Auguste Martinat
Plan de reprise d’activité

Table des matières

Plan de reprise d'activité du 21/05/2025

Auguste Martinat

1. Objectifs du PRA

- Garantir la continuité de l'activité informatique en cas d'incident majeur.
- Limiter les pertes de données et assurer un retour à la normale dans des délais acceptables.
- Prioriser la restauration des services critiques.
- Réduire l'impact sur les utilisateurs et les métiers.

2. Portée du PRA

- Périmètre technique : Serveurs virtualisés sous Proxmox, contrôleurs de domaine, services critiques (AD, fichiers, supervision, GLPI, sauvegardes).
- Périmètre fonctionnel : Utilisateurs internes (admin, RH, élèves), services métiers (compta, RH, support, IT).

3. Liste des actifs et criticité

Équipement	Fonction principale	Criticité	Reprise prévue	RTO	RPO
Active Directory	Authentification, GPO, DNS	Critique	AD secondaire (ADSecours)	1h	15 min
ADSecours	Backup AD, bascule auto	Critique	Automatique	1h	15 min
Zabbix Server	Supervision du SI	Moyenne	Sauvegarde + VM	4h	1h
GLPI	Gestion des tickets / parc	Moyenne	Restauration Veeam	24h	12h
SRVFichier	Serveur de fichiers principal	Critique	Réplication SRVFichier2	2h	30 min
SRVFichier 2	Réplication / redondance fichiers	Critique	Actif-passif	2h	30 min
Veeam	Sauvegarde/restauration VM & fichiers	Critique	Hébergé sur Proxmox HA	1h	15 min
Proxmox 2/3	Hyperviseurs (cluster)	Critique	HA + redéploiement auto	30 min	15 min
Routeur/Switch	Accès réseau local et Internet	Critique	Matériel de secours dispo	1h	-
PC utilisateurs	Accès applicatif	Faible	Image + déploiement rapide	24h	12h

4. Risques identifiés

Risque	Probabilité	Impact	Mesures de mitigation
Panne matérielle (serveur Proxmox)	Moyenne	Critique	Cluster Proxmox + HA
Corruption AD	Faible	Critique	AD secondaire + réplication
Ransomware	Moyenne	Critique	Sauvegarde Veeam isolée
Panne réseau (Switch/Routeur)	Moyenne	Élevé	Équipement de secours en stock
Erreur humaine	Moyenne	Élevé	Procédures documentées + sauvegardes
Inondation / incendie	Faible	Critique	Sauvegardes externalisées

5. Scénarios de sinistre

5.1 Perte d'un hôte Proxmox

Solution : bascule automatique des VM sur nœud survivant + restauration via Veeam si besoin.

5.2 Panne de l'Active Directory principal

Solution : Bascule automatique sur ADSecours.

5.3 Infection ransomware

Solution :

- Isolation réseau
- Suppressions VM chiffrées
- Restauration via Veeam

5.4 Corruption du SRVFichier

Solution : bascule vers SRVFichier2 ou restauration depuis snapshot/sauvegarde

6. Procédures de reprise (standardisées)

1. **Détection de l'incident**
   Outils : Zabbix / alerte utilisateur GLPI
2. **Classification de l'incident**
   - Critique, majeure, mineure
   - Évaluation impact et étendue
3. **Activation du PRA**
   - Validation par RSSI / responsable infra
4. **Mise en œuvre de la reprise**
   - Bascule sur composants de secours
   - Restauration des données si nécessaire
5. **Retour à la normale**
   - Vérification de l'intégrité
   - Remise en production contrôlée
   -
6. **Post-mortem**
   - REX (retour d'expérience)
   - Documentation de l'incident

7. Communication en cas de crise

Rôle	Responsable	Moyen de contact
Responsable Infra	Auguste	Téléphone / Email
Responsable PRA	Auguste	Téléphone
Support utilisateurs	Service IT	GLPI / Téléphone
Direction	Directeur	Email / Réunion

8. Tableau de sauvegarde

Nom de la sauvegarde	Type de données	Fréquence	Outil utilisé	Destination	Temps de sauvergardes	Temps de restauration	Temps de rétention	Taille sauvegarde	Taille du NAS	Responsable
Backup_AD	Active Directory (comptes, groupes, GPO, etc.)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	18 minutes 11 secondes	~30 à 40 min	7 jours	~25 GB	1 TO	Administrateur
Backup_Client	Données des postes clients (profils, documents, etc.)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	18 minutes 06 secondes	~30 à 40 min	7 jours	~28 GB	1 TO	Administrateur
Backup_Compta	Données comptables (logiciel de compta, bases SQL)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	11 minutes 37 secondes	~20 à 25 min	7 jours	~23,7 GB	1 TO	Administrateur
Backup_DFS	Données partagées via le système de fichiers distribué (DFS)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	9 minutes 14 secondes	~15 à 20 min	7 jours	~60 GB	1 TO	Administrateur
Backup_GLPI	Données du logiciel GLPI (base de données + fichiers)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	4 minutes 10 secondes	~10 à 15 min	7 jours	~32 GB	1 TO	Administrateur
Backup_SRVFichier	Serveur de fichiers principal (partages utilisateurs)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	5 minutes 39 secondes	~10 à 20 min	7 jours	~12,5 GB	1 TO	Administrateur
Backup_Test	Machine ou environnement de test (VM ou dossiers)	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	4 minutes 08 secondes	~5 à 10 min	7 jours	~32 GB	1 TO	Administrateur
Backup_Zabbix	Configuration et base de données de supervision Zabbix	Quotidien (1 fois par jour, le soir)	Veeam	NAS (192.168.200.24)	3 minutes 56 secondes	~5 à 10 min	7 jours	~32 GB	1 TO	Administrateur

9. Sauvegardes complémentaires : Dumps de bases de données

En complément des sauvegardes effectuées via Veeam Backup sur le NAS (192.168.200.24), des dumps réguliers des bases de données critiques sont également réalisés. Ces dumps permettent une restauration rapide en cas de corruption, perte ou erreur humaine sur les bases de données.

Bases concernées :

- **GLPI** : dump SQL quotidien, stocké localement et sur le NAS
- **Zabbix** : dump quotidien de la base PostgreSQL ou MySQL

Caractéristiques :

- **Fréquence** : 1 fois par jour (tâche CRON automatisée)
- **Format** : .sql compressé
- **Stockage** : local temporaire + export vers NAS
- **Rétention** : 7 jours

Ces dumps sont une **double couche de sécurité** avec les sauvegardes Veeam, et permettent une restauration très rapide des seules bases, sans restaurer toute la VM.

10. Tests & mise à jour du PRA

- Tests semestriels : restauration d'une VM, perte AD, etc.
- Révisions : à chaque changement d'infra ou mise à jour critique.
- Traçabilité : journal des tests + leçons apprises.

11. Points d'amélioration

11.1 Automatisation complète des tests de restauration

- **Objectif** : S'assurer que les sauvegardes sont réellement exploitables.
- **Amélioration proposée** : Mise en place de tests automatiques hebdomadaires de restauration (sandbox Veeam).
- **Bénéfice** : Fiabilité accrue des sauvegardes, conformité aux exigences de l'ANSSI.

11.2 Documentation centralisée et versionnée

- **Objectif** : Disposer d'une documentation PRA à jour, accessible même en cas de sinistre.
- **Amélioration proposée** : Utilisation de Git + Wiki interne (type Gitea ou GitLab) pour versionner les procédures de reprise.
- **Bénéfice** : Réduction du temps de recherche d'information lors d'un incident.

11.3 Externalisation des sauvegardes critiques

- **Objectif** : Garantir la reprise même en cas de perte totale du site physique.
- **Amélioration proposée** : Réplication des sauvegardes Veeam vers un cloud **sécurisé** ou un site distant.
- **Bénéfice** : Résilience face aux sinistres majeurs (incendie, vol, etc.).

11.4 Formation du personnel à la reprise d'activité

- **Objectif** : Rendre les équipes autonomes en cas d'incident majeur.
- **Amélioration proposée** : Sessions de formation annuelles + mises en situation (tests de PRA).
- **Bénéfice** : Réduction des erreurs humaines et amélioration des temps de réaction.

11.5 Optimisation du RTO/RPO

- **Objectif** : Réduire encore les durées d'interruption (RTO) et de perte de données (RPO).
- **Amélioration proposée** : Utilisation de sauvegardes différentielles/incrémentielles plus fréquentes pour les services critiques (AD, GLPI).
- **Bénéfice** : Amélioration de la continuité de service.

12. Règle de sauvegarde 3–2–1 : État de conformité

La règle 3-2-1 est une stratégie de sauvegarde reconnue visant à garantir la sécurité et la disponibilité des données en cas de panne, de corruption ou de sinistre majeur.

Principe de la règle 3-2-1 :

3 copies des données
2 supports de stockage différents
1 copie hors site (externalisée)

État actuel de l'infrastructure (situation en entreprise)

Élément	Présent ?	Détail technique
3 copies des données	✅	1 originale (VM/serveur) + 1 sauvegarde Veeam + 1 dump SQL
2 types de supports	⚠️ Partiel	Sauvegarde sur NAS uniquement (192.168.200.24) – Pas de support réellement différent (ex. bande, cloud)
1 copie hors site	❌	Aucune externalisation vers un site distant ou cloud

Analyse : ce qui fonctionne

- Les sauvegardes sont quotidiennes et automatisées via Veeam.
- Des dumps de bases de données sont réalisés en complément.
- Les données critiques sont bien dupliquées (VM + sauvegarde + dump).

Points à améliorer pour respecter pleinement la règle 3-2-1

	Solution recommandée	Bénéfice
❌ Support de type différent (bande, disque USB, etc.)	Ajouter un second support physique ou utiliser une solution de sauvegarde en bande ou disque externe, même hebdomadaire	Diversification des risques (ex : ransomware ciblant un NAS)

❌Externalisation des sauvegardes	Réplication vers un cloud (ex : Veeam Cloud Connect, stockage chiffré sur AWS, Azure, OVH) ou NAS déporté (site distant)	Reprise possible même en cas de destruction complète du site

Conclusion

L'infrastructure respecte partiellement la règle 3-2-1.
Elle est robuste localement, mais nécessite :

- un support de sauvegarde secondaire différent du NAS,
- une copie externalisée pour atteindre un niveau de résilience optimal.

13. Le switch

Rôle du switch dans l'infrastructure

- Centralise les connexions physiques entre :
  - Serveurs virtualisés (Proxmox 1, 3)
  - Active Directory + ADSecours
  - Serveurs GLPI, Zabbix, fichiers
  - Postes utilisateurs (Compta, RH, Admin, Élèves)
  - NAS de sauvegarde
  - Routeur
- Fournit l'alimentation PoE si des équipements le nécessitent

14. Risques en cas de panne :

Risque	Impact immédiat
Panne du switch principal	Rupture totale de connectivité interne
Ports défaillants	Isolement de certaines machines ou services
Mauvaise configuration	Problèmes d'accès aux services, au réseau

15. Mesures de prévention / reprise

Mesure	Statut	Détail
Switch de secours prêt à l'emploi	⚠️ Partiel	Pas de redondance physique dédiée aujourd'hui. Un switch non utilisé est disponible
Sauvegarde de la configuration	✅	Export régulier de la config (via interface ou console CLI)
Numérotation claire des ports	✅	Documentation des ports pour relier les services critiques rapidement
Redondance réseau (2e switch en LACP)	❌	Non implémentée – possible évolution future pour haute disponibilité réseau

16. Axe d’amélioration

- Mettre en place un 2e switch en parallèle (redondance active avec LACP ou STP).
- Stocker la configuration du switch sur un partage réseau ou cloud.
- Préparer un script de reconfiguration rapide en cas de remplacement d’urgence.