

# Grande panne du domaine allemand .DE

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 Mai 2010. Dernière mise à jour le 17 Mai 2010

<http://www.bortzmeyer.org/point-de-en-panne.html>

---

De environ 1130 UTC à 1315 UTC, le TLD allemand, .DE a été en panne presque complète.

On peut voir le résultat en interrogeant successivement les serveurs DNS faisant autorité, avec dig :

```
% for ns in $(dig +short NS de.); do
  echo $ns
  dig @$ns A google.de
done

f.nic.de ... NOERROR
z.nic.de ... NXDOMAIN
s.de.net ... NOERROR
a.nic.de ... NXDOMAIN
c.de.net ... NOERROR
l.de.net ... NXDOMAIN
```

Dans l'exemple ci-dessus, trois (ce sont parfois deux) serveurs de noms de DENIC répondent que le domaine `google.de` n'existe pas (NXDOMAIN)... (À noter qu'il y avait eu une présentation de l'infrastructure technique de DENIC à la réunion OARC de Prague <[https://www.dns-oarc.net/files/workshop-201005/DENICnewSetup\\_OARC2010.pdf](https://www.dns-oarc.net/files/workshop-201005/DENICnewSetup_OARC2010.pdf)> quelques jours avant la panne.)

Le problème affectait les domaines dont le nom commence par les lettres F à Z (`facebook.de` marchait encore mais pas `ford.de`). Cela laisse donc à penser que le générateur de zones qui fabrique le fichier à partir de la base de données a stoppé en plein milieu de son travail... (L'analyse de DENIC <<http://www.denic.de/en/denic-in-dialogue/news/2733.html>>, publiée ultérieurement, indique que le générateur de zones a bien fonctionné mais que c'est la copie du fichier de zone vers les serveurs qui avait été interrompue en route.) Cela ressemble donc beaucoup, mais en moins radical (une partie de la base était toujours là) à la panne qui avait affecté .SE <<http://www.bortzmeyer.org/panne-de-point-se.html>> et aussi à la grande panne de .COM en 1997 <<http://www.merit.edu/mail.archives/nanog/1997-07/msg00539.html>>.

Donc, `denic.de`, `bund.de` (le gouvernement) ou `bild.de` marchaient, alors que `google.de`, `tageszeitung.de` ou `heise.de` avaient le problème.

Avec un script plus compliqué et qui fait plus de tests :

```
for domain in bild bund denic facebook ford google heise tageszeitung; do
  for ns in $(dig +short NS de.); do
    echo $ns
    dig @$ns A $domain.de
  done
done
```

On obtient ce résultat (en ligne sur <http://www.bortzmeyer.org/files/point-de-panne-12-mai-1300.txt>) (vu au moment où la panne était en cours de réparation, seul un serveur avait encore le problème).

Ce genre de pannes est-elle évitable ? Elle n'est pas due à une défaillance matérielle des serveurs (le DNS est très robuste face à ce genre de problèmes) mais à une bogue, qui a affecté les données. Éviter ce type de pannes nécessiterait donc d'écrire du logiciel sans bogue... J'ai lu sur un forum de neuneus l'opinion comme quoi il faudrait s'inspirer des méthodes de la NASA et faire écrire deux logiciels différents par deux équipes différentes, puis comparer les résultats avant publication. Cette approche est utilisée dans certains logiciels (par exemple le logiciel de gestion de DNSSEC, OpenDNSSEC <<http://www.opendnssec.org/>>, a un auditeur, un vérificateur de la zone signée, écrit par un auteur différent, dans un langage de programmation différent) mais elle n'est pas généralisable, pour de bêtes questions de coût. On ne peut pas à la fois vouloir des noms de domaine toujours moins cher, exiger toujours plus de nouvelles fonctions chez le registre et demander qu'on fasse de la sécurité de luxe.

Je recommande la lecture du premier rapport de DENIC <<http://www.denic.de/en/denic-in-dialogue/news/2733.html>>, qui inclut une analyse technique. Pour ceux qui aiment les graphes, Heise online a publié un graphique montrant la chute de trafic <<http://www.heise.de/ix/meldung/Raetselraten-um-den.html?view=zoom;zoom=1>> due à la panne. Par contre, je n'ai pas trouvé pour l'instant d'article intéressant en français ou en anglais sur cette affaire et certains sont même pleins d'erreurs (comme <<http://cert.lexsi.com/weblog/index.php/2010/05/12/385-panne-internet-geante-en-allemande-et-> qui ajoutait .at à la panne - ce que personne n'a vu mais ils ont corrigé depuis - ou comme <<http://www.tld.sc/en/2010/05/what-went-wrong-at-the-de-registry-earlier-today/>> qui prétendait - cela a été corrigé depuis - que tous les noms avaient disparus - signe qu'il n'ont pas testé avant d'écrire - , qui invente des soi-disant pannes de .biz et .nu - que personne ne semble avoir remarqué - et qui prétendait à tort que DENIC n'utilise que BIND alors que la moitié de leurs serveurs sont des nsd). Dans la langue de Karl Liebknecht, vous pouvez consulter « *"DNS-Fehler legen Domain .de lahm"* <<http://www.heise.de/newsticker/meldung/DNS-Fehler-legen-Domain-de-lahm-3-Update-999068.html>> », sur l'excellent Heise online.