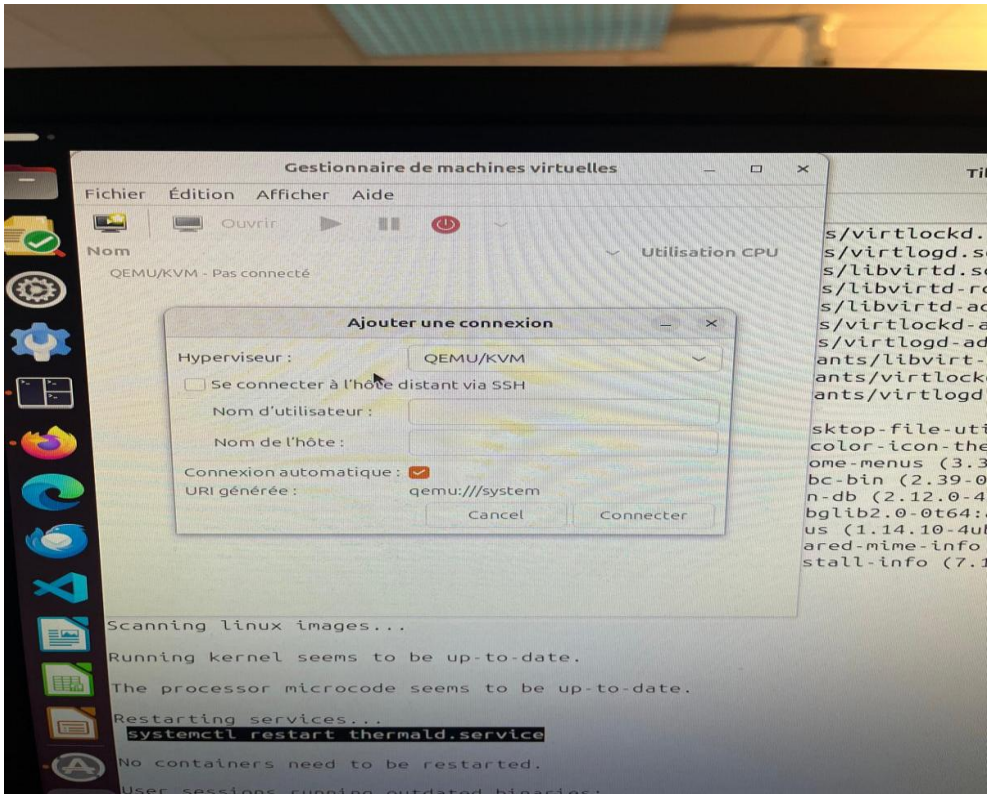
Exemple de connexion à distance : **ssh admspoit@ptspgsh001**

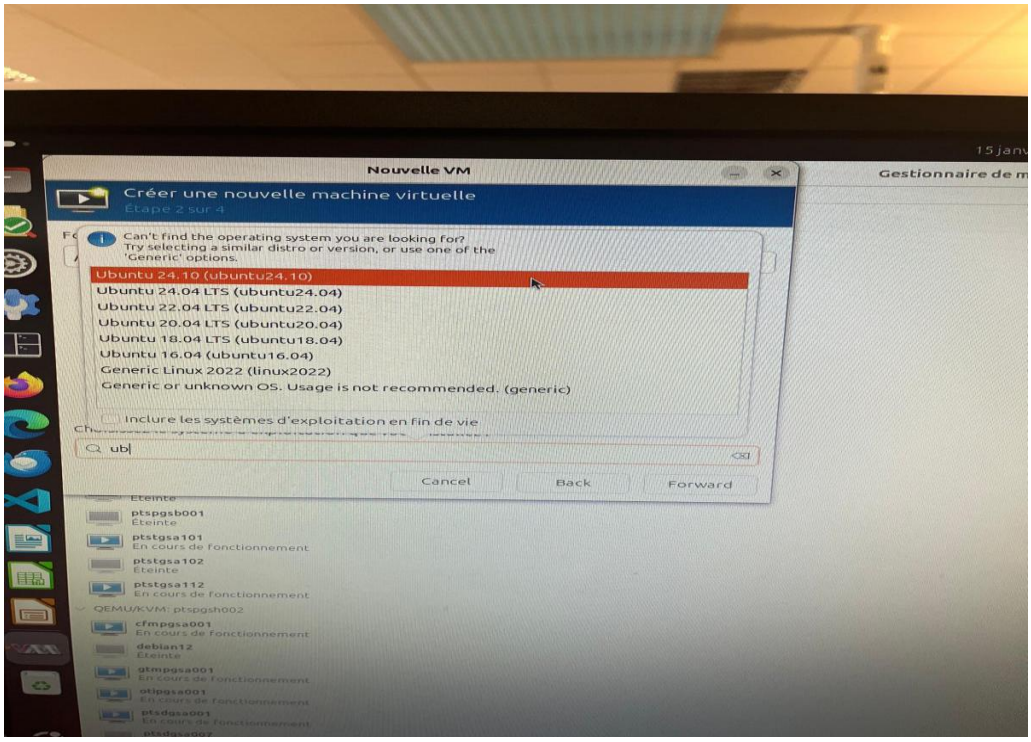
## 3. Installation des outils de gestion

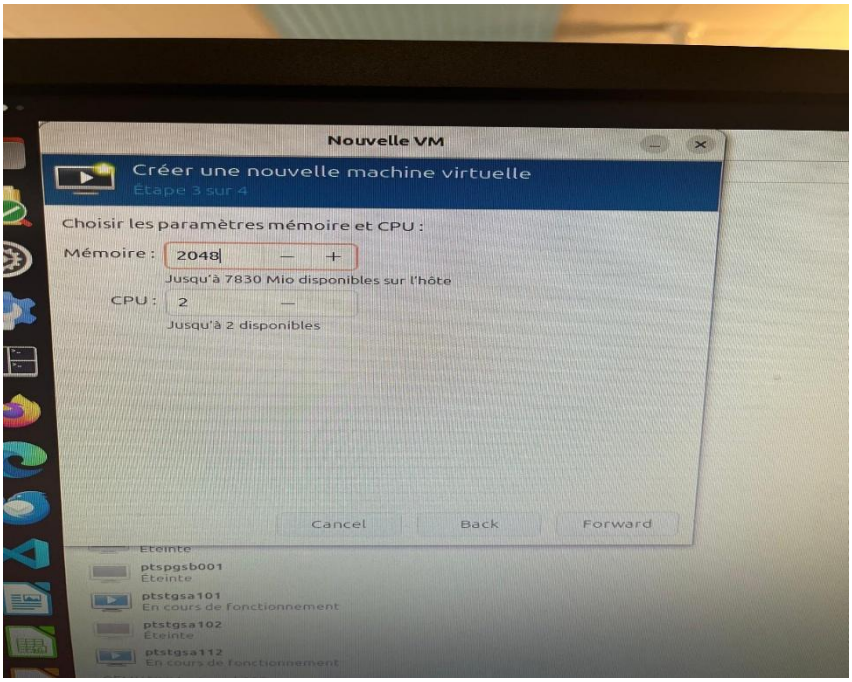
L'accès graphique aux hyperviseurs nécessite l'outil virt-manager sur le poste local.

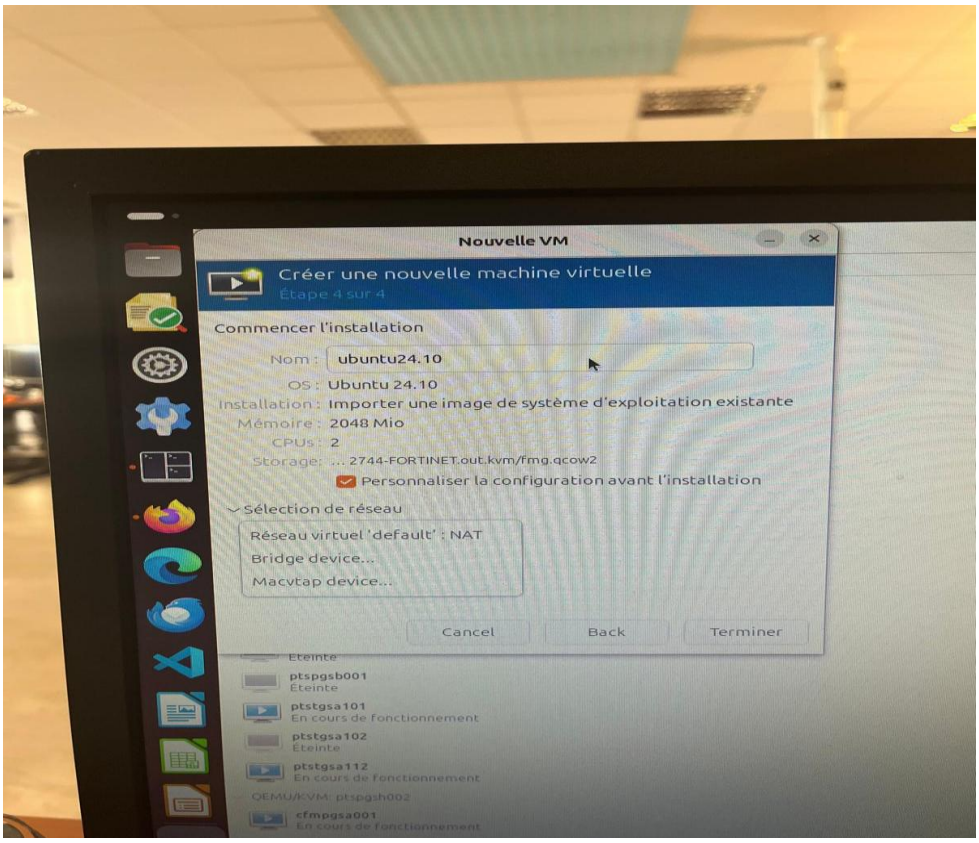
**Commandes :** sudo apt install virt-manager

Après avoir tapé la commande La fenêtre Virtual Machine Manager s'ouvre, j'ai eu l'environnement KVM qui s'est affiché, où je pourrais ajouter une connexion. J'ai rempli toutes les informations .




Nouvelle VM
Créer une nouvelle machine virtuelle
Étape 3 sur 4
Choisir les paramètres mémoire et CPU :
Mémoire : 2048
Jusqu'à 7830 Mio disponibles sur l'hôte
CPU : 2
Jusqu'à 2 disponibles
Cancel
Back
Forward
ptspgsb001
Éteinte
ptstgsa101
En cours de fonctionnement
ptstgsa102
Éteinte
ptstgsa112
En cours de fonctionnement


Nouvelle VM
Créer une nouvelle machine virtuelle
Étape 4 sur 4
Commencer l'installation
Nom : ubuntu24.10
OS : Ubuntu 24.10
Installation : Importer une image de système d'exploitation existante
Mémoire : 2048 Mio
CPUs : 2
Storage : ... 2744-FORTINET.out.kvm/fmg.qcow2
Personnaliser la configuration avant l'installation
Sélection de réseau
Réseau virtuel 'default' : NAT
Bridge device...
Macvtap device...
Cancel
Back
Terminer
ptspgsb001
Éteinte
ptstgsa101
En cours de fonctionnement
ptstgsa102
Éteinte
ptstgsa112
En cours de fonctionnement

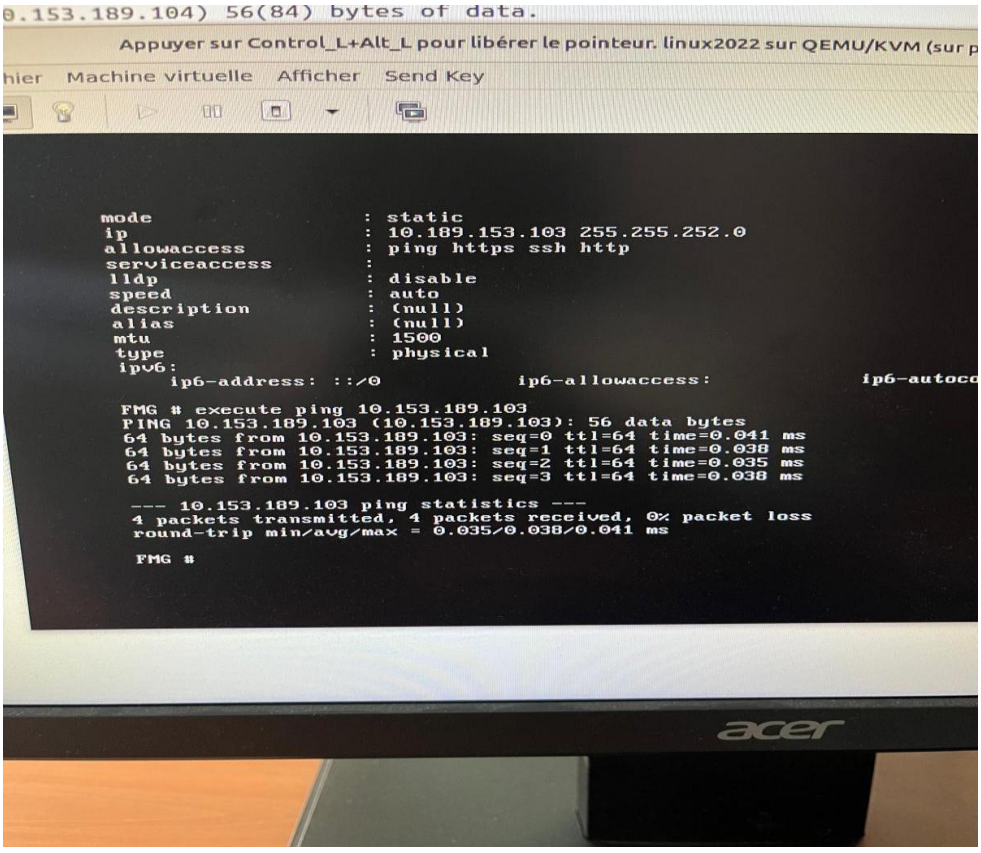
J’ai pu déployer la VM , mais je n’ai pas terminé la configuration de cette VM à cause quelques soucis (Commandes qui ne fonctionnent pas , problèmes d’Internet ) .

Pour avoir accès au FortiManager en cli , je me suis identifié par le Login : admin sans mettre de mot de passe .

## A. Configuration Réseau de base (CLI FortiManager)

Une fois la console ouverte, voici les commandes utilisées pour donner une IP à la patte d'administration .

Avant toutes ces configurations , j’en ai fait plusieurs qui n’ont pas fonctionné .



**Bloc de commandes :**

- ## Configuration de l'interface VLAN

Pour segmenter le trafic, j'ai créé une interface virtuelle liée au port physique.

```
config system interface
  edit "vlan160"
    set vlanid 160
    set interface "port1"
    set ip 10.153.189.103  255.255.255.0
    set allowaccess ping https ssh http webservice
  next
end
```

- ## Configuration de la Route Statique (Passerelle)

Afin de permettre la communication avec l'extérieur du sous-réseau, j'ai défini la passerelle par défaut.

**Note technique :** Sur FortiManager, la syntaxe pour la route nécessite d'éditer un index (ex: edit 1).

```
config system route
  edit 1
    set device "vlan160"
    set gateway 10.153.189.249
```

***next***

***end***

**DNS :** Si le ping 10.153.189.249 fonctionne mais pas **ping google.com**, il manque la configuration DNS :

***config system dns***

***set primary 10.154.59.104***

***set secondary 10.156.32.33***

***end***

## Incident technique et Résolution

Problème rencontré : Après avoir configuré l'adresse IP (10.153.189.103) et autorisé l'accès HTTPS, il était impossible d'accéder à l'interface graphique via un navigateur Web, bien que la VM réponde au ping.

**Diagnostic :** L'Appliance FortiManager nécessite des ressources minimales pour initialiser ses services de gestion. En vérifiant l'état du système, il est apparu que les ressources allouées initialement étaient insuffisantes pour charger l'interface Web et la base de données de gestion.

Solution apportée :

- Arrêt de la VM sur l'hyperviseur via virt-manager.
- Augmentation des ressources : Ajout de 200 Go de stockage / ressources CPU (vérifie bien s'il s'agissait de 200 Go de disque ou d'un boost CPU, car 200 Go de CPU n'existe pas, c'est probablement du Disque dur pour les logs et la base de données).
- Redémarrage de la VM.

**Résultat** : Après l'extension des ressources, le service Web s'est initialisé correctement et l'accès à l'interface graphique a été rendu possible.

## Configuration du Proxy

Pour permettre au FortiManager de communiquer avec l'extérieur (notamment pour l'activation des licences et les mises à jour FortiGuard), j'ai dû configurer les paramètres du proxy de l'infrastructure.

***config system proxy***

***set status enable***

***set server 10.154.61.6***

***set port 3128***

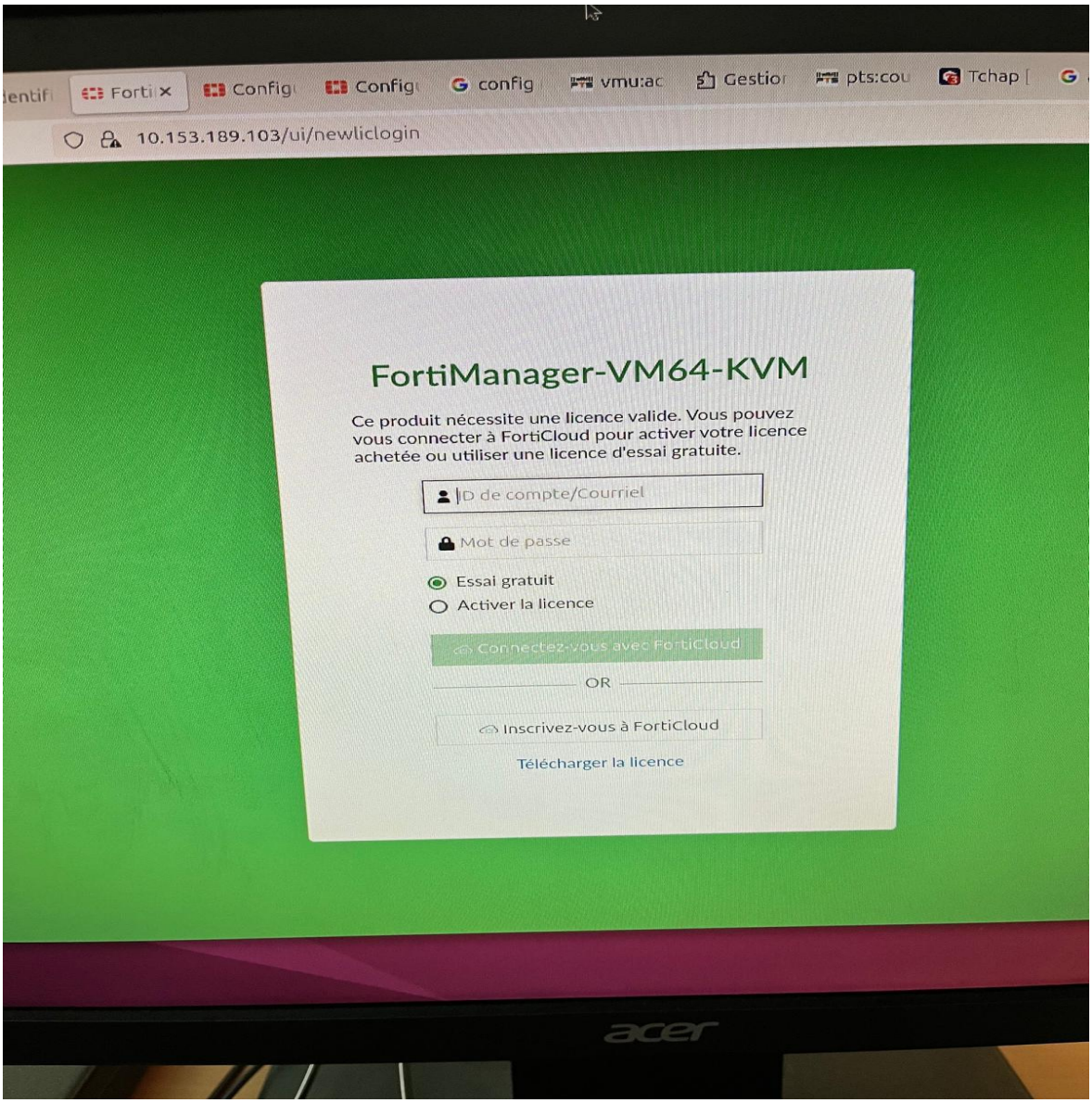
***end***

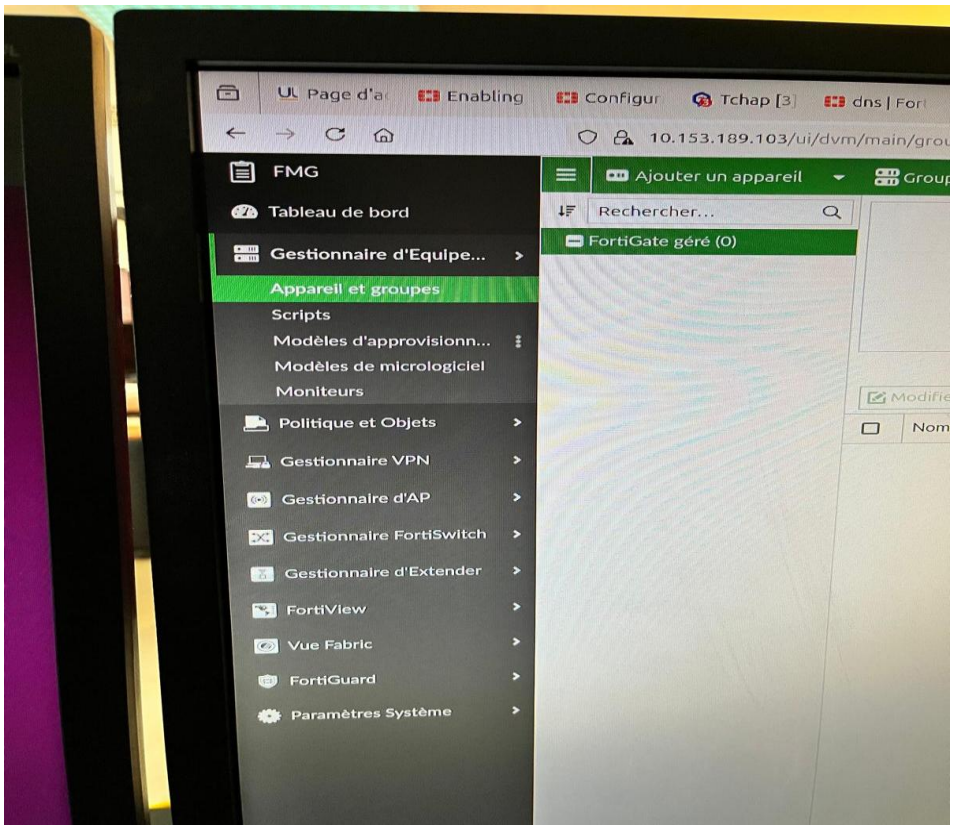
## Incident technique et Résolution

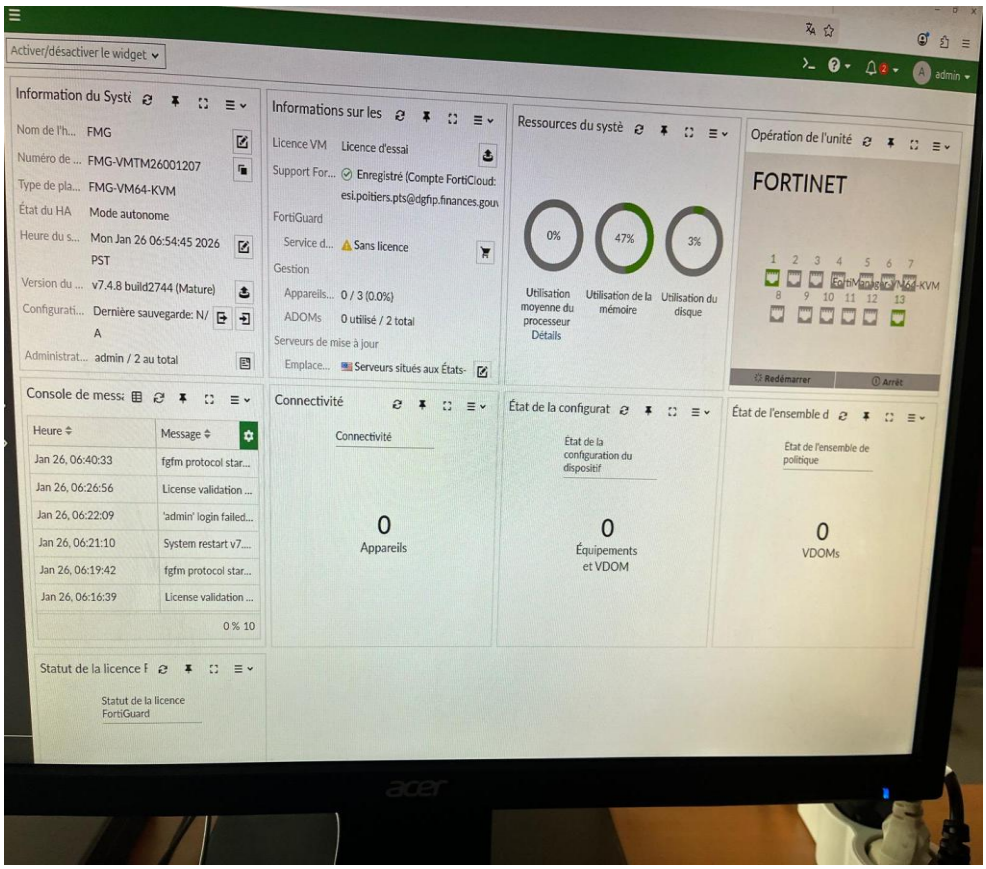
Après configuration du Proxy, j'ai un problème avec le **My user agent,** qui était différent de celui du navigateur, voilà pourquoi je n'avais toujours pas accès à mon GUI .

J'ai pu le modifier grâce à une commande.

***set User - Agent "Mozilla/5.0 (X11; Linux x86_64; rv:140.0)***


10.153.189.103/ui/newliclogin
FortiManager-VM64-KVM
Ce produit nécessite une licence valide. Vous pouvez vous connecter à FortiCloud pour activer votre licence achetée ou utiliser une licence d'essai gratuite.
ID de compte/Courriel
Mot de passe
Essai gratuit
Activer la licence
Connectez-vous avec FortiCloud
OR
Inscrivez-vous à FortiCloud
Télécharger la licence
acer


Page d'a
Enabling
Configur
Tchap [3]
dns | For
10.153.189.103/ui/dvm/main/grou
FMG
Tableau de bord
Gestionnaire d'Equipe...
Appareil et groupes
Scripts
Modèles d'approvisionn...
Modèles de micrologiciel
Moniteurs
Politique et Objets
Gestionnaire VPN
Gestionnaire d'AP
Gestionnaire FortiSwitch
Gestionnaire d'Extender
FortiView
Vue Fabric
FortiGuard
Paramètres Système
Ajouter un appareil
Group
Rechercher...
FortiGate géré (0)
Modifie
Nom


Activer/désactiver le widget
admin
Information du Systè
Nom de l'h... FMG
Numéro de ... FMG-VMTM26001207
Type de pla... FMG-VM64-KVM
État du HA Mode autonome
Heure du s... Mon Jan 26 06:54:45 2026 PST
Version du ... v7.4.8 build2744 (Mature)
Configurati... Dernière sauvegarde: N/A
Administrat... admin / 2 au total
Informations sur les
Licence VM Licence d'essai
Support For... Enregistré (Compte FortiCloud: esi.poitiers.pts@dgfip.finances.gouv
FortiGuard
Service d... Sans licence
Gestion
Appareils... 0 / 3 (0.0%)
ADOMs 0 utilisé / 2 total
Serveurs de mise à jour
Emplace... Serveurs situés aux États-
Ressources du systè
0%
47%
3%
Utilisation moyenne du processeur
Utilisation de la mémoire
Utilisation du disque
Détails
Opération de l'unité
FORTINET
Redémarrer
Arrêt
Console de messa
Heure
Message
Jan 26, 06:40:33 fgfm protocol star...
Jan 26, 06:26:56 License validation ...
Jan 26, 06:22:09 'admin' login failed...
Jan 26, 06:21:10 System restart v7....
Jan 26, 06:19:42 fgfm protocol star...
Jan 26, 06:16:39 License validation ...
0 % 10
Connectivité
Connectivité
0
Appareils
État de la configurat
État de la configuration du dispositif
0
Équipements et VDOM
État de l'ensemble d
État de l'ensemble de politique
0
VDOMs
Statut de la licence F
Statut de la licence FortiGuard
acer

# Activité réalisée : Mise à jour de firmwares sur des serveurs physiques

Au cours de mon stage, j'ai participé à une **demande d'intervention** concernant la **préparation de nouveaux serveurs HPE ProLiant destinés à accueillir des hyperviseurs**.
L'objectif de cette intervention était de **mettre à jour les firmwares** des serveurs afin de garantir la compatibilité, la sécurité et la stabilité du matériel avant sa mise en production.

## Définition : qu'est-ce qu'un firmware ?

Un **firmware** est un **logiciel intégré directement dans un composant matériel** (carte mère, contrôleur, disque, carte réseau, etc.).
Il permet au matériel de fonctionner correctement et d'interagir avec le système d'exploitation.
La mise à jour des firmwares permet :

- de corriger des bugs,
- d'améliorer la stabilité,
- d'ajouter des correctifs de sécurité,
- d'assurer la compatibilité avec de nouveaux systèmes ou logiciels.

# Description du travail réalisé

Pour réaliser cette intervention, nous avons utilisé l'outil **iLO (Integrated Lights-Out)**, qui permet l'**administration à distance des serveurs physiques**, même lorsqu'ils sont éteints ou en cours de démarrage.

Les principales étapes observées et réalisées ont été les suivantes :

1. **Connexion à l'interface iLO**

Je me suis connectée à l'interface web d'administration du serveur afin d'accéder aux informations matérielles et aux outils de gestion.

2. **Ouverture de la console distante**

La console distante permet de visualiser l'écran du serveur à distance, comme si l'on était physiquement devant la machine.

3. Redémarrage du serveur

Le serveur a été redémarré afin d'accéder aux menus de démarrage et aux outils de maintenance.

4. **Accès au Boot Menu et aux outils système**

Depuis le menu de démarrage, il est possible d'accéder aux utilitaires permettant la maintenance, la configuration et la mise à jour des composants

5. **Vérifications et préparation du système**
   Avant la mise à jour, certaines vérifications ont été effectuées :

- identification du modèle du serveur,
- vérification des versions de firmware,
- contrôle de l'état matériel

# V. BILAN DU STAGE

## 5.1. Compétences techniques acquises (SISR)

Au cours de mon stage au pôle PTS de la DGFIP, j'ai pu développer plusieurs compétences techniques liées à l'administration et à l'exploitation d'infrastructures informatiques.

1. Administration systèmes et virtualisation
    - Observation et participation au **déploiement de machines virtuelles**.
    - Compréhension du fonctionnement d'une **infrastructure virtualisée** et du rôle des hyperviseurs.

- Utilisation d'outils de déploiement et de gestion d'infrastructures virtualisé
- Compréhension des étapes nécessaires avant une mise en production.

2. Sécurité des réseaux et administration des pare-feux
    - Traduction de **demandes de flux en règles de pare-feu**
    - Découverte de l'administration centralisée avec **FortiManager**
    - Compréhension du rôle d'un **bastion (Wallix)** dans la sécurisation des accès.

3. Maintenance et administration de serveurs
    - Mise à jour de **firmwares** sur des serveurs physiques HPE.
    - Utilisation d'un outil d'administration à distance (**iLO**).
    - Vérification de l'état matériel et des versions système.

**6. Méthodes de travail en environnement professionnel**

- Travail à partir de **demandes d'intervention (DI)** et de procédures.
- Compréhension des étapes de **mise en production (MEP).**

## 5.2. Compétences transversales et savoir-être.

Au cours de mon stage à la DGFIP de Poitiers, j'ai pu développer plusieurs compétences transversales et qualités professionnelles.

**1. Capacité d'observation et d'apprentissage**

Étant intégrée dans une équipe d'exploitants systèmes, j'ai dû observer des procédures techniques, poser des questions et prendre des notes afin de comprendre le fonctionnement de l'infrastructure et des outils utiles.

**2. Adaptation à un environnement professionnel**

Ce stage m'a permis de découvrir le fonctionnement d'une administration et de m'adapter :

- aux outils professionnels,
- aux vocabulaires techniques propres à la DGFIP
- au rythme et aux exigences d'un service informatique.

# CONCLUSION

Ce stage effectué au sein de la Direction Générale des Finances Publiques, sur le site de l'ESI de Poitiers, a constitué une expérience particulièrement enrichissante tant sur le plan technique que professionnel.

Il m'a permis de découvrir le fonctionnement réel d'une infrastructure informatique d'envergure nationale, organisée autour d'exigences fortes en matière de sécurité, de disponibilité et de continuité de service. J'ai pu comprendre concrètement comment sont structurées les différentes zones d'un système d'information sécurisé, comment sont gérés les accès administrateurs via un bastion, et comment s'organisent les déploiements et mises en production dans un environnement sensible.

Les missions auxquelles j'ai participé, telles que le déploiement et la migration de machines virtuelles, la configuration d'un FortiManager, l'ouverture de flux via gestion centralisée ou encore la mise à jour de firmwares sur serveurs physiques, m'ont permis de mettre en application les notions étudiées en BTS SIO SISR. Ce stage m'a également permis de développer ma capacité d'analyse face à des incidents techniques, notamment lors des problèmes liés aux ressources systèmes ou à l'accès à l'interface graphique.

Au-delà des compétences techniques, cette immersion m'a appris à travailler dans un cadre professionnel structuré, avec des procédures précises, des demandes d'intervention formalisées et des

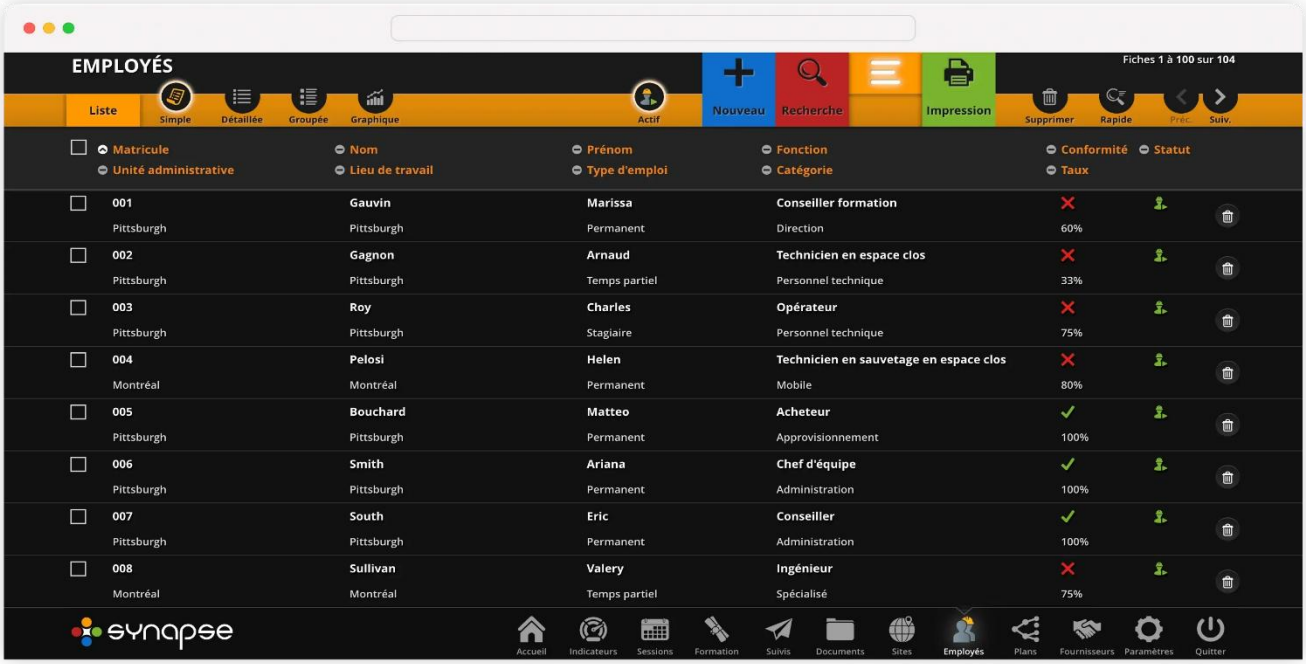
contraintes de sécurité importantes. J'ai pris conscience que le métier d'administrateur systèmes et réseaux demande rigueur, méthode, sens des responsabilités et capacité d'adaptation.

Cette expérience a confirmé mon intérêt pour le domaine de l'infrastructure et de la cybersécurité. Elle représente une étape importante dans la construction de mon projet professionnel et dans mon évolution vers un poste à responsabilités dans l'administration des systèmes et des réseaux.

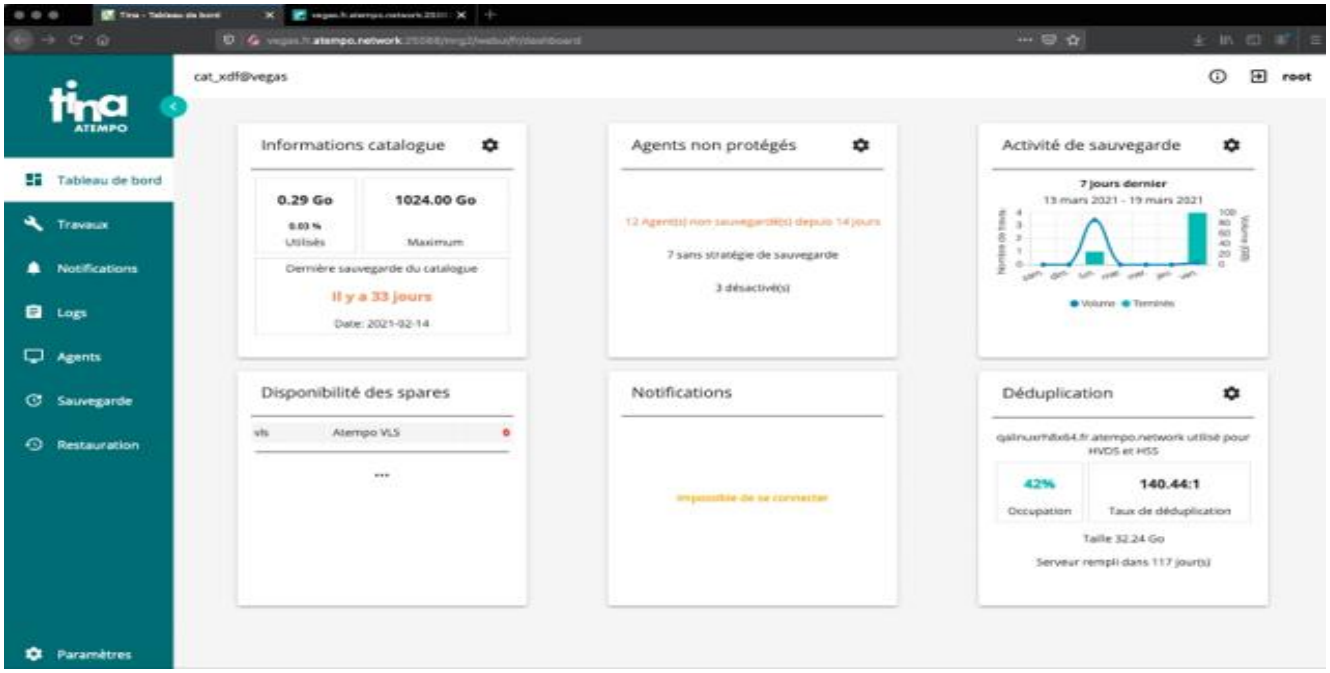
En conclusion, ce stage a pleinement répondu aux objectifs fixés en début de formation et constitue une véritable transition entre l'apprentissage théorique et la réalité du terrain.

## IMAGES DES CERTAINS OUTILS :

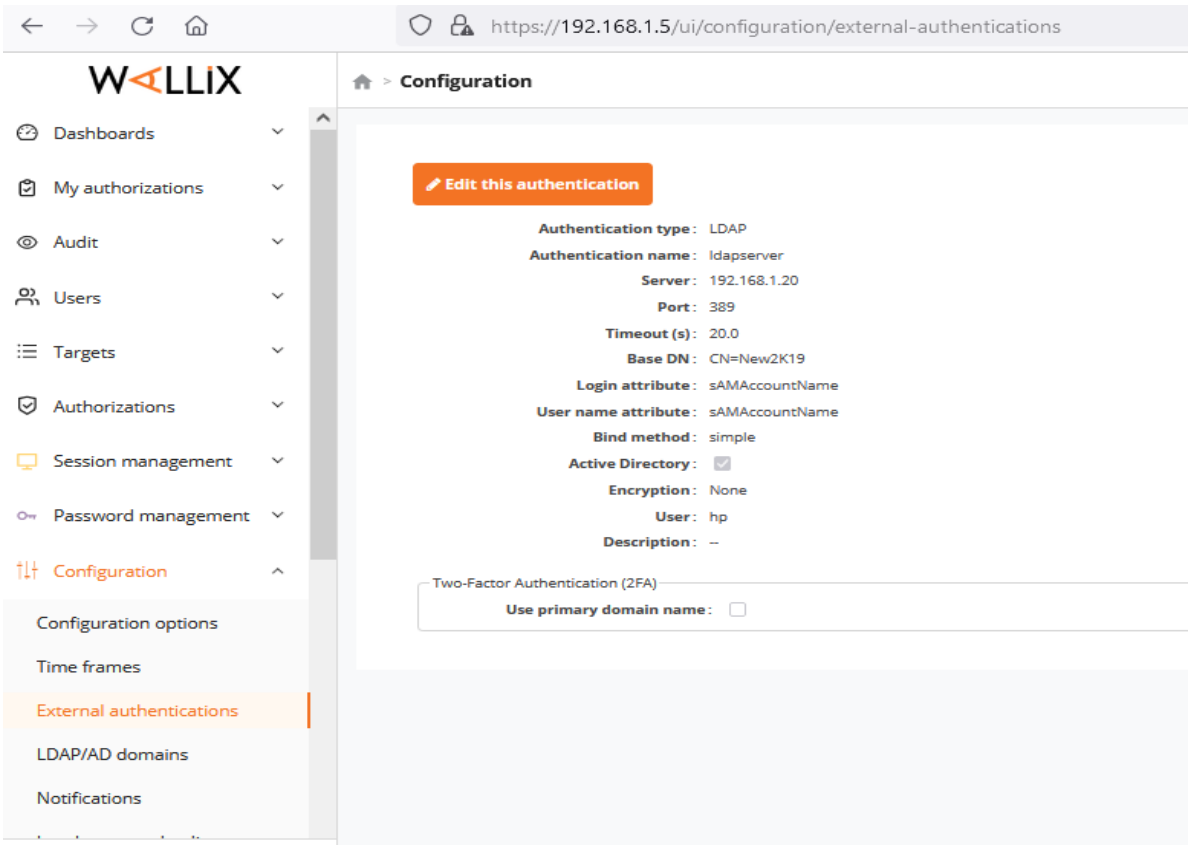
**SYNAPSE** :



## TINA :


cat_xdf@vegas
root
Tableau de bord
Travaux
Notifications
Logs
Agents
Sauvegarde
Restauration
Paramètres
Informations catalogue
0.29 Go
1024.00 Go
Maximum
Dernière sauvegarde du catalogue
Il y a 33 jours
Agents non protégés
7 sans stratégie de sauvegarde
3 désactivé(s)
Activité de sauvegarde
7 jours dernier
Disponibilité des spares
Atempo VLS
Notifications
Déduplication
42%
Occupation
140.44:1
Taux de déduplication

## WALLIX :


https://192.168.1.5/ui/configuration/external-authentications
WALLIX
Configuration
Dashboards
My authorizations
Audit
Users
Targets
Authorizations
Session management
Password management
Configuration
Configuration options
Time frames
External authentications
LDAP/AD domains
Notifications
Edit this authentication
Authentication type: LDAP
Authentication name: ldapserver
Server: 192.168.1.20
Port: 389
Timeout (s): 20.0
Base DN: CN=New2K19
Login attribute: sAMAccountName
User name attribute: sAMAccountName
Bind method: simple
Active Directory:
Encryption: None
User: hp
Description: --
Two-Factor Authentication (2FA)
Use primary domain name:

# Remerciements

Je tiens à adresser mes sincères remerciements à **Monsieur Martin Rosso**, mon tuteur de stage, pour son accompagnement, sa disponibilité et les explications qu'il m'a apportées tout au long de cette période.
Je remercie également **Monsieur Christophe Martins**, ainsi que l'ensemble des membres du **PTS**, pour le temps qu'ils ont consacré à m'expliquer des notions techniques importantes et à me faire découvrir leur travail au quotidien.

Je souhaite aussi remercier **Madame Padovani**, qui m'a permis de réaliser ce stage au sein de la **DGFIP de Poitiers**.

Ce stage m'a permis d'acquérir des **compétences utiles dans le cadre de ma formation**, mais également de mieux comprendre le fonctionnement d'un environnement de travail professionnel. Il a renforcé mon intérêt pour le domaine de l'informatique et confirmé mon choix d'orientation.

Au-delà des compétences techniques, ce stage m'a également permis de développer des compétences transversales, telles que le travail en équipe, la communication, la participation à des réunions et la rédaction de comptes rendus. J'ai ainsi compris que l'informatique ne se limite pas à l'exécution de commandes ou au développement, mais qu'elle repose aussi sur l'échange, la collaboration et l'organisation.

Enfin, je remercie l'ensemble de **L'ESI de Poitiers** pour la qualité de l'accueil et de l'encadrement.