RFC 5426 : Transmission of syslog messages over UDP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 mars 2009

Date de publication du RFC : Mars 2009

https://www.bortzmeyer.org/5426.html

La nouvelle version du protocole syslog offre désormais le choix du protocole de transport. Il y aura un RFC par transport et celui-ci normalise le transport sur UDP.

Le RFC 5424 [1], qui définit la nouvelle version du protocole syslog comporte une innovation : le protocole de transport peut être choisi séparément du format des données transmises. Historiquement, syslog a toujours été transporté sur UDP et notre RFC normalise cette pratique. Le transport UDP est même rendu obligatoire, pour assurer l'interopérabilité.

Le RFC est court, car il y a peu de détails à préciser. Parmi ceux-ci, notons les questions de taille des paquets (section 3.2), où un minimum est imposé (480 octets en IPv4) et où il est recommandé de se tenir à la MTU du lien comme maximum (le maximum théorique étant celui d'UDP, 65535 octets).

Le RFC normalise également le port utilisé (c'est le port historique, 514).

La section 4 détaille les conséquences pour syslog de la nature non-fiable d'UDP. Les paquets syslog transmis sur UDP peuvent donc être perdus et l'application doit en tenir compte. De même, UDP ne fournissant pas de contrôle de congestion, un émetteur syslog doit donc prendre soin de ne pas émettre de messages au maximum de ses capacités.

Enfin, la section 5, consacrée à la sécurité, rappelle l'absence presque complète de sécurité du transport UDP, qui ne protège contre rien, rendant son utilisation à l'extérieur du réseau local très dangereuse.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5424.txt