Fiche savoirs : le service DNS

Le protocole de résolution de noms de domaine DNS

La communication sur un réseau local ou sur Internet nécessite d'utiliser des adresses IP pour pouvoir communiquer. Il est cependant plus facile d'utiliser des noms que des adresses IP.

Le système **DNS (Domain Name System)** permet :

- d'établir la **correspondance** entre un **nom pleinement qualifié (FQDN)** et un enregistrement (le plus souvent une **adresse IP**).
- à des hôtes du réseau de **soumettre des requêtes** à un **serveur DNS récursif** pour obtenir l'adresse IP d'un hôte.

Exemple : le site web www.ac-limoges.fr est associé à l'adresse IP 152.195.34.53.

Cette traduction des noms en adresses IP doit toujours être réalisée puisque que seule l'adresse IP permet de communiquer sur le réseau.

- Le terme employé pour la traduction d'un nom DNS FQDN en adresse IP est celui de **résolution** de nom DNS,
- Le terme employé pour déterminer l'adresse IP assodiée à un nom DNS FQDN en adresse IP est celui de **résolution inverse** de l'adresse IP.

Arborescence DNS

Le système DNS est un modèle en **arborescence hiérarchique** avec une gestion décentralisée des données (chacun étant responsable des données de sa zone).

Le système de noms DNS se présente sous forme d'un arbre inversé avec

- pour sommet **la racine** représenté par un **point**;
- et un ensemble de nœuds représentant des domaines identifiés par un ou plusieurs éléments (fr, education.fr, org, com, etc.).

Les domaines de **premier niveau** comme fr, com sont appelé **Top Level Domain** (TLD).

Dans un domaine on peut créer :

- **un ou plusieurs sous-domaines**
- ainsi qu'une **délégation** pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur.

Un serveur de noms particulier s'occupe d'un **nœud** de l'arborescence ou d'un ensemble de nœuds sur lequel il aura **autorité** : on dit que le serveur gère une **zone d'autorité**.

Ce serveur de noms gére l'attribution des noms et résoudra les noms via une base de données (matérialisée le plus souvent par ce qu'on appelle un fichier de zone) distincte pour chaque nœud.

Chaque information élémentaire de la base de données DNS est un objet appelé **resource record** (RR). Un nœud peut contenir aussi bien des domaines que des noms de machines.

Les deux types de serveurs DNS

Il y a deux grands types de serveur DNS :

- Le **serveur DNS récursif** appelé aussi **résolveur** qui dispose uniquement d'un cache et de l'adresses des serveurs racines :
  - Il est **sollicité par des hôtes** afin de répondre à leurs requêtes.
  - Si la réponse n'est pas dans son cache, il sollicitera l'ensemble des serveurs faisant autorité concernés en partant d'un **serveur racine**,
  - le service utilisé avec l'OS Debian est le service **Unbound**.
- Le **serveur DNS faisant autorité** gère une ou plusieurs zones et les enregistrements associés. Les serveurs racines ou gérant les TLD sont des serveurs faisant autorité.
  - le service utilisé avec l'OS Debian est le service **bind9**

L'ordinateur client dispose dans sa configuration réseau **d'un ou plusieurs serveurs DNS récursifs** déclarés sous la forme d'adresses IP (dans **/etc/resolv.conf** sous Debian GNU/Linux). Lorsque ce dernier souhaitera résoudre un nom de domaine (pour se connecter à un site web par exemple), il contactera le **serveur DNS récursif** défini précédemment afin d'obtenir une réponse.

Fonctionnement global de la résolution DNS pour le contexte CUB

- Le client du LAN souhaite obtenir l'adresse IP correspondant au nom de domaine FQDN www.undomaine.fr (www.undomaine.fr. IN A?). Pour cela, il sollicite le serveur DNS récursif défini dans ses paramètres réseaux.
- Le serveur récursif vérifie s'il a déjà la réponse dans son cache, ce qui n'est pas le cas. Il décide donc de solliciter le serveur racine le plus proche. Le serveur racine lui indique qu'il ne dispose pas de l'information recherchée mais qu'il connaît les serveurs faisant autorité sur le TLD .fr.
- Le serveur récursif sollicite maintenant l'un des serveurs faisant autorité sur le TLD .fr. Ce dernier lui indique qu'il n'a pas l'information recherchée mais qu'il connaît le ou les serveurs faisant autorité sur le sous-domaine undomaine.fr.
- Le serveur récursif contacte ensuite le serveur faisant autorité sur le domaine undomaine.fr. Ce dernier dispose de l'information recherchée dans son fichier de zone sous la forme d'un enregistrement. Il l'a fourni au serveur récursif.
- Ce dernier stocke l'information dans son cache et la transmet enfin au client.

Fonctionnement de la résolution DNS pour le domaine cub.fr

1. Le client souhaite obtenir l'adresse IP correspondant au nom de domaine FQDN dc0.lan.galeway.cub.fr (dc0.lan.galeway.cub.fr. IN A?) auprès du serveur récursif défini dans ses paramètres réseaux.
2. Le serveur récursif vérifie s'il a déjà la réponse dans son cache, ce qui n'est pas le cas. Il décide donc de solliciter le serveur faisant autorité sur le domaine cub.fr. Attention ! Ce fonctionnement n'est pas le fonctionnement normal d'un serveur récursif qui commencera par contacter l'un des serveurs racines en premier lieu. Dans le cas présent, le domaine cub.fr étant un domaine fictif, nous avons paramétré le serveur récursif pour qu'il sollicite directement le serveur faisant autorité sur ce domaine via les directives « private-zone » et « stub-zone ».
3. Le serveur faisant autorité sur le domaine cub.fr répond au serveur récursif qu'il ne détient pas l'information souhaitée mais qu'il connaît (grâce à la délégation de zone) les serveurs faisant autorité sur galeway.cub.fr.
4. Le serveur récursif interroge donc l'un des serveurs faisant autorité sur galeway.cub.fr situé dans la DMZ de l'agence.
5. Le serveur faisant autorité sur galeway.cub.fr répond au serveur récursif qu'il ne détient pas l'information mais qu'il connaît le ou les serveurs faisant autorité sur le sous-domaine lan.galeway.cub.fr .
6. Le serveur récursif interroge ensuite le serveur DNS faisant autorité sur lan.galeway.cub.fr.
7. Ce dernier dispose de l'enregistrement (RR) recherché et fournit la réponse au serveur récursif.
8. Le serveur récursif stocke la réponse dans son cache et la transmet au client.

Topologie DNS d'une agence

Remarque : la configuration IP des serveurs de la DMZ fait référence à un serveur DNS externe récursif (9.9.9.9). En effet, les serveurs de la DMZ n'ont pas la légitimité à accéder à des serveurs internes.

Conseils

CONSEIL

Lorsque l'on met en place un service DNS faisant autorité sur une zone, s'assurer que la **récursivité soit bloquée**, que les **évènements soient journalisés**. Enfin garantir la continuité du service à l'aide d'au **minimum deux serveurs DNS** répartis dans des zones géographiques distinctes.

CONSEIL

Lorsque l'on met en place un **service DNS récursif**, s'assurer de la séparation des rôles. **Éviter** sauf cas particulier que le récursif soit ouvert, c'est à dire accessible par tout le monde, y compris sur Internet. En effet, les serveurs récursifs sont souvent sollicités par des personnes mal intentionnées afin de participer à des attaques DDoS par amplification. Penser également à assurer la continuité du service en disposant de plusieurs serveurs autonomes.

CONSEIL

Dès qu'un problème se pose spécifiquement au niveau du service DNS, il est important d'avoir les bons outils pour le résoudre :

- dig ou nslookup.

- named-checkconf.
- lecture des fichiers journaux.
- capture de trames à l'aide de Wireshark ou tcpdump.
- utilisation d'outils comme ZoneMaster dans le cas d'un nom de domaine exploité sur Internet.

CONSEIL

Dans le cas d'un nom de domaine exploité sur Internet, être extrêmement vigilant sur la sécurité d'accès au bureau d'enregistrement (couple login/mot de passe fort ou 2FA) car c'est par lui que s'opère la délégation. Certaines attaques DNS célèbres ont consisté simplement à pirater le compte d'accès au registar afin de rediriger l'ensemble des requêtes pour un domaine particulier vers des serveurs pirates.

Les tests et commandes

- obtenir l'adresse IP correspondant au nom de domaine FQDN www.debian.org auprès du serveur récursif défini dans mes paramètres réseaux.

```
$ dig A www.debian.org
```

- obtenir le nom de domaine correspondant à l'adresse IPv4 publique 78.243.223.34 (résolution inverse) <code shell> $ dig -x 78.243.223.34 </code>
- obtenir la liste des serveurs faisant autorité sur le domaine fdn.fr <code shell> $ dig NS fdn.fr </code>
- obtenir la liste des serveurs faisant autorité sur la racine du système DNS <code shell> $ dig NS . </code>
- obtenir l'adresse IPv6 globale correspondant au nom de domaine free.fr en sollicitant le serveur récursif de Google (8.8.8.8) et en obtenant le détail des échanges <code shell> $ dig +trace AAAA free.fr @8.8.8.8 </code>
- Gestion du service Bind 9 <code shell> $ sudo service bind9 stop $ sudo service bind9 start $ sudo service bind9 restart $ sudo service bind9 reload $ sudo service bind9 status </code>
    - Vérification de la syntaxe des fichiers de configuration et du fichier de zone <code shell> $ sudo named-checkconf -z </code> Consultation du fichier de log créé lors de l'activité afin de réaliser des diagnostics et garder une traçe <code shell> $ sudo cat /var/log/bind.log </code>

Glossaire

FQDN (Fully Qualified Domain Name, nom de domaine complet)

RFC 819 : ce terme désigne un nom de domaine où tous les composants sont cités. Par exemple, www.debian.org. est un FQDN alors que www tout court ne l'est pas. En toute rigueur, un FQDN devrait toujours s'écrire avec un point à la fin (pour représenter la racine) mais ce n'est pas toujours le cas.

Sous-domaine (subdomain)

Domaine situé sous un autre, dans l'arbre des noms de domaines. Sous forme texte, un domaine est sous-domaine d'un autre si cet autre est un suffixe. Ainsi debian.org est un sous-domaine de .org et ainsi de suite, jusqu'à la racine, le seul domaine à n'être sous-domaine de personne.

Serveur récursif (ou résolveur complet)

Un serveur récursif qui sait suivre les renvois et donc fournir un service de résolution complet. Des logiciels comme **Unbound** ou **PowerDNS Resolver** assurent cette fonction. Il est en général situé chez le **FAI** ou dans le réseau local de l'organisation où on travaille, mais il peut aussi être sur la machine locale.

Serveur faisant autorité (authoritative server)

Serveur DNS qui connait (**fait autorité**) les données de une ou plusieurs zones et peut donc y répondre (RFC 2182, section 2).

f.root-servers.net fait autorité pour la racine, **d.nic.fr** fait autorité pour **fr**, etc.

Des logiciels comme **NSD** ou **Knot** assurent cette fonction. Les serveurs faisant autorité sont gérés par divers acteurs, les registres, les hébergeurs DNS (qui sont souvent en même temps bureaux d'enregistrement).

La commande **dig NS $ZONE** donne la liste des serveurs faisant autorité pour la zone $ZONE.

Zone

Une zone est un groupe de **domaines contigus et gérés ensemble**, par le même ensemble de serveurs de noms. en Effet une zone ne se limite pas forcémentr à un seul domaine. Par exemple le domaine **gouv.fr** n'est pas une zone séparée. Il est dans la même zone que **fr**. **gouv.fr** n'a pas d'enregistrement NS ou de SOA.

Parent

Domaine situé au dessus du domaine en cours. Par exemple le parent de wikipedia.org est org.

Délégation (delegation)

Ce concept est central dans le système DNS, qui est un système décentralisé. En ajoutant un ensemble d'enregistrements NS pointant vers les serveurs de la zone enfant, une zone parent délègue une partie de l'arbre des noms de domaine à une autre entité. L'endroit où se fait la délégation est donc une coupure de zone.

Colle (glue records)

Lorsqu'une zone est déléguée à des serveurs dont le nom est dans la zone enfant, la résolution DNS se heurte à un problème d'œuf et de poule. Pour trouver l'adresse de ns1.mazone.example, le résolveur doit passer par les serveurs de mazone.example, qui est déléguée à ns1.mazone.example et ainsi de suite… On rompt ce cercle vicieux en ajoutant, dans la zone parent, des données qui ne font pas autorité sur les adresses de ces serveurs (RFC 1034, section 4.2.1). Il faut donc bien veiller à les garder synchrones avec la zone enfant. Source : RFC 7719 - DNS Terminology par Stéphane Bortzmeyer (https://www.bortzmeyer.org/7719.html)

Les principaux types d’enregistrements (RR)

SOA (Start of authority)

Enregistrement important qui contient les informations liées à la zone telles que le numéro de série, le serveur maitre, l’adresse mail du responsable de la zone.

NS

Permet de définir le ou les serveurs faisant autorité sur la zone.

A

Enregistrement le plus couramment rencontré. Il fait correspondre un nom de domaine à une adresse IPv4.

AAAA

Fait correspondre un nom de domaine à une adresse IPv6.

CNAME

Enregistrement permettant de définir qu’un nom de domaine soit un alias d’un autre.

MX

Définit le ou les noms du ou des serveurs de courriels du domaine.

PTR

Enregistrement inverse de A ou AAAA. Il fait correspondre une adresse IP à un nom de domaine.

TXT

Enregistrement qui définit une chaîne de caractères.

Schéma de résolution de nom par un hôte

- Article Wikipédia concernant DNS (https://fr.wikipedia.org/wiki/Domain_Name_System)

La résolution et le domaine inverse

Dans la plupart des recherches DNS (Domain Name System), les clients effectuent une recherche directe, à savoir une recherche basée sur le nom DNS d'un autre ordinateur stocké dans un enregistrement de ressource hôte (A). Ce type de requête attend une adresse IP comme données de ressource pour la réponse.DNS propose également un processus de recherche inversée, dans lequel les clients utilisent une adresse IP connue et recherchent un nom d'ordinateur sur la base de cette adresse.

Une recherche inversée assume la forme d'une question du type «Pouvez-vous me donner le nom DNS de l'ordinateur qui utilise l'adresse IP 192.168.1.20 ?». DNS n'a pas été conçu initialement pour prendre en charge ce type de requête. L'un des problèmes liés à la prise en charge du processus de requête inversée est la différence dans la façon dont l'espace de noms DNS organise et indexe les noms et la façon dont les adresses IP sont affectées. Si la seule méthode permettant de répondre à la question précédente consiste à rechercher dans tous les domaines de l'espace de noms DNS, une requête inversée prendrait trop longtemps et exigerait trop de traitement pour être réellement utile.

Pour résoudre ce problème, un domaine spécial, le domaine in-addr.arpa, a été défini dans les normes DNS et réservé dans l'espace de noms DNS Internet afin de fournir un moyen fiable et pratique d'effectuer des requêtes inversées. Pour créer l'espace de noms inversé, des sous-domaines dans le domaine in-addr.arpa sont formés, à l'aide du classement inversé des nombres dans la notation décimale séparée par des points des adresses IP.

La déclaration inverse est importante sur les adresses IP publiques Internet puisque l'absence d'une résolution inverse est considérée comme une erreur opérationnelle (RFC 1912) qui peut entraîner le refus d'accès à un service. Par exemple, un serveur de messagerie électronique se présentant en envoi avec une adresse IP n'ayant pas de résolution inverse (PTR) a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier (message de refus de type : IP lookup failed).

- Source : Cours de Marie-Pascale Delamare, professeure d'Informatique et Wikipédia : http://www.linux-france.org/prj/edu/archinet/systeme/ch30s03.html

Sûreté et sécurité du système DNS

La création de DNS date de 1983. C'est donc un protocole assez ancien. À l'époque la notion de sécurité n'était pas forcément primordiale et l'accent était mis davantage sur l'efficacité du protocole. Ainsi, il a été défini que le port d'écoute des serveurs DNS serait le port 53/UDP. Pour certaines tâches spécifiques, le port 53/TCP pourra être utilisé également.

L'émergence d'une vraie réflexion concernant la sécurité de ce protocole est apparue assez tardivement. Les attaques les plus communes concernant DNS sont les suivantes :

- Le **cybersquatting** est une attaque qui consiste à déposer un nom de domaine en portant volontairement atteinte aux droits d'un tiers pour lui nuire ou en retirer profit.
- Le **détournement d'un nom de domaine** consiste à pirater le compte lié à un domaine sur le site d'administration du bureau d'enregistrement afin de modifier les serveurs DNS faisant autorité sur cette zone. Ainsi toutes les requêtes concernant le domaine seront redirigées vers les serveurs des attaquants.
- **L'empoisonnement** vise à intoxiquer le résolveur pour qu'il considère que le serveur « pirate » est légitime, en lieu et place du serveur originel. Cette opération permet notamment de capter et de détourner les requêtes vers un autre site web sans que les utilisateurs puissent s'en rendre compte.
- **Le déni de service et le déni de service distribué** ont pour objectif de rendre l'accès à un service impossible ou très pénible. La différence entre les 2 attaques résident au niveau de l'attaquant. Un DoS implique une seule source quand le DDoS implique des sources multiples (des réseaux de machines zombies nommés BotNet).
- **Attaque par réflexion** des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées.

Bonnes pratiques

Voici les bonnes pratiques et les mécanismes de sécurité qui permettent d'avoir une ligne directrice afin de garantir un niveau de sécurité correcte de ce service qui s'avère souvent critique.

- Assurer la meilleure redondance possible, de manière à ce qu'un serveur affecté par une attaque puisse être remplacé en toute transparence par d'autres serveurs disposant des mêmes informations mais situés sur d'autres réseaux. Il est donc recommandé d'avoir au minimum deux serveurs DNS répartis dans des zones géographiques distinctes. La capacité du service DNS à résister à

une panne puis à revenir à son état nominal se nomme la résilience.

- Veiller à utiliser des versions à jour des logiciels DNS, notamment de BIND, corrigées par les « patchs » appropriés, afin de ne pas être vulnérable à des attaques portant sur des failles de sécurité déjà bien identifiées.
- Assurer une surveillance régulière de ces serveurs à l'aide d'un outil de supervision et de leur configuration avec des programmes comme zonemaster (https://www.zonemaster.fr/domain_check).
- Envisager un plan de continuité d'activité, permettant à la victime d'une attaque de poursuivre, ou de reprendre en cas d'incident grave, ses activités avec un minimum d'indisponibilité de ses services.
- Déployer DNSSec, protocole de sécurisation du DNS par l'authentification des serveurs et la signature cryptographique des enregistrements, ce système limitant notamment les attaques par empoisonnement.
- Déployer DoT, protocole qui permet de chiffrer les échanges à l'aide du protocole TLS entre un client et un serveur DNS récursif.
- Déployer le mécanisme d'authentification TSIG entre les serveurs maîtres et esclaves, mécanisme permettant d'éviter qu'une machine illégitime puisse récupérer des informations sensibles depuis le serveur maître.
- source : DNS : types d'attaque et techniques de sécurisation publié par l'AFNIC (https://www.afnic.fr/wp-media/uploads/2021/01/DNS-types-dattaques-et-techniques-de-se%CC%81curisation.pdf).