PLAN DE REPRISE ET CONTINUITÉ D'ACTIVITÉ

Infrastructure Andrea Hardy

Version 2.0 - Février 2026

Table des matières

1. Introduction

1.1 Objectif

Ce document définit les procédures de continuité et de reprise d'activité pour l'infrastructure Andrea Hardy. Il garantit la disponibilité des services critiques et la récupération rapide en cas d'incident majeur.

Périmètre :

- Hyperviseurs Proxmox (Limoges et Poitiers)
- Infrastructure réseau (routeur, switches, VLANs)
- Serveurs applicatifs (WordPress, GLPI)
- Bases de données (MySQL, PostgreSQL)
- Systèmes de supervision et sauvegarde (Veeam, Zabbix)
- Stockage Cloud Azure Files

1.2 Évolutions depuis v1.0

Nouveautés majeures de cette version :

- Ajout du stockage Cloud Azure Files pour sauvegardes externalisées
- Déploiement d'un site secondaire Proxmox à Poitiers (réplication temps réel)
- Architecture multi-sites avec redondance géographique
- RTO et RPO améliorés grâce à la réplication Proxmox
- Conformité renforcée avec la règle 3-2-1-1-0

2. Classification et Priorités

Matrice de criticité des services :

Service	Criticité	RTO	RPO
Bases de données	Critique	1 heure	15 minutes
Infrastructure réseau	Critique	30 minutes	N/A (config versionnée)
WordPress	Haute	2 heures	1 heure
GLPI	Moyenne	4 heures	4 heures

Définitions :

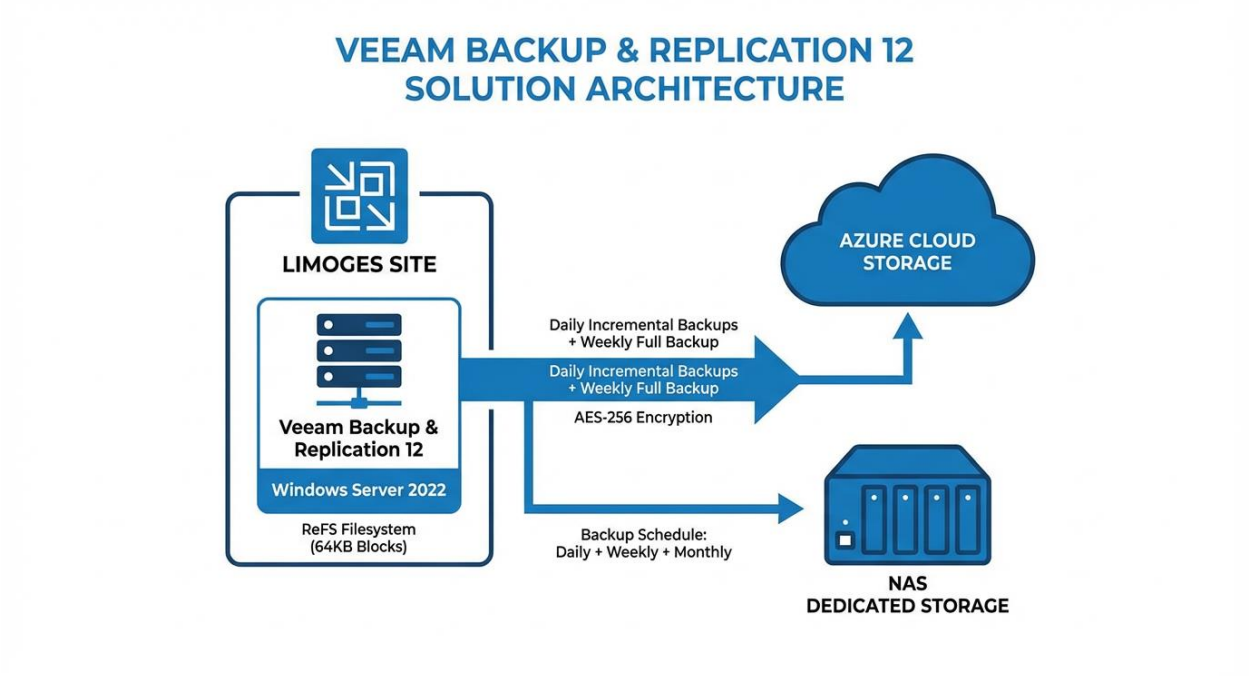
- **RTO (Recovery Time Objective) :** Durée maximale acceptable d'interruption de service
- **RPO (Recovery Point Objective) :** Perte de données maximale acceptable

3. Architecture de Sauvegarde

3.1 Solution Veeam (Site principal)

Veeam Backup & Replication 12 déployé sur Windows Server 2022 pour le site de Limoges :

- Système de fichiers ReFS (blocs 64 Ko) pour performances optimales
- Sauvegardes incrémentielles inversées + complète hebdomadaire
- Chiffrement AES-256 pour sécurité des données
- Sauvegarde locale sur NAS dédié
- Export vers Azure Cloud pour copie hors site

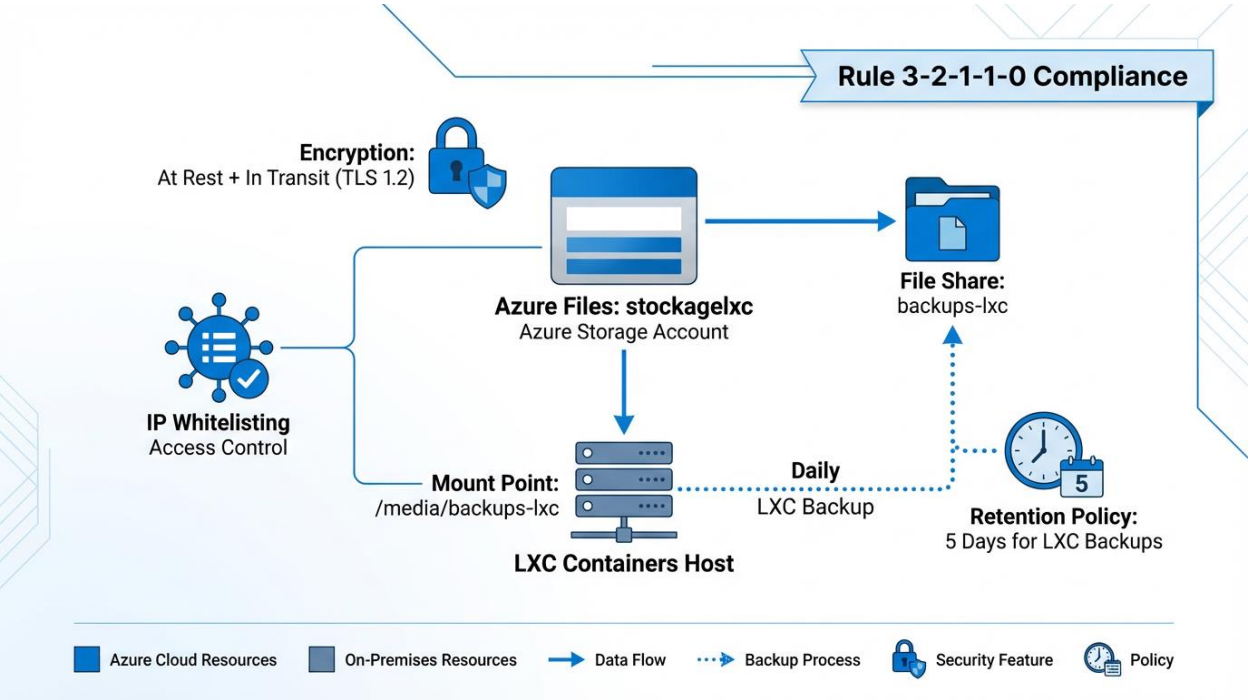


3.2 Sauvegarde Cloud Azure

Stockage Azure Files configuré pour externalisation des sauvegardes :

- Compte de stockage : stockagelxc
- Partage de fichiers : backups-lxc
- Montage CIFS/SMB 3.0 sur Proxmox Limoges
- Sauvegardes containers LXC quotidiennes vers Azure
- Chiffrement au repos et en transit (TLS 1.2)
- Accès restreint par IP (whitelisting)
- Rétention : 5 jours pour sauvegardes containers
- Règle 3-2-1-1-0 respectée : 3 copies, 2 supports, 1 hors site, 1 immuable, 0 erreur

Point de montage : `/media/backups-lxc`



3.3 Réplication Proxmox Limoges → Poitiers

Site de Disaster Recovery avec réplication synchrone des VMs critiques :

- Proxmox VE 8.x déployé sur site secondaire (Poitiers)
- Réplication bidirectionnelle Proxmox pour VMs critiques
- Synchronisation toutes les 15 minutes pour BDD et services critiques
- Synchronisation toutes les heures pour services haute priorité
- Infrastructure réseau identique (VLANs, firewall)
- Capacité de bascule rapide (RTO < 1h pour services critiques)
- Tests de bascule mensuels automatisés

Note importante : Le site de Poitiers peut fonctionner en mode autonome pendant la reconstruction du site principal. Les données sont synchronisées dans les deux sens.

3.4 Politique GFS

Stratégie Grandfather-Father-Son (GFS) pour Veeam :

Type	Fréquence	Rétention	Horaire
Quotidien (Son)	Chaque nuit	7 jours	2h00
Hebdomadaire (Father)	Dimanche	4 semaines	23h00
Mensuel (Grandfather)	1er du mois	12 mois	1h00

3.5 Tests de Restauration

Programme de tests réguliers obligatoires :

- **Mensuels :** Restauration VM aléatoire depuis Veeam + Test restauration container depuis Azure
- **Trimestriels :** Restauration base de données complète + Tests de réplication Proxmox
- **Semestriels :** Simulation bascule complète site Limoges → Poitiers
- **Annuels :** Exercice PRA complet avec cellule de crise + Audit externe

4. Plan de Reprise d'Activité (PRA)

4.1 Déclenchement

Le PRA s'active dans les cas suivants :

- Sinistre physique majeur (incendie, inondation, coupure électrique prolongée)
- Cyberattaque massive (ransomware, compromission totale)
- Panne matérielle critique (hyperviseur, stockage, réseau)
- Corruption de données massive
- Indisponibilité site principal > 2 heures

4.2 Procédure en 7 Étapes

Étape 1 : Évaluation (30 min)

1. Convocation cellule de crise (RSSI + Admin Senior + Direction)

2. Identification de la cause racine et étendue du sinistre

3. Inventaire des systèmes affectés et impact métier

4. Décision : restauration locale vs bascule Poitiers

5. Notification direction et parties prenantes

Étape 2 : Isolation (15 min)

5. Déconnexion des systèmes compromis du réseau

6. Révocation des certificats SSH et clés API

7. Isolation du serveur Veeam (si compromis)

8. Désactivation comptes utilisateurs si nécessaire

9. Conservation des logs pour investigation forensique

Étape 3 : Préparation (30 min)

10. Vérification de l'état de l'hyperviseur Proxmox cible

11. Nettoyage des VMs corrompues (si restauration locale)

12. Restauration de la configuration réseau depuis Git

13. Validation de la disponibilité des sauvegardes (Veeam/Azure)

14. Préparation des ressources (stockage, CPU, RAM)

Étape 4 : Restauration Services Critiques (1-4h)

Ordre de priorité et délais cibles :

Priorité	Service	Délai cible
1	Infrastructure réseau (VLANs, firewall)	30 min
2	Bastion Teleport (accès sécurisé)	1h
3	Bases de données (MySQL, PostgreSQL)	1h
4	WordPress / GLPI	2h
5	Zabbix (supervision)	4h

Note : En cas de bascule sur Poitiers, les VMs répliquées peuvent être démarrées immédiatement (RTO < 1h). Sinon, restauration depuis Veeam ou Azure.

Étape 5 : Vérification (1h)

- Tests de démarrage de toutes les VMs restaurées
- Tests de connectivité réseau (interne et externe)
- Vérification de l'intégrité des bases de données
- Tests fonctionnels des applications web
- Vérification des sauvegardes post-restauration

Étape 6 : Remise en Production (30 min)

- Validation finale par le RSSI
- Communication aux utilisateurs (email + portail)
- Réactivation des accès utilisateurs
- Mise en place de la surveillance renforcée (24h)
- Documentation de l'incident dans GLPI

Étape 7 : Analyse Post-Incident (2-4h)

À réaliser dans les 48h suivant la résolution :

- Chronologie détaillée des événements
- Analyse de la cause racine (méthode des 5 Pourquoi)
- Comparaison RTO/RPO théoriques vs réels
- Identification des points d'amélioration
- Rapport de synthèse pour la direction
- Mise à jour du PRA/PCA si nécessaire

4.3 Scénarios de Reprise

Scénario A : Panne locale réversible

Panne matérielle ou logicielle sans compromission majeure (ex: crash disque, bug applicatif).

- Restauration sur site depuis Veeam (sauvegardes locales)
- Si containers LXC : restauration depuis Azure Cloud
- RTO visé : 2-4h
- Pas de bascule Poitiers nécessaire

Scénario B : Cyberattaque (ransomware)

Compromission massive avec chiffrement des données.

- Isolation immédiate de tous les systèmes
- Vérification intégrité des sauvegardes Veeam/Azure
- Restauration depuis points de sauvegarde antérieurs à l'attaque
- Réinitialisation complète des mots de passe et certificats
- RTO visé : 4-8h
- Possibilité de bascule Poitiers si réplication non compromise

Scénario C : Sinistre majeur site Limoges

Destruction physique ou indisponibilité prolongée du datacenter principal (incendie, inondation, coupure électrique > 6h).

- Activation immédiate du site de Poitiers
- Démarrage des VMs répliquées (services critiques opérationnels en < 1h)
- Restauration services secondaires depuis Azure Cloud
- Redirection DNS vers nouvelle infrastructure
- RTO visé : 1-2h pour services critiques, 4-6h pour services complets
- Fonctionnement en mode dégradé jusqu'à reconstruction site principal

5. Plan de Continuité d'Activité (PCA)

Le PCA maintient un niveau minimum de service en mode dégradé pendant la crise, permettant aux utilisateurs de continuer leurs activités essentielles.

5.1 Modes Dégradés

Service	Priorité	Mode Dégradé
Bases de données	Critique	Bascule réplica lecture seule sur Poitiers
WordPress	Haute	Page de maintenance avec contacts et infos
GLPI	Moyenne	Accès lecture seule, tickets par email temporairement

5.2 Communication de Crise

Protocole de communication avec les utilisateurs :

Moment	Action
T+0 (immédiat)	Email à tous les utilisateurs : incident déclaré, services affectés
T+30 min	Mise à jour sur l'avancement de la résolution
Toutes les heures	Point de situation (% progression, nouveaux délais)
Résolution	Email de clôture avec retour d'expérience utilisateurs

Canaux de communication : Email principal + SMS pour incidents critiques + Page statut sur site web

6. Annexes

6.1 Contacts d'Urgence

Rôle	Nom	Téléphone	Email
RSSI	Andrea Hardy	+33 X XX XX XX XX	rssi@andrea-hardy.fr
Admin Senior	Andrea Hardy	+33 X XX XX XX XX	admin@andrea-hardy.fr
Direction	Andrea Hardy	+33 X XX XX XX XX	direction@andrea-hardy.fr

6.2 Inventaire des Infrastructures

Site Principal - Limoges

- Hyperviseur : Proxmox VE 8.x
- Serveur Veeam : Windows Server 2022
- Stockage local : NAS Synology
- Stockage Cloud : Azure Files (stockagelxc)
- VMs critiques : BDD, WordPress, GLPI, Zabbix, Teleport

Site Secondaire - Poitiers

- Hyperviseur : Proxmox VE 8.x (réplica)
- Réplication : Synchronisation 15 min (BDD) / 1h (autres)
- Capacité : Identique au site principal
- Réseau : Configuration identique (VLANs, firewall)

_____

RSSI Andrea Hardy
Février 2026