Fonctionnement du DNS

Fonctionnement du DNS

9 septembre 2013

Stéphane **Bortzmeyer**
stephane+dns@bortzmeyer.org

Sans rapport

File Edit View History Delicious Bookmarks Tools Help

C... | 1024px-... | Potamoc... | Nom de ... | ietf dnso... | Large bo... | Free Trial | PiHub – ... | Pourquoi... | Pota... | Linode - ...

www.potamochère.fr

reveal.js

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline | Resize | Tools | View Source | Options

Potamochère

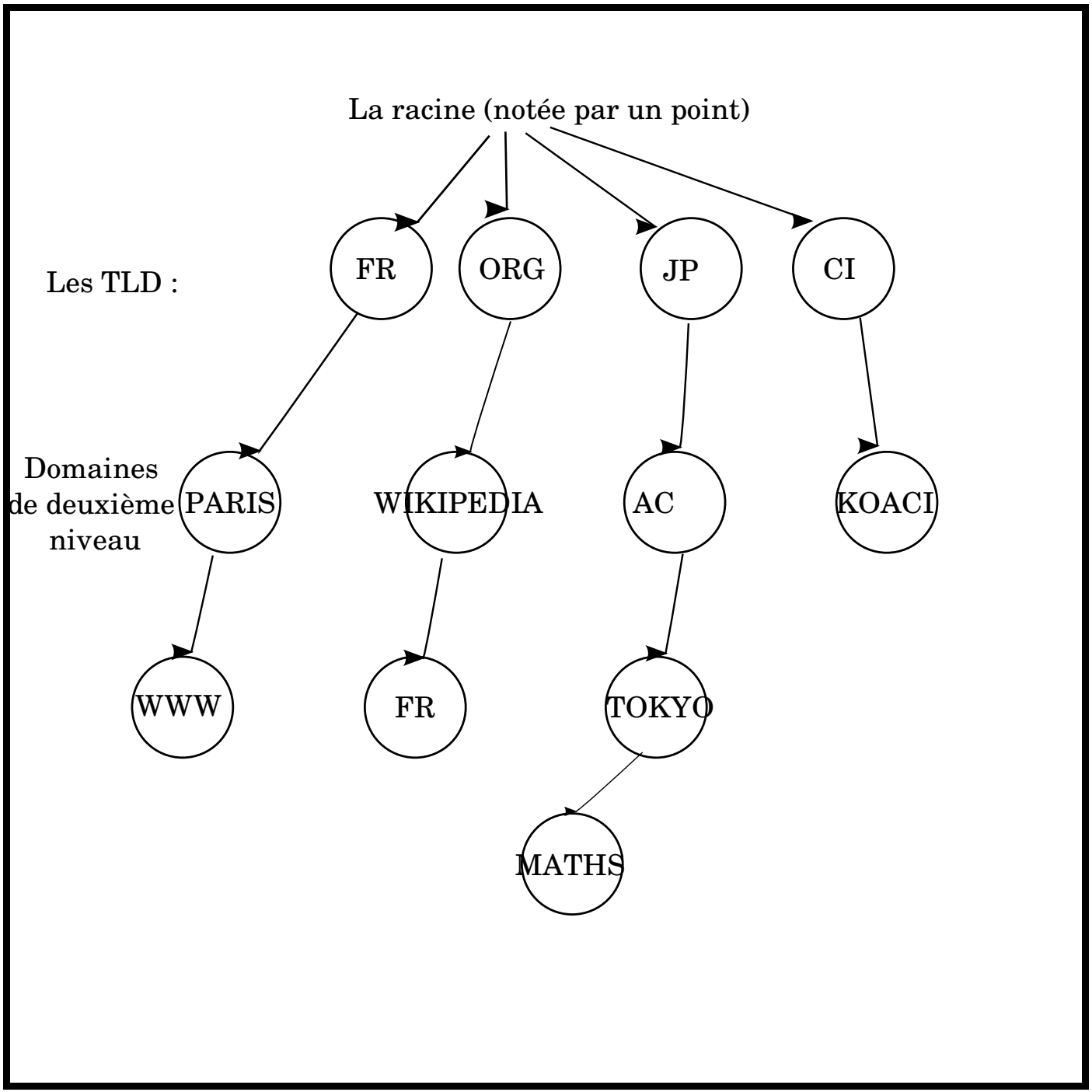
C’est quoi, le DNS ?

1. Une technologie d'*infrastructure* : indispensable mais invisible.
2. Une base de données répartie et décentralisée,
3. Qui associe des données à des *noms de domaine*.

D’abord, les noms de domaine

1. Des noms uniques et mémorisables (`tyrion.lannister.got`),
2. Un vecteur d'identité,
3. Un nommage arborescent : racine, puis TLD (*Top-Level Domain*) puis domaine de deuxième niveau, de troisième niveau et ainsi de suite,
4. Le nombre de composants dans un nom est quelconque (2, 3, 4... ; mais 1 pose quelques problèmes).

Arborescence


La racine (notée par un point)
Les TLD :
FR
ORG
JP
CI
Domaines de deuxième niveau
PARIS
WIKIPEDIA
AC
KOACI
WWW
FR
TOKYO
MATHS

À quoi ça sert ?

`www.bortzmeyer.org` contre `2605:4500:2:245b::42`

1. Stabilité des noms (par rapport aux adresses IP),
2. Noms plus jolis que les adresses.

Et si je suis persan ?

Comment peut-on être persan ?

Non, sérieusement, le cas est prévu

الوكالة - التونسية - للانترنت . تونس ou கேரேஜ் . சிங்கப்பூர்

sont des noms de domaine valides (technique dite « IDN » ou « noms de domaine en Unicode »)

Et si je veux .truc, .machin ou .chose ?

On peut toujours configurer des serveurs pour des TLD bidons.

Mais ils ne seront utilisable que depuis peu de réseaux.

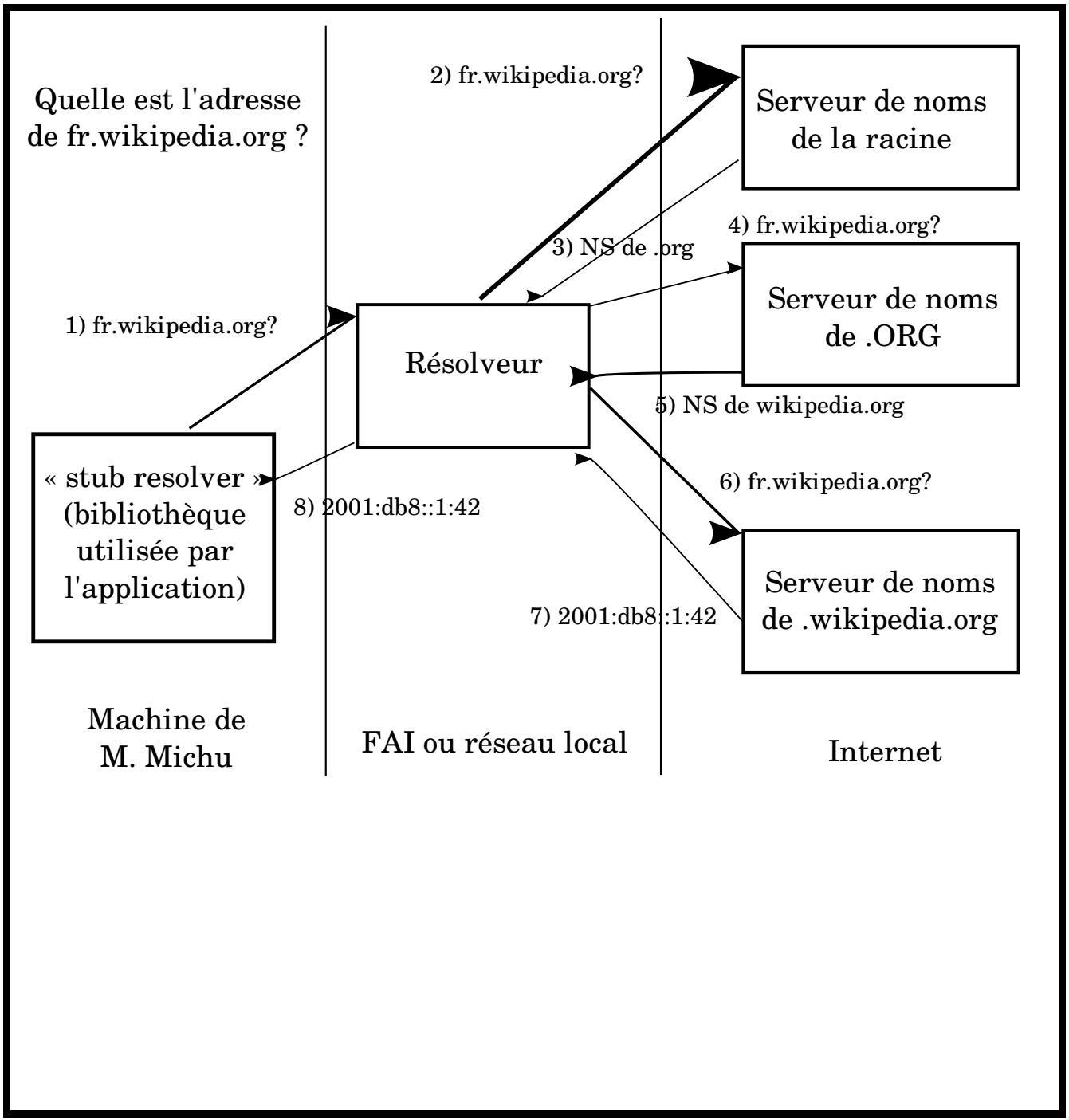
Un projet sympa (mais sans intérêt pratique) : **.42**.

Nommage et protocole

- Les *noms de domaine* : des identificateurs
- Le *DNS* : un protocole réseau pour résoudre ces noms en données

Le DNS n'est qu'une des techniques possibles. Les noms de domaine lui survivront sans doute.

Résolution


Quelle est l'adresse de fr.wikipedia.org ?
2) fr.wikipedia.org?
Serveur de noms de la racine
4) fr.wikipedia.org?
3) NS de .org
Serveur de noms de .ORG
1) fr.wikipedia.org?
Résolveur
5) NS de wikipedia.org
« stub resolver » (bibliothèque utilisée par l'application)
6) fr.wikipedia.org?
8) 2001:db8::1:42
Serveur de noms de .wikipedia.org
7) 2001:db8::1:42
Machine de M. Michu
FAI ou réseau local
Internet

Vocabulaire important

- *Serveur faisant autorité* : serveur DNS qui connait le contenu d'un domaine. Exemple : les serveurs de l'AFNIC qui connaissent ce qu'il y a dans `.fr` et peuvent répondre. Ou les serveurs de `lacantine.org` (chez Bearstech)
- *Résolveur* ou serveur récursif : serveur DNS qui ne connait rien mais pose des questions aux serveurs faisant autorité et mémorise les réponses. Chez le FAI, ou sur le réseau local ou chez Google.

Avec dig

```
% dig AAAA www.bortzmeyer.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11397
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1
...
;; ANSWER SECTION:
www.bortzmeyer.org.  10791  IN  AAAA  2605:4500:2:245b::42
...
;; Query time: 2937 msec
;; SERVER: 192.168.10.110#53(192.168.10.110)
;; WHEN: Wed Aug 14 17:46:47 2013
;; MSG SIZE  rcvd: 164
```

Les serveurs

```
% check-soa -i fr
d.ext.nic.fr.
        192.5.4.2: OK: 2222295704 (47 ms)
        2001:500:2e::2: OK: 2222295704 (62 ms)
d.nic.fr.
        194.0.9.1: OK: 2222295704 (27 ms)
        2001:678:c::1: OK: 2222295704 (29 ms)
e.ext.nic.fr.
        193.176.144.22: OK: 2222295704 (50 ms)
        2a00:d78:0:102:193:176:144:22: OK: 2222295704 (106 ms)
f.ext.nic.fr.
        194.146.106.46: OK: 2222295704 (48 ms)
        2001:67c:1010:11::53: OK: 2222295704 (68 ms)
g.ext.nic.fr.
        194.0.36.1: OK: 2222295704 (50 ms)
        2001:678:4c::1: OK: 2222295704 (81 ms)
```

Où sont les serveurs ?

Un peu partout (notamment grâce à l'anycast).

Des centaines de sites physiques pour la racine, par exemple.

Sécurité

Cf. **exposé à la Journée du Conseil Scientifique AFNIC** de juillet 2012

- Risques autour de l'enregistrement (détournement, saisie, justice privée),
- Risques techniques de panne (assurer la résilience),
- Risques techniques de sécurité (attaques par empoisonnement). Déploiement de DNSSEC.

Empoisonnement

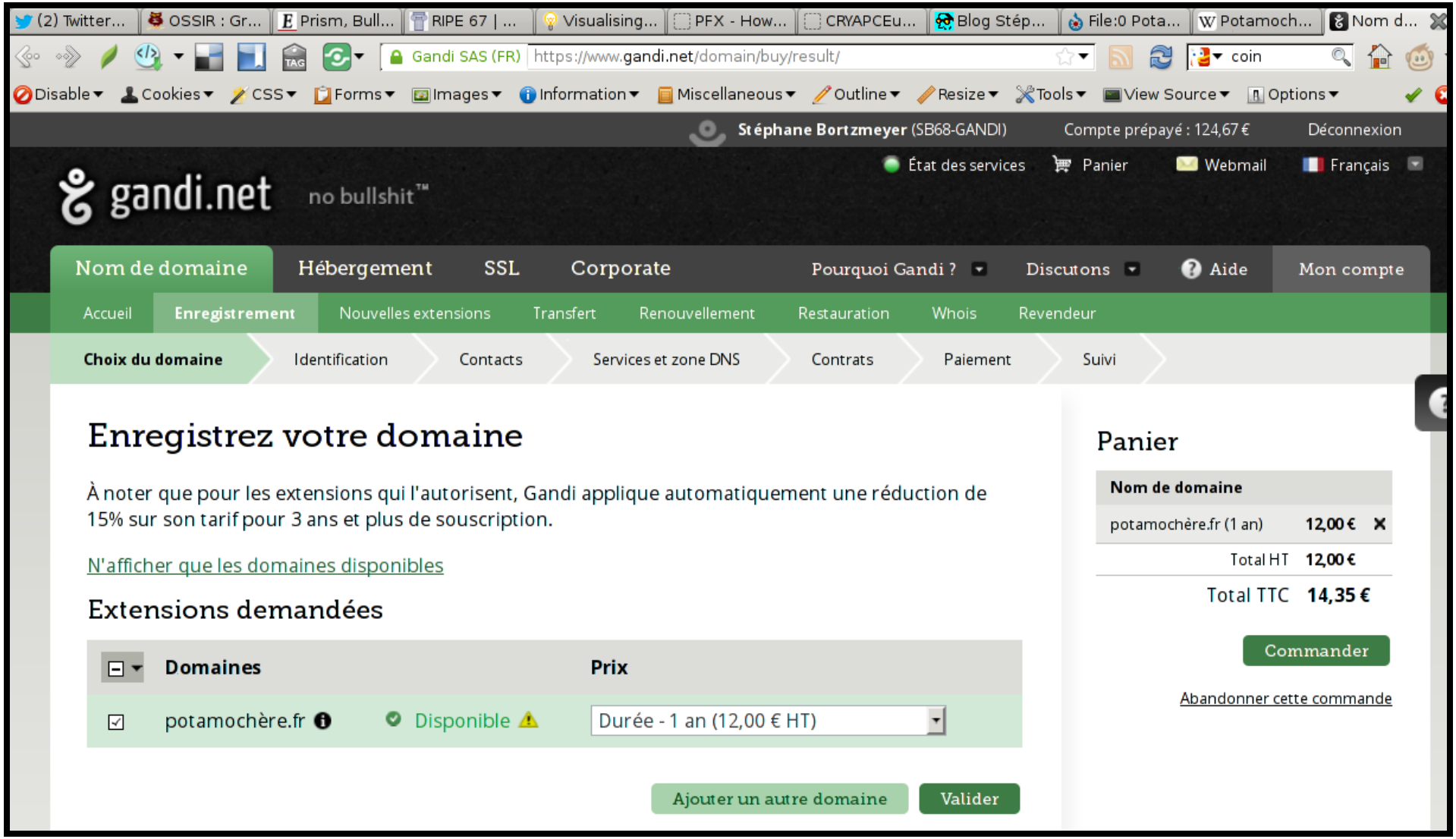
Réponse envoyée par le méchant *avant* celle du serveur faisant autorité.

Peut être acceptée dans certains cas.

DNSSEC

1. Signature cryptographique des enregistrements,
2. Permettant de vérifier leur authenticité.
3. Mais attention ! Cela nécessite une administration DNS bien plus rigoureuse.
4. En cours de déploiement.

Achat


(2) Twitter...
OSSIR : Gr...
Prism, Bull...
RIPE 67 | ...
Visualising...
PFX - How...
CRYAPCEu...
Blog Stép...
File:0 Pota...
Potamoch...
Nom d...
Gandi SAS (FR)
https://www.gandi.net/domain/buy/result/
coin
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
Stéphane Bortzmeyer (SB68-GANDI)
Compte prépayé : 124,67 €
Déconnexion
État des services
Panier
Webmail
Français
gandi.net
no bullshit™
Nom de domaine
Hébergement
SSL
Corporate
Pourquoi Gandi ?
Discutons
Aide
Mon compte
Accueil
Enregistrement
Nouvelles extensions
Transfert
Renouvellement
Restauration
Whois
Revendeur
Choix du domaine
Identification
Contacts
Services et zone DNS
Contrats
Paiement
Suivi
Enregistrez votre domaine
À noter que pour les extensions qui l'autorisent, Gandi applique automatiquement une réduction de 15% sur son tarif pour 3 ans et plus de souscription.
N'afficher que les domaines disponibles
Extensions demandées
Domaines
Prix
potamochère.fr
Disponible
Durée - 1 an (12,00 € HT)
Ajouter un autre domaine
Valider
Panier
Nom de domaine
potamochère.fr (1 an)
12,00 €
Total HT
12,00 €
Total TTC
14,35 €
Commander
Abandonner cette commande

Registres et Bureaux d'Enregistrement

Pour la plupart des TLD, vous devez passer par un intermédiaire, le Bureau d'Enregistrement (BE)

Dans le cas de `potamochère.fr`, Gandi -> AFNIC.

Gouvernance

Qui dirige ? Eux ?

Gouvernance

Ou eux ?

Les organisations et leurs pouvoirs

Relations subtiles et processus mous

- Gouvernement des États-Unis (a mis la main sur la racine **en 1998**),
- ICANN (par délégation du précédent),
- Registres de TLD (**Verisign**, **AFNIC**, **Afilias**, etc), et BE
- Opérateurs de résolveurs (résolveurs menteurs de certains FAI, blocage des pubs Google par Free),
- Auteurs de logiciels (permettent DNSSEC ou pas).

Alternatives

« Nous vous rappellons qu'il existe d'autres possibilités »

Mais pas de miracles : les alternatives ont
aussi leurs inconvénients.

- Identificateurs fondés sur le contenu comme les magnets de BitTorrent
- Identificateurs fondés sur la cryptographie comme ceux de BitMessage

Le financement

Qui paie pour toute cette infrastructure ?

L'essentiel est financé par les titulaires qui enregistrent des noms et paient pour cela.

La racine est financée... de manière diverse.

Conclusion

1. Une technologie indispensable : rien sur l'Internet ne marche sans le DNS
2. De multiples questions non répondues depuis des années (sécurité, stabilité, financement, gouvernance)
3. Techniquement, un des plus grands succès de l'Internet et des réseaux informatiques
4. Politiquement, un sujet de contentieux qui durera sans doute longtemps

Un peu de technique

Pour ceux qui ne sont pas encore morts...

Quels logiciels utiliser et comment les configurer ?

BIND

Sans doute le serveur DNS le plus répandu.

Peut faire serveur faisant autorité *ou* résolveur.

```
 # Le plus simple résolveur
acl me {
                2001:db8:43::/48;
};
options {
        recursion yes;
        allow-recursion   { mynetwork; };
        allow-query-cache { mynetwork; };
        allow-query { mynetwork; };
};
```

BIND

```
 # Le plus simple serveur faisant autorité
# Pour le TLD "example"
options {
        recursion no;
};
zone "example" {
        type master;
        file "example";
};
```

Et le fichier `example` contient les données.

Données

```
@       IN      SOA     ns1.nic root@nic (
                2013071800              ; Serial
                7200            ; Refresh
                1800            ; Retry
                2419200         ; Expire
                600 )   ; Negative Cache TTL

@       IN      NS      ns1.nic.example.
        IN      NS      ns1.pch.net.

www     IN    AAAA   2001:db8::bad:dcaf
```

NSD

Serveur faisant autorité pour plusieurs gros TLD (et la racine)

```
zone:
        name: "example"
        zonefile: "example"
```

Unbound

Résolveur

```
server:
  interface: ::0
  interface: 0.0.0.0
  access-control: 2001:db8:43::/48 allow
```