

Politique de Sauvegarde et Stratégie de Cyber-Résilience

Politique de Sauvegarde et Stratégie de Cyber-Résilience

Projet: Proposition d'Évolution et de Sécurisation du Système d'Information XANADU

CLIENT :	XANADU S.A.
THÉMATIQUE :	Continuité d'Activité et Reprise après Sinistre (PCA/PRA)
OBJECTIFS :	Garantie d'un RTO <= 4heures (Critique) et Implémentation du Modèle 3-2-1-1-0

Équipe Projet CESITECH

- ❖ Adonis ROUSSE
- ❖ Thibaud DOURLENS
- ❖ Samuel BANKOUEZI
- ❖ Rémi ROULLET
- ❖ Fernando FERREIRA PIAIA

Politique de Sauvegarde et Stratégie de Cyber-Résilience

TABLE DES MATIÈRES

1. Politique de Sauvegarde et Plan de Reprise	3
1.1 Analyse de l'Existant et Vulnérabilités	3
1.2. Définition des Métriques RTO/RPO Cibles	3
2. Architecture Cible de Cyber-Résilience	4
2.1 Mise en Œuvre du Modèle 3-2-1-1-0	4
2.2 Sécurisation et Contrôle d'Accès (RBAC)	4
3. Stratégie de Protection Détaillée par Workload	5
3.1 Protection des Systèmes Critiques (Tier 1 : ERP et Services Fichiers)	5
3.2 Protection des Postes Clients et Télétravail	5
4. Topologie de Sauvegarde Logique et Flux	6
5. Gouvernance et Traçabilité	7
5. Politique de Rétention	7
5. Traçabilité, Auditabilité et Disponibilité	7
6. Glossaire	8-9

Politique de Sauvegarde et Stratégie de Cyber-Résilience

1. Politique de Sauvegarde et Plan de Reprise

1.1. Analyse de l'Existant et Vulnérabilités

Le système de sauvegarde existant de XANADU repose sur un NAS avec des partages ouverts et une copie sur disque externe alterné, connecté au Contrôleur de Domaine (DC). Cette architecture est non seulement chronophage, mais elle est surtout extrêmement vulnérable aux rançongiciels, qui peuvent facilement corrompre les sauvegardes si le NAS est accessible depuis le réseau de production. Le plan actuel ne permet en aucun cas de garantir un retour à la normale dans les délais de 4 heures requis par la direction. La nouvelle politique doit donc s'orienter vers la centralisation des données, l'isolation (air-gap), l'immutabilité et l'automatisation pour garantir la stabilité, la fiabilité et la sécurité.

1.2. Définition des Métriques RTO/RPO Cibles

La stratégie de sauvegarde est directement dictée par les objectifs de reprise fixés par la Direction (RTO maximal de 4 heures pour les services critiques). Les données sont classées en trois Tiers de criticité :

Catégorie de Données (BIA)	RTO Cible (Reprise)	RPO Cible (Perte Max.)	Justification Technique
Critiques (Tier 1) : ERP (DB/VM), Dossiers Juridique, Direction, Sinistres.	<= 4 heures	<= 15 minutes	Nécessite l'Instant VM Recovery et le Point-in-Time Recovery (PITR) pour la base de données.
Importantes (Tier 2) : Fichiers Partagés (Client, Commerce), Emails O365.	<= 8 heures	<= 4 heures	Sauvegardes et réplications plus fréquentes que quotidiennes.
Moins Critiques (Tier 3) : Dossiers personnels centralisés.	<= 24 heures	<= 24 heures	Sauvegarde centralisée quotidienne.

Politique de Sauvegarde et Stratégie de Cyber-Résilience

2. Architecture Cible de Cyber-Résilience

Pour garantir la continuité des activités face à la menace des rançongiciels , l'architecture de sauvegarde doit être blindée. Nous adoptons le modèle de référence 3-2-1-1-0 (évolution de la règle 3-2-1).

2.1. Mise en Œuvre du Modèle 3-2-1-1-0

Le plan de sauvegarde repose sur une architecture sécurisée :

- 3 Copies de Données : L'original en production, une copie locale et une copie hors site.
- 2 Supports Différents : Production (Disque SAN/VM) et Stockage Dédié (Disque/Cloud). Un mélange de supports disques et d'un service cloud est recommandé.
- 1 Copie Hors Site : Stockée sur une plateforme Cloud Object Storage pour une protection géographique.
- 1 Copie Immutable (WORM) : La copie Cloud doit être configurée en mode Write Once, Read Many (WORM) pour empêcher sa modification ou sa suppression par un attaquant, même avec des droits d'administrateur. La protection immuable est essentielle pour la défense contre les ransomwares.
- 0 Erreur de Restauration : Mise en place de tests de restauration réguliers et automatisés (SureBackup ou équivalent) pour valider l'atteinte des RTO cibles et garantir que la restauration se fera sans erreur.

2.2. Sécurisation et Contrôle d'Accès (RBAC)

Pour isoler le référentiel de sauvegarde de l'environnement de production (et donc des rançongiciels), une stricte séparation des privilèges (RBAC) est appliquée:

- Comptes Techniques Distingués : Des comptes techniques distincts sont créés entre les opérations d'écriture unique (sauvegarde) et les opérations de lecture/gestion (restauration/politique de rétention). Le compte utilisé par l'agent de sauvegarde ne doit pas avoir le droit de supprimer les copies.
- Protection de l'Administration : L'accès à la console d'administration de la sauvegarde doit être sécurisé par l'Authentification Multifactorielle (MFA).

Politique de Sauvegarde et Stratégie de Cyber-Résilience

3. Stratégie de Protection Détailée par Workload

3.1. Protection des Systèmes Critiques (Tier 1 : ERP et Services Fichiers)

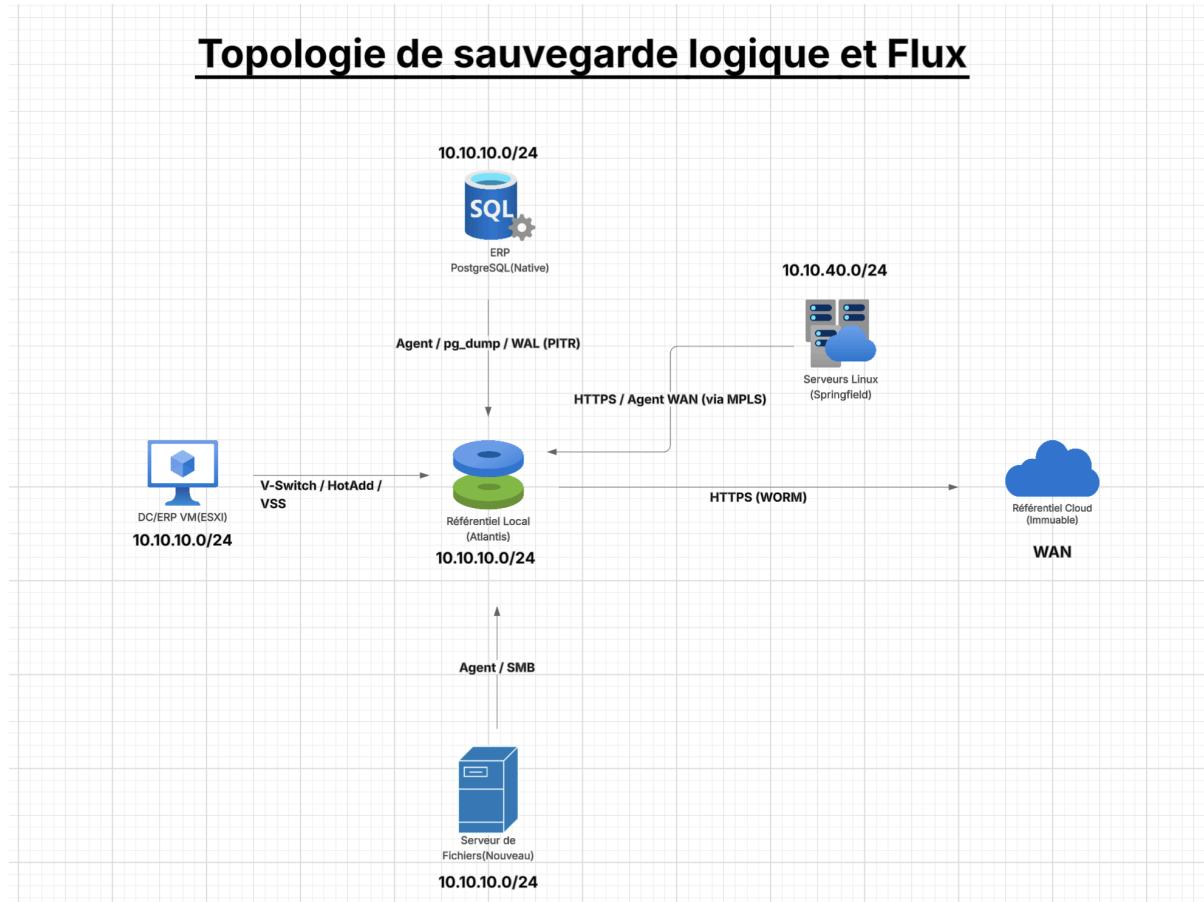
Workload	Méthode de Protection Cible	Justification RTO/RPO
ERP (VM ESXi) - Images VM	Sauvegarde sans agent au niveau de l'hyperviseur (VMware).	Utilisation de l'Instant VM Recovery pour restaurer l'accès au service en quelques minutes (RTO <= le 4h)
ERP (Base PostgreSQL) - Transactionne	Archivage Continu (PITR) des journaux de transactions (WAL).	La sauvegarde de l'image VM seule n'est pas suffisante pour garantir la cohérence transactionnelle de la base de données. ¹⁷ Le PITR garantit un RPO <= 15 min.
Serveur de Fichiers (Nouveau) (Partages & dossiers redirigés)	Sauvegarde d'image VM et granulaire des fichiers.	Consolide les données critiques et importantes (800 Go) sur une seule cible protégée par le modèle 3-2-1-1-0.

3.2. Protection des Postes Clients et Télétravail

- Centralisation des Données Utilisateurs : Le plan impose de mettre fin à la vulnérabilité des données locales et des sauvegardes USB. Les dossiers personnels (5 Go chacun) seront centralisés sur le nouveau Serveur de Fichiers d'Atlantis via la Redirection de Dossiers (GPO). Cette méthode sécurise les données des 60 utilisateurs itinérants et en télétravail.
- Sauvegarde Office 365 : Les systèmes natifs de rétention de Microsoft 365 ne constituent pas une sauvegarde complète contre les suppressions accidentelles ou malveillantes. Une solution de sauvegarde tierce (ex: Veeam Backup for Microsoft 365 Community Edition pour les 10 premiers utilisateurs) est requise pour protéger Exchange Online (Emails) et OneDrive

Politique de Sauvegarde et Stratégie de Cyber-Résilience

4. Topologie de Sauvegarde Logique et Flux



Politique de Sauvegarde et Stratégie de Cyber-Résilience

5. Gouvernance et Traçabilité

5.1. Politique de Rétention

Pour garantir l'intégrité et la disponibilité des données, la traçabilité des opérations est fondamentale :

- Rétention Opérationnelle (Atlantis) : 14 jours glissants (quotidien) pour toutes les données, afin d'assurer une restauration rapide et locale (RTO).
- Rétention de Cyber-Résilience (Cloud Immuable) : 90 jours (mensuel/trimestriel) pour les images VM critiques et la DB ERP, permettant de récupérer après la découverte tardive d'une menace dormante.

5.2 Traçabilité, Auditabilité et Disponibilité

Pour garantir l'intégrité et la disponibilité des données, la traçabilité des opérations est fondamentale :

- Audit Trail : Le système de sauvegarde doit enregistrer et conserver les logs des événements critiques : succès/échecs des sauvegardes, modifications de politiques, tentatives d'accès non autorisé, et surtout, les opérations de restauration de données critiques.
- Test du PRA : L'efficacité de la politique est validée par la simulation. Des tests de reprise après sinistre doivent être planifiés et menés au moins trimestriellement pour mesurer concrètement le RTO et valider que la restauration à partir de la copie immuable fonctionne (principe du "Zéro Erreur").

Politique de Sauvegarde et Stratégie de Cyber-Résilience

6. Glossaire

Mots techniques	Définition et Contexte dans le Projet
RTO (Recovery Time Objective)	Objectif de Temps de Reprise. Représente la durée maximale tolérée pour rétablir une fonction métier ou un système après un incident (panne, cyberattaque). Pour XANADU, le RTO critique est fixé à 4 heures.
RPO (Recovery Point Objective)	Objectif de Point de Reprise. Représente la quantité maximale de données (mesurée en temps) que l'entreprise peut accepter de perdre en cas de sinistre. Ce seuil dicte la fréquence des sauvegardes. Pour l'ERP, l'objectif est très serré : <= 15 minutes
BIA (Business Impact Analysis)	Analyse d'Impact Métier. Processus d'évaluation qui classe les systèmes et les données selon leur criticité (Tier 1, 2, 3) pour déterminer les exigences RTO et RPO
3-2-1-1-0	Règle de Cyber-Résilience. Évolution du standard 3-2-1, essentielle pour la lutte anti-rançongiciel. Elle exige : 3 copies de données, sur 2 supports différents, 1 copie hors site, 1 copie immuable ou air-gapped, et 0 erreur de restauration (test de validité).
Immutabilité / WORM	Write Once, Read Many. Caractéristique d'un référentiel de stockage où les données, une fois écrites, ne peuvent être ni modifiées ni supprimées pendant une période définie. C'est la ligne de défense principale contre les rançongiciels qui ciblent les sauvegardes.
Air-Gap	Isolation Physique ou Logique. Représente la séparation complète d'une copie de sauvegarde du réseau de production. Une solution hors ligne est considérée comme plus robuste qu'une solution WORM en ligne pour contrer les menaces persistantes.
RBAC (Role-Based Access Control)	Contrôle d'Accès Basé sur les Rôles. Stratégie de sécurité cruciale pour la sauvegarde, visant à séparer les priviléges. Par exemple, le compte technique qui écrit la sauvegarde ne doit pas avoir le droit de la supprimer.
	Write-Ahead Logging. Les journaux de

Politique de Sauvegarde et Stratégie de Cyber-Résilience

PostgreSQL WAL	transactions utilisés par la base de données ERP de XANADU. L'archivage continu de ces logs permet d'atteindre le RPO très faible <= 15 min requis par l'exigence PITR .
Instant VM Recovery	Restauration Instantanée de Machine Virtuelle. Méthode qui permet de redémarrer une machine virtuelle (VM) critique, comme celles de l'ERP ou du DC, directement depuis le fichier de sauvegarde. Cette technique est nécessaire pour atteindre l'objectif RTO de 4 heures .
GPO / Redirection de Dossiers	Stratégie de Groupe. Fonctionnalité de l'Active Directory utilisée pour appliquer des configurations centralisées. La Redirection de Dossiers est utilisée pour forcer les dossiers locaux des utilisateurs (Documents, Bureau) à être stockés sur un serveur de fichiers centralisé , garantissant leur sauvegarde (Tier 3).
PRA	Plan de Reprise d'Activité : Document stratégique qui décrit les procédures à suivre pour redémarrer les systèmes informatiques et l'activité après un sinistre majeur
PCA	Plan de Continuité d'Activité: Ensemble de mesures organisationnelles et techniques permettant de maintenir les activités essentielles en cas de crise ou de perturbation.