





Script de l'oral du Jalon

4

WIZARDS & DICE

 Créateur : Arthur YANG – Responsable Documentation & Administratif
 Date de Création : 29/01/2025




 Modificateur : Arthur YANG – Responsable Documentation & Administratif
 Date de modification : 08/02/2025
 Version : 1.1



Table des matières :

I. Introduction.....	2
II. Présentation globale de l'infrastructure.....	2
Structure des sites.....	2
Réseaux existants.....	3
Interconnexion des sites via VPN.....	3
Connexion aux sites via VPN.....	3
III. Sécurisation et supervision (R5.Cyber.11).....	5
Segmentation et protection du réseau.....	5
Authentification et gestion des accès.....	5
Supervision et surveillance en temps réel.....	6
Stratégie de sauvegarde.....	6
Redondance et continuité de service.....	7
Recommandations de sécurité.....	8
IV. Point techniques et d'avancement.....	10
Avancement technique et état du projet.....	10
Choix des solutions et justification des technologies.....	11
V. Planning et organisation.....	15
Prochaines étapes.....	15
Organisation et planification.....	15
VI. Conclusion.....	17

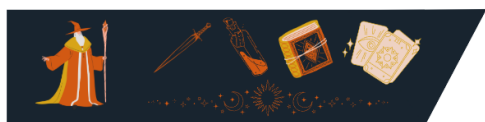
Le script ci-dessous sert de **Guideline** plutôt que de texte à réciter mot pour mot. Il contient des éléments rédigés, mais aussi des points clés que chacun pourra développer à sa manière s'il en a envie.

Chacun est libre de **ne pas suivre le texte à la lettre**, tant que l'idée principale et les informations essentielles sont respectées.

L'ordre du script/texte suit le plan de la table des matières et dans l'ordre d'apparition des noms.

Pour une facilitation d'apprentissage de l'ordre pour parler, voici le roulement :

Arthur :
Hugo :
Axel :
Loïs :





I. Introduction

- Mise en introduction

Arthur

Bonjour monsieur ! Aujourd'hui, nous allons vous présenter l'avancement technique du projet Wizards & Dice, notre plateforme e-commerce dédiée aux jeux de rôle. Pour rappel, notre objectif est simple, c'est de créer un site qui soit performant, sécurisé et évolutif, capable de répondre aux besoins des clients, qu'ils soient débutants ou expérimentés."

Dans cette présentation, on va vous expliquer où nous en sommes d'un point de vue technique, les choix qu'on a faits pour construire notre infrastructure, comment on s'organise pour la suite et surtout comment gère-t-on la sécurité et la supervision du projet en lien avec la ressource R5.Cyber.11.

On va suivre un plan structuré : d'abord la présentation globale de l'infrastructure, ensuite ce qui concerne la sécurisation et la supervision, puis le point technique et d'avancement du projet, et enfin l'organisation et le planning pour la suite.

II. Présentation globale de l'infrastructure

Hugo

Avant d'entrer dans le détail de ce qui est fait et ce qu'il reste à faire, on va d'abord poser le cadre général de notre infrastructure. Notre infrastructure repose sur une architecture distribuée entre deux sites d'hébergement, situés chez Hugo (moi) et Loïs.

Structure des sites

Hugo

L'infrastructure est répartie sur deux sites identiques où chacun est équipé de son propre accès Internet et de son pare-feu dédié, hébergeant aussi chacun l'ensemble des services nécessaires au bon fonctionnement du projet.

Les deux sites disposent d'un réseau opérateur d'adressage distinct, mais partagent une configuration identique et les mêmes services pour assurer une continuité d'activité et un basculement automatique si nécessaire. De plus, dans ces réseaux fournis par l'opérateur, les deux sites fonctionnent sur des réseaux nommés "LAN Stormshield" distincts, bien qu'ils partagent la même configuration et les mêmes services.





Chaque site est équipé d'un hyperviseur Proxmox, qui permet l'hébergement et la gestion des machines virtuelles avec différents services. Un site surveille ses propres VMs ainsi que la connectivité au sein du tunnel IPSec reliant les deux infrastructures, garantissant ainsi une communication fluide et sécurisée entre les deux emplacements.

Chaque hyperviseur héberge plusieurs services critiques, notamment les bases de données, le serveur web, les solutions de monitoring et les outils de gestion des accès.

Réseaux existants

Axel

Chaque site fonctionne avec son propre plan d'adressage IP et des VLANs segmentés en fonction des usages : serveurs, utilisateurs, bases de données et zones exposées à Internet comme la DMZ. Cette segmentation assure une isolation claire des services, optimise les performances et renforce la sécurisation du trafic réseau."

Interconnexion des sites via VPN

Axel

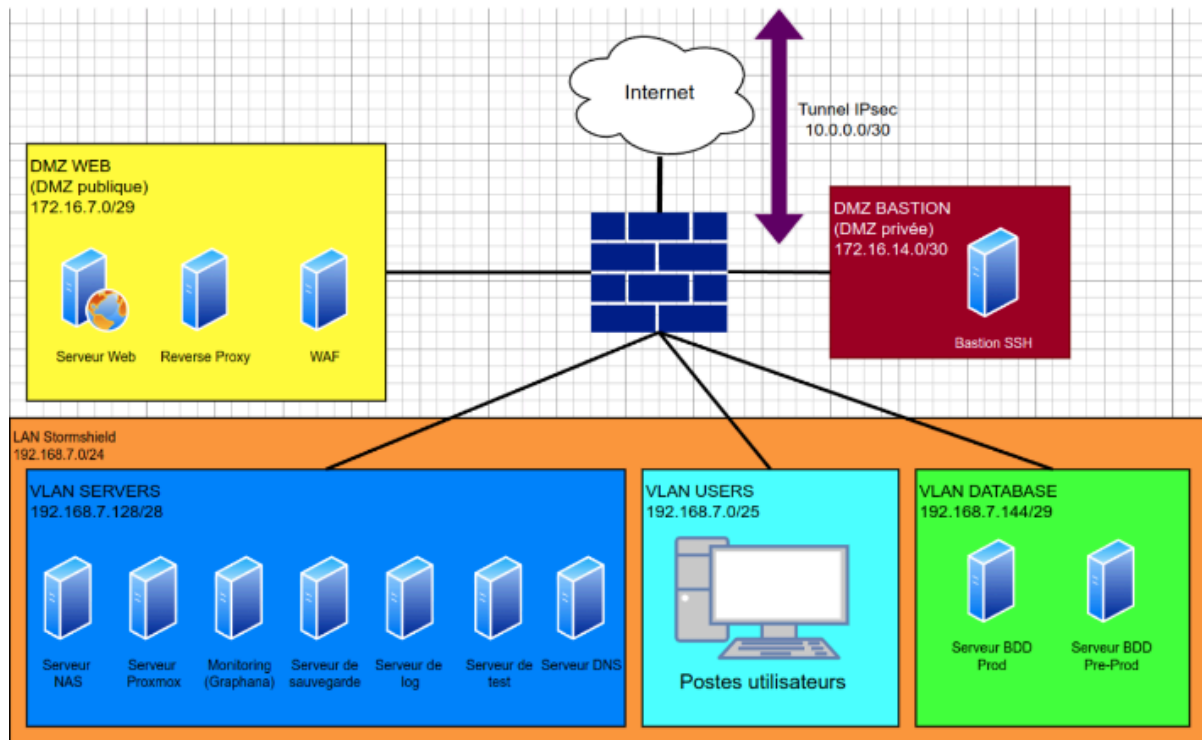
Pour assurer une communication sécurisée entre les deux sites, la mise en place un VPN IPSec permet un échange fluide des données tout en garantissant un niveau de sécurité. Ce tunnel VPN est essentiel pour la gestion centralisée et l'accès aux ressources distantes sans compromettre la sécurité de l'infrastructure.

Connexion aux sites via VPN

Axel

De plus, en complément du VPN IPSec, la mise en place d'un VPN SSL pourra permettre un accès distant sécurisé aux administrateurs et utilisateurs ayant besoin de se connecter aux ressources internes sans être physiquement présents sur l'un des sites.





(Utiliser le schéma de l'infrastructure pour expliquer dans le support)





III. Sécurisation et supervision (R5.Cyber.11)

Segmentation et protection du réseau

Loïs

Passons maintenant à la sécurisation et la supervision du projet. Ces éléments sont essentiels pour garantir la protection des données et la disponibilité des services.

Loïs

Notre architecture repose sur une segmentation rigoureuse du réseau, permettant d'isoler les différents services et de limiter la propagation des menaces en cas d'attaque. Cette segmentation est assurée par des **VLANs distincts**, chacun ayant un rôle précis dans l'infrastructure. La **DMZ Web (172.16.7.0/29)** contient les services exposés à Internet, comme le serveur web, le reverse proxy et le WAF, et représente la zone la plus surveillée. La **DMZ Bastion (172.16.14.0/30)** est dédiée au Bastion SSH, un point d'accès unique pour l'administration, limitant ainsi les risques d'intrusion. Le **VLAN SERVERS (192.168.7.128/28)** héberge les services internes tels que le NAS, les hyperviseurs Proxmox, le monitoring, la sauvegarde et les logs. Le **VLAN USERS (192.168.7.0/25)** est réservé aux postes utilisateurs, restreignant leur accès aux seules ressources nécessaires. Enfin, le **VLAN DATABASE (192.168.7.144/29)** contient les bases de données en production et pré-production, garantissant une isolation renforcée contre tout accès non autorisé. Tous ces segments sont filtrés et sécurisés via un pare-feu Stormshield, qui applique des règles strictes de contrôle du trafic, limitant les communications aux seuls flux explicitement autorisés et réduisant ainsi les risques d'attaques latérales.

Authentification et gestion des accès

Arthur

Pour éviter tout accès non autorisé, nous avons mis en place des politiques de gestion des accès robustes basées sur plusieurs principes fondamentaux.

Bastion SSH obligatoire

Tous les accès aux machines serveurs passent par un bastion SSH unique, évitant toute exposition directe sur Internet. L'authentification ne se fait qu'avec des clés SSH, interdisant totalement l'usage de mots de passe pour réduire le risque de compromission.

Gestion centralisée des accès

L'ensemble des utilisateurs et des permissions est géré via un annuaire LDAP, permettant une administration simplifiée et une meilleure traçabilité.





Journaux d'accès et audits

Chaque connexion aux systèmes critiques est enregistrée et analysée pour détecter toute activité anormale.

Toutes ces mesures garantissent que seuls les utilisateurs autorisés peuvent accéder aux services critiques, tout en offrant une visibilité complète sur les accès.

Supervision et surveillance en temps réel

Arthur

Une infrastructure sécurisée ne se limite pas à la prévention, il est également crucial d'assurer une supervision continue. Nous pouvons mettre en place un système de monitoring basé sur plusieurs outils complémentaires.

Grafana

Cela nous permet de collecter et d'afficher en temps réel les métriques des serveurs, des bases de données et des services réseau.

Centralisation des logs (Loki/Promtail)

Toutes les actions administratives, les connexions et les événements système sont collectés et stockés via Loki et Promtail, une solution de logging légère et optimisée pour Grafana. Promtail est utilisé pour récupérer et envoyer les logs des différentes machines, tandis que Loki permet une indexation efficace sans nécessiter de stockage lourd comme une base de données Elasticsearch. L'intégration native avec Grafana offre une visualisation dynamique des logs et facilite l'analyse en temps réel.

Alertes automatisées :

Des notifications sont envoyées en cas d'anomalie, comme une augmentation anormale de la charge serveur ou une tentative de connexion suspecte. Grafana Alerting, en combinaison avec Loki, permet d'envoyer des alertes en temps réel aux administrateurs, garantissant une réactivité immédiate face aux incidents.

En cas d'incident, notre système de supervision permet une détection rapide des événements critiques et une analyse approfondie des logs pour identifier l'origine du problème. Grâce à la synergie entre Loki, Promtail et Grafana, nous disposons d'un monitoring avancé, assurant une traçabilité efficace et une gestion proactive de la sécurité et des performances du système.

Stratégie de sauvegarde

Hugo

Pour garantir l'intégrité des données et assurer une reprise rapide en cas de problème, nous avons défini une stratégie de sauvegarde rigoureuse.





Sauvegarde des machines virtuelles

Chaque site dispose d'un Proxmox Backup Server (PBS) dédié, permettant de sauvegarder non seulement les VMs et les conteneurs, mais aussi l'hyperviseur Proxmox lui-même. Ces sauvegardes sont stockées sur un NAS.

Planification et gestion des sauvegardes

Les sauvegardes sont orchestrées via Proxmox VE (PVE), qui centralise et automatise les jobs de sauvegarde. Une sauvegarde quotidienne de l'ensemble des hôtes est réalisée sur le NAS du site principal, tandis qu'une sauvegarde hebdomadaire est effectuée sur un disque dur interne ou externe pour une conservation plus longue.

Stockage sécurisé des backups

Les sauvegardes tournent de 22h à 6h, minimisant ainsi l'impact sur les performances du système. En dehors de cette plage horaire, les disques de sauvegarde externe doivent être déconnectés et transportés hors site par Hugo ou Loïs.

Cette approche nous permet d'être prêts à restaurer nos services rapidement, quelles que soient les circonstances.

Redondance et continuité de service

Hugo

L'un des enjeux majeurs de notre infrastructure est d'assurer une haute disponibilité et une continuité de service, même en cas de panne matérielle ou logicielle. Pour cela, nous avons mis en place un système de redondance permettant d'optimiser la tolérance aux pannes et la résilience globale de l'infrastructure.

Mode site principal / secondaire

L'un des sites est considéré comme primaire, tandis que l'autre est considéré comme second site capable de reprendre toute la charge en cas de panne sur le 1er et inversement bien sûr. Mais bien sûr, que ce soit sur les 2 sites, il y a la présence des mêmes services et tournent en même temps.

Bases de données en master-slave

Les bases de données sont configurées avec une réplication en master-slave, garantissant un failover automatique en cas d'incident sur le serveur principal. Des outils comme Master High Availability ou Orchestrator sont utilisés pour gérer cette réplication et éviter les interruptions de service.

Synchronisation des fichiers via rsync

Étant donné que les hôtes virtuels se trouvent dans une DMZ publique, le contenu des sites est synchronisé via rsync à travers un tunnel SSH, garantissant ainsi une réplication sécurisée et efficace des fichiers critiques.





Avec ce système, nous pouvons assurer la continuité du service en cas de panne sur un site, tout en optimisant la charge entre les deux hôtes en temps normal.

De plus, la connexion des utilisateurs repose sur un enregistrement DNS dynamique, qui nous permet de rediriger automatiquement le trafic vers un site fonctionnel en cas d'incident.

Avec un failover DNS, un fournisseur DNS dédié permet de basculer automatiquement vers une autre IP publique en cas de défaillance de l'un des sites. Puis avec l'optimisation des performances avec un équilibrage de charge DNS, cela nous permet une meilleure répartition du trafic entre les deux sites en temps normal.

Recommandations de sécurité

Axel

En complément des mesures de sécurisation déjà mises en place, nous avons réalisé une revue de sécurité détaillée afin d'analyser les risques potentiels et d'appliquer les bonnes pratiques en cybersécurité. Cette évaluation s'est concentrée sur plusieurs aspects critiques : l'exposition des services sur Internet, la protection des accès distants et la gestion des flux internes entre nos différentes zones réseau.

L'un des premiers points analysés concerne les services exposés sur Internet, notamment dans la DMZ publique où sont hébergés notre serveur web, notre reverse proxy et notre Web Application Firewall (WAF). L'objectif est ici de réduire au maximum la surface d'attaque en restreignant les accès aux seuls ports nécessaires et en appliquant des filtres rigoureux.

Nous avons donc mis en place plusieurs mesures clés pour renforcer la sécurité de cette zone. Tout d'abord, nous avons **forcé l'utilisation du HTTPS**, interdisant toute connexion non sécurisée en HTTP. Ensuite, nous réalisons **des scans réguliers des ports ouverts** afin de détecter d'éventuelles expositions involontaires. Enfin, un filtrage strict des flux entrants et sortants est appliqué via le pare-feu, de manière à ne laisser circuler que les communications autorisées.

Grâce à ces protections, nous limitons au maximum les risques d'intrusion sur les services accessibles depuis l'extérieur, tout en conservant une flexibilité nécessaire à l'administration de l'infrastructure.

Loïs

Un des aspects les plus critiques de la cybersécurité concerne **la gestion des accès distants**. L'administration de notre infrastructure doit pouvoir se faire de manière sécurisée, sans jamais exposer directement les services internes sur Internet. Pour cela, nous avons mis en place deux types de VPN afin d'assurer une connexion chiffrée et contrôlée entre les sites et pour les administrateurs.

Le VPN IPSec permet d'établir un tunnel sécurisé site-à-site, assurant une interconnexion fluide entre nos deux infrastructures sans compromettre la sécurité. En complément, nous avons déployé un VPN SSL via Stormshield, réservé aux administrateurs ayant besoin d'un accès à distance.





Pour garantir un haut niveau de protection, nous avons mis en place plusieurs précautions concernant l'accès au VPN SSL.

Accès restreint à un port spécifique

Le service VPN SSL est uniquement accessible via le port sslvpn défini sur le pare-feu Stormshield, limitant ainsi l'exposition aux attaques et empêchant les tentatives de force brute sur d'autres ports ouverts.

Portail captif sécurisé

Un portail captif est déployé en interne et en externe, accessible uniquement sur un port dédié, afin de renforcer le contrôle des connexions entrantes.

Attribution d'une IP dédiée

Chaque connexion VPN SSL reçoit une adresse IP issue du réseau VPNSSL, lui attribuant les mêmes privilèges qu'un utilisateur interne tout en maintenant un contrôle strict des accès.

Traçabilité complète des connexions

Tous les accès VPN, qu'ils soient IPSec ou SSL, sont enregistrés dans les logs avancés du pare-feu. La journalisation des connexions permet un audit détaillé et une détection rapide des comportements suspects.

Ce dispositif assure une connexion sécurisée pour les utilisateurs distants tout en maintenant une visibilité complète sur les accès à l'infrastructure.

Arthur

Cette revue de sécurité nous permet d'évaluer et de renforcer la protection de notre infrastructure sur plusieurs niveaux : segmentation réseau, sécurisation des accès distants, contrôle des flux inter-VLAN et mise en place d'une supervision avancée. Cependant, la cybersécurité est un processus continu, et il y a bien sûr plusieurs axes d'amélioration à intégrer dans notre stratégie pour renforcer la sécurité.





IV. Point techniques et d'avancement

Avancement technique et état du projet

Arthur

Nous allons maintenant faire un point sur l'état d'avancement technique du projet Wizards & Dice. Voir ce qui est déjà en place, ce qui fonctionne, ainsi que les choix des technologies et leur justification.

Dans un premier temps, Hugo a réalisé une étude technique et une revue de sécurité pour le projet. Ces documents nous offrent une vue d'ensemble et une meilleure compréhension de l'architecture mise en place.

Mais concrètement, plusieurs éléments clés de l'infrastructure ont été déployés et configurés. Le pare-feu Stormshield est désormais en place, avec une segmentation réseau active et des VLANs utilisateurs bien définis sur le site d'Hugo. Les premières règles de filtrage ont été appliquées, garantissant une séparation claire des flux entre chaque zone. Pour assurer une connectivité sécurisée, un VPN SSL a été mis en place sur le pare-feu Stormshield, venant compléter ceux déjà existants sur les box des sites d'Hugo et de Loïs. La gestion des accès a également été renforcée avec la création d'un serveur Active Directory et d'un domaine. De plus, un serveur dédié au bastion SSH a été déployé afin de sécuriser l'administration des machines. Enfin, plusieurs serveurs essentiels ont été mis en place et sont prêts à être configurés, notamment un serveur de monitoring (Grafana), un serveur de logs (Loki), un serveur web (Apache) destiné à l'hébergement du site, ainsi qu'un serveur de sauvegarde basé sur Proxmox Backup Server.

Hugo

Nous avons également intégré un NAS en RAID 5 à l'infrastructure, qui servira pour le stockage des backups des hôtes. Un serveur de sauvegarde est installé mais non configuré, avec les datastores configurés sur l'un des nœuds (chez Hugo). Enfin, le NAT dynamique est fonctionnel sur le stormshield pour permettre aux services internes d'accéder à Internet tout en gardant un contrôle strict sur les flux sortants.

Ensuite, nous avons installé et déployé les Proxmox VE sur les deux machines physiques qui possèdent l'hyperviseur, permettant d'héberger et de gérer nos machines virtuelles et conteneurs. Bien que le clustering ne soit pas encore mis en place, chaque hyperviseur est à un certain niveau, opérationnel et accessible pour l'administration.

Tout ce qui est évoqué pour l'avancement technique, concerne principalement qu'un seul site pour l'instant, chez Hugo même si quelques éléments ont été configurés et déployés pour le site de Loïs (Proxmox) et quelques serveurs.





Choix des solutions et justification des technologies

Axel

Hyperviseur et virtualisation

L'un des choix fondamentaux a été la virtualisation de l'infrastructure via Proxmox VE. Ce choix s'explique pour plusieurs raisons : c'est une solution open-source robuste, qui supporte aussi bien la virtualisation complète (VM) que les conteneurs LXC, ce qui nous permet d'optimiser l'utilisation des ressources. Contrairement à VMware ESXi qui nécessite une licence payante, Proxmox nous offre une flexibilité totale et une intégration native avec Proxmox Backup Server (PBS) pour une gestion optimisée des sauvegardes.

Nous avons aussi adopté une architecture mixte avec des machines virtuelles et des conteneurs LXC. Les conteneurs sont utilisés pour des services légers qui peuvent partager le noyau de l'hôte, comme le serveur web, le serveur WAF, le reverse proxy et le monitoring, tandis que les VMs sont réservées aux services critiques nécessitant un isolement complet, comme les bases de données et le serveur de sauvegarde. Ce choix permet d'optimiser la charge, d'améliorer les performances et de réduire la consommation de ressources.

Loïs

Sauvegarde / NAS

Hugo l'a déjà mentionné, mais nous avons choisi de séparer le stockage en plusieurs espaces dédiés afin d'assurer la pérennité des données et d'améliorer la tolérance aux pannes. Cette approche permet de limiter l'impact d'une défaillance et d'optimiser la gestion des ressources.

Le NAS, intégré à l'infrastructure, est accessible via NFS sécurisé avec un tunnel SSH, garantissant un accès rapide tout en maintenant un haut niveau de sécurité. L'intégration prochaine avec Active Directory viendra renforcer l'authentification et centraliser la gestion des droits d'accès. Cela permettra d'améliorer la sécurité tout en facilitant l'administration une fois le déploiement achevé.

Pour les sauvegardes, nous avons opté pour Proxmox Backup Server (PBS), une solution spécifiquement conçue pour s'intégrer avec Proxmox. Ce choix nous permet d'assurer une gestion efficace des backups des machines virtuelles, avec une optimisation du stockage, une déduplication intégrée et des performances adaptées à nos besoins.

Nous avons privilégié un RAID 5 sur un NAS 4 baies, ce qui permet une tolérance aux pannes tout en optimisant l'espace de stockage disponible. Chaque hôte Proxmox dispose également de disques internes, assurant une première couche de redondance locale avant l'envoi des sauvegardes vers le NAS ou un stockage externe.





Arthur

Pare-feu

La sécurisation de notre plateforme est un élément fondamental, donc le choix technologique a été fait en prenant en compte certaines pratiques en matière de cybersécurité.

Au niveau de l'infrastructure, nous avons opté pour Stormshield en tant que pare-feu plutôt que des solutions comme pfSense ou WatchGuard, pour plusieurs raisons stratégiques :

Une approche certifiée et éprouvée

Stormshield bénéficie de certifications de sécurité (ANSSI, EAL4+, etc.), ce qui renforce la confiance dans sa capacité à protéger des environnements sensibles.

Une segmentation stricte des VLANs

Contrairement à pfSense, Stormshield permet une gestion avancée des réseaux segmentés avec un contrôle rigoureux des flux, évitant tout débordement entre les zones sensibles.

Une intégration native avec notre VPN IPSec

Contrairement à WatchGuard, qui nécessite souvent des configurations plus complexes, Stormshield offre une compatibilité immédiate avec nos besoins en VPN site-à-site et utilisateurs distants.

De plus, pour renforcer la sécurité des accès, nous avons intégré un bastion SSH sécurisé afin d'éviter toute exposition directe des machines critiques sur Internet. L'accès aux services est strictement limité via VPN, et nous avons mis en place une authentification basée sur des clés SSH, garantissant une protection renforcée contre les tentatives d'intrusion.

Hugo

Monitoring/log

Pour garantir la stabilité et la disponibilité de notre infrastructure, nous avons mis en place une solution de supervision complète basée sur **Grafana** et **Loki/Promtail**.

Grafana nous permet de visualiser les métriques en temps réel, facilitant le suivi des performances et l'anticipation d'éventuelles dégradations.

Loki a été retenu pour sa légèreté et son intégration native avec **Grafana**, permettant une indexation efficace sans dépendre d'une base de données lourde comme Elasticsearch. **Promtail**, quant à lui, assure la récupération et l'envoi des logs de nos services, garantissant une centralisation fluide et un suivi en temps réel des événements critiques.

Contrairement à des solutions plus complexes comme **Graylog** ou **ELK**, Loki est particulièrement adapté à notre besoin, car il offre une gestion efficace des logs applicatifs et système sans consommer trop de ressources, tout en permettant une recherche rapide et une corrélation des événements en temps réel.





Axel

Applicatif et serveur web (Apache/Wordpress)

Passons maintenant aux choix du côté applicatif. Comme Wizards & Dice est une plateforme e-commerce, nous avons comparé plusieurs solutions avant d'opter pour **WordPress + WooCommerce**.

Nous avons envisagé des alternatives comme PrestaShop ou Magento, mais elles présentaient des inconvénients majeurs pour notre projet :

- Magento est trop complexe à administrer et trop gourmand en ressources, ce qui nécessite un hébergement beaucoup plus robuste.
- PrestaShop, bien que performant pour un site e-commerce, est moins flexible pour gérer un blog et des contenus communautaires, ce qui est un élément clé pour notre vision de Wizards & Dice.

Avec **WordPress + WooCommerce**, nous avons un compromis idéal :

- Facilité de mise en place et d'administration, même pour des utilisateurs non techniques.
- Écosystème riche en extensions, permettant d'ajouter rapidement de nouvelles fonctionnalités comme la gestion des stocks, les avis clients ou encore les paiements.
- Optimisation pour le SEO, qui est crucial pour le référencement de notre site.
- Flexibilité pour intégrer des éléments communautaires, comme un blog, des forums ou un système de gestion de membres.

En ce qui concerne le serveur web, nous avons opté pour **Apache** plutôt que **Nginx**. Apache est un choix pertinent pour WordPress, notamment grâce à sa compatibilité native avec **.htaccess**, qui permet une gestion fine des redirections et des règles de sécurité. De plus, il offre une meilleure compatibilité avec de nombreux modules PHP et une configuration plus intuitive, ce qui facilite son administration.

Loïs

Services importants supplémentaires

En complément des choix déjà évoqués, nous avons également dû définir les technologies utilisées pour certains services clés, comme le DNS interne, la gestion des logs, le reverse proxy, et la supervision. Chacun de ces services joue un rôle essentiel dans l'infrastructure et a été sélectionné en fonction de ses performances, de sa compatibilité avec le reste du système et de sa simplicité d'administration.

Ainsi, pour garantir la stabilité et la sécurité de notre infrastructure, nous avons fait des choix techniques stratégiques sur trois points clés : les environnements de test, la gestion du trafic via un **WAF** et un reverse proxy, et l'administration DNS interne.





Pour l'environnement de test, nous avons opté pour une machine virtuelle dédiée au staging plutôt qu'un conteneur LXC. Une VM offre une meilleure isolation et gestion des snapshots, ce qui permet de tester les mises à jour et simuler des pannes sans impacter la production.

Côté trafic, nous utilisons **ModSecurity** comme WAF, car il permet une protection avancée contre les attaques web tout en étant plus flexible et économique que des solutions propriétaires.

En complément, Nginx a été choisi comme reverse proxy, car il est plus performant qu'Apache pour gérer un grand nombre de connexions simultanées et intègre du caching et du load balancing.

Enfin, pour la gestion DNS interne, nous avons retenu **BIND9** couplé à **Webmin**, qui offre un contrôle précis des enregistrements DNS internes. **PiHole**, bien qu'efficace pour le filtrage, est moins adapté aux besoins d'une infrastructure de cette taille.

Nos choix se basent sur la performance, la flexibilité et la sécurité.

Arthur

De manière générale, nos choix technologiques reposent sur l'optimisation des ressources et la performance. Nous avons privilégié les conteneurs LXC pour leur faible consommation et leur rapidité, sauf pour les services critiques comme la base de données et l'environnement de test, qui nécessitent une isolation plus poussée via des VMs.

Cette logique s'applique à l'ensemble de notre stack technique : Proxmox a été retenu pour sa flexibilité et son efficacité en virtualisation, Grafana et Loki pour leur légèreté dans la supervision, et Stormshield pour son approche robuste en matière de pare-feu et de segmentation réseau.

Hugo

Tous ces choix techniques nous permettent d'avoir une infrastructure cohérente, performante et sécurisée. Que ce soit au niveau du réseau, des services web, du stockage, de la supervision ou de la gestion des accès, chaque composant a été sélectionné pour garantir un fonctionnement optimal tout en assurant une évolutivité.





V. Planning et organisation

Prochaines étapes

Axel

Nous avançons sur le déploiement des services et serveurs, mais plusieurs étapes restent encore à finaliser avant d'avoir une infrastructure pleinement opérationnelle.

Actuellement, nous déployons le Bastion SSH, le serveur de logs, ainsi que plusieurs services transverses comme l'Active Directory, le DNS, les bases de données et le serveur web. Ces éléments forment le socle de notre architecture et doivent être bien intégrés avant de passer aux étapes suivantes.

Les tâches en cours avancent bien, mais nous rencontrons quelques défis techniques. Par exemple, la configuration avancée du pare-feu nécessite des ajustements, et la mise en cluster des hyperviseurs Proxmox est conditionnée à l'établissement d'un VPN IPsec stable entre les deux sites.

Les prochaines étapes incluent la mise en place du serveur de test, du reverse proxy, du WAF et du monitoring. Une fois ces briques en place, nous devons finaliser la configuration complète de l'infrastructure, à la fois au niveau système et applicatif, pour s'assurer que chaque service fonctionne correctement et communique de manière sécurisée.

Un autre point critique à venir est la **sécurisation de l'infrastructure**. Cela concerne **la sécurité réseau** (pare-feu, segmentation VLAN, restrictions d'accès) et **la sécurité applicative** (durcissement des services, protection contre les vulnérabilités, monitoring des activités suspectes).

Enfin, la dernière étape clé sera l'implémentation et la mise en production du site e-commerce, ce qui inclut le paramétrage de WordPress et WooCommerce, l'optimisation des performances et les derniers tests fonctionnels avant la validation du Proof of Concept (POC).

Organisation et planification

Loïs

Pour structurer notre progression et respecter les délais en vue du dernier jalon, qui est la validation du Proof of Concept (POC), nous nous basons sur **un planning détaillé** avec un **diagramme de Gantt**. Chaque tâche est découpée en phases précises avec des dépendances claires, ce qui nous permet d'optimiser notre travail et de prioriser les actions les plus critiques.

Nous avons réparti le travail en trois grands axes.





Finalisation du déploiement des services

Cela inclut la mise en place des derniers serveurs et la configuration réseau. Cette phase est essentielle pour stabiliser notre infrastructure et garantir une bonne interconnexion entre les services.

Sécurisation et durcissement

Dès que tous les services seront en place, nous procéderons à l'application des mesures de sécurité, à la fois sur l'infrastructure réseau et les applications. Cela inclut le renforcement du pare-feu, la mise en place de certificats HTTPS, l'audit des accès, et le monitoring avancé.

Implémentation du site et tests finaux

Une fois l'environnement sécurisé, nous pourrions finaliser le site web, ajuster les dernières optimisations de performance et effectuer des tests complets avant la mise en production. L'objectif est de valider toutes les fonctionnalités et la stabilité de la plateforme avant le POC.

Nous avançons en suivant ce planning méthodique pour garantir un déploiement efficace et sécurisé, tout en anticipant les éventuels imprévus techniques et en nous adaptant aux contraintes du projet.





VI. Conclusion

Arthur

En résumé, nous déployons une infrastructure distribuée et sécurisée, en avançant progressivement vers un environnement stable et optimisé pour notre site e-commerce. La mise en place de la base est en train de se mettre en place avec la segmentation réseau, la virtualisation des services et les premières mesures de supervision, mais il reste encore des étapes cruciales à finaliser, notamment la sécurisation avancée, l'intégration applicative et la mise en production. L'objectif final est de valider notre Proof of Concept (POC) en garantissant performance, résilience et sécurité. Avec une approche méthodique et un suivi rigoureux, nous sommes en bonne voie pour livrer une plateforme fiable et évolutive.

