



HAL
open science

Sauvegardes délocalisées et reprise d'activité au SIMSU

Laure Perret, Didier Mathian, William Marchal

► **To cite this version:**

Laure Perret, Didier Mathian, William Marchal. Sauvegardes délocalisées et reprise d'activité au SIMSU. JRES (Journées réseaux de l'enseignement et de la recherche) 2013, Renater, Dec 2013, Montpellier, France. ⟨hal-04805017⟩

HAL Id: hal-04805017

<https://hal.science/hal-04805017v1>

Submitted on 26 Nov 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY-NC 4.0 - Attribution - Non-commercial use - International License

Sauvegardes délocalisées et reprise d'activité au SIMSU

Laure Perret
Didier Mathian
William Marchal

Service Informatique Mutualisé du Site Universitaire - Université Joseph Fourier
31 rue des mathématiques
B.P. 53 – 38041 Grenoble Cedex 9

Résumé

Le SIMSU est un Service Informatique Mutualisé. Il a pour mission la mise en place ainsi que l'exploitation d'infrastructures et d'applications pour les 7 établissements de Grenoble et de Savoie (applications de gestion de la scolarité, du personnel, financière, annuaires, messagerie, réseau... pour environ 70 000 utilisateurs).

Ces deux dernières années, la virtualisation massive et l'augmentation du nombre de serveurs ont rendu obsolètes une partie des solutions de sauvegarde et de reprise d'activité en place. Suite à l'implication des responsables administratifs dans une étude du coût d'une potentielle perte de notre logiciel de gestion financière et comptable SIFAC (de l'ordre de 1 million d'euros par université) et l'incertitude quant au temps de reprise, la révision de nos procédures de reprise d'activité est devenue une priorité. Un premier périmètre d'urgence a été défini, englobant quelques applications jugées bloquantes, mais nous avons dimensionné notre infrastructure de façon à pouvoir couvrir tout notre périmètre de production.

Cette présentation développe

- la façon dont nous avons, en nous appuyant sur notre infrastructure virtualisée, fait évoluer notre architecture et délocalisé notre système de sauvegarde ;*
- notre retour d'expérience sur plusieurs outils comme Veeam Backup & Recovery, VDR, rsync ;*
- les étapes de notre démarche, les raisons de nos choix, les difficultés que nous avons rencontrées ;*
- un tour d'horizon de différentes problématiques touchant à la reprise d'activité : la définition des priorités et du mode dégradé, les implications réseau, les tests et leurs limitations, etc ;*
- un bilan des services rendus, les limites du nouveau système et les pistes pour continuer.*

Mots-clefs

Sauvegardes délocalisées, PRA, datacenter, infrastructure, virtualisation

1 Contexte

Le Service Informatique Mutualisé du Site Universitaire de Grenoble (SIMSU) est une structure inter-universitaire, qui assure la mise à disposition d'applications mutualisées (logiciels AMUE de scolarité, ressources humaines, ..., développements locaux, progiciels, annuaires, etc) aux 7 établissements du site Grenoble – Savoie. Il regroupe environ 40 informaticiens opérant quelques 300 serveurs et 50 bases de données, pour un total de 70 000 utilisateurs. Le groupement « Datacentre » (8 personnes, 5 ETP) a pour charge l'infrastructure supportant ces applications. La contrainte essentielle qui sous-tend toutes nos actions est la préservation des données applicatives.

Dans cette optique, nous cherchons constamment à faire évoluer nos mécanismes de sauvegarde.

1.1 Evolution des sauvegardes

Initialement basée sur un parc serveurs majoritairement physiques, 90% de l'activité de sauvegarde concernait les données. Avec l'arrivée de la virtualisation et les possibilités de reprise offertes par le clonage de machines virtuelles, nous avons fait évoluer nos pratiques de sauvegardes des systèmes (tout en gardant nos données sauvegardées en mode

fichier sur notre robot de sauvegarde) : nous avons commencé par lancer manuellement des clones lors de la mise en production ou lors de mises à jour majeures. Avec la diminution du nombre de serveurs physiques et l'explosion du nombre de machines virtuelles nous avons commencé à chercher des solutions logicielles pour la gestion de notre parc virtuel, comme VDR (Vmware Data Recovery). Mais ces processus ont vite montré leurs limites :

- les administrateurs des machines oubliaient de faire la demande de clonage après une mise à jour majeure ;
- des erreurs fréquentes de *Data Recovery* constatées, la faute à un produit manquant de robustesse ;
- ces sauvegardes et/ou clones étaient sur la même architecture que la production : pas d'externalisation ;
- quant aux sauvegardes de données, nos investigations nous ont permis de mettre en exergue certaines défaillances : une désynchronisation entre le système de sauvegarde et l'arrêt de l'application pouvait engendrer des sauvegardes inconsistantes. De plus, la volumétrie des données sauvegardées ayant beaucoup augmenté avec les possibilités de stockage étendues, des dépassements de fenêtre de sauvegarde sont apparus.

1.2 Externalisation

Depuis longtemps, des mécanismes PRA sont liés aux mécanismes de sauvegarde afin d'assurer la préservation des données applicatives en cas d'incident majeur sur le site du SIMSU :

- externalisation des sauvegardes système sur CD et une partie des bases de données sur bandes ;
- installation de baies de secours pour une possibilité de reprise (PRA local entre 2 salles) ;
- archivage de copies de sauvegardes dans un coffre ignifugé.

Ces mécanismes ont également montré leurs limites :

- pour le stockage externalisé de médias :
 - sécurisation du lieu de stockage insuffisante pour les données confidentielles (gestion financière, gestion RH, gestion de scolarité, documents internes confidentiels ...) ;
 - limitation de la quantité de données à externaliser : comment faire pour les nombreuses applications jugées moins critiques, mais nécessaires ?
 - processus manuels, donc soumis aux aléas de présence d'une personne physique ;
- pour les baies de secours : salles différentes, mais sur un même site.

1.3 Actions

Conscients des faiblesses de notre système et dans une logique d'amélioration continue, nous avons lancé en parallèle plusieurs projets de consolidation, du stockage redondant aux sauvegardes.

Un audit de notre système financier a fait prendre conscience aux décideurs de l'importance de renforcer le système de reprise d'activité. Le coût de la perte des données financières a été estimé à 1 millions d'euros par université et l'externalisation des sauvegardes jugée insuffisante, car les incertitudes sur le délai et le coût de reprise étaient trop importantes. Il a été décidé d'allouer des ressources en vue de garantir en priorité le redémarrage du système financier en cas d'incident majeur au SIMSU. Afin de répondre rapidement aux exigences de l'audit, des moyens humains ont été réaffectés à la consolidation du PRA.

Dans cette dynamique, les projets de consolidation en cours ont été réorganisés afin d'intégrer les nouvelles contraintes. En particulier, nous avons étudié et mis en place une solution de sauvegarde et de reprise délocalisée.

2 Étude de l'architecture de PRA

2.1 Besoins et contraintes

Les contraintes et les besoins ont été validés lors de l'étude de l'architecture de PRA, en particulier la nécessité de se trouver sur un site géographiquement distant.

Les contraintes liées à la sauvegarde délocalisée :

- raccordement réseau : assurer la sécurité des transferts de données, maîtriser les équipements et garder des débits importants pour sauvegarder nos machines ;
- puissance de traitement, pour pouvoir effectuer des sauvegardes à grande échelle ;
- volumétrie suffisante pour stocker plusieurs jeux de sauvegarde ;
- gestion robuste des sauvegardes permettant d'assurer la cohérence des bases de données.

Les contraintes liées à la reprise d'activité :

- propagation des VLAN sur le site PRA ;
- puissance de calcul suffisante pour faire fonctionner les machines virtuelles restaurées jusqu'à ce que l'incident sur le site de production soit résolu ;
- volumétrie suffisante pour pouvoir garder en parallèle les machines restaurées et les sauvegardes.

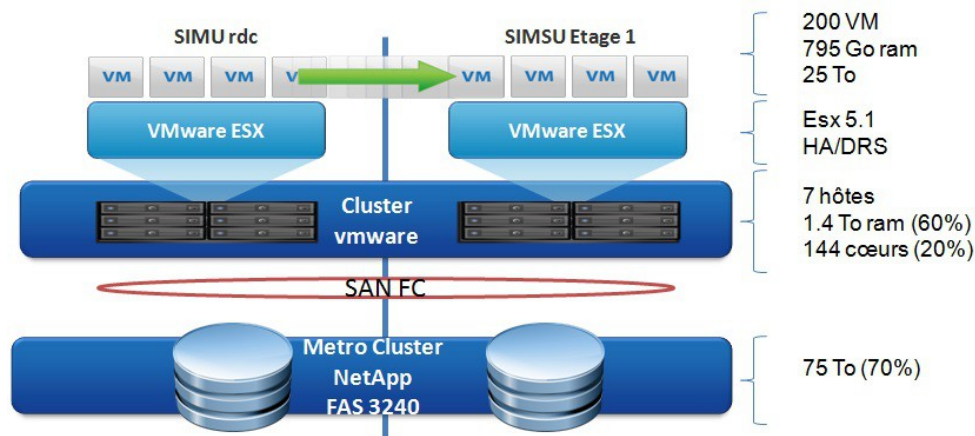


Figure 1-Infrastructure SIMSU

Bien que robuste, redondante et répartie sur deux étages ...

... notre infrastructure ne convenait pas aux nouvelles exigences, car installée sur un même site.

2.2 Étude de solutions

Nous avons étudié les solutions qui s'offraient à nous pour intégrer ces contraintes et tout d'abord la nécessité de trouver un site satisfaisant nos exigences en terme de puissance électrique, de climatisation et d'infrastructure réseau. 3 sites ont été envisagés :

- sur le domaine universitaire : les salles existantes ne correspondaient pas ou étaient déjà surchargées. Un projet de salle était en cours d'étude, mais pas suffisamment avancé ;
- à l'hôpital : la salle n'a pas été construite dans les temps ;
- au centre-ville, dans les locaux de Grenoble-INP (à 9 km du SIMSU, appelé « site Viallet ») : notre collaboration de longue date avec les équipes de Grenoble-INP nous a permis de nous installer dans l'une de leurs salles serveur.

Restait à trouver la solution technique la plus adaptée.

2.2.1 1^{ère} solution : évoluer en « stretch metro-cluster »

Une des possibilités était de faire évoluer notre infrastructure SAN NetApp en « stretch metro-cluster » (écriture en Y vers 2 sites distants).

Les coûts trop élevés (changement des switches d'interconnexion, licence ...), les risques liés à la modification d'architecture (déplacement d'une partie du metro-cluster) et le nombre de fibres optiques nécessaire pour relier les 2 parties du cluster, ont disqualifié cette solution.

2.2.2 2^{ème} solution : nouvelle infrastructure de sauvegarde délocalisée

Nous nous sommes alors orientés vers la construction d'une nouvelle infrastructure de sauvegarde sur le site Viallet. Nous avons bénéficié d'accès au routeur et d'une liaison par fibres déjà maîtrisée par le SIMSU, de la récupération d'un châssis « Blade » (issu d'un autre projet inachevé) et de l'accès à une baie de disque déjà en place sur Viallet pour des projets communs.

Nous avons procédé par étapes :

- le maquetage réseau et matériel avec la baie existante et un serveur ESX prélevé sur notre site SIMSU ;
- la mise en place de Veeam Backup & Recovery et les tests associés;
- la mise en place d'un premier périmètre délimitant les ressources prioritaires : le périmètre dit « urgent » ;
- l'achat de baies de disque et de serveurs pour construire l'architecture cible ;
- l'extension du périmètre à toutes nos machines de production.

Nous allons voir dans les chapitres suivants quelles solutions réseau, matérielles et logicielles ont été ainsi déployées.

3 L'infrastructure réseau

3.1 Mode sauvegarde

Un état simplifié de notre réseau en mode « sauvegarde », c'est à dire en fonctionnement courant, est représenté sur la figure suivante.

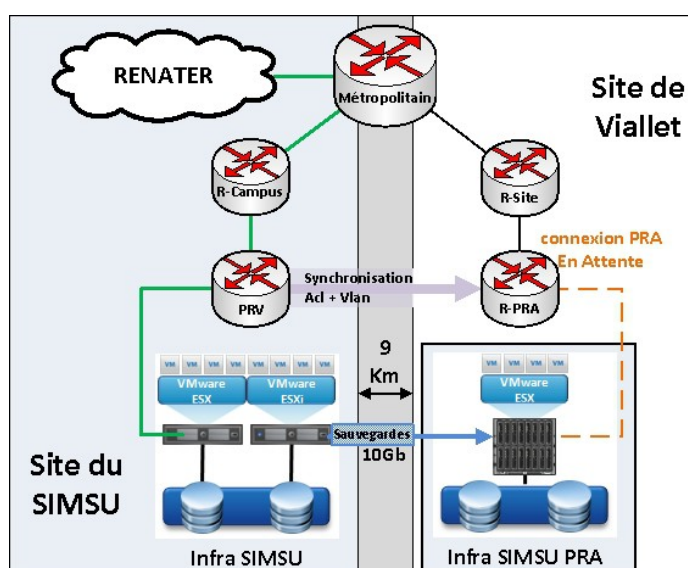


Figure 2-Mécanismes et architecture réseau, mode sauvegarde

La partie gauche du schéma représente l'infrastructure de notre site principal (à noter la présence dans nos locaux d'un nœud du réseau métropolitain, ainsi que les équipements RENATER).

La partie droite représente le site PRA de Viallet à environ 9 Km, hébergeant notre extension d'infrastructure.

Notre solution repose principalement sur deux mécanismes préventifs :

1. La sauvegarde quotidienne (soir) sur le deuxième site via une fibre dédiée en 10 Gb/s.
2. La synchronisation des ACL et VLAN entre les routeurs de chaque site.

Ainsi, les informations nécessaires pour retrouver un accès aux données sont disponibles sur le site de PRA.

3.2 Mode bascule

Le schéma suivant reprend de manière plus détaillée notre infrastructure et traite un cas de panne générale sur l'ensemble de notre parc serveurs et baies (surtension, inondation, incendie localisé....) :

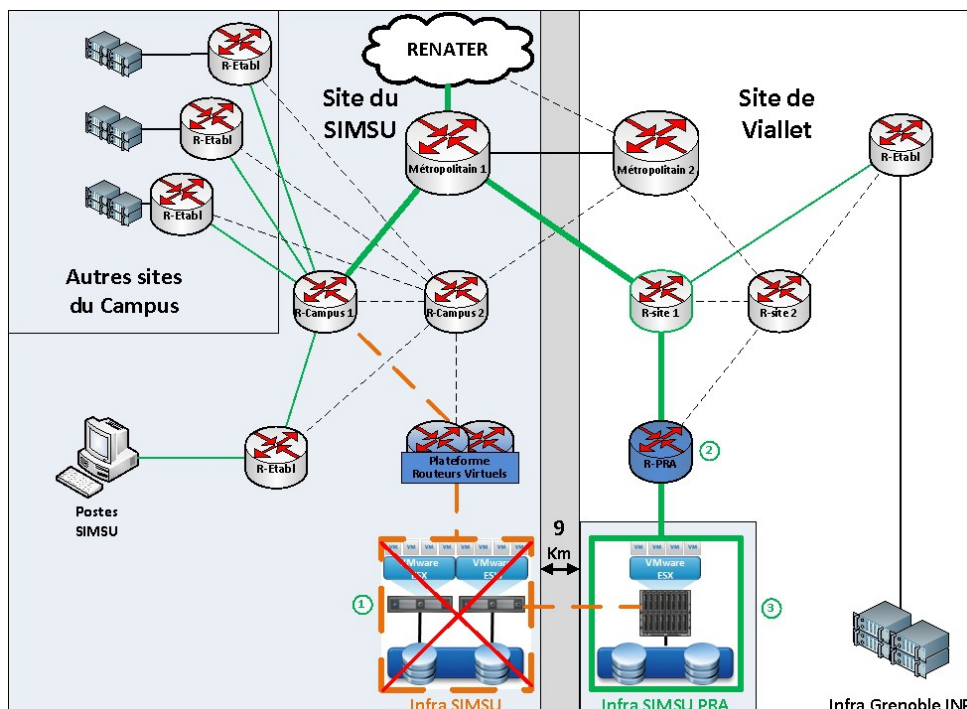


Figure 3-Bascule réseau

Un sinistre sur les serveurs et baies de stockage du SIMSU rend l'accès aux services impossibles.

- Le routeur R-PRA étant déjà configuré grâce au script de synchronisation, il ne reste plus que l'activation des liens vers les deux routeurs R-site 1 et R-site 2 pour annoncer les VLAN.
- L'accès aux services est, d'un point de vue « réseau », de nouveau possible.

Le SIMSU fournit l'unique accès à RENATER, au réseau métropolitain et l'interconnexion des établissements du campus. Un incendie ou autre sinistre structurel sur l'ensemble du bâtiment aurait donc des conséquences graves. Ce scénario, de par son ampleur, ne peut pas être pris en charge par notre PRA actuel.

4 L'infrastructure matérielle

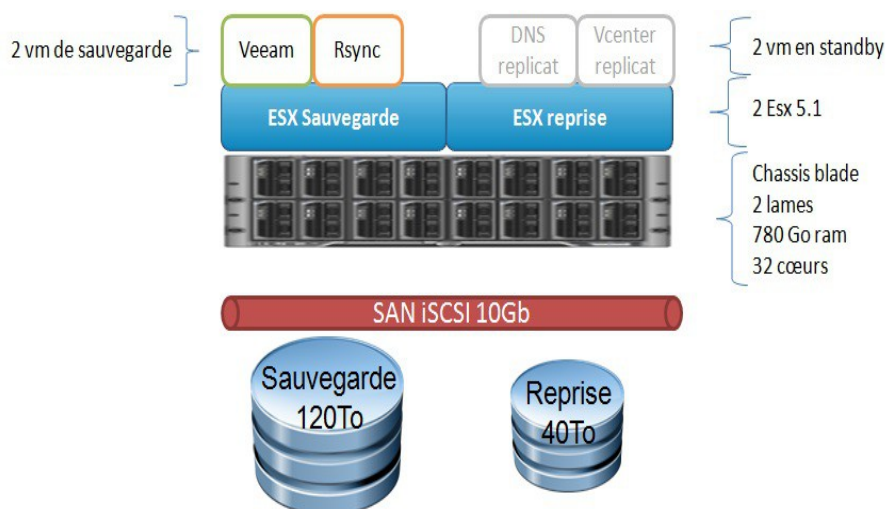


Figure 4-Infrastructure du site PRA-Viallet

L'infrastructure mise en place sur le site PRA est composée de :

- 1 châssis blade DELL M1000e avec commutateurs internes (power connect M6220, M8024, M8024-k 10GbE SW) redondés : il permettent d'avoir un réseau IP et SAN redondé à 10Gb/s et un réseau d'administration des hyperviseurs à 1Gb/s.
- 2 lames (PowerEdge M620, 32 cœurs, 780Go de RAM). Cela correspond environ aux ressources réellement consommées sur notre infrastructure de production.
- 2 licences ESX standard : nous n'avons besoin que des fonctionnalités standard, pas de déplacements de machines virtuelles à chaud, pas de besoins de haute disponibilité. En fonctionnement sauvegarde, nous dédions un hyperviseur à la sauvegarde et un autre à la reprise.
- 2 baies de disques, afin de séparer les fonctionnalités de sauvegarde et de reprise, sans fonctionnalités avancées mais évolutives et avec des performances importantes :
 - Baie de sauvegarde (DELL MD 3660i) de 120 To, volumétrie calculée pour avoir plusieurs jeux de sauvegardes de nos serveurs de production.
 - Baie de reprise (DELL MD 3600i+1200) de 40 To, volumétrie calculée pour restaurer les VM de production. Elle assurera l'ensemble des accès disque en cas de bascule.

Ces acquisitions, dimensionnées pour assurer les sauvegardes et la période de transition entre une bascule de site (sachant que des performances moindres seraient tolérées) et un retour à la normale représentent un investissement de 38 800 € HT. Au cas où la période de transition devait se prolonger, nous recherchons des solutions qui nous permettraient d'augmenter rapidement les ressources des hyperviseurs (livraison express de DELL, externalisation ...).

5 Solution logicielle

Cette figure représente nos mécanismes de sauvegarde locales et distantes. Ces mécanismes correspondent à des solutions logicielles détaillées ci-après.

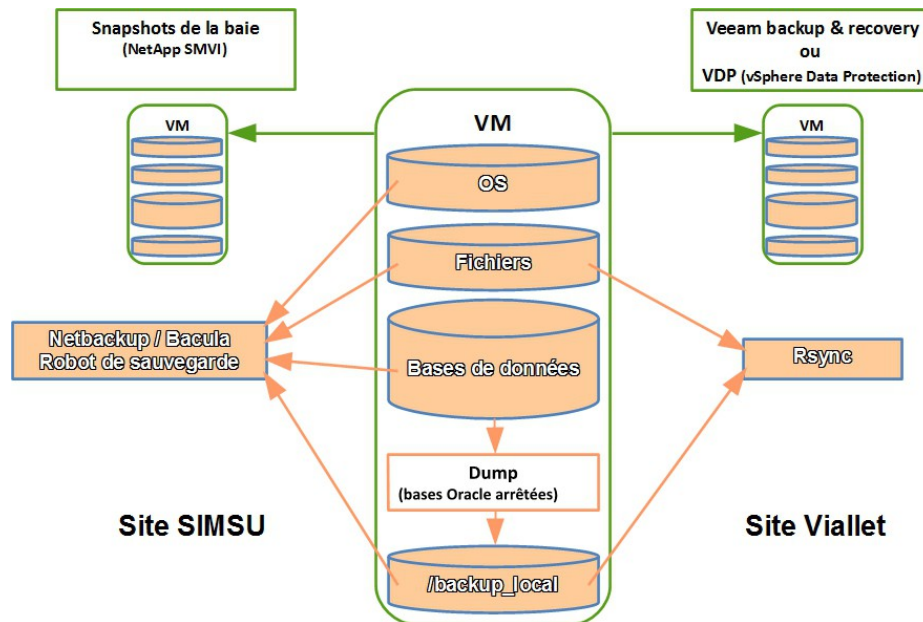


Figure 5-Mécanismes de sauvegarde locales et distantes

Les deux sites y sont représentés. Les mécanismes qui aboutissent à une sauvegarde des machines virtuelles complètes sont en vert, ceux qui permettent une sauvegarde au niveau des fichiers sont en orange.

L'ensemble des mécanismes en place tente de minimiser les risques de pertes de données en respectant la règle du « 3, 2, 1 » : 3 jeux de sauvegardes sur 2 sites, dont 1 distant.

5.1 Logiciels de sauvegarde des machines virtuelles

5.1.1 Sur le site SIMSU : SMVI

Sur le site SIMSU, la baie NetApp possède un outil de *snapshots*¹ automatiques, s'interfaçant avec VMWare vSphere : SMVI (Snap Manager for Virtual Infrastructure). Ces *snapshots* se déroulent en 3 temps pour chaque *datastore*² :

1. un *snapshot* VMWare pour chaque machine du *datastore*, pour figer un état de la machine,
2. un *snapshot* du LUN correspondant au *datastore*, stocké dans la baie NetApp,
3. destruction du *snapshot* vmware.

Ils sont stockés en local, sur le volume correspondant, signifiant qu'ils sont perdus en cas de perte de la baie et qu'ils occupent de l'espace disque. La rétention est réglée à une semaine, avec destruction automatique des *snapshots* les plus anciens si la taille de l'espace réservé aux *snapshots* devient trop grande (cela risquerait de perturber le fonctionnement des machines en activité).

La restauration se fait via le *plug-in* vCenter Netapp permettant de restaurer individuellement une machine virtuelle de manière très simple et très rapide.

1. Instantané des données. Suite à un *snapshot*, le système enregistre les données modifiées sur un espace différent de celui où sont stockées les données initiales.

2. Zone de stockage de données, contenant plusieurs machines virtuelles.

5.1.2 Sur le site PRA-Viallet : Veeam Backup & Recovery ou VDP

Sur le site Viallet, a été installé le logiciel Veeam Backup & Recovery (ci-après VBR), qui assure les sauvegardes des machines virtuelles de production. Deux modes de sauvegarde sont utilisés:

- Le mode « *reverse incremental* » : ce mode permet d'avoir une sauvegarde complète de la machine virtuelle dans son état le plus récent et de garder les sauvegardes antérieures sous forme d'incrément. VBR transfère uniquement ce qui a été modifié sur la machine source, puis il reconstruit une image complète à partir de l'ancienne image et du nouvel incrément. Ceci permet de restaurer facilement et rapidement la dernière version de la machine, tout en garantissant un retour en arrière possible par reconstruction. Ce mode de sauvegarde compresse et dé-duplique les données offrant d'importants gains de place (jusqu'à un facteur 9 dans notre cas). Nous avons une rétention de 7 jours.
- La réplication : ce mode offre la possibilité d'avoir une machine virtuelle à jour et prête à redémarrer immédiatement. L'avantage est de ne pas avoir à restaurer la machine : elle est opérationnelle *au clic*, économisant beaucoup de temps. En contrepartie, il n'y a ni compression, ni déduplication. Ces réplicas sont stockés directement sur la baie de reprise. Comme le mode « *reverse incremental* », le mode réplication ne transfère que les données qui ont été modifiées sur la machine virtuelle. La rétention est gérée via des *snapshots*.

La sauvegarde est paramétrée pour automatiquement gérer les machines virtuelles présentes dans un dossier que nous avons défini dans VMWare vCenter.

La restauration est intuitive et se fait via l'interface d'administration de VBR, elle permet des restaurations de machines virtuelles complètes ou disque par disque. La durée de restauration dépend bien entendu de la quantité de données à restaurer.

VDP (VMWare vSphere Data Protection) vient en complément de VBR de façon marginale : il est utilisé pour quelques hyperviseurs hébergés pour lesquels les licences VBR n'ont pas été acquises. La dernière version (5.5) permet de restaurer une machine directement, sans recours à la console VMWare vCenter ... ce qui est particulièrement utile pour restaurer le vCenter. C'est un complément satisfaisant, bien que limité : il ne permet pas de choisir le type de sauvegarde et est très peu verbeux sur ce qu'il fait (ce qui le rend très difficile à dépanner).

5.2 Sauvegarde fichiers

5.2.1 Export des bases de données

Pour tous les serveurs de bases de données, nous avons écrit des scripts qui effectuent des exports des bases et stockent le résultat dans un répertoire séparé du système (/backup_local), tout comme l'impose l'AMUE pour ses applications. Dans le cas des bases Oracle, un script stoppe les bases avant d'effectuer la sauvegarde, puis les relance. Pour les bases mysql, un autre script utilise l'outil *mysqldump* en mode « bases ouvertes », verrouillant en écriture les tables en cours de sauvegarde. Ces scripts sont ordonnancés la nuit, à des heures de faible activité et compatibles avec les fenêtres de sauvegardes et de traitements sur les tables. Un script de rotation des fichiers assure une rétention de 3 jours dans le répertoire de stockage local. Les inconvénients de cette méthode :

- la nécessité de disposer d'un espace disque supplémentaire, qui se retrouvera également dans les sauvegardes des machines virtuelles,
- la nécessité d'arrêter les bases Oracle.

Malgré ces inconvénients, cette méthode garantit la cohérence de la sauvegarde et permet de sauvegarder les fichiers d'export de façon différée par un logiciel extérieur.

Le restauration se fait via des scripts propres à chaque application. Chaque base peut être restaurée individuellement.

5.2.2 Sur le site SIMSU : Netbackup / Bacula

La sauvegarde de fichiers sur le site SIMSU est actuellement effectuée par le logiciel *NetBackup* sur une librairie de bandes. Dans le cadre de ce projet, a été décidé d'abandonner cet outil pour se tourner vers l'outil libre *Bacula*, en utilisant un stockage sur disque. Cette décision vient essentiellement du fait que cette partie de la sauvegarde se présente comme un complément dit « de confort » par rapport aux autres mécanismes en place : les fonctionnalités recherchées

sont une facilité de restauration et une possibilité de déléguer les restaurations aux utilisateurs. Dans cette optique, la dépense pour un logiciel comme NetBackup ou ses concurrents ne se justifiait pas. La question s'est posée de savoir sur quel site réaliser la sauvegarde de fichiers : fallait-il la délocaliser ? Il a été décidé de les garder sur le site SIMSU, essentiellement pour deux raisons : éviter l'encombrement de la bande passante et surtout garder des sauvegardes sur site (en cas de panne du site distant ou de coupure réseau).

La restauration se fait via l'interface d'administration et permet de restaurer avec une granularité de niveau fichier.

5.2.3 Sur le site PRA-Viallet : rsync

Les exports des bases stockés dans le répertoire `/backup_local` des serveurs, ainsi que les fichiers importants sont envoyés sur le site de Viallet via des scripts utilisant l'outil `rsync`. Le script est adapté aux besoins sur chaque serveur et permet une fréquence de sauvegarde quotidienne et une rétention d'une semaine, sur un serveur virtuel dédié au stockage de ces données raccordé à la baie de sauvegarde. Cette rétention vient en complément du répertoire `/backup_local` et des sauvegardes de machines virtuelles : en cas de reprise d'activité, elle permet de reconstruire les bases dans l'état de la veille (alors que les machines virtuelles ne sont pas nécessairement sauvegardées tous les jours). Pour les serveurs sous Windows, nous utilisons le logiciel « *delta copy* », qui ne possède pas cette notion de rétention.

La restauration se fait avec une commande `rsync` depuis la machine virtuelle concernée.

5.3 Logiciels de surveillance

L'ensemble de ces mécanismes est surveillé quotidiennement : des notifications par mail sont envoyées par les scripts et par les logiciels de sauvegarde et l'application de supervision *Centreon*, basée sur *Nagios*, veille à la présence des bons fichiers dans les répertoires `/backup_local`. *NetBackup* est traité à part et nécessite, quant à lui, l'utilisation de sa propre interface pour repérer les erreurs de la nuit. Ces moyens de surveillance sont d'autant plus utiles que les administrateurs d'applications expriment de plus en plus le besoin de suivre le fonctionnement des sauvegardes et s'assurer de la fiabilité de la restauration des données.

6 Scénario de reprise

6.1 Le sinistre

Pour mémoire, le scénario envisagé est un sinistre dans nos salles serveur qui aurait pour conséquence la destruction des salles, mais qui n'impacterait pas les nœuds d'interconnexion RENATER/Métropolitain situés dans une autre salle.

6.2 Par où commencer et ... avec quels moyens?

Le logigramme suivant résume les moyens utilisés et les étapes suivies pour notre scénario de reprise :

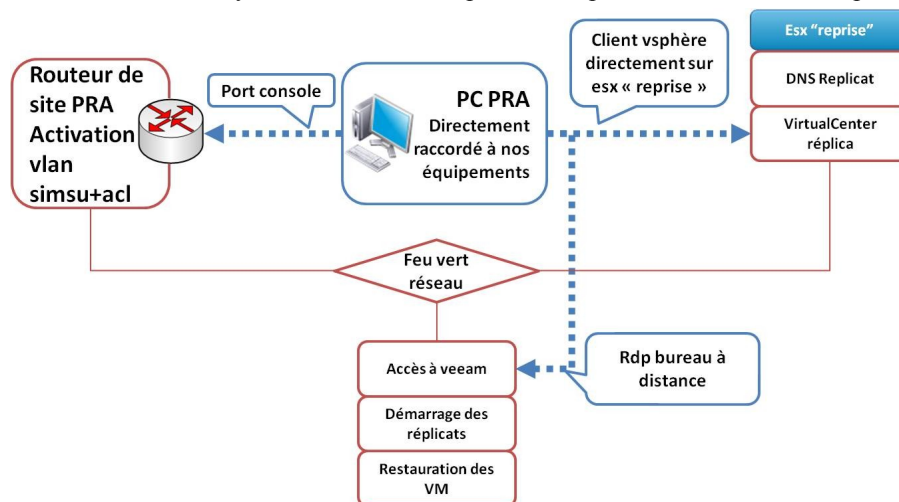


Figure 6 - Scénario de reprise

6.2.1 Opérations préalables

1. Le routage réseau : l'annonce de nos VLAN sur le site de PRA s'effectue suite à la bascule réseau décrite dans le chapitre « solution réseau ».

2. et 3. Un Serveur de nom et le Virtualcenter : des replicas, mis régulièrement à jour et stockés sur notre hyperviseur de reprise, garantissent la remise en route du DNS puis du vCenter, éléments essentiels au fonctionnement de l'architecture globale.

Ces 3 opérations se font depuis un poste de travail (nommé PC PRA) installé sur le site Viallet et partageant le même VLAN que l'hyperviseur de reprise (ce qui nous assure de pouvoir y accéder).

6.2.2 Opérations de restauration

Ces opérations réalisées nous amènent au « Feu vert réseau » : les conditions sont rassemblées pour que nous puissions restaurer les machines via Veeam Backup & Recovery.

Plusieurs critères régissent l'ordonnement de la restauration : l'importance de l'application, les interdépendances et la consommation de ressources. Par exemple, le service d'annuaire LDAP, normalement équilibré sur plusieurs serveurs, sera lancé avant les applications qui en dépendent, mais sur une seule machine. Cette étape est très longue (nous verrons les tests effectués plus loin). C'est pourquoi certaines machines ont des réplicas prêts à redémarrer, en plus de leurs sauvegardes.

Après ces opérations, nous pouvons dire que, du point de vue infrastructure, la reprise d'activité technique est terminée : les services sont de nouveau disponibles. Les équipes applicatives entrent alors en action, afin de restaurer les données sauvegardées grâce à *rsync* et effectuer les tests.

6.2.3 Autres opérations

Le scénario présenté infra n'est qu'une première étape, car un PRA va plus loin qu'une simple reprise d'activité technique et il conviendra de ne pas négliger les problématiques touchant la chaîne d'alerte, la documentation, la mise à disposition des locaux pour les personnes ressources techniques et applicatives, etc.






6.3 Scénarios qui ont été testés


- Test de bascule réseau : nous avons déroulé le script de bascule de VLAN pour un VLAN de test. En ¼ d'heure, ce VLAN et ses machines hébergées, étaient accessibles par le routeur du site PRA.
- Test de reprise SIFAC : suite à l'audit SIFAC et à la mise en place de cette architecture PRA, nous avons décidé de tester la reprise d'activité de SIFAC. En accord avec les établissements, nous avons une journée pour restaurer les machines SIFAC de production sur le site PRA. Suite aux restaurations effectués par VBR, puis *rsync*, une restauration SAP a été lancée. Nous avons relevé les temps suivants :

RESTAURATION VEEAM (VM)	27/08/2013	Volumétrie
toutes (7 VM)	6H30	4,00 To
1 VM seule	1H	0,80 To
RESTAURATION RSYNC (svg base)	27/08/2013	Volumétrie
toutes (7 VM)	1H	1,00 To
1 VM seule	13 min	0,20 To
RESTAURATION SAP (restauration base)	27/08/2013	
toutes (7 VM)	1H	
1 VM seule	11 min	

7 Bilan et perspectives

Le tableau ci-dessous propose un bilan des incidents traités et montre en vert les apports du projet :

	Incident	Niveau de service	Mécanisme local	Mécanisme délocalisé
	Panne matérielle Panne électrique	Continuité d'activité	Cluster VmWare + Netapp	
	Perte d'un fichier	RPO : J-1 (svg la nuit) RTO : <1H Granularité : fichier	Netbackup ou Bacula	
	Corruption Base d'une base de donnée	RPO : J-1 (svg la nuit) RTO : <1/2 j Granularité : BD	Netbackup ou Bacula	rsync (site Viallet)
	Corruption VM/système	RPO : J-1 RTO : <2H Granularité : vm	SMVI (site SIMSU)	Veeam (site Viallet)
	Incident site SIMSU (excepté réseau)	RPO : J-1 RTO : 1 à n jours. Granularité : 1 ou n vm		PRA :


Amélioration du niveau de service

- Ce projet a considérablement augmenté le niveau du service offert. Avant, nous externalisons uniquement les données sans garantie de réutilisation. Aujourd'hui, nous externalisons des machines virtuelles complètes et nous avons une architecture prête à reprendre l'activité : en cas de sinistre, plus besoin de remonter une salle serveur, ni de réinstaller les systèmes d'exploitation et les applications.
- Ce projet n'a pu être mené à bien qu'avec l'implication de notre service réseau et de nos collègues de Grenoble INP qui, ayant été invités aux réflexions dès le début du projet, ont ainsi pris conscience que les enjeux nous concernaient tous.
- Il a insufflé une prise de conscience et a forcé une remise en cause des procédures en cas de sinistre. Il s'élargit notamment à la partie réseau.
- Nous souhaitons profiter de cette expérience pour systématiser les simulations de reprise d'activité. Car un PRA n'est valide que s'il est régulièrement éprouvé par des tests.
- Enfin, nous commençons à réfléchir aux problématiques d'archivage, en envisageant l'hébergement sur un troisième site géographique.