Subdivision Administrative des Iles du Vent
ARRIVÉE LE
- 5 NOV. 2026
N° ..... / IDV

Commune de FAA'A

SEANCE DU CONSEIL MUNICIPAL DU 27 OCTOBRE 2026

DELIBERATION N° 71/2026

Approuvant le dossier technique et le plan de financement prévisionnel relatifs au renouvellement de l'infrastructure informatique communale

Date de convocation :
20 octobre 2026

Date de séance :
27 octobre 2026

Date de publication de la liste des délibérations :
28 octobre 2026

NOMBRE DE CONSEILLERS

EN EXERCICE :	35
PRESENTS :	23
PROCURATIONS : ...	08
VOTANTS :	31
POUR :	31
CONTRE :	00
ABSTENTION :	00

Le mardi 27 octobre 2026 à 9h, le Conseil Municipal, légalement convoqué, s'est réuni dans la salle du Conseil Municipal de la mairie en séance publique sous la présidence de Monsieur Tetuahau TEMARU, Premier Adjoint, et ce conformément aux articles L 2121-10 et L 2121-14 du Code Général des Collectivités Territoriales applicable aux communes de Polynésie Française.

Étaient présents :

Nom – Prénom	Prés.	Abs.	Procuration
TEMARU Oscar		X	
TEMARU Tetuahau	X		
LAURENT Victoire	X		
SANFORD Vetea			E. TOKORAGI
VANAA Emma	X		
TERIITEHAU Roberto	X		
TEAUNA ép POIA Clarisse			R. RICHMOND
PURENI Tunui	X		
TOKORAGI Ella	X		
BERNARDINO Joël		X	
TEMARU ép LE GALL Tevai	X		
TEFAATAU-FIRUU ép MATI Juliana	X		
AUBRY Joseph	X		
TEURU ép MAI Bélinda	X		
NIVA Pauline			O. TOKORAGI
TAUMIHAU ép RICHMOND Roti	X		
SALOMON Ariena	X		
MAI Gérard	X		
MAI CLARK ép PATU Andrée			T. GRAND-PITTMAN
TOKORAGI Ole	X		
TEUIRA Jean-Paul	X		
CROLAS Tamaehu	X		
TEANOMAUI ép HIKUTINI Lucie	X		
MAMATUI ép GRAND-PITTMAN Tekakwitha	X		
RICHMOND Maruia		X	
ARIIOTIMA Matuanui			T. PURENI
LE CAILL Turatahi	X		
MERETA Nohoarii			R. TERIITEHAU
MAI Georges		X	
OPETA Temana			T. TEMARU
SIAOU CHIN Pascal	X		
TUPANA Moihara			P. SIAOU CHIN
AITAMAI Mara	X		
CADOUSTEAU Myriam	X		
TOKORAGI Wilson	X		

COMMUNE DE FAA'A ★ TAHITI - Polynésie Française ★ République Française

Les conseillers présents représentant la majorité des membres en exercice, qui sont au nombre de 23, il a été procédé conformément à l'article L 2121-15 du Code Général des Collectivités Territoriales applicable aux communes de Polynésie Française, à la nomination d'un secrétaire de séance pris dans le sein du Conseil Municipal, Victoire LAURENT ayant obtenu la majorité des suffrages a été désignée pour remplir cette fonction qu'elle a acceptée.

Madame Roti RICHMOND a ensuite exposé à l'assemblée que :

L'infrastructure informatique de la mairie de Faa'a constitue aujourd'hui un levier essentiel au bon fonctionnement des services municipaux. Elle permet l'exploitation des applications métier, la gestion des données communales, les échanges administratifs ainsi que la continuité des services rendus à la population.
Toutefois, les équipements actuellement en service ont été déployés il y a près de neuf ans et présentent désormais un niveau d'obsolescence préoccupant. Cette ancienneté ne permet plus de garantir durablement la performance, la disponibilité et la sécurité du système d'information communal.
Par ailleurs, le taux d'utilisation de l'infrastructure atteint environ 87 % de sa capacité, limitant les possibilités d'évolution du système d'information et l'intégration de nouveaux outils numériques nécessaires à la modernisation des services communaux.
En cas d'incident majeur, la commune pourrait faire face à une interruption prolongée de ses services numériques, compromettant le fonctionnement des services municipaux, la qualité de l'accueil du public et la continuité du service public.
Le renouvellement de cette infrastructure répond également à un enjeu majeur de cybersécurité. Le renforcement des dispositifs de sauvegarde, de sécurisation et de reprise d'activité permettra de mieux protéger les données communales et de réduire l'exposition aux menaces informatiques et aux cyberattaques.
Afin de garantir la pérennité de son système d'information et d'accompagner sa transformation numérique, la commune souhaite engager un programme de renouvellement de son infrastructure informatique comprenant notamment le renouvellement des serveurs, des solutions de stockage, des équipements de sauvegarde et des dispositifs de sécurité associés.
Sur la base d'une première évaluation technique, le coût prévisionnel de cette opération est estimé à environ 60 millions de F CFP.
Il est ainsi proposé au conseil municipal d'approuver le dossier technique afin d'assurer la continuité des missions de service public, la protection des données communales et le développement futur des services numériques de la collectivité.
Tel est l'objet du projet de délibération ci-après, conformément à l'avis favorable émis par la commission Communication et Système d'information intégré le mercredi 23 septembre 2026.

Le Conseil Municipal, après avoir entendu l'exposé de Madame Roti RICHMOND :

Vu la loi organique n°2004-192 du 27 février 2004 modifiée portant statut d'autonomie de la Polynésie française et la loi n°2004-193 du 27 février 2004 complétant le statut d'autonomie de la Polynésie française ;

Vu la loi n°71-1028 du 24 décembre 1971 modifiée relative à la création et à l'organisation des communes dans le territoire de la Polynésie française promulguée par arrêté n°31/AA du 6 janvier 1972 ;

Vu l'ordonnance n°2007-1434 du 5 octobre 2007 modifiée portant extension des première, deuxième et cinquième parties du Code général des collectivités territoriales aux communes de la Polynésie française, à leurs groupements et à leurs établissements publics ;

Vu le décret n°2008-1020 du 22 septembre 2008 portant extension des première, deuxième et cinquième parties du Code général des collectivités territoriales aux communes de la Polynésie française, à leurs groupements et à leurs établissements publics ;

Vu l'arrêté n°173/AA du 30 janvier 1965 instituant deux communes ayant respectivement pour chef-lieu PIRAE et FAA'A et étendant à ces communes toutes les dispositions applicables à celles de PAPEETE et d'UTUROA conformément à l'article 58 du décret n°57-812 du 22 juillet 1957 ;

Vu la délibération n°05/2026 du 12 février 2026 adoptant le budget principal de la commune de Faa'a au titre de l'exercice 2026 ;

Vu le dossier technique relatif à l'étude portant sur le renouvellement de l'infrastructure informatique communale ;

Vu le rapport de présentation et l'avis de la commission communication et système d'information intégré du 23 septembre 2026 ;

Dans sa séance du 27 octobre 2026 ;

ADOPTE A L'UNANIMITE DES SUFFRAGES EXPRIMES

Article 1er : Sont approuvés le dossier technique et le plan de financement prévisionnel de l'opération suivante :

Nature de l'opération	Montant de l'opération (en FCFP TTC) FINANCEMENT FONDS PROPRES COMMUNE
Renouvellement de l'infrastructure informatique communale	60 000 000

Article 2 : La dépense y afférente sera prise en charge par le budget communal, exercice 2026, section d'investissement.

Article 3 : La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal administratif dans un délai de 2 mois à compter de sa publication et de sa transmission au représentant de l'Etat, et est prise pour servir et valoir ce que de droit.

Fait et délibéré à FAA'A, le 27 octobre 2026.

La Secrétaire de Séance,

Victoire LAURENT

COMMUNE DE FAA'A
TAHITI - Polynésie Française
République Française

Le Président de Séance,

Tetuahau TEMARU

Le Maire de la Commune de Faa'a atteste, sous sa responsabilité, que le présent acte a été publié le 05 NOV. 2026
et transmis au Haut-commissaire de la République en Polynésie française le 05 NOV. 2026

Commune de Faa'a
Direction Générale des Services
PCI / Service Informatique
Tél : 40 800 988 – Mail : informatique@mairiefaaa.pf

Une nouvelle infrastructure informatique de la Mairie de Faa'a

I

1 Introduction 2
2 Le constat 2
2.1 L'obsolescence de l'infrastructure actuelle 2
2.2 Les sauvegardes 3
3 Le risque d'arrêt matériel et de perte d'information 3
3.1 L'arrêt matériel 3
3.2 La perte d'information 4
4 L'acquisition de la nouvelle infrastructure 4
4.1 Le contexte international des achats en informatique 4
4.2 La description technique de la future infrastructure 5
4.3 L'achat de la future infrastructure 6
5 Les autres actions de modernisation 7
6 Conclusion 7
Annexe 1 : Apparition d'alerte rouge dans les traces système 9

Commune de Faa'a
Direction Générale des Services
PCI / Service Informatique
Tél : 40 800 988 – Mail : informatique@mairiefaaa.pf

1 Introduction

Le présent document expose l'urgente nécessité de remplacer l'infrastructure informatique de la Mairie de Faa'a .En effet, le Système d'Information (SI) de la Mairie de Faa'a fait face à une situation d'urgence absolue, identifiée par le Responsable de la Sécurité des Systèmes d'Information (RSSI) (courrier joint en Annexe I) et confirmée par des experts externes.

Plusieurs risques majeurs menacent aujourd'hui la continuité des services municipaux, avec des conséquences potentielles graves : interruption prolongée des activités informatiques, perte irréversible de données critiques, et incapacité à répondre aux exigences de sécurité et de conformité.

Cette crise résulte de deux défis interdépendants :

- Une infrastructure obsolète : les serveurs physiques, âgés de 9 ans (avec fin de support en février 2021), présentent un risque élevé de panne irréversible, aggravé par une surcapacité opérationnelle (87 % de charge, bien au-delà du seuil tolérable de 80 %).
- L'absence de sauvegardes fiables : sans mécanisme de restauration validé, toute défaillance matérielle ou cyberattaque (ex. chiffrement des données) pourrait entraîner une perte définitive des données essentielles (RH, finances, etc.).

Face à ces menaces, des actions immédiates s'imposent pour sécuriser le cœur informatique, garantir la résilience du SI, et préparer sa modernisation à moyen terme.

2 Le constat

2.1 L'obsolescence de l'infrastructure actuelle

Le machines (les serveurs physiques) constituant le SI du cœur de la mairie de Faa'a sont vieilles de 9 ans. La fin du support de base sur le sujet est donnée pour le 27 février 2021.

En mai 2026, une alarme critique a été détectée par l'outil de supervision de l'infrastructure actuelle. Les mesures prises à la suite de cet incident sont consignées dans la fiche jointe en Annexe 2, à la suite du présent document.

A la suite de la prise en compte de l'alarme critique, un audit rapide a été lancé par la société INFONECS. Le rapport « Annexe 3 », est donné en pièce jointe. Leurs experts sur le sujet nous ont également averti des conséquences à ne pas renouveler l'infrastructure. Tous nous disent qu'il est urgent de renouveler cette infrastructure. Nous verrons les conséquences pratiques de ne pas renouveler l'infrastructure plus bas dans le document. L'obsolescence des logiciels et des équipements entraîne plusieurs risques.

Lors d'un redémarrage, les logiciels peuvent exiger des mises à jour de sécurité régulières, lesquelles nécessitent parfois le remplacement des machines. Le redémarrage des serveurs pourrait alors être bloqué dans l'attente de l'acquisition des mises à jour requises.

La nouvelle infrastructure fournira des équipements modernes ainsi que des logiciels récents pour les administrer.

Selon les experts locaux, l'ancienneté des équipements impose de mener toute intervention ou remise en service avec une extrême prudence, impliquant des compétences spécifiques et des certifications régulièrement renouvelées.

2.2 La surcapacité des serveurs

En mai 2026 également, nous avons constaté que la capacité globale des serveurs était utilisée à 91 %. Des opérations réalisées en dehors des heures de service ont permis de ramener ce taux à 87 %. Ce niveau reste toutefois supérieur au seuil maximal recommandé de 80 %.

Nous allons devoir appliquer des mesures d'optimisation drastiques (archivage de données froides, suspension éventuelle de services non critiques) pour tenter de soulager les serveurs actuels d'ici la livraison du nouveau matériel.

À terme, l'arrivée **de la nouvelle infrastructure informatique** viendra définitivement régler ce problème. Elle sera dimensionnée pour supporter largement l'activité de la mairie sans jamais atteindre la zone rouge.

2.3 Les sauvegardes

Nous ne pouvons pas effectuer de manipulations poussées sur les serveurs actuels, par conséquent, avec le risque de ne pas pouvoir restaurer les données en cas d'arrêt.

Pire encore, à ce jour, nous n'avons pas la certitude que les sauvegardes existantes de nos machines virtuelles puissent être restaurées correctement en cas de besoin.

Enfin, il n'y a pas de sauvegarde "hors ligne" qui nous aurait permis de ne pas être touché par les rançongiciels des pirates.

Le stockage de la nouvelle infrastructure nous permettra de sécuriser les sauvegardes de nos serveurs, les sauvegardes normales ainsi que les sauvegardes hors ligne.

3 Le risque d'arrêt matériel et de perte d'information

3.1 L'arrêt matériel

En cas d'arrêt physique des matériels, nous ne sommes pas certains de pouvoir les relancer.

Si nous ne pouvons relancer le SI, nous serons obligés d'acheter la nouvelle infrastructure informatique en urgence.

Dans le pire de cas, la mairie se retrouvera sans informatique pendant 3 à 4 mois le temps de les commander et de les installer.

Enfin, les achats en urgence (par avion) de matériels informatiques sont énormément plus chers que les achats normaux (par bateau).

3.2 La perte d'information

En cas de de perte d'information due à un crash partiel du SI, nous ne sommes pas sûrs de la fiabilité des sauvegardes pour pouvoir retrouver l'ensemble des informations manquantes du SI.

Cela pourrait être critique surtout pour certains métiers comme les RHs, les finances, ou autres métiers critiques.

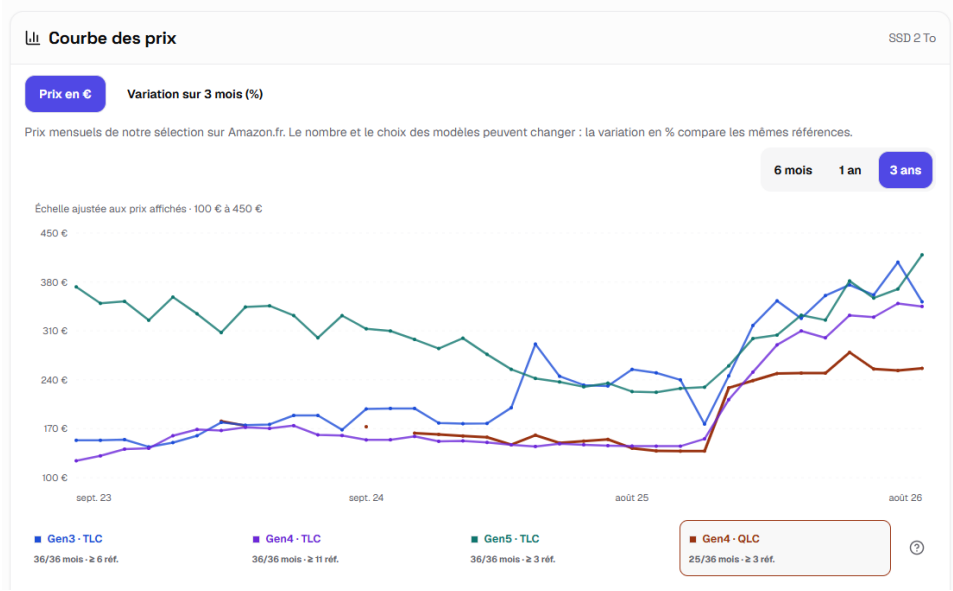
En cas de chiffrement des données (sauvegarde comprise) par les pirates, nous serions à leur merci sans possibilité de recouvrement des données autres qu'en leur payant le montant de la rançon demandée.

Outre l'aspect financier, le point le plus important est l'image négative que cela donnerait.

4 L'acquisition de la nouvelle infrastructure

4.1 Le contexte international des achats en informatique

Il est essentiel d'engager l'acquisition du matériel sans délai : la forte demande, liée à l'essor de l'intelligence artificielle, exerce déjà une pression croissante sur le prix des mémoires flash, et tout report pourrait alourdir sensiblement le coût de l'investissement.



Depuis novembre 2025, nous pouvons constater sur le graphique précédent, l'évolution du prix moyen des disques de 2 téraoctets : le tarif a quasiment doublé.

Et par ricochet, cela est vrai pour l'ensemble des matériels informatiques.

4.2 La description technique de la future infrastructure

Le choix technologique retenu pour remplacer notre matériel vieillissant repose sur un principe simple : **la continuité absolue du service public**. L'objectif n'est pas seulement de moderniser, mais de construire une infrastructure robuste, capable de résister aux pannes et aux cyberattaques, tout en simplifiant le travail de notre équipe informatique en sous-effectif.

Le nouveau système repose sur cinq piliers stratégiques :

1. Le cœur du système : 3 serveurs travaillant "en équipe" Au lieu de dépendre d'une machine isolée qui paralyserait la mairie en cas de panne, nous faisons l'acquisition d'un bloc de 3 nouveaux serveurs fonctionnant de manière synchronisée.

- **Le bénéfice (Zéro coupure) :** C'est le principe de la roue de secours automatique. Si l'un des serveurs subit une panne matérielle sévère, les deux autres absorbent sa charge instantanément. Les agents de la mairie et les administrés ne subiront aucune coupure.
- **La performance :** Ce matériel est largement dimensionné pour absorber la surcharge que nous connaissons aujourd'hui, offrir un fonctionnement fluide et rapide des logiciels métiers, et stocker de manière pérenne les archives numériques de la commune.

2. Le réseau à très haute vitesse : Pour que nos agents puissent travailler efficacement sans subir de ralentissements (les fameux "bugs" ou logiciels qui "moulinent"), la refonte intègre de nouveaux équipements de communication (commutateurs).

- **Le bénéfice :** Nous remplaçons nos petites routes départementales par une autoroute numérique fluide. De plus, ces équipements sont doublés : si l'un tombe en panne, le trafic passe automatiquement par le second.

3. Le cerveau logiciel : Un pilotage intelligent et sécurisé Le pilotage de cette nouvelle infrastructure sera confié à des logiciels de dernière génération (solutions Nutanix et Windows 2025), garantis et maintenus pour les 5 prochaines années.

- **Le bénéfice (Gain de temps) :** Pour notre équipe informatique, actuellement en manque d'effectifs, c'est un gain de temps inestimable. Le système s'autogère en grande partie et alerte de manière claire avant qu'un problème grave ne survienne.

4. L'assurance-vie de notre infrastructure informatique : C'est la pièce maîtresse de notre défense face aux risques de piratage et de demandes de rançons (comme cela est arrivé à Mahina). Nous ajoutons une machine isolée, dotée d'une très grande capacité de stockage, uniquement dédiée aux sauvegardes.

- **Le bénéfice (La garantie de restauration) :** Cette machine testera automatiquement et régulièrement nos sauvegardes dans une "bulle déconnectée". C'est l'assurance logique pour le Conseil Municipal qu'en cas de cyberattaque ou de sinistre majeur, la Mairie possède une copie saine de toutes ses données (RH, État Civil, Finances) et pourra redémarrer son activité.

5. L'évolutivité : Ce système absorbera parfaitement nos besoins actuels et futurs car évolutif.

- **Le bénéfice :** Si la Mairie déploie de nouveaux services numériques à l'avenir, nous pourrons ajouter de nouveaux serveurs dans l'infrastructure facilement sans souci particulier.

Les détails techniques de la future architecture technique seront définis dans le Cahier des Clauses Techniques et Particulières (CCTP) du marché qui sera lancé à la suite de la validation du budget en Conseil Municipal.

4.3 L'achat de la future infrastructure

L'installation définitive interviendra d'ici 3 à 4 mois.

Pour garantir la sécurité des données des citoyens et la continuité totale des services de la commune, le projet d'acquisition de la nouvelle infrastructure sécurisée (3 serveurs hyperconvergés) a été chiffré.

Ce premier retour budgétaire d'un prestataire de la place couvre non seulement l'achat du matériel haute performance et l'accompagnement à la mise en œuvre, mais également **l'ensemble des licences et du support technique pour les 5 prochaines années**.

Désignation de l'investissement (Budget de modernisation)	Investissement	Fonctionnement
3 Serveurs de nouvelle génération	32 526 132	
Abonnements et Licences sécurisées (Hyperviseur sur 5 ans + Windows Server)		12 449 749
Équipements Réseau Haute Vitesse (Switchs, câblage sécurisé)	4 963 377	
Prestations de services (Intégration et déploiement)	3 200 000	
TOTAL GÉNÉRAL T.T.C. (Incluant 5 ans de support)	**40 689 509**	**12 449 749**

Commenté [GU1]: Sépare l'investissement du fonctionnement, stp.

Un investissement d'environ 53 millions de FCFP lissé sur une exploitation de 5 ans représente un coût d'environ 10,6 millions FCFP par an. C'est le prix de l'assurance absolue contre la paralysie des services municipaux et la perte irréversible des données de la commune.

5 Les autres actions de modernisation

- Machine "Admin" : Besoin d'un PC dédié pour réaliser les opérations de maintenance (DE en cours).
- Documentation : Formalisation des procédures pour permettre à un nouvel arrivant de comprendre le SI, étape clé vers la conformité ISO 9001.
- Outils de gestion et Intelligence Artificielle : Le futur système de virtualisation sera doté de son propre tableau de bord simplifié. En complément, nous déploierons des outils basés sur l'IA pour automatiser la documentation et générer des indicateurs de performance clairs pour la Direction Générale et les élus.

6 Conclusion

La situation actuelle du SI de la Mairie de Faa'a est critique : matériel obsolète, sauvegardes défaillantes, et surcapacité des serveurs créent un risque systémique pour l'administration municipale.

Sans action rapide, une panne majeure pourrait paralyser les services pendant plusieurs mois, avec des pertes de données irréversibles et des coûts financiers exponentiels (achats d'urgence, indisponibilité des services).

La mesure principale proposée dans ce document — acquisition d'une infrastructure temporaire, mise en place de sauvegardes fiables (hors ligne) — constituent les premières actions d'une feuille de route prioritaire pour :

- Lever les risques immédiats (crash matériel, perte de données).

- Stabiliser le SI en réduisant la charge et en sécurisant les données.
- Préparer la transition vers une infrastructure pérenne

La livraison est prévue sous 3 à 4 mois.

L'urgence est double :

- Opérationnelle : Agir dès maintenant pour éviter un effondrement du SI.
- Stratégique : Structurer une gestion durable du SI, avec des compétences internes renforcées, une documentation exhaustive (conforme à l'ISO 9001), et des outils automatisés (dont l'IA pour la supervision et la documentation).

La sécurisation et la modernisation du système d'information permettront également de déployer, dans des conditions maîtrisées, les nouveaux services numériques en cours de validation.

Commune de Faa'a
Direction Générale des Services
PCI / Service Informatique
Tél : 40 800 988 – Mail : informatique@mairiefaaa.pf

Annexe 1 : Apparition d'alerte rouge dans les traces système

Date et heure de la prise de connaissance : Début mai 2026

Date estimée de survenance : fin décembre 2025

Nature de l'incident : disponibilité

Origine : défaillance technique

Catégories de données concernées : Toutes

Catégories et nombre approximatif de personnes concernées :

Tous (usagers / salariés / partenaires – 30.000 (nombre d'habitants).

Conséquences probables :

- Image de la commune dégradée,
- Arrêt des serveurs pendant 3 à 4 mois,
- Perte financière forte,
- Arrêt du travail à la mairie pendant le temps donné

Mesures prises et proposées :

- Détermination de la panne derrière l'alerte rouge
- Matériels de l'infrastructure défectueux
- Actions urgentes à réaliser : Audit rapide de l'alerte par INFONECS
- Actions à la suite de l'audit
    - Changement de l'infrastructure obsolète,
    - Courriers d'alerte par courrier Responsable de la Sécurité du Système d'Information (RSSI),
    - Mise en œuvre d'un Plan de Reprise d'Activité,

Constat

- Lors de l'audit,
    - L'alarme rouge a fait apparaitre que les contrôleurs RAID des 3 serveurs étaient défaillants, menant au possible arrêt non voulu des serveurs physiques ;
    - L'obsolescence de l'infrastructure en est la cause ;
- Des actions urgentes sont demandées et listées plus haut.

Jean-Pierre CLAUDE
RSSI externalisé pour la Commune de Faa'a

Papeete, le 5 mai 2026

À l'attention de :

Monsieur le Directeur Général des Services

Commune de Faa'a

Copie : Monsieur Eugène SANFORD, Directeur des Systèmes d'Information

Objet : Alerte de sécurité majeure sur le Système d'Information de la commune

Référence : *Échange technique avec la DSI ayant mis en évidence l'état critique de l'infrastructure*

Monsieur le Directeur Général des Services,

Faisant suite à l'échange technique tenu récemment avec la Direction des Systèmes d'Information, et compte tenu de la gravité des constats partagés à cette occasion, je me permets, en ma qualité de RSSI externalisé de la commune, de vous adresser la présente note afin de porter formellement à votre connaissance une situation de risque majeur pesant sur le Système d'Information.

Cette démarche s'inscrit pleinement dans mon devoir d'alerte. Les éléments ci-dessous appellent, selon mon analyse et celle de la DSI, une décision rapide de votre part.

> **⚠ Risque d'arrêt total des services communaux**
> L'infrastructure technique qui supporte aujourd'hui l'ensemble des applications métier de la commune est vétuste, n'est plus couverte par une maintenance constructeur, et ne peut plus être maintenue en interne dans des conditions satisfaisantes. Une panne majeure entraînerait l'indisponibilité de la quasi-totalité des services numériques de la mairie.

1. Une infrastructure qui est le socle de tous les services numériques

L'infrastructure hébergée dans la salle serveur de la mairie constitue le socle technique sur lequel reposent l'intégralité des applications métier de la commune. Concrètement, elle héberge à elle seule l'ensemble des services suivants :

- Les applications de Ressources Humaines et de gestion de la paie ;
- Les applications financières et comptables ;
- L'État civil et la gestion des élections ;
- La gestion du courrier ;

C2 - Confidentiel

- La supervision technique du service de l'eau ;
- Les serveurs de fichiers communaux et les espaces de travail partagés ;
- Les services techniques transversaux (annuaire, authentification, impression, etc.).

Sans cette infrastructure, les agents communaux ne peuvent ni accéder à leurs applications, ni à leurs fichiers de travail. Les guichets reposant sur ces applications (état civil, accueil du public, finances, RH) ne peuvent plus fonctionner normalement.

2. Conséquences directes d'une panne majeure

En cas de défaillance significative de cette infrastructure — défaillance que le contexte décrit ci-après rend chaque jour plus probable — les conséquences pour la commune seraient les suivantes :

- **Arrêt complet des applications métier :** RH, finances, état civil, courrier, supervision de l'eau, applications du SPIC déchets, gestion du patrimoine, etc.
- **Indisponibilité totale des fichiers :** les serveurs de fichiers et les espaces partagés ne sont plus accessibles. Les documents en cours de traitement par les agents deviennent inaccessibles.
- **Impact sur les services au public :** guichets état civil, élections, accueil — tous les services dépendant des applications hébergées sont perturbés ou interrompus.
- **Impact sur les services H24 :** le service de l'eau, qui assure une continuité de service 24h/24, et la supervision associée sont directement impactés.
- **Seul service qui resterait fonctionnel :** la messagerie électronique, hébergée chez Microsoft (Exchange Online) et donc indépendante de l'infrastructure interne. Tout le reste est à l'arrêt.

Il est important de souligner que la durée d'une telle interruption ne se compte pas en heures, mais potentiellement en jours, voire en semaines, compte tenu des éléments exposés ci-après.

3. Vétusté avancée du matériel

Le cœur de l'infrastructure (serveurs de virtualisation et stockage) a été acquis et mis en service en 2017. Ce matériel atteint aujourd'hui sa neuvième année de production, durée qui dépasse très largement le cycle de vie normalement admis pour ce type d'équipements (5 à 7 ans).

À cette obsolescence physique s'ajoute une obsolescence logicielle critique : la version de l'hyperviseur en production (VMware ESXi 6.5 et 6.7) n'est plus supportée par l'éditeur depuis plusieurs années. Cela signifie qu'aucun correctif de sécurité n'est plus diffusé, alors même que des vulnérabilités sont régulièrement publiées sur ces versions.

Par ailleurs, les ressources matérielles disponibles (notamment la mémoire vive) sont aujourd'hui en limite d'usage par rapport à la charge réelle des applications.

C2 - Confidentiel

4. Absence de maintenance constructeur

Le matériel a été fourni par BULL. Or, BULL n'existe plus en tant qu'entité opérationnelle assurant le support sur ce matériel. Concrètement :

- Aucun contrat de maintenance constructeur n'est plus en vigueur sur le matériel critique de production ;
- En cas de panne d'un composant majeur (carte mère, contrôleur de stockage, alimentation redondée défaillante, etc.), aucune pièce de rechange n'est garantie ni dans un délai contractuel, ni à un coût maîtrisé ;
- Aucun ingénieur constructeur n'est mobilisable pour intervenir sur ce matériel.

Concrètement, en cas d'incident matériel, il n'existe plus de filière officielle de remise en service. La commune dépend de pièces récupérables d'occasion, sans garantie de disponibilité ni de délai.

5. Absence de ressources humaines pour assurer la maintenance

Le service informatique de la commune est composé de trois agents dont la mission première est le support aux utilisateurs et la gestion des applications métier. Cette équipe :

- Ne dispose pas de l'expertise spécifique à la maintenance d'une infrastructure de virtualisation et de stockage en production ;
- Est dimensionnée pour le fonctionnement courant, et ne peut pas absorber un incident matériel ou une opération de migration d'envergure ;
- Ne dispose pas d'astreinte structurée ; les interventions hors heures ouvrées reposent sur la bonne volonté des agents.

L'absence simultanée de support constructeur et de compétences internes spécialisées sur ce matériel ancien expose la commune à un risque opérationnel que nous considérons comme inacceptable au regard des missions de service public assurées.

6. Liaisons fibre inter-bâtiments défaillantes

À ces problématiques de cœur d'infrastructure s'ajoute un point de fragilité connu et récurrent sur les liaisons fibre optique reliant les bâtiments du site principal et certains sites satellites :

- Des coupures fréquentes sont constatées sur ces liaisons, sans qu'une cause racine n'ait pu être traitée durablement à ce jour ;
- Chaque coupure entraîne une perte d'accès partielle au Système d'Information pour les utilisateurs des bâtiments concernés (applications, fichiers, téléphonie sur IP) ;
- Ces incidents impactent en premier lieu la continuité du service rendu aux agents et, indirectement, l'accueil du public dans les bâtiments concernés ;

C2 - Confidentiel

- Au-delà de la gêne opérationnelle, ces coupures masquent les éventuels signaux faibles de défaillance de l'infrastructure centrale et compliquent le diagnostic en cas d'incident plus large.

Cette fragilité du réseau d'accès vient se cumuler à la fragilité de l'infrastructure centrale décrite plus haut : un incident sur l'un ou l'autre des deux périmètres entraîne, dans les faits, les mêmes conséquences pour l'utilisateur final, à savoir l'impossibilité d'utiliser les outils de travail.

7. Synthèse et recommandation

Les cinq facteurs ci-dessus se cumulent et se renforcent mutuellement : un matériel vieillissant qui n'est plus couvert par le constructeur et qui ne peut plus être maintenu en interne dans des conditions de sécurité acceptables. Chacun de ces facteurs, pris isolément, constituerait déjà une situation préoccupante. Leur conjonction caractérise un risque majeur, susceptible de provoquer une interruption brutale et durable des services numériques de la commune.

8. Appel à décision et recommandations

Au regard des éléments exposés, et compte tenu de l'agenda communal (élections du premier trimestre 2026, continuité du service de l'eau et des permanences d'état civil), il m'apparaît indispensable de lancer sans attendre les actions suivantes. Trois recommandations sont formulées, par ordre de priorité :

Recommandation n°1 — URGENT

Tester sans délai le bon fonctionnement du Plan de Reprise d'Activité (PRA)
Compte tenu de la fragilité de l'infrastructure de production, le PRA constitue aujourd'hui le dernier filet de sécurité de la commune. Or il n'a pas fait l'objet d'un test complet récent. Il est impératif de vérifier, dans les plus brefs délais, que les sauvegardes répliquées sur le site de Papenoo sont exploitables et que les VM critiques (RH, Finances, État civil, Courrier, Eau) peuvent y être redémarrées dans des délais compatibles avec la continuité du service public.

Recommandation n°2 — Lancer formellement la consultation pour le renouvellement de l'infrastructure

La Direction des Systèmes d'Information doit, dans un calendrier resserré, élaborer un cahier des charges et engager une consultation pour le renouvellement de l'infrastructure socle. Au regard des délais habituels (rédaction du cahier des charges, publication de la consultation, dépouillement, contractualisation, livraison du matériel ou mise à disposition de l'environnement, migration des applications), un démarrage immédiat est nécessaire pour viser un déploiement effectif au cours du second semestre 2026, conformément à la cible évoquée par la DSI.

C2 - Confidentiel

Recommandation n°3 — Étudier l'externalisation totale ou partielle du SI et/ou du PRA

Compte tenu du sous-dimensionnement reconnu de l'équipe interne, de l'absence d'expertise sur la maintenance matérielle et de l'urgence de la situation, la DSI gagnerait à faire étudier dans le cadre de cette consultation des scénarios d'externalisation — qu'il s'agisse de l'ensemble du Système d'Information, de la seule production, ou a minima du Plan de Reprise d'Activité. L'externalisation présente l'avantage de transférer à un opérateur spécialisé la responsabilité du maintien en conditions opérationnelles et de sécurité, dans le cadre d'engagements de service contractualisés (SLA, RPO/RTO, fenêtres de maintenance, gestion des correctifs).

Ces trois recommandations ne sont pas exclusives : la première (test PRA) doit être engagée sans attendre, indépendamment des choix structurants qui seront faits ; les deuxième et troisième s'inscrivent dans la même démarche de consultation, dont elles définissent le périmètre.

9. Conclusion

Je vous remercie par avance de l'attention que vous porterez à ces éléments et reste naturellement à votre disposition, ainsi qu'à celle de la Direction des Systèmes d'Information, pour vous présenter en détail les conclusions de cette analyse, les scénarios envisageables (modernisation sur site, externalisation, solution hybride) et les ordres de grandeur associés en termes de calendrier et de budget.

Nous vous prions d'agréer, Monsieur le Directeur Général, l'expression de notre considération distinguée.

Jean-Pierre CLAUDE
Responsable de la Sécurité des Systèmes d'Information
RSSI externalisé pour la Commune de Faa'a
Jean-pierre.claude@exodata.pf — +689 87 27 51 77

C2 - Confidentiel

ANNEXE TECHNIQUE

à destination de la Direction des Systèmes d'Information

La présente annexe synthétise l'inventaire et le fonctionnement de l'infrastructure socle de la mairie, sur la base des éléments techniques recueillis auprès de la DSI et de l'export RVTools du 12 décembre 2025 (fait avec Jimmy POETAI)

A.1 Vue d'ensemble de l'architecture

L'infrastructure de la commune s'articule autour de deux sites principaux :

- **Site principal — Mairie de Faa'a :** salle serveur abritant le cluster de virtualisation de production, le stockage primaire, les pare-feu, le bastion d'administration et l'interconnexion réseau.
- **Site PRA — Datacenter TNT à Papenoo :** baie en colocation (mutualisée avec les communes de Papeete et Arue) hébergeant un serveur de réplication et un NAS de sauvegarde, reliée au site principal par un lien PROLAN dédié de 60 Mbps.
- **Sites satellites :** directions et services déportés (eau, déchets, patrimoine, cuisine centrale, salle Poheroa, cimetière, centre de sécurité, Fare Vaa'a, etc.) reliés au site principal par liaisons Wi-Fi point à point ou liens PROLAN.

A.2 Plateforme de virtualisation (VMware vSphere)

Le cœur de production est un cluster vSphere 6.7 avec vSAN Standard, hébergeant l'ensemble des machines virtuelles métier de la commune.

Hôte	Modèle	CPU (cœurs)	RAM	ESXi
esx1.faaa.local	Dell PowerEdge R740xd	Intel Xeon Gold 6130 (16c)	128 Go	6.5
esx2.faaa.local	Dell PowerEdge R740xd	Intel Xeon Gold 6130 (16c)	128 Go	6.5
esx3.faaa.local	Dell PowerEdge R740xd	Intel Xeon Gold 6130 (16c)	128 Go	6.5
PRA Papenoo	HPE ProLiant DL380 Gen10	Intel Xeon Gold 5215 (20c)	128 Go	6.7

Volumétrie : 102 machines virtuelles inventoriées, dont 42 en production active, pour environ 33 Tio de stockage utilisé. Les 60 VM hors tension correspondent à des environnements legacy, des modèles ou des bacs à sable n'ayant pas été supprimés.

Point d'attention sécurité : VMware ESXi 6.5 est en fin de support général depuis octobre 2022, et VMware ESXi 6.7 depuis octobre 2023. Aucun correctif de sécurité n'est plus diffusé pour ces versions, alors qu'elles ont fait l'objet ces dernières années de vulnérabilités critiques (notamment exploitées par des campagnes de rançongiciel ciblant ESXi). Le

C2 - Confidentiel

matériel sous-jacent (acquis en 2017 auprès de BULL) n'est par ailleurs plus sous contrat de maintenance.

A.3 Stockage et sauvegardes

- **Stockage primaire :** vSAN Standard distribué sur les trois nœuds Dell R740xd du site mairie.
- **NAS de sauvegarde local :** Synology RS2423+ — 64 To, hébergé en salle serveur mairie.
- **Stockage déporté :** Synology RS3617RPxs — 16 To, hébergé sur le site PRA de Papenoo.
- **Logiciel de sauvegarde :** Veeam Backup & Replication 11.0.1.1261, avec WAN accelerator pour la réplication vers le PRA.
- **Politique de rétention :** rétention courte de 7 à 10 jours ; une sauvegarde complète quotidienne et une réplication asynchrone vers le PRA.
- **Fenêtres de sauvegarde :** sauvegarde locale de 15h30 à 21h45 (~6h15) ; réplication vers Papenoo de 21h45 à ~12h le lendemain (~14h15).
- **Test PRA :** tous les deux ans environ ; une restauration majeure réalisée en 2024.

Point d'attention : la version Veeam 11 est elle-même en fin de support standard. La rétention courte (7-10 jours) et l'absence de tests SureBackup automatisés limitent la résilience face à un incident de type rançongiciel à propagation lente.

A.4 Réseau et sécurité périmétrique

- **Pare-feu :** deux Fortinet FortiGate 100F en cluster actif/passif, segmentés en deux VDOM (réseau interne ; supervision des cinq bassins d'eau via APN privé 4G).
- **Segmentation :** VLAN administration, sauvegarde et serveurs isolés des VLAN utilisateurs ; tout flux remonte au FortiGate qui assure le filtrage.
- **Commutation :** deux HP Aruba 2920 24G PoE en distribution salle serveur.
- **Internet :** FTTH IP fixe Optimal Pro (800 Mbps down / 200 Mbps up) pour l'accès internet utilisateur ; opérateur ONATI.
- **Liens inter-sites :** PROLAN agrégés à 100 Mbps (60 Mbps dédiés à la réplication, le reste pour les sites satellites : centre de sécurité 10 Mbps, Fare Vaa'a 10 Mbps, etc.).
- **Liaisons fibre inter-bâtiments :** interconnexions optiques entre les bâtiments du site principal et certains satellites, qui font l'objet de coupures fréquentes non encore résolues.
- **Accès distant :** VPN désactivé sur le FortiGate ; les accès d'administration passent exclusivement par le bastion Systancia avec MFA Google Authenticator.

C2 - Confidentiel

Point d'attention : les FortiGate font régulièrement l'objet de vulnérabilités critiques (FortiOS) qui exigent une réactivité forte sur les correctifs. Le dispositif est correctement segmenté, mais la fenêtre de patch dépend de la disponibilité des équipes.

Point d'attention complémentaire : les coupures récurrentes sur les liaisons fibre inter-bâtiments dégradent la disponibilité perçue par les utilisateurs et compliquent le diagnostic en cas d'incident plus large. Une investigation dédiée (qualification du câblage, mesures réflectométriques, vérification des connecteurs et des transceivers) est à programmer.

A.5 Services hébergés sur l'infrastructure

L'infrastructure socle héberge les applications métier suivantes (les plus critiques figurent en gras) :

- **Ressources Humaines / paie** (critique)
- **Finances / comptabilité publique** (critique)
- **État civil et gestion des élections** (critique — élections communales 1er trimestre 2026)
- **Gestion du courrier** (critique)
- **Supervision technique du service de l'eau** (continuité H24/7j7)
- Serveurs de fichiers et espaces partagés
- Annuaire Active Directory et services techniques associés
- Bastion d'administration Systancia
- Applications du SPIC déchets, Direction du patrimoine, Cuisine centrale

A.6 Services hébergés à l'extérieur (non impactés)

Pour mémoire, les services suivants ne dépendent pas de l'infrastructure socle et continueraient à fonctionner en cas de panne majeure de celle-ci :

- **Messagerie :** Microsoft Exchange Online (210 boîtes), avec sauvegarde Keepit.
- **Police municipale et pompiers :** logiciel LOGIPOL en SaaS, indépendant de l'infrastructure.
- **EDR :** Harfanglab, supervisé par le SOC 6e Sens Pacifique.

A.7 Cadre de conformité applicable

La commune est concernée par la directive NIS 2, qui impose aux entités essentielles et importantes des obligations renforcées en matière de gestion des risques cyber, de continuité d'activité, de gestion des correctifs et de notification des incidents. L'état actuel de l'infrastructure (matériel hors maintenance, hyperviseur sans correctifs de sécurité, rétention de sauvegarde courte, équipe interne sous-dimensionnée) est difficilement compatible avec ces exigences.

A.8 Synthèse des risques techniques principaux

C2 - Confidentiel

Risque	Cause	Niveau
Panne matérielle non réparable	Matériel de 2017, plus de maintenance constructeur (BULL), pas de pièces détachées garanties	**Élevé**
Compromission via vulnérabilité hyperviseur	ESXi 6.5/6.7 en fin de support, plus de correctifs de sécurité	**Élevé**
Délai de remise en service prolongé	Pas de support constructeur, équipe interne non spécialisée, pas d'astreinte structurée	**Élevé**
Perte de données récentes en cas d'incident	Rétention courte (7-10 j), absence de tests SureBackup automatisés	**Modéré**
Saturation de ressources (RAM)	Capacité juste au regard de la charge actuelle, croissance non absorbable	**Modéré**
Coupures réseau utilisateurs	Liaisons fibre inter-bâtiments défaillantes, cause racine non traitée	**Modéré**

— Fin de l'annexe technique —

C2 - Confidentiel

Rapport d'audit : Environnement VMware en vue du remplacement de la batterie du contrôleur RAID

infonecs™

CLIENT	Mairie de Faaa
CHARGE D'AFFAIRES INFONECS	Jean-Raymond BESSEYRE Email: jean-raymond.besseyre@infonecs.pf Tel : +689 40 54 33 00 Vini : +689 87 03 87 41
TYPE/REF DE DOCUMENT	**Rapport d'audit**
NOMBRE DE PAGES	33

Table des matières

1. SYNTHESE EXECUTIVE 4
2. OBJET DU RAPPORT 5
3. PERIMETRE DE L'AUDIT 5
4. DEROULE CHRONOLOGIQUE DE L'ANALYSE 6
5. ÉTAT DES LIEUX 7

5.1 Serveurs physiques 7
5.2 Processeurs et memoire 8
5.3 Controleurs RAID et batteries 9
5.4 BIOS, iDRAC et firmwares materiels 10
5.5 Administration materielle via iDRAC 10

6. ÉTAT DE L'ENVIRONNEMENT VMWARE ET VSAN 11

6.1 Version VMware 11
6.2 Utilisation du stockage vSAN 12
6.3 Politique vSAN appliquee 13
6.4 Alertes vCenter et vSAN Health 14
6.5 Configurations historiques observees 15
6.6 Taille des disques virtuels 16

7. ANALYSE RESEAU 17

7.1 Reseau vSAN et reseau des machines virtuelles 17
7.2 vSwitch locaux et absence de vSwitch distribue 19

8. ANALYSE SAUVEGARDE ET REPLICATION 20

8.1 Version Veeam 20
8.2 État general des sauvegardes 21
8.3 Replication vers Papenoo 22
8.4 Depots de sauvegarde 23
8.5 SureBackup non exploite 23
8.6 Declaration du vCenter dans Veeam 24

9. RISQUES IDENTIFIES 25
10. PHASES ENVISAGEABLES 27

10.1 Distinction entre actions immediates et actions a planifier 27
10.1.1 Actions immediates recommandees 27
10.1.2 Actions a ne pas realiser immediatement sans plan de maintenance 28
10.2 Phase 1 – Traitement de l'urgence materielle 29

10.3 PHASE 2 – SECURISATION DE L'EXPLOITATION 30
10.4 PHASE 3 – REMISE A NIVEAU PROGRESSIVE DE L'INFRASTRUCTURE 31
10.5 PHASE 4 – RENOUVELLEMENT OU REFONTE DE L'INFRASTRUCTURE 32

11. RECOMMANDATION FINALE 33

1. SYNTHESE EXECUTIVE

L'audit réalisé met en évidence que l'alerte initiale liée à la batterie du contrôleur RAID ne doit pas être traitée comme un incident matériel isolé.

L'infrastructure repose sur un cluster VMware vSAN composé de trois serveurs Dell PowerEdge R740XD. Les trois hôtes présentent un défaut similaire sur la batterie du contrôleur RAID, ce qui indique un vieillissement homogène des composants. Dans un environnement vSAN, ce point est critique, car les disques locaux des serveurs participent directement au stockage distribué du cluster.

L'analyse a également mis en évidence plusieurs facteurs aggravants : les serveurs ne sont plus couverts par le support constructeur, les firmwares BIOS, iDRAC, contrôleur RAID et disques sont fortement obsolètes, l'environnement VMware repose sur une version ESXi ancienne, et le datastore vSAN est utilisé à plus de 90 %. Cette saturation limite fortement la capacité à mettre un hôte en maintenance sans arrêt préalable de certaines machines virtuelles ou libération d'espace.

Les sauvegardes semblent globalement fonctionnelles, mais certains jobs de réplication présentent des échecs. Avant toute intervention matérielle ou logicielle sur les hôtes, il est donc indispensable de confirmer l'état réel des sauvegardes, de valider la restauration des machines virtuelles critiques et de corriger les réplications défaillantes.

Le réseau vSAN présente également un point de vigilance important. Bien qu'une séparation physique existe au niveau des interfaces réseau des serveurs, les flux semblent converger ensuite sur la même infrastructure réseau, avec une absence apparente d'isolation VLAN dédiée pour le vSAN. Cette configuration augmente le risque de perturbation entre les flux utilisateurs, serveurs et stockage.

La priorité consiste donc à traiter l'urgence matérielle de manière contrôlée, hôte par hôte, après validation des sauvegardes, de la réplication et de l'état de santé vSAN. Les mises à jour firmware et les évolutions VMware doivent être envisagées dans un second temps, avec un plan de maintenance détaillé. Une réflexion sur le renouvellement ou la refonte de l'infrastructure doit également être engagée, compte tenu de l'âge de la plateforme, de son obsolescence logicielle et de la saturation du stockage.

En synthèse, l'infrastructure reste fonctionnelle, mais elle présente une accumulation de risques matériels, logiciels, capacitaires et opérationnels. La situation nécessite une action progressive, structurée et prudente.

2. OBJET DU RAPPORT

Le présent rapport a pour objet de présenter les constats réalisés dans le cadre d'un audit technique de l'infrastructure VMware vSAN de la Mairie de Faaa.

Cet audit fait suite à une alerte de supervision signalant un défaut matériel sur l'un des serveurs du cluster. Les premières vérifications ont permis d'identifier un défaut lié à la batterie du contrôleur RAID.

Compte tenu de l'utilisation de VMware vSAN, l'analyse a été élargie afin d'évaluer l'impact potentiel de ce défaut sur le stockage distribué, la disponibilité des machines virtuelles, la capacité de maintenance des hôtes et les conditions préalables à toute intervention.

Ce rapport vise donc à formaliser les constats, les risques identifiés et les recommandations associées.

3. PERIMETRE DE L'AUDIT

Le périmètre de l'audit couvre les éléments contribuant au bon fonctionnement de l'infrastructure VMware vSAN, à savoir :

- Les trois serveurs physiques composant le cluster VMware
- Certains composants matériels internes des serveurs liés au stockage
    - Les contrôleurs RAID et leurs batteries
    - Les disques participant au stockage vSAN
- Les versions de firmware et de BIOS pouvant avoir un impact sur la maintenance ou la stabilité de l'environnement
- L'environnement VMware ESXi et vCenter
    - La configuration vSAN
    - Les réseaux physiques et virtuels utilisés par les hôtes
- La fabric de stockage vSAN
- Le système de sauvegarde et de réplication Veeam
- Les modalités d'administration matérielle des serveurs, notamment via iDRAC

Le périmètre ne couvre pas l'analyse fonctionnelle des applications métiers hébergées dans les machines virtuelles, ni l'ordre d'arrêt ou de redémarrage applicatif des services. Ces éléments relèvent de la connaissance métier du client et devront être définis par celui-ci avant toute opération de maintenance nécessitant l'arrêt de machines virtuelles.

Il est également important de préciser que le redémarrage de certaines machines virtuelles peut déclencher l'application de mises à jour en attente au niveau système ou applicatif. Ces mises à jour peuvent, dans certains cas, provoquer des effets de bord ou des incompatibilités avec certains logiciels métiers. Cet aspect reste hors périmètre du présent audit et doit être traité par le client ou ses prestataires applicatifs.

4. DEROULE CHRONOLOGIQUE DE L'ANALYSE

L'audit n'a pas été réalisé sur la base d'un accès complet immédiat à l'ensemble des composants de l'infrastructure. Les constats ont été établis progressivement, en fonction des accès disponibles et des informations collectées.

Dans un premier temps, l'analyse a été déclenchée par une alerte de supervision concernant un défaut matériel. Cette première phase a permis d'identifier un problème lié au contrôleur RAID, et plus précisément à la batterie du contrôleur, au travers d'un accès ESXi.

Dans un second temps, l'analyse a été élargie afin d'identifier ce qui était hébergé sur le stockage interne du serveur concerné. Cette étape a mis en évidence l'utilisation de VMware vSAN, ce qui a changé le niveau de criticité du défaut constaté.

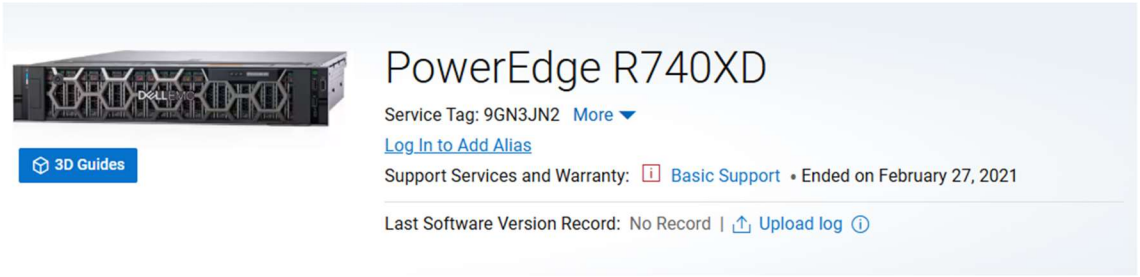
Dans un troisième temps, un accès temporaire aux interfaces iDRAC a été mis en place afin d'obtenir une vision plus précise de l'état matériel des serveurs. Ces accès n'étaient pas exploités de manière permanente avant l'audit. Leur activation a été réalisée uniquement pour les besoins de l'analyse, puis désactivée à l'issue des opérations.

Cette chronologie est importante : certaines informations matérielles détaillées n'ont pu être collectées qu'après l'activation temporaire des accès iDRAC. Elles ne pouvaient donc pas être connues au moment de la première analyse issue de la supervision.

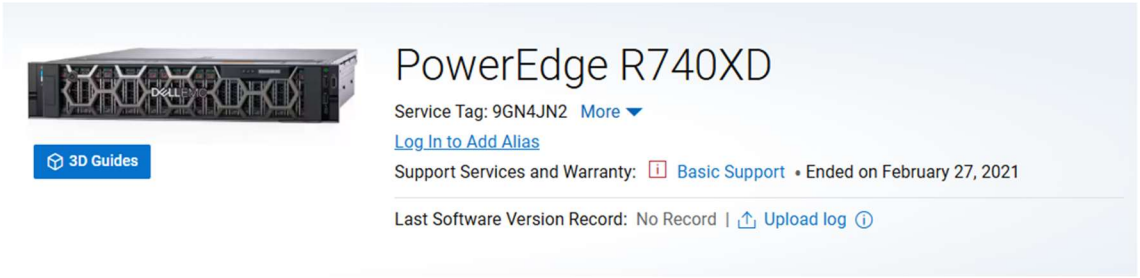
5. ÉTAT DES LIEUX

5.1 Serveurs physiques

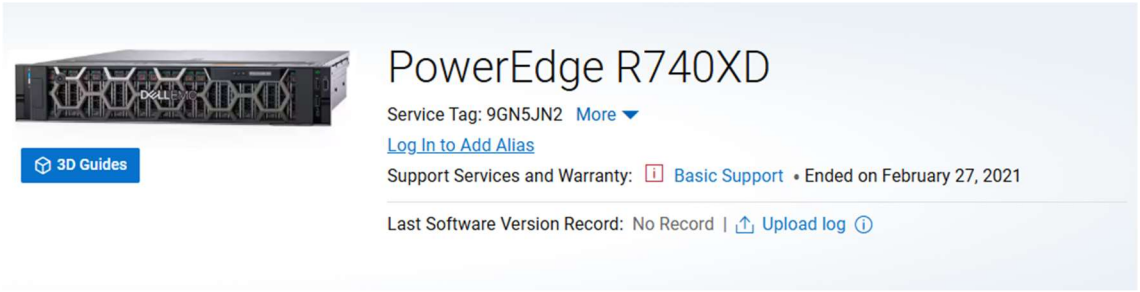
L'infrastructure repose sur trois serveurs Dell PowerEdge R740XD composant le cluster VMware :



Support for PowerEdge R740XD | Drivers & Downloads | Dell US



Support for PowerEdge R740XD | Overview | Dell US



Support for PowerEdge R740XD | Overview | Dell US

Les numéros de service relevés sont les suivants :

- 9GN**3**JN2
- 9GN**4**JN2
- 9GN**5**JN2

Ces numéros de service sont consécutifs, ce qui laisse supposer que les serveurs ont été acquis ou mis en service sur une période proche. Ce point est cohérent avec le constat d'un vieillissement similaire des composants, notamment les batteries des contrôleurs RAID.

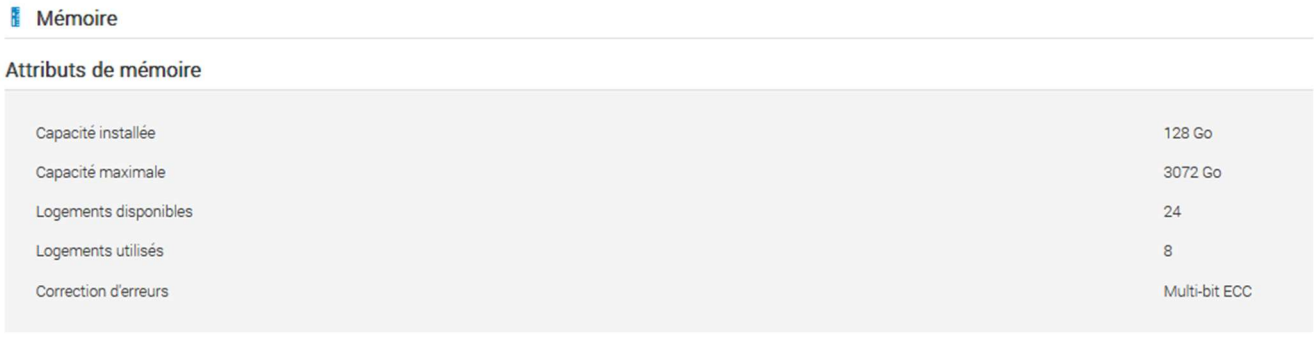
Le support constructeur des serveurs est arrivé à échéance le 27 février 2021. Ce point constitue un risque important dans le contexte d'une infrastructure vSAN, car l'environnement repose directement sur les composants matériels internes des hôtes.

En cas de panne matérielle, l'absence de support constructeur actif peut compliquer l'accès aux pièces de remplacement, allonger les délais d'intervention et limiter les possibilités d'assistance constructeur.

5.2 Processeurs et mémoire

Les serveurs sont équipés de processeurs Intel Xeon Gold 6130 cadencés à 2,10 GHz.

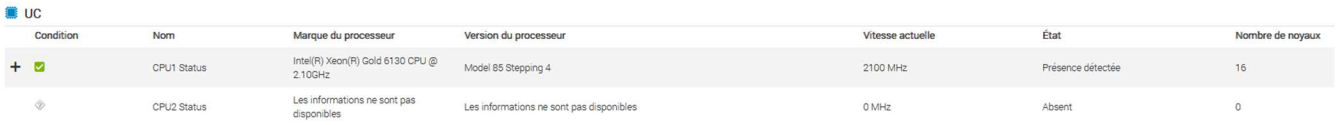
Ce processeur dispose de six canaux mémoire. Or, les serveurs sont actuellement équipés de huit barrettes mémoire DDR4 2666 MHz de 16 Go.



Cette configuration est fonctionnelle, mais elle n'est pas optimale d'un point de vue architecture mémoire. Elle peut provoquer une répartition non parfaitement équilibrée sur les canaux mémoire, ce qui peut générer de l'entrelacement ou une utilisation moins homogène des canaux disponibles.

Ce point ne constitue pas un incident bloquant dans l'état actuel, mais il mérite d'être signalé. Une évolution future pourrait consister à rééquilibrer la mémoire avec une configuration plus cohérente, par exemple douze barrettes mémoire dans le cas d'un seul processeur, afin d'exploiter de façon équilibré les six canaux mémoire.

Si un second processeur devait être ajouté, la répartition mémoire devrait également être étudiée afin d'éviter un déséquilibre entre les sockets et une utilisation optimale des canaux mémoires.



5.3 Contrôleurs RAID et batteries

Les serveurs sont équipés de contrôleurs Dell PERC H730P.

Les versions relevées sont les suivantes :

- Firmware actuel du contrôleur : 25.5.3.0005
- Dernière version disponible identifiée sur le support Dell : 52.30.0-6347

Le firmware du contrôleur RAID est donc fortement obsolète. Ce point doit être pris en compte dans toute opération de maintenance, car les contrôleurs participent directement à la présentation du stockage local utilisé par vSAN.

Les batteries des contrôleurs RAID présentent un défaut sur les trois serveurs depuis janvier 2026. Le fait que les trois serveurs soient concernés par le même type de défaut renforce l'hypothèse d'un vieillissement homogène des composants.

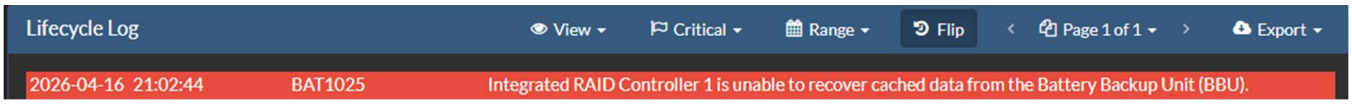
9GN3JN2



9GN4JN2



9GN5JN2



Dans le cadre d'un remplacement, deux approches peuvent être envisagées :

- Commander un contrôleur complet afin de sécuriser l'approvisionnement en pièce compatible
- Remplacer uniquement la batterie du contrôleur si cela est techniquement possible, afin de limiter les risques liés au remplacement complet du contrôleur.

Le remplacement complet du contrôleur RAID présente davantage de risques, notamment en ce qui concerne la reconnaissance de la configuration RAID existante, les écarts de firmware et les différences éventuelles de comportement du contrôleur.

Dans le contexte d'un environnement vSAN, cette intervention doit être préparée avec prudence et réalisée hôte par hôte, après vérification complète de l'état du cluster, des sauvegardes et de la capacité à maintenir l'accessibilité des machines virtuelles.

5.4 BIOS, iDRAC et firmwares matériels

L'audit a également permis d'identifier plusieurs versions de firmware fortement obsolètes sur les serveurs.

Les versions relevées sont notamment les suivantes :

- BIOS actuel : 1.2.11
- Dernière version recommandée identifiée : 2.27.0
- iDRAC actuel : 3.15.17.15
- Dernière version disponible identifiée pour ce modèle : 7.00.00.184
- Firmware du contrôleur PERC H730P actuel : 25.5.3.0005
- Dernière version disponible identifiée : 52.30.0-6347
- Firmware des disques Toshiba actuel : EB01
- Version recommandée identifiée : EB04

Cette liste n'est pas exhaustive. Elle concerne uniquement les composants susceptibles d'avoir un impact direct ou indirect sur la maintenance, les performances ou la stabilité du stockage vSAN.

Ces informations sont issues des éléments disponibles sur le support Dell et doivent être validées avant toute opération de mise à jour.

Les disques Toshiba participant au vSAN font également l'objet d'une mise à jour firmware recommandée. Toutefois, cette opération doit être considérée avec une grande prudence. Les disques concernés participent au stockage distribué du cluster une mise à jour mal préparée peut donc présenter un risque opérationnel important.

À ce stade, ces mises à jour sont donc mentionnées comme recommandations techniques, et non comme actions à réaliser immédiatement sans plan de maintenance détaillé.

5.5 Administration matérielle via iDRAC

Les interfaces iDRAC n'étaient pas utilisées de manière opérationnelle avant l'audit.

Pour rappel, l'iDRAC permet d'administrer un serveur Dell à distance, y compris lorsque le système d'exploitation est indisponible, figé ou lorsque le serveur est arrêté mais encore alimenté. Il permet notamment :

- De consulter l'état matériel du serveur
- D'accéder aux journaux matériels
- De réaliser des opérations de maintenance à distance
- De mettre à jour certains firmwares
- De redémarrer ou arrêter un serveur
- De faciliter le diagnostic en cas d'incident critique.

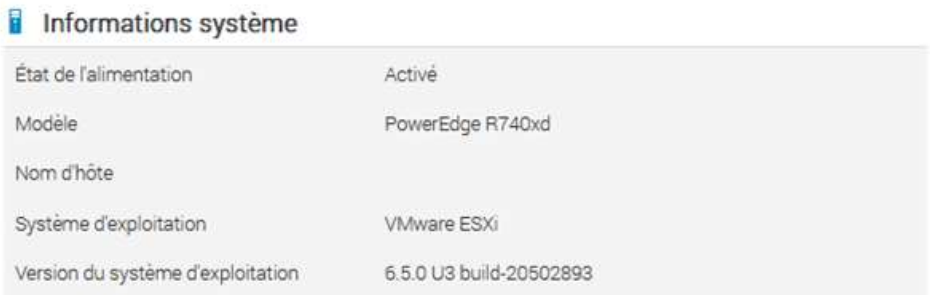
Dans le cadre de l'audit, les accès iDRAC ont été activés temporairement afin de collecter les informations nécessaires, puis désactivés.

La mise en service durable des interfaces iDRAC est fortement recommandée, mais uniquement dans un réseau d'administration dédié, isolé des VLAN utilisateurs, serveurs et stockage. Cet accès doit être strictement contrôlé, documenté et réservé aux personnes habilitées.

6. ÉTAT DE L'ENVIRONNEMENT VMWARE ET VSAN

6.1 Version VMware

L'environnement VMware est en version ESXi 6.5.0 Update 3, build 20502893.



Cette version est obsolète et n'est plus adaptée à une infrastructure critique reposant sur VMware vSAN. En cas d'incident majeur, notamment sur la couche vSAN, l'ouverture d'un ticket de support auprès de l'éditeur peut être fortement limitée ou compromise.

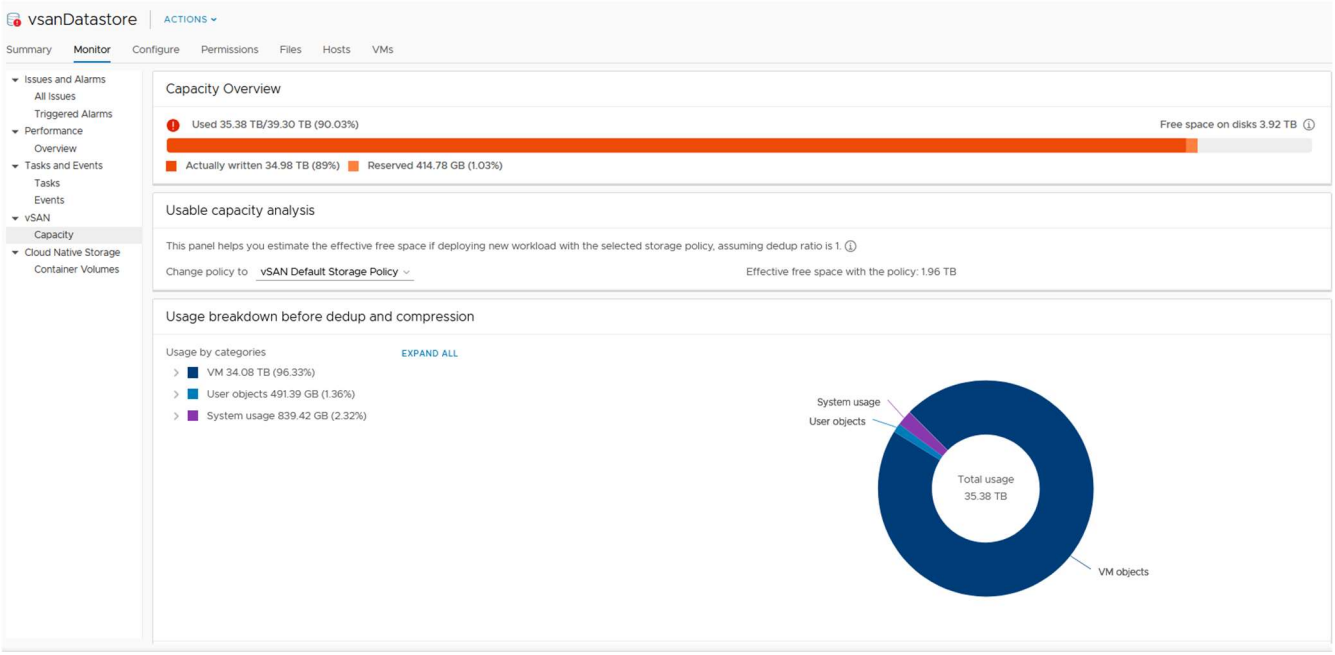
Cette situation augmente les risques liés :

- À l'absence de correctifs récents
- Aux vulnérabilités de sécurité non corrigées
- Aux problèmes de compatibilité matérielle
- Aux limites de support éditeur
- Aux difficultés de mise à jour
- À la compatibilité avec les versions récentes des outils de sauvegarde.

Les alertes vCenter remonte d'ailleurs des points liés à l'obsolescence de la version VMware et à des configurations vSAN étendues nécessitant une mise à niveau ESXi.

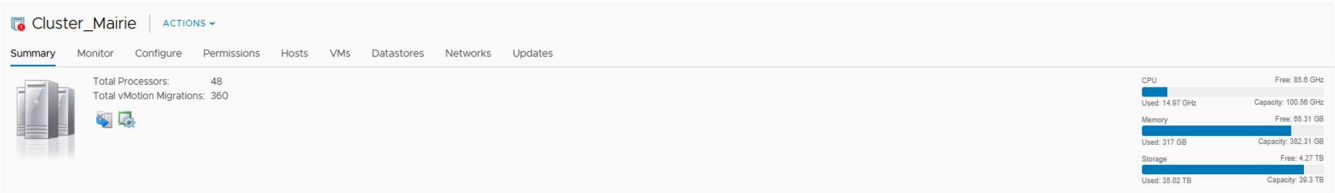
6.2 Utilisation du stockage vSAN

Le datastore vSAN est utilisé à environ 90 %.



La consommation globale des ressources du cluster est la suivante :

- CPU : 14,97 GHz utilisés sur 100,56 GHz disponibles
- Mémoire : 317 Go utilisés sur 382,31 Go disponibles
- Stockage : 35,02 To utilisés sur 39,3 To disponibles

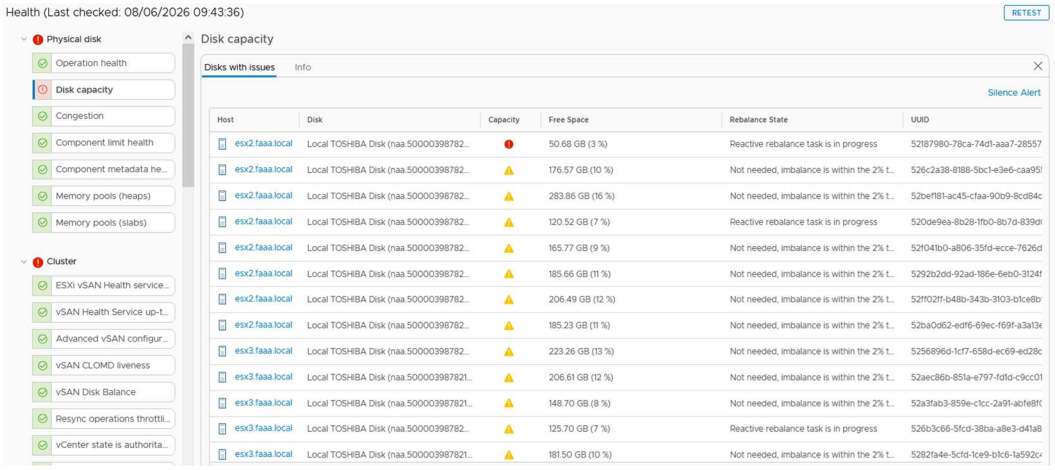


Le point bloquant principal concerne donc le stockage, puis dans une moindre mesure la mémoire. Le CPU dispose encore d'une marge confortable.

L'utilisation du vSAN à plus de 90 % constitue un risque important. Elle limite fortement la capacité du cluster à absorber une opération de maintenance, notamment la mise en maintenance d'un hôte.

Dans un cluster composé uniquement de trois nœuds, la mise en maintenance d'un serveur avec l'option "Ensure Accessibility" peut devenir difficile, voire impossible sans arrêt préalable de certaines machines virtuelles ou libération d'espace significative.

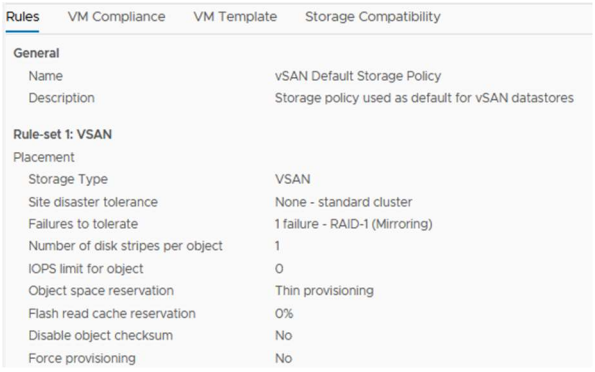
Cette situation est confirmée par les alertes vSAN Health indiquant des avertissements de capacité disque sur l'ensemble des disques. Le manque d'espace disponible provoque également des opérations de rééquilibrage fréquentes afin d'optimiser la distribution des données.



6.3 Politique vSAN appliquée

La politique vSAN par défaut appliquée est la suivante :

- Storage Type : vSAN
- Site disaster tolerance : None – standard cluster
- Failures to tolerate : 1 failure – RAID-1 Mirroring
- Number of disk stripes per object : 1
- IOPS limit for object : 0
- Object space reservation : Thin provisioning
- Flash read cache reservation : 0 %
- Disable object checksum : No
- Force provisioning : No.



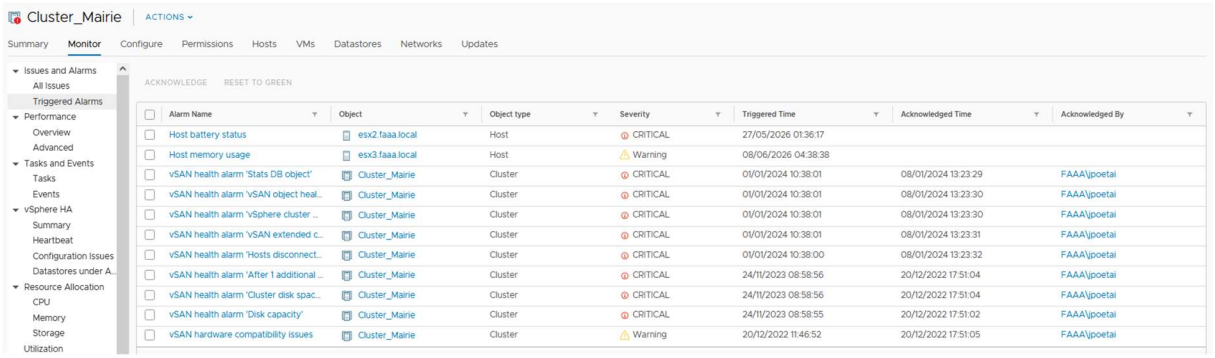
Cette politique signifie que les objets vSAN sont configurés pour tolérer une panne, avec une protection de type RAID-1 par miroir.

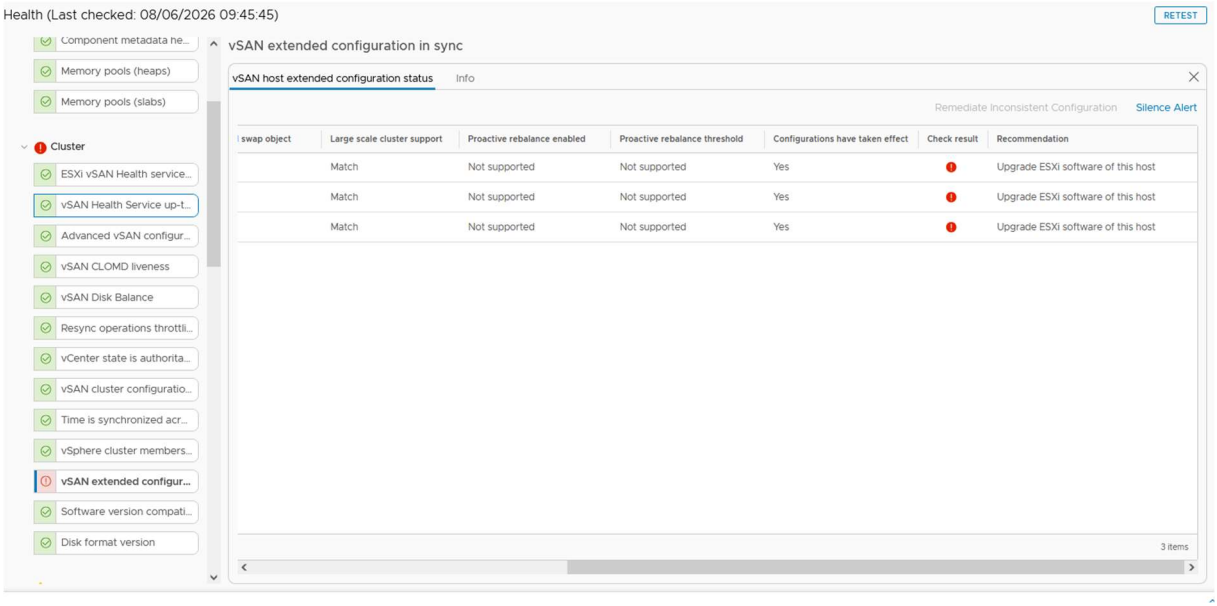
Dans un cluster à trois nœuds, cette stratégie implique qu'une maintenance ou une panne d'hôte doit être abordée avec prudence, surtout lorsque le datastore est déjà utilisé à plus de 90 %. Le cluster doit conserver suffisamment de ressources et d'espace pour maintenir l'accessibilité des objets et éviter de dégrader davantage la situation.

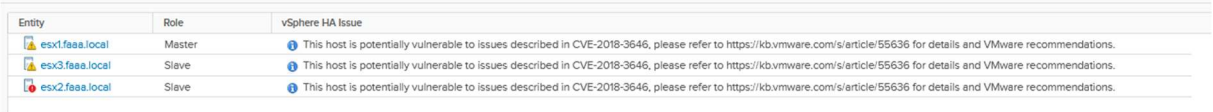
6.4 Alertes vCenter et vSAN Health

Les alertes remontées par vCenter concernent principalement :

- Les défauts de batterie des contrôleurs RAID
- L'obsolescence de la version VMware
- Les alertes de capacité disque vSAN
- Les configurations vSAN nécessitant une montée de version ESXi
- Certains avertissements de sécurité liés à la plateforme VMware
- Des alertes de consommation mémoire.







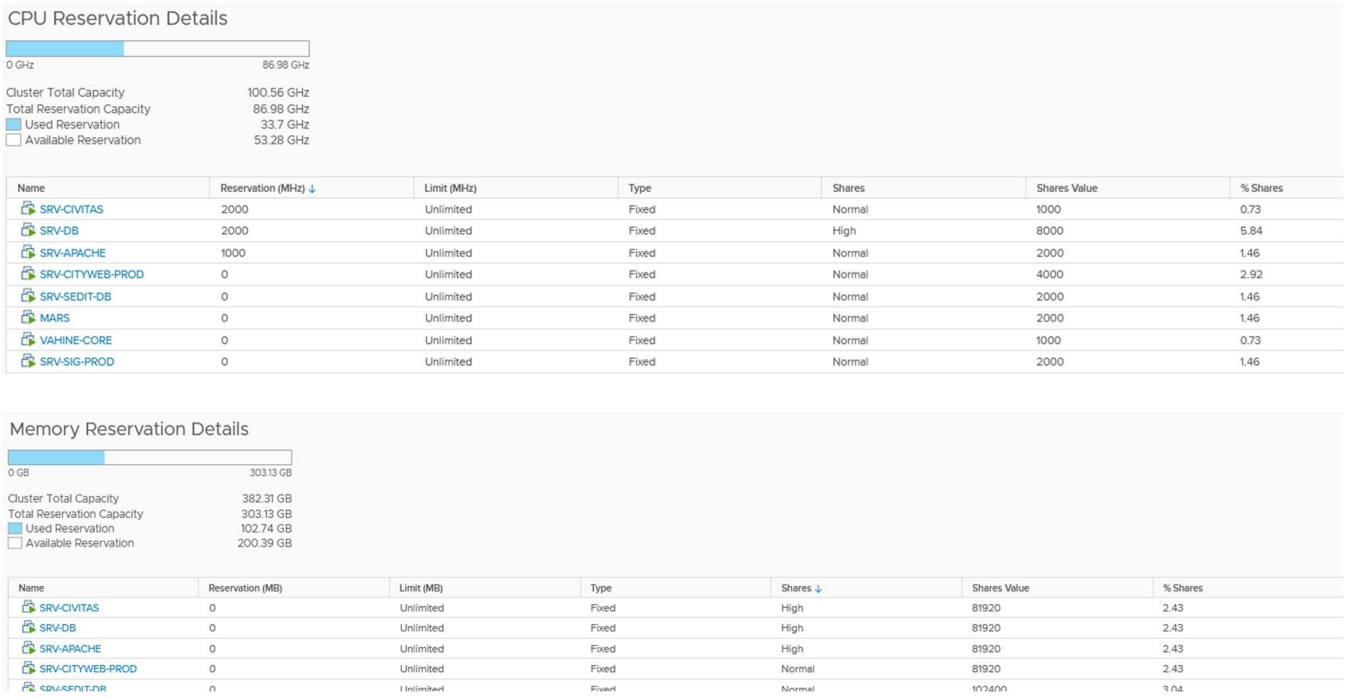
Les alertes mémoire semblent notamment liées à la volonté initiale du client de déplacer les machines virtuelles hébergées sur le serveur ayant remonté l'alerte batterie vers les deux autres nœuds.

Cependant, dans le contexte observé, cette approche ne traite pas le problème de fond. Le stockage étant distribué via vSAN, et les trois serveurs présentant le même type de défaut batterie, déplacer les machines virtuelles d'un nœud vers les deux autres ne suppriment pas le risque. Cela peut même augmenter la pression sur les ressources restantes.

6.5 Configurations historiques observées

L'audit a permis d'identifier certaines configurations probablement historiques qui ne semblent plus justifiées aujourd'hui.

Certaines machines virtuelles disposent notamment de réservations CPU ou de priorisations mémoire. Ces paramètres peuvent avoir été mis en place pour répondre à un besoin ponctuel, mais ils doivent être réévalués. Dans un environnement contraint en mémoire et en stockage, des réservations non justifiées peuvent limiter la capacité de répartition des ressources par VMware et compliquer les opérations de maintenance.



CPU Reservation Details

0 GHz — 86.98 GHz

Cluster Total Capacity	100.56 GHz
Total Reservation Capacity	86.98 GHz
Used Reservation	33.7 GHz
Available Reservation	53.28 GHz

Name	Reservation (MHz)	Limit (MHz)	Type	Shares	Shares Value	% Shares
SRV-CIVITAS	2000	Unlimited	Fixed	Normal	1000	0.73
SRV-DB	2000	Unlimited	Fixed	High	8000	5.84
SRV-APACHE	1000	Unlimited	Fixed	Normal	2000	1.46
SRV-CITYWEB-PROD	0	Unlimited	Fixed	Normal	4000	2.92
SRV-SEDIT-DB	0	Unlimited	Fixed	Normal	2000	1.46
MARS	0	Unlimited	Fixed	Normal	2000	1.46
VAHINE-CORE	0	Unlimited	Fixed	Normal	1000	0.73
SRV-SIG-PROD	0	Unlimited	Fixed	Normal	2000	1.46

Memory Reservation Details

0 GB — 303.13 GB

Cluster Total Capacity	382.31 GB
Total Reservation Capacity	303.13 GB
Used Reservation	102.74 GB
Available Reservation	200.39 GB

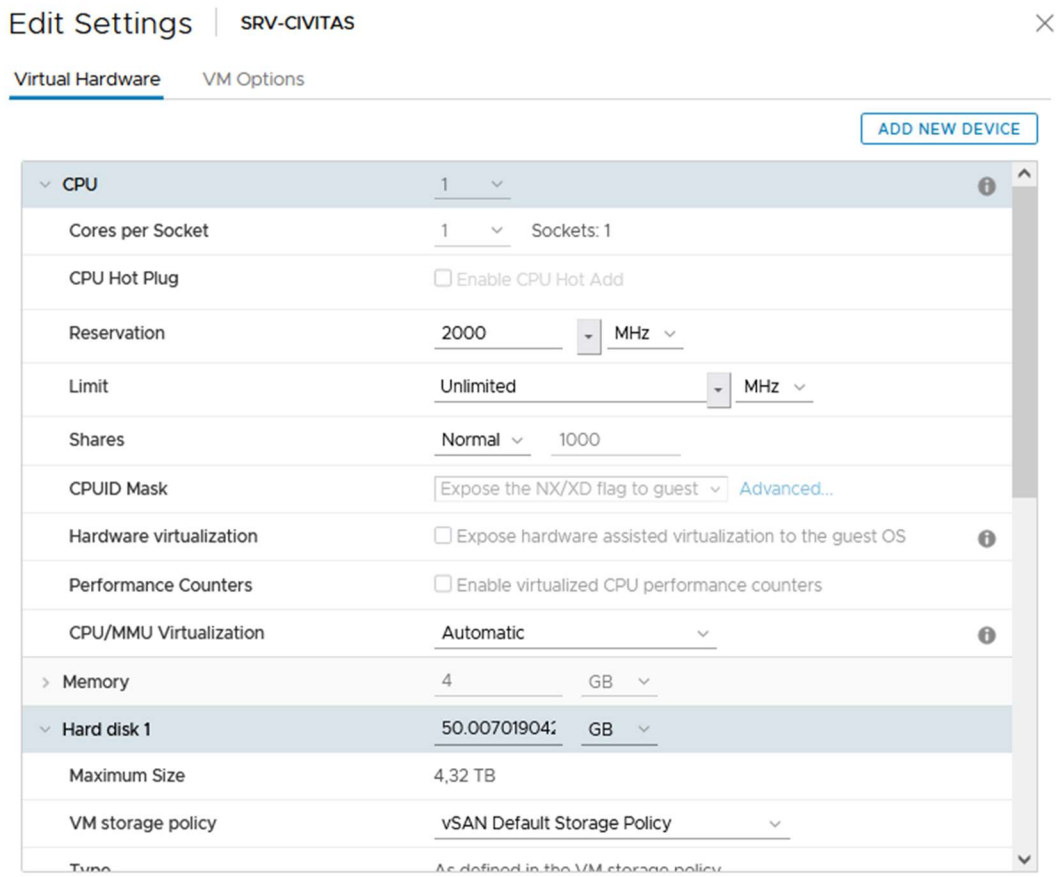
Name	Reservation (MB)	Limit (MB)	Type	Shares	Shares Value	% Shares
SRV-CIVITAS	0	Unlimited	Fixed	High	81920	2.43
SRV-DB	0	Unlimited	Fixed	High	81920	2.43
SRV-APACHE	0	Unlimited	Fixed	High	81920	2.43
SRV-CITYWEB-PROD	0	Unlimited	Fixed	Normal	81920	2.43
SRV-SEDIT-DB	0	Unlimited	Fixed	Normal	102400	3.04

Il est recommandé de revoir ces paramètres machine par machine et de supprimer les réservations qui ne sont plus nécessaires.

6.6 Taille des disques virtuels

Certaines machines virtuelles disposent de disques virtuels dont la taille présente plusieurs chiffres après la virgule.

Il est recommandé d'utiliser des tailles entières pour les disques virtuels, notamment afin d'éviter des interprétations incorrectes ou des comportements inattendus avec certains outils de sauvegarde, dont Veeam.



Si une correction est appliquée, la taille devra être arrondie au nombre entier supérieur. Il n'est pas possible de réduire simplement la taille d'un disque virtuel sans opération spécifique de migration ou de reconstruction.

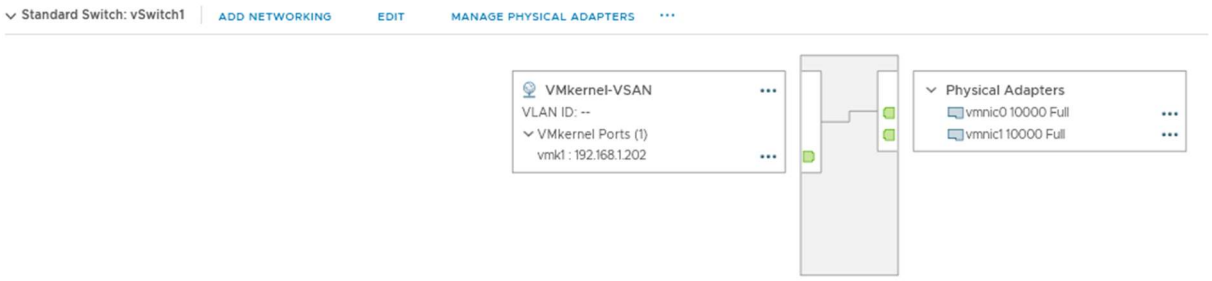
Cette correction doit donc être planifiée avec précaution.

7. ANALYSE RESEAU

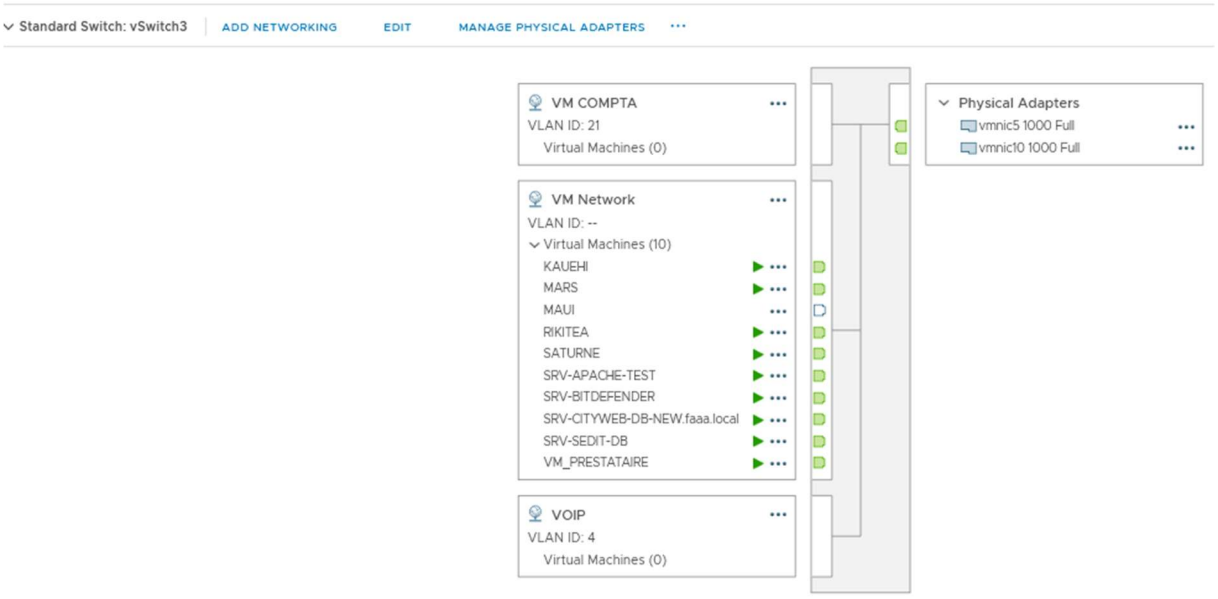
7.1 Réseau vSAN et réseau des machines virtuelles

Les hôtes disposent d'une séparation physique en sortie de serveur :

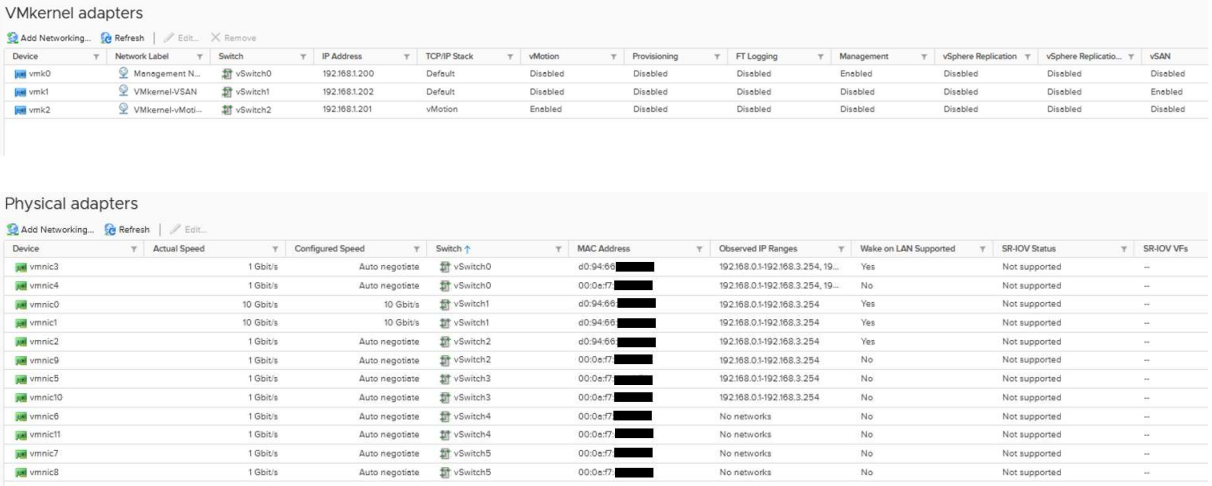
- Deux liens physiques SFP+ 10 Gb pour la fabric de stockage vSAN, rattachés au vSwitch 1



- Deux liens cuivre Base-T 1 Gb pour le réseau des machines virtuelles.



Cette séparation au niveau des hôtes est positive.


VMkernel adapters

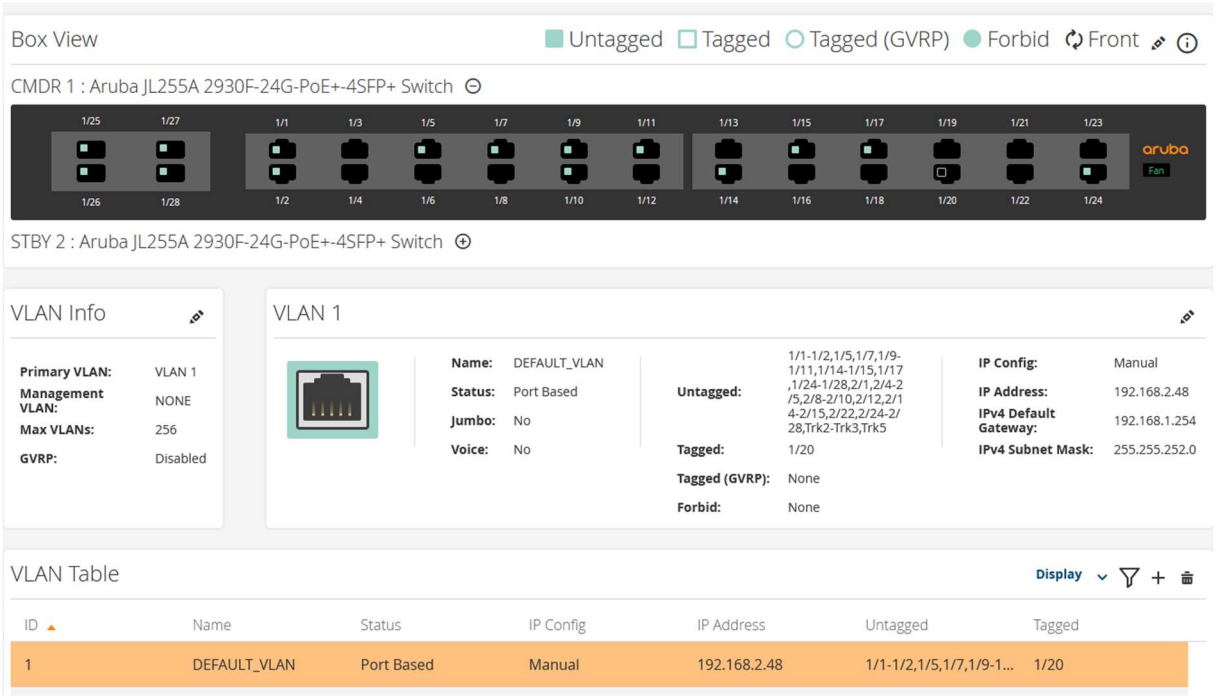
Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion	Provisioning	FT Logging	Management	vSphere Replication	vSphere Replicatio...	vSAN
vmk0	Management N...	vSwitch0	192.168.1.200	Default	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
vmk1	VMkernel-VSAN	vSwitch1	192.168.1.202	Default	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
vmk2	VMkernel-vMoti...	vSwitch2	192.168.1.201	vMotion	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Physical adapters

Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP Ranges	Wake on LAN Supported	SR-IOV Status	SR-IOV VFs
vmnic3	1 Gbit/s	Auto negotiate	vSwitch0	d0:94:66[redacted]	192.168.0.1-192.168.3.254, 19...	Yes	Not supported	--
vmnic4	1 Gbit/s	Auto negotiate	vSwitch0	00:0e:f7[redacted]	192.168.0.1-192.168.3.254, 19...	No	Not supported	--
vmnic0	10 Gbit/s	10 Gbit/s	vSwitch1	d0:94:66[redacted]	192.168.0.1-192.168.3.254	Yes	Not supported	--
vmnic1	10 Gbit/s	10 Gbit/s	vSwitch1	d0:94:66[redacted]	192.168.0.1-192.168.3.254	Yes	Not supported	--
vmnic2	1 Gbit/s	Auto negotiate	vSwitch2	d0:94:66[redacted]	192.168.0.1-192.168.3.254	Yes	Not supported	--
vmnic9	1 Gbit/s	Auto negotiate	vSwitch2	00:0e:f7[redacted]	192.168.0.1-192.168.3.254	No	Not supported	--
vmnic5	1 Gbit/s	Auto negotiate	vSwitch3	00:0e:f7[redacted]	192.168.0.1-192.168.3.254	No	Not supported	--
vmnic10	1 Gbit/s	Auto negotiate	vSwitch3	00:0e:f7[redacted]	192.168.0.1-192.168.3.254	No	Not supported	--
vmnic6	1 Gbit/s	Auto negotiate	vSwitch4	00:0e:f7[redacted]	No networks	No	Not supported	--
vmnic11	1 Gbit/s	Auto negotiate	vSwitch4	00:0e:f7[redacted]	No networks	No	Not supported	--
vmnic7	1 Gbit/s	Auto negotiate	vSwitch5	00:0e:f7[redacted]	No networks	No	Not supported	--
vmnic8	1 Gbit/s	Auto negotiate	vSwitch5	00:0e:f7[redacted]	No networks	No	Not supported	--

Cependant, les flux convergent ensuite vers un stack de switchs Aruba JL255A 2930F 24G-PoE+ 4SFP+. Il n'existe donc pas de séparation physique complète au niveau de la couche switch.

De plus, le réseau de stockage vSAN et le réseau utilisateur semblent être configurés sur le même VLAN. Ce point est problématique.

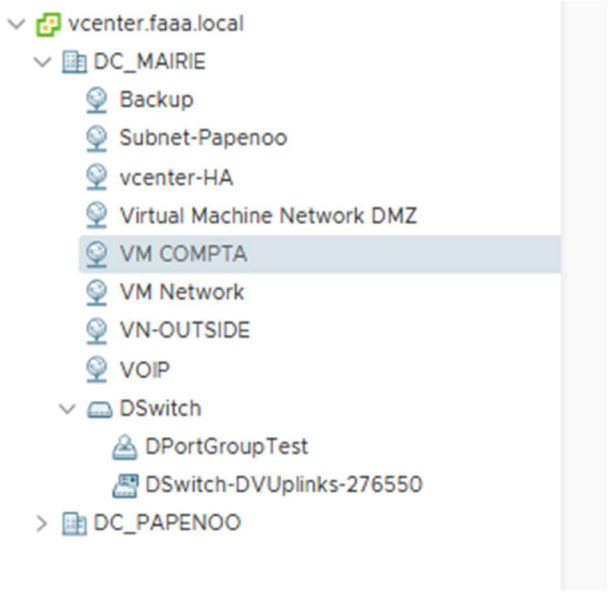


Le réseau vSAN doit être isolé afin d'éviter toute pollution croisée entre les flux utilisateurs, les flux serveurs et les flux de stockage. Dans une architecture vSAN, le réseau est un composant critique. Une saturation, une mauvaise priorisation ou une mauvaise configuration peut provoquer des ralentissements, des erreurs de synchronisation ou des comportements instables.

Il est donc recommandé de séparer le réseau vSAN dans un VLAN dédié, voire idéalement sur une infrastructure réseau dédiée ou fortement isolée selon les contraintes du client.

7.2 VSwitch locaux et absence de vSwitch distribué

Il a été constaté que les réseaux virtuels semblent configurés via des vSwitch locaux par hôte, et non via un vSwitch distribué.



Cette configuration fonctionne, mais elle présente des limites d'exploitation. Lorsqu'un nouveau réseau doit être créé, il est nécessaire de le créer manuellement sur chaque hôte du cluster. Dans le cas présent, cela implique de répéter l'opération trois fois.

Cette approche augmente le risque d'erreur de configuration, notamment en cas d'écart de nommage, de VLAN ID, de teaming ou de politique réseau entre les hôtes.

Dans un cluster VMware, l'utilisation d'un vSwitch distribué permettrait de centraliser la configuration réseau, de réduire le risque d'écart entre hôtes et de simplifier l'administration.

8. ANALYSE SAUVEGARDE ET REPLICATION

8.1 Version Veeam

Le serveur de sauvegarde utilise Veeam Backup & Replication en version 11.



Une mise à jour de Veeam pourrait être pertinente afin de bénéficier des corrections, améliorations et évolutions fonctionnelles des versions plus récentes.

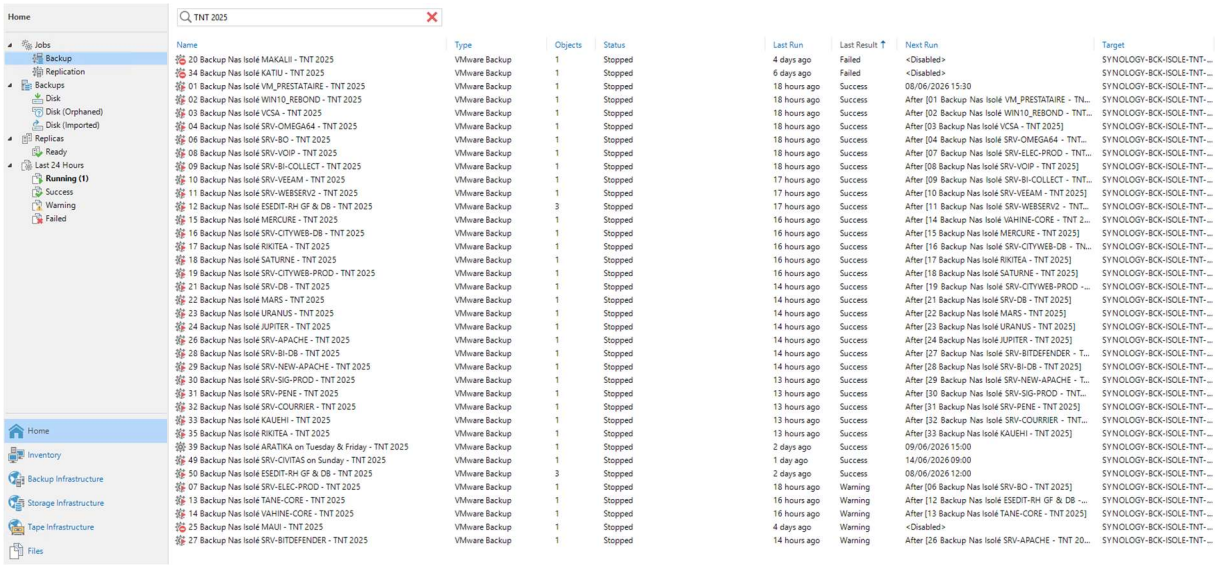
Toutefois, cette mise à jour doit être étudiée avec prudence, car l'environnement VMware source est en ESXi 6.5. Il est donc nécessaire de vérifier la compatibilité entre la version cible de Veeam et la version VMware actuellement utilisée.

Il ne faut pas moderniser Veeam sans vérifier la rétrocompatibilité avec l'environnement existant. Une mise à jour de Veeam sans validation préalable de la compatibilité avec l'environnement VMware existant pourrait introduire de nouveaux risques d'exploitation.

8.2 État général des sauvegardes

Les sauvegardes semblent globalement fonctionnelles.

Cependant, plusieurs optimisations peuvent être envisagées, notamment le regroupement des machines virtuelles de même type dans des jobs cohérents afin de mieux bénéficier de l'effet de déduplication.



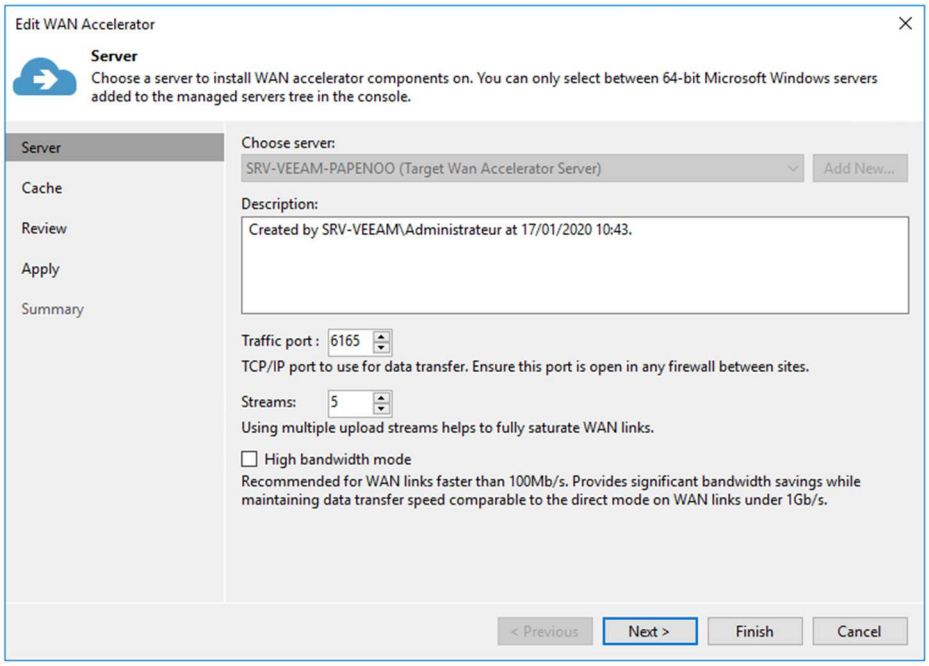
Avant toute opération matérielle ou logicielle sur l'infrastructure vSAN, le client doit disposer :

- D'une sauvegarde récente et valide de l'ensemble de l'infrastructure
- D'une réplication fonctionnelle des machines virtuelles critiques
- D'une capacité de restauration vérifiée
- D'une visibilité claire sur les échecs éventuels de sauvegarde ou de réplication.

Dans le contexte actuel, toute intervention sur les hôtes doit être conditionnée à la validation préalable de la sauvegarde et de la réplication.

8.3 Réplication vers Papenoo

Le système de réplication utilise la technologie WAN Accelerator afin d'envoyer les données vers un datacenter situé à Papenoo.



Ce choix est pertinent dans un contexte de réplication distante, car le WAN Accelerator permet d'optimiser les transferts sur des liens distants ou contraints.

La réplication semble fonctionnelle en partie, mais certains jobs présentent des échecs. Ces échecs devront être analysés et corrigés avant toute opération à risque sur l'infrastructure de production.

Name	Type	Objects	Status	Last Run	Last Result	Next Run ↑	Target
010 Replication SRV-ESEDIT Papenoo	VMware Replication	1	Stopped	4 days ago	Failed	<Disabled>	192.168.6.200
031 Replication SATURNE Papenoo	VMware Replication	1	Stopped			<Disabled>	192.168.6.200
034 Replication SRV-DCS Papenoo	VMware Replication	1	Stopped	9 days ago	Failed	<Disabled>	192.168.6.200
035 Replication SRV-CIVITAS Papenoo	VMware Replication	1	Stopped	8 days ago	Failed	<Disabled>	192.168.6.200
033 Replication KAUEHI Papenoo	VMware Replication	1	Stopped	2 days ago	Failed	13/06/2026 09:00	192.168.6.200
002 Replication MARS Papenoo	VMware Replication	1	Stopped	12 hours ago	Failed	After [001 Replication MAUI Papenoo]	192.168.6.200
003 Replication SRV-WEBSERVE2 Papenoo	VMware Replication	1	Stopped	12 hours ago	Success	After [002 Replication MARS Papenoo]	192.168.6.200
004 Replication SRV-ESEDIT-GF Papenoo	VMware Replication	1	Stopped	12 hours ago	Success	After [003 Replication SRV-WEBSERVE2 Papenoo]	192.168.6.200
005 Replication SRV-BI-DB Papenoo	VMware Replication	1	Stopped	12 hours ago	Success	After [004 Replication SRV-ESEDIT-GF Papenoo]	192.168.6.200
006 Replication SRV-BI-COLLECT Papenoo	VMware Replication	1	Stopped	11 hours ago	Success	After [005 Replication SRV-BI-DB Papenoo]	192.168.6.200
007 Replication SRV-ESEDIT-DB Papenoo	VMware Replication	1	Stopped	11 hours ago	Success	After [006 Replication SRV-BI-COLLECT Papenoo]	192.168.6.200
008 Replication SRV-ESEDIT-RH Papenoo	VMware Replication	1	Stopped	8 hours ago	Success	After [007 Replication SRV-ESEDIT-DB Papenoo]	192.168.6.200
009 Replication RIKITEA Papenoo	VMware Replication	1	Stopped	7 hours ago	Success	After [008 Replication SRV-ESEDIT-RH Papenoo]	192.168.6.200
011 Replication SRV-BO Papenoo	VMware Replication	1	Stopped	7 hours ago	Success	After [009 Replication RIKITEA Papenoo]	192.168.6.200
012 Replication SRV-SEDIT-DB Papenoo	VMware Replication	1	Stopped	7 hours ago	Success	After [011 Replication SRV-BO Papenoo]	192.168.6.200
013 Replication SRV-OMEGA64 Papenoo	VMware Replication	1	Stopped	7 hours ago	Success	After [012 Replication SRV-SEDIT-DB Papenoo]	192.168.6.200
014 Replication SRV-DB Papenoo	VMware Replication	1	Stopped	6 hours ago	Success	After [013 Replication SRV-OMEGA64 Papenoo]	192.168.6.200
015 Replication SRV-APACHE Papenoo	VMware Replication	1	Stopped	6 hours ago	Success	After [014 Replication SRV-DB Papenoo]	192.168.6.200
016 Replication SRV-BITDEFENDER Papenoo	VMware Replication	1	Stopped	6 hours ago	Failed	After [015 Replication SRV-APACHE Papenoo]	192.168.6.200
017 Replication SRV-COURRIER Papenoo	VMware Replication	1	Stopped	6 hours ago	Success	After [016 Replication SRV-BITDEFENDER Papeno...	192.168.6.200
018 Replication SRV-ELEC-PROD Papenoo	VMware Replication	1	Stopped	5 hours ago	Success	After [017 Replication SRV-COURRIER Papenoo]	192.168.6.200
019 Replication SRV-CITYWEB-PROD Papenoo	VMware Replication	1	Stopped	5 hours ago	Success	After [018 Replication SRV-ELEC-PROD Papenoo]	192.168.6.200
020 Replication SRV-CITYWEB-DB Papenoo	VMware Replication	1	Stopped	3 hours ago	Success	After [019 Replication SRV-CITYWEB-PROD Pape...	192.168.6.200
021 Replication SRV-VOIP Papenoo	VMware Replication	1	Stopped	3 hours ago	Success	After [020 Replication SRV-CITYWEB-DB Papenoo]	192.168.6.200
022 Replication VCSA Papenoo	VMware Replication	1	Stopped	3 hours ago	Success	After [021 Replication SRV-VOIP Papenoo]	192.168.6.200
023 Replication SRV-NEW-APACHE Papenoo	VMware Replication	1	Stopped	2 hours ago	Success	After [022 Replication VCSA Papenoo]	192.168.6.200
024 Replication SRV-SIG-PROD Papenoo	VMware Replication	1	Stopped	1 hour ago	Success	After [023 Replication SRV-NEW-APACHE Papeno...	192.168.6.200
025 Replication SRV-PENE Papenoo	VMware Replication	1	Stopped	1 hour ago	Success	After [024 Replication SRV-SIG-PROD Papenoo]	192.168.6.200
026 Replication TANE-CORE Papenoo	VMware Replication	1	Stopped	1 hour ago	Success	After [025 Replication SRV-PENE Papenoo]	192.168.6.200
027 Replication VAHINE-CORE Papenoo	VMware Replication	1	Stopped	1 hour ago	Success	After [026 Replication TANE-CORE Papenoo]	192.168.6.200
028 Replication JUPITER Papenoo	VMware Replication	1	Stopped	44 minutes ago	Success	After [027 Replication VAHINE-CORE Papenoo]	192.168.6.200
029 Replication URANUS Papenoo	VMware Replication	1	6% completed at...	10 minutes ago		After [028 Replication JUPITER Papenoo]	192.168.6.200
030 Replication MERCURE Papenoo	VMware Replication	1	Stopped	1 day ago	Failed	After [029 Replication URANUS Papenoo]	192.168.6.200
032 Replication WIN10_REBOND	VMware Replication	1	Stopped	2 days ago	Failed	After [033 Replication KAUEHI Papenoo]	192.168.6.200
001 Replication MAUI Papenoo	VMware Replication	1	Stopped	13 hours ago	Success	After [35 Backup Nas Isolé RIKITEA - TNT 2025]	192.168.6.200

8.4 Dépôts de sauvegarde

Des incohérences d'affichage ont été constatées sur certains dépôts de sauvegarde. Certains repositories affichent un espace utilisé supérieur à la capacité réelle disponible.

Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	SRV-VEEAM	C:\Backup	99,5 GB	28,2 GB	0 B	Created by Veeam Backup
NAS-PAPENOO	SMB	SRV-VEEAM-PAPENOO	\\192.168.6.202\VEEAM-VM	14 TB	3,6 TB	86 GB	Created by SRV-VEEAM\Administrateur at 08/01/2...
SYNOLOGY-BCK-ISOLEE	SMB	SRV-VEEAM	\\192.168.30.2\veeam	20,9 TB	3,4 TB	103,5 GB	NAS RS1221+
SYNOLOGY-BCK-ISOLEE-2	SMB	SRV-VEEAM	\\192.168.30.2\veeam	20,9 TB	3,4 TB	0 B	Created by SRV-VEEAM\veeam at 08/01/2024 11:00.
SYNOLOGY-BCK-ISOLEE-3	SMB	SRV-VEEAM	\\192.168.30.2\veeambck	20,9 TB	3,4 TB	4,3 TB	Created by SRV-VEEAM\veeam at 08/01/2024 11:10.
SYNOLOGY-BCK-ISOLE-TNT-2025	SMB		\\192.168.30.3\veeambck\	41,9 TB	31 TB	1,3 PB	Created by SRV-VEEAM\jpoetai-veeam at 23/07/2...
test	SMB		\\192.168.30.2\veeam\13 Backup Nas Is...	20,9 TB	3,4 TB	0 B	Created by SRV-VEEAM\veeam at 14/12/2022 08:19.

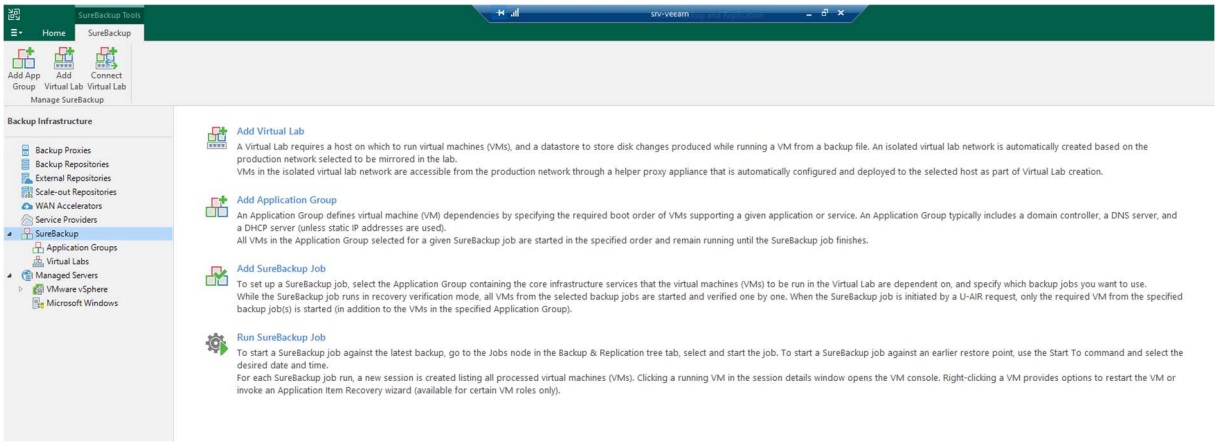
Ce comportement doit être analysé, notamment si une refonte du système de sauvegarde est envisagée. L'ensemble des stockages de sauvegarde est actuellement présenté par un NAS Synology en SMB. Cette configuration fonctionne, mais elle laisse Veeam dépendre du système de fichiers du NAS pour le stockage des sauvegardes.

Une alternative consisterait à présenter le stockage au serveur Veeam en iSCSI. Le serveur Windows hébergeant Veeam pourrait alors formater le volume en ReFS, ce qui permettrait potentiellement d'améliorer les performances et d'optimiser l'espace grâce aux mécanismes propres à ReFS, notamment dans le cadre des sauvegardes synthétiques et des blocs clonés.

Cette évolution devra toutefois être étudiée et testée avant mise en production.

8.5 SureBackup non exploité

Le client dispose d'une licence Veeam Enterprise Plus, mais la fonctionnalité SureBackup n'est pas exploitée.



SureBackup permet de tester automatiquement la restauration de machines virtuelles dans un environnement isolé afin de vérifier que les sauvegardes sont exploitables.

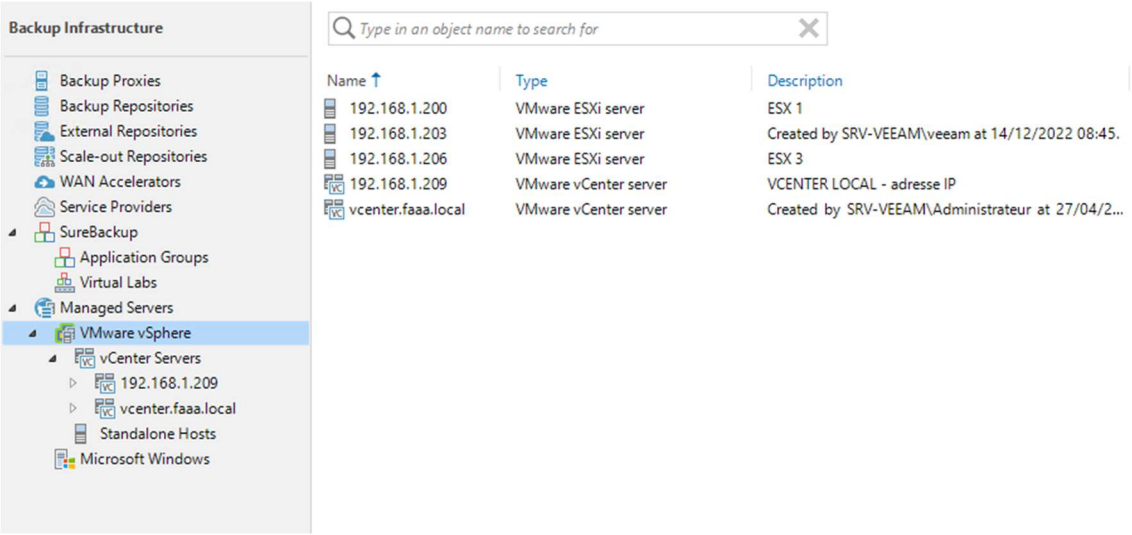
Dans le contexte actuel, les ressources disponibles sur le cluster VMware sont limitées, notamment en raison de la forte consommation mémoire et stockage. La mise en place d'un Virtual Lab complet avec Application Groups pourrait donc être restreinte.

Cependant, une approche progressive reste envisageable. En regroupant les machines virtuelles de même type dans des jobs cohérents, il serait possible de tester au moins une machine représentative par job. L'objectif serait de valider que les fichiers de sauvegarde VBK ou VIB sont exploitables.

Cette démarche permettrait d'améliorer la confiance dans la sauvegarde sans nécessairement consommer des ressources importantes.

8.6 Déclaration du vCenter dans Veeam

Il a été constaté que le vCenter est déclaré à la fois en adresse IP et en FQDN dans les serveurs managés Veeam.



Le client indique que cette configuration a été mise en place à la suite d'un problème ponctuel de résolution DNS.

Toutefois, cette approche n'est pas recommandée. Elle peut créer des doublons de configuration et des comportements ambigus dans Veeam. De plus, ce fonctionnement avec double déclaration est déprécié dans les versions récentes de Veeam.

La bonne pratique consisterait à corriger la résolution DNS ou, à défaut, à renseigner une entrée appropriée dans le fichier hosts du serveur Windows hébergeant Veeam. Cela permettrait de conserver une seule déclaration cohérente du vCenter dans Veeam.

9. RISQUES IDENTIFIES

Les principaux risques identifiés sont les suivants :

- Défaut batterie sur les contrôleurs RAID des trois serveurs
- Firmware contrôleur RAID fortement obsolète
- BIOS et iDRAC fortement obsolètes
- Disques Toshiba participant au vSAN avec mise à jour firmware recommandée
- Serveurs hors support constructeur depuis février 2021
- Version VMware ESXi 6.5 obsolète
- Datastore vSAN utilisé à plus de 90 %
- Capacité limitée à mettre un hôte en maintenance sans arrêt préalable de machines virtuelles
- Alertes vSAN Health liées à la capacité disque
- Opérations de rebalance fréquentes liées au manque d'espace
- Réseau vSAN non isolé au niveau VLAN
- Absence apparente de vSwitch distribué
- Sauvegarde globalement fonctionnelle mais perfectible
- Réplication partiellement en échec
- SureBackup non exploité malgré une licence Enterprise Plus
- Incohérences d'affichage sur certains repositories Veeam
- Double déclaration du vCenter dans Veeam.

Infrastructure VMware vSAN – Analyse à la suite d'alertes matérielles et de supervision

Le tableau ci-dessous présente une synthèse priorisée des risques identifiés, de leur impact potentiel et des actions recommandées.

Risque identifié	Impact potentiel	Urgence	Action recommandée
Défaut batterie sur les contrôleurs RAID des trois serveurs	Dégradation du comportement du contrôleur, risque sur les écritures, instabilité potentielle du stockage local utilisé par vSAN	Critique	Remplacer les batteries hôte par hôte après validation des sauvegardes, réplications et état vSAN
Datastore vSAN utilisé à plus de 90 %	Difficulté à maintenir l'accessibilité des objets vSAN, impossibilité potentielle de mettre un hôte en maintenance, rebalance fréquente	Critique	Libérer de l'espace, identifier les VM non critiques, supprimer ou déplacer les données inutiles avant maintenance
Cluster limité à trois nœuds	Faible marge de manœuvre en cas de panne ou maintenance, résilience limitée pendant intervention	Critique	Préparer toute opération hôte par hôte, vérifier la politique vSAN et éviter toute intervention simultanée
Serveurs hors support constructeur	Accès incertain aux pièces, délai d'intervention allongé, absence d'assistance constructeur	Élevée	Vérifier la disponibilité des pièces, envisager renouvellement ou extension de support si possible
VMware ESXi 6.5 obsolète	Absence de support éditeur, vulnérabilités non corrigées, limites de compatibilité avec outils récents	Élevée	Étudier une trajectoire de montée de version ou de migration vers une plateforme supportée
Firmwares BIOS, iDRAC, PERC et disques obsolètes	Risques de bugs connus, incompatibilités, instabilité matérielle, difficultés de maintenance	Élevée	Planifier les mises à jour uniquement après validation compatibilité et sauvegarde complète
Réseau vSAN non isolé dans un VLAN dédié	Risque de perturbation des flux stockage par les flux utilisateurs ou serveurs	Élevée	Isoler le trafic vSAN dans un VLAN dédié, vérifier la configuration réseau sur chaque hôte
iDRAC non exploité durablement	Difficulté de diagnostic ou d'intervention distante en cas d'incident critique	Moyenne à élevée	Remettre les iDRAC en service dans un VLAN d'administration isolé et sécurisé
Réplication Veeam partiellement en échec	Reprise d'activité incertaine en cas d'incident majeur	Élevée	Corriger les jobs en échec et valider les VM critiques répliquées
Sauvegardes non testées automatiquement avec SureBackup	Incertitude sur l'exploitabilité réelle des sauvegardes	Moyenne	Mettre en place des tests SureBackup progressifs sur des VM représentatives
Double déclaration du vCenter dans Veeam	Risque de doublons, comportements ambigus, incompatibilité avec les versions récentes	Moyenne	Corriger la résolution DNS puis conserver une seule déclaration cohérente du vCenter
Repositories Veeam présentant des incohérences d'affichage	Mauvaise visibilité sur la capacité réelle, risque de saturation ou d'erreur d'exploitation	Moyenne	Analyser les repositories, vérifier les volumes NAS/SMB et étudier une évolution vers iSCSI/ReFS
Réservations CPU ou priorisations mémoire historiques	Répartition moins efficace des ressources, contraintes inutiles sur le cluster	Moyenne	Revoir les paramètres VM par VM et supprimer les réservations non justifiées
Tailles de disques virtuels atypiques avec décimales	Risque d'interprétation incorrecte par certains outils, notamment de sauvegarde	Faible à moyenne	Arrondir au supérieur lors d'une opération planifiée, sans réduction directe des disques

10. PHASES ENVISAGEABLES

L'objectif des phases présentées ci-dessous n'est pas de proposer plusieurs scénarios alternatifs, mais de définir une trajectoire progressive de traitement des risques identifiés.

Les actions doivent être menées par ordre de priorité, en commençant par les points les plus critiques pour la disponibilité immédiate de l'infrastructure, puis en poursuivant vers des actions de sécurisation, d'optimisation et, à terme, de renouvellement.

10.1 Distinction entre actions immédiates et actions à planifier

10.1.1 Actions immédiates recommandées

Les actions suivantes doivent être engagées en priorité, car elles conditionnent la sécurité de toute intervention sur l'infrastructure.

Avant toute opération sur les hôtes, il est nécessaire de valider l'état complet des sauvegardes et des réplications. Cette validation doit inclure l'identification des machines virtuelles critiques, la vérification des derniers points de restauration disponibles et la correction des jobs de réplication en échec.

L'état de santé vSAN doit être contrôlé avant chaque intervention. Il faut notamment vérifier les alertes critiques, l'état des objets, les éventuelles resynchronisations en cours, la capacité disponible et la possibilité réelle de placer un hôte en maintenance.

Le remplacement des batteries de contrôleur RAID doit ensuite être réalisé hôte par hôte, sans intervention simultanée sur plusieurs serveurs. Chaque opération doit être suivie d'un contrôle complet de l'état matériel, de l'état vSAN et de l'absence de resynchronisation anormale.

Compte tenu de l'utilisation du datastore vSAN à plus de 90 %, une libération d'espace doit être engagée dès que possible. Cela peut passer par la suppression de données inutiles, l'arrêt temporaire de certaines machines virtuelles non critiques, le déplacement de charges ou l'archivage de données anciennes. Cette saturation expose l'infrastructure à un risque accru lors des opérations de maintenance.

La réplication Veeam vers Papenoo doit également être fiabilisée avant toute opération structurante. Les jobs en échec doivent être analysés et corrigés afin de garantir une capacité de reprise minimale en cas d'incident. Enfin, les accès iDRAC doivent être remis en service de manière durable, mais uniquement dans un réseau d'administration dédié, isolé et contrôlé. Cela permettra de faciliter les futures opérations de diagnostic, de supervision matérielle et de maintenance distante.

10.1.2 Actions à ne pas réaliser immédiatement sans plan de maintenance

Les mises à jour firmware BIOS, iDRAC, contrôleur RAID et disques ne doivent pas être réalisées dans l'urgence. Même si elles sont recommandées à moyen terme, elles concernent des composants directement liés à la stabilité du stockage vSAN. Une mise à jour mal préparée pourrait introduire un risque supérieur au problème qu'elle cherche à corriger.

La montée de version VMware ne doit pas non plus être engagée sans étude préalable. L'environnement actuel repose sur ESXi 6.5, avec des serveurs hors support constructeur et des firmwares anciens. Il est donc nécessaire de vérifier la compatibilité matérielle, les chemins de mise à niveau possibles, les prérequis vCenter/ESXi, ainsi que la compatibilité avec Veeam.

La mise à jour de Veeam doit être étudiée en cohérence avec la version VMware cible. Une mise à jour de Veeam sans validation préalable de la compatibilité avec l'environnement ESXi existant pourrait créer des incompatibilités supplémentaires.

La refonte des repositories de sauvegarde, notamment une éventuelle migration de SMB vers iSCSI avec formatage ReFS côté serveur Windows, doit être testée avant mise en production. Cette évolution peut être pertinente, mais elle doit être planifiée avec une stratégie de migration et de retour arrière.

La séparation du réseau vSAN dans un VLAN dédié est recommandée, mais elle doit être préparée avec soin. Une erreur de VLAN, de MTU, de teaming ou de configuration vmkernel peut provoquer une perte de communication vSAN entre les hôtes. Cette action doit donc être documentée, testée et réalisée pendant une fenêtre de maintenance.

Enfin, toute réflexion de renouvellement ou de refonte de l'infrastructure doit faire l'objet d'une étude dédiée. Elle devra comparer le maintien en condition opérationnelle de l'existant, l'ajout de capacité, la migration vers une version VMware supportée, l'évolution de la sauvegarde et les alternatives possibles de virtualisation.

10.2 Phase 1 – Traitement de l'urgence matérielle

Cette première phase consiste à traiter prioritairement le défaut des batteries de contrôleur RAID sur les trois serveurs.

Il s'agit de l'action minimale à engager afin de réduire le risque immédiat pesant sur l'infrastructure vSAN. Le défaut étant présent sur les trois hôtes, il ne doit pas être considéré comme un incident isolé.

Cette phase doit inclure :

- La vérification de l'état de santé vSAN avant toute intervention
- La validation des sauvegardes et des réplications disponibles
- L'identification précise des pièces compatibles
- La préparation d'un mode opératoire d'intervention
- Le remplacement des batteries de contrôleur RAID hôte par hôte
- La mise en maintenance contrôlée de chaque hôte, selon les capacités réelles du cluster
- Le contrôle de l'état vSAN après chaque intervention
- La vérification de l'absence de resynchronisation ou d'alerte critique persistante après intervention

Compte tenu de l'utilisation du datastore vSAN à plus de 90 %, cette phase doit être menée avec prudence. La mise en maintenance d'un hôte avec l'option "Ensure Accessibility" peut être difficile, voire impossible, sans arrêt préalable de certaines machines virtuelles ou libération d'espace.

Cette phase ne traite pas les risques structurels liés à l'obsolescence VMware, au manque d'espace vSAN, aux firmwares anciens, au réseau ou à la sauvegarde. Elle permet uniquement de réduire le risque matériel immédiat.

10.3 Phase 2 – Sécurisation de l'exploitation

Cette deuxième phase vise à sécuriser l'exploitation quotidienne de l'infrastructure après traitement de l'urgence matérielle.

Elle a pour objectif de réduire les risques opérationnels identifiés pendant l'audit, sans engager immédiatement une refonte complète de l'infrastructure.

Cette phase doit inclure :

- La remise en service durable des interfaces iDRAC dans un VLAN d'administration isolé
- La documentation des accès d'administration matérielle
- La clarification de l'état réel des sauvegardes
- La correction des jobs de réplication en échec
- La vérification de la capacité de restauration des machines virtuelles critiques
- La suppression des réservations CPU non justifiées
- La suppression ou la révision des priorisations mémoire non nécessaires
- La revue des tailles de disques virtuels atypiques
- Le nettoyage de la configuration Veeam, notamment la double déclaration du vCenter en IP et en FQDN
- La correction de la résolution DNS du vCenter depuis le serveur Veeam
- La séparation du réseau vSAN dans un VLAN dédié
- La vérification des configurations réseau sur chaque hôte

Cette phase doit permettre de fiabiliser l'exploitation courante, de réduire les écarts de configuration et de mieux préparer les futures opérations de maintenance.

Elle constitue une étape importante avant toute action plus structurante, car il serait risqué d'engager une montée de version ou des mises à jour firmware sur une infrastructure dont la sauvegarde, la réplication, les accès d'administration ou les réseaux ne sont pas parfaitement maîtrisés.

10.4 Phase 3 – Remise à niveau progressive de l'infrastructure

Cette troisième phase consiste à engager une remise à niveau progressive de l'infrastructure, après traitement des urgences et sécurisation de l'exploitation.

Elle vise à réduire les risques techniques accumulés, notamment ceux liés aux versions anciennes des composants matériels et logiciels.

Cette phase doit inclure :

- L'étude d'une montée de version VMware
- La validation de la compatibilité matérielle Dell et VMware
- L'analyse détaillée des prérequis de mise à jour ESXi et vCenter
- L'étude des mises à jour BIOS
- L'étude des mises à jour iDRAC
- L'étude des mises à jour du contrôleur RAID PERC H730P
- L'étude des mises à jour firmware des disques participant au vSAN
- La vérification de la compatibilité entre la version cible de VMware et la version cible de Veeam
- L'étude d'une mise à jour de Veeam Backup & Replication
- L'optimisation ou la refonte des repositories de sauvegarde
- L'étude d'une présentation des stockages de sauvegarde en iSCSI avec formatage ReFS côté serveur Windows
- La mise en œuvre progressive de tests SureBackup sur des machines virtuelles représentatives
- L'amélioration de l'architecture réseau VMware, notamment l'étude d'un vSwitch distribué

Les mises à jour firmware des composants participant au vSAN doivent être considérées avec une attention particulière. Elles ne doivent pas être réalisées comme de simples opérations de maintenance standard, car les disques, contrôleurs et composants serveur participent directement à la stabilité du stockage distribué.

Cette phase nécessite donc un plan de maintenance détaillé, une validation des sauvegardes, une fenêtre d'intervention adaptée et une stratégie de retour arrière clairement définie.

10.5 Phase 4 – Renouvellement ou refonte de l'infrastructure

Cette quatrième phase consiste à envisager le renouvellement complet ou partiel de l'infrastructure.

Elle doit être étudiée lorsque les actions de correction, de sécurisation et de remise à niveau ne suffisent plus à garantir un niveau de risque acceptable, ou lorsque le coût de maintien en condition opérationnelle devient trop élevé par rapport à la valeur résiduelle de l'infrastructure.

Cette phase permettrait de traiter durablement les risques suivants :

- Serveurs hors support constructeur
- Version VMware obsolète
- Firmwares fortement anciens
- Capacité vSAN insuffisante
- Limites de maintenance liées à un cluster trois nœuds fortement consommé
- Dépendance à une architecture vieillissante
- Difficulté à garantir le support éditeur en cas d'incident majeur
- Besoin de modernisation de la sauvegarde
- Besoin d'une architecture réseau plus propre
- Nécessité de retrouver une marge d'évolution en capacité, performance et résilience

Cette phase devra faire l'objet d'une étude technique et budgétaire dédiée.

Elle pourra notamment comparer plusieurs orientations possibles :

- Renouvellement des serveurs existants
- Extension de capacité du cluster actuel, si techniquement et économiquement pertinente
- Migration vers une version VMware supportée
- Refonte de l'architecture vSAN
- Étude d'une alternative de virtualisation
- Refonte du système de sauvegarde et de réplication
- Amélioration de la segmentation réseau et de l'administration matérielle

Cette phase constitue la cible long terme. Elle ne remplace pas les actions urgentes des phases précédentes, mais permet de définir une trajectoire durable pour sortir progressivement d'une infrastructure vieillissante, fortement contrainte en capacité et limitée en support.

11. RECOMMANDATION FINALE

Au regard des constats réalisés, il est recommandé de ne pas traiter cet incident comme un simple remplacement de batterie de contrôleur RAID.

L'alerte initiale a révélé une situation plus large : les trois serveurs présentent le même type de défaut matériel, les firmwares critiques sont fortement obsolètes, l'environnement VMware repose sur une version ancienne, le vSAN est utilisé à plus de 90 %, et la capacité de mise en maintenance d'un hôte est fortement contrainte.

La priorité immédiate doit être la suivante :

1. Valider l'état complet des sauvegardes et des réplications
2. Identifier les machines virtuelles critiques
3. Libérer de l'espace sur le vSAN ou arrêter temporairement certaines machines virtuelles si nécessaire
4. Vérifier l'état de santé vSAN avant toute intervention
5. Remplacer les batteries des contrôleurs RAID hôte par hôte
6. Contrôler l'état du cluster après chaque opération
7. Corriger les échecs de réplication
8. Isoler le réseau vSAN dans un VLAN dédié
9. Remettre en service les iDRAC dans un réseau d'administration dédié
10. Définir une trajectoire de mise à niveau ou de renouvellement de l'infrastructure.

Les mises à jour firmware BIOS, iDRAC, contrôleur RAID et disques doivent être considérées comme nécessaires à moyen terme, mais elles ne doivent pas être réalisées sans plan de maintenance détaillé, validation de compatibilité et sauvegarde préalable.

La recommandation principale est donc d'adopter une approche progressive : traiter l'urgence matérielle, sécuriser l'exploitation, puis planifier une remise à niveau ou un renouvellement de l'infrastructure.

En l'état, la mise en maintenance d'un serveur physique ne doit pas être engagée sans préparation, car la saturation du vSAN et la taille réduite du cluster limitent fortement la marge de manœuvre.