RFC 7854 : BGP Monitoring Protocol (BMP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 juin 2016

Date de publication du RFC : Juin 2016

https://www.bortzmeyer.org/7854.html

Ce nouveau protocole **BMP** ("*BGP Monitoring Protocol*") va faciliter le travail des administrateurs réseaux qui font du BGP. Il permet d'obtenir sous une forme structurée les tables BGP. Avant, la solution la plus répandue était d'utiliser l'interface en ligne de commande du routeur (`show ip bgp routes` sur un Cisco), et d'analyser le résultat depuis son programme, une méthode qui est très fragile, le format de sortie ayant été conçu pour des humains et pas pour des programmes.

Les tables convoitées sont bien sûr la RIB mais aussi des informations comme les mises à jour de routes reçues. BMP donne accès à une table BGP nommée Adj-RIB-In, « "*Adjacent [peers] Routing Information Base - Incoming*" », définie dans le RFC 4271 [1], section 1.1. Elle stocke les informations brutes (avant les décisions par le routeur) transmises par les pairs BGP.

BMP fonctionne (section 3) en établissant une connexion TCP avec le routeur convoité. Celui-ci envoie ensuite l'information qu'il veut. Il n'y a pas de négociation ou de discussion au début. Dès que la connexion est établie, le routeur transmet. Il envoie d'abord des messages "*Peer Up*" pour chacun de ses pairs, puis des messages "*Route Monitoring*" pour toute sa base de routes (la section 5 les décrit plus en détails). Une fois que c'est fait, le routeur transmet des messages indiquant les changements : "*Route Monitoring*" en cas d'annonce ou de retrait d'une route, "*Peer Up*" ou "*Peer Down*" s'il y a des changements chez les pairs. Autres messages possibles : "*Stats Report*" pour envoyer des statistiques globales (voir les sections 4.8 et 7), "*Initiation*" et "*Termination*" pour les débuts et fins de sessions, "*Route Mirroring*" pour envoyer verbatim les annonces BGP reçues (c'est une vision de plus bas niveau que "*Route Monitoring*" et cela permet, par exemple, d'analyser des annonces BGP syntaxiquement incorrectes, cf. section 6).

Le client BMP ne transmet jamais de message au serveur (au routeur), à tel point que le routeur peut parfaitement fermer la moitié de la connexion TCP, ou mettre sa fenêtre d'envoi à zéro (ou encore, jeter tous les messages qui seraient envoyés). Toute la configuration est dans le routeur.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4271.txt`

Le format des messages est décrit en section 4. C'est du classique. On trouve dans le message un numéro de version (actuellement 1), la longueur du message, le type du message (la liste des types est indiquée plus haut) représentée par un entier (0 pour "*Route Monitoring*", 1 pour "*Stats Report*" (ou " *Statistics Report*" <https://www.rfc-editor.org/errata_search.php?rfc=7854&eid=4722>), etc), puis les données. À noter que le type arrive après la longueur, alors que c'est en général le contraire (encodage TLV).

Pour la plupart des messages BMP, il y aura un second en-tête, rassemblant les informations sur le pair (son adresse IP, son AS, etc).

Les différents paramètres numériques sont désormais stockés dans un registre IANA <https://www.iana.org/assignments/bmp-parameters/bmp-parameters.xml>.

Quelques petits mots sur la sécurité pour finir. Pour économiser ses ressources, le routeur peut évidemment (section 3.2) restreindre l'ensemble des adresses IP autorisées à se connecter en BMP à lui, tout comme il peut limiter le nombre de sessions BMP (par exemple, une au maximum par adresse IP, cinq au total). Il peut aussi y avoir des questions de confidentialité (section 11). Bien sûr, la liste des routes dans la DFZ est publique, mais ce n'est pas forcément le cas des "*peerings*" privés ou de VPN utilisant BGP comme ceux du RFC 4364. Donc, attention à bien restreindre l'accès.

BMP est en cours d'élaboration depuis pas mal de temps déjà. Résultat, des mises en œuvre ont eu le temps d'apparaitre. Wireshark sait analyser le BMP <https://code.wireshark.org/review/#/c/7192/>. Et il existe deux récepteurs (clients) libres, BMPreceiver <https://code.google.com/p/bmpreceiver> et OpenBMP <http://www.openbmp.org/>. Côté serveur (routeur), Cisco et Juniper savent envoyer du BMP.