# Un site Web multi-serveur multi-organisations sans trop de travail

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 mars 2020

https://www.bortzmeyer.org/miroir-web-dns.html

---

Je viens de configurer un site Web qui est composé de plusieurs serveurs gérés par plusieurs personnes. Cet article est juste un partage d'expérience pour raconter quelques techniques utiles pour ce genre de service.

Le problème de départ était de distribuer certaines des ressources pédagogiques disponibles sur le site du CNED malgré la surcharge de leur serveur, qui était souvent inaccessible <https://www.numerama.com/politique/611438-coronavirus-les-sites-scolaires-tombent-face-a-laffluence.html>. Caroline De Haas avait copié les fichiers <https://twitter.com/carolinedehaas/status/1239615279484874761>, il restait à les héberger. Il fallait aller vite (ces ressources étaient utiles aux parents d'élèves pendant la phase de confinement) et que cela ne soit pas trop cher puisque c'était fait par des volontaires. D'un autre côté, contrairement à ce qu'essaient de vous faire croire les ESN, simplement distribuer des fichiers statiques ne nécessite pas beaucoup de travail, et il n'y a pas besoin d'un serveur costaud. Pour des raisons aussi bien techniques (répartir la charge) que politiques (je trouve plus sympas les projets collectifs), le service devait être réparti sur plusieurs machines. On n'a évidemment pas manqué de volontaires <https://mastodon.gougere.fr/@bortzmeyer/103837697320848188> et, rapidement, de nombreuses machines étaient disponibles. Reste à coordonner tout cela.

Le cahier des charges était que le service devait être disponible pour des utilisateurs ordinaires. Donc, du Web classique, pas de BitTorrent (qui aurait sans doute été mieux adapté à ce travail) et encore moins d'IPFS (très joli mais franchement difficile à gérer). Donc, juste un URL à connaitre, http://ressources-pedagogiques.org/. Pour réaliser un tel service, on peut faire passer toutes les requêtes HTTP par un répartiteur de charge (facile à réaliser, par exemple avec nginx) et envoyer ensuite aux différents serveurs. Problèmes, le répartiteur de charge est un SPOF, et cela n'est pas forcément efficace de rajouter systématiquement un intermédaire. Des solutions de plus haute technologie étaient possibles, à base d'"*anycast*" BGP, par exemple, mais pas accessibles à un groupe de volontaires sans moyens particuliers.

La solution choisie était donc de compter sur le DNS. On met les adresses de tous les serveurs dans le DNS et c'est le client DNS qui assure une répartition (plus ou moins raisonnable) du trafic. C'est loin d'être optimal mais c'est très simple, très robuste (presque aucun SPOF) et accessible à tous.

Le domaine `ressources-pedagogiques.org` est installé sur plusieurs serveurs DNS <`https://dns.bortzmeyer.org/ressources-pedagogiques.org/NS`>. Chaque fois qu'un serveur est configuré, je le teste et je l'ajoute à la zone. Le nom a actuellement 32 adresses IP <`https://dns.bortzmeyer.org/ressources-pedagogiques.org`>. Si vous utilisez dig, vous pouvez les afficher (ou bien se servir du "*DNS looking glass*", en suivant le lien précédent) :

```
% dig +bufsize=4096 AAAA ressources-pedagogiques.org

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> AAAA ressources-pedagogiques.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31490
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
ressources-pedagogiques.org. 6168 IN AAAA 2a03:7220:8080:f00::1
ressources-pedagogiques.org. 6168 IN AAAA 2a01:cb19:815f:cb00:f6b5:20ff:fe1b:bec3
ressources-pedagogiques.org. 6168 IN AAAA 2a01:cb08:89a3:b900:21e:6ff:fe42:2565
ressources-pedagogiques.org. 6168 IN AAAA 2a01:4f9:4a:1fd8::26
ressources-pedagogiques.org. 6168 IN AAAA 2a01:4f8:1c1c:42c9::1
ressources-pedagogiques.org. 6168 IN AAAA 2605:4500:2:245b::42
ressources-pedagogiques.org. 6168 IN AAAA 2001:4b98:dc0:43:216:3eff:fec4:c1a7
ressources-pedagogiques.org. 6168 IN AAAA 2001:41d0:a:f4b4::1
ressources-pedagogiques.org. 6168 IN AAAA 2001:41d0:a:1370::1
ressources-pedagogiques.org. 6168 IN AAAA 2001:bc8:47b0:723::1
ressources-pedagogiques.org. 6168 IN AAAA 2001:bc8:4400:2400::5327
ressources-pedagogiques.org. 6168 IN AAAA 2001:67c:288:32::38
ressources-pedagogiques.org. 6168 IN AAAA 2001:470:1f13:2f:0:ff:fe01:500

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Mar 22 15:33:41 CET 2020
;; MSG SIZE  rcvd: 443
```

(Et refaire la manipulation pour les adresses IPv4.)

Pour se synchroniser, les serveurs s'alimentent sur un site de référence, `https://source.ressources-pedago` (ce nom, lui, ne pointe que vers une seule machine), typiquement en rsync (la documentation pour les gérants des serveurs miroir est sur le site <`https://source.ressources-pedagogiques.org/`>.)

Voilà, c'est tout simple et ça marche. Mais il existe quelques pièges. Le premier est celui de la vérification des miroirs. Dans un tel service, géré par des personnes variées, il peut y avoir des miroirs mal configurés, qui tombent en panne, ou bien qui ne se synchronisent plus. Il est donc crucial de les tester, avant la mise en service, puis de temps en temps. J'utilise pour cela un petit script shell, `check.sh`, qui récupère les noms dans le DNS et appelle curl pour tester :

```
% ./check.sh
2001:470:1f13:2f:0:ff:fe01:500 failed
%
```

Ici, il y avait un problème de routage vers une adresse, et tous les autres serveurs sont corrects. Si vous lisez le script, l'option la plus intéressante de curl est `--connect-to`, qui permet de tester spécifiquement chaque serveur (il ne suffit pas de tester le service général.) Notez que Marc Chantreux a développé une version améliorée de ce script, .

Une version légèrement différente du script me permet de tester un nouveau serveur lorsqu'on me le signale, :

---

`https://www.bortzmeyer.org/miroir-web-dns.html`

```
...
Connected to 2605:4500:2:245b::42 (2605:4500:2:245b::42) port 80 (#0)
> GET /ressources/CP/5CPM9TEWB0016_CahierDeBord_Presentation.pdf HTTP/1.1
> Host: ressources-pedagogiques.org
> User-Agent: ressources-pedagogiques.org checker
...
< HTTP/1.1 200 OK
< Content-Length: 262219
< Content-Type: application/pdf
...
```

Tester que les serveurs marchent est une chose, il est également bon de vérifier qu'ils sont à jour. Le script de mise à jour du serveur de référence `source.ressources-pedagogiques.org` met la date dans un fichier, qu'on peut récupérer pour voir si tous les serveurs ont la même (ils lancent typiquement rsync depuis cron) :

```
% ./updates.sh
2a03:7220:8080:f00::1 : 2020-03-20 13:47:37+00:00
2a01:cb19:815f:cb00:f6b5:20ff:fe1b:bec3 : 2020-03-20 13:47:37+00:00
2a01:cb08:89a3:b900:21e:6ff:fe42:2565 : 2020-03-20 13:47:37+00:00
2a01:4f9:4a:1fd8::26 : 2020-03-20 13:47:37+00:00
2a01:4f8:1c1c:42c9::1 : 2020-03-20 13:47:37+00:00
2605:4500:2:245b::42 : 2020-03-20 13:47:37+00:00
2001:4b98:dc0:43:216:3eff:fec4:c1a7 : 2020-03-20 13:47:37+00:00
2001:41d0:a:f4b4::1 : 2020-03-20 13:47:37+00:00
2001:41d0:a:1370::1 : 2020-03-20 13:47:37+00:00
2001:bc8:47b0:723::1 : 2020-03-20 13:47:37+00:00
2001:bc8:4400:2400::5327 : 2020-03-20 13:47:37+00:00
2001:67c:288:32::38 : 2020-03-20 13:47:37+00:00
2001:470:1f13:2f:0:ff:fe01:500 : ERROR 000
204.62.14.153 : 2020-03-20 13:47:37+00:00
195.154.172.222 : 2020-03-20 13:47:37+00:00
185.230.78.228 : 2020-03-20 13:47:37+00:00
185.34.32.38 : 2020-03-20 13:47:37+00:00
163.172.222.36 : 2020-03-20 13:47:37+00:00
163.172.175.248 : 2020-03-20 13:47:37+00:00
159.69.80.58 : 2020-03-20 13:47:37+00:00
95.217.83.231 : 2020-03-20 13:47:37+00:00
92.243.17.60 : 2020-03-20 13:47:37+00:00
91.224.149.235 : 2020-03-20 13:47:37+00:00
91.224.148.15 : 2020-03-20 13:47:37+00:00
86.250.18.250 : 2020-03-20 13:47:37+00:00
83.205.2.135 : 2020-03-20 13:47:37+00:00
62.210.124.111 : 2020-03-20 13:47:37+00:00
51.255.9.60 : 2020-03-20 13:47:37+00:00
51.15.229.92 : 2020-03-20 13:47:37+00:00
37.187.123.180 : 2020-03-20 13:47:37+00:00
37.187.19.112 : 2020-03-20 13:47:37+00:00
5.135.190.125 : 2020-03-20 13:47:37+00:00
```

Une telle configuration ne permet pas facilement de mettre du HTTPS sur le service : il faudrait distribuer la clé privée à tous les miroirs. À noter également que l'utilisation d'un nom de domaine unique permet à chaque gérant de miroir d'avoir une chance d'obtenir un certificat (et, en effet, j'ai vu dans le journal passer le vérificateur de Let's Encrypt.)

Autre sujet de réflexion : la vie privée. Personne n'a la main sur tous les serveurs du service, il faut donc faire confiance à chaque gérant de miroir pour respecter les principes de protection des données (pas trop de données dans le journal, et ne pas trop les garder.)

---

Pourrait-on ajouter des miroirs ? Il y a un léger problème technique avec des limites DNS. Il y a l'ancienne limite de 512 octets (qui n'est normalement plus d'actualité depuis longtemps ; notez qu'en IPv6, avec DNSSEC, on a déjà dépassé cette vieille limite.) Il y a la limite plus significative de 1 500 octets (la MTU d'Ethernet.) Mais, surtout, il est plus difficile d'assurer la qualité, notamment de la synchronisation, avec beaucoup de machines. Il faut tester, prendre contact avec les administrateurs des serveurs, relancer, etc.

---

https://www.bortzmeyer.org/miroir-web-dns.html