Mise en place d'une solution de sauvegarde mutualisée pour le Grand Est

Alain Heinrich, Benoît Marchal

Mise en place d’une solution de sauvegarde mutualisée pour le Grand Est

Alain Heinrich
Université de Strasbourg
Direction du Numérique

Benoît Marchal
Université de Lorraine
Direction du numérique

Résumé

Les universités de Strasbourg et de Lorraine ont collaboré pour mettre en place une infrastructure de sauvegarde distribuée, déployée dans leurs datacenters respectifs, localisés à Strasbourg et à Nancy. Cette démarche vise à proposer un service de sauvegarde de données à l'ensemble des partenaires de la région Grand Est. Elle s'inscrit dans le cadre de l'initiative ADAGE (Alliance pour un DAtacenter Grand Est), laquelle ambitionne de mettre en place une offre de service pour l'Enseignement Supérieur et la Recherche (ESR) à l'échelle régionale, dans le contexte de la labellisation des datacenters.

Ce service se distingue par son approche "Cloud", fonctionnant selon le modèle BaaS (Backup as a Service). L'objectif principal étant d'offrir aux utilisateurs un maximum d'autonomie en mettant à leur disposition des instances de sauvegarde à la demande, avec une interface Web unifiée facilitant les délégations.

Dans cet article, nous reviendrons sur les étapes clés du projet, de son origine à l’exploitation de la solution co-gérée par une équipe interuniversitaire en passant par l’étude des besoins, des solutions du marché et du processus de mise en place de la solution technique retenue. Nous aborderons également la création d’un lien réseau spécifique entre les datacenters, ainsi que les besoins liés au nouveau type d’attaques : immuabilité, analyse en temps réel des modifications, etc.

Nous vous proposons, après un an d’exploitation commune, un retour d’expérience avec quelques données chiffrées. Nous détaillerons enfin notre offre de services : conditions d’accès, disponibilité, sécurité et calcul des tarifs.

Mots-clefs

Sauvegarde, mutualisation, offre de service

1 Introduction

1.1 Adage quesako

Dans le cadre de la labellisation des datacenters en région, les universités du Grand Est (Université de Haute Alsace, Université de Lorraine, Université de Reims Champagne Ardenne, Université de Strasbourg, et Université Technologique de Troyes) ont présenté un projet commun intitulé ADAGE : Alliance pour un DAtacenter en Grand Est (https://adage.esr-grandest.fr/). Les datacenters de Nancy et de Strasbourg ont été retenus pour l’hébergement des services, et celui de Reims associé pour le calcul.

Un certain nombre de services sont ou seront mis en place pour offrir des solutions communes à la communauté ESR de la région. Le premier en production est le BaaS : Backup As A Service.

1.2 Première offre de service à Strasbourg

En 2020, la Direction du Numérique de l'Université de Strasbourg (Unistra) a décidé de renouveler son infrastructure de sauvegarde. Ce projet visait non seulement à moderniser les capacités de sauvegarde pour les besoins internes, mais aussi à créer une offre de service de type Backup as a Service (BaaS) destinée aux laboratoires et composantes de l'université. L'objectif était de fournir une solution centralisée et évolutive, capable de répondre aux exigences croissantes de protection des données dans un environnement académique.

L'équipe en charge du projet a rencontré les principaux éditeurs de logiciels de sauvegarde sur le marché. Ces éditeurs ont d'abord été évalués sur la base de critères techniques précis et d'une première estimation financière. Cette première évaluation a permis de présélectionner cinq éditeurs pour une phase de Proof of Concept (POC).

Durant les POC, les différentes solutions ont été installées directement sur des serveurs de l'université, avec une assistance technique fournie par les éditeurs eux-mêmes. Un cahier de test commun a été utilisé pour évaluer chaque solution de manière homogène, et la même durée de cinq jours a été allouée à chaque POC afin de garantir une analyse approfondie et équitable.

À l'issue de ces tests, Commvault a été retenu comme solution finale. En plus de ses atouts techniques, comme la gestion multi-tenant et son interface web d'administration intuitive, Commvault permet aux utilisateurs de réaliser la quasi-totalité des tâches courantes d'administration, rendant la gestion des sauvegardes plus accessible et autonome. Ce choix a également été motivé par son adéquation financière avec les besoins à long terme de l'université.

1.3 Besoins lorrains (étude comparative, négociation des prix, ...)

L'université de Lorraine (UL) utilisait le logiciel TimeNavigator de la société Atempo avec un contrat de site pour 5 ans et une date d'échéance au 31 décembre 2022. Ce logiciel était présent à l'université depuis sa création en 2012 et était utilisé auparavant par trois des quatre universités fusionnées. Il était bien connu et maîtrisé par les équipes locales.

Atempo propose une licence site, calculée en fonction du nombre d'étudiants. Financièrement c'est intéressant lors de la construction des budgets.

Une nouvelle étude était nécessaire pour revoir l'architecture mise en place. En effet depuis nos premières installations, de nouvelles fonctionnalités étaient apparues sans que nous les mettions en œuvre : la sauvegarde des VMs, la déduplication à la source et les sauvegardes synthétiques pour n'en citer que quelques-unes. L'autonomie des administrateurs de serveurs devait rester totale pour les restaurations, une bonne gestion des droits était donc essentielle. Ceci est un résumé très rapide car la liste des attendus prendrait plusieurs pages. L'étude a été réalisée au cours de l'année 2022.

C'est à cette époque que le projet ADAGE a été lancé et il nous a semblé logique d'essayer de fusionner nos pratiques avec l'Unistra c'est ainsi que nous avons regardé plus en détails les possibilités du logiciel Commvault utilisé à Strasbourg.

Ce projet commun a nécessité plus de temps qu'initialement prévu et nous avons pu prolonger d'une année notre contrat avec Atempo.

Grâce à une modification des tarifs de Commvault, cette solution qui nous paraissait techniquement élaborée et répondant à nos besoins, mais financièrement inabordable a pu rentrer dans notre budget.

2 Présentation de Commvault et de ses composants

Nous souhaitons vous présenter les principaux éléments d'une infrastructure de sauvegarde Commvault et la manière dont nous les avons implémentés. Pour plus de détails, vous pouvez consulter le site officiel de Commvault (https://www.commvault.com/). Ce qui nous importe ici, c'est de montrer les fonctionnalités qui nous ont permis d'offrir un service fiable, sécurisé et redondant.

2.1 Commserve

Le Commserve est le serveur central d'une architecture Commvault, il assure plusieurs fonctions :

– *Coordination et gestion :* il agit comme le centre de contrôle pour l'ensemble du système de sauvegarde. Il coordonne toutes les opérations de sauvegarde, de restauration, d'archivage et de réplication de données.

– *Base de données et indexation* : il contient une base de données qui stocke des informations sur tous les fichiers, applications et machines gérés dans l'environnement. Cela permet une gestion et un suivi centralisés de toutes les activités de sauvegarde et de restauration.

– *Planification et orchestration des tâches :* il planifie et orchestre les tâches de sauvegarde et de restauration, en s'assurant que chaque opération est exécutée en fonction des politiques définies (fréquences, fenêtres de sauvegarde, rétention, etc.).

– *Reporting et monitoring :* il fournit des rapports détaillés sur l'état des sauvegardes, la consommation des ressources, les erreurs éventuelles, et les tendances. Il permet également un suivi en temps réel des opérations via une interface web.

– *Gestion multi-tenant* : il gère des environnements multi-tenant, il permet d'administrer plusieurs clients ou départements au sein de la même infrastructure, tout en maintenant l'isolation avec des politiques spécifiques pour chaque entité.

– *Sécurité et contrôle des accès* : il gère les droits d'accès, en permettant aux administrateurs de définir quels utilisateurs ou groupes peuvent accéder à certaines ressources ou effectuer des tâches spécifiques.

En cas de dysfonctionnement du CommServe, il est possible (et recommandé) de mettre en place une ou plusieurs autres machines appelées "CommServe LS" (pour Live Sync), qui peuvent prendre la main et devenir le serveur principal. Nous hébergeons le CommServe primaire à Strasbourg et le CommServe LS à Nancy. Ce sont des machines virtuelles (VMs) hébergées sur des hyperviseurs autonomes dédiés à la sauvegarde.

Le CommServe héberge l'interface d'administration de la solution. À l'origine, une interface Java était utilisée, mais elle a été remplacée par une interface Web au fil des évolutions. C'est cette interface qui permet aux administrateurs système de gérer les sauvegardes et les restaurations.

2.2 MediaAgents

Un Media Agent (MA) dans Commvault est un composant qui gère le flux de données entre les sources de données (clients) et les systèmes de stockage. Il assure les fonctions suivantes :

– *Gestion du transfert de données :* il est responsable du transfert des données de sauvegarde ou de restauration entre les machines clientes (serveurs, postes de travail, etc.) et les cibles de stockage (disques, bandes, stockage dans le cloud, etc.).

– *Déduplication* : il héberge la base de déduplication (DDB).

– *Répartition de charge* : dans des environnements où plusieurs MA sont déployés, Commvault répartit la charge de traitement des données entre eux, permettant une meilleure distribution des ressources et des performances accrues.

– *Tolérance aux pannes et reprise :* si un MA tombe en panne, un autre peut prendre le relais pour assurer la continuité des sauvegardes et restaurations, garantissant ainsi la disponibilité des données.

Nous avons choisi de sauvegarder uniquement sur disques, dans cette architecture un MA peut stocker jusqu'à 500 To de données. Nous avons choisi du matériel standard (serveurs Dell ou HPE), avec des disques internes et des baies de disques en attachement direct, ce qui permet de maintenir un coût du stockage bas. L'extension de volumétrie se fait par l'ajout de nouveaux MA. Chaque serveur doit inclure 4 à 5 To de disque flash pour la base de déduplication et les index.

On peut regrouper jusqu'à 4 MA dans une disklib virtuelle, qui sera vue comme un seul espace de stockage, ce qui permet une gestion plus simple et une optimisation de la déduplication.

Nous avons ainsi sept disklibs répartis dans nos datacenters de Strasbourg et de Nancy.

2.3 Access node

Un access node est un serveur, virtuel dans notre cas, qui sert d'intermédiaire pour le traitement et le transfert des données, pour la sauvegarde sans agents des VMs (VMware, Openstack, etc.), le stockage objet, ainsi que les systèmes de stockage NFS et CIFS.

Un VSA est un access node spécifique. Il discute directement, grâce aux API, avec la solution de virtualisation. Il extrait les snapshots, compresse, chiffre, et envoie les données vers le stockage via le MA.

Toutefois, les access nodes ne sont pas nécessaires pour les serveurs sur lesquels l'agent Commvault est déjà installé, car ces serveurs peuvent gérer directement les opérations de sauvegarde et de restauration.

Le nombre d'access nodes est à adapter en fonction de l'infrastructure et des performances souhaitées.

2.4 Mise à jour des agents

Commvault offre une fonctionnalité de mise à jour centralisée des agents, permettant de gérer facilement les mises à jour sur tous les clients à partir du CommServe. Cette fonctionnalité simplifie considérablement le processus de mise à jour et ne nécessite pas d'accès aux machines des utilisateurs de l'offre. Les serveurs de l'infrastructure Commvault bénéficient également de cette fonctionnalité.

2.5 Type de licences (à la VM, au To structuré ou non, ...)

Les tarifs des licences Commvault dépendent du type de données sauvegardées :

– *Serveurs virtuels* : une licence VM par serveur sauvegardé, sans limite de volumétrie.

– *Au To pour les données « non structurées »* : serveurs physiques, serveurs de fichiers et stockage objets.

– *Au To pour les données « structurées »* : base de données sur serveur physique et Kubernetes.

– *À la boîte mail* : Exchange ou Office 365.

L'ensemble des serveurs composant l'infrastructure de sauvegarde ne compte pas. Les données d'une VM sauvegardée soit au travers des snapshots, soit au travers de montages externes avec l'installation d'un agent ne compte que pour une licence VM (et donc pas de licence To).

2.6 Déduplication, sauvegarde synthétique, souplesse, plan de sauvegarde, gestion des droits

La solution permet de faire de la déduplication à la source et diminue ainsi l'usage du réseau. Il en est de même avec l'usage de sauvegardes synthétiques (reconstitution de sauvegardes *full* à partir de données connues des sauvegardes présentes) qui ne nécessite aucun échange réseau entre l'infrastructure et le serveur à sauvegarder.

Une sauvegarde se définit au travers d'un plan. Celui-ci va prendre en compte :

– *La planification* : quand, à quelle heure, la fréquence et les contraintes horaires (interdiction pendant les heures ouvrées par exemple).

– *Les données à sauvegarder* : où je les trouve, celles que j'exclus.

– *Le stockage* : primaire, copie éventuelle.

– *La parallélisation* : le nombre de sauvegardes possibles en même temps. C'est assez difficile à calculer.

Dans nos politiques actuelles, nous assurons une première sauvegarde dans le *datacenter* local, puis nous faisons une copie sur l'autre site.

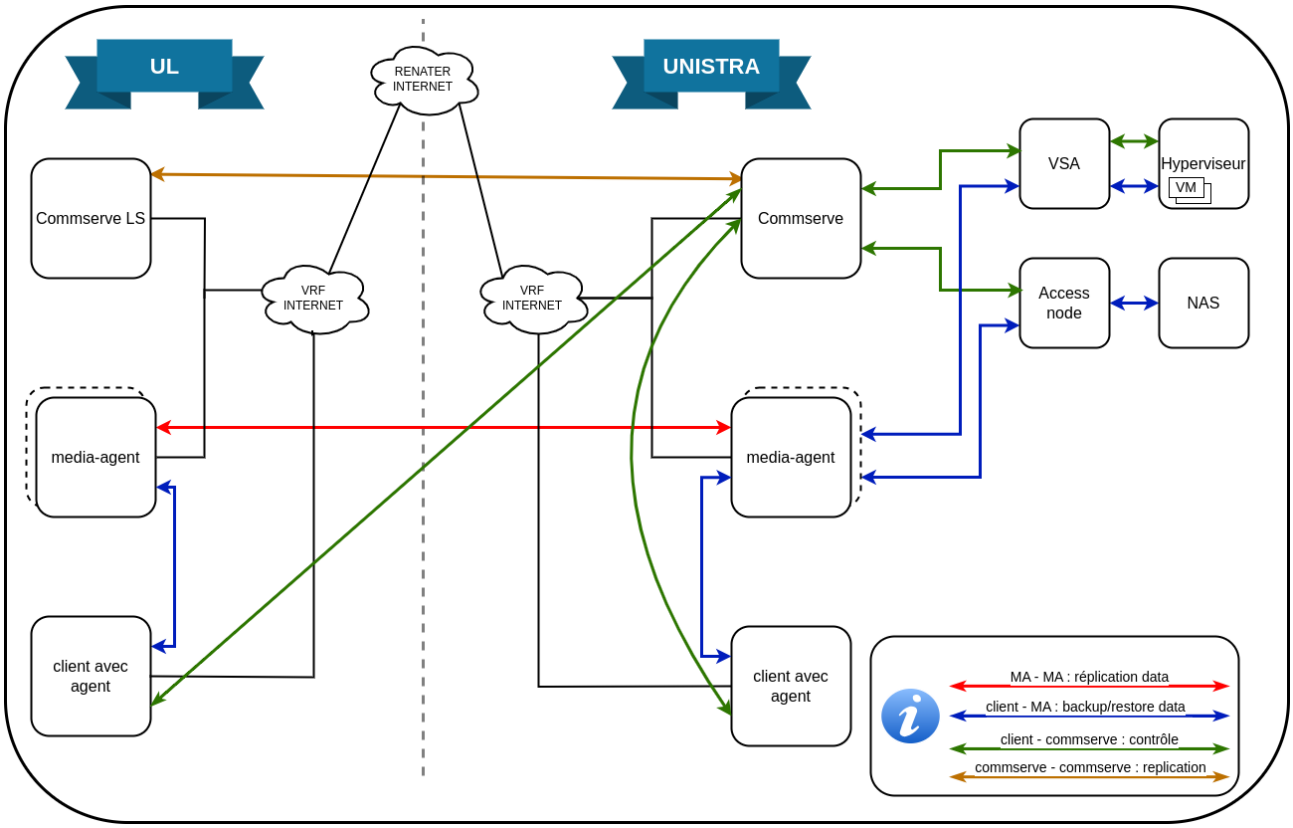
Les utilisateurs sont définis en interne et regroupés pour gérer leurs droits. Nous n'avons pas souhaité, même si c'est possible, de liaison avec les SI des établissements pour des questions de sécurité : la compromission des comptes administrateurs AD est un vecteur d'attaques fréquemment utilisé pour altérer des données de sauvegarde.

3 Mise en place de l'architecture et des offres de services

3.1 Évolution de la solution retenue pour étendre à plusieurs établissements (principe de gestion inter équipes)

3.1.1 Infrastructure matérielle mise en place sur chacun des sites

Voici un schéma de l'infrastructure mise en place. Pour le simplifier, nous n'avons pas reporté la partie VSA et access node à l'UL, mais c'est la même chose avec les flux de contrôle vers le Commserve et les flux de données vers les MA locaux.



Nous avons, dans chacune des deux universités, des MA spécifiques et des MA pour la réplication de l'autre :

– Pour l'UNISTRA, cela représente 1 Po pour le local et 1 Po pour la la réplication de l'UL.

– Pour l'UL, nous avons 2 Po pour le local[1] et 1 Po pour la réplication de l'UNISTRA.

Actuellement nous offrons des services de sauvegarde :

– Avec un agent installé sur le serveur, les fichiers locaux ou distants type NFS, CephFS ...

– Avec un proxy spécifique pour la sauvegarde des NAS en NDMP, NFS ou CIFS ou des buckets S3.

1 l'UL n'utilise pas la totalité de ses 2Po, c'est pour cette raison que la réplication vers l'Unistra ne nécessite pas encore de volume supérieur à 1Po

– Avec des VSA, pour une sauvegarde sans agent des VMs (OpenStack, VMware ...), il en faut au moins un par infrastructure d'hyperviseurs ou projet OpenStack.

La multiplication des VSA permet d'augmenter le parallélisme des sauvegardes et donc de tenir dans les fenêtres de sauvegarde de nuit (sauf pour les sauvegardes les plus volumineuses de plusieurs To). La déduplication à la source n'empêche pas le parcours d'arbre lorsque des mécanismes de type Change Block Tracking (CBT) ne peuvent être mis en œuvre.

3.1.2 Liaison réseau spécifique (routage à la source)

Renater, à notre demande, a mis en place une liaison spécifique directement entre nos deux datacenters. À ce jour, pendant la phase de test, nous avons 3 x 10 Gb/s. À terme il est prévu un passage à 100 Gb/s.

L'infrastructure étant répartie, l'usage dans chacune de nos universités de réseaux privés a contraint nos équipes réseaux respectives à mettre en place un routage à la source naté (SNAT). Cela permet ainsi aux machines accessibles uniquement en réseau privé d'une université d'être accessible aux serveurs de l'autre université. Dans les faits, toutes les communications vers les serveurs de l'infrastructure situés sur la seconde université passent par ce lien, qu'elles soient en adressage public ou privé. L'usage de VRF (Virtual Routing and Forwarding) permet de forcer ce routage.

Le logiciel de sauvegarde permet de définir des topologies spécifiques. Par exemple, un serveur privé va ouvrir et maintenir une connexion avec le serveur principal pour ensuite permettre l'échange dans les deux sens. Dans cette topologie, appelée oneway c'est le client qui ouvre les connexions. Si rien n'est précisé, c'est le serveur qui ouvre les connexions.

3.1.3 Facturation (forfait : vm, espace disque, duplication 2 sites, ...)

Tout d'abord, pour accéder au service, il faut être membre de la communauté ESR de la région ou bien être hébergé sur des infrastructures localisées dans nos datacenters (cas de l'AMUE par exemple).

Ensuite, nous mettons en place une convention définissant le niveau de service, les engagements de chacun, la durée, etc.

Au vu du système de tarification de l'éditeur, deux éléments entrent dans le calcul des coûts : le nombre de VMs ou de To pour les machines physiques (coût des licences), puis nous rajoutons bien évidemment :

– nos coûts d'infrastructure (hébergement, fluides, MA, hyperviseurs spécifiques …),

– le coût RH de la gestion de la solution,

– la possibilité ou non de dupliquer la sauvegarde sur l'autre université. Ceci est fortement conseillé.

La tarification n'est pas encore définitivement fixée à ce jour.

3.2 Les tenants (avantages, inconvénients, ...)

Commvault offre des capacités multi-tenant qui permettent de gérer plusieurs entités ou clients au sein d'une même infrastructure, tout en maintenant l'isolement et la personnalisation pour chaque tenant.

Un administrateur de tenant est autonome pour l'exploitation de ses sauvegardes, il pourra par exemple :

– sauvegarder de nouvelles machines et leur associer le plan de sauvegarde adapté,

– modifier les horaires de sauvegardes,

– restaurer ses données,

– paramétrer des alertes,

– exécuter des tâches de reporting,

– création d'utilisateurs locaux au sein du tenant.

L'intervention d'un administrateur de l'infrastructure sera uniquement nécessaire si l'utilisateur souhaite modifier la durée de rétention des données au sein de ses plans de sauvegarde.

3.3 Les problèmes rencontrés

Dans un tel projet, mélangeant des informaticiens de deux universités, quelques problèmes sont apparus au cours du temps.

3.3.1 Prise en compte de l'humain

Tout d'abord un problème humain (mais pas de personne ;)) est apparu : la gestion des projets et les missions des personnels diffèrent entre les universités. Il a fallu que chacun comprenne le fonctionnement de l'autre. À partir de là, les différents besoins ont pu être intégrés pour être pris en compte.

La gestion en *tenants* a offert la possibilité aux deux établissements d'opérer de manière légèrement différente : l'UL avait l'habitude de tout gérer pour les administrateurs de serveurs, alors qu'à l'Unistra, les administrateurs de tenant sont complètement autonomes.

Le nommage des objets est important pour retrouver ses petits : leur pré-fixage court permet de savoir à qui il appartient, ce n'était pas forcément utile auparavant lorsqu'un seul établissement exploitait la solution.

3.3.2 La technique

L'expérience de l'Unistra a permis de comprendre la mise en œuvre d'une telle solution complexe pour arriver ensuite à une réalisation exploitable facilement.

Après une première installation avec un partenaire local, l'infrastructure nécessaire avait été définie pour l'Unistra, celle-ci a été étendue ensuite pour intégrer l'UL.

Une formation de l'ensemble de l'équipe par l'éditeur a soudé celle-ci. Le langage est devenu commun, les procédures ont pu être définies.

Les deux équipes réseaux travaillent ensemble depuis un moment déjà. La solution proposée devrait permettre d'étendre celle-ci à d'autres services que la sauvegarde. Il est envisagé par exemple d'offrir dans chacun des *datacenters* de l'hébergement pour l'autre et de mettre ainsi en place des PRA/PCA, du stockage redondant (Ceph ou NAS)...

Pour le moment, le routage assuré par Renater ne permet pas de faire basculer facilement le serveur principal vers un LS situé dans l'autre université, c'est un point que nous allons étudier plus en détail car la perte du site de l'Unistra, qui est maître sur le réseau du serveur principal, empêcherait toute sauvegarde/restauration à l'UL.

3.3.3 Les licences

Il a été très compliqué de comprendre la notion de licence et en particulier l'usage des licences au To. C'est en regardant comment était calculé notre décompte que nous avons enfin compris qu'un agent sur une VM ne consommait rien (dans notre version actuelle du logiciel), que ce soient des To structurés ou non.

Pour l'éditeur, un établissement est égal à un compte (CID = Commvault ID). Il a fallu faire accepter que quel que soit l'émetteur du bon de commande (Unistra ou UL), il fallait le relier au même CID, tout en gardant la possibilité à l'avenir que chacun reprenne ses achats.

Pour un partenaire, il a donc été décidé que l'achat de licences se ferait soit par l'Unistra, soit par l'UL pour simplifier. On demande un engagement du partenaire pour couvrir l'investissement initial. Les souscriptions sont soit sur 3 ans, soit sur 5 ans.

4 Bilan d'exploitation

Au 15 septembre 2024, nous sauvegardons 2400 serveurs découpés en 2200 VM et 440 serveurs avec agents[2], ceci réparti sur 35 tenants.

Cela représente 2,7 Po sur disques en primaire sur nos MA et 1,7 Po en secondaire.

Chaque jour, nous avons 2800 jobs de sauvegardes pour quelques jobs de restauration.

Notre taux moyen de déduplication tourne autour de 6,25.

Le débit réseau moyen entre nos deux *datacenters* se situe aux alentours de 330 Mbits/s (sens ULUnistra) et 500 Mbits/s (sens Unistra-UL) avec des pointes à 12,5 Gbits/s dans chaque sens.

Dans le cadre de la sauvegarde, sortir la donnée de son environnement est très important. Sur certains types de gros volumes (Ceph...) nous pouvons, de temps en temps, faire une sauvegarde hebdomadaire pour repartir en cas de crash.

5 Avenir

Que nous reste-t-il à faire dans un avenir proche ? Quels points nous semblent importants, en voici une courte liste :

– Pour le moment, nous n'avons pas mis en place d'immuabilité des sauvegardes. Ceci est possible sur du stockage objets S3. Étant donné que chaque université possède des clusters Ceph, il reste à définir où mettre les sauvegardes, la durée et le volume nécessaire.

– L'analyse des malwares est possible sur des MA sous Windows, nous attendons donc une version plus récente qui apportera cette fonctionnalité sous Linux.

– De nouveaux hyperviseurs sont en cours de déploiement dans nos universités. C'est le cas de Proxmox par exemple. Commvault n'est pas capable de sauvegarder sans agent ce type d'hyperviseur. Nous attendons des solutions plus centralisées, comme pour les VMs avec la possibilité alors de prendre des *snapshots* et donc de réaliser des *backups* plus consistants.

– Enfin, nous déployons des clusters Kubernetes. La gestion des licences, dans notre version, n'est pas raisonnable (une VM par objet). La version 10.34, annoncée en septembre, intégrera cet aspect.

2 Une VM peut contenir un agent, ce qui explique la différence sur les totaux.

6 Conclusion

Les utilisateurs de l'offre sont globalement satisfaits, ils apprécient l'autonomie que leur confère la solution. Une fois ceux-ci intégrés, les coûts d'exploitation de la solution restent raisonnables, grâce à l'efficacité de l'administration centralisée et des outils de gestion.

La mutualisation entre les sites de Strasbourg et Nancy a renforcé la fiabilité du service, en permettant la réplication des données entre les deux sites, offrant ainsi une meilleure résilience et sécurité des sauvegardes. Cette mutualisation permet de diminuer les coûts et d’offrir un service de qualité y compris aux petites structures.

Ce qui nous semble capital, c’est et ce sera toujours l’intégrité des sauvegardes des données et des configurations pour pouvoir repartir rapidement en cas de problème.