

Service de messagerie communauté enseignement/recherche (PARTAGE)

Laurent Aublet-Cuvelier

GIP RENATER
23-25, rue Daviel
75013 Paris

Ludovic Ishiomin

GIP RENATER
23-25, rue Daviel
75013 Paris

Didier Benza

Mission Sécurité-Défense, INRIA
2004, route des Lucioles
06902 Sophia-Antipolis

Résumé

Le projet de Messagerie collaborative a été initié par le GIP RENATER à la demande du Groupe de Consultation sur les Services (des experts issus des membres du GIP). Ce groupe a fixé les objectifs du projet : mettre en œuvre un service de messagerie mutualisé pour l'enseignement et la recherche et comprenant des extensions collaboratives. Ce service devait par ailleurs respecter des exigences de sécurité et de disponibilité très élevées.

Nous décrivons le périmètre fonctionnel de la plate-forme, du point de vue de l'utilisateur final (messagerie, agenda, tâches, partages, etc.) mais aussi du point de vue des administrateurs du système d'information des établissements utilisateurs du service. Nous présentons le système de support fonctionnel et opérationnel de la plate-forme, l'interface dont disposeront les services informatiques des établissements. Parallèlement, nous décrivons les engagements de niveau de service.

Nous exposons l'implémentation de la plate-forme : outre l'architecture globale du service, nous donnons des indications sur l'infrastructure IaaS qui héberge la plate-forme et les interactions avec les couches logicielles qui fournissent le service (notamment à travers les systèmes de support opérationnel). En effet, l'infrastructure d'hébergement, d'une part, et le service de messagerie, d'autre part, sont fournis par deux prestataires différents, pilotés par le GIP.

Enfin, nous présentons les perspectives d'évolution à différents niveaux : d'une part, les optimisations possibles de l'infrastructure pour suivre la croissance de la plate-forme, via l'utilisation de technologies différentes, par exemple ; d'autre part, les évolutions fonctionnelles envisagées, comme l'intégration avec d'autres outils collaboratifs.

Mots-clefs

Messagerie, Agenda, Tâches, Intégration, Délégation d'administration, API, SaaS, IaaS, SLA

1 Introduction

Le Groupe de Consultation sur les Services (GCS) est un groupe d'experts issus des établissements membres du GIP RENATER. Il étudie, conseille ou préconise des évolutions dans l'offre de service du GIP. La messagerie électronique est le premier service auquel ce groupe s'est intéressé, car il y voyait des possibilités très intéressantes de mutualisation de moyens et des gains importants pour les utilisateurs, en termes de disponibilité notamment.

Après quelques échanges avec les acteurs de la communauté afin de valider le potentiel du service et son intérêt pour les établissements, le GIP RENATER a donc lancé un projet de service de messagerie autour d'un groupe d'établissements pilotes. L'appel d'offres a été organisé pendant l'été 2013 et le service est actuellement en cours de déploiement. Il a été nommé PARTAGE [1] : une messagerie collaborative « as a Service » spécialisée pour l'enseignement et la recherche.

L'objet de cet article est de présenter les grandes fonctionnalités disponibles dès le démarrage du service PARTAGE. Nous détaillons aussi certains éléments de l'infrastructure qui l'héberge.

2 Présentation générale

2.1 Etude fonctionnelle avancée

Le GCS avait déjà très largement décrit le besoin fonctionnel et les objectifs en terme de niveau de service et tarifaire. Nous avons néanmoins complété cette analyse initiale par une étude approfondie du besoin fonctionnel, notamment à l'aide de questionnaires et d'échanges avec les établissements candidats à la phase pilote. Nous avons dû trouver ensemble le bon niveau de compromis, propre à une offre de service multi-établissement. Nous avons été aidés en cela par le constat que les besoins des établissements consultés étaient finalement relativement proches, car ceux-ci appartiennent tous à une même communauté.

En effet, les logiciels de messagerie collaborative sont en général conçus pour être utilisés par un établissement, sous une administration unique en son sein. Par ailleurs, ces logiciels sont très ergonomiques pour un usage interne, mais ils offrent des passerelles limitées avec le monde extérieur. Nous avons constaté que s'il était possible de créer une offre SaaS à partir de l'un ou l'autre de ces logiciels, ils ne permettaient pas nécessairement d'atteindre la dimension communautaire attendue de notre projet, les contraintes simultanées de visibilité et d'isolation demandées par les établissements et le niveau de délégation d'administration souhaité.

Il a donc fallu trouver un compromis acceptable entre des demandes divergentes :

- les établissements sont indépendants,
- mais ils appartiennent à une même communauté ;
- ils ont besoin d'une certaine isolation de leur service de messagerie,
- mais un utilisateur d'un établissement doit pouvoir collaborer avec celui d'un autre établissement pour que la plateforme atteigne toute sa dimension.

Par ailleurs, la plateforme PARTAGE doit aussi pouvoir permettre à ses utilisateurs de collaborer avec des utilisateurs d'autres plateformes similaires dans la communauté.

Il fallait en outre assurer la possibilité de d'intégrer des développements de passerelles logicielles avec l'écosystème des services utilisés par la communauté, tels que les autres outils collaboratifs proposés par le GIP RENATER ou des composants du système d'information des établissements largement répandus dans notre communauté (applications de gestion de salle, de scolarité, de gestion des congés, etc).

Nous devons donc choisir un logiciel qui assure les fonctions de messagerie collaborative de base, qui soit capable d'interagir avec des logiciels extérieurs et auquel on pourrait facilement ajouter des briques fonctionnelles pour intégrer ces services de l'écosystème.

In fine, notre choix s'est porté sur le logiciel Zimbra Collaboration Suite, afin de disposer de toutes les fonctionnalités de base de messagerie collaborative et de profiter d'une API riche et documentée permettant d'ajouter en périphérie des fonctions (service de redirection à vie, annuaires « pages blanches » de tout ou partie des utilisateurs de la plate-forme, fonction de messagerie instantanée). Cette API permet le développement de modules, s'exécutant directement dans l'interface utilisateur et de créer des interfaces avec d'autres applications. Par ailleurs, un grand nombre de développements de telles interfaces ont déjà été faits dans la communauté. L'acquisition des licences logicielles a été effectuée via l'UGAP.¹

1. L'UGAP est un établissement public industriel et commercial. Le recours à la centrale d'achat, elle-même soumise au Code des marchés publics pour toutes ses procédures, dispense ses clients de toute mise en concurrence et publicité préalables

2.2 Appel d'offre

Une fois le contexte logiciel choisi, nous avons dû lancer un appel d'offre pour l'hébergement, le déploiement et l'exploitation du service.

Nous avons fait le choix de séparer en lots distincts l'hébergement de la plateforme et l'exploitation du service de messagerie afin d'optimiser les coûts du marché. Les offres d'hébergement sont en effet en plein essor et nous souhaitons bénéficier de la meilleure concurrence possible sur ce lot. La séparation en deux lots est aussi pour nous un gage de réversibilité : il est possible de changer de titulaire pour un lot sans mettre en péril l'ensemble du service.

Un lot *Infrastructure as a Service* (IaaS) concerne donc purement l'hébergement : il s'agit pour le prestataire de fournir un *data center* virtuel, permettant la mise en place de l'infrastructure nécessaire au déploiement de la plate-forme applicative (des *unités d'œuvre* permettent de commander les composants réseau, les équipements de sécurité, les machines virtuelles, etc.). Le choix a été explicitement fait de fournir dans ce lot uniquement les composants de base, sans les configurations ou le système d'exploitation (OS : *Operating System*). La limite de responsabilité du titulaire du lot IaaS a été définie de la façon la plus précise possible et elle s'arrête à l'affichage des tests du « BIOS » de la machine virtuelle. L'OS (installation et configuration) est du ressort du lot messagerie.

L'autre lot « Messagerie » concerne donc toute la partie applicative : le déploiement de l'architecture logique de la plate-forme et son exploitation. Dans ce lot, il convient donc de spécifier l'architecture et la configuration des différents composants de la plate-forme et leurs interactions. Parmi ces composants, on retrouve des éléments d'infrastructure (découpage en sous-réseaux, firewall, load balancer, etc.) et les composants logiciels du service (Zimbra mais aussi les composants périphériques).

3 Description fonctionnelle

3.1 Particularités de cette offre de service

Le service PARTAGE est un « Software as a Service » dédié à la messagerie, comme il en existe d'autres sur le marché. Ce qui fait la particularité de ce service tient à ses co-locataires : il est dédié à la communauté enseignement/recherche. Dans les offres SaaS classiques, chaque client est complètement isolé des autres, c'est même un critère primordial de choix d'une solution pour les entreprises. Dans l'offre PARTAGE, si chacun est indépendant, chaque locataire fait néanmoins partie d'une même communauté. Les échanges et les collaborations sont possibles entre utilisateurs d'établissements différents.

La mutualisation de l'infrastructure permet des économies échelles, mais doit également faciliter l'interaction entre les membres de la communauté (les « locataires »). Il est donc indispensable que certains services puissent être partagés entre les utilisateurs de différents établissements. Ainsi, il paraît évident qu'un utilisateur de l'établissement A puisse partager son agenda, s'il le souhaite, avec un utilisateur de l'établissement B en profitant de toutes les possibilités de gestion de droits et de délégation offertes par le service à ses usagers. De même, un service de messagerie instantanée doit permettre à un utilisateur le dialogue au-delà de son établissement. Enfin, on doit proposer certains services « globaux », comme un annuaire de toute ou partie des utilisateurs de la plate-forme.

Si certains services sont nativement intégrés à la plate-forme, d'autres doivent pouvoir faire l'objet d'extensions particulières, notamment pour l'interaction avec des applications externes à la plate-forme (système d'information de l'établissement, autres outils collaboratifs, etc.). Chaque établissement doit pouvoir choisir dans un catalogue les extensions qu'il souhaite offrir à ses usagers. Une extension peut avoir du sens pour un établissement et pas pour un autre, par exemple une extension qui permet d'interfacer l'agenda avec un logiciel de gestion de salles qui n'est déployé que dans certains établissements.

3.2 Fonctions pour l'utilisateur

Nous décrivons, ci-après, les grandes fonctionnalités pour l'utilisateur. Il ne s'agit pas ici de faire une description exhaustive, celle-ci étant proposée dans la documentation du projet. On peut cependant indiquer que le service offre deux catégories de compte :

- une première catégorie regroupant les personnels : enseignants, chercheurs, thésards, ingénieurs, techniciens et

administratifs ;

- une deuxième catégorie regroupant les étudiants.

3.2.1 Messagerie

La plate-forme PARTAGE offre toutes les fonctions classiques de courrier électronique : envoi et réception de courriers, gestion de plusieurs boîtes aux lettres, répondeur automatique, filtres personnels sur les courriers.

Le filtrage antisпам du service est assuré en amont par le service Antispam Mutualisé de RENATER (cf. § 5)

Chaque compte peut disposer, en plus de son identité principale (adresse mail par défaut), d'identités supplémentaires, y compris dans un autre domaine que le domaine principal (par exemple, le compte principal prenom.nom@example.org peut également avoir les identités nom@example.org ou encore nom@example.net). Tous les mails vers ces différentes adresses convergent alors vers le même compte de messagerie.

3.2.2 Contacts

Chaque compte permet de gérer un carnet d'adresses personnel. De plus, chaque utilisateur a accès à l'annuaire de son établissement ainsi qu'à un annuaire global de plate-forme, voire à d'autres annuaires (annuaire d'un autre établissement ou annuaires externes).

La configuration permet de limiter les carnets d'adresses utilisés par défaut pour les mécanismes d'auto-complétion, lors de la saisie, pour éviter de rechercher un contact pour l'auto-complétion dans un annuaire trop large engendrant des temps de réponses inacceptables.

3.2.3 Agenda

Chaque utilisateur a la possibilité de gérer plusieurs agendas (personnels, de ressources, etc.). La plate-forme intègre la gestion d'invitation à un rendez-vous, ainsi que la recherche de disponibilités communes à une liste de participants à une réunion en cours de création. La solution permet de gérer des délégations afin de permettre, par exemple, à un(e) assistant(e) de gérer l'agenda d'un directeur ou à un technicien de gérer l'agenda d'une ressource.

Bien évidemment, la gestion des fuseaux horaires est parfaitement prise en compte.

3.2.4 Tâches

Le service permet la gestion de tâches simples (date limite, gestion de pièces jointes, attribution à un tiers).

3.2.5 Fichiers

De même, le service permet une gestion simple de fichiers (dépôts, indexation, etc.). Chaque utilisateur peut disposer d'un « porte-document » dans lequel il peut déposer des fichiers de petite taille. Une gestion de droits basique lui permet de donner des droits en lecture/écriture sur le porte-document à d'autres utilisateurs du service ou des droits en lecture seulement avec ou sans authentification à des utilisateurs externes au service.

3.2.6 Partages entre utilisateurs

Comme indiqué précédemment, tous les objets manipulés (fichiers, agendas, dossiers de messagerie, tâches, contacts) peuvent être partagés avec les autres utilisateurs du service, voire pour certains d'entre-eux avec des utilisateurs externes (fichiers, agendas, contacts).

Ces partages sont gérés via une gestion des droits d'accès aux dossiers (mails, agendas, tâches, etc.). Il est ainsi possible de gérer finement des droits sur ses propres dossiers (lecture, ajout, modification, suppression).

On peut, par exemple, déléguer la gestion d'un agenda à un collaborateur, n'autoriser qu'un accès en lecture à un dossier de courriers, etc.

3.2.7 Interfaces pour les utilisateurs

L'accès aux fonctions offertes par le service est possible à la fois via une interface web évoluée ou via des clients lourds.

L'interface Web dispose de différents niveaux de sophistication de l'interface minimaliste utilisable sur un terminal mobile (aux capacités – débit réseau, taille d'écran – limitées), jusqu'à une interface complète (AJAX) permettant les glisser/déposer, etc.

Les protocoles normalisés sont aussi directement accessibles par les clients lourds (POP, IMAP, CalDAV, WebDAV,

LDAP, etc.).

Enfin, la plate-forme permet aussi l'utilisation du protocole Activesync pour les périphériques mobiles et MAPI pour certains clients lourds. À noter que la synchronisation des périphériques mobiles avec Activesync est proposée pour toutes les catégories de comptes (personnels mais aussi étudiants). La synchronisation MAPI n'est proposée que pour les personnels.

3.3 Fonctions complémentaires globales

Outre les fonctions de base d'une messagerie collaborative au sein d'un établissement, le service met en œuvre, dès l'origine, quelques fonctions additionnelles globales. Il propose un annuaire de type « pages blanches » qui recense l'ensemble des coordonnées des utilisateurs du service. La publication des informations concernant un utilisateur dans cet annuaire est cependant laissée à la discrétion de l'administrateur du domaine de messagerie de l'établissement.

Le service permet aussi l'usage d'une messagerie instantanée accessible entre les utilisateurs, quel que soit leur établissement (via un client lourd ou l'interface Web). Ce service a disparu de la liste des fonctionnalités intégrées à Zimbra Collaboration Suite, mais il a été jugé indispensable par les établissements pilotes. Un développement spécifique de type Zimlet est donc intégré dans l'offre de service. D'autres fonctions seront progressivement intégrées (cf. § 6.2).

3.4 Fonctions pour l'administrateur

Les administrateurs d'un établissement ont à leur disposition une interface spécifique pour gérer le service fourni à leurs utilisateurs. Il s'agit de gérer l'ensemble des paramètres des domaines et des comptes associés de leur établissement, ainsi que d'opérer ou de faire opérer des fonctions de support aux utilisateurs. Cette interface est accessible au travers d'une application dédiée : le système de support fonctionnel ou BSS². En parallèle, les administrateurs ont également accès à des informations de supervision et de statistiques, au travers du système de support opérationnel ou OSS³.

3.4.1 Système de support fonctionnel (BSS)

Le BSS intègre un ensemble de primitives d'actions sur la plate-forme, afin de permettre les opérations d'administration des domaines de l'établissement.

Tout d'abord, le BSS permet les actions de paramétrage et de peuplement de la plate-forme.

- Paramétrage des domaines : un administrateur peut définir les paramètres généraux de chaque domaine qu'il gère (ceci intègre également des options de personnalisation de l'interface web accessible par les utilisateurs telles que le logo de l'établissement, la charte de couleurs, etc.).
- Gestion des catégories d'utilisateurs : ce système permet de choisir des options par catégorie d'utilisateurs tels que les quotas par utilisateur ou les droits d'accès aux fonctions de base⁴.
- Gestion des comptes utilisateurs : outre la création ou la suppression, le système permet également de paramétrer un compte d'utilisateur, notamment les informations de base (nom, prénom, etc.), les identités alternatives (alias du compte), la publication ou non dans les différents annuaires de plate-forme, etc. Il est également possible de surcharger le quota d'un compte (par rapport à la définition du quota de la catégorie de l'utilisateur).
- Gestion des autres comptes : configuration des comptes de ressources (salle, équipement, etc.) auxquels sont associés un ou plusieurs contacts (utilisateurs en charge de la gestion de la ressource).
- Gestion de groupes : Le système permet également aux administrateurs la gestion de groupes de personnes. Ces groupes peuvent notamment être utilisés pour automatiser des partages (par exemple, un ensemble de collaborateurs ayant accès à un agenda particulier).

Le BSS fournit une interface « self-service » qui permet notamment aux administrateurs des établissements d'effectuer

2. Business Support System

3. Operation Support System

4. Possibilité de restreindre une catégorie d'utilisateurs à un sous ensemble des fonctions bases. Par exemple, interdire l'utilisation de la fonction de gestion de fichiers pour privilégier un système interne à l'établissement, interdire les partages externes, etc

les tâches de gestion et de support auprès de leurs utilisateurs sans passer par le service de support du service s'ils le souhaitent. Pour un administrateur de domaine, il est ainsi possible d'accéder à l'environnement d'un utilisateur du domaine afin de l'assister. Enfin, le BSS est également le point d'accès au centre d'opération du service (support et maintien en condition opérationnelle opéré par le prestataire), via un système de gestion de ticket.

3.4.2 Système de support opérationnel (OSS)

Le système de support opérationnel propose aux administrateurs toutes les informations utiles au suivi du fonctionnement du service. Il propose les informations de santé de la plate-forme (disponibilité et charge des composants, annonce de maintenance, incidents en cours, etc.). Il fournit de plus des statistiques d'utilisation aux administrateurs d'établissement (nombre de domaines, nombre de comptes et typologie, utilisation de l'espace de stockage globalement alloué et par utilisateur, etc.)

Il permet en outre de disposer d'alertes sur des taux d'utilisation (par exemple, lorsqu'un utilisateur atteint son quota).

3.4.3 Méthodes d'accès aux systèmes de support

L'accès aux systèmes de support (OSS et BSS) est disponible sous deux formes : via une interface web (authentification nominative de l'administrateur via la fédération d'identité) ou via une API REST pour permettre l'automatisation de tâches et l'intégration dans le système d'information de l'établissement (l'authentification utilise alors un mécanisme de clé et de tickets à durée de vie). De surcroît, l'essentiel des fonctions de gestions du BSS est également disponible pour des traitements par lots, via le dépôt de fichiers de synchronisation. Cela rend possible, par exemple, une alimentation massive de compte utilisateurs, sans répéter des appels à l'API. Les opérations sont alors menées de manière asynchrone.

4 Architecture

4.1 Séparation Infrastructure/Services

Dans la conception de l'appel d'offres, il a été décidé de séparer en deux lots distincts la fourniture d'une infrastructure d'hébergement, l'intégration et l'exploitation des différents éléments applicatifs de PARTAGE. À première vue, ce choix peut être considéré comme une complexité supplémentaire. Les inconvénients sont listés ci-dessous.

- Un soumissionnaire d'un lot unique, dans le cadre d'un tel appel d'offre, va chercher à optimiser globalement la solution, à la fois d'un point de vue technique, financier, et également du point de vue des risques. La séparation en deux lots empêche une optimisation globale.
- La rédaction du DCE nécessite de décrire, *a priori*, les interfaces nécessaires entre les deux lots, afin de clarifier le plus précisément possible les tâches et les rôles de chacun. Un RACI⁵ a d'ailleurs été défini entre les différents partenaires.
- Le pilotage global par trois acteurs différents de la prestation rendue aux utilisateurs (titulaire lot 1, titulaire lot 2, maîtrise d'ouvrage) est nécessairement plus compliqué : il faut notamment éviter un jeu de ping-pong entre les deux prestataires.

La décomposition en deux lots permet de distinguer les différentes briques technologiques et de tirer le meilleur parti du marché pour chacune d'elles. Comme cela a déjà été dit, les fournisseurs potentiels du lot 1 sont bien plus nombreux que les fournisseurs du lot 2. La concurrence étant plus importante sur ce lot, les tarifs obtenus sont globalement meilleurs.

Cela permet aussi de mieux appréhender la structure des coûts du service offert à l'utilisateur final et de disposer d'axes d'amélioration. C'est aussi la traduction dans le marché de métiers différents. Dans la plupart des institutions, les personnels en charge de l'hébergement sont dans des équipes différentes des personnels en charge de la gestion des services applicatifs. Des contrats de services internes sont passés entre ces équipes (OLA⁶) potentiellement très loin des besoins réels pour fournir les SLA⁷ prévus pour le service. La séparation en deux lots nous permet de transformer ces OLA en des SLA et donc de contrôler que le niveau de service mis en œuvre au niveau de l'hébergement est bien celui

5. Responsible, Accountable, Consulted, Informed. Pour chaque UO du marché qui est responsable, consulté, informé et qui est l'autorité

6. Operational Level Agreement

7. Service Level Agreement

qui est nécessaire.

Nous voyons le deuxième point comme un avantage plutôt qu'un inconvénient en terme de pilotage du marché : dans une perspective de moyen/long terme, s'il fallait ré-internaliser l'un ou l'autre lot, la définition précise des activités à mettre en œuvre est déjà décrite. De plus, il est bien plus facile de prévoir le renouvellement ou le transfert d'un lot que de l'ensemble de la prestation.

Enfin, sur le dernier point, ce mode de pilotage est mis en œuvre au GIP pour ce qui concerne le réseau lui-même.

La diversité des acteurs sur le marché de l'hébergement, ainsi que la diversité des solutions techniques d'hébergement ou de fourniture d'infrastructure virtuelle ont conduit à définir un lot pour cette partie de la prestation globale. Une contrainte forte, qui s'avère « payante » au vu de l'actualité récente, portait sur la sécurité de l'hébergement des données, dans le respect du droit français, pour garantir, notamment, la confidentialité. Faire de cette prestation un lot spécifique facilite grandement le contrôle de cette exigence, que ce soit pour le dépouillement des offres ou au cours de la vie du marché. L'autre contrainte posée par le CCTP consistait à demander une infrastructure « élastique », pouvant être allouée à la hausse comme à la baisse, que ce soit en terme de CPU, de RAM ou de stockage, afin de n'utiliser à un moment donné que les ressources strictement nécessaires au bon fonctionnement du service. Cette capacité à augmenter ou diminuer les ressources fournies doit pouvoir être réalisée sans délai. Cela implique donc *a minima* la fourniture d'une interface Web de configuration et d'allocation/destruction de celles-ci.

In fine, le résultat de l'appel d'offre a désigné Cloudwatt, pour le lot IaaS. Cloudwatt est l'un des deux fournisseurs de « cloud souverain » en France. L'offre conjointe SCC/Netixia a été retenue dans le cadre du lot 2, déploiement et maintien en condition opérationnelle de la solution Zimbra. L'offre IaaS de Cloudwatt est construite à partir de la solution Open Source Open Stack [2].

4.2 Infrastructure réseau

Il n'était pas envisageable de ne pas pouvoir maîtriser d'une manière ou d'une autre la connectivité réseau à RENATER du fournisseur IaaS. L'actualité récente d'internautes français n'obtenant pas une qualité de service suffisante pour utiliser confortablement telle ou telle plate-forme de contenu rappelle que ce sujet n'est pas anodin. Plutôt que spécifier un objectif en terme de débit, de latence ou de gigue entre RENATER et le réseau du titulaire du lot 1, objectif qui aurait nécessité des outils de surveillance de ces indicateurs, un raccordement direct du titulaire sur un Noeud RENATER a été imposé (au même titre qu'un utilisateur/réseau de collecte). Et bien évidemment, pour assurer une redondance d'accès, le titulaire se doit de mettre en œuvre un deuxième lien de son infrastructure d'hébergement vers un autre NR. Ainsi, la plate-forme est vue comme un site utilisateur raccordé à RENATER.

Le titulaire du lot 2 doit spécifier les différentes zones internes à la plate-forme, non accessibles directement depuis l'extérieur.

D'autres composants réseaux ont été intégrés dans l'appel d'offre comme des Unités d'Œuvre fournies par le titulaire du lot 1.

- Service DNS pour enregistrer les machines internes et celles accessibles depuis l'extérieur sans avoir à déployer les logiciels sur des machines spécifiques.
- Firewall pour définir la politique de sécurité et contrôler la matrice des flux entre les différentes zones (VLANs) de la plate-fome.
- Accélérateur SSL afin de libérer les serveurs proxy applicatifs de la charge induite par le chiffrement des flux.
- Répartiteur de charge des flux TCP des utilisateurs sur les serveurs proxy.

Ces composants sont à la disposition du titulaire du lot 2 qui devra réaliser la configuration et le paramétrage de ceux-ci.

4.3 Stockage

Il a été demandé au titulaire de l'infrastructure d'hébergement de fournir trois types de volumes de stockage pouvant être alloué pour construire le service :

- un stockage rapide, ayant de très bonnes performances en terme de débit d'I/O, destiné à recevoir l'OS des machines, les logs générés par Zimbra, ainsi que les messages entrants et les courriels les plus accédés par les

utilisateurs ; la taille de ce type de volume est limitée (quelques centaines de Go tout au plus) ;

- un stockage plus lent, ayant des performances de débit d'I/O moindres, destiné à recevoir les courriels archivés par l'utilisateur, ou ceux n'étant pas souvent accédés ; la taille de ce type de volume peut atteindre à minima le To, les bonnes pratiques Zimbra suggèrent de se limiter à 2 To par volume⁸ ;
- un stockage destiné à la sauvegarde (sauvegarde système ou sauvegarde Zimbra), hébergé dans un autre lieu géographique.

Tous ces volumes peuvent être alloués dynamiquement à la demande.

4.4 Maintien en condition opérationnelle

Chaque titulaire est responsable du maintien en condition opérationnelle de la partie de la plate-forme qu'il fournit. Bien évidemment, le titulaire du lot 2 est dépendant de la bonne « santé » de l'infrastructure qu'il opère pour exploiter les différents composants (OS et logiciels) qu'il a intégré. Au delà des engagements de disponibilité auxquels chaque titulaire est tenu, il est important d'avoir une vision plus fine des interactions des différents composants de la plate-forme, au travers d'indicateurs divers.

Par exemple, les taux d'utilisation CPU vu par la plate-forme d'hébergement sont intéressants à observer, afin de vérifier si les machines virtuelles ne sont pas globalement sous-utilisées. De même, des indicateurs d'I/O au niveau des serveurs dédiés au stockage des boîtes aux lettres permettent de s'assurer que les performances des volumes disques fournis par la plate-forme d'hébergement sont au niveau attendu.

5 Sécurité du service

Le service PARTAGE doit bien évidemment être disponible 24h sur 24 et 7 jours sur 7.

Pour cela, à la fois l'infrastructure sous-jacente et le service de messagerie collaborative font l'objet d'une supervision et d'un maintien en condition opérationnelle en 24/7, effectué par deux centres opérationnels distincts (chacun des titulaire du lot) mais qui peuvent interagir.

La délégation de l'authentification vers un annuaire d'établissement a été proscrite. Pour l'accès aux interfaces utilisateurs web, c'est la fédération d'identité RENATER, qui est privilégiée. Pour l'accès via les clients lourds (ou en cas d'indisponibilité de l'authentification via la fédération d'identité), les données d'authentification sont stockées dans un annuaire interne de la plate-forme, mais elles peuvent être synchronisées à partir de données extraites des annuaires d'établissement, via les APIs. Ainsi, aucune composante du service hébergé ne dépend directement de la disponibilité d'une infrastructure fournie par l'établissement.

Le filtrage antispam des mails entrants est assuré par le service antispam mutualisé de RENATER. Il existe également des mécanismes de filtrage du flux sortant, notamment pour se prémunir des conséquences d'une utilisation anormale d'un compte utilisateur (suite à un phishing ou simplement un mauvais usage, etc.).

Afin de se prémunir de compromissions, l'architecture générale du service fait également l'objet d'une attention particulière, avec notamment la mise en place de principes de sécurité tels que des architectures 3 tiers pour les services et l'utilisation de composants de filtrage aux frontières (cf. § 4).

Ainsi, tous les accès aux centres vitaux de la plate-forme ne sont possibles que via des passerelles sécurisées. Par exemple, l'accès à certains éléments n'est possible qu'à travers des passerelles de rebond, avec authentification forte (c'est le cas de l'accès aux fonctions d'administrateur général de la plate-forme qui n'est possible qu'après authentification sur un serveur SSH intermédiaire avec authentification nominative par bi-clé et tunneling de port).

La confidentialité des données est notamment assurée par les exigences de l'hébergement : en France et de droit français.

6 Perspectives

8. Notamment à cause des délais de reconstruction

6.1 Optimisation du stockage

Les boîtes aux lettres sont actuellement stockées en utilisant des volumes SAN : Zimbra gère ses éléments en utilisant les appels système POSIX classiques de gestion de fichiers. Cela induit une limite pratique à 2 To par volume, ce qui génère des effets de seuils sur le nombre d'utilisateurs qu'un serveur de stockage peut prendre en charge en moyenne. Par conséquent, pour équilibrer la charge entre serveurs de stockage, le titulaire du lot 2 peut être amené à déplacer fréquemment des boîtes aux lettres d'un serveur à un autre (cette opération se fait sans impact notable pour l'utilisateur).

Un moyen d'éviter ce genre de manipulation consiste à utiliser du stockage objet (système de stockage objet distribué de type CEPH⁹, par exemple). Dans cette configuration, Zimbra utilise directement l'API fournie par le système de stockage pour déposer ou lire ses objets, ce dernier assurant la concurrence d'accès et le passage à l'échelle de la quantité de données à stocker. Avec un tel stockage, les limites de volumétrie et les performances en I/O de chaque serveur augmente, ce qui signifie qu'on peut mettre beaucoup plus d'utilisateurs par serveur en conservant les performances. De plus le stockage distribué augmente nativement la résilience du stockage. Enfin, le recul des limites de volumétrie induit moins de travail de manipulation des boîtes pour le titulaire du lot 2.

6.2 Interfaces avec d'autres logiciels et extensions

Le service est doté d'API à tous les niveaux d'interaction.

L'API du BSS, pour les fonctions d'administration, permet l'intégration avec le système d'information de l'établissement. Chaque établissement peut ainsi intégrer, dans son propre workflow de gestion des utilisateurs, les appels nécessaires pour peupler, en parallèle à ses propres bases de données, les domaines qu'il gère sur le service PARTAGE. On peut ainsi envisager le développement mutualisé de connecteurs entre un logiciel de la communauté et PARTAGE pour être mis à disposition des établissements (par exemple, un connecteur permettant d'automatiser la création/destruction de comptes par synchronisation à partir d'un logiciel de gestion du personnel).

Il en va de même pour les fonctions destinées aux utilisateurs. Les API de Zimbra (Web services et protocoles normalisés¹⁰) permettent d'envisager des interactions avec l'environnement de l'établissement (publication d'emploi du temps vers les étudiants, interaction avec un E.N.T.¹¹, etc.) Un établissement pilote a ainsi le projet de définir des agendas correspondant aux filières de ses étudiants, synchronisés avec le système de gestion des emplois du temps interne. Le partage vers les étudiants concernés permet de leur proposer un emploi du temps à jour (y compris des changements de salle) auxquels ils pourront accéder directement depuis leur smartphone.

Enfin, il est possible d'intégrer directement dans Zimbra Collaboration Suite de nouvelles fonctionnalités, grâce au mécanisme des Zimlets. Il s'agit d'extensions logicielles, qui permettent d'ajouter des fonctions directement utilisables depuis l'interface web de l'utilisateur et capables d'interagir avec des logiciels externes. Le choix des Zimlets proposées à chaque catégorie d'utilisateurs au sein d'un établissement est configurable via le BSS.

Il existe de nombreuses Zimlets (par exemple, la fonction « click to call », paramétrable avec un IPBX, pour composer automatiquement un numéro de téléphone présent dans un courrier ou le carnet d'adresse). Certaines Zimlets ont déjà été développées dans la communauté. Le GIP RENATER prévoit le développement de certaines Zimlets pour l'interaction avec les outils proposés à la communauté (serveur de listes de diffusion, services de visioconférence, etc.). Nous avons aussi créé un projet dans la forge de RENATER pour recenser, mutualiser et rendre visibles les développements de Zimlets dans notre communauté.

7 Conclusion

Ce service, mis en place à la demande d'établissements représentatifs de la communauté et ayant participé à la rédaction des spécifications, est désormais opérationnel. Il peut accueillir un très grand nombre d'utilisateurs, qu'ils soient enseignants, chercheurs, administratifs ou étudiants (de l'ordre du million), pour leur permettre d'échanger bien plus facilement leurs données au delà de leur établissement de rattachement de manière sécurisée et maîtrisée :

9. CEPH est un nouveau module de stockage en mode block d'OpenStack qui propose aussi une interface REST de stockage objet. Une interface compatible avec le protocole S3 d'Amazon est disponible. <http://ceph.com/docs/master/radosgw/>

10. IMAP, CalDAV, etc.

11. Espace Numérique de Travail

- hébergement en France avec un contrat de droit français, dans un datacenter Tiers III+,
- architecture redondée,
- service disponible 24x7,
- contrôle fin par les établissements des données partagées par leurs utilisateurs,
- conformité au RGS,
- réversibilité du service pour les établissements.

L'interopérabilité avec d'autres outils utilisés dans la communauté est prévue, et l'ouverture de la solution aux autres briques du système d'information des établissements apporte une réelle plus-value.

Liens de référence

[1] <http://www.renater.fr/partage>

[2] <http://www.openstack.org>