Service de messagerie électronique en université : si vis pacem, para bellum

Daniel Le Bray, Quentin Desre

Service de messagerie électronique en université : si vis pacem, para bellum

Daniel Le Bray
Université Le Havre Normandie
25 rue Philippe Lebon
76600 Le Havre

Quentin Desré
Université Le Havre Normandie
25 rue Philippe Lebon
76600 Le Havre

Résumé

Malgré l'émergence et la place grandissante de nouveaux outils de communication, la messagerie électronique reste de nos jours un medium hautement utilisé par les communautés universitaires et scientifiques. Pour faire face aux risques et répondre aux besoins et aux exigences de disponibilité, de fiabilité et de résilience, il nous a semblé nécessaire de repenser notre architecture de service et de l'inscrire dans une démarche pérenne et évolutive.

Si la réflexion que nous avons menée repose sur des stratégies (planification, anticipation) et des tactiques (quelles actions entreprendre ? Comment réagir ?), ce n'est pas dans les écrits de Sun Tzu que nous nous sommes plongés, mais sur les bonnes pratiques et l'expérience acquise au fil du temps. La sécurité d'un serveur ou la disponibilité d'un composant ne sont pas des points isolés ; c'est par une approche globale que nous avons repensé l'ensemble de notre service de messagerie afin qu'il cible au mieux les attentes en termes d'usage, d'exploitation et d'évolution.

Nous avons donc étudié, testé et retenu plusieurs solutions techniques pour adresser les multiples formes que recouvre ce service. Cette démarche nous permet aujourd'hui de répondre aux divers aspects de la politique d'usage (CAA, SPF, DKIM, DMARC), de la politique d'accès (SASL, Postgrey, Postfwd), de la séparation des flux (différents périmètres d'accès, les échanges SMTP, les manipulations des boîtes aux lettres), du filtrage d'hôtes (IPTables, Fail2Ban), de la protection des échanges (Rspamd, SpamAssassin, ClamAV), de la disponibilité (serveurs physiques et virtuels, KeepAlived), de la supervision et du maintien opérationnel des processus (statistiques, journaux, Monit).

Mots-clefs

E-mail, Architecture, Résilience, Sécurité, Postfix, Dovecot Director, PostFWD, RSpamd, Fail2Ban

1 État des lieux et survol des risques

Comme dans beaucoup d'établissements, le service de messagerie électronique à longtemps été mis en œuvre avec quelques serveurs physiques et juste ce qu'il faut de ressources pour un traitement acceptable. Notre service ne dérogeait pas à la règle et s'articulait basiquement autour de quatre serveurs physiques : deux pour le traitement des requêtes SMTP, fonctionnant en mode actif/passif avec bascule manuelle, deux pour les requêtes POP3/IMAP, l'un pour la population étudiante et l'autre pour les personnels. Une interface de type *webmail* était également disponible sur le serveur web de l'établissement pour les personnels et une autre pour les étudiants sur leur serveur dédié. Chaque serveur disposait de son propre stockage local pour ses tâches.

Bien qu'étant une petite université comptabilisant environ 10 000 usagers, le temps et les ressources nécessaires au fonctionnement du service ne cessaient de croître. Ceci du fait de l'augmentation progressive mais continuelle de l'usage de la messagerie ainsi que de l'ajout de fonctionnalités devenant de plus en plus nécessaires ; typiquement, un filtrage par antivirus et antispam des messages entrant et l'augmentation des espaces de stockage.

L'avantage principal d'une telle architecture est son apparente simplicité. Apparente car, en y regardant de plus près, cette simplicité induit par ailleurs un grand manque de souplesse dans son fonctionnement et son cycle de vie. Les inconvénients et les risques sont par contre relativement nombreux. Parmi eux, l'indisponibilité de tout ou partie du service causé par un souci réseau, matériel ou logiciel. L'efficacité et l'évolutivité de cette approche sont extrêmement réduites ; seul un changement de matériel permet de monter en puissance mais au coût d'interruptions de service et d'une plus grande lourdeur des opérations de maintenance. Finalement, ce qui semblait être simple s'avère être relativement complexe et le résultat assez peu satisfaisant.

La réflexion pour repenser ce service s'est donc imposée d'elle-même, avec pour objectif d'apporter une réponse convenable en termes de mise en œuvre, de maintenabilité, d'évolution, de performance et de disponibilité.

2 Les besoins et les exigences

Notre étude s'est appuyée sur les moyens techniques dont nous disposions ou auxquels nous pouvions prétendre et sur les besoins en termes d'usage. L'objectif principal a été de chercher à adresser au mieux les exigences attendues d'un service performant, facilement maintenable et adapté à un usage continu.

Parmi les points primordiaux se trouve la haute disponibilité. Le service doit être opérationnel à tout moment et ne pas être impacté négativement par une opération de maintenance ou un événement quelconque lié aux divers systèmes et logiciels. Cet aspect est fortement couplé à la notion de résilience : l'absence ou la panne d'un composant ne doivent pas entraver le fonctionnement global du service. Il est nécessaire de prendre en compte tous les aspects liés à l'exploitation des systèmes en réseau pour tendre vers un service résilient. Les alimentations des matériels doivent être redondées et raccordées sur des circuits électriques différenciés dont au moins un est protégé par

onduleur. Les serveurs sont répartis dans au moins deux locaux techniques distincts. Il faut s'assurer que le trafic réseau puisse être maintenu malgré la défaillance d'un adaptateur ou d'un concentrateur.

La performance est bien évidemment un point crucial. L'architecture proposée doit être capable de supporter la charge de travail demandée et offrir son service avec des temps de réponse qui ne gênent pas l'usager. Et, l'usage d'un tel service n'étant pas linéaire, il est important de pouvoir faire évoluer au besoin un ensemble de ressources afin de s'assurer une possibilité de croître, de faire face à un changement d'ordre de grandeur ou d'absorber des pics de charge plus importants. Cette mise à l'échelle, ou scalabilité[1], est de nos jours fortement simplifiée avec les solutions de virtualisation.

Concernant le vaste domaine de la sécurité, nous nous efforçons d'inclure systématiquement des mécanismes adaptés à chaque étape et pour chaque ensemble fonctionnel. Notre réflexion s'attache donc à composer avec l'arsenal d'outils existants, qu'il s'agisse du stockage des données avec des sauvegardes, de l'intégrité d'une transaction avec du chiffrement ou la prise en compte des menaces courantes véhiculées par les messages électroniques, comme le *spam* ou les tentatives d'hameçonnage avec les logiciels dédiés ou des services tiers. Comme tout service numérique, la messagerie est régie par des règles d'usage et des politiques d'accès, plus ou moins explicites. Il est parfois délicat de distinguer un client légitime effectuant de mauvaises transactions d'un autre, illégitime mais s'appliquant à faire des actions correctes mais abusives. L'un des défis auquel nous avons eu à faire face et pour lequel nous avons entamé une réponse est la rédaction et la prise en compte de ces règles d'usage en nous appuyant sur le filtrage réseau avec fail2ban et la régulation des flux avec Postfwd.

Comme l'a bien résumé le directeur du pôle Ressources Système d'une grande université[2] : « Quel que soit le type de technologie, si elle n'est pas maîtrisée par les équipes techniques, on court droit à la catastrophe… ». La maîtrise technologique ne doit pas nous échapper ni, dans la mesure du possible, dépendre d'un vendeur tiers. Cet aspect peut paraître anecdotique ou peu opportun mais résonne auprès de toutes celles et ceux qui ont déjà été confrontés à l'arrêt subit d'une technologie ou d'un matériel. Au-delà de l'intérêt intrinsèque des logiciels libres ou *open source*, il nous apparaît important de privilégier les offres logicielles non propriétaires dans notre architecture, en particulier pour rester en cohérence avec l'ensemble de notre parc et ne pas affaiblir notre capacité de maintenance. Pour les matériels c'est beaucoup moins aisé de ne pas dépendre d'un fournisseur particulier et le choix est souvent guidé par des aspects financiers ou décisionnels qui peuvent nous échapper. Mais notre réflexion se doit d'incorporer ces éléments afin d'éviter des situations exotiques ou délicates.

Enfin les coûts, qu'ils soient financiers ou jour*homme, doivent être raisonnables et maîtrisés. L'apport des solutions de virtualisation est ici important, tant cette technologie facilite l'augmentation de son potentiel de ressources tout en gardant le contrôle de son enveloppe budgétaire.

1. Cet anglicisme n'est pas très beau mais il existe bel et bien dans le domaine de l'informatique

2. Merci Mathieu !

3 Les réponses apportées

Pour tenter de répondre au mieux à l'ensemble des objectifs fixés, nous avons donc défini et mis en place notre nouvelle architecture de service au fil du temps. La mouture actuelle est le fruit de multiples itérations et évolutions, certaines plus conséquentes que d'autres, mais toutes s'intégrant dans la démarche globale d'aboutir à un service pérenne et satisfaisant.

Nous avons commencé à virtualiser des serveurs au cours de l'année 2012. Cette étape cruciale a été un déclencheur pour la remise en cause de nombreux éléments de notre système d'information. C'est ainsi qu'en 2015, nous avons initié la réflexion sur le service de messagerie électronique. Nous avons commencé à véritablement restructurer les différents éléments de notre architecture en 2016, avec la séparation des rôles SMTP externes et internes, et réalisé notre dernière mouture à la fin de l'année 2018, avec la mise en place du service Dovecot Director.

3.1 Architecture matérielle

L'architecture matérielle du service de messagerie repose sur une paire de serveurs physiques et plusieurs serveurs virtuels. Ces serveurs sont hébergés dans deux salles distinctes réparties sur deux sites. Bien que nous ayons une totale confiance dans notre infrastructure de virtualisation, nous avons fait le choix de conserver des serveurs physiques plutôt que de tout virtualiser. Cette décision découle en partie du fait que les serveurs de virtualisation sont montés progressivement en puissance, moins rapidement que la demande de machines virtuelles. Nous devions nous assurer de pouvoir disposer de l'ensemble des ressources d'un serveur sans être impacté par d'autres serveurs virtuels. Plus concrètement, il nous a semblé opportun de privilégier la disponibilité des serveurs assurant le rôle d'échangeur de courriers, *mail exchanger* ou MX, ceux-ci assurant le point d'entrée pour le service de courrier électronique. Nous avons donc décidé, pour ces fonctions de MX, d'utiliser un couple de serveurs physiques et virtuels. Ceci évoluera sans doute dans le futur.

Chaque serveur physique possède deux ports Ethernet 10G agrégés et répartis sur deux concentrateurs. Il est ainsi immédiatement possible d'augmenter la bande passante et d'assurer une redondance de lien pour la disponibilité d'un serveur. Les serveurs virtuels bénéficient quant à eux de l'infrastructure de virtualisation qui s'appuie sur une dorsale à 40 Gbit/s. Sans chercher à réinventer la roue, nous avons décomposé les divers rôles du service de messagerie en suivant un schéma simple : SMTP interne/externe, relais, routage, stockage.

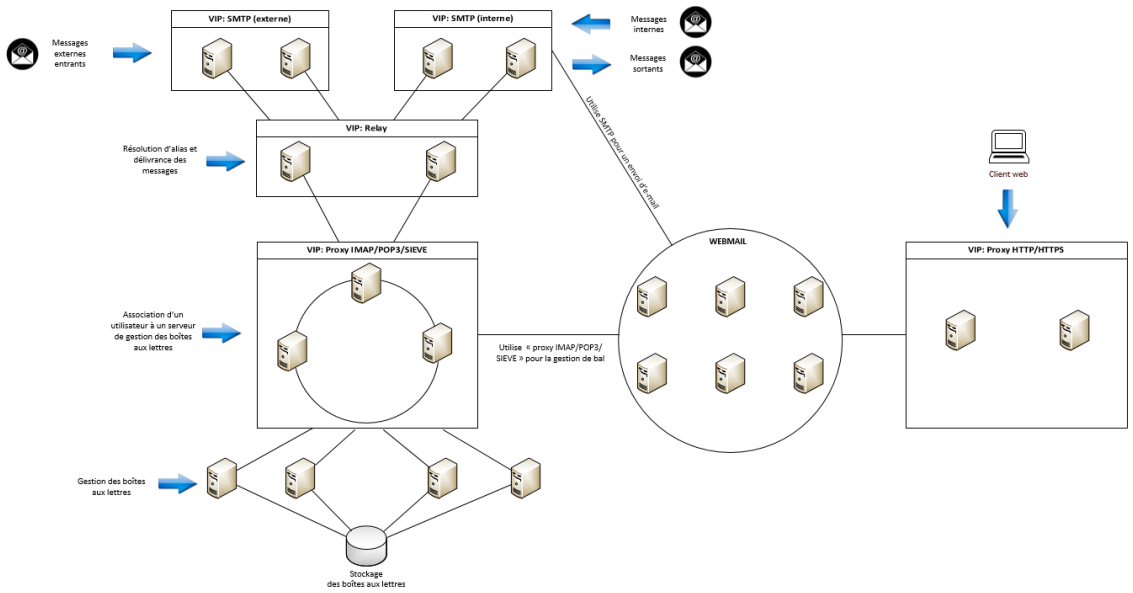

Figure 1 - Vue globale de l'architecture matérielle

En amont on va donc trouver une paire de serveurs qui assurent la prise en charge de tout le trafic d'échanges de messages provenant de l'extérieur du réseau d'établissement, que l'on nomme « SMTP externe », et une paire de serveurs pour tout le reste du trafic, nommés « SMTP interne ». Ce dernier a pour rôle de prendre à sa charge toutes les requêtes provenant du réseau interne ou de tout utilisateur dûment authentifié, quelle que soit sa provenance. Il assure également l'envoi des messages de tous les usagers du service vers les diverses destinations demandées.

Quand un courrier a été accepté par les échangeurs, il est ensuite envoyé vers les serveurs de relais. Cette fonction est mise en place par un couple de serveurs virtuels fonctionnant en répartition de charge avec une adresse IP virtuelle et prend en charge la gestion de l'ensemble des adresses de courrier, basiquement les alias, pour les acheminer vers le mandataire des boîtes aux lettres.

À la différence d'une simple répartition de charge avec une adresse IP virtuelle entre deux serveurs, le service de mandataire est fourni par un trio de serveurs virtuels fonctionnant en anneau. À titre d'illustration, le triplet de serveurs (A,B,C) va établir des connexions $A \rightarrow B$, $B \rightarrow C$ et $C \rightarrow A$. Ce mode de fonctionnement permet d'assurer une répartition de charge avec une forte tolérance aux pannes. Son rôle est essentiellement de s'assurer de la disponibilité d'un serveur de boîte aux lettres, d'y associer un utilisateur et de maintenir cette correspondance en place ou de la remplacer si le serveur initialement retenu n'est pas ou plus disponible. Quand un message doit être délivré, le mandataire récupère ou crée une correspondance. Le message est donc acheminé vers le serveur associé aux utilisateurs destinataires du message.

Les messages qui doivent être remis aux usagers sont délivrés par un ensemble de quatre serveurs virtuels. Ceux-ci sont indépendants les uns des autres et sont configurés au niveau du service de mandataire. Il est possible d'ajouter ou de retirer des serveurs

très simplement en paramétrant les serveurs qui doivent être utilisés auprès des mandataires.

Le stockage des données est effectué au travers d'un stockage commun reposant sur des volumes NFS exportés par un serveur de fichier faisant office de NAS. Cet équipement repose sur une grappe de deux serveurs dédiés fonctionnant en mode actif-actif.

Enfin, un accès de type *webmail* est également disponible aux usagers. C'est un groupe de six serveurs virtuels qui fournit ce rôle afin d'assurer une disponibilité et une performance en adéquation avec les usages attendus.

3.2 Architecture logicielle

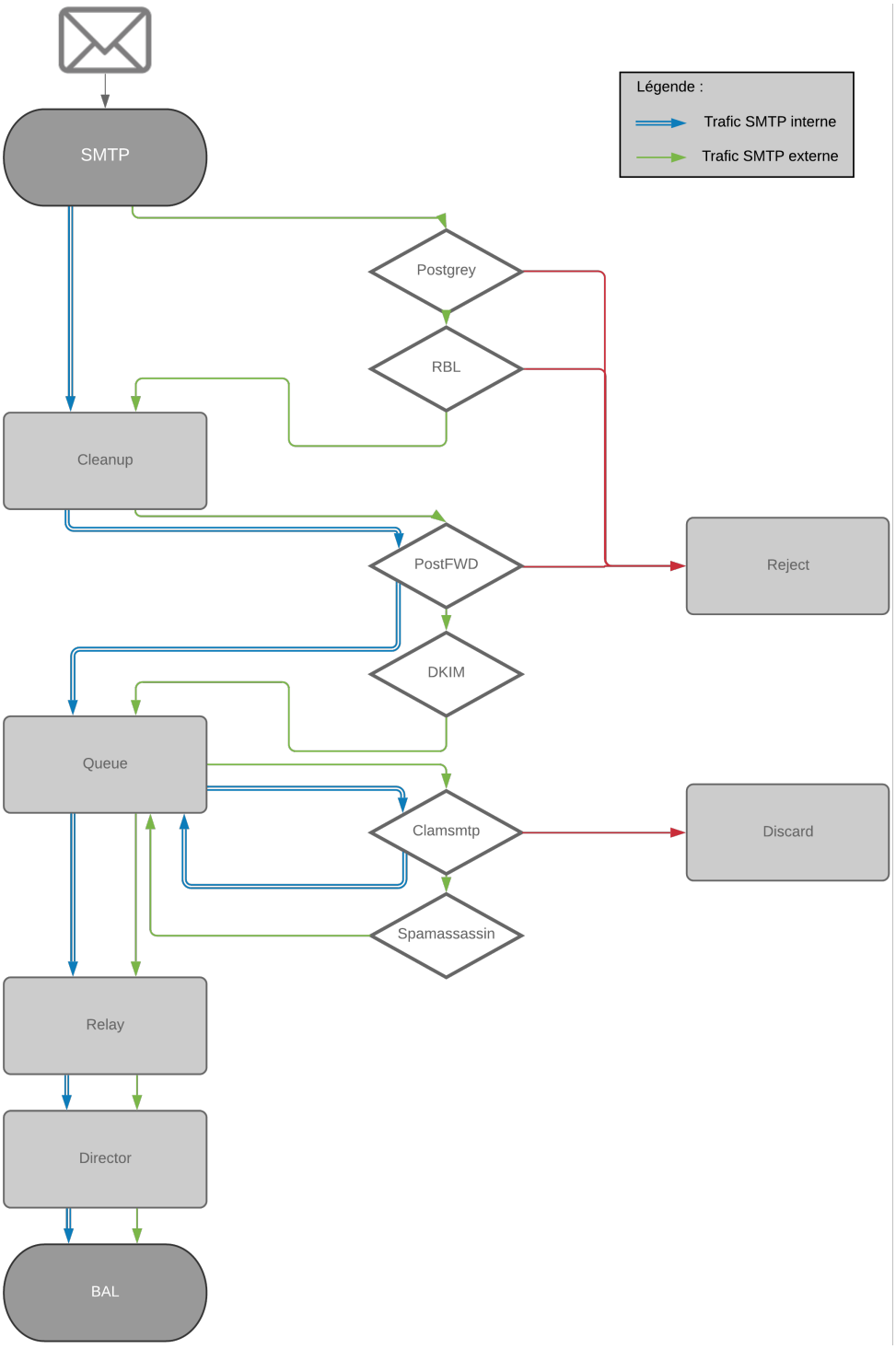

Figure 2 - Schéma des flux SMTP

Afin de mettre en place cette architecture de courrier électronique, nous nous sommes appuyés sur bon nombre d'outils logiciels et l'écriture de quelques scripts. À

l'exception de l'infrastructure de virtualisation, s'appuyant sur la solution VMware, et du système de stockage, tous les composants logiciels sont disponibles sous une licence libre ou *open source*.

Tous nos serveurs tournent sous la distribution Debian. Nous avons conscience qu'il n'est jamais optimal de mettre tous ses œufs dans le même panier, mais factuellement, on utilise uniquement ce système d'exploitation pour les différents serveurs fournissant ce service. Les systèmes Debian nous ont séduits depuis des années pour la qualité de leur offre et leur stabilité. Bien que cela reste une éventualité envisageable, il ne nous semble pas aujourd'hui particulièrement judicieux d'introduire un autre système d'exploitation au détriment de notre efficacité ou de la simplicité d'administration et de gestion que nous avons acquises.

En amont du service de messagerie électronique, nous trouvons bien évidemment un service DNS, élément d'infrastructure incontournable de tout service numérique classique. Nous utilisons le logiciel PowerDNS comme serveur autoritatif pour gérer notre zone et ses enregistrements. En dehors des entrées définissant les MX du domaine, nous reposons aussi sur les enregistrements CAA, *Certification Authority Authorization*, pour indiquer quelles sont les autorités de certifications valides pour nos certificats. Afin de concrétiser et faciliter l'application d'une politique d'accès, nous définissons également des enregistrements SPF, DKIM et DMARC. Bien qu'une politique laxiste soit actuellement déployée pour ces mécanismes, il est fort probable qu'ils soient utilisés de façon plus stricte dans le futur. La résolution des noms de domaine est elle aussi assurée par des serveurs PowerDNS ainsi que par le logiciel DNSmasq. Ce dernier permet de réduire considérablement le nombre de requêtes vers les résolveurs en conservant un cache en local sur les serveurs.

Au cœur du service de messagerie électronique, nous trouvons le fameux logiciel Postfix. Comme beaucoup, nous utilisions historiquement Sendmail pour assurer notre service SMTP, mais la simplicité offerte par Postfix, tant pour la configuration que la maintenance, son lot de fonctionnalités et de facilités nous ont conquis depuis plusieurs années. Le traitement des courriers réalisé sur les serveurs SMTP externes est assuré par un arsenal d'outils habituels dans un tel environnement ; on y retrouve l'antivirus ClamAV, la solution d'antispam SpamAssassin et les fonctionnalités aujourd'hui assez classiques telles que la vérification des signatures DKIM avec OpenDKIM, la gestion de liste grise, ou *greylisting*, mise en œuvre avec le logiciel Postgrey, les *Realtime Blackhole List*, ou listes noires en temps réel permettant d'interrompre une connexion dès la phase de transaction avec un serveur de courrier réputé comme indésirable.

Les serveurs SMTP internes sont sensiblement identiques, ils se distinguent par l'omission du *greylisting* et des RBL mais se voient ajouter l'authentification SASL auprès de l'annuaire d'établissement LDAP. De plus, les protocoles Submission/TLS et SMTPS sont disponibles pour des connexions chiffrées de bout en bout.

Un élément important de notre service pour l'application de règles d'usage est l'outil *Postfix firewall daemon*, ou PostFWD. Ce logiciel s'appuie sur la délégation de politique d'accès de Postfix pour appliquer un ensemble de règles comme on le ferait classiquement avec pare-feu pour le réseau. Cette solution, simple mais efficace, permet de définir rapidement des limitations basées sur divers critères, comme la taille d'un

message ou le nombre d'occurrences d'un expéditeur, pour décider si un message doit être ou non accepté par le service de messagerie. La mise en place de restrictions ou de règles d'usage se trouve grandement facilitée. Il nous est par exemple possible de limiter le nombre de messages par minute d'un compte étudiant d'une façon différente de celles d'un personnel administratif ou d'un enseignant.

Les serveurs de relais reposent eux aussi sur Postfix pour réceptionner les messages en SMTP et les transférer en LMTP vers le service mandataire. Le choix de LMTP nous a semblé évident en raison de la nature du trafic concerné, à savoir un flux à destination d'un *Mail Delivery Agent*, et à également été guidé par la volonté de pouvoir exploiter Sieve et potentiellement d'autres modules de Dovecot, comme les quotas. La gestion des alias s'appuie sur des scripts Perl que nous avons écrits pour gérer automatiquement les adresses issues de l'annuaire référentiel LDAP et les exceptions manuelles.

Les serveurs assurant le rôle de mandataire et de gestion des boîtes aux lettres se basent sur le logiciel Dovecot. Nous utilisions historiquement les logiciels UW IMAP et Qpopper pour fournir nos accès IMAP et POP3. Ces solutions étaient relativement satisfaisantes au quotidien, mais souffraient d'un manque de performances et de réactivité dans leur développement. Après avoir testé diverses alternatives, le logiciel Dovecot, orienté sécurité et performance, est rapidement devenu une évidence pour remplacer ces services. En particulier, sa prise en main rapide, sa grande facilité de gestion et son offre de fonctionnalités ont été décisives pour nous encourager à adopter ce logiciel. C'est donc aussi très logiquement que nous avons retenu le composant Dovecot Director pour assurer le rôle de mandataire. Ce dernier est extrêmement performant et possède un fonctionnement résilient adapté à notre architecture. Son mécanisme d'association « utilisateur ↔ serveur » partagé entre ses nœuds permet de s'affranchir des soucis de verrouillage avec des volumes NFS que nous pouvions rencontrer précédemment. Du côté des usagers, les protocoles IMAP, POP3 et Sieve sont mis à disposition pour offrir une gestion complète de leur messagerie avec des fonctionnalités de filtrage et de réponse automatique. Tout comme pour la partie SASL des serveurs SMTP, nous reposons sur l'annuaire LDAP de l'établissement pour l'authentification des sessions utilisateurs.

L'interface *webmail* était historiquement basée sur le logiciel RoundCube. Nous avons par la suite migré vers le collecticiel[3] SOGo afin d'offrir aux utilisateurs un accès à leur messagerie et à un agenda au travers du web. L'interface, depuis la version 3, est relativement bien adaptée aux usages nomades actuels et permet d'être exploitée sur tout type de périphérique. Celle-ci permet également d'éditer directement les règles de filtrage mises en œuvre par Sieve, comme une réponse automatique en cas d'absence, d'une façon assez conviviale. Ce logiciel dépend d'un service de bases de données que nous exploitons à l'aide d'une grappe Galera pour MariaDB et d'un service Memcached.

En dehors de ces logiciels propres à la mise en œuvre de la messagerie électronique, nous utilisons divers autres composants plus ou moins essentiels au bon fonctionnement ou à la maintenance de notre architecture de service. Parmi eux, le logiciel Keepalived est utilisé pour maintenir une adresse IP virtuelle partagée entre plusieurs serveurs.

3. Traduction française du terme *groupware*

Simple à mettre en œuvre et robuste à l'usage, cet outil nous permet de bénéficier immédiatement d'une répartition de charge tout en garantissant la disponibilité d'un service. Le logiciel Monit offre quant à lui la possibilité de surveiller des services ou des fichiers sur un serveur. Très pratique, cet outil peut se charger de stopper ou redémarrer un processus suivant un ensemble de conditions préalablement définies. Avec le logiciel fail2ban, nous bénéficions d'une gestion automatisée de règles du pare-feu IPtables, permettant de limiter ou pallier des tentatives d'intrusion ou de DDOS. Les journaux des différents logiciels sont déportés sur un volume NFS de notre serveur de fichier NAS. Le script Perl pflogsumm est utilisé pour obtenir un rapport sur l'activité journalière du service. Nous avons également écrit des scripts pour utiliser ces journaux avec le logiciel Mailgraph et générer des graphiques d'usage.

S'agissant des sauvegardes, celles-ci sont réalisées au niveau fichier et au niveau machines virtuelles. Les données, de type fichier, sont quotidiennement sauvegardées avec le logiciel Borg. Se basant sur une approche incrémentale, nous offrons une rétention de 7 jours. Dans la multitude d'outils possibles, ce dernier à retenu notre attention grâce à ses capacités de déduplication et ses performances. En complément de cette sauvegarde classique des fichiers, nous assurons également une sauvegarde quotidienne des machines virtuelles avec le logiciel Veeam. Cette solution est particulièrement efficace pour optimiser les durées de sauvegardes et nous permettre, au besoin, de restaurer un serveur virtuel en toute simplicité.

4 Bilan et perspectives

4.1 Où en est-on ? Est-on satisfait de nos actions ?

Globalement, nous sommes relativement satisfaits du travail que nous avons fourni pour améliorer ce service. Il est toujours difficile, voire délicat, de juger objectivement ses propres réalisations, mais l'effort collectif et l'investissement humain que nous avons prodigué ne s'avèrent pas vains. Nous avons pu dégager du temps pour mettre en œuvre notre projet qui, en retour, nous permet maintenant de dégager du temps pour s'affairer à d'autres projets. Du côté des usagers, les commentaires de satisfaction ont été peu nombreux, ce qui est plutôt la norme, mais surtout, en dehors de cas isolés regrettant l'ancien logiciel de *webmail*, aucune plainte ou remontée négative ne nous est parvenue, ce qui en soi est déjà une victoire !

L'architecture actuelle fonctionne sans interruption en production depuis janvier 2019.

Les gains de performance sont nettement perceptibles, les temps de traitements ont été réduits et les systèmes sont capables d'absorber de plus grosses quantités de demandes ou des pics de charge sans sourciller. Au niveau de la maintenance, l'essentiel de nos actions est concentré uniquement sur l'application des mises à jour quotidiennes ; en dehors de rares cas, nous n'avons plus à intervenir sur le fonctionnement des divers composants.

La gestion quotidienne et la tierce maintenance applicative sont simplifiées et rationalisées. L'utilisation d'un superviseur de processus comme Monit nous permet de

ne pas avoir à se préoccuper des petits soucis de fonctionnement de tel ou tel logiciel. Même si cela peut paraître anecdotique, les remontées statistiques et les graphiques ont eux aussi un rôle important pour s'assurer du bon fonctionnement du service. Ils permettent de rapidement isoler un comportement étrange ou suspect et de visuellement se représenter l'activité du service. La Figure 3 par exemple retrace l'activité mensuelle du SMTP externe.

Figure 3 - Graphique d'activité mensuelle du SMTP externe

L'utilisation de filtrage automatisé avec fail2ban et l'application de règles d'usage ou d'accès avec Postfwd nous soulagent grandement pour la sécurisation du service. Auparavant, un utilisateur dont le compte était exploité pour émettre du *spam*, suite à un hameçonnage ou non, provoquait la mise en liste noire d'au moins un serveur SMTP auprès d'au moins un service tel que Yahoo Mail, Hotmail ou Gmail. La réputation basée sur des notes, utilisée par certaines listes noires utilisant le DNS (DNSBL), était également impactée négativement. Des actions humaines et du temps sont alors généralement nécessaires pour expliciter la situation auprès de ces divers fournisseurs et observer un retour à la normale. L'intégration des règles d'usage avec Postfwd telles que « un compte utilisateur ne peut pas envoyer plus de 10 messages par minute » permet d'éviter ces désagréments.

Nous avions déjà testé et utilisé un mandataire IMAP/POP3[4], en l'occurrence le logiciel Perdition, pour distinguer les flux entre les populations d'étudiants et des personnels. Mais finalement, bien que ce choix n'ait pas été retenu initialement, c'est le service Dovecot Director qui a été mis en place pour gérer l'ensemble des demandes de gestion de boîtes aux lettres entre les usagers et les serveurs dédiés. Son mode de fonctionnement en grappe de serveurs, son ensemble de fonctionnalités et sa capacité à pallier les soucis de verrouillage sur des accès concurrents d'un volume NFS nous ont particulièrement séduits.

La disponibilité du service est à ce stade très acceptable. En dehors du stockage qui reste à fiabiliser, tous les composants sont résilients et procurent un fonctionnement non disruptif exigé par notre communauté d'usagers. Chaque serveur fonctionne au minimum en couple avec une adresse IP virtuelle, la connectique réseau est répartie sur différents équipements actifs et les systèmes sont géographiquement placés dans des salles systèmes distinctes. Différentes sauvegardes journalières sont effectuées avec une rétention de sept jours ; des instantanés sont réalisés directement au niveau de la baie de stockage NAS et une sauvegarde de l'ensemble des données est assurée par deux systèmes dédiés dont l'un est déporté sur un troisième site.

4.2 Les évolutions envisageables ou envisagées : ce qu'on pourrait faire en plus, à la place ou différemment

Bien évidemment, il reste encore des actions à mener pour tendre vers un état « finalisé » , même si par nature un tel service a vocation à continuer d'évoluer. Dans l'immédiat, outre l'évolution du service des listes de diffusion, les points qui nous semblent les plus importants sont : améliorer le fonctionnement et les performances en exploitant le logiciel Rspamd et remplacer le service de stockage utilisé pour les boîtes aux lettres.

Un point que nous gardons à l'esprit mais sur lequel nous n'avons pas encore véritablement tranché est la possibilité d'utiliser différents logiciels pour un même service. Par exemple, utiliser un système alternatif à Debian ou encore, plutôt que d'utiliser uniquement Postfix pour le trafic SMTP ou LMTP, déployer Sendmail, Qmail ou Exim. Ceci pourrait éventuellement améliorer l'aspect sécurité du service, évitant qu'une faille exploitable dans un logiciel impacte la totalité de la solution.

4.2.1 Le service des listes de diffusion

Un point pas forcément crucial[5], mais néanmoins important sur lequel nous avons entamé une évolution est celui des listes de diffusion. Nous avons l'objectif de faire évoluer notre service de listes de diffusion en reprenant les principes mis en œuvre au niveau de la messagerie. Nous utilisons le logiciel Sympa et nous avons d'ores et déjà commencé à tester un fonctionnement s'intégrant totalement dans l'architecture globale du service de messagerie. Reprenant le principe d'une paire de serveurs partageant une adresse IP virtuelle pour fournir le service, nous avons bon espoir de finaliser ce mode

4. Quelques irréductibles parmi nos usagers ne jurent que par ce protocole pourtant désuet et source d'ennuis, mais notre rôle est avant tout de fournir le service demandé

5. Enfin tout dépend bien sûr du point de vue qu'on adopte ;)

de fonctionnement dans un délai raisonnable et compléter ainsi notre offre de messagerie électronique.

4.2.2 Le logiciel Rspamd

Les tests que nous avons effectués jusqu'ici avec Rspamd ont été très prometteurs. Cet outil nous permettrait dans un premier temps de remplacer avantageusement les services rendus par les démons SpamAssassin pour l'analyse antispam et OpenDKIM pour les signatures ou les vérifications de signatures DKIM. Ses performances élevées en font un outil précieux pour optimiser le temps de traitement global d'un message et son intégration avec le logiciel Postfix permet également de simplifier les traces de journalisation.

Actuellement, un message est initialement accepté par Postfix, qui va le transmettre aux différents sous-services avant de le récupérer pour le délivrer ou non vers la boîte d'un usager. Bien qu'il soit possible d'écrire des scripts pour faciliter la trace d'un message dans les journaux, le fait de ne pas avoir de changement de *Message-ID* pour tout le traitement d'un message offre une simplification non négligeable.

Une autre fonctionnalité fortement intéressante concerne l'intégration d'un antivirus comme ClamAV. La prise en charge d'un analyseur antiviral par Rspamd offre une amélioration du traitement en nous permettant de refuser un message dès sa soumission par un client de messagerie. Un message explicite est affiché directement au niveau du client et aucun autre traitement n'est effectué par le serveur. Voir par exemple la Figure 4 illustrant l'alerte affichée par le logiciel Thunderbird lors de l'envoi d'un message contenant un virus.

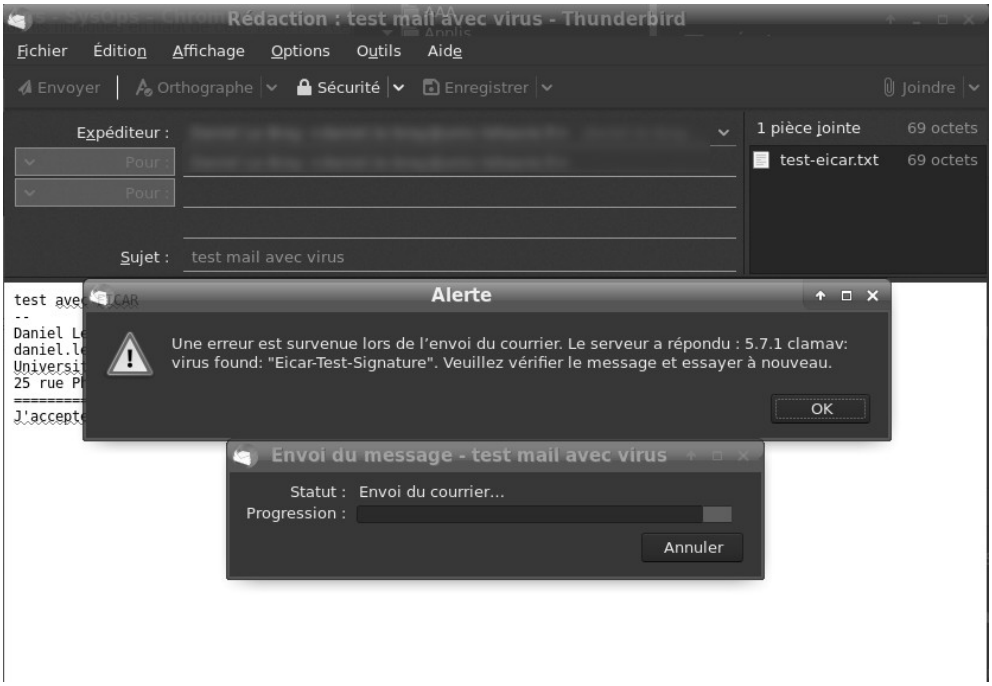

Figure 4 - Alerte d'un virus lors de l'envoi

4.2.3 Le système de stockage

Le système de stockage sur lequel nous nous appuyons à l'heure actuelle pour les boîtes aux lettres, un serveur de stockage en réseau NAS, est relativement fiable et performant. Mais il possède un gros défaut, celui d'être physiquement implanté sous forme de deux équipements localisés dans la même salle système. Sans trop entrer dans les détails, la technologie exploitée par ces systèmes impose, pour un fonctionnement actif-actif, d'avoir accès à l'intégralité des baies de disques de la solution. Nos besoins jusqu'ici se contentaient d'un tel mode opératoire, mais l'évolution de la fiabilisation de nos services nous oblige à repenser nos méthodes.

La réponse à cette volonté de fiabilité est arrivée d'elle-même avec l'investissement d'une nouvelle solution de stockage pour l'établissement. Constitué de deux baies distinctes, physiquement localisées dans des salles système différentes, ce nouveau dispositif de stockage fonctionne en mode actif-passif en s'appuyant sur une réplication asynchrone et une liaison dorsale Ethernet 40 Gb entre les salles. Certes, ce mécanisme ne nous évite pas de subir une coupure en cas de catastrophe avec le stockage actif, mais nous permet malgré tout de s'intégrer dans un plan de reprise d'activité. En s'appuyant sur une automatisation de la bascule entre le nœud actif et le nœud passif, nous devrions être en mesure de réduire l'impact négatif d'une telle catastrophe et d'obtenir rapidement un retour à la normale des services exploitant ce stockage.