Groupe de travail Réseau
Request for Comments : 5426
Catégorie : Sur la voie de la normalisation

A. Okmianski, Cisco Systems, Inc.
mars 2009
Traduction Claude Brière de L'Isle

Transmission des messages Syslog sur UDP

Résumé
Le présent document décrit le transport des messages syslog sur UDP/IPv4 ou UDP/IPv6. L'architecture en couches du protocole syslog fournit la prise en charge d'un nombre quelconque de transpositions de transport. Cependant, pour les besoins d'interopérabilité, les mises en œuvre du protocole syslog sont obligées de prendre en charge la présente transposition de transport.

Table des matières

1. Introduction

La [RFC3164] pour information décrit le protocole syslog comme il a été observé dans les mises en œuvre existantes. Elle décrit le format des messages syslog et un transport UDP [RFC0768]. Ensuite, un protocole syslog sur la voie de la normalisation a été défini dans la [RFC5424].

La RFC 5424 spécifie une architecture en couches qui fournit la prise en charge d'un nombre quelconque de transpositions de couche de transport pour transmettre les messages syslog. Le présent document décrit la transposition de transport UDP pour le protocole syslog.

Le transport décrit dans ce document peut être utilisé pour transmettre des messages syslog sur IPv4 [RFC0791] et sur IPv6 [RFC2460].

Les administrateurs et architectes de réseau devraient connaître les problèmes significatifs de fiabilité et de sécurité de ce transport, qui découlent de l'utilisation de UDP. Ils sont documentés dans cette spécification. Cependant, ce transport est léger et s'appuie sur l'utilisation populaire existante de UDP pour syslog.

2. Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Protocole de transport

3.1 Un message par datagramme

Chaque datagramme syslog UDP DOIT contenir seulement un message syslog, qui PEUT être complet ou tronqué. Le message DOIT être formaté et tronqué conformément à la [RFC5424]. Des données supplémentaires NE DOIVENT PAS être présentes dans la charge utile du datagramme.

3.2 Taille de message

Cette transposition de transport prend en charge la transmission de messages syslog jusqu'à 65535 octets moins la longueur de l'en-tête UDP. Cette limite découle de la taille maximum supportée par UDP de 65535 octets spécifiée dans la [RFC0768]. Pour IPv4, la taille maximum de charge utile est de 65535 octets moins l'en-tête UDP et moins l'en-tête IP parce que IPv4 a un champ de longueur de 16 bits qui inclut aussi la longueur de l'en-tête.

Les receveurs syslog IPv4 DOIVENT être capables de recevoir des datagrammes avec des tailles de message jusqu'à et inclus 480 octets. Les receveur syslog IPv6 DOIVENT être capables de recevoir des datagrammes avec des tailles de message jusqu'à et inclus 1180 octets. Tous les receveurs syslog DEVRAIENT être capables de recevoir des datagrammes avec des tailles de message jusqu'à et inclus 2048 octets. La capacité de recevoir des messages plus grands est encouragée.

Les restrictions et recommandations ci-dessus établissent une base pour l'interopérabilité. La taille minimum de message requise a été déterminée sur la base de la taille minimum de MTU que les hôtes Internet sont obligés de prendre en charge : 576 octets pour IPv4 [RFC0791] et 1280 octets pour IPv6 [RFC2460]. Les datagrammes qui se conforment à ces limites ont les plus grandes chances d'être livrés parce qu'ils n'exigent pas de fragmentation.

Il est RECOMMANDÉ que les envoyeurs syslog restreignent les tailles de message afin que les datagrammes IP n'excèdent pas la plus petite MTU du réseau utilisé. Cela évite la fragmentation des datagrammes et de possibles problèmes entourant la fragmentation, comme une découverte incorrecte de la MTU.

La fragmentation peut être indésirable parce qu'elle augmente le risque de perte du message juste à cause de la perte d'un fragment du datagramme. Syslog n'a pas de facilité d'accusé de réception, et donc il n'y a pas de moyen efficace de traiter la retransmission. Cela rend impossible à syslog d'utiliser la découverte de la MTU du chemin de couche de mise en paquet [RFC1191]. Quand la MTU du réseau n'est pas connue à l'avance, l'hypothèse la plus sûre est de restreindre les messages à 480 octets pour IPv4 et 1180 octets pour IPv6.

3.3 Accès de source et de cible

Les receveurs Syslog DOIVENT prendre en charge d'accepter les datagrammes Syslog sur l'accès UDP bien connu 514, mais PEUVENT être configurés à écouter sur un accès différent. Les envoyeurs Syslog DOIVENT prendre en charge l'envoi de datagrammes de message Syslog à l'accès UDP 514, mais PEUVENT être configurés à envoyer des messages à un accès différent. Les envoyeurs Syslog PEUVENT utiliser tout accès de source UDP pour transmettre les messages.

3.4 Adresse IP de source

L'adresse IP de source des datagrammes NE DEVRAIT PAS être interprétée comme l'identifiant de l'hôte qui a généré le message syslog. L'entité qui envoie le message syslog pourrait être simplement un relais. Le message syslog lui-même contient l'identifiant du générateur du message.

3.5 Structure UDP/IP

Chaque datagramme UDP/IP envoyé par la couche transport DOIT adhérer complètement à la structure spécifiée dans la [RFC0768] sur UDP et IPv4 [RFC0791] ou IPv6 [RFC2460], selon le protocole utilisé.

3.6 Sommes de contrôle UDP

Les envoyeurs Syslog NE DOIVENT PAS désactiver les sommes de contrôle UDP. Les envoyeurs syslog IPv4 DEVRAIENT utiliser les sommes de contrôle UDP lors de l'envoi des messages. Noter que la [RFC2460] rend obligatoire l'utilisation des sommes de contrôle UDP lors de l'envoi de datagrammes sur IPv6.

Les receveurs Syslog NE DOIVENT PAS désactiver les vérifications de somme de contrôle UDP. Les receveurs syslog IPv4 DEVRAIENT vérifier les sommes de contrôle UDP et DEVRAIENT accepter un message syslog avec une somme de contrôle de zéro. Noter que la [RFC2460] rend obligatoire l'usage de sommes de contrôle pour UDP sur IPv6.

4. Considérations de fiabilité

UDP est un protocole non fiable, à faibles frais généraux. Cette Section discute les questions de fiabilité inhérentes à UDP que les mises en œuvre et les utilisateurs devraient connaître.

4.1 Datagrammes perdus

Cette transposition de transport ne fournit aucun mécanisme pour détecter et corriger la perte des datagrammes. Les datagrammes peuvent être perdus dans le transit par suite d'encombrement, de corruption, ou de tout autre problème intermittent du réseau. La fragmentation IP exacerbe ce problème parce que la perte d'un seul fragment va résulter en l'élimination du message entier.

4.2 Corruption de message

Les datagrammes UDP/IP peuvent être corrompus dans le transit à cause d'erreurs du logiciel, du matériel, ou du réseau . Cette transposition de transport spécifie l'utilisation des sommes de contrôle UDP pour permettre la détection de la corruption en plus des sommes de contrôle utilisées dans IP et les protocoles de couche 2. Cependant, les sommes de contrôle ne garantissent pas la détection de corruption, et cette transposition de transport ne fournit pas de mécanisme d'accusé de réception ou de retransmission de message.

4.3 Contrôle d'encombrement

Parce que syslog peut générer des quantités illimitées de données, transférer ces données sur UDP est généralement problématique, parce que UDP n'a pas de mécanisme de contrôle de l'encombrement. Les mécanismes de contrôle de l'encombrement qui répondent à l'encombrement en réduisant les taux de trafic et en établissant un certain degré d'équité entre les flux qui partagent le même chemin sont vitaux pour le fonctionnement stable de l'Internet [RFC2914]. C'est pourquoi le transport TLS [RFC2425] de syslog est de mise en œuvre EXIGÉE et est RECOMMANDÉ pour une utilisation générale.

Les seuls environnements où le transport syslog UDP PEUT être utilisé comme solution de remplacement au transport TLS sont ceux des réseaux gérés, où le chemin de réseau a été explicitement provisionné pour le trafic UDP syslog à travers des mécanismes d'ingénierie du trafic, comme de limitation de taux ou de réservations de capacités. Dans tous les autres environnements, le transport TLS [RFC2425] DEVRAIT être utilisé.

4.4 Livraison en séquence

Le transport IP utilisé par UDP ne garantit pas que la séquence de livraison de datagrammes va correspondre à l'ordre d'envoi des datagrammes. L'horodatage contenu dans chaque message syslog peut servir comme guide grossier pour établir l'ordre de séquence. Cependant, il ne va pas aider dans les cas où plusieurs messages ont été générés dans le même créneau temporel, où l'envoyeur n'a pas pu générer d'horodatage, ou où des messages sont générés par des hôtes différents dont les horloges ne sont pas synchronisées. L'ordre d'arrivée des message syslog via ce transport NE DEVRAIT PAS être utilisé comme un guide d'autorité pour établir une séquence absolue ou relative des événements sur les hôtes d'envoi syslog.

5. Considérations sur la sécurité

L'utilisation de cette spécification sur un réseau non sécurisé n'est PAS RECOMMANDÉE. Plusieurs considérations sur la sécurité de syslog sont discutées dans la [RFC5424]. Cette section se concentre sur les considérations de sécurité spécifiques du transport syslog sur UDP. Certaines des questions de sécurité soulevées dans cette section peuvent être atténuées par l'utilisation de IPsec comme défini dans la [RFC4301].

5.1 Authentification de l'envoyeur et falsification de message

Cette transposition de transport ne fournit pas de forte authentification de l'envoyeur. Le receveur du message syslog ne va pas être capable d'assurer que le message a bien été envoyé de l'envoyeur rapporté, ou de si le paquet a été envoyé d'un autre appareil. Cela peut aussi conduire à un cas d'erreur d'identité si une machine configurée de façon inappropriée envoie des messages syslog à un receveur en se représentant comme une autre machine.

Cette transposition de transport ne fournit pas de protection contre la falsification de message syslog. Un attaquant peut transmettre des messages syslog (soit à partir de la machine d'où les messages sont délibérément envoyés, soit à partir de toute autre machine) à un receveur.

Dans un cas, un attaquant peut cacher la vraie nature d'une attaque parmi de nombreux autres messages. Par exemple, un attaquant peut commencer à générer des messages falsifiés indiquant un problème sur une machine. Cela peut attirer l'attention des administrateurs du système, qui vont passer leur temps à investiguer le soit-disant problème. Pendant ce temps, l'attaquant pourrait être capable de compromettre une machine différente ou un processus différent sur la même machine.

De plus, un attaquant peut générer de faux messages syslog pour donner de fausses indications sur l'état des systèmes. Par exemple, un attaquant peut arrêter un processus critique sur une machine, qui pourrait générer une notification de sortie. L'attaquant peut ensuite générer une fausse notification que le processus a été redémarré. Les administrateurs du système pourraient accepter cette fausse information et ne pas vérifier que le processus n'a en fait pas été redémarré.

5.2 Observation de message

Cette transposition de transport n'assure pas la confidentialité des messages en transit. Si les messages syslog sont en clair, c'est comme cela qu'ils vont être transférés. Dans la plupart des cas, passer des messages en clair, lisibles par l'homme, est un avantage pour les administrateurs. Malheureusement, un attaquant pourrait aussi être capable d'observer le contenu lisible par l'homme des messages syslog. L'attaquant pourrait alors utiliser les connaissances obtenues de ces messages

pour compromettre une machine. Il est RECOMMANDÉ que des informations non sensibles soient transmises via cette transposition de transport ou que la transmission de telles informations soit restreinte à des réseaux proprement sécurisés.

5.3 Répétition

La falsification et l'observation de messages peuvent être combinées en une attaque en répétition. Un attaquant pourrait enregistrer un ensemble de messages qui indiquent une activité normale d'une machine. Plus tard, un attaquant pourrait retirer cette machine du réseau et répéter les messages syslog avec de nouveaux horodatages. Les administrateurs pourraient ne rien trouver d'anormal dans les messages reçus, et leur réception indiquerait faussement une activité normale de la machine.

5.4 Livraison non fiable

Comme discuté précédemment à la Section 4, les considérations sur la fiabilité, le transport UDP n'est pas fiable, et les paquets qui contiennent les messages de datagrammes syslog peuvent être perdus en transit sans être remarqués. Il peut y avoir des conséquences sur la sécurité à la perte d'un ou plusieurs messages syslog. Les administrateurs pourraient ne pas être informés du développement d'un problème potentiellement sérieux. Des messages pourraient aussi être interceptés et éliminés par un attaquant comme moyen de cacher des activités non autorisées.

5.5 Priorisation et différentiation de message

Cette transposition de transport ne rend pas obligatoire la priorisation des messages syslog sur le réseau ou quand ils sont traités sur l'hôte receveur sur la base de leur sévérité. Sauf si une certaine priorisation est mise en œuvre par l'envoyeur, le receveur, et/ou le réseau, l'implication de sécurité d'un tel comportement est que le receveur syslog ou les appareils du réseau pourraient être submergés par des messages à faible sévérité et être forcés d'éliminer des messages de sévérité potentiellement élevée.

5.6 Déni de service

Un attaquant pourrait submerger un receveur en lui envoyant plus de messages qu'il ne peut en être traité par l'infrastructure ou l'appareil lui-même. Les développeurs DEVRAIENT tenter de fournir des caractéristiques qui minimisent cette menace, comme de restreindre facultativement la réception de messages à un ensemble d'adresses IP de source connues.

6. Considérations relatives à l'IANA

Ce transport utilise l'accès UDP 514 pour syslog, comme enregistré dans le registre des numéros d'accès de l'IANA.

7. Remerciements

L'auteur remercie de leurs contributions Chris Lonvick, Rainer Gerhards, David Harrington, Andrew Ross, Albert Mietus, Bernie Volz, Mickael Graham, Greg Morris, Alexandra Fedorova, Devin Kowatch, Richard Graveman, et tous les autres qui ont commenté les diverses versions de cette proposition.

8. Références

8.1 Références normatives

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980.

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, DOI 10.17487/RFC0791, septembre 1981.

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

(MàJ par RFC8174)

[RFC2425] T. Howes, M. Smith, F. Dawson, "Type de contenu MIME pour informations de répertoire", septembre 1998. *(Obsolète, voir* RFC6350) *(P.S.)*

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2914] S. Floyd, "Principes du contrôle d'encombrement", BCP 41, DOI 10.17487/RFC2914, septembre 2000.

[RFC5424] R. Gerhards, "Le protocole Syslog", mars 2009. (*Remplace la* RFC3164, *P.S.*)

8.2 Références pour information

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", DOI 10.17487/RFC1191, novembre 1990.

[RFC3164] C. Lonvick, "Protocole BSD de Syslog", août 2001. *(Information)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, décembre 2005. *(P.S.) (Remplace la* RFC2401)

Adresse de l'auteur

Anton Okmianski
Cisco Systems, Inc.
595 Burrard St., Suite 2123
Vancouver, BC V7X 1J1
Canada

téléphone : +1-978-936-1612
mél : aokmians@cisco.com