Utilisation pratique des sondes RIPE Atlas

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Utilisation pratique des sondes RIPE Atlas

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Plan du tutoriel

Il y a peu de plate-formes de mesures de l'Internet

- Les SamKnows de l'Union Européenne
- Grenouille, Netalyzr (logiciel)
- Les sondes privées de boîtes comme Dyn (ex-Renesys)
- Et, bien sûr, chaque opérateur mesure **son** réseau...

L'Atlas

- Un petit boîtier voué aux mesures **actives**. L'Atlas ne voit pas le trafic et ne peut donc pas le mesurer.
- L'Atlas est installée par des volontaires, chez M. Michu, dans un centre de données, au bureau...
- Elles sont gérées centralement par le RIPE-NCC.
- Permettent des UDM (*User-Defined Measurements*). Atlas est un « botnet gentil ».
- `https://atlas.ripe.net/`

Quelques choix et leurs raisons

- Matériel $\longrightarrow$ complet contrôle (par opposition au logiciel tournant sur une machine Windows plein de malwares).
- Centralisé, pour l'authenticité (pas d'attaque Sybil).

Chiffres sur les Atlas

7 juillet 2015

```
14336 probes
8339 connected
        131 anchors
        2510 with working IPv6 (30.1 %) -
             3020 capable of IPv6 (36.2 %))
        2071 (24.8 %) home, 623 (7.5 %) office,
             526 (6.3 %) datacentre,
             15 (0.2 %) mobile, 11 (0.1 %) hackerspace
        3992 with NAT (47.9 %)
```


Atlas par pays ou AS

7 juillet 2015

```
Top countries:
US: 971 (11.6 %)
DE: 892 (10.7 %)
FR: 743 (8.9 %)
GB: 584 (7.0 %)
NL: 458 (5.5 %)
RU: 433 (5.2 %)
CZ: 247 (3.0 %)
IT: 237 (2.8 %)

Top AS:
AS 7922 (COMCAST-7922 - Comcast Cable Communications): 336 (4.0 %)
AS 6830 (LGI-UPC Liberty Global Operations B.V.): 297 (3.6 %)
AS 12322 (PROXAD Free SAS): 234 (2.8 %)
AS 3320 (DTAG Deutsche Telekom AG): 217 (2.6 %)
AS 3215 (AS3215 Orange S.A.): 137 (1.6 %)
AS 9143 (ZIGGO Ziggo B.V.): 89 (1.1 %)
AS 3265 (XS4ALL-NL XS4ALL Internet BV): 87 (1.0 %)
AS 5089 (NTL Virgin Media Limited): 81 (1.0 %)
```

Plan du tutoriel

Les bases

- Il faut un compte RIPE (se crée en ligne)
- Il faut des **crédits**. On les obtient en hébergeant une sonde, ou une ancre ou en étant LIR ou en demandant à un copain ou en étant sponsor du RIPE.
- On a une liste limitative de tests : ping, traceroute, DNS, TLS, HTTP (avec limites), NTP
- Chaque mesure vise **une** machine, la **cible** (*target*)
- Ensuite, c'est intuitif et convivial :-)
  `https://atlas.ripe.net/` Plein d'options disponibles

Mes crédits

ernet Measurements > RIPE Atlas > My Atlas > My Credits

Account Information

This is where you're able to view the history of your credit use. There are visualisations available, and you can also transfer credits to someone else.

27,261,070

22,060.44 credits / hour

History | Charts & Archives | Transfer

Page 1 of 241 › »

Time	Comment	Change	Balance
2015-07-03 08:35 UTC	Administrative: Transfer Administratively transferred after LIR request	+ 1,000,000	27,261,070
2015-07-03 06:16 UTC	Measurement: 2060427 Samples: 1728	- 1,728	26,261,070
2015-07-03 01:02 UTC	Probe ID:10673 Probe uptime	+ 19,395	26,262,798

afnic

Créer une mesure

Create a New Measurement

Step 1 Definitions

Ping measurement to epp.nic.fr

Target: epp.nic.fr
An IP address or hostname

Address Family*: IPv6

Packets: 3

Size: 48

Description: Ping measurement to epp.nic
A free-form description of this measurement

Interval: 240
How often this should be done (seconds between samples). Note that this value is ignored for one-off measurements.

Resolve on Probe:
Force the probe to do DNS resolution

+ Ping | + Traceroute | + DNS | + SSL | + NTP

Step 2 Probe Selection

Worldwide 50

afnic

Mesures uniques ou répétées

- Mesures uniques (*one-off*)
- Mesures répétées périodiquement (attention, cela coûte vite cher en crédits)

Analyser les résultats

- Un outil interactif en ligne, le Sismographe
- Télécharger les résultats bruts (en JSON) et les analyser comme on veut.
- `wget -O 2068624.json https://atlas.ripe.net/api/v1/measurement/2068624/result`

Analyse du JSON avec Sagan

- Sagan est une bibliothèque d'analyse
  `https://atlas.ripe.net/docs/sagan/`
- Automatise une partie des tâches d'analyse

Exemple Sagan

```
from ripe.atlas.sagan import PingResult
import ujson

results = ujson.loads(open("2068624.json").read())

for result in results:
    my_result = PingResult(result)
    print my_result.rtt_median
```

Plan du tutoriel

Déclencher une UDM par l'API

- HTTP + REST + des paramètres en JSON : on ne peut plus simple. Clé d'API à obtenir auprès du site Web.
- Pour apprendre, la doc' ou bien l'option *Measurement API Compatible Specification* dans l'interface Web.
- Permet des expériences reproductibles.

UDM avec curl

```
% curl --dump-header - -H "Content-Type: application/json" \
       -H "Accept: application/json" -X POST -d '{
 "definitions": [
  {
   "target": "whois.nic.fr", "packets": 3, "type": "ping"
  }
 ],
 "probes": [
  {
   "type": "area", "value": "WW", "requested": 50
  }
 ],
 "is_oneoff": true
}' https://atlas.ripe.net/api/v1/measurement/?key=YOUR_KEY_HERE
```

`https://atlas.ripe.net/docs/measurement-creation-api/` pour la doc'

Sélection des sondes

On peut les choisir par :

- Numéro d'AS
- Pays (ou zone géographique comme « Europe »)
- Préfixe IP (en pratique, ne marche pas)
- Manuellement, avec leurs ID
- Reprendre celles d'une précédente mesure

Attention, la sélection n'est pas aléatoire. N'espérez pas de la représentativité.

Si ça se passe mal

Codes de retour HTTP :

- 400 Mauvais paramètres dans le blob JSON, relisez la doc'
- 401 Mauvaise clé d'API

Depuis un langage de programmation

[On utilisera Python pour les exemples.]

```
# https://atlas.ripe.net/docs/measurement-creation-api/
data = { "definitions": [
           { "target": "blog.afnic.fr", "description": "Ping my blog",
           "type": "ping", "af": 6, "is_oneoff": True} ],
         "probes": [
             { "requested": 5, "type": "area", "value": "WW" } ] }
request.add_header("Content-Type", "application/json")
request.add_header("Accept", "application/json")
conn = urllib2.urlopen(request, json.dumps(data))
```

Emballer dans une bibliothèque

```
import RIPEAtlas

data = { "definitions": [
    { "type": "ping", "af": 6, "is_oneoff": True, "packets": 3} ],
         "probes": [
             {"requested": requested, "type": "area", "value": "WW"}] }
measurement = RIPEAtlas.Measurement(data)
results = measurement.results(wait=True)
```

Il existe bien d'autres bibliothèques/outils !

Analyser le JSON

- Simple à faire à la main : des bibliothèques dans tous les langages de programmation.
- Un langage aux structures de données dynamiques est conseillé (Python, Ruby, JavaScript. . .) En C ou en Go, c'est plus pénible.
- Le texte JSON est un (grand) tableau, un élément par sonde, chacun étant un objet JSON.
  `https://atlas.ripe.net/docs/data_struct/`
- Les réponses DNS sont partiellement binaires : une bibliothèque DNS peut être nécessaire.

Scripts utiles

On n'est pas forcé de tout programmer. . . `https://github.com/RIPE-Atlas-Community/ripe-atlas-community-contrib`

Test ICMP

Pour évaluer la joignabilité de votre serveur.

```
%  python reachability+retrieve.py -v -r 50 2001:67c:2218:30::10
{'definitions': [{'target': '2001:67c:2218:30::10', 'af': 6, 'packets': 3, '
Measurement #2068648 to 2001:67c:2218:30::10 uses 50 probes
44 probes reported
Test done at 2015-07-03T09:26:24Z
Tests: 111 successful tests (86.7 %), 2 errors (1.6 %), \
       15 timeouts (11.7 %), average RTT: 114 ms
```

Attention, il faut comparer avec d'autres. Beaucoup d'Atlas ont une connectivité IPv6 pourrie, 10 % est le taux d'échec « normal ».

Test DNS de la censure

```
% python resolve-name.py --country=FR islamic-news.info
Measurement #2068739 for islamic-news.info/A uses 499 probes
[] : 3 occurrences
[90.85.16.52] : 9 occurrences
[213.186.33.5] : 450 occurrences
Test done at 2015-07-03T12:04:25Z
```

90.85.16.52 est le serveur Web du Ministère de l'Intérieur, vers lequel les DNS menteurs doivent rediriger.
`http://www.bortzmeyer.org/censure-francaise.html`

Test DNS de la censure, autre pays

```
% python resolve-name.py --country=CN --requested=30 www.facebook.com
Measurement #1854647 for www.facebook.com/A uses 15 probes
[66.220.158.19] : 4 occurrences
[179.60.192.3] : 2 occurrences
[31.13.79.246] : 3 occurrences
[31.13.68.84] : 3 occurrences
[173.252.74.22] : 1 occurrences
[153.122.20.47] : 2 occurrences
[31.13.68.70] : 3 occurrences
[67.205.10.141] : 1 occurrences
[173.252.73.52] : 1 occurrences
[114.200.196.34] : 1 occurrences
[31.13.76.102] : 1 occurrences
Test done at 2015-02-04T11:11:19Z
```

Plan du tutoriel

Quelques conseils pour les programmeurs

- Programmez de manière défensive : les objets JSON n'ont pas toujours tous les membres documentés.
- Ne supposez pas que tout s'est passé comme demandé. Par exemple, vous pouvez avoir moins de sondes que demandé.

Quelques conseils pour les analystes

- Ne testez pas que pendant un problème : 10 % de perte en IPv6 peut être l'état normal.
- Attention aux limiteurs de trafic (surtout en testant 8.8.8.8).
- Toujours noter l'heure (en UTC, bien sûr). Ça peut marcher à un moment et pas à un autre.

Les ancres

- Des serveurs dédiés à la mesure : peuvent servir d'**amers** pour les sondes Atlas
- 134 ancres au 2 juillet 2015
  `https://atlas.ripe.net/about/anchors/`
- Pinguez sans modération

Test d'une ancre

```
% python reachability+retrieve.py -v -r 50 \
    $(dig +short +nodnssec AAAA us-phx-as53824.anchors.atlas.ripe.net)
    {'definitions': [{'target': '2607:fad0:42:a06:0:1:0:1', 'af': 6,
          'packets': 3, 'type': 'ping', 'is_oneoff': True,
          'description': 'Ping 2607:fad0:42:a06:0:1:0:1'}],
      'probes': [{'requested': 50, 'type': 'area', 'value': 'WW'}]}
Measurement #2068744 to 2607:fad0:42:a06:0:1:0:1 uses 50 probes
45 probes reported
Test done at 2015-07-03T12:09:43Z
Tests: 107 successful tests (82.3 %), 2 errors (1.5 %), \
    21 timeouts (16.2 %), average RTT: 118 ms
```


Supervision

On peut ne récupérer que les dernières mesures, et Atlas met un membre JSON qui indique le nombre de problèmes.

Ici, configuré pour Icinga/Nagios

```
# Atlas https://atlas.ripe.net/docs/status-checks/ https://atlas.ripe.net/mea
define service {
   ...
   service_description Test_Atlas
   check_command check_http!-I atlas.ripe.net  -r 'global_alert":false' \
     --ssl=1 \
     -u /api/v1/status-checks/2060427/?permitted_total_alerts=2
}
```

traceroute

- On peut faire des traceroute depuis les sondes Atlas
- Exemple, test ping, deux sondes timeoutent, on traceroute pour comprendre ce qui leur arrive
- `http://www.bortzmeyer.org/traceroute-atlas.html`

Exemple traceroute

```
% python traceroute.py --probes 10704 -f   217.70.190.232
Measurement #2068768 Traceroute 217.70.190.232 uses 1 probes
1 probes reported
Test done at 2015-07-03T12:44:53Z
From:  107.145.116.99    33363    BHN-TAMPA - BRIGHT HOUSE NETWORKS, LLC,US
Source address:  10.0.1.41
Probe ID:  10704
1    10.0.1.1    None    None    [0.775, 0.517, 0.493]
2    [u'*', u'*', u'*']
3    72.31.195.20    33363    BHN-TAMPA - BRIGHT HOUSE NETWORKS, LLC,US    [
4    71.44.61.10    None    None    [10.808, 13.601, 13.772]
5    72.31.220.136    33363    BHN-TAMPA - BRIGHT HOUSE NETWORKS, LLC,US
6    72.31.188.170    33363    BHN-TAMPA - BRIGHT HOUSE NETWORKS, LLC,US
7    4.68.70.153    3356    LEVEL3 - Level 3 Communications, Inc.,US    [13.
8    4.69.134.106    3356    LEVEL3 - Level 3 Communications, Inc.,US    [44
9    4.59.246.114    3356    LEVEL3 - Level 3 Communications, Inc.,US    [39
10    217.70.176.229    29169    GANDI-AS GANDI SAS,FR    [113.353, 113.738,
11    217.70.176.182    29169    GANDI-AS GANDI SAS,FR    [158.308, 113.603,
12    [u'*', u'*', u'*']
13    [u'*', u'*', u'*']
...
```

DNSmon

`https://atlas.ripe.net/dnsmon/` Supervision de zones DNS importantes par les sondes Atlas. À noter que le JSON peut être récupéré si vous voulez faire des analyses vous-même.

Utile pour surveiller les SLA (*Service Level Agreements*) :

```
Serveur;Version IP;Protocole;Nombre de sondes;Nombre de mesures;\
  Disponibilite moyenne;RTT moyen;RTT median;Mesure Atlas
d.nic.fr;IPv4;UDP;47;402954;99.70;63.64;26.47;1413662
d.nic.fr;IPv6;UDP;47;402955;99.82;62.62;23.53;1413670
```

[Mais prudence : une panne n'est pas forcément du fait de la cible.]

Et HTTP ?

- Non trivial : risque de DoS, petite requête mais grosse réponse, risques politiques si une sonde en Arabie Saoudite accède au site Web de Charlie Hebdo.
- Prévu pour l'automne 2015 avec cette restriction :
  - Uniquement vers les ancres

Étiquettes

- Les sondes ont des étiquettes (*tags*)
- Certaines sont attribuées automatiquement (`system-ipv6-works`, `system-ipv4-rfc1918`)
- D'autres manuellement par les utilisateurs (`home`, `fibre`)
- On peut sélectionner les sondes ainsi (seulement cette étiquette, pas cette étiquette)

Élimination des maillons faibles

En utilisant les étiquettes

```
% python reachability+retrieve.py -r 100 -v -t 1 2001:67c:2218:30::10
Tests: 73 successful tests (80.2 %), 1 errors (1.1 %), \
    17 timeouts (18.7 %), average RTT: 82 ms
```

```
% python reachability+retrieve.py -r 100 -v -t 1 \
          --exclude home,ipv6-tunnel --include system-ipv6-works   2001:67c
Tests: 96 successful tests (96.0 %), 0 errors (0.0 %), \
          4 timeouts (4.0 %), average RTT: 73 ms
```

Plan du tutoriel

À vous de jouer

- Hébergez des sondes Atlas. Gros manques en Chine et en Inde : `https://labs.ripe.net/Members/emileaben/improving-ripe-atlas-coverage-what-networks-are-missing`
- Hébergez une ancre
- Développez du code et partagez-le
- Faites des mesures et partagez les résultats (par exemple en `https://labs.ripe.net/`)