RFC 5153 : IPFIX Implementation Guidelines

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 juin 2008

Date de publication du RFC : Avril 2008

https://www.bortzmeyer.org/5153.html

Le protocole IPFIX, décrit désormais dans les RFC 7011 [1] et RFC 7012, permet à une machine d'observation (en général un routeur) d'envoyer des résumés sur le trafic observé à une machine de récolte, qui produira ensuite de jolis camemberts. Ce RFC donne des conseils aux programmeurs qui développent des systèmes IPFIX, jusqu'à citer en section 10 une liste des erreurs de mise en œuvre les plus courantes.

C'est donc un document non-normatif (section 2 pour les détails), qui ne remplace pas les RFC qui spécifient le protocole mais qui les complète, si on développe un observateur ou un récolteur IPFIX.

Comme le rappelle la section 1.2, IPFIX fonctionne en envoyant des tuples TLV. Des gabarits ("*Template*") décrivent les données possibles (des gabarits standards sont décrits dans le RFC 7012) et des enregistrements IPFIX ("*Data Record*") contiennent les données elles-mêmes. Les tuples peuvent être envoyés avec plusieurs protocoles de transport, SCTP étant recommandé.

Après ces préliminaires, commencent les conseils aux implémenteurs. La section 3 discute l'implémentation des gabarits. Par exemple, l'exporteur devrait envoyer le gabarit avant les données. Mais, selon le protocole de transport utilisé, le gabarit peut arriver après et le récolteur devrait donc être patient, ne pas jeter immédiatement les données où le "*Template ID*" est inconnu (section 3.1).

Les données envoyées en IPFIX sont typiquement de grande taille et le programmeur doit donc faire attention à la taille des messages envoyés. Il ne faut pas dépasser la MTU en UDP (section 3.5).

La section 4 couvre les responsabilités de l'exporteur. Ainsi, 4.3 lui rappelle de maintenir les compteurs (par exemple le nombre de paquets d'un flot), y compris sur une longue période. S'il risque de ne

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7011.txt

pas en être capable, il doit plutôt utiliser des compteurs différentiels ("*Delta Counter*", section 3.2.3 du RFC 7012). 4.5 se consacre aux enregistrements qui portent l'indication de l'heure et rappelle donc qu'il faut synchroniser ses horloges, par exemple avec NTP.

Ceux qui développent le logiciel du récolteur liront plutôt la section 5 qui leur rappellera, par exemple, que les identificateurs des gabarits ("*Template ID*") ne sont uniques que par exporteur (plus rigoureusement, par "*observation domain*") et qu'il faut donc maintenir une liste par exporteur.

La section 6 est consacrée aux problèmes de transport. Contrairement à beaucoup d'autrs protocoles IETF, où un seul protocole de transport est spécifié, afin de maximiser l'interopérabilité, IPFIX offre un grand choix : UDP, TCP et SCTP, ce dernier étant le seul obligatoire (avec son extension PR du RFC 3758). La section 6.1 justifie ce choix et rappelle quelques conséquences de l'utilisation de SCTP. Par exemple, l'extension PR ("*Partial Reliability*") permet d'envoyer les enregistrements avec différents niveaux de fiabilité (ceux liés à la facturation nécessitant typiquement davantage de soins que ceux de simple statistique).

En revanche, la section 6.2, consacrée à UDP, explique pourquoi ce protocole est dangereux et comment limiter les risques (notamment en ne l'utilisant qu'au sein de réseaux fermés et contrôlés). Cela peut être le cas si on met à jour un système Netflow en IPFIX, puisque Netflow n'utilisait que UDP.

La section 7 est consacrée aux "*middleboxes*", les machines intermédiaires comme les coupe-feux ou les routeurs NAT. Perturbant les flots mesurés, elles entrainent de délicats problèmes pour la mesure, par exemple la nécessité de bien choisir le point exact d'observation (section 7.2). Comme ces intermédiaires peuvent modifier certaines caractéristiques du flot comme le port, l'information transmise par IPFIX peut devenir très variable (section 7.3.3).

La section 8 est dédiée à la sécurité. IPFIX sert souvent à transporter des données sensibles et la section 8.1 rappelle qu'il peut être prudent d'utiliser DTLS ou TLS, afin d'éviter qu'un indiscret ne prenne connaissance des informations.