





# Plan de reprise d'activité

## WIZARDS & DICE

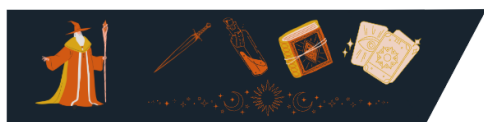
 Créateur : Arthur YANG – Responsable Documentation & Administratif  
 Date de Création : 12/05/2025

 Modificateur : Arthur YANG – Responsable Documentation & Administratif  
 Date de modification : 12/05/2025  
 Version : 1.0



# Table des matières :

<b>Table des matières :</b> .....	<b>1</b>
<b>I. Introduction générale au PRA</b> .....	<b>2</b>
A) Objectifs du PRA.....	2
B) Périmètre du PRA.....	2
<b>II. Scénarios de reprise d'activité</b> .....	<b>3</b>
A) Défaillance critique de site (AARD/DRYN).....	3
1/ Perte totale d'un hôte Proxmox.....	3
B) Perte de connectivité Internet (site unique).....	3
1/ Symptôme : Box Internet KO ou plus de connectivité.....	3
C) Corruption ou suppression accidentelle des bases de données.....	4
1/ Base corrompue ou vidée.....	4
D) Erreur humaine ou compromission (attaque, suppression, ransomware).....	4
1/ Compromission WordPress ou accès admin non autorisé.....	4
2/ Suppression involontaire d'un environnement de test ou de pré-production.....	4
E) Panne matérielle sur le NAS ou PBS.....	5
1/ NAS inaccessible.....	5
2/ NAS ou disque externe corrompu ou détruit.....	5
<b>III. Organisation et coordination</b> .....	<b>6</b>
A) Rôles et responsabilités.....	6
B) Documentation associée.....	6
C) Vérification post-reprise.....	6
<b>IV. Suivi et test du PRA</b> .....	<b>7</b>
A) Fréquence des tests.....	7
1/ Tests annuels.....	7
2/ Vérification des sauvegardes NAS.....	7





# I. Introduction générale au PRA

Cette section présente les mesures techniques et organisationnelles mises en œuvre pour assurer la reprise des activités critiques en cas d'incident majeur. Contrairement au PCA, qui vise à maintenir un service minimal en condition dégradée, le PRA se concentre sur la restauration rapide de l'activité après un sinistre. Ce document s'appuie sur les composants techniques existants (Proxmox, NAS, PBS) et les procédures de restauration déjà définies dans le dossier "wizards-n-dices\Infrastructure".

## A) Objectifs du PRA

Le PRA a pour but de :

- Garantir la reprise des services critiques (site web, bases de données, accès SSH) en moins de quelques heures en cas d'incident majeur.
- S'assurer que les données sauvegardées sont accessibles et restaurables depuis un autre site.
- Définir les étapes et responsabilités associées à la reprise.

## B) Périmètre du PRA

Le PRA couvre l'infrastructure hébergée à domicile sur les deux sites AARD et DRYN :

- Hyperviseurs Proxmox
- NAS et PBS
- Routage VPN IPSec
- Serveurs virtuels et conteneurs
- Lien avec les serveurs OVH pour le domaine






## II. Scénarios de reprise d'activité

### A) Défaillance critique de site (AARD/DRYN)

#### 1/ Perte totale d'un hôte Proxmox

En cas de perte complète du site AARD (ex. incendie, panne matérielle majeure), les sauvegardes disponibles sur le site DRYN permettent une restauration complète.



##### Procédure :

- Action immédiate : restauration des VMs critiques via l'autre hôte Proxmox.
-  Voir procédure dans :  
wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Procédure\_Restauration\_VM.pdf
- Délai cible de reprise : 2h pour les VMs vitales (site, BDD, bastion).
- Une vérification réseau est faite avant toute restauration (DHCP, NAT).

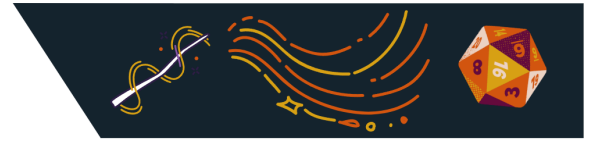
### B) Perte de connectivité Internet (site unique)

#### 1/ Symptôme : Box Internet KO ou plus de connectivité

##### Procédure :

- Diagnostic rapide sur la box (Freebox/SFR).
-  Reconfiguration manuelle de l'entrée DNS OVH pour basculer vers l'IP du second site.
  -  Voir procédure :  
wizards-n-dices\Infrastructure\OVH\DNS\_Manuel\_Switch.pdf
- Pour les données critiques, restaurer temporairement les services à distance via l'autre site.





## C) Corruption ou suppression accidentelle des bases de données

### 1/ Base corrompue ou vidée

#### Procédure :

- Restaurer un snapshot BDD depuis PBS (en local ou distant)
- Tester la validité des données
- Relancer les services WordPress
- 📁 Voir procédure : wizards-n-dices\Infrastructure\PBS\Restauration\_BDD.pdf

## D) Erreur humaine ou compromission (attaque, suppression, ransomware)

### 1/ Compromission WordPress ou accès admin non autorisé

#### Procédure :

- Isolation de la VM WordPress via pare-feu
- Analyse des logs avec Promtail
- Restauration d'un snapshot antérieur validé
- Réinitialisation des accès admin WordPress
- 📁 Voir procédure : wizards-n-dices\Infrastructure\Logs\Analyse\_Compromission\_WP.pdf

### 2/ Suppression involontaire d'un environnement de test ou de pré-production

Ce scénario couvre la perte accidentelle d'une machine virtuelle non critique, utilisée à des fins de tests (environnement de staging, serveur RDS, etc.). Bien que non bloquant pour l'activité commerciale, il est important de restaurer ces environnements pour assurer la continuité des évolutions techniques, des tests fonctionnels et des vérifications avant mise en production.





### Procédure :

- Identifier la VM concernée dans l'interface Proxmox.
- Vérifier la présence de la dernière sauvegarde dans le PBS (locale ou distante).
- Lancer une restauration manuelle depuis l'interface de **Proxmox Backup Server** vers un nœud disponible (AARD ou DRYN).
- Réassigner les ressources nécessaires (RAM, CPU) selon le modèle initial.
- Vérifier la connectivité et les services déployés sur la VM restaurée.
- Documenter l'incident dans le journal interne et valider le fonctionnement via un test utilisateur.

## E) Panne matérielle sur le NAS ou PBS

### 1/ NAS inaccessible

#### Procédure :

- Récupération des sauvegardes sur disque externe (hors site)
- Import manuel dans PBS du site opposé
- Relancer la restauration via Proxmox Restore
- 📁 Voir procédure :  
wizards-n-dices\Infrastructure\NAS-PROXMOX-SVG\Procédure\_Restauration\_Ext  
erne.pdf

### 2/ NAS ou disque externe corrompu ou détruit.

- Recourir à la sauvegarde distante (site secondaire).
- Connexion VPN et restauration depuis le PBS distant (site miroir).
- Vérification des datastores dans :  
Infrastructure\NAS-PROXMOX-SVG\Configuration\_PBS.pdf





## III. Organisation et coordination

### A) Rôles et responsabilités

Rôle	Personne	Actions clés
Responsable technique	Hugo	Déclenchement du PRA, restauration des VMs
Supervision & Logs	Arthur	Vérification des journaux, surveillance de l'activité
Communication client	Axel	Information aux utilisateurs et MAJ site maintenance
Suivi opérationnel	Loïs	Contrôle post-reprise et remontée d'alerte

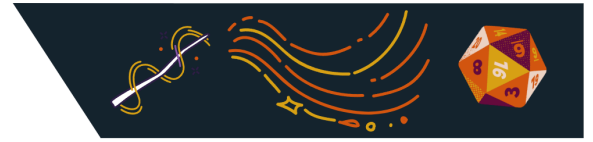
### B) Documentation associée

📁 Toutes les procédures détaillées sont disponibles dans :  
wizards-n-dices\Infrastructure\

### C) Vérification post-reprise

- Contrôle de l'intégrité des données (bdd, fichiers).
- Surveillance via Grafana des performances et charges.
- Test utilisateur sur le parcours d'achat complet.





## IV. Suivi et test du PRA

Cette section précise le cadre de vérification du PRA et la responsabilité de la reprise en condition opérationnelle.

### A) Fréquence des tests

#### 1/ Tests annuels

Un test de restauration des VMs critiques est effectué tous les 12 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.

