




Oral du jalon 4 – Script WIZARDS & DICE

 Créateur : Arthur YANG – Responsable Documentation & Administratif

 Date de Création : 29/01/2025

 Dernier modificateur : Axel MOURILLON – Chef de projet

 Date de modification : 16/02/2025

 Version : 2.0



Table des matières

I. Introduction.....	2
II. Présentation globale de l'infrastructure.....	2
A) Structure des sites.....	2
B) Réseaux.....	3
1/ Réseaux existants.....	3
2/ Interconnexion des sites.....	3
3/ Connexion aux sites via VPN.....	3
III. Sécurisation et supervision (R5.Cyber.11).....	3
IV. Point techniques et d'avancement.....	6
V. Planning et organisation.....	9
VI. Conclusion.....	9

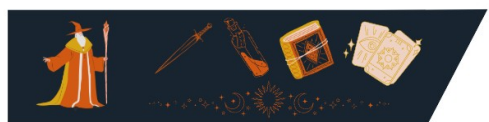
Le script ci-dessous sert de **Guideline** plutôt que de texte à réciter mot pour mot.
Il contient des éléments rédigés, mais aussi des points clés que chacun pourra développer à sa manière s'il en a envie.

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

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

A) Structure des sites

HUGO

Présentation de l'infrastructure

- L'architecture repose sur deux sites d'hébergement situés chez Hugo et Loïs.

Structure des sites

- Chaque site possède :
 - Son propre accès Internet et son pare-feu dédié.
 - L'ensemble des services nécessaires au projet.
- Les sites ont :
 - Les mêmes services pour garantir la continuité d'activité et un basculement automatique.
 - Un réseau LAN spécifique à chaque site, mais avec une configuration et des services identiques.

Infrastructure technique

- Chaque site dispose :
 - D'un hyperviseur Proxmox pour héberger et gérer les machines virtuelles.
 - D'un tunnel IPSec assurant une communication fluide et sécurisée entre les sites.
 - De plusieurs services critiques, notamment :
 - Bases de données
 - Solutions de monitoring
 - Serveur web
 - Outils de gestion des accès

B) Réseaux

AXEL

1/ Réseaux existants

- Chaque site : un plan d'adressage IP et VLANs segmentés par usage
- VLAN : servers, users, BDD et DMZ
- Segmentation : services isolés / performances optimisées / trafic sécurisés

2/ Interconnexion des sites

- VPN IPSec : communication sécurisée entre sites
- Tunnel VPN : gestion centralisée et accès aux ressources distantes le tout en sécurité

3/ Connexion aux sites via VPN

- VPN SSL : complément du VPN IPSec ; accès distant sécurisé
⇒ Pour les connexion des admins et des users hors site





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

A) Segmentation et protection du réseau

LOÏS

Qu'est-ce qu'on retrouve dans les VLAN de notre réseau (VU diapo pour les arddressage – rester sur le plan) :

- DMZ WEB → Serveur web, le reverse proxy et le WAF
- DMZ PRIVÉE → Bastion
- VLAN SERVEUR → Service interne : monitoring Graphana / sauvegarde / NAS / Hyperviseurs de Proxmox, serveur de teste, serveur DNS
- VLAN DATABASE → VM qui support les bases de données de production et préproduction : garantir l'isolation du service

Tous ces segments sont filtrés et sécurisés **via un pare-feu Stormshield** → **Contrôler le trafic**

B) 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.

1/ 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.

2/ 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.

C) Authentification et gestion des accès

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.





1/ Grafana

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

2/ 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.

3/ 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.

D) Stratégie de sauvegarde

HUGO

Objectif

- Assurer l'intégrité des données et garantir une reprise rapide en cas de problème.
- Sauvegarde des machines virtuelles

Chaque site dispose d'un Proxmox Backup Server (PBS) dédié.

- Sauvegarde des VMs, conteneurs et de l'hyperviseur Proxmox lui-même.
- Stockage des sauvegardes sur un NAS.

Planification et gestion des sauvegardes

- Sauvegardes orchestrées via Proxmox VE (PVE) pour automatiser les jobs.
- Sauvegarde quotidienne sur le NAS du site secondaire à 2h pour minimiser l'impact sur les performances.
- Sauvegarde hebdomadaire sur un disque dur externe pour une conservation plus longue et offline 18h après la réunion hebdomadaire.

Bénéfice

- Permet une restauration rapide des services quelles que soient les circonstances.





E) Redondance et continuité de service

Objectif

- Assurer une haute disponibilité et une tolérance aux pannes pour garantir la continuité des services.

Architecture de redondance

- Les deux sites fonctionnent en parallèle avec un mode primaire / secondaire.
- En cas de panne sur un site, l'autre peut reprendre la charge automatiquement.

Gestion des bases de données

- Mise en place d'une réplication master-slave permettant un failover en cas d'incident.

Synchronisation des fichiers

- Synchronisation des fichiers critiques entre les sites via rsync, permettant une mise à jour efficace et sécurisée des données.

Gestion du trafic et accès utilisateurs

- DNS dynamique et Failover DNS permettant un basculement rapide vers une autre IP en cas de panne.

F) Recommandations de sécurité

AXEL

Revue de sécurité réalisée

⇒ Analyser les risques potentiels, appliquer les bonnes pratiques de cybersécurité

Plusieurs aspects critiques revus :

- Surface exposé à Internet
- Protection des accès distants
- Gestion des flux internes (entre site / VLAN)

Analyse de la surface exposé

- DMZ publique : serveur web / reverse proxy / WAF
⇒ Objectifs : Réduire au maximum la surface d'attaque ; restreindre et filtrer les flux trafic nécessaire

Éléments mis en place suite à la revue de sécurité

- Interdiction d'HTTP ⇒ utilisation d'HTTPS forcé
- Revue régulières des ports ouverts (scan) : détection d'expositions involontaires
- Filtrage strict des flux au niveau du pare-feu [de chaque site]

But : limiter les risques d'intrusion depuis l'extérieur / conserver de la flexibilité pour l'administration de l'infra

LOIS

Recommandations de sécurité -> Axel plutot -> deux types de VPN

VPN IPSec : intersite

VPN SSL : adminstrateur via stormshield

Pour renforcer VPN SSL :

- Uniquement accessible via le port sslvpn défini sur le pare-feu Stormshield
- Un portail captif est déployé en interne et en externe





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

Pour les deux VPN : on a une traçabilité complète des connexions -> enregistrés dans les logs avancés du pare-feu -> surveiller cette accès sensible

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

A) 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

Infrastructure et stockage

- Un NAS en RAID 5 a été intégré pour le stockage des sauvegardes des hôtes.
- Un serveur de sauvegarde est installé et configuré.
- Les datastores sont configurés sur l'ensemble des nœuds.

Réseau et connectivité

- Un NAT dynamique est fonctionnel, assurant l'accès des services internes à Internet tout en maintenant un contrôle strict sur les flux sortants.

Déploiement des hyperviseurs

- Les hyperviseurs sont installés et permettent l'hébergement et la gestion des machines virtuelles et conteneurs.
- Le clustering est en place à travers le tunnel Ipsec.

État d'avancement

- L'essentiel du travail a été réalisé sur un seul site pour l'instant.
- Certains éléments ont déjà été configurés et déployés pour le second site.





B) Choix des solutions et justification des technologies

1/ Hyperviseur et virtualisation

AXEL

Virtualisation de l'infrastructure par Proxmox VE (PVE)

- Solution open-source, robuste, et gratuite
- Supporte les VM et les conteneurs ⇒ optimisation des ressources
- Intégration native de gestion des sauvegardes avec PBS (*mentionné par Hugo*)

Architecture mixte de VM et de conteneurs LXC

- VMs pour les services critiques / un isolement complet : BDD, sauvegardes, AD
 - Conteneurs pour des services légers partageant le noyau d'un hôte : serveurs web / WAF / monitoring et reverse proxy
- ⇒ Améliorer les perf et optimiser et réduire la consommation des ressources

2/ Pare-feu

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.
- Passage et certifs
- Connaissance de base en cours d'acquisition, certifs déjà par hugo.
- Facilité de configuration
- Subjectif mais config vpn , filters , systeme facile.

3/ Monitoring et gestion des logs

HUGO

- Loki a été choisi pour la gestion des logs applicatifs et système.
- Il permet une recherche rapide et une corrélation des événements en temps réel.
- Sa mise en place est optimisée en termes de ressources par rapport à d'autres solutions plus complexes. Donc solution plus adaptée à notre format « maquette ».





4/ Applicatif et serveur web (Apache/Wordpress)

AXEL

Côté applicatif : plateforme e-commerce donc WordPress + WooCommerce.

PrestaShop envisagé : performant mais moins flexible pour certaines de nos fonctionnalités (ex : blog)

- Magento envisagé : trop complexe à administrer trop gourmand en ressources

Le cas WordPress + WooCommerce : compromis idéal

- Facilité de déploiement / administration (même pour des non-techniques)
- Écosystème riche en extensions : ajout rapide de nouvelles fonctionnalités (paiements, gestion des stocks, avis clients, ...)
- Optimisé pour le SEO [Search Engine Optimization] : référencement du site
- Flexibilité pour intégration d'éléments communautaires (blog, forums, système de membres)

Serveur web Apache plutôt que Nginx

- Compatibilité avec .htaccess : gestion des redirections et des règles de sécurité.
- Meilleure compatibilité avec les modules PHP
- Configuration plus intuitive : facilite son administration

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.





V. Planning et organisation

C) Étapes à venir

AXEL

Citer les 3 parties du déploiement : Déploiement ; Configuration ; Sécurisation / Site

En cours : déploiement basique des services et serveurs ⇒ Socle de notre architecture

- Bastion SSH (partiellement déployé)
- Serveur de logs
- Bases de données
- Services transverses (notamment LDAP)

Défis techniques : choses retors mais qui avancent

- Configuration avancée du pare-feu nécessite des ajustements
- Ajustement de la récente mise en cluster des hyperviseurs Proxmox

Les étapes suivantes (techniques only) :

- *Fin étape 1 (Déploiement)* : Mise en place du reverse proxy, du WAF et de la supervision / monitoring infra

D) planification à plus long terme

LOÏS

Etape suivante -> ajuster la configuration en fonction des bons services : système, réseau et applicatif :

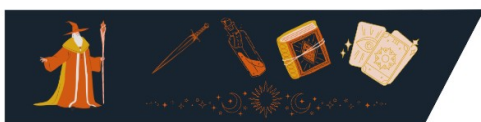
⇒ Chaque service doit fonctionner correctement et de façon stable

Etape sécurisation de l'infrastructure

- Niveau Réseau: pare-feu Stormshield, segmentation VLAN, restrictions d'accès
- Niveau Système: pare-feu sur les VM, restrictions des logiciels
- Niveau Applicative: durcissement des services, protection contre les vulnérabilités, monitoring des activités suspectes (à voir au niveau du temps)

Etape parallèle Implémentation et la mise en production du site e-commerce

- Paramétrage de WordPress et WooCommerce
- Optimisation des performances
- Tests fonctionnels avant la validation du Proof of Concept (POC).





VI. Conclusion

LOIS

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.

