Groupe de travail Réseau
Request for Comments : 3888
Catégorie : Information

T. Hansen, AT&T Laboratories
September 2004
Traduction Claude Brière de L'Isle

Modèle et exigences du suivi de message

Résumé
Les acheteurs de systèmes de messages d'entreprise demandent souvent : Puis-je suivre les messages ? Le suivi de message est la capacité à découvrir le chemin qu'a pris un certain message à travers un système de messagerie et l'état actuel d'acheminement de ce message. Le présent document fournit un modèle de suivi de message qui peut être utilisé pour comprendre l'infrastructure de messages à l'échelle de l'Internet et d'améliorer encore ces capacités en incluant le suivi de message, ainsi que les exigences pour les solutions proposées de suivi de message.

1. Position du problème

Considérons l'envoi d'un colis par l'intermédiaire d'une société de livraison de paquets. Un fois qu'on a envoyé le colis, on aimerait bien être capable de savoir si le colis a bien été livré ou non, et si non, où il se trouve actuellement et quel est son état. Noter que l'état d'un colis peut ne pas inclure si il a été livré à celui à qui il était adressé, mais juste la destination. De nombreux transporteurs de paquets fournissent aujourd'hui de tels services, souvent via une interface de la Toile.

Le suivi de message étend cette capacité à l'infrastructure de messages à l'échelle de l'Internet, de façon analogue au service fourni par les transporteurs de colis : la capacité à localiser rapidement où est un message (un colis) et déterminer si le message (colis) a été livré ou non à sa destination finale. Une approche par la normalisation Internet va permettre le développement d'applications de suivi de message qui pourront fonctionner dans un environnement de messagerie multi-fournisseurs et encouragera le fonctionnement à travers les frontières administratives.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Définitions

Les termes qui suivent relèvent du suivi de message. Les termes Agent d'utilisateur de suivi *(Tracking User Agent)* et Serveur de suivi *(Tracking Server)* sont nouveaux, tandis que tous les autres termes ont été collectés à d'autres sources.

Agent d'utilisateur de messagerie (MUA, *Mail User Agent*) d'origine
L'agent d'utilisateur de messagerie d'origine est le logiciel utilisé pour composer et générer un message. C'est le logiciel qui se trouve dans un ordinateur personnel.

Agent de soumission de messagerie (MSA, *Mail Submission Agent*) d'origine
L'agent de soumission de messagerie accepte un message provenant d'un agent d'utilisateur, y ajoute ou le modifie pour le rendre conforme aux règles de l'Internet et/ou à la politique du site, et injecte le message dans le réseau. Le MSA peut être le MTA initial ou peut relayer le message à un MTA.

Agent de transfert de message (MTA, *Message Transfer Agent*)
Un agent de transfert de message accepte un message et le déplace vers sa destination. Cette destination peut être locale ou atteinte via un autre MTA. Il peut utiliser une file d'attente locale pour mémoriser le message avant de le transférer plus loin. Tout MTA peut générer une notification de non livraison.

Agent de transfert de message (MTA, *Message Transfer Agent*) intermédiaire
Un MTA intermédiaire est un MTA qui accepte un message pour le transférer quelque part ailleurs.

Agent de transfert de message final
C'est un MTA qui accepte un message pour une livraison locale. Il est l'endroit final où est accepté un message. Le MTA final est celui qui envoie les notifications d'état de livraison (DSN, *Delivery Status Notification*). (Les MTA intermédiaires peuvent aussi envoyer une DSN si ils relayent à un MTA qui n'a pas la capacité de DSN.)

Agent de transfert de message étranger
Un MTA étranger assure la livraison des messages en utilisant d'autres protocoles que ceux spécifiés pour la messagerie Internet, comme un système de messagerie X.400.

Agent de transfert de message passerelle (GW-MTA, *Gateway Message Transfer Agent*)
Un MTA passerelle accepte un message à transférer à un MTA étranger en dehors de l'espace du protocole Internet.

Agent de livraison local (LDA, *Local Delivery Agent*)
L'agent de livraison local livre le message au magasin local de messages. (Le MTA et le LDA sont souvent combinés dans le même programme.)

Notification d'état de livraison (DSN, *Delivery Status Notification*)
Une notification d'état de livraison [RFC3464] est produite par un MTA lorsque un message n'est pas bien livré, soit à son prochain bond, soit au magasin de message final, ou lorsque il est bien livré, soit à un MTA étranger, soit à un agent de livraison local, soit à un MTA sans capacité de DSN. Les notifications positives ne sont effectuées [RFC3461] que lorsque spécifiquement demandées.

Notification de non livraison (NDN, *Non-Delivery Notification*)
Une notification de non livraison est une forme particulière de DSN qui indique l'échec de la livraison.

Notification de disposition de message (MDN, *Message Disposition Notification*)
Elle est utilisée pour faire rapport de la disposition d'un message après qu'il a été bien livré à un receveur.

Agent d'utilisateur de suivi (TUA, *Tracking User Agent*)
Un agent d'utilisateur de suivi veut trouver des informations sur un message au nom d'un utilisateur. Il est le demandeur ou l'initiateur d'une telle demande. (MUA et TUA pourraient être combinés dans le même programme.)

Serveur de suivi
Un serveur de suivi fournit des information de suivi à un client de suivi. Il est le dépositaire des informations sur un message pour la traversée d'un certain MTA. (Le serveur de suivi et le MTA peuvent fonctionner sur le même système.)

3. Entités

Les entités impliquées dans un suivi de message sont : les agents d'utilisateur de message, les agents de soumission de message, les agents de transfert de message, les agents d'utilisateur de suivi, et les serveurs de suivi.

4. Exigences

Ce sont les exigences que toute solution de suivi de message doit être capable de satisfaire :

La solution de suivi de message :
** DOIT s'adapter à l'Internet.
** DOIT être facile à déployer.
** DEVRAIT maximiser la réutilisation des technologies et infrastructures existantes, déjà déployées.
** Si possible, DEVRAIT étendre les protocoles existants et non en inventer de nouveaux.
** DEVRAIT avoir un faible coût de mise en œuvre. (Afin de faciliter l'incorporation dans les produits existants.)
** DOIT restreindre le suivi d'un message au générateur du message (ou à un délégué).
** DOIT être capable de faire l'authentification.
** PEUT permettre au générateur de déléguer cette responsabilité à un tiers.
** DEVRAIT avoir la propriété de permettre la délégation message par message de la responsabilité du suivi.
** DOIT exige d'un agent d'utilisateur de suivi qu'il prouve qu'il lui est permis de demander les informations de suivi.

** DOIT être capable d'identifier les messages de façon univoque.
** DOIT exiger que chaque message ait une identification univoque.

5. Modèles d'interaction

Il y a plusieurs modèles selon lesquels le suivi des messages peut être activé, par lesquels les messages peuvent être suivis, et par lesquels les informations peuvent être demandées et rassemblées.

5.1 Modèles permettant le suivi

L'enveloppe ou l'en-tête de message doit contenir assez d'informations pour suivre un message et restituer en toute sécurité les informations sur le message. Tout message qui n'a pas assez d'informations pour le suivre est par définition non suivable.

Si il n'y a pas assez d'informations disponibles dans les enveloppes ou les en-têtes de message standard actuelles, le standard courant devra être étendu. Le MUA ou le MSA doit déterminer les informations supplémentaires et permettre le suivi en ajoutant les informations supplémentaires soit à l'enveloppe, soit à l'en-tête.

Cela conduit à deux modèles d'activation de suivi : l'activation passive et l'activation active.

5.1.1 Modèle d'activation passive

Le modèle "d'activation passive" suppose qu'il y a suffisamment d'informations disponibles. Aucune interaction d'UA ou de MSA ne survient pour activer le suivi ; il est activé par défaut.

5.1.2 Modèle d'activation active

Le modèle "d'activation active" exige que le MUA et le MSA échangent des informations lorsque le message est soumis. Cet échange indique que l'enregistrement de la traversée du message devrait être effectué, ainsi que la fourniture d'assez d'informations supplémentaires pour permettre au message d'être suivi. Ces informations devront être passées en tant que de besoin aux MTA suivants.

5.2 Modèles de demande de suivi

Il y a plusieurs modèles par lesquels peuvent être demandées les informations de suivi.

5.2.1 Modèle de demande passive

Le modèle de "demande passive" exige une activation active pour indiquer qu'une certaine forme de suivi est à effectuer. Les informations de suivi peuvent être renvoyées immédiatement (comme une forme de télémétrie) ou envoyées à un tiers pour restitution ultérieure.

5.2.2 Demande passive d'informations de suivi

Les formes d'informations de suivi passives qui pourraient éventuellement être demandées sont les suivantes. Noter qu'il existe déjà des mécanismes pour demander les informations marquées avec un (+). Les références pour de tels mécanismes sont énumérées à la fin de ces entrées.

** envoyer une DSN d'un message arrivant à un MTA intermédiaire.
** (+) envoyer une DSN d'un message rejeté à un MTA intermédiaire [RFC3464].
** (+) envoyer une DSN d'un message qui quitte un MTA intermédiaire et va à un autre MTA [RFC2852].
** envoyer une DSN d'un message qui arrive à un MTA final.
** (+) envoyer une DSN d'un message rejeté à un MTA final [RFC3464].
** (+) envoyer une DSN d'un message livré à un magasin de messages d'un utilisateur [RFC3464].
** (+) envoyer une DSN d'un message livré à un MTA étranger [RFC3464].
** (+) envoyer une DSN d'un message lu par un utilisateur final [RFC3798].

5.3 Modèle de demande active

Le modèle de "demande active" exige une interrogation active par un agent d'utilisateur d'un usager au MSA, aux MTA intermédiaires et au MTA final, ou à un tiers, pour trouver l'état du message tel que connu par ce MTA. La demande active va fonctionner avec l'activation passive ou active.

5.3.1 Chaînage de serveur ou référence de serveur

Lorsque des informations de suivi ont été demandées à un serveur de suivi, et lorsque le message a été passé à un autre MTA dont ce serveur de suivi n'a aucune connaissance, il y a deux choix de modèle :

** le premier serveur de suivi va contacter le prochain serveur de suivi et l'interroger sur l'état et repasser l'état combiné (chaînage de serveur) ou
** le premier serveur de suivi va retourner l'adresse du prochain MTA et c'est le client de suivi qui a la responsabilité de contacter le prochain serveur de suivi (référence de serveur).

5.3.2 Demande active d'informations de suivi

Les formes d'informations de suivi actives qui pourraient être demandées sont les suivantes. (Noter qu'il n'existe actuellement aucun mécanisme pour demander de telles informations.)

** le message a été mis en file d'attente pour livraison ultérieure,
** le message a été livré en local,
** le message a été livré à un autre MTA,
** le message a été livré à un MTA étranger,
** demander à un serveur de suivi différent,
** je sais mais je ne peux pas vous le dire,
** je ne sais pas.

5.4 Combinaison des informations de DSN et de MDN avec les informations de suivi de message

Les informations qui seraient restituées par le suivi de message et les informations qui sont retournées des demandes de DSN et de MDN tentent toutes de répondre à la question "qu'est-il arrivé au message XX" ? Les informations fournies par chacun sont complémentaires par nature, mais similaires. Un agent d'utilisateur de suivi pourrait utiliser les trois sources d'informations possibles pour présenter une vue totale de l'état d'un message.

Les deux notifications DSN et MDN utilisent les formats définis dans la [RFC3462]. Cela suggère que les informations retournées par les solutions de suivi de message devraient aussi être similaires.

6. Considérations sur la sécurité

6.1 Résumé des considérations de sécurité

Les vulnérabilités de la sécurité sont détaillées dans la [RFC3885], la [RFC3886] et la [RFC3887]. Ces considérations incluent :

** la vulnérabilité à l'espionnage ou aux attaques en répétition lorsque utilisé dans des sessions non chiffrées,
** une dépendance au caractère aléatoire du secret par message,
** le fait de s'appuyer sur TLS,
** les attaques par interposition,
** le fait que le serveur conserve le niveau de sécurité lorsque il effectue le chaînage,
** le déni de service
** le souci de la confidentialité,
** les falsifications par des serveurs malveillants.

6.2 Identification et authentification de message

C'est un modèle de sécurité pour l'identification et l'authentification de message qui pourrait être déployé. (Il peut y en avoir d'autres.)

Un agent d'utilisateur de suivi doit prouver qu'il lui est permis de demander des informations de suivi sur un message. Chaque message conforme à la [RFC0822] est supposé contenir un en-tête Identifiant de message. Un mécanisme possible est que le générateur calcule un hachage unidirectionnel A à partir de l'identifiant du message + un horodatage + un secret par usager. L'utilisateur calcule alors un autre hachage unidirectionnel B comme étant le hachage de A. L'usager inclut B dans le message soumis, et conserve A. Plus tard, lorsque l'usager fait une demande de suivi de message au système de messagerie ou à l'entité de suivi, il soumet A dans la demande de suivi. L'entité qui reçoit la demande de suivi utilise alors A pour calculer B, car il a déjà fourni B, vérifiant que le demandeur est authentique. En résumé,

A = H(Identifiant de message + horodatage + secret)

B = H(A)

Un autre mécanisme possible pour A est d'ignorer l'identifiant de message et l'horodatage et d'utiliser juste un hachage unidirectionnel à partir d'un grand nombre aléatoire (>128 bits). B serait calculé comme ci-dessus. En résumé,

A = H(grand nombre aléatoire)

B = H(A)

Cette technique est similaire aux méthodes utilisées pour les mots de passe à utilisation unique [RFC2289]. Le succès de ces techniques dépend du caractère aléatoire du secret par utilisateur ou du grand nombre aléatoire, qui peut être incroyablement difficile dans certains environnements.

Si le générateur d'un message devrait déléguer sa demande de suivi à un tiers en lui envoyant A, cela serait vulnérable à l'espionnage sur des sessions non chiffrées. L'usager peut décider message par message si ce risque est acceptable.

7. Références pour information

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2289] N. Haller, C. Metz, P. Nesser, M. Straw, "Système de mot de passe à utilisation unique", février 1998. (STD0061)

[RFC2852] D. Newman, "Extension de service SMTP Livraison par", juin 2000. *(P.S.)*

[RFC3461] K. Moore, "Extension de service du protocole simple de transfert de messagerie (SMTP) pour les notifications d'état de livraison (DSN)", janvier 2003. (*MàJ par* RFC3798, RFC3885, RFC5337, RFC6533) *(D.S.)*

[RFC3462] G. Vaudreuil, "Type de contenu Multipart/Report pour les rapports des messages administratifs du système de messagerie", janvier 2003. (*Remplacée par* RFC6522, SDT73*)*

[RFC3464] K. Moore, G. Vaudreuil, "Format extensible de message pour les notifications d'état de livraison", janvier 2003. (*MàJ par* RFC4865, RFC5337, RFC6533) *(D.S.)*

[RFC3798] T. Hansen et G. Vaudreuil, éd., "Notification de disposition de message", mai 2004. (*MàJ par* RFC5337, RFC6533) *(D.S.)*

[RFC3885] E. Allman, T. Hansen, "Extension de service SMTP pour le suivi de message", septembre 2004. *(P.S.)*

[RFC3886] E. Allman, "Format de message extensible pour les réponses de suivi de message", septembre 2004. *(P.S.)*

[RFC3887] T. Hansen, "Protocole d'interrogation de suivi de message", septembre 2004. *(P.S.)*

8. Remerciements

Le présent document est le produit des apports de nombreuses personnes et de nombreuses sources, parmi lesquelles tous

les membres du groupe de travail Suivi de message : Philip Hazel, Alexey Melnikov, Lyndon Nerenberg, Chris Newman, et Gregory Neil Shapiro. Il doit beaucoup aux travaux antérieurs de Gordon Jones, Bruce Ernst, et Greg Vaudreuil. En particulier, je tiens aussi à remercier Ken Lin de ses contributions considérables aux premières versions du document.

9. Adresses de l'auteur

Tony Hansen
AT&T Laboratories
Middletown, NJ 07748
USA

téléphone : +1.732.420.8934
mél : tony+msgtrk@maillennium.att.com

10. Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.