





Plan de continuité d'activité

WIZARDS & DICE

 Créateur : Arthur YANG – Responsable Documentation & Administratif
 Date de Création : 11/05/2025

 Modificateur : Arthur YANG – Responsable Documentation & Administratif
 Date de modification : 11/05/2025
 Version : 1.0



Table des matières :

Table des matières :	1
I. Introduction générale au PCA	2
A) Objectifs du PCA	2
B) Périmètre du PCA	2
II. Plan de continuité d'activité	3
A) Perte ou panne d'un hyperviseur Proxmox	3
1/ Arrêt brutal d'un hôte Proxmox (site AARD ou DRYN)	3
2/ Cluster Proxmox non joignable	3
B) Indisponibilité du site e-commerce en production	4
C) Corruption ou perte de données sur le NAS	5
1/ Panne matérielle (disques défectueux, RAID HS)	5
2/ Données corrompues ou incomplètes	5
3/ Perte d'accès au NAS local ou crash des sauvegardes	5
D) Autres incidents techniques	6
1/ Problème de connectivité VPN entre les deux sites	6
2/ Incident sur WordPress ou WooCommerce	6
3/ Incident sur les serveurs de l'infrastructure	6
III. Suivi et test du PCA	7
A) Fréquence des tests	7
1/ Tests semestriels	7
2/ Vérification des sauvegardes NAS	7





I. Introduction générale au PCA

Cette section présente les mesures préventives mises en œuvre pour maintenir l'activité critique de Wizards & Dice en cas de dégradation partielle ou totale de l'environnement technique. Contrairement au PRA, le PCA s'inscrit dans une logique d'anticipation et de maintien temporaire de l'activité, même dans un contexte fortement perturbé. Ce document s'appuie sur l'infrastructure en place (deux sites avec redondance, Proxmox, NAS, PBS) et les scénarios d'indisponibilité identifiés.

A) Objectifs du PCA

Le PCA a pour objectif de :

- **Assurer un service minimal** (site e-commerce, accès clients, consultation catalogue) même en cas d'indisponibilité partielle.
- **Garantir un accès sécurisé à distance** pour l'administration technique.
- **Prévoir des solutions de contournement temporaires** avant un retour à la normale via le PRA.

B) Périmètre du PCA

Le PCA couvre les activités essentielles suivantes :

- Affichage et consultation du catalogue produits via WordPress/WooCommerce
- Accès aux bases de données utilisateurs et commandes
- Administration distante via Bastion SSH
- Synchronisation minimale des sauvegardes entre les deux sites
- Et d'autres plus tard...

Ces éléments sont considérés comme prioritaires pour maintenir une présence commerciale et la continuité des commandes en cas d'incident.





II. Plan de continuité d'activité

Cette section présente les actions prévues pour garantir la continuité de service de l'infrastructure Wizards & Dice en cas d'incident majeur. Les scénarios traités ici correspondent aux risques identifiés comme prioritaires : perte d'un serveur, panne du site e-commerce, corruption de sauvegardes ou indisponibilité du stockage principal. L'objectif est de permettre une reprise rapide de l'activité sans perte critique de données.

A) Perte ou panne d'un hyperviseur Proxmox

1/ Arrêt brutal d'un hôte Proxmox (site AARD ou DRYN)

En cas de panne matérielle ou logicielle de l'hyperviseur (alimentation, carte mère, système Proxmox inaccessible), les VMs hébergées sur cette machine deviennent inaccessibles.

Deux cas sont possibles :

Si les disques sont intacts (ZFS ou LVM non corrompus), il est recommandé de transférer les disques physiques dans un second hôte ou de booter Proxmox depuis un live ISO pour accéder manuellement aux VMs.

Si la panne est critique ou les données inaccessibles, on bascule sur les sauvegardes journalières disponibles sur le NAS local ou le disque de secours.

👉 En cas de panne prolongée, les VMs critiques (site web, bases de données, bastion SSH) seront restaurées sur l'autre hôte depuis PBS.

📁 Procédure technique sur le GIT :

wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Procédure_restoration_VM.pdf

2/ Cluster Proxmox non joignable

Si le cluster PVE devient indisponible (panne réseau ou split-brain), il est possible de basculer les VMs manuellement sur un hôte secondaire configuré.

Voir procédure dans :

📁 wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Failover_cluster_hosts.pdf





B) Indisponibilité du site e-commerce en production

Le site web WordPress/WooCommerce est hébergé sur le site AARD. En cas de défaillance de ce site (coupure réseau, perte de Proxmox, problème logiciel sur la VM web, problème sur le serveur web), une intervention manuelle est requise pour relancer le service depuis le site DRYN.

Voici les étapes à suivre :

1. Vérifier si la VM web du site DRYN est prête à être lancée

VM clonée ou restaurée en avance via rsync + PBS, avec le même contenu et base de données.

2. Accéder au tableau de bord OVH → [OVH MANAGER](#)

3. Aller dans “Domaines” > clamond.fr > Zone DNS

➤ Modifier les enregistrements A :

Nom	Ancienne IP (AARD)	Nouvelle IP (DRYN)
@ (racine)	xxx.xxx.xxx.1	xxx.xxx.xxx.2
www	xxx.xxx.xxx.1	xxx.xxx.xxx.2

4. Vérifier que le reverse proxy et le serveur web répondent bien sur DRYN avant de basculer.
5. Attendre la propagation DNS (de quelques secondes à 10–15 min selon TTL).
6. Une fois le site visible sur la nouvelle IP, faire des tests rapides : affichage page produit, commande, connexion admin.

📁 Pour plus de détails sur la procédure DNS OVH et test de basculement sur le GIT :
wizards-n-dices\Infrastructure\SitesWeb\Failover_OVH.txt





C) Corruption ou perte de données sur le NAS

1/ Panne matérielle (disques défectueux, RAID HS)

Le NAS principal fonctionne en RAID 5, ce qui permet une tolérance à la perte d'un disque. Si plusieurs disques tombent en panne ou si le volume RAID devient illisible, les sauvegardes doivent être restaurées depuis un support secondaire.

Un disque externe est connecté chaque semaine et mis à jour automatiquement, puis débranché pour stockage sécurisé.

📁 Voir la procédure complète :

wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Restore_NAS_backup.pdf

2/ Données corrompues ou incomplètes

Les jobs de sauvegarde Proxmox intègrent des vérifications d'intégrité (checksum, hashes). En cas de détection d'une corruption sur une archive :

- La version précédente du backup est utilisée pour restaurer les services.

En cas de suspicion de ransomware ou d'effacement volontaire, les snapshots précédents sont également disponibles pour une restauration propre.

3/ Perte d'accès au NAS local ou crash des sauvegardes

Si le NAS est inaccessible (panne matérielle, erreur réseau), la priorité est de restaurer l'accès au stockage local. Vérifiez la connectivité réseau (ping, SSH) et l'état des disques dans l'interface d'administration du NAS.

Si le NAS est hors service, les sauvegardes critiques doivent être montées à partir du disque de secours prévu à cet effet. Un disque externe est disponible pour chaque site, à brancher manuellement sur le serveur de sauvegarde (PBS) si besoin.

➡ Procéder à la restauration manuelle de la dernière archive des VMs critiques.

📁 Voir :

wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Procédure_montage_disquesecours.pdf

wizards-n-dices\Infrastructure\PBS\Restaurer_VM_depuis_externe.pdf





D) Autres incidents techniques

1/ Problème de connectivité VPN entre les deux sites

En cas de rupture du tunnel IPsec entre les sites AARD et DRYN, la synchronisation des données et les accès administratifs inter-sites sont suspendus.

→ Diagnostiquer l'état du tunnel depuis l'interface du firewall Stormshield. Redémarrer manuellement le service VPN si nécessaire.

→ Si le tunnel ne peut pas être rétabli, passer temporairement en mode isolé pour le site actif, en redirigeant le DNS uniquement vers ce site.

📁 Voir :
wizards-n-dices\Infrastructure\VPN\Procédure_diagnostic_tunnelIPSec.pdf
wizards-n-dices\Infrastructure\DNS\Basculer_entréeDNS_SiteActif.pdf

2/ Incident sur WordPress ou WooCommerce

Un bug, une mise à jour défectueuse ou une faille peut rendre le CMS WordPress inopérant.

→ Première étape : accéder au back-end si possible pour désactiver les plugins ou restaurer un thème par défaut.

→ Si l'accès admin est aussi affecté, restaurer la dernière sauvegarde WordPress depuis le serveur PBS, ou utiliser un snapshot local du conteneur LXC.

→ Vérifier également l'intégrité de la base de données MySQL. Une restauration partielle est possible si seul le front-end est impacté.

📁 Voir :
wizards-n-dices\Infrastructure\WordPress\Procédure_rollback_MAJ_WP.pdf
wizards-n-dices\Infrastructure\PBS\Restaurer_siteWP_snapshot.pdf

3/ Incident sur les serveurs de l'infrastructure

Si un problème survient sur les différents serveurs des fichiers de configurations textes sont présent dans : wizards-n-dices\Infrastructure\

Même si elles ne sont pas spécifiques à beaucoup de problèmes, ces fichiers peuvent être utiles quand même sur certains.





III. Suivi et test du PCA

Cette section précise le cadre de vérification du PCA et la responsabilité du maintien en condition opérationnelle.

A) Fréquence des tests

1/ Tests semestriels

Un test de restauration des VMs critiques est effectué tous les 6 mois pour vérifier la validité des sauvegardes.

2/ Vérification des sauvegardes NAS

Le NAS effectue un rapport hebdomadaire de l'espace disque et de l'état des datastores, envoyé automatiquement par mail via SMTP.

