Rapport de stage

Projet : Sauvegarde inaltérable des données du système d'information d'AG2R LA MONDIALE

Rapport rédiger et présenter par : TAMETCHOP TEMKOU Borel

Alternant chez AG2R LA MONDIALE

Sous la supervision de : **Yannick LAFOUCRIERE**

Expert système de stockage et sauvegarde distribués chez AG2R LA MONDIALE

Document confidentiel

SOMMAIRE

Introduction

Dans le cadre de notre formation et en tant qu'alternant, nous sommes partagés entre les enseignements à l'école et les enseignements en entreprise, ceci pour faciliter notre immersion dans le monde du travail. Pour mon alternance, j'ai intégré le groupe AG2R LA MONDIALE plus précisément la Direction de l'organisation des systèmes d'information au sein l'équipe Coordination SDI, Ressources IT et Orchestration en tant qu'assistant IT. Au cours de cette expérience professionnelle, j'ai travaillé sur la mise en place de l'infrastructure de sauvegarde inaltérable. Ce projet dont l'objectif est de mettre sur pied une infrastructure de stockage et sauvegarde isolée du reste du réseau et entièrement autonome constituera la pierre angulaire notre rapport.

1. Présentation de l'entreprise

AG2R LA MONDIALE est né de l'union de deux organismes de protection sociale et patrimoniale, La mondiale et AG2R. À la suite d'un rapprochement avec le groupe Réunica, spécialiste en retraite et prévoyance sociale, le groupe mutualiste AG2R LA MONDIALE REUNICA est devenu l'un des plus grands acteurs de la protection sociale et patrimoniale en France. Il se base sur son expertise et ses conseils pour permettre à chacun de mieux protéger sa vie et celle de ses proches tout en conjuguant responsabilités individuelles avec solidarités professionnelles et intergénérationnelles. Le groupe propose aux particuliers, aux indépendants et aux entreprises des solutions d'assurances de biens, la prévoyance santé, la retraite complémentaire, épargne.
L'engagement sociétal qui est la raison d'être du groupe s'articule autour de trois composantes du développement durable :

- L'efficacité économique : soutenir l'activité économique en investissant dans l'économie réelle au plus près des besoins des territoires, piloter son organisation financière dans une démarche d'investissement responsable ;
- Equité sociale : concentrer nos actions sur 4 axes prioritaires d'intervention : la prévention santé, l'habitat, le retour à l'emploi et l'aide aux aidants. Aider les personnes en difficulté par le versement d'aides individuelles et la contribution à des projets collectifs, aux côtés d'associations ;
- Durabilité environnementale : prendre en compte l'impact de nos actions et adopter des comportements éco-responsables ;
- Mobiliser pour accompagner : les actifs, retraités et particuliers, au quotidien et face aux difficultés. Les entreprises et les institutions dans leur appréhension de la santé, de l'absentéisme, de la qualité de vie au travail, du management des âges et du handicap de leurs salariés.

Pour cette alternance, j'ai été affecté à la direction de l'organisation et des systèmes d'information dont le rôle est d'accompagner l'entreprise dans sa vision stratégique en adaptant le système d'information à tous les métiers de l'entreprise. La DOSI est constituée de 6 directions à l'intérieur desquelles on retrouve des sous-directions et des équipes. J'ai intégré la direction Operations & Services IT, dans la sous-direction Infrastructures et Cloud et dans l'équipe Coordination SDI, Ressources IT & Orchestration**.** Cette équipe a pour rôle, le

maintien en condition opérationnelle et l'administration des infrastructures de stockage, de sauvegarde et de virtualisation du groupe AG2RLM, mais également de fournir une interface de provisionnement des ressources informatiques de cette infrastructure.

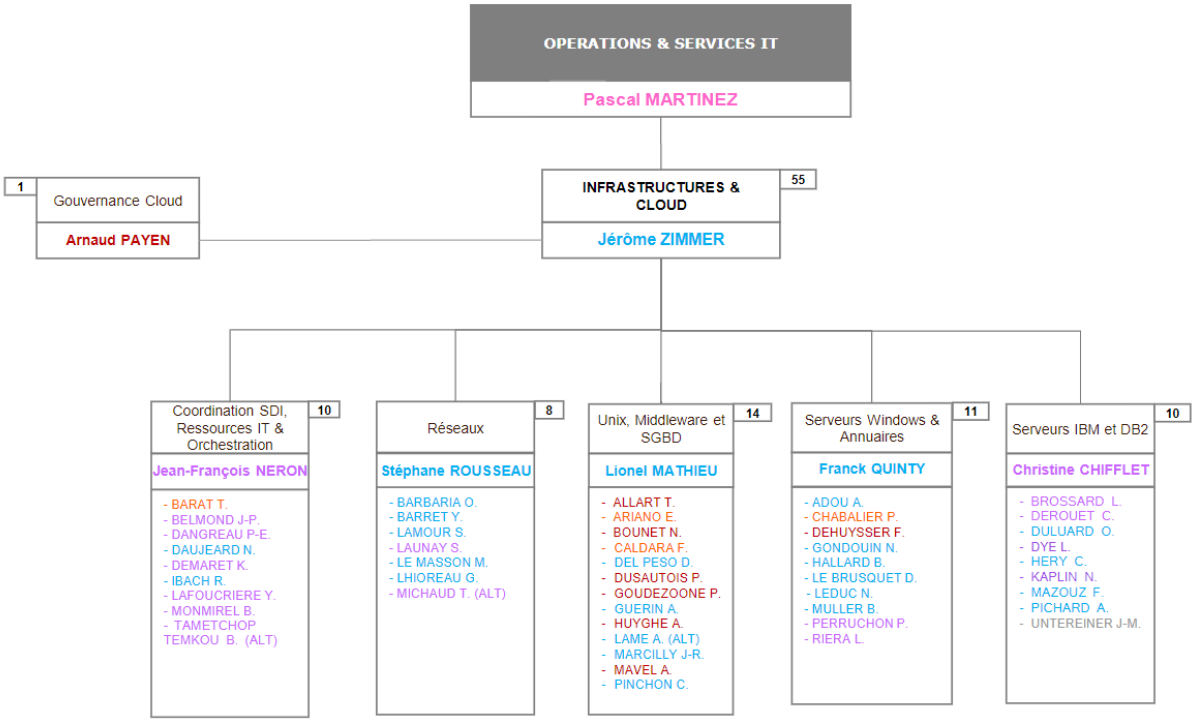


Figure 1: organigramme de la direction opérations & services IT

2. Contexte du projet

Face à l'augmentation des failles de sécurité et aux développements des attaques visant plus particulièrement l'intégrité et la disponibilité, il devient plus qu'important pour les entreprises d'améliorer de manière continue la sécurité de leurs systèmes d'information. AG2R LA MONDIALE en sa qualité d'OSE (entreprise fournissant des services nécessaires à l'activité économique et sociale de la nation) doit renforcer les mesures de sécurité sur ses différentes plateformes de production et de secours afin d'assurer une reprise d'activité en cas d'attaque informatique visant son système d'information. C'est dans c'est optique que naît le projet de sauvegarde inaltérable.

2.1 Les objectifs du projet

Ce projet vise à réduire l'impact d'une cyberattaque pouvant être décrit par les scénarios suivants :

- Un évènement redouté :
  - Perte d'intégrité seulement (ex : suppression en masse des données métiers et de leurs sauvegardes)
  - Perte d'intégrité et disponibilité (ex : rançongiciel propagé sur l'ensemble du SI)
- Une source de menace :
  - Externe (ex : hacktiviste, prestataire)
  - Interne (ex : salarié)
- Une nature d'attaque :
  - Logique (ex : intrusion par internet et mouvement latéral)
  - Physique (ex : incendie sur les locaux d'ALM)

3. Etude de l'existant

Le système d'information du groupe AG2R LA MONDIALE est subdivisé en deux parties, l'infrastructure nominale (de production) et l'infrastructure de PSI (de secours).

3.1 Infrastructure nominale

C'est l'infrastructure principale de collecte et de traitement, hébergeant les données actives utilisées par les applications métiers du groupe. Il est composé des baies de stockage, des systèmes de sauvegarde, des équipements réseaux d'interconnexion, des serveurs physiques et

virtuels. Il est subdivisé en deux régions indépendantes, disposant chacune de ses propres équipements. Les systèmes de sauvegarde et de stockage de chaque région disposent d'une copie des données actives. Les snapshots serveurs sont effectuées à un instant T afin de faire une restauration en cas de besoin. Aucune communication de type réplication des données n'est possible entre les deux zones.

3.2 Infrastructure PSI

Pour assurer une reprise d'activité en cas de sinistre, les données de production sont répliquées vers le deuxième data center qui est le plan de secours informatique (PSI) en cas de perte totale de l'infrastructure de production. Les données stockées proviennent des réplications asynchrones des infrastructures de sauvegarde et de stockage de production. Cette infrastructure est destinée à devenir nominale en cas de destruction totale des systèmes nominaux.

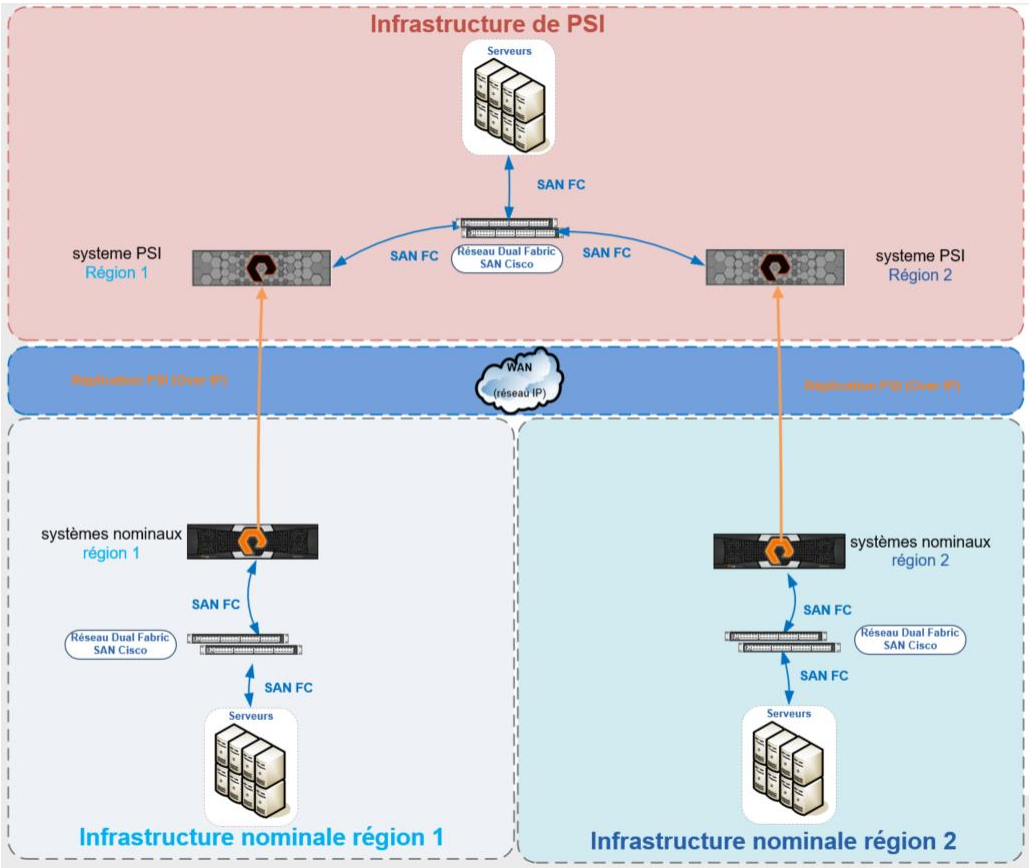


Figure 2 : Architecture du système de stockage initiale

4. Présentation du projet

Afin de se prémunir des ransomwares et tous autres pratiques pouvant mettre en péril l'intégrité des données, le groupe AG2R LAMONDIALE à lancer le projet de sauvegarde inaltérable. En plus des systèmes de sauvegarde et réplication des données de l'infrastructure nominale vers l'infrastructure de PSI, une troisième est infrastructure de PSI CYBER est mise en place pour apporter une couche supérieure de sécurité aux données de l'entreprise.

Le projet de sauvegarde inaltérable (PSI Cyber) consiste à mettre en place une infrastructure de sauvegarde et de stockage isolée du reste du réseau de l'entreprise. Entièrement automatisée, elle se connecte à l'infrastructure de PSI pour les réplications des données et se déconnecte de cette infrastructure une fois les processus terminés. Les processus de connexion au réseau de production et les réplications sont automatisés via des scripts PowerShell planifiés qui s'exécutent sur un serveur de pilotage qui se trouve dans la zone de PSI CYBER. Les résultats de l'exécution des scripts et logs des équipements sont transmis aux plateformes de supervision du réseau de production via une passerelle unidirectionnelle grâce à l'équipement data diode.

4.1 Développement du projet

Il consiste à présenter la méthodologie de gestion de projet utilisée ainsi les jalons du projet.

4.1.1 Méthode et outils utilisés

La sauvegarde inaltérable étant un projet interne de construction d'une plateforme automatisée et autonome de stockage et sauvegarde, il est question de faire des tests de fonctionnement à chaque étape de réalisation du projet, d'où l'utilisation de la méthode en V pour gérer le projet.

Une réunion de l'équipe de projet est organisée chaque mois afin de suivre la progression du projet et les points de blocage.

Une réunion hebdomadaire sur le stockage est tenue chaque mercredi, pendant laquelle on passe en revue, les tâches terminées et les tâches en cours.

4.1.2 Etapes du projet

La réalisation de ce projet a été défini selon les jalons suivants :

Jalons	Objectifs

Expression des besoins énoncée par La direction des risques opérationnels (DRO)	• Présenter les risques que pourrait subir AG2R LA MONDIALE en cas d'une cyberattaque (externe ou interne)
Définir les Scénarios de protection des données par la direction de l'organisation des systèmes d'information (DOSI)	• Proposer des solutions pour assurer la résilience du système d'information du groupe en cas d'attaque interne ou externe
Cadrage du projet	• Définir le périmètre du projet (couverture des risques, le type de données concernées) • Valider et définir les modalités d'exécution du projet • Chiffrage du projet • Lancer la communication du projet aux équipes

Tableau 1: les jalons du projet

4.2 Les missions réalisées

Durant la réalisation de ce projet, les tâches qui m'ont été confiées sont les suivantes :

Développement des scripts PowerShell :

- Script d'inventaire des baies de stockage pure Storage ;
- Script de vérification de destruction d'un volume ou Lun dans les baies ;
- Script de mise à jour des modules PowerShell ;
- Script de backup des configurations des switches LAN, SAN et des baies de stockages Pure Storage.

Rédaction des documentations de :

- Configuration du serveur de pilotage ;
- Configuration de l'équipement data diode ;
- Configuration du serveur NTP ;
- Maintien en condition opérationnelle de la plateforme de sauvegarde inaltérable ;
- Plan d'adressage IP des équipements de la plateforme de sauvegarde inaltérable.

Configuration des équipements :

- Data diode (configuration + installation) ;
- Serveur NTP (configuration + installation) ;
- Serveur de pilotage (configuration +installation) ;
- Baie de stockage Pure Storage (configuration) ;

5. Mise en place de l'infrastructure

Pour cette plateforme isolée du réseau de production, les équipements informatiques suivants ont été nécessaires pour sa conception :

- **Un serveur NTP orbitica** : c'est le serveur de temp de la plateforme, il est responsable de la synchronisation des horaires avec tous les équipements de la plateforme. Grâce à son antenne GPS, elle reçoit l'heure de référence depuis les satellites.

- **Les baies de stockage Pure Storage FlashArray** : ce sont les systèmes de stockage dans lesquels seront hébergés les copies des données. Ils sont constitués de disque SSD montés en Raid pour assurer la tolérance au panne mécanique.

- **Le serveur de pilotage** : c'est le serveur d'orchestration de la plateforme, il fonctionne avec le système d'exploitation Windows server 2019 et permet de gérer :
  - L'automation des taches de la plateforme via les scripts PowerShell grâce à son gestionnaire de tâche,
  - La collection des résultats de l'exécution des scripts PowerShell dans le répertoire d'envoi de la data diode
  - L'administration des équipements de la plateforme
  - La mise à jour de tous les composants matériels et logiciels de la plateforme

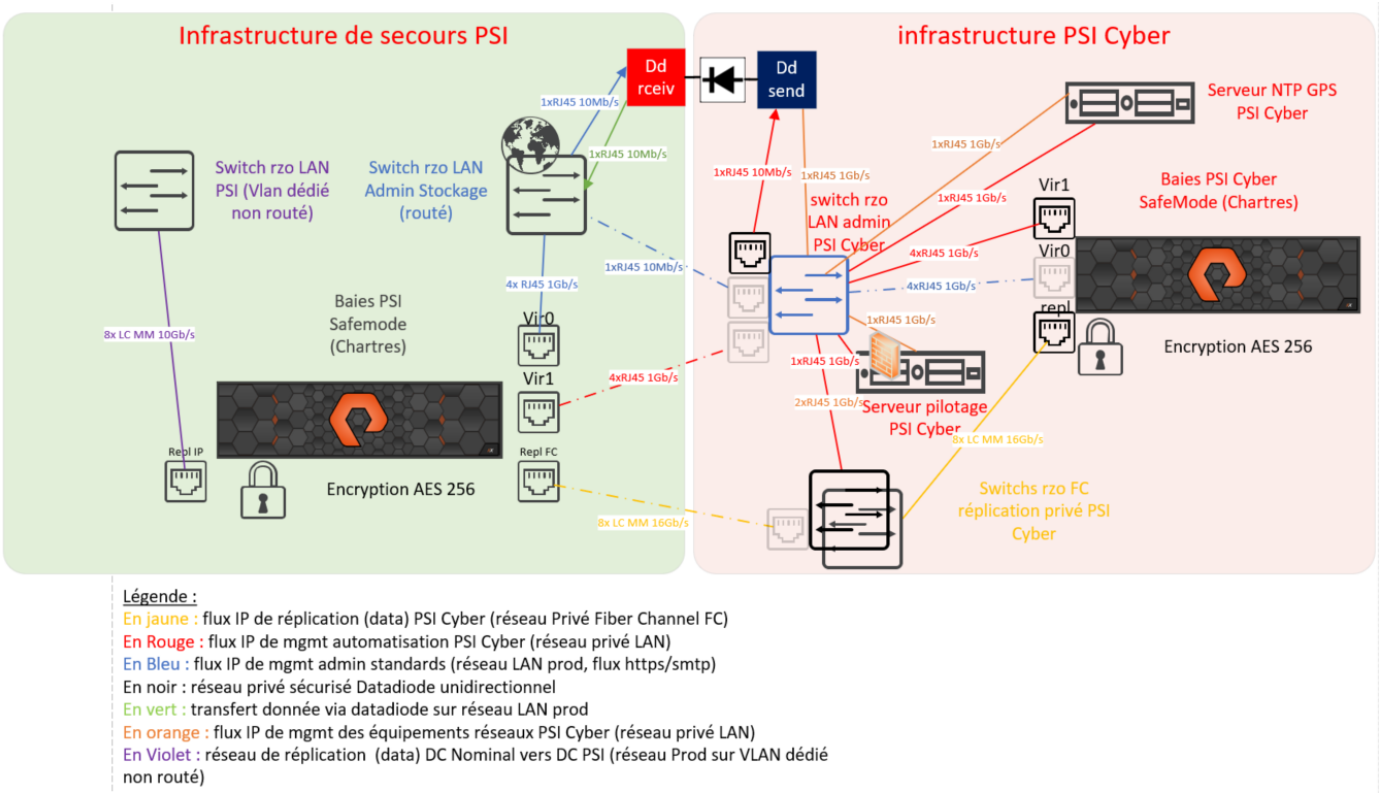
- **La data diode** : elle joue le rôle de passerelle unidirectionnelle entre le réseau de PSI CYBER et le réseau de production. Elle est composée de deux serveurs, l'un gère la transmission sur l'interface « Send » et l'autre gère la réception sur l'interface « Receive ». Son rôle est de transmettre le résultat des scripts d'automatisation, les logs des équipements et les notifications par mail vers les plateformes de supervision hors PSI Cyber.

- **Switches réseaux type SAN FC Cisco** : ce sont les équipements d'interconnexion réseau qui permettent le transfert des données en mode bloc en utilisant le protocole fiber channel pour liaison avec les baies de stockage. Ils sont montés sous forme de fabric pour assurer la haute disponibilité des équipements de stockage.

- **Switches réseaux type LAN Cisco :** ce sont les commutateurs de niveau deux qui interconnecte les équipements de la plateforme et gère les flux de données et de management**.**

- **Serveurs VMware ESXi :** c'est hyperviseur de niveau un qui héberge les serveurs de l'infrastructure de sauvegarde Commvault dédiée à la plateforme de sauvegarde inaltérable. Ces serveurs sont connectés au réseau de PSI et accèdent aux systèmes de stockage Pure Storage uniquement par le biais d'un réseau SAN (stockage de données) sans possibilité d'altérer les données sécurisées par les baies de stockage Pure Storage.

Tous ces équipements ont été interconnectés selon l'architecture suivante :



Légende :
En jaune : flux IP de réplication (data) PSI Cyber (réseau Privé Fiber Channel FC)
En Rouge : flux IP de mgmt automatisation PSI Cyber (réseau privé LAN)
En Bleu : flux IP de mgmt admin standards (réseau LAN prod, flux https/smtp)
En noir : réseau privé sécurisé Datadiode unidirectionnel
En vert : transfert donnée via datadiode sur réseau LAN prod
En orange : flux IP de mgmt des équipements réseaux PSI Cyber (réseau privé LAN)
En Violet : réseau de réplication (data) DC Nominal vers DC PSI (réseau Prod sur VLAN dédié non routé)

Figure : architecture de la plateforme de sauvegarde inaltérable

5.2 Transfert de données vers la plateforme inaltérable

Les données transférées proviennent des baies de stockage de l'infrastructure de PSI. Elles sont transférées via les mécanismes de réplications asynchrone entre baies de stockages de PSI et de PSI CYBER d'une part et d'autre part grâce aux mécanismes de dash copie entre le système de sauvegarde de nominale et celui de PSI CYBER. Ces opérations sont réalisées une fois par mois en se basant sur les dernières sauvegardes et snapshots du weekend.

5.2.1 Transfert de données pour les plateformes VMware utilisant le système de fichier VMFS et IBM AIX

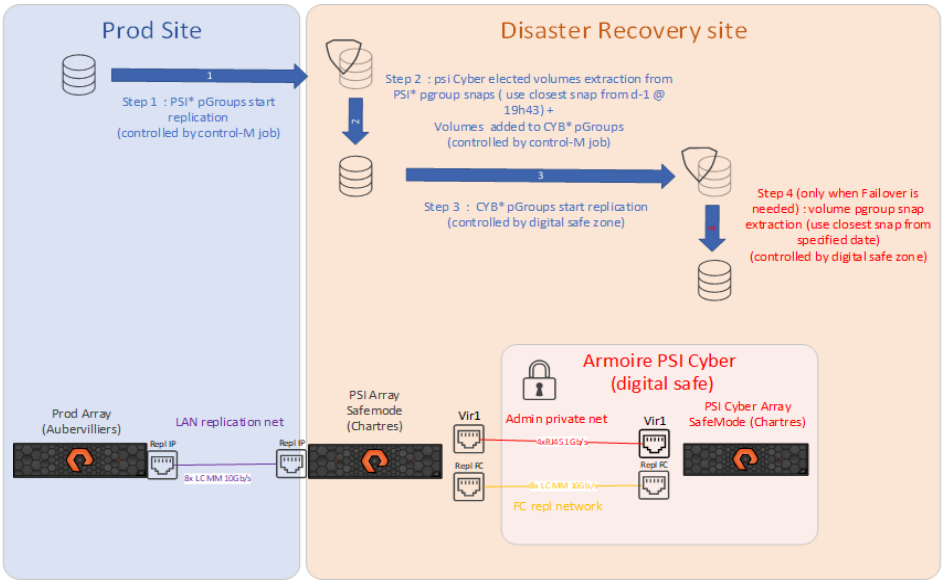


Figure 3 : réplication des données des serveurs VMware et IBM AIX

Elle se déroule en plusieurs étapes :

- Etape 1 : Sur les baies Pure Storage de production, les données de production sont associées à des « protections groupes » permettant leur réplication vers les baies de PSI. Cette tâche est déclenchée et supervisée quotidiennement par l'équipe Pilotage Informatique d'AG2R LA MONDIALE.
- Etape 2 : Extrait les volumes des protections groupes PSI et les ajoutées vers les protections groupes CYB
- Etape 3 : Réplication des protections groupes CBY vers les baies de psi cyber

5.2.2 Transfert de données pour les plateformes VMware utilisant le système de fichier vVols

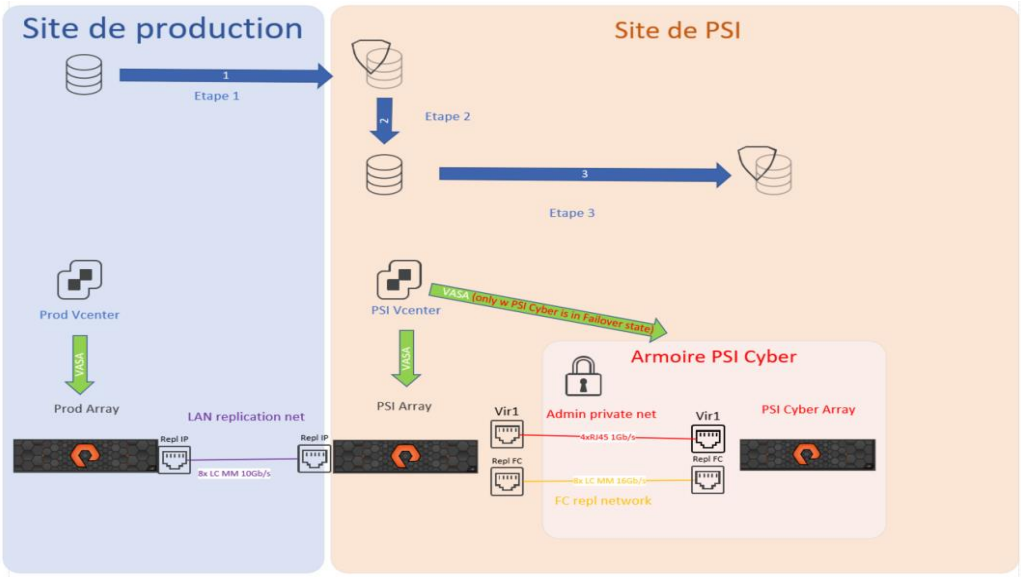


Figure 4 : réplication des données des serveurs VMWare utilisant les vVols

Elle se déroule en plusieurs étapes :

- Etape 1 : Sur les baies pure Storage de production, créons des protections groupes PSI à partie des volumes de données et répliquons-les sur les baies de PSI cyber.
- Etape 2 : Extrait les volumes des protections groupes PSI et les ajoutées vers les protections groupes CYB
- Etape 3 : Réplication des protections groupes CBY vers les baies de psi cyber

5.2.3 Transfert des données des Hyperviseur HPUX

Les hyperviseurs HPUX utilisant les baies de stockage du constructeur HDS, il est impossible de réaliser les réplications entre baies de stockages HDS et Pure Storage, nous utilisons la solution de sauvegarde CommVault monté sur hyperviseur VMware pour répliquer les sauvegardes complètes des données de production HPUX vers les baies de stockage Pure Storage de la plateforme de PSI cyber.

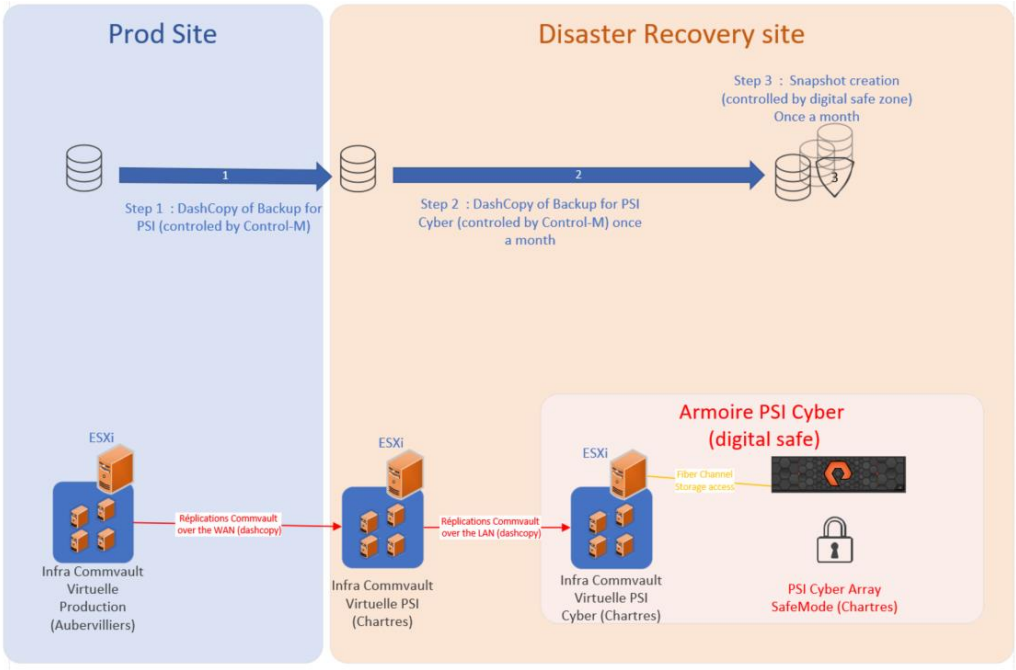


Figure 5: réplication des données des serveurs HPUX

Elle se déroule en plusieurs étapes :

- Etape 1 : une sauvegarde complète des données de production est réalisée et stocker sur l'infrastructure CommVault nominale, puis une copie de ces sauvegardes est répliquée vers l'infrastructure CommVault de PSI. Ces taches sont déclenchées et supervisées quotidiennement par l'équipe pilotage informatique.
- Etape 2 : une ultime réplication des données sauvegardées est réalisée entre l'infrastructure CommVault de PSI et celui de PSI CYBER. Cette tâche est déclenchée et supervisée 1 fois par mois par l'équipe Pilotage Informatique d'AG2R LA MONDIALE.
- Etape 3 : Un snapshot de ces données sauvegardées est réalisé sur les baies Pure Storage pour les protéger de toute altération. Cette opération est réalisée une fois par mois via une routine planifiée et déclenchée depuis le réseau isolé de la plateforme de sauvegarde inaltérable (PSI Cyber). Le résultat de cette opération est transmis via la passerelle Data diode pour un contrôle automatisé par l'équipe Pilotage Informatique d'AG2R LA MONDIALE.

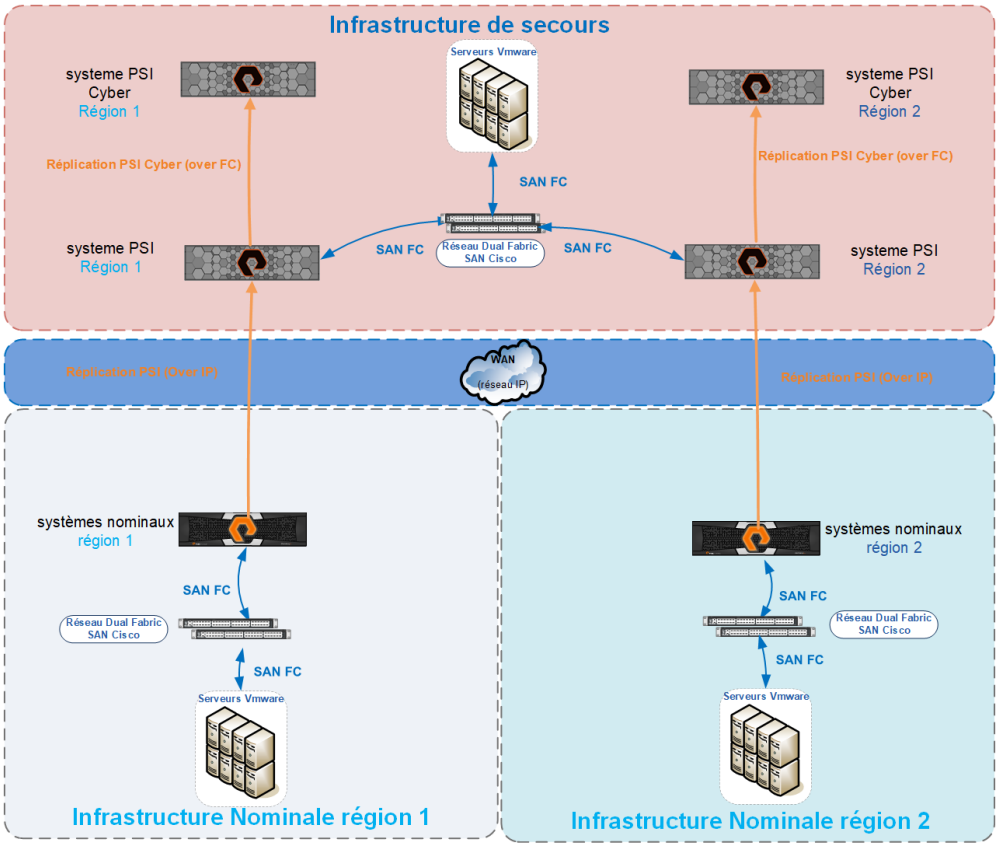


Figure 6 : architecture du système de stockage finale

5.2.3 Fréquence des sauvegardes et duré de conservation des données

La sauvegarde des données critiques vers la plateforme de sauvegarde inaltérable sera réalisée une fois par mois, le troisième mercredi du mois. Les données copiées seront celle du weekend précédent. Elles seront conservées dans les baies pour une durée de 9 mois avant d'être supprimer.

5.2.4 Contrôle de la plateforme de sauvegarde inaltérable

Déconnecter du reste du réseau, le seul moyen de communication de la plateforme avec l'extérieur est la data diode. Pour être analyser :

- Les logs des équipements (switch, serveur de temp, baies de stockage) de la plateforme de sauvegarde ultime seront transférés vers les serveurs de Syslog pour via la data diode.

- Les résultats des scripts d'inventaires et taches planifiées sont générés sous forme de fichier dans le serveur de pilotage. Ils sont transférés vers la plateforme AVGS grâce au protocole remote file transfert service (RFTS) via la data diode.
- Les baies Pure Storage et les switches réseaux sont configurés pour envoyer des alertes par mail grâce au relais simple mail transfer protocol (SMTP) de la data diode.
- Les logs du serveur de pilotage, sont collectés grâce à l'agent log Insight installé sur le serveur et transmis à la plateforme vRealize par le biais de la data diode.

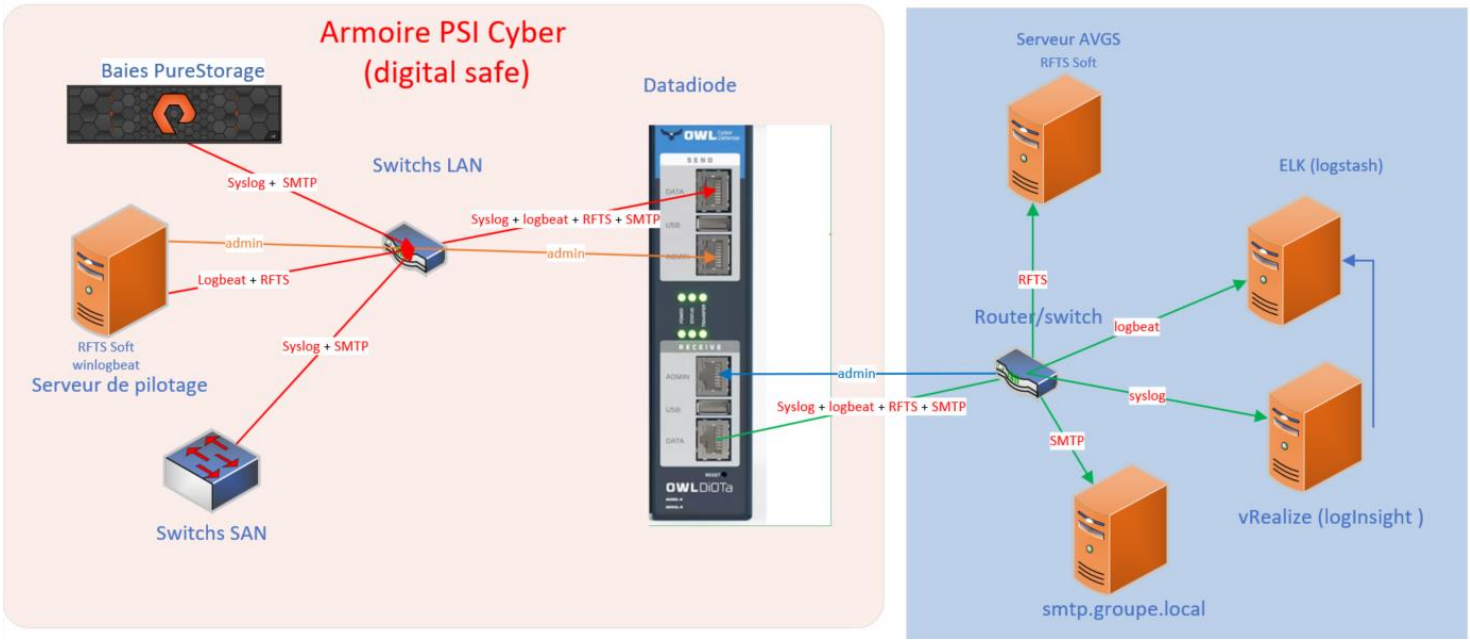


Figure 7 : mécanismes de contrôle et de supervision de la plateforme inaltérable

6. Protection ultime

Pour s'assurer que les données stockées dans la plateforme inaltérable restent intègres, la fonction Safemode est activé sur les baies pure Storage. Elle permet de créer des snapshots en lecture seule des données sauvegardés, une fois les sauvegardes intégrales réalisées.

Les avantages du Safemode :

Protection accrue : Les ransomwares ne peuvent pas éradiquer (supprimer définitivement), modifier ou crypter les snapshots SafeMode. En outre, seules quelques personnes désignées au sein d'AG2RLM peuvent travailler directement avec le support technique Pure Storage afin de configurer la fonctionnalité, modifier la politique ou supprimer manuellement les snapshots.

Flexibilité : La cadence de création et de suppression des snapshots reste personnalisable, cependant elle ne peut être réduite grâce au safemode.

Restauration rapide des données : les données protégées par snapshots sont re connectables rapidement aux serveurs pour les relire.

Protection des investissements : PureStorage inclut les snapshots SafeMode sans frais supplémentaires. Votre abonnement ou votre contrat de support et maintenance couvrent les améliorations.

7. Problèmes rencontrés

Durant la mise en place de la plateforme les difficultés ont été les suivantes :

- L'intégration des codes de retour d'exécution dans les scripts PowerShell

Solution : création des logs après exécution de chaque script

- Le transfert des logs du serveur de pilotage, avec l'agent logstack installé sur le serveur n'a pas fonctionné car l'agent logstack utilise une transmission TCP et la data diode est unidirectionnel.

Solution : j'ai remplacé l'agent logstack par l'agent log insight qui utilisé le protocole UDP.

Conclusion

La sauvegarde inaltérable apporte une nouvelle couche sécuritaire à la stratégie de résilience du système d'information du groupe, en limitant l'impact d'une cyberattaque interne ou externe sur son système d'information. Ce projet cadre avec la vision stratégique de l'entreprise qui est de « prendre la main sur demain », car il permet d'améliorer la cyber résilience du groupe en limitant la quantité de données perdues et le temps d'indisponibilité de ses plateformes dans le contexte d'une crise cyber.

Liste des figures