Faire réaliser des mesures par les sondes Atlas

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 janvier 2013

https://www.bortzmeyer.org/atlas-udm.html

Le réseau des sondes **Atlas**, créé et géré par le RIPE-NCC, couvre l'Europe (et au delà) de petites machines connectées à l'internet et qui effectuent en permanence des mesures diverses, qui servent par exemple de base aux très intéressants articles des RIPE Labs <https://labs.ripe.net/>. Cela permet par exemple de détecter une bogue présente dans beaucoup de routeurs <https://www.bortzmeyer.org/reseau-128.html>. Les Atlas ne savaient faire au début que des mesures commandées par le RIPE-NCC. Depuis quelque temps, les utilisateurs peuvent également commander des mesures selon leur goût, un système connu sous le nom d'**UDM**, "*User-Defined Measurements*" <https://atlas.ripe.net/udm/>.

D'abord, un avertissement, ce système n'est **pas** public. Il est réservé à ceux qui hébergent une sonde Atlas et/ou financent le déploiement de plusieurs sondes. Si vous êtes intéressé par l'hébergement d'une sonde, voyez cet article des RIPE labs <https://labs.ripe.net/Members/dfk/active_measurements/hosting-a-probe-for-active-measurements/> et candidatez <https://atlas.ripe.net/apply/>. Ceci dit, la meilleure solution est en général d'aller à une réunion RIPE et essayer d'obtenir une sonde (pas toujours facile mais j'en ai eu une <https://www.bortzmeyer.org/atlas-yaounde.html>).

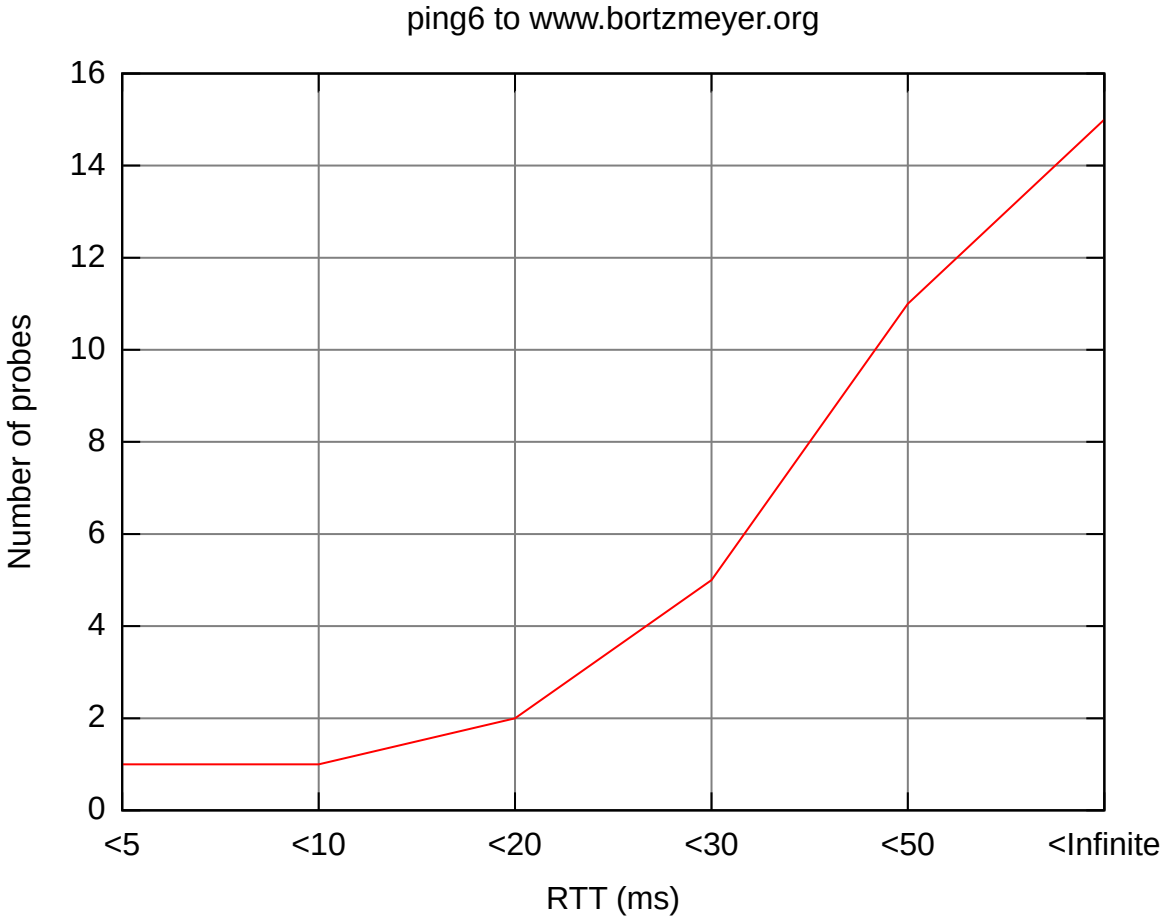
Si vous avez davantage d'argent, l'autre solution est de devenir "*sponsor*" <https://atlas.ripe.net/sponsors>. Vous payez et vous obtenez plein de crédits qui permettent de définir vos propres mesures.

Donc, supposons que vous avez obtenu des crédits, vous avez créé votre compte, passons à la technique. Tout cela étant bien documenté <https://atlas.ripe.net/doc/udm> (voir aussi un excellent tutoriel <http://cnds.eecs.jacobs-university.de/users/nmelnikov/aims2013-ripe-atlas.html>), je vais me contenter de montrer deux cas pratiques. Supposons d'abord que je veuille tester la connectivité IPv6 de mon blog, en pinguant www.bortzmeyer.org. Je clique sur "*New measurement*", et je configure quelques paramètres du test :

Ensuite, j'indique la cible visée, ici www.bortzmeyer.org :

On choisit ensuite l'origine des mesures. On peut indiquer un pays particulier, un AS particulier, une sonde particulière, etc. On choisit aussi le nombre de sondes (évidemment, plus de sondes =¿ plus de crédits consommés). Ici, je choisis d'utiliser 20 sondes, réparties dans le monde entier (les statisticiens noteront que ce n'est pas énorme et qu'il faudra donc interpréter les résultats avec prudence). On n'a plus qu'à sélectionner les heures UTC de début (de mon expérience, elle n'est pas vraiment respectée) et de fin de la mesure (là encore, plus c'est long, plus on consomme de crédits).

On obtient ensuite les résultats. On peut les regarder depuis l'interface Web (sous forme d'un tableau et d'un graphe), ou les récupérer sous la forme d'un fichier JSON, qui est documenté `<https://atlas.ripe.net/doc/data_struct>` mais, bon, rien qu'en lisant le fichier, on devine. Une fois que j'ai récupéré le fichier JSON (si vous voulez une copie (en ligne sur `https://www.bortzmeyer.org/files/atlas-udm-ping6-wwwbortzmeyer.org.json`)...), on peut l'analyser à loisir. Mettons qu'on veuille le nombre cumulé de sondes par intervalle de RTT. On va utiliser un programme Python, (en ligne sur `https://www.bortzmeyer.org/files/atlas-udm-ping6-cumul.py`). Il produit un fichier CSV qu'on demande ensuite à Gnuplot d'afficher : On voit que la majorité des sondes



obtiennent une réponse en moins de 50 milli-secondes.

Testons un deuxième cas avec un autre protocole qu'ICMP, le DNS. Mettons que nous nous intéressions au RTT des requêtes DNS pour un TLD. Prenons `.pf` comme exemple. Il n'a que deux serveurs de noms, tous les deux en Polynésie. Le temps de réponse de ces serveurs est-il suffisant depuis le reste du monde ? On programme une mesure par 15 sondes, posant aux deux serveurs de `.pf` la question `SOA pf.`. On récupère une réponse JSON (copie du fichier (en ligne sur `https://www.bortzmeyer.`

org/files/atlas-udm-dns-ns1manapf.json)) et on l'analyse avec le programme (en ligne sur https://www.bortzmeyer.org/files/atlas-udm-dns-auth.py). Les temps de réponse, pour les deux serveurs, sont :

```
% python atlas-udm-dns-auth.py ns1.mana.pf.json
15 probes

Minimum: 254.4 ms
Maximum: 473.7 ms
Average: 299.7 ms
Median: 280.2 ms

% python atlas-udm-dns-auth.py ns2.mana.pf.json
15 probes

Minimum: 251.2 ms
Maximum: 472.2 ms
Average: 298.7 ms
Median: 272.5 ms
```

Donc, en effet, les temps de réponse sont bien trop élevés (et ce n'est pas un accident sur un petit nombre de sondes anormales, regardez la médiane <https://www.bortzmeyer.org/mediane-et-moyenne.html>).

Dans ce cas, on a juste regardé le temps de réponse, sans voir le contenu. En théorie, le DNS est un espace de nommage unifié et le contenu devrait être le même pour toutes les sondes. Mais, dans un monde de censure, de filtrage et de DNS menteurs <https://www.bortzmeyer.org/dns-menteur.html>, ce n'est pas forcément le cas. En demandant aux sondes de regarder (auprès de leur résolveur par défaut) les adresses IP de search.xxx (moteur de recherche spécialisé dans le porno et étant sous le TLD .xxx qui est parfois filtré), on peut avoir les contenus des réponses DNS, sous une forme brute : uniquement les bits qui passent sur le câble. On utilise DNS Python <https://www.bortzmeyer.org/dnspython.html> pour disséquer ce contenu. Avec une analyse par le programme (en ligne sur https://www.bortzmeyer.org/files/atlas-udm-dns-content.py), on peut trouver une sonde qui ne voit pas le même contenu que les autres :

```
Wrong value at probe XXXXX: ['67.215.65.130'] (previous was ['199.253.28.243', '199.253.28.244'])
```

Et, en effet, l'examen de l'entrée correspondante à ce numéro montre que l'adresse IP du résolveur de cette sonde est celle d'OpenDNS <https://www.bortzmeyer.org/opendns-non-merci.html> qui, par défaut, censure ce qui pourrait choquer les yeux chastes. Le réseau des sondes Atlas peut ainsi être utilisé pour analyser l'effet local de la censure ou du filtrage (comme celui des publicités par Free <https://www.bortzmeyer.org/free-adgate.html>).

Voilà, une dernière chose : vous n'êtes pas obligé de faire des mesures vous-même, il existe des mesures publiques (regardez la première image dans cet article, la case "*Public*" cochée), si elles correspondent à peu près à ce que vous voulez, vous pouvez simplement regarder leurs résultats.

Bonnes mesures !