Article : Plateformes mutualisées sur Grenoble : Virtualisation & Stockage - Automatisation & Modèle économique

Mathieu Panel
DGDSI Université Grenoble Alpes
43 Rue des Mathématiques
38400 Saint Martin d'Hères

Guenael Sanchez
DGDSI Université Grenoble Alpes
43 Rue des Mathématiques
38400 Saint Martin d'Hères

Résumé

L'Université Grenoble Alpes porte depuis 5 ans des plateformes mutualisées autour des thématiques du stockage de données (SUMMER), de la virtualisation (WINTER) et du cœur de réseau pour les DataCentres (SPRING).

Ces plateformes connaissent un engouement certain dans la communauté universitaire. Ainsi SUMMER dépasse les 3 Péta-octets de stockage, WINTER s'approche des 1.000 machines virtuelles hébergées et SPRING compte désormais 1.700 ports réseau, représentant une centaine d'ayant-droits différents, chacun bénéficiant d'accès délégués aux outils métiers.

Cette montée en puissance amène des défis importants pour les équipes en charge. Comment formaliser, faciliter et automatiser les différents processus métiers ? Du provisionnement d'espace de stockage ou de machine virtuelle, en passant par la configuration réseau, la délégation des accès aux services, les validations hiérarchiques, la facturation ou le suivi des contrats de location. Comment ne rien oublier, éviter les tâches rébarbatives, suivre les demandes dans le temps ?

Grâce à un partenariat entre les équipes techniques et administratives, nous vous présenterons les outils mis en place pour fluidifier les différentes procédures, et proposer des tableaux de bord pertinents. Nous aborderons également le côté organisationnel humain, en détaillant les rôles et les fonctions des différents acteurs, de l'utilisateur au personnel administratif, en passant par les différentes équipes techniques. En nous appuyant sur les technologies BonitaSoft, sur les API des outils VMware, Netapp et Cisco, et sur les outils issus de notre référentiel BIPER, nous regarderons comment a été construit le dialogue entre ces différentes briques, guidée par les modélisations BPMN des processus métiers.

Mots-clefs

Virrtualisation, Stockage, Mutualisation, Automatisation, Modèle économique.

1 Contexte Grenoblois

L'Université Grenoble Alpes regroupe, depuis 2016, les trois Universités historiques du bassin Grenoblois. Bientôt, l'UGA, structurée en *UI* (Université Intégrée), comptera dans ses rangs, les autres structures d'enseignement supérieur / recherche comme Grenoble INP, etc.

Suite à une enquête réalisée en 2013 sur les besoins de stockage de données, et le recensement des infrastructures matérielles existantes, le constat de la multiplicité des solutions disséminées dans de "petites" salles machine est posé.

Dans un souci de rationaliser les dépenses, liées au fonctionnement et à la maintenance de ces installations, et dans l'espoir d'une économie d'échelle, l'Université de Grenoble lance plusieurs projets mutualisés sur les thématiques : Stockage de données, Réseau des DataCentre & Virtualisation.

Dans cet article, nous vous présentons ces plateformes, leurs modes de fonctionnement, tant technique qu'humain, leurs interactions, et le modèle économique associé à chacune d'entre elles.

Nous conclurons sur quelques retours d'expérience, tant du point de vue utilisateur, qu'administrateur, ou financier.

2 Plateforme SPRING – Réseau des DataCentres

La plateforme SPRING [1] fournit du réseau 10G/40G aux différents matériels installés dans les 3 DataCentre retenus par l'UGA dans sa politique de rationalisation des salles machines.

Ces 3 DataCentre offrent des niveaux de sécurisation climatique, énergétique & d'accès différents selon les besoins de l'utilisateur concerné.

La plateforme SPRING est administrée par une équipe d'une dizaine de personnes, issues des milieux de la recherche ou des DSI, et consacrent chacun environ 20% de leur temps de travail à cette tâche.

Les plateformes SUMMER & WINTER, décrite dans ce document sont connectées ou en cours de raccordement au réseau SPRING. Le choix technique de SPRING de partir sur une fabrique IP Cisco ACI permet une intégration et des interactions poussées entre les différents projets qui sont décrites dans les paragraphes suivants.

3 Plateforme WINTER – Virtualisation

La plateforme WINTER [2] est désormais en vitesse de croisière ! Avec plus de 1 000 VMs hébergées, pour une quarantaine d'ayants droit différents, la DSI bien sûr, mais aussi des laboratoires, UFR ou autres projets divers.

Nous sommes dans la troisième année de fonctionnement, et nos objectifs initiaux en terme de quantité de calcul, mémoire vive et stockage sont atteints deux ans avant la date prévue ! Nous nous engageons donc dans une politique de renouvellement du matériel par tranches successives pour faire face sereinement à la demande grandissante.

Une dizaine de personnes compose le Comité Technique WINTER, en charge de l'administration de la plateforme. Nous avons élaboré des procédures afin d'essayer de ne rien oublier dans la réalisation des différentes tâches récurrentes.

L'erreur étant humaine, et les tâches répétitives, nous avons démarré une réflexion sur l'automatisation possible autour de la plateforme WINTER. Nous avons souhaité, dès le départ, que les utilisateurs de la plateforme soient le plus autonomes possible dans les différentes tâches du quotidien d'un administrateur de machines virtuelles :

- Demander la création de nouvelles VMs ;
- Donner/Enlever des droits d'administration à des tiers ;
- Sauvegardes supplémentaires (instantanés) et restauration self-service ;
- Demander des autorisations réseau, des alias DNS, etc.

La mise en place de ces délégations implique d'interagir avec plusieurs outils différents. Tant pour l'utilisateur final que pour les administrateurs de la plateforme. D'où la nécessité de développer l'automatisation des tâches.

3.1 Automatisation

3.1.1 Fonctionnement général

Un workflow pour simplifier, centraliser et piloter ces différentes étapes a été créé. Il a nécessité une réflexion autour des différents acteurs des différentes tâches pour affiner les droits de chacun. Ce processus est ajouté au panel d'applications de la DGD-SI et est déployé sur la plateforme Bonita[1] de l'établissement.

Les différentes interactions avec le système d'information sont assurées par des connecteurs (JAVA) en entrée ou en sortie des tâches. La création et la configuration de machines virtuelles se font via les API REST VMware.

Sur le schéma BPNM ci-dessous, on retrouve les 3 lanes BPNM regroupant les acteurs du processus : demandeur, technique et administration. Le demandeur saisit les informations requises à sa demande de création de VM puis, à la validation de son formulaire un cas du processus est instancié. Il y a ensuite une validation faite par les

1. Bonita est une plateforme d'automatisation des processus, qui permet leur création, intégration exploitation et suivis.

équipes techniques ainsi qu'un enrichissement des données (type de matériel, contraintes liées aux os..). Le cas est ensuite aiguillé aux responsables administratifs pour la facturation. Les connecteurs de notifications informent en continu l'ordonnateur de l'entité hébergée.

Les acteurs des différentes tâches sont récupérés depuis notre référentiel de rôle, mais un filtre d'acteur peut aussi être associé à un groupe LDAP. Les notifications sont également assurées par des connecteurs et peuvent contenir n'importe quelle variable du workflow.

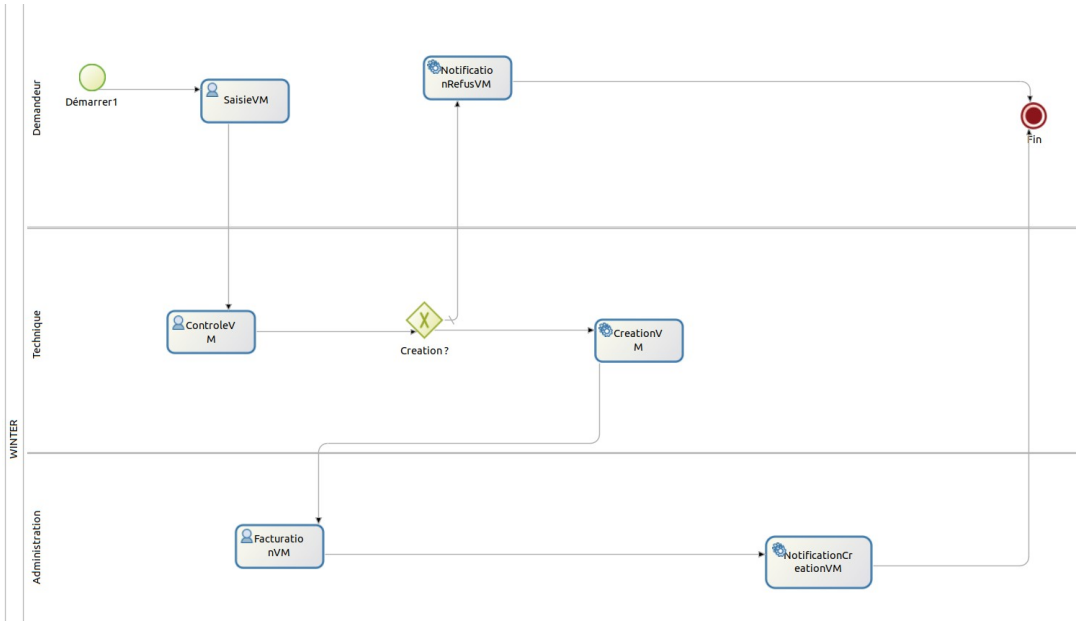

Figure 1: Représentation d'un workflow dans l'outil Bonita

Les différents connecteurs associés aux tâches :

- Saisie VM : Contrôle des droits (requête dans notre référentiel, Mysql) ;
- Contrôle VM : Notification (notification des équipes techniques qu'une tâche est disponible : Connecteur natif Bonita), API REST VM (création de la VM, JAVA, REST).

L'utilisation du moteur de workflow Bonita permet un reporting des différents cas instanciés. Ces données sont également "requêtable" via les API de Bonita pour les intégrer dans d'autres applications.

3.1.2 Interface avec VMware

Pour créer les machines virtuelles dans VMware, nous utilisons l'API REST mise à disposition. L'appel à l'API se fait dans un connecteur en sortie de la tâche ControleVM (cf. schéma ci-dessus).

Une fois authentifié via l'API, un objet JSON (exemple en annexe) est construit avec les données saisies dans les différents formulaires du processus. Cet objet est ensuite posté à l'API pour la création de la VM. L'organisation dans les différents "folders" de Vmware peut également être pilotée par l'API, nous pouvons par exemple organiser les VM par Laboratoire, UFR ou toute autre entité.

3.1.3 Prochaines évolutions

La force d'un outil de workflow est la facilité de mise en œuvre de l'évolution des processus. Nous serons donc capables d'ajouter les différents acteurs souhaitant s'intégrer à celui-ci. Nous envisageons déjà d'impliquer les équipes réseaux avec le pilotage du filtrage, du DNS et du DHCP. Il est également possible d'enrichir les liens avec le système d'information en ajoutant des connecteurs, par exemple celui avec SIFAC[2].

4 Plateforme SUMMER

La plateforme SUMMER [3] continue sur sa lancée ! Nous avons dépassé 3To de données stockées pour une quarantaine d'ayants droit, que ce soit des services administratifs ou des unités/laboratoires de recherche.

Le renouvellement par tranches successives de l'infrastructure, et l'ajout régulier de nouvelles briques de stockage, nous a permis, de revoir notre politique tarifaire à la baisse, permettant au plus grand nombre d'utilisateurs d'accéder au service.

Une douzaine de personnes, informaticiens à la DSI, en laboratoire ou en UFR, dédient 20 % de leurs temps de travail pour les différentes tâches afférentes à la plateforme.

Afin de répondre plus largement aux diverses demandes des utilisateurs, le catalogue de services de la plateforme SUMMER s'est considérablement agrandi. Initialement prévue pour ne stocker principalement que du mode bloc, c'est finalement un usage en mode fichiers qui l'emporte (et de très loin). De nouveaux besoins apparaissent également comme le stockage objet sur lequel nous sommes en phase de tests.

L'intégration poussée avec l'Active Directory de l'UGA a permis au plus grand nombre, de bénéficier d'un partage de fichier authentifié, sans avoir besoin de dupliquer tout ou partie du référentiel des utilisateurs, avec toutes les problématiques que cela peut entraîner (accès à un mot de passe unique, synchronisation, etc.).

L'intégration la plus aboutie est une application en ligne, basée sur le référentiel UGA, dénommée "Dossiers Partagés". Cette application permet à un public non-informaticien de créer & gérer une arborescence de dossiers, et de piloter les groupes d'accès en lecture seule ou lecture/écriture.

Exemple : La responsable administrative d'un laboratoire peut créer divers répertoires sur son espace de stockage, par projets de recherche par exemple, et donner aux différentes équipes les droits de "contributeurs" (lecture/écriture) sur leurs dossiers. Quand une personne arrive (ou part) du SI, ses droits sont automatiquement propagés sur les partages de fichiers.

Cette intégration entre Stockage, Active Directory & référentiel de l'UGA nécessite une bonne dose d'automatisation et d'interactions entre les différentes briques.

2. Outil de Gestion Financière et Comptable (GFC)

À noter que si un ayant-droit souhaite utiliser son propre référentiel (Active Directory, Samba, LDAP), cela reste possible, mais il ne pourra alors bénéficier des outils d'automatisation.

4.1 Automatisation

4.1.1 Fonctionnement

L'application "Dossiers Partagés" est une vue spécifique de notre référentiel des groupes et des personnes. À chaque action elle génère un message qui est envoyé à notre courtier de messages (broker protocol AMQP, Rabbit MQ). Ce message est ensuite consommé par un client qui va créer ou peupler les groupes dans l'Active Directory et appliquer les ACLs nécessaires sur les dossiers. L'architecture avec broker permet de simplifier la communication entre les différents clients et éventuellement d'en ajouter. Elle nous donne également une vision sur le nombre de messages transmis et sur la consommation de ces derniers. Nous pouvons mettre efficacement les clients à jour sans risque de perte de message, ils sont stockés dans la file AMQP et seront consommés quand le consommateur se reconnectera dessus.

4.1.2 Application "Dossiers Partagés"

Cette application permet de donner des droits à des personnes et des groupes sur des dossiers. Elle contrôle la cohérence des droits appliqués, une personne n'ayant pas de droit de lecture dans un dossier parent ne peut pas avoir de droit dans le dossier enfant. Deux types de dossiers peuvent être créés : dossiers de types feuilles terminales (gestion des sous dossiers dans le navigateur de fichier de l'utilisateur) et dossiers de types applications (gestion uniquement via l'application). À chaque action un message JSON est généré et publié sur la file AMQP adéquate. Les messages sont : soit donner/retirer des accès à une personne sur un répertoire, soit créer un répertoire, soit supprimer un répertoire. La gestion des espaces partagés est cloisonnée, les ayants droit peuvent gérer de façon autonome leurs espaces. Il est également possible de définir des profils gestionnaires pour faciliter l'assistance et l'accompagnement des ayants droit.

4.1.3 Consommateur

Le consommateur est codé en JAVA et écoute en permanence la file AMQP. Il interprète les messages puis exécute les actions. Trois types de droits sont disponibles lecteur, contributeur et gestionnaire. Les groupes venant de l'application "Dossiers Partagés" sont remis à plat et répartis dans des groupes avec la syntaxe suivante partage_[type_droit]_[id_dossier]. Une ACL est ensuite appliquée sur le dossier avec ce groupe et les droits "Windows".

Exemple de droits :

```
AclEntryPermission.READ_DATA,
AclEntryPermission.READ_ACL,
AclEntryPermission.READ_ATTRIBUTES,
AclEntryPermission.READ_NAMED_ATTRS,
AclEntryPermission.WRITE_DATA,
AclEntryPermission.EXECUTE,
AclEntryPermission.APPEND_DATA,
AclEntryPermission.DELETE_CHILD,
AclEntryPermission.SYNCHRONIZE
```

À la création des dossiers des contrôles d'unicités sont faits (en plus de ceux de l'application "Dossiers Partagés") et récupérés dans des exceptions afin d'être loggués. La suppression se passe en deux phases, une première où le consommateur masque le dossier et retire l'ACL, et une deuxième où un script périodique supprime définitivement tous les dossiers masqués depuis 6 mois. Un système de rotation de log (log4j) permet un dépannage et un suivi efficace.

5 Modèles économiques

Bien que les investissements initiaux soient réalisés par l'UGA, les différents services fournis par les plateformes SUMMER & WINTER ne sont pas offerts aux usagers. Une politique de refacturation a été mise en place, validée par les instances de l'UGA et est régulièrement révisée (à la baisse) en fonction des investissements & jouvences réalisés.

N'ayant pas de vocation commerciale et/ou lucrative, la politique tarifaire ne cherche pas nécessairement un équilibre ou un bénéfice financier. Le curseur doit être réglé de manière subtile entre incitation financière forte des utilisateurs à adhérer aux services de ces plateformes mutualisées, et la recherche d'un certain équilibre financier pour l'établissement.

Premier critère, le rattachement administratif de l'ayant droit. L'UGA a choisi de ne jamais répercuter les coûts liés aux ressources humaines dédiées au projet, les fluides ou les infrastructures techniques pour les structures sous tutelle UGA. Si l'entité appartient à la COMUE grenobloise, une participation à hauteur de 50% de ces frais est incluse dans la facturation. Enfin, lorsqu'il s'agit de structures extérieures à la COMUE, 100% des frais dits "frais d'infrastructure" sont facturés.

C'est le cas notamment, de certains prestataires privés (conventionnés UGA et Renater), qui hébergent données et/ou machines virtuelles sur SUMMER & WINTER.

À côté de ces frais d'infrastructures, il était nécessaire de trouver un moyen de facturation le plus juste possible. Pour WINTER, les axes de calcul se sont orientés autour des coûts unitaires pour :

- 1 coeur logique (vCPU) ;
- 1Go de mémoire vive (RAM) ;
- 1Go de stockage ;
- 1Go de sauvegarde (optionnel) .

Les tarifs sont modulés par le niveau de service attendu :

- VM critique : on s'attend à ce que la VM soit redémarrée en cas de défaillance d'un DataCentre.
  - Le coût du vCPU est doublé car réservé en double ;
  - Le coût du Go de RAM est doublé car réservé en double ;
  - Le coût du Go de stockage est doublé car répliqué de manière synchrone .
- VM "normale" : on ne s'attend pas à ce que la VM soit redémarrée en cas de défaillance, mais on souhaite tout de même que son stockage soit répliqué pour éviter une perte de données ;
- VM non-critique : niveau de service minimum.

Ces coûts unitaires ont été calculés sur la base des coûts d'investissements matériels (serveurs hôtes) et logiciels (licences VMware/VSAN/vCenter/VEEAM).

Pour nous situer, et garder une capacité d'incitation, nous avons fait comparer ces coûts à diverses offres privées accessibles en ligne. Les tarifs WINTER restent globalement dans les tarifs habituellement pratiqués pour ce type de service.

Pour le stockage de données sur SUMMER, la philosophie est un peu différente. l'UGA ne refacture que le coût de la volumétrie. Le prix des contrôleurs de stockage Netapp [3] reste à charge de l'UGA.

SUMMER offre également plusieurs niveaux de classe de service :

- Stockage simple : la donnée est stockée de manière redondée sur un seul site ;
- Stockage sauvegardé : la donnée est dupliquée quotidiennement sur un site tiers avec 30 jours d'historique :
  - Le coût du To est d'environ 180 % le prix du To "simple" ;
- Stockage répliqué synchrone : la donnée est dupliquée en temps réel, de manière synchrone sur un site tiers :
  - Le coût du To est d'environ 190 % le prix du To "simple".

Il est possible de combiner réplication & sauvegarde. Nos offres commencent à partir d'une location minimale de 5To.

Pour les plus petits utilisateurs, de plus en plus nombreux, souhaitant acquérir une petite volumétrie (de 500Go à 5To), nous avons développé une offre simplifiée, et un prix divisé par deux, voire gratuit dans certains cas. Le but étant d'éviter, autant que possible, l'utilisation de disques durs externes, non sécurisés, non chiffrés & fragiles.

Nous réfléchissons également à un modèle financier dégressif pour les ayant-droits dépassant 50 To de données.

Le bilan investissements versus “revenus locatifs”, est malgré tout, assez proche de l’équilibre, pour chacune des plateformes.

Un des aspects, non calculé ici, sont également les économies d’échelles réalisées par la réduction ou, a minima, la “non création” de nouvelles “salles machines” avec tous les frais qui en dépendent.

6 Conclusion

Avec 5 ans de recul sur le stockage mutualisé, et un peu plus de 2 ans concernant la virtualisation, nous constatons que ces deux plateformes répondent à un besoin fort et grandissant de la communauté grenobloise. Du point de vue technique, ces deux plateformes donnent une entière satisfaction et ont démontré leur capacité d’adaptation et d’évolution aux besoins des utilisateurs du site.

Entre les structures qui n’ont pas les moyens humains / financiers / techniques de mettre en œuvre de telles solutions, et ceux qui auraient les moyens mais préfèrent mettre leurs efforts ailleurs et profiter de ces outils mutualisés, tous les indicateurs de suivi sont en progression ! Ces choix économiques, validés politiquement, sont cohérents avec les capacités de financement des ayants droit, et le prix de solutions alternatives disponibles sur le marché.

Néanmoins, notre point de vigilance se situe davantage sur les équipes en charge de l’administration et de l’évolution de ces plateformes. Aujourd’hui, les équipes dégagent l’équivalent de 20 % d’ETP chacun, mais nous ressentons de plus en plus le besoin de renforcer nos équipes, tant en nombre qu’en compétences.

La diversification des catalogues de service est une richesse pour l’utilisateur mais un casse-tête pour les équipes techniques, nous obligeant à certains choix. Exemple pour SUMMER et le stockage mutualisé, certaines spécificités du catalogue sont désormais l’apanage de binômes/trinômes quand auparavant, toute l’équipe était capable de gérer l’ensemble du service proposé. Néanmoins, cela reste pour les personnes du comité technique, l’occasion unique de pouvoir monter en compétence sur des matériels et technologies qu’ils n’auraient pu acquérir seuls.

Bibliographie

[1] Julien Tomassone *et al*. ACI, la solution SDN du datacentre de la Communauté Université Grenoble Alpes. Dans Actes du congrès JRES2017, Montpellier, Novembre 2017 ; https://conf-ng.jres.org/2017/document_revision_1910.html?download

[2] Guenael Sanchez et al. WINTER : virtualisation hyperconvergée Full-Flash multi-site. Dans Actes du congrès JRES2017, Montpellier, Novembre 2017 ; https://conf-ng.jres.org/2017/document_revision_1923.html?download

[3] Dimitri Rapacchi et al. SUMMER : 4 ans de stockage mutualisé et réparti. Dans Actes du congrès JRES2017, Montpellier, Novembre 2017 ; https://conf-ng.jres.org/2017/document_revision_2869.html?download