Noms de domaines et DNS

Ce cours est distribué gratuitement sous licence CC BY-NC-SA 4.0 par Thibaud FRICHET - formation.tfrichet.fr

Prérequis :

- Fondamentaux réseaux : adressage IP, ports, etc.

- Noms de domaine
- Protocole DNS
- Certification et registars
- DynDNS : Dynamic DNS

Noms de domaine

Introduction

Un nom de domaine est une adresse lisible par l'humain, traduisant une adresse IP. Quelques exemples : `tfrichet.fr`, `formation.tfrichet.fr`, etc.

```
sh-5.2$ ping tfrichet.fr -c 2
PING tfrichet.fr (51.68.45.52) 56(84) octets de données.
64 octets de infra.tfrichet.fr (51.68.45.52) : icmp_seq=1 ttl=48 temps=15.5 ms
64 octets de infra.tfrichet.fr (51.68.45.52) : icmp_seq=2 ttl=48 temps=15.7 ms

--- statistiques ping tfrichet.fr ---
2 paquets transmis, 2 reçus, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 15.469/15.575/15.682/0.106 ms
sh-5.2$
sh-5.2$ ping formation.tfrichet.fr -c 2
PING formation.tfrichet.fr (51.68.45.52) 56(84) octets de données.
64 octets de infra.tfrichet.fr (51.68.45.52) : icmp_seq=1 ttl=48 temps=16.8 ms
64 octets de infra.tfrichet.fr (51.68.45.52) : icmp_seq=2 ttl=48 temps=15.5 ms

--- statistiques ping formation.tfrichet.fr ---
2 paquets transmis, 2 reçus, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 15.539/16.192/16.846/0.653 ms
```

ccTLD et gTLD

ccTLD : extensions de pays

Les `country-code Top-Level Domain` ou `ccTLD` sont gérés par des registres nationaux (par exemple l'Afnic pour la France) et sont toujours composés de **2 lettres.**

Quelques exemples : `.fr` (France), `.us` (États-Unis), `.de` (Allemagne)

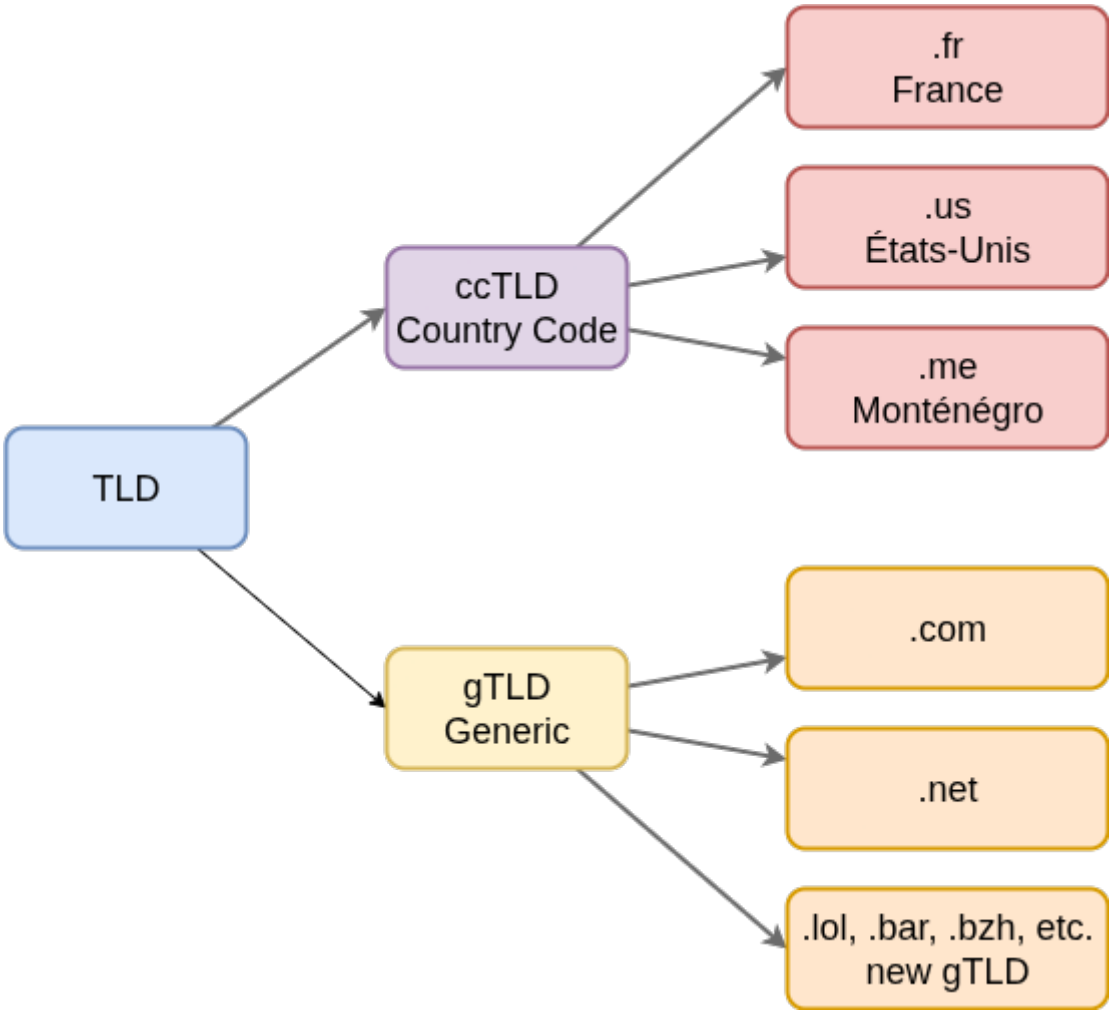
Voir la liste complète sur : https://fr.wikipedia.org/wiki/ISO_3166-1#Table_de_codage

gTLD : extensions génériques

Les `gTLD` pour `generic Top-Level Domain` sont composés de **3 lettres ou plus** : `.com`, `.org`, `.net`.

- Gérés par des **registres accrédités par l'ICANN**.

- Peuvent être ouverts, ciblés ou semi-fermés.
- Inclus les `new gTLD` depuis 2013 : `.paris`, `.info`, `.tech`, `.space`, etc.



Autorités de gestion

ICANN

Internet Corporation for Assigned Names and Numbers

- **Statut :** Organisation internationale à but non lucratif.
- **Mission :** Coordonne les "identifiants uniques" d'Internet (noms de domaine, adresses IP, protocoles).
- **Autorité :** Supervise la gestion globale du système des noms de domaine (DNS) et attribue l'autorité aux registres nationaux pour chaque extension.
- **Enjeux :** Garantit la stabilité, la sécurité et l'unicité d'Internet à l'échelle mondiale.

AFNIC

Association Française pour le Nommage Internet en Coopération

- **Statut :** Association loi 1901, missionnée par l'État.
- **Mission :** Gère les noms de domaine et extensions françaises : `.fr`, `.re`, `.pm`, `.yt`, `.wf`, `.tf`
- **Autorité :** Délégation de l'ICANN et de l'État français pour administrer les noms de domaine nationaux.
- **Enjeux :** Propose un Internet fiable et accessible pour les acteurs français.

> En résumé, l'ICANN régule le système mondial des noms de domaine, alors que l'AFNIC administre principalement les domaines français sous la supervision et la délégation de l'ICANN et des autorités françaises.

Quelques règles

ccTLD

- Chaque pays définit ses propres règles.
- L'ICANN n'a **aucune autorité** sur les ccTLD.
- Les ccTLD dépendent de la législation de leur pays.

> Attention à l'usage détourné, par exemple : `.tv` (Tuvalu), `.me` (Monténégro), `.co` (Colombie).

Attribution des gTLD

Il existe plusieurs types de gTLD : **ouverts**, **ciblés** ou **semi-fermés**.

gTLD ouverts

Ce sont des extensions de domaine accessibles à tous, sans restriction particulière. Exemples : `.com`, `.net`, `.info`, `.org`, etc.

Tout le monde peut enregistrer un domaine sous ces gTLD, particuliers comme entreprises, sans justifier d'une activité ou un statut.

gTLD ciblés

Ce sont des extensions liées à un thème, une profession, une activité ou une communauté.

Elles sont soumises à des règles d'attribution plus ou moins strictes et sont ouvertes à l'ensemble des acteurs liés à ce thème, parfois avec des restrictions modérées (auto-déclaration ou preuve d'activité).

Exemples :

- `.bank` (réservé aux institutions bancaires)
- `.pharmacy` (réservé aux pharmacies)
- `.museum` (réservé aux musées)

gTLD semi fermés

Ces extensions ne sont accessibles qu'à certaines organisations avec des conditions d’attribution strictes.

Exemples :

- `.aero` : industrie aéronautique
- `.bnpparibas`
- `.sony`
- `.gov` : administration américaine

Protocole DNS

Le **DNS** (Domain Name System) est un système hiérarchique et distribué permettant de résoudre les noms de domaine en adresses IP.

Caractéristiques

- **Port :** `UDP 53` `TCP 53`
- **Propagation DNS :** Lorsqu'un enregistrement est modifié, la mise à jour peut prendre de quelques minutes à 48 heures selon le `TTL` défini.
- **Serveurs racine :** 13 ensembles de serveurs (A à M) qui orientent les requêtes vers les serveurs de domaine de premier niveau (TLD) comme `.com`, `.fr`, etc.

Serveurs DNS : FAI et alternatifs

Les FAI proposent leurs propres serveurs DNS à leurs abonnés.
Ces serveurs sont souvent configurés automatiquement sur les box ou routeurs.

Si ils sont généralement à proximité géographique de l'abonné, ils peuvent parfois être filtrés ou limités.

> Un DNS menteur fournit volontairement de fausses informations de résolution de noms de domaine, par exemple pour bloquer l'accès à certains sites ou rediriger vers des pages spécifiques.
> Ce type de manipulation est utilisé par des FAI ou des gouvernements pour censurer ou filtrer le contenu en ligne.

Il existe des serveurs DNS alternatifs, tels que **Google DNS** `8.8.8.8`, **Cloudflare** `1.1.1.1`, **Quad9** `9.9.9.9`, etc.

Zone DNS

Une **zone DNS** contient les enregistrements associés à un domaine ou un sous-domaine. Elle est gérée par un serveur faisant autorité.

Champs principaux

Type	Description	Exemple
A	Associe un nom de domaine à une adresse IPv4	`formation.tfrichet.fr. IN A 51.68.45.52`
AAAA	Associe un nom de domaine à une adresse IPv6	`starwars.com. IN AAAA 2600:1408:c400:e::17cd:6a08`
CNAME	Alias d'un autre nom de domaine	`www.tfrichet.fr. IN CNAME tfrichet.fr.`
TXT	Texte libre, souvent utilisé pour SPF ou autre (vérification Google par exemple)	
NS	Serveurs DNS faisant autorité	`tfrichet.fr. IN NS dns12.ovh.net.`

Champs emails

Type	Description	Exemple
MX	Serveurs de messagerie	`example.com. IN MX 10 mail.example.com.`
SPF	Spécifie les serveurs autorisés à envoyer des emails	`TXT "v=spf1 a: include:_spf.protonmail.ch ~all"`
DKIM	Clé publique pour la signature des emails	`default._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIIB..."`
DMARC	Politique de traitement des emails non conformes	`_dmarc.example.com. IN TXT "v=DMARC1; p=reject; rua=mailto:dmarc@example.com"`

> Voir la liste complète :
> https://help.ovhcloud.com/csm/fr-dns-zone-records?id=kb_article_view&sysparm_article=KB0063452

Certification et registars

Certification

Les échanges sur Internet sont sécurisés à l'aide du chiffrement : HTTPS, VPN, SSH, etc.

Cette sécurité repose sur des certificats. Un certificat comprend :

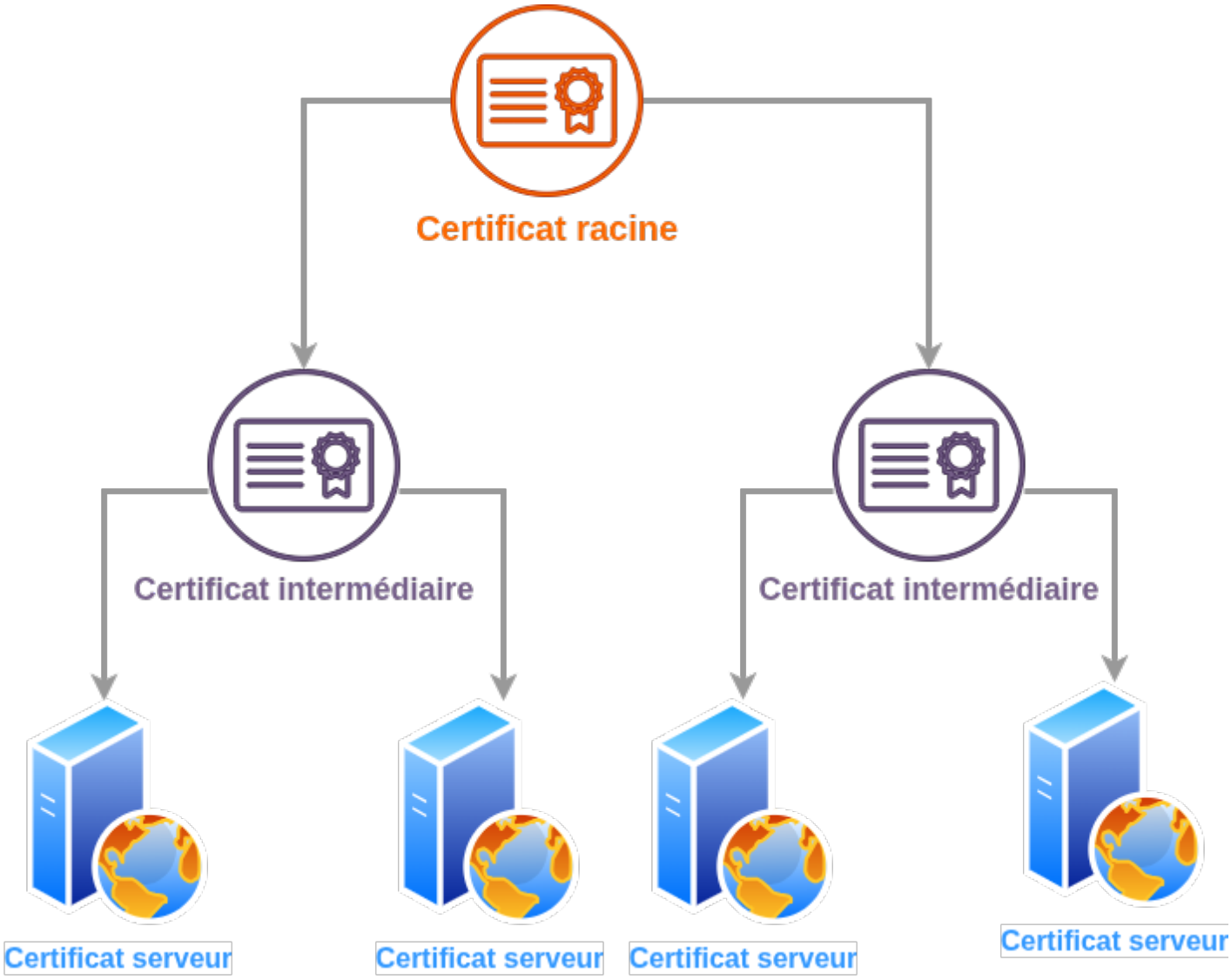
- Le nom de domaine
- La clé publique du serveur
- Sa période de validité
- La signature d'une autorité de certification (CA)

> La signature de l'autorité de certification est cruciale : elle prouve que le certificat provient d'une entité de confiance reconnue par les navigateurs.

Chaîne de délégation

La confiance dans un certificat repose sur une chaîne de certification.

Celle-ci commence par une autorité racine, dont le certificat est auto-signé et intégré dans les systèmes d'exploitation et navigateurs. Cette autorité racine délègue ensuite la signature des certificats à des autorités intermédiaires, qui émettent les certificats utilisés par les sites web.



Ce modèle permet de limiter les risques : en cas de compromission d'une autorité intermédiaire, il est possible de la révoquer sans affecter l'ensemble de l'écosystème.

La création ou le renouvellement d'un certificat racine est une opération hautement sensible qui nécessite des conditions de sécurité physique et logique très strictes. Généralement, les clés cryptographiques sont transportées de manière sécurisée et générées dans un environnement fermé, blindé et isolé du réseau.
Plusieurs témoins sont présents tout au long du processus afin de garantir la traçabilité et la transparence des opérations.

> Ce niveau de précaution est indispensable car la compromission d'une autorité racine mettrait en danger la confiance de l'ensemble des connexions sécurisées sur Internet.

Voir article dédié chez Cloudflare :

https://www.cloudflare.com/fr-fr/learning/dns/dnssec/root-signing-ceremony/

Letsencrypt

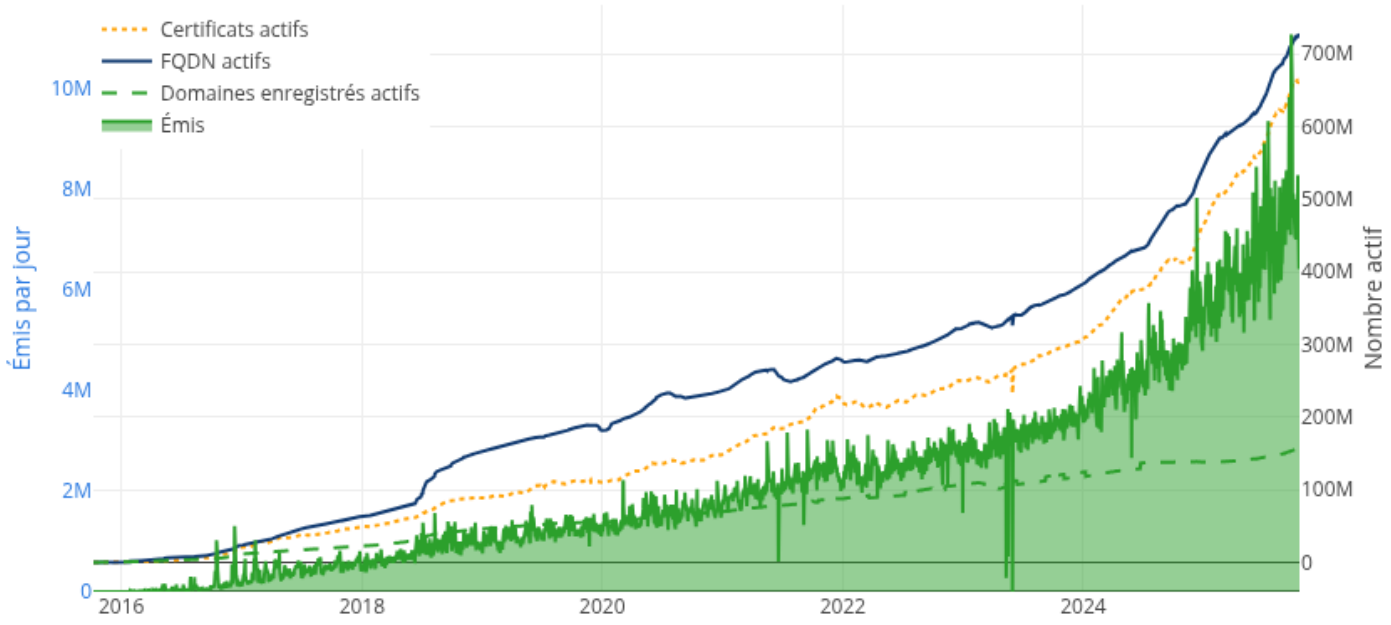
Lancée en 2015 par l'**Internet Security Research Group,** Let's Encrypt est une autorité de certification gratuite, automatisée et ouverte.

Son objectif est de démocratiser l'usage du HTTPS en **supprimant les barrières techniques et financières**.

Les certificats émis par Let's Encrypt sont reconnus par les navigateurs, car l'autorité est signée par une chaîne de confiance incluant l'autorité racine ISRG Root X1.

La popularité de Letsencrypt est incontestable.

https://letsencrypt.org/fr/stats-dashboard/



Registars français

Registar	Volumétrie
OVHCloud	~ 5 millions de domaines
LWS	~ 800k domaines
Gandi	~2,5 millions de domaines (2019)

Registar	Volumétrie
Netim	-
Scaleway (Illiad)	-
O2switch	~ 500k domaines
Ikoula	-

DynDNS : Dynamic DNS

DynDNS (pour Dynamic DNS) est un service qui permet d'associer un nom de domaine à une adresse IP qui peut changer fréquemment.

Il est principalement utilisé pour permettre l'accès distant à des services hébergés derrière des adresses **IP publiques dynamiques** (caméra, NAS, serveur web, etc.).

Par exemple, les adresses IP attribuées par des FAI peuvent changer régulièrement.

Fonctionnement

1. Un nom de domaine dynamique est créé via un fournisseur DynDNS.
2. Un client DynDNS (sur un routeur, NAS, PC, etc.) vérifie périodiquement l'adresse IP publique.
3. À chaque changement d'IP, le client envoie la nouvelle IP au service DynDNS.
4. Le fournisseur DynDNS met à jour l’adresse DNS : le nom de domaine pointe toujours sur l'IP à jour.
5. Depuis l'extérieur, le service est toujours accessible, même après un changement d'IP.

> La plupart des hébergeurs et registars proposent un service de DynDNS.

Exemple de configuration

Gestion des accès et des sous-domaines chez OVH :

Noms de domaine / tfrichet.fr / DynHost

tfrichet.fr

Roadmap & Changelog | Actions

Informations générales | Zone DNS | Serveurs DNS | Redirection | DynHost | GLUE | DS Records

DynHOST vous permet de faire pointer un sous-domaine vers une adresse IP dynamique qui sera mise à jour dans votre zone DNS à chaque changement de celle-ci.

Ajouter un DynHost

Gérer les accès

Recherche DynHost

DynHost	Cible
test.tfrichet.fr	93.1

Guides

DynHost

« ‹ 1 › »

100 | Page 1 / 1

Client DynDNS sur un NAS Synology :

