





Critères de dispo réels de l'infrastructure

WIZARDS & DICE

 Créateur : Arthur YANG – Responsable Documentation & Administratif
 Date de Création : 18/05/2025


 Modificateur : Arthur YANG – Responsable Documentation & Administratif
 Date de modification : 18/05/2025
 Version : 1.0



Table des matières :

Table des matières :	1
I. Introduction.....	2
II. Disponibilité de l'infrastructure.....	2
III. Niveau de sécurité observé.....	3
IV. Limites constatées et axes d'amélioration.....	4





I. Introduction

Ce document vise à préciser les critères de disponibilité réels et le niveau de sécurité observé sur l'infrastructure du projet Wizards & Dice, auto-hébergée sur deux sites distincts (AARD et DRYN). Il constitue une base de référence permettant d'évaluer les capacités actuelles de l'infrastructure à maintenir les services en ligne, protéger les données et assurer la continuité d'activité. Il nous assistera également lors des derniers jalons concernant la connaissance réelle de l'infrastructure.

II. Disponibilité de l'infrastructure

L'infrastructure repose sur une architecture répartie entre deux sites physiques (AARD et DRYN), conçue pour garantir une continuité minimale de service même en cas d'incident sur l'un des deux lieux. Cette redondance partielle repose sur plusieurs composantes clés.

Tout d'abord, chaque site dispose d'un hôte Proxmox autonome, permettant d'assurer la virtualisation des services critiques. Cela inclut notamment les serveurs WordPress (web), les bases de données MariaDB (bdd), le bastion SSH, ainsi que les outils de supervision et d'administration. En cas de perte d'un hôte (panne matérielle, sinistre), l'autre hôte est en mesure de reprendre les services via une restauration planifiée.

Les sauvegardes jouent un rôle central dans cette stratégie. Proxmox Backup Server (PBS) est déployé sur chaque site et réalise des sauvegardes programmées journalières selon la criticité des machines virtuelles. Ces sauvegardes sont stockées à la fois localement sur un NAS et à distance sur un disque externe ou le site secondaire, afin de couvrir les risques liés à une perte physique ou une corruption des données.

Une solution de bascule manuelle a été mise en place. Elle repose sur la capacité à identifier rapidement l'incident, à rétablir le service via une restauration des machines critiques (WordPress, BDD, bastion, monitoring) et à reconfigurer les accès réseaux nécessaires (redirection DNS pour le site web, relance VPN, etc.). Bien que manuelle, cette procédure a été testée lors de simulations et documentée de façon opérationnelle.

Le lien entre les deux sites est maintenu par un tunnel VPN IPSec configuré statiquement. Celui-ci permet non seulement la synchronisation des sauvegardes ou des fichiers, mais également la supervision croisée et l'administration à distance. En cas de défaillance Internet sur un site, l'autre peut temporairement prendre le relais pour servir les contenus essentiels.

Les services principaux (site e-commerce sous WordPress, base de données MariaDB, accès SSH au bastion, interface Grafana pour les logs et la supervision) ont tous été pensés pour être redéployés rapidement en fonction des priorités définies. Cela garantit une reprise des activités commerciales ou administratives dans des délais jugés acceptables pour le contexte du projet.





III. Niveau de sécurité observé

La sécurité de l'infrastructure Wizards & Dice repose sur une stratégie défensive multicouche combinant des outils techniques, des contrôles systématiques et une segmentation logique rigoureuse. L'objectif est de réduire la surface d'attaque et de garantir la protection des services critiques même en cas d'incident.

L'accès au système est contrôlé via une segmentation réseau stricte entre les services publics (site WordPress, supervision Grafana) et les composants internes. Toutes les opérations d'administration passent obligatoirement par un bastion SSH, configuré avec des restrictions d'adresses IP sources, une authentification, et des journaux d'accès centralisés. En périphérie, un pare-feu Stormshield agit comme filtrage principal au niveau du réseau physique.

Chaque serveur (Proxmox, NAS, conteneurs applicatifs) est protégé localement par un pare-feu logiciel (UFW) configuré avec des règles restrictives. En complément, AppArmor est activé pour fournir une couche de confinement basique au niveau des processus sensibles. Cela permet de limiter les privilèges même en cas de compromission partielle.

Des outils de sécurité supplémentaires sont en place pour renforcer la défense du système :

- Fail2ban est déployé sur les services exposés pour bloquer automatiquement les adresses IP suspectes.
- Lynis est utilisé périodiquement pour auditer la configuration système et proposer des améliorations.
- Et d'autres...

La supervision est assurée par le trio Promtail, Grafana et Loki. Ces outils permettent de collecter, afficher et analyser en temps réel les logs système, les comportements utilisateurs, les anomalies de performance ou les tentatives de connexion non autorisées. Ils constituent un axe central de détection précoce des incidents.

Les données sensibles et critiques sont sauvegardées de manière chiffrée et stockées sur plusieurs supports (NAS local et disque dur externe). Les sauvegardes sont testées régulièrement et font l'objet de vérifications d'intégrité afin de garantir leur exploitabilité en cas de restauration.

Enfin, toutes les configurations critiques sont centralisées dans une documentation interne. Pour les composants techniques dont la documentation officielle était lacunaire (comme Guacamole), Hugo a complété les paramétrages en s'appuyant sur des ressources fiables telles que IT-Connect et l'appui ponctuel de ChatGPT, ce qui a permis de garantir un fonctionnement stable tout en optimisant le temps de déploiement.





IV. Limites constatées et axes d'amélioration

Un document similaire pour ce qu'il n'a pas été mis en place sera effectué plus tard. Il suffit de consulter ce document lorsqu'il sera disponible.

