

Nouvelle version de Zonecheck, la 2.1

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 février 2010

<https://www.bortzmeyer.org/zonecheck-2-1.html>

Le 12 février, une nouvelle version de Zonecheck <<http://www.zonecheck.fr/>> a été publiée <<http://lists.gnu.org/archive/html/zonecheck-announce/2010-02/msg00000.html>>.

Écrit en Ruby, Zonecheck <<http://www.zonecheck.fr/>> est un logiciel de test de la configuration d'une zone DNS, pour voir si elle est correctement installée sur les serveurs de noms. Cette vérification nécessiterait à la main des dizaines d'appels à la commande dig, pour s'assurer que tout est correct. Zonecheck automatise le tout. D'une manière générale, tester doit être fait avec un logiciel car c'est une opération longue et fastidieuse, qu'un humain a peu de chances de mener jusqu'au bout correctement.

Ainsi, je peux voir si mes serveurs de noms sont tous bons :

```
% zonecheck bortzmeyer.org
ZONE : bortzmeyer.org.
NS <= : a.dns.gandi.net. [217.70.179.40]
NS    : c.dns.gandi.net. [217.70.182.20]
NS    : b.dns.gandi.net. [217.70.184.40]

-----|
~~~~ |  avertissement  | | ~~~~~
-----|

a> Les serveurs de nom font tous partie du même AS
| Conseil: ZoneCheck
| Afin d'éviter de perdre la connectivité avec les serveurs DNS
| autoritaires en cas de problèmes de routage dans le Système Autonome,
| il est conseillé d'héberger les serveurs sur différents AS.
|-----|
| : Tous les serveurs de noms font partie du même Système Autonome (AS
| : numéro 29169), essayez d'en héberger certains sur un autre.
| .....|
=> générique

...
==> SUCCÈS (mais 5 avertissement(s))
```

D'autres zones ne sont pas aussi correctes :

```
% zonecheck zataz.com
ZONE : zataz.com.
NS <= : ns1.eurodns.com. [80.92.65.2]
NS      : ns2.eurodns.com. [80.92.67.140]
...

-----
| fatal |
-----

f> [TEST enregistrement MX peut être résolu]: le domaine n'existe pas (IN/ANY: mailing.zataz.com.)
=> ns1.eurodns.com./80.92.65.2

==> ÉCHEC (et 1 avertissement(s))
```

Et, en effet, le serveur de courrier désigné n'existe pas :

```
% dig @ns1.eurodns.com MX zataz.com
...
;; ANSWER SECTION:
zataz.com.          3600    IN      MX      10 mail.zataz.com.
zataz.com.          3600    IN      MX      20 mailing.zataz.com.
...

% dig @ns1.eurodns.com A mailing.zataz.com
...
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49758
```

À noter que Zonecheck sépare la **politique** (quels tests on fait et un résultat positif est-il obligatoire) du moteur de tests qui les applique. L'administrateur système peut éditer le profil des tests et retirer (ou rendre facultatif) certains tests, à volonté. Par exemple, par défaut, Zonecheck teste que les adresses IP des serveurs de noms ne sont pas des "bogons" mais, s'ils le sont, cela ne produit qu'un simple avertissement :

```
<check name="ip_bogon" severity="w" category="ip"/>
```

Si on trouve ce test trop laxiste, il suffit de changer `severity` de 'w' ("warning") à 'f' ("fatal"). Si, à l'inverse, on trouve ce test inutile ou tout simplement trop coûteux en ressources, on peut le désactiver complètement en retirant l'élément `<check>` du profil. C'est une caractéristique unique parmi les logiciels de tests DNS.

Zonecheck est un logiciel libre sous licence GPL. Comme d'autres logiciels libres, son histoire a connu des moments de désintérêt (voir le long délai qui s'était écoulé depuis la version précédente) et de « résurrection ». Merci à Fabien Chabanne pour avoir pris en charge cette nouvelle version, et à Stéphane d'Alu pour le programme original.