Bonnes pratiques de gestion d'un service de listes de diffusion

David Verdin, Laurence Moindrot, José-Marcio Martins da Cruz, Dominique Lalot, Luc Veillon

▶ **To cite this version:**

David Verdin, Laurence Moindrot, José-Marcio Martins da Cruz, Dominique Lalot, Luc Veillon. Bonnes pratiques de gestion d'un service de listes de diffusion. JRES (Journées réseaux de l'enseignement et de la recherche) 2015, Renater, Dec 2015, Montpellier, France. ⟨hal-04805637⟩

HAL Id: hal-04805637

https://hal.science/hal-04805637v1

Submitted on 26 Nov 2024

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

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

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

Bonnes pratiques de gestion d'un service de listes de diffusion

David Verdin
GIP RENATER

Laurence Moindrot
Université de Strasbourg

José-Marcio Martins Da Cruz
MINES ParisTech

Dominique Lalot
Université d'Aix-Marseille

Luc Veillon
Académie d'Orléans-Tours

Résumé

Les services de listes de diffusion sont omniprésents dans les établissements d'enseignement et de recherche et ils ne peuvent plus être déployés sans respecter un certain nombre de bonnes pratiques. En effet, ils véhiculent une masse importante d'informations critiques et sont fortement intégrés dans nos systèmes d'information. Cet article présente les bonnes pratiques recensées par plusieurs listmasters de notre communauté ; il aborde notamment les notions d'intégration au système d'information, la messagerie, les usages, l'exploitation, l'informatique et les libertés et le niveau de service.

Mots-clefs

listes de diffusion, bonnes pratiques, Sympa, messagerie, système d'informations, exploitation

1 Introduction

Chaque année RENATER participe à l'initiative CBP (Campus Best Practice), dans le cadre du programme européen GEANT (GN3+/NA3/T2). L'objectif principal des CBP est de mettre en place des groupes de travail autour de problématiques communes rencontrées au sein des campus français et de rédiger des documents présentant les bonnes pratiques à mettre en œuvre sur ces problématiques.

En 2014, un groupe de travail « listes de diffusion » constitué de six listmasters de différents établissements de notre communauté a travaillé sur la rédaction d'un document de recommandations sur les bonnes pratiques pour « opérer un service de listes de diffusion ».

Cet article se propose de présenter les axes principaux de ces bonnes pratiques. Les thèmes abordés reflètent les expériences et difficultés communes qui ont été recensées dans ce groupe dont notamment :

- la messagerie ;
- l'intégration au système d'information ;
- les usages ;
- l'exploitation ;
- la conformité avec la loi informatique et libertés ;
- le niveau de service.

2 Messagerie

Les serveurs de listes étant par essence des distributeurs de messages, ils doivent reposer sur des systèmes de messagerie optimaux.

2.1 Infrastructure

Dans les serveurs de listes de diffusion assurant un niveau de trafic important, il est préférable d'avoir des instances différentes pour les MTAs entrant et sortant. Le MTA sortant est beaucoup plus sollicité et l'utilisation d'une instance unique peut perturber la réception de messages lorsqu'il y a beaucoup de messages en cours de distribution. Un serveur de listes peut être vu comme un amplificateur : pour chaque message en entrée peut correspondre un nombre très important de messages en sortie.

2.2 Conformité aux normes (RFCs et autres normes techniques)

Pour éviter tout dysfonctionnement dans la distribution des messages (par exemple, les rejets d'un filtre antispam trop « sensible »), il est important que le serveur de listes respecte scrupuleusement les normes techniques. Les deux normes principales sont la RFC 5321 [Klensin 2008], qui traite du protocole SMTP et qui concerne surtout le MTA sortant du serveur de listes, et la RFC 5322 [Resnik 2008] qui traite de la mise en forme des messages et de ses entêtes et qui concerne surtout le moteur du serveur de listes.

2.3 Placement en DMZ ou en intranet

La décision de placer un serveur de listes dans la DMZ ou dans l'intranet dépend du contenu du serveur et de la diversité des abonnés, mais en général, il s'agit d'un service dont le placement est typiquement en DMZ. Le serveur de listes doit être placée dans la zone Intranet, avec un éventuel accès extérieur par VPN ou similaire, s'il s'agit d'un service purement interne à l'organisme ou si le serveur abrite des données confidentielles, dans les archives ou dans des zones de partage de documents. Le placement en DMZ est nécessaire lorsque le serveur héberge des listes de diffusion ouvertes ou si le serveur contient des abonnés externes sans lien particulier avec l'organisme.

2.4 Filtrage Antispam

2.4.1 Filtrage en entrée

L'effort de filtrage doit être effectué en priorité sur le trafic entrant. Les filtres antispam classent, généralement, les messages en trois catégories, selon un score : des « hams », des « spams » et des « unsure ». Une bonne stratégie de traitement par le serveur de listes peut ressembler à ceci : les *“hams”* sont traités normalement ; les *“unsure”* sont soumis à modération ; les *“spams”* sont détruits.

2.4.2 Traitement du spam en sortie

En sortie, il ne s'agit pas à proprement de filtrage de spam mais de mesures visant à éviter que le serveur de listes soit vu comme étant un *spammeur*. En effet, tout serveur inconnu délivrant un nombre important de messages à un nombre important de destinataires peut être vu, a priori, comme un spammeur. Nous suggérons alors de mettre en place des mécanismes pour ne pas insister lorsqu'un serveur distant rejette temporairement un message (greylisting, …), de limiter le nombre de destinataires par domaine pour chaque message dans une même transaction, de limiter le nombre de transactions dans la même connexion SMTP avec un serveur distant, de ralentir la cadence d'émission si le serveur destinataire commence à refuser tous les messages avec des rejets temporaire, de gérer les erreurs et de supprimer les utilisateurs inconnus.

2.5 Authentification du domaine émetteur (DKIM, SPF, DMARC)

DKIM [Allman et al. 2007], SPF [Wong & Schlitt 2006] et DMARC [DMARC 2014-2] sont des méthodes d'authentification du domaine émetteur d'un message, permettant de vérifier qu'un message a bien été envoyé le domaine indiqué dans le champ *From*. L'intérêt de l'utilisation de ces mécanismes est de permettre aux domaines destinataires de mettre en place des règles de filtrage allégées ou alors d'être

plus condescendants vis à vis des messages envoyés par le serveur de listes.

2.6 Chiffrement et Signature

S/MIME permet de chiffrer et signer des courriels. La signature permet de garantir l'intégrité du courriel à son arrivée. Le chiffrement empêche que le contenu du courriel soit lu s'il est intercepté[Ramsdell & Turner 2010] [Ramsdell & Turner 2010-2]. Pour que la signature S/MIME soit respectée, le serveur de listes doit pouvoir ne pas modifier le corps du courriel lors du traitement d'un message signé.

3 Intégration dans le système d'information (SI)

Les différents services de listes de diffusion proposés aujourd'hui sur le marché sont beaucoup plus que de simples serveurs de publipostage à un ensemble d'utilisateurs. En effet de nombreux systèmes hébergeurs de listes permettent de répondre aux usages avancés des outils collaboratifs. Ils doivent ainsi s'intégrer au mieux dans les systèmes d'information et répondre aux politiques des établissements.

3.1 Principes de base

L'intégration du service de listes de diffusion dans le système d'information doit respecter les principes de sécurité en termes de confidentialité et de restriction d'accès aux données. Il est recommandé de choisir un service de listes ouvert et respectant les normes et les standards, pour permettre une meilleure compatibilité et interopérabilité à long terme.

3.2 Portail d'accès

Le portail d'accès (ou environnement numérique de travail) est devenu dans nos établissements un outil indispensable qui permet aux différents utilisateurs, en fonction de leur profil, de disposer d'un environnement de travail spécifique, lui donnant accès aux outils de travail collaboratifs, de communication, etc. Il est essentiel que le service de listes de diffusion puisse s'intégrer dans le portail d'accès.

3.3 Sources de données

Dans la majorité des services de listes de diffusion, la gestion (création, alimentation, mise à jour, suppression) peut se faire manuellement, mais également automatiquement, à partir de différentes sources de données. Dans le contexte des établissements de l'enseignement supérieur et du secondaire, nous recommandons un système capable de s'interconnecter avec un maximum de sources différentes et notamment les sources de données métier comme les bases des ressources humaines, les bases des étudiants ou encore l'annuaire d'établissement [Aumont & Salaün 2001].

3.4 Authentification

Afin de répondre aux nouvelles méthodes d'authentification utilisées aujourd'hui, le système de listes de diffusion doit supporter plusieurs systèmes d'authentification comme une authentification simple sur une base de données locale, une authentification simple LDAP, une authentification unique via SSO Web CAS ou encore une authentification déléguée via une fédération d'identité respectant le format SAMLv2. Le mieux étant que le système puisse combiner plusieurs méthodes d'authentification pour les populations différentes d'utilisateurs [Aumont & Salaün 2003].

3.5 Les différentes interfaces d'accès aux services de listes

Afin de s'intégrer au mieux dans le système d'information, le service de listes de diffusion doit offrir différentes interfaces de connexion et d'administration pour permettre une interopérabilité maximale avec le système d'information et ses applications. Le service devra notamment posséder une interface de gestion en ligne de commande ; une interface de gestion via la messagerie électronique ; une interface web et un accès de type web-services comme SOAP ou REST.

3.6 Les serveurs de listes comme fournisseurs de service

Les listes de diffusion créées peuvent facilement devenir des groupes réutilisables dans vos différentes applications ou dans vos référentiels. Il faut cependant faire attention à la qualité des données, certaines listes manuelles n'étant pas mises à jour, et garder en mémoire que les données des serveurs de listes sont des données applicatives, elles permettent d'alimenter et enrichir un référentiel, mais ne sont pas le référentiel.

Ainsi les adresses de listes peuvent être ajoutées au carnet d'adresses général de l'établissement, pour que les utilisateurs en aient connaissance et les utilisent.

Les listes de diffusion peuvent également être utilisées par les gestionnaires de groupe de vos outils de travail collaboratif comme par exemple l'agenda partagé.

4 Usages

Un moteur de listes a pour objectif de faciliter la diffusion de messages électroniques à un grand nombre de destinataires. Lorsque l'usage de la messagerie s'est développé, en particulier dans le milieu professionnel, les utilisateurs ont été confrontés à plusieurs difficultés et notamment la fiabilité de leur carnet d'adressesou le partage des anciens échanges.

Le moteur de listes propose des solutions techniques à ces besoins. Pour cela, il s'appuie sur un référentiel d'utilisateurs et sur un référentiel de listes. Une liste est une adresse de messagerie appartenant au périmètre du moteur de listes, qui extrait de son référentiel d'utilisateurs ceux qui sont rattachés à cette liste.

En termes d'usage, on va distinguer l'abonné, le propriétaire, le modérateur, le listmaster.

4.1 Contrôle de l'information et scénarii

L'échange de l'information peut être libre (chacun participe aux échanges, sans modération) ou restreint (l'information doit être validée avant publication, ou ne peut être émise que par une source autorisée). La liste peut être ouverte (tout le monde peut s'y abonner), restreinte ou fermée. Les abonnés peuvent être visibles ou pas. Pour répondre à ces différents usages, le moteur de listes dispose de scenarii d'autorisations qui couvrent tous ces champs [Aumont & Salaün 1999].

4.2 Nommage

Lorsque l'on gère des centaines, voire des milliers de listes il est nécessaire de mettre en place des règles de nommage pour homogénéiser les libellés et éviter les ambiguïtés. Plusieurs règles de nommage existent dans nos divers établissements. Nous recommandons de mettre en place un comité de nommage dans votre établissement qui garantit et édicte les règles de nommage.

En ce qui concerne les listes étudiantes, leur nom peut être déduit des codes étapes définis dans les logiciels de scolarité, des UFR, ou du niveau de formation.

Pour les autres listes structurelles, deux possibilités sont à votre disposition pour les adresses des listes de diffusion. Il est possible de préfixer vos listes PREFIX-<liste>@domaine.fr ou bien de créer des sous-domaines <liste>@SOUS-DOMAINE.domaine.fr dans votre domaine de messagerie qui correspondent alors à différents robots de listes dans l'outil de gestion de listes de diffusion.

4.3 Autorisation de diffusion

L'autorisation de postage aux listes peut être variée : envoi autorisé à tous, envoi autorisé aux adresses internes de votre établissement (intranet), envoi autorisé aux membres de la liste, envoi autorisé à la direction de l'établissement pour les listes générales des membres du personnels, envoi autorisé à un nombre limité de personnes à définir (responsable d'une entité, responsable de scolarité, responsable de service, etc.).

Une possibilité de modération peut s'ajouter à ces options. Plus le droit d'envoi est ouvert, plus la gestion est facile et moins la diffusion des messages est contrôlée. Il faut trouver le juste équilibre pour chaque liste en fonction de leur utilisation.

4.4 Cycle de vie des listes

Lorsque l'on travaille sur un campus universitaire ou dans un établissement du secondaire, les listes de diffusion liées à la gestion des étudiants suivent le cycle de vie d'une année universitaire ou scolaire. Il est alors nécessaire d'automatiser au maximum la gestion (création, mise à jour et suppression) de ces listes.

D'autres listes peuvent également être gérées automatiquement, comme par exemple la liste des membres du personnel, ou bien des listes spécifiques par entité, catégorie de personnel, fonction, etc. Les sources de données de ces listes sont vos divers référentiels personnels et étudiants (bases de données, annuaires, etc.).

4.5 Le cas des listes étudiantes

Les listes de diffusion liées à la gestion des étudiants suivent le cycle de vie d'une année universitaire ou scolaire. Elles sont créées à la rentrée. Pour la suppression, cela dépend du nommage des listes. Si les listes étudiantes ne sont pas suffixées par l'année en cours, elles doivent être renommées ou supprimées et recréées à la rentrée. Si on suffixe les listes étudiantes avec l'année universitaire ou scolaire en cours, cela permet de conserver plus longtemps les anciennes listes. Il faut déterminer avec les responsable de la scolarité le délai de conservation de ces listes.

Les abonnés des listes automatiques sont mis à jour à partir des sources de données auxquelles les listes se rapportent. On peut cependant se poser la question de la mise à jour manuelle des listes si les référentiels ne sont pas à jour ou si l'on souhaite ajouter des abonnés supplémentaires.

4.6 Archivage

Lorsqu'une liste est supprimée, il est souvent utile d'archiver les données (liste des membres, courriels) pendant une certaine période. Une année de rétention des archives semble suffisante dans un établissement d'enseignement supérieur, où la validité des données repose sur l'année scolaire en cours

5 Exploitation

La déclinaison des rôles (listmaster, propriétaire, modérateur, abonnés) dans un moteur de listes permet de déléguer une grande partie de l'exploitation fonctionnelle à des tiers. L'exploitation du moteur de listes étant souvent assurée par l'équipe qui endosse le rôle de listmaster, ce chapitre décrit les tâches et difficultés les plus fréquemment rencontrées par un exploitant/listmaster.

5.1 Exploitation des listes

5.1.1 Distinction des domaines virtuels

Avant d'aborder les questions d'exploitation, il est important de formaliser l'architecture du moteur de listes qui sera mis en place.

Dans le cas d'une diffusion institutionnelle interne à l'organisation, le domaine de diffusion doit être protégé, les sources de données des listes doivent utiliser autant que possible les référentiels du personnel et des étudiants, le nommage des listes doit être construit selon des règles précises, voire automatisables ; les scénarios doivent être travaillés pour pouvoir répondre aux règles communes de diffusion ; le serveur doit est localisé en interne.

Dans le cas d'un service public, le domaine de diffusion doit être ouvert, les sources de données sont rarement automatisées, les scénarios doivent rester le plus standard possible ; le serveur peut être localisé en DMZ, même s'il est préférable de le protéger par un reverse proxy.

Même si on mutualise ces deux types de listes sur un seul serveur, il est préférable de mettre en place

plusieurs domaines virtuels et de monter un robot distinct pour chaque domaine.

Les tâches d'exploitation sont plus lourdes dans le cas d'un domaine destiné à la diffusion institutionnelle, en particulier pour industrialiser la création et l'alimentation des listes, et élaborer des scénarios répondant aux nécessités d'un contrôle fin de la diffusion.

5.1.2 Industrialisation de la création de listes

Les grandes organisations comme les universités, segmentent leur diffusion sur un emboîtement de critères mêlant la temporalité (quelle année), la scolarité (quelle étape, quelle matière, quel cursus) et les ressources humaines (quel statut, quel corps...).

Les listes doivent être regroupées par typologie et suivre le même modèle en termes d'autorisations, de modes de diffusion, de taille de message, de définition des rôles et des sources de données.

5.1.3 Nettoyage des listes obsolètes

Une fois réglé les modalités de création de listes, la difficulté principale d'un exploitant réside dans le nettoyage des listes obsolètes comme celles qui ne sont plus utilisées depuis un longue période ou dont le propriétaire n'est plus joignable ou dont le taux d'erreurs est élevé. Pour éviter tout problème, en particulier dans le cas d'un service ouvert à l'extérieur, il est indispensable d'anticiper les différents cas de figure que l'on pourra rencontrer, en détaillant les processus que l'exploitant mettra en œuvre.

5.2 Changement de version du moteur de listes

Pour garantir la continuité du service de listes, il faudra préparer la mise à jour de manière à réduire le risque de retour arrière. Voici quelques règles à suivre lors de la mise à jour de vos moteurs de listes :

- lire les RELEASE NOTES ;
- disposer d'un serveur de préproduction, copie conforme de la production pour tester la mise à jour au préalable ;
- sauvegarder l'ensemble du moteur de listes, librairies comprises avant la mise jour ;
- stopper l'arrivée des courriels en amont et s'assurer que les dernières diffusions sont terminées.

5.3 Maintien en condition opérationnelle

Afin de maintenir en condition opérationnelle le service de liste de diffusion, l'exploitant doit s'assurer de la disponibilité du service de listes en mettant en place une supervision du moteur, de la base interne, du portail web, et des sources de données externes (un suivi nagios ou équivalent est recommandé) ; en mettant en œuvre la sauvegarde des bases de donnés et des fichiers de configuration du gestionnaire de listes ; et en permettant un suivi des performances du serveur de listes et de la messagerie, en particulier l'occupation des spools.

6 Informatique et libertés

Les données à caractère personnel qui sont concernées par les services de liste sont l'adresse électronique, le nom et le prénom et éventuellement une image représentant l'utilisateur (avatar).

Les contenus échangés, relèvent eux plutôt du contenu éditorial, mais peuvent contenir les données personnelles et doivent donc être protégés au même titre. Ces données interviennent selon trois axes : le maintien d'une liste de personnes abonnées à une liste de diffusion, les archives de la liste, les journaux des applications.

6.1 Confidentialité

Avant tout, il convient de distinguer les informations relevant de l'activité professionnelle et celles relevant de la vie privée. Ensuite, dans les données professionnelles, il faut distinguer celles qui doivent rester confidentielles et celles qui peuvent être publiques. On peut définir des listes totalement masquées, où toute action est limitée voire impossible, en dehors de l'envoi de messages. Dans les cas extrêmes,

l'existence même de la liste doit rester secrète.

6.2 Droit de se désabonner d'une liste

Le droit de modification peut avoir des limites, notamment si l'abonnement à une liste de diffusion entre dans les obligations liées à l'occupation d'une fonction. Une liste d'information du personnel, par exemple, peut interdire le désabonnement, parce que le fait d'appartenir à l'établissement impose de recevoir les messages d'information du personnel. Dans tout autre cas, l'utilisateur doit disposer de moyens clairs de désabonnement.

6.3 Droit d'accès à ses données personnelles

Tout abonné doit pouvoir facilement savoir quelles données personnelles le concernant sont utilisées par le service de listes.

6.4 Traçabilité de l'activité des listes

La traçabilité des échanges est indispensable pour vérifier l'intégrité des données. Cette sécurisation est rendue possible par le biais de plusieurs mécanismes comme la signature des messages ou la conservation de logs sur une durée légale maximale (un an en France) qui permet de contrôler les accès aux données.

6.5 La réglementation

La France dispose d'une réglementation précise en matière de protection de la vie privée.

6.5.1 Réglementation sur les listes

Jusqu'à il y a quelques années, la situation semblait claire. Elle était exprimée par la voix de la FAQ de la liste droit-net [Aumont & De Marco 2002]. La CNIL avait mis en place les normes simplifiées 15 et 23 permettant de faire une déclaration d'adoption de ces normes via le formulaire CERFA 99001.

Tout ceci a été modifié par la loi n° 2004-801 du 6 août 2004 [Loi 2004]. Comme on le voit sur la même FAQ de droit-net [Aumont & De Marco 2004], ceci remet en question les recommandations préalables vis à vis des listes de diffusion.

Ces normes simplifiées ont été abrogées par la dispense de déclaration n°7 [CNIL 2006], et la dispense de déclaration n°8 [CNIL 2010]. La déclaration n°7 dispense les services de listes non commerciaux de toute déclaration CNIL, et la dispense n° 8 fait de même pour les associations.

Il reste désormais la norme simplifiée n°48 [CNIL 2012] qui porte sur les clients et prospects.

S'il existe un CIL dans l'établissement, nul besoin de "déclaration CNIL" à proprement parler : une description/inscription au Registre suffit (sauf si les données sont réputées sensibles).

6.5.2 Réglementation sur les archives

Ce point reste flou dans les textes. Seul l'article 36 de la loi de 1978 [Loi 1978] indique qu'on ne peut conserver des archives "qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques".

Les archives des listes de démarchage commercial ne rentrent pas dans ce cadre mais, sur un service de listes d'établissement, un bon nombre de messages échangés dans les listes peuvent servir de référence et ont donc un intérêt "historique ou scientifique". Les autres, en revanche, devraient disparaître au nom du droit à l'oubli.

Il y a une délibération de la CNIL qui porte sur les archives publiques [CNIL 2012-2].

6.5.3 Réglementation sur les journaux

Nous conservons pendant un an des journaux du serveur de listes. Ces journaux contiennent, quand elle est disponible, l'adresse électronique de la personne effectuant une action sur le serveur. L'accès à ces journaux doit être protégé mais rendu accessible en cas de saisie par des services judiciaires.

7 Niveau de service

Un moteur de listes intervient dans un mécanisme de diffusion asynchrone par nature, puisque s'appuyant sur la messagerie électronique. Néanmoins, il peut proposer des interfaces, pour les utilisateurs et pour son administration, qui peuvent faire l'objet d'une négociation sur un accord de niveau de service. Les points qui peuvent être associés à un niveau de service sont la disponibilité du mécanisme de messagerie en réception et en émission, la capacité à hiérarchiser les envois selon les listes, la disponibilité des interfaces, la réactivité des administrateurs pour toutes les tâches qui sont soumises à leur contrôle.

Les leviers d'action pour augmenter le niveau de service couvrent le domaine organisationnel comme le domaine technique.

7.1 Organisation autour du service de listes

Le service de listes repose sur une équipe clé, les « listmaster ». Administrateurs du moteur de listes, ils reçoivent et doivent traiter dans les délais requis les requêtes des utilisateurs transmises par le serveur. La fonction de listmaster doit être partagée par plusieurs intervenants. On peut augmenter le niveau de service en répartissant les listmaster sur différents domaines de messagerie et en organisant des plages horaires plus larges. Une équipe de supervision doit également être mise en place pour surveiller les infrastructures nécessaires au bon fonctionnement du service [Racvision].

7.2 Mécanismes techniques pour augmenter le niveau de service

Pour augmenter le niveau de service du serveur de listes, une attention particulière sera apportée à la mise en place de serveurs en haute disponibilité ou en cluster pour les services de bases de données, le serveur SMTP, le serveur HTTP ou le moteur de listes lui-même. La mise en place d'un mécanisme de proxy et de traitement de certificat en amont du frontal web est également un plus. Pour fiabiliser les données, la mise en place de sauvegarde devra être mise en œuvre.

Conclusion

Cet article a présenté les bonnes pratiques qui nous semblent essentielles pour opérer une service de listes qui soit à la fois performant et durable. Forts de ce bel assemblage bien cohérent, il nous semble pertinent de profiter de la conclusion pour le démonter et instiller un peu de doute salvateur dans l'esprit du lecteur – s'il n'y était pas déjà. En effet :

- bien que l'ensemble des propositions présentées ici aient fait l'objet d'un consensus au sein de notre groupe ;
- bien que nous pensions composer une panel raisonnablement représentatif de la communauté enseignement supérieur recherche ;
- bien que nous ayons réellement fait de notre mieux ;

… nous sommes conscients des limites qu'un tel exercice présente. Nous ne prétendons pas avoir atteint l'exhaustivité ni épuisé le sujet - loin de là. D'une part parce que l'on peut présenter d'autres solutions aux problèmes que nous avons évoqués et d'autre part parce que le domaine de la messagerie et des listes de diffusion est, techniquement parlant, en constante évolution ; nos recommandations sont donc sujettes à péremption.

Il est possible que vous ayez été horrifié par certaines de nos recommandations ou que vous lisiez ce document en 2017 et qu'une nouvelle technologie soit arrivée, changeant totalement la donne. Nous vous invitons à nous en faire part, voire encore mieux : à en faire part à la communauté. Tout comme cet article est le fruit d'une collaboration, le progrès de nos services repose sur la constante coopération qui s'établit entre collègues. Donc, pour finir, rendons à la communauté ce qui lui appartient : adressez vos remarques sur cet article à sympa-fr@listes.renater.fr. C'est sans doute la meilleure adresse.

Plus d'informations sur :

https://www.renater.fr/IMG/pdf/operer_un_serveur_de_listes_de_diffusion_v271114.pdf

Bibiographie

[Allman et al. 2007] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, 2007 : « RFC 4871 : DomainKeys Identified Mail (DKIM) Signatures » http://www.ietf.org/rfc/rfc4871.txt

[Aumont 2009] S. Aumont, 2009 : « Mailing lists and DKIM » https://spaces.internet2.edu/display/ddx/Mailing+lists+and+DKIM

[Aumont & De Marco 2002] S. Aumont and E. De Marco, 2002 : « FAQ de la liste droit-net » https://groupes.renater.fr/droit-net/fom-serve/cache/82.html

[Aumont & De Marco 2004] . Aumont and E. De Marco, 2004 : « FAQ de la liste droit-net » https://groupes.renater.fr/droit-net/fom-serve/cache/42.html

[Aumont & Salaün 1999] S. Aumont and O. Salaün, 1999 (updated 2011) : « Sympa reference manual : authorization scenarios » https://www.sympa.org/manual/authorization-scenarios

[Aumont & Salaün 2000] S. Aumont and O. Salaün, 2000 (updated 2010) : « Sympa reference manual : S/MIME and HTTPS » https://www.sympa.org/manual/x509

[Aumont & Salaün 2001] S. Aumont and O. Salaün, 2001 (updated 2013) : « Sympa reference manual for handling external data sources » https://www.sympa.org/manual/parameters-data-sources

[Aumont & Salaün 2003] S. Aumont and O. Salaün, 2003 (updated 2014) : « Sympa reference manual : l authentication » https://www.sympa.org/manual/authentication

[Bouteille 2004] G. Bouteille, 2004 (updated 2013) : « Sympa reference manual : list families » https://www.sympa.org/manual/list-families

[CNIL 2006] CNIL, 2006 : « Dispense de déclaration n° 7 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/107/

[CNIL 2010] CNIL, 2010 : « Dispense de déclaration n° 8 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/106/

[CNIL 2012] CNIL, 2012 : « Norme simplifiée n° 48 » http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/184/

[CNIL 2012-2] CNIL, 2012 : « Délibération de la CNIL sur les archives publiques » http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/quelles-sont-les-donnees-a-caractere-personnel-concernees-par-la-diffusion-sur-internet-de-docum/

[DMARC 2014] dmarc.org, 2014: « DMARC FAQ » http://www.dmarc.org/faq.html#s3

[DMARC 2014-2] dmarc.org, 2014: « Domain-based Message Authentication, Reporting and Conformance (DMARC) Specification » http://www.dmarc.org/specification.html

[Hoffman 1999] P. Hoffman, editor, 1999 : « RFC 2634: Enhanced security services for S/MIME » http://tools.ietf.org/html/rfc2634

[Klensin 2008] J. Klensin, 2008: « RFC 5321: Simple Mail Transfer Protocol – section 5.4.5 » http://tools.ietf.org/html/rfc5321#section-4.5.4

[Levine 2014] J.R. Levine, 2014: « Yahoo addresses a security problem by breaking every mailing list in the world » http://jrl.guru/Email/yahoobomb.html

[Loi 1978] Texte de loi, 1978 : « Article 36 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/#Article36

[Loi 2004] Texte de loi, 2004 : « Loi n° 2004-801 du 6 août 2004 » http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676

[Racvision] Projet du Ministère de l'éducation nationale, normalisant les pages de supervision à insérer dans chaque application afin d'en mesurer différents indicateurs de disponibilité. Des pages et procédures spécifiques sont développées pour surveiller le fonctionnement de la messagerie et d'un poteur de liste. http://racvision.orion.education.fr/presentation/index.html

[Ramsdell & Turner 2010] B. Ramsdell and S. Turner, 2010 : « RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2: Certificate Handling »

http://tools.ietf.org/html/rfc5750

[Ramsdell & Turner 2010-2] B. Ramsdell and S. Turner, 2010 : « RFC 5750: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2: Message Specification » http://tools.ietf.org/html/rfc5751

[Resnik 2008] P. Resnik, 2008: « RFC 5322: Internet message format » http://tools.ietf.org/html/rfc5322

[Verdin 2013] D. Verdin, 2013 : « User-friendly automatic lists » https://www.sympa.org/manual/list-families#user-friendly_automatic_lists

[Verdin 2014] D. Verdin, 2014: « Sympa online help on DMARC » https://www.sympa.org/manual/dmarc

[Wong & Schlitt 2006] M. Wong and W. Schlitt, 2006 : « RFC 4408 : Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1 » http://www.ietf.org/rfc/rfc4408.txt

[Zhuk 2002] S. Zhuk, 2002: « Sympa reference manual : list_check_smtp parameter » https://www.sympa.org/manual/conf-parameters/part2#list_check_smtp