

La présentation de l'entreprise et du service

1) Présentation de l'entreprise

Durant les deux dernières années, j'ai été en alternance à La Plateforme_ Marseille. La Plateforme_ est une école du numérique située à Marseille, qui propose des formations en informatique, avec quatre spécialités: cybersécurité, intelligence artificielle et développement web et logiciel.

La Plateforme_ a été fondée avec la volonté de répondre aux besoins croissants du marché du numérique dans le sud de la France.

N'importe qui peut s'y inscrire, l'école s'adresse à des publics variés que ce soit étudiants, personnes en reconversion ou professionnels en quête de montée en compétences.

L'école adopte une pédagogie innovante basée sur la pratique, les projets concrets et le travail en équipe, dans un environnement technique réel. Il n'y a pas de cours magistraux comme on en a l'habitude.

2) Présentation de l'entreprise et du service :

Durant mon alternance à La Plateforme_, j'ai intégré le Pôle Systèmes, Réseaux et Support IT en tant qu'administrateur systèmes, réseaux et support. J'ai été amené à intervenir sur de nombreux volets techniques, aussi bien en interne que sur les différents sites de l'école.

J'ai notamment participé à :

- Administration d'équipements réseau tels que des caméras de surveillance, des bornes Wi-Fi, et un serveur dédié sur site
- Travaux d'infrastructure physique : réflexion sur l'emplacement optimal des caméras de surveillance et des bornes Wi-Fi, installation et configuration sur le terrain, réalisation de câblage réseau, montage de baies informatiques, et interventions dans les différents bâtiments de La Plateforme_
- Le support utilisateur sur les postes étudiants et administratifs
- La gestion complète de la plateforme MDM Jamf School pour l'administration des iMacs utilisés par l'un des services de La Plateforme_.
- Le déploiement et la configuration de solutions open source comme ALCASAR pour le contrôle des accès réseau
- La rédaction de documentation technique et le maintien des procédures
- L'automatisation de certaines tâches via scripts (Bash, cron...)

Résumé du Dossier Professionnel

1. Cisco Packet Tracer : Les topologies des infrastructures réseaux

Dans un objectif de renforcement des compétences en architecture réseau, j'ai utilisé Cisco Packet Tracer pour concevoir et simuler différentes topologies (étoile, bus, anneau, maillée, arbre) en configurant PC, switches et routeurs virtuels. Ce projet m'a permis de mieux comprendre le fonctionnement et les avantages/inconvénients de chaque structure réseau.

2. Déploiement de Zabbix pour le monitoring centralisé d'une infrastructure virtuelle

Afin de répondre à un besoin d'évolution vers une gestion proactive, j'ai installé Zabbix sur une VM Debian 12 pour superviser en temps réel les ressources (CPU, RAM, disque, réseau) d'un système cible. J'ai configuré l'agent Zabbix, les templates de monitoring, ainsi que l'envoi d'alertes par email via un type de média personnalisé.

3. Cybersécurité : Découverte des Vulnérabilités avec Nessus, Attaques avec Metasploit

Dans un environnement contrôlé, j'ai utilisé Nessus Essentials sur Kali Linux pour scanner la VM vulnérable Metasploitable2. Les vulnérabilités critiques identifiées (comme la faille UnrealIRCd) ont été exploitées avec Metasploit, démontrant ainsi la chaîne complète de détection, analyse et exploitation de failles de sécurité.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

Résumé du Dossier Projet :

Le sommaire du dossier projet va aborder les points suivants :

- 1• La liste des compétences mises en œuvre dans le cadre du projet
- 2• Le cahier des charges ou l'expression des besoins du projet
- 3• La gestion de projet (planning et suivi, environnement humain, objectifs de qualité)
- 4• Les solutions retenues (critères de décision, évaluation, argumentation)
- 5• Les spécifications techniques du projet, élaborées par le candidat, y compris pour la sécurité
- 6• La présentation de la mise en œuvre

1. Liste des compétences mobilisées (lors du projet)

- Virtualisation (KVM, QEMU, Virt-Manager)
- Installation et configuration de systèmes Linux (Debian, Mageia)
- Mise en œuvre d'un portail captif (ALCASAR)
- Intégration LDAP Google Workspace
- Sécurisation réseau (iptables, règles SSH)
- Supervision (Zabbix, ELK)
- Automatisation (cron, scripts bash)
- Architecture réseau
- Gestion de projet technique

2. Expression des besoins (Cahier des charges)

- Créer une VM sécurisée pour ALCASAR, indépendante du serveur en production.
- Centraliser les accès avec un annuaire LDAP Google Workspace.
- Renforcer la sécurité : cloisonnement, filtrage SSH, alertes mail.
- Implémenter un système de supervision et de sauvegarde (snapshots, monitoring).
- Faciliter la maintenance avec une solution virtualisée.

3. Gestion de projet

- Planning : déroulement par étapes claires (préparation matériel, RAID, OS, VM, ALCASAR, LDAP, supervision...).
- Suivi : validation de chaque étape via tests et captures d'écran.
- Environnement humain : réalisé en autonomie avec échanges sur forums et support technique interne.

4. Solutions retenues et critères de choix

- KVM au lieu de VMware : performances supérieures, open-source, support du PCI passthrough.
- ALCASAR en VM Mageia : facilité de snapshot, isolation, déploiement simplifié.
- Stunnel + LDAP Google Workspace : méthode la plus stable, évite les modifications internes d'ALCASAR.
- Zabbix pour supervision temps réel / ELK pour analyse post-événement.

5. Spécifications techniques (sécurité incluse)

Pour le matériel :

- Serveur DELL physique avec 128 Go de RAM
- Disques configurés en RAID 1 via carte PERC H710

Les systèmes d'exploitations utilisés :

- Debian 11 (sans interface graphique) sur l'hôte
- Mageia 9 sur la VM ALCASAR

Pour la virtualisation :

- Hyperviseur : KVM avec QEMU + libvirt + virt-manager
- Utilisation du PCI Passthrough pour l'accès direct aux cartes réseau

Pour le réseau du serveur :

- IP WAN publique : 37.26.187.4/29

Pour le réseau de la VM :

Configuration manuelle des interfaces

- IP WAN publique : 37.26.187.5/29
- IP LAN : 10.10.0.1/16

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

Partitionnement VM ALCASAR :

/ : 40 Go
/tmp : 15 Go
/var : le reste du disque
/home : 15 Go
swap : 15 Go

Pour la sécurité :

- Règle iptables SSH : seule une IP autorisée peut se connecter
- Alerte mail automatique à chaque connexion SSH
- Authentification LDAP via Google Workspace avec certificat (stunnel)
- Cloisonnement VM / hôte pour limiter les risques d'intrusion

Pour la Supervision & Sauvegarde :

- Snapshots automatiques via cron (virsh snapshot)
- Monitoring : Zabbix (temps réel) + ELK (analyse de logs)

6. Présentation de la mise en œuvre

La mise en œuvre du projet s'est déroulée en plusieurs phases, de la préparation du serveur jusqu'à la supervision avancée de la solution déployée. J'ai veillé à suivre une démarche rigoureuse, avec une documentation systématique à chaque étape.

-Préparation du serveur physique

J'ai commencé par assembler le serveur DELL destiné à héberger l'ensemble de l'infrastructure. Celui-ci est équipé de 128 Go de RAM et de plusieurs disques connectés à une carte RAID PERC H710, que j'ai configurée en RAID 1 depuis le BIOS. Cette configuration garantit une meilleure tolérance aux pannes, en stockant les données en miroir sur deux disques.

Installation du système hôte

Le système d'exploitation Debian 11 a été installé sans interface graphique, afin d'optimiser les performances et la sécurité du serveur. Ce choix technique limite la surface d'attaque en réduisant les services actifs et conserve un système léger adapté à un environnement de production.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

Mise en place de la virtualisation avec KVM

Pour garantir l'isolement des environnements, j'ai déployé une infrastructure de virtualisation basée sur KVM + QEMU + Libvirt, accompagnée de Virt-Manager pour la gestion graphique des machines virtuelles.

Ce choix permet :

de bénéficier d'une performance proche du matériel réel (grâce à l'intégration directe dans le noyau), de créer facilement des snapshots réguliers, et d'isoler la VM ALCASAR de l'hôte Debian.

Création et configuration de la VM ALCASAR

J'ai ensuite créé une machine virtuelle dédiée sous Mageia 9, système recommandé pour ALCASAR. La VM a été configurée avec 32 Go de RAM et 16 cœurs CPU, afin de supporter la charge réseau générée par plusieurs centaines d'utilisateurs.

Deux interfaces réseau physiques lui ont été directement attribuées via la technologie PCI Passthrough :

une pour l'accès à Internet (WAN),
une pour le réseau local des utilisateurs (LAN).

Cette méthode permet à ALCASAR de bénéficier d'un accès natif aux cartes réseau, améliorant ainsi les performances et la fiabilité.

Installation d'ALCASAR

L'image ISO de Mageia 9 fournie par le projet ALCASAR a été utilisée. Le script d'installation alcasar.sh a été exécuté, ce qui a automatiquement :

- configurer le pare-feu,
- mis en place le serveur DHCP/DNS,
- installer le portail captif.

Une attention particulière a été portée au partitionnement du disque, en respectant les recommandations d'ALCASAR (/var, /tmp, /swap...).

Intégration LDAP Google Workspace

L'un des objectifs majeurs du projet était de remplacer les comptes locaux par une authentification centralisée via l'annuaire LDAP de Google Workspace.

Face aux limites natives d'ALCASAR avec les annuaires externes, j'ai testé deux méthodes :

- La modification directe du script alcasar-ldap.sh,

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

-L'usage d'un proxy sécurisé avec Stunnel.

La méthode retenue fut la seconde, car elle ne nécessite aucune modification interne d'ALCASAR. Elle redirige les requêtes LDAP locales vers le serveur LDAPS de Google, avec authentification par certificat et clé privée. Cette approche est plus stable, plus maintenable et compatible avec l'interface web d'ALCASAR.

Sécurisation des accès SSH

Pour limiter l'exposition du serveur, j'ai mis en place une règle iptables qui bloque tous les accès SSH sauf depuis une IP précise. De plus, un script de notification mail a été installé : à chaque connexion SSH, une alerte est envoyée à mon adresse e-mail via msmtpt, permettant une surveillance en temps réel.

Sauvegardes avec snapshots

Afin de sécuriser les modifications majeures, des snapshots automatiques hebdomadaires de la VM ALCASAR ont été configurés via cron. Ce mécanisme garantit un retour rapide à un état stable en cas d'erreur ou de mise à jour problématique.

Supervision avec Zabbix et ELK

Deux outils ont été imaginé pour le monitoring :

- Zabbix pour la supervision en temps réel des ressources système (CPU, RAM, disques, trafic...),
- ELK Stack (Elasticsearch, Logstash, Kibana) pour la centralisation et l'analyse des logs (notamment connexions SSH, erreurs système, alertes).

Cela permet une double visibilité : instantanée avec Zabbix, et analytique avec ELK, renforçant la sécurité et la capacité de diagnostic.