

La panne des serveurs DNS d'Oleane

Stéphane Bortzmeyer

21 février 2016

La panne des serveurs DNS d'Oleane

Cet article documente mes observations sur la panne des serveurs DNS d'Oleane du 19 février 2016. En fait, c'est surtout un *prétexte* pour avoir un article pour montrer les possibilités des différentes versions de Markdown, pour la publication des RFC sur l'enregistrement du type MIME `text/markdown`. (« prétexte » est mis en évidence, selon une syntaxe qui marche depuis le Markdown originel.)

Le texte au début (après les pour-cents) est vu comme du commentaire par certains Markdown, comme des *métadonnées* par d'autres (Pandoc) et considéré comme du texte à passer tel quel par d'autres (comme le Markdown originel, CommonMark ou GitHub).

Récit

Le début de la panne a eu lieu vers 1415 UTC. Les serveurs `ns{0,1,2,3,4,5,6}.oleane.net` ne répondent plus aux requêtes DNS en UDP ou TCP (RST).

Vers 1520 UTC, certains des serveurs ont commencé à répondre à nouveau, vers 1530 UTC, tout était revenu.

Conséquences

Les nombreux domaines dont tous les serveurs de noms étaient en `oleane.net` (comme `ladepeche.fr` ou `defense.gouv.fr`) ne fonctionnent plus du tout. Vu avec (cette syntaxe pour les liens marche depuis le Markdown originel) [check_soa](#) :

```
% check-soa -i --ns 'ns0.oleane.net ns1.oleane.net' ville-brignoles.fr
ns0.oleane.net.
194.2.0.30: ERROR: read udp 194.2.0.30:53: connection refused
```

```

ns1.oleane.net.
    194.2.0.60: ERROR: read udp 194.2.0.60:53: connection refused

% ping -c 3 ns0.oleane.net
PING ns0.oleane.net (194.2.0.30) 56(84) bytes of data.
64 bytes from ns0.oleane.net (194.2.0.30): icmp_seq=1 ttl=53 time=9.04 ms
64 bytes from ns0.oleane.net (194.2.0.30): icmp_seq=2 ttl=53 time=7.67 ms
64 bytes from ns0.oleane.net (194.2.0.30): icmp_seq=3 ttl=53 time=8.00 ms

--- ns0.oleane.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 23043ms
rtt min/avg/max/mdev = 7.676/8.241/9.044/0.592 ms

% date -u
Fri Feb 19 14:52:57 UTC 2016

% telnet ns0.oleane.net 53
Trying 194.2.0.30...
telnet: Unable to connect to remote host: Connection refused

% check-soa -i --ns 'ns4.oleane.net ns5.oleane.net' defense.gouv.fr
ns4.oleane.net.
    194.2.0.4: ERROR: read udp 194.2.0.4:53: connection refused
ns5.oleane.net.
    194.2.0.5: ERROR: read udp 194.2.0.5:53: connection refused

```

Ces apostrophes inverses pour marquer du code n'étaient pas dans le Markdown originel, qui utilisait une indentation du texte (peu pratique, encore que le Control-C > d'Emacs aide bien) comme dans l'exemple suivant. La première technique permet de mettre le nom du langage, pour les Markdown qui font de la beautification du code (Github, par exemple).

Et, après le redémarrage :

```

% date -u
Fri Feb 19 15:29:24 UTC 2016

% check-soa -i defense.gouv.fr
ns4.oleane.net.
    194.2.0.4: OK: 2015042281 (9 ms)
ns5.oleane.net.
    194.2.0.5: OK: 2015042281 (9 ms)

```

Analyse

- Les serveurs répondaient (ICMP et TCP RST). Ils répondaient vite et systématiquement, alors qu'il n'y avait jamais aucune réponse DNS. Ce n'est donc pas un problème électrique (qui aurait éteint les machines) ni un problème de routage.
- Il y avait toujours une réponse ICMP donc ce ne ressemble pas à une attaque par déni de service volumétrique (où on aurait eu parfois des réponses).
- Le plus probable est donc qu'une erreur d'administration système a stoppé les serveurs DNS sur toutes ces machines.

(La syntaxe des listes est également une fonction du Markdown originel.)

Conclusion

Comme le note l'[observatoire de la résilience de l'Internet français](#) :

La dispersion des serveurs DNS dans des AS différents [en France] reste donc toujours faible avec la majeure partie des zones ayant tous leurs serveurs au sein d'un unique AS.

C'était le cas ici : ces zones mettaient « tous leurs œufs dans le même panier » et une seule panne pouvait donc tout arrêter.

Au passage, cette façon de faire des citations existe depuis le Markdown originel.

Annexe : traitement Markdown

Avec le Markdown originel de Gruber (téléchargé en <http://daringfireball.net/projects/downloads/Markdown>)

Notez au passage que certains programmes transforment automatiquement l'URL ci-dessus en lien hypertexte.

```
% perl ~/Downloads/Markdown_1.0.1/Markdown.pl panne-dns-oleane-2016.md
<h1>La panne des serveurs DNS d'Oleane</h1>
...
```

Avec Pandoc¹ (notez la note de base de page, syntaxe **spécifique à Pandoc**) :

¹Une des particularités importantes de Pandoc est sa capacité à produire bien d'autres formats que le HTML.

```
% pandoc --to html panne-dns-oleane-2016.md
<h1 id="la-panne-des-serveurs-dns-doleane">La panne des serveurs DNS d'Oleane</h1>
...
```

Avec Discount :

```
% markdown panne-dns-oleane-2016.md
<h1>La panne des serveurs DNS d'Oleane</h1>
...
```

Avec la mise en œuvre de référence de [CommonMark](#) :

```
% cmark panne-dns-oleane-2016.md
<h1>La panne des serveurs DNS d'Oleane</h1>
...
```

Le script à copier-coller pour re-générer les fichiers en cas de modification² :

```
pandoc --to html --output panne-dns-oleane-2016.html panne-dns-oleane-2016.md
pandoc --to latex --latex-engine=xelatex --output panne-dns-oleane-2016.pdf panne-dns-oleane-2016.md
```

²Pensez aussi à mettre à jour le Gist