DNS : Domain Name Server

Présentation

Le service DNS, responsable de l'association entre les noms lisibles (FQDN – Fully Qualified Domain Name) et l'adresse IP de la machine hébergeant effectivement le service, est devenu l'ossature de l'accès au Web et autres Intranet, au même niveau de criticité que le câblage : la mise en panne de ce service pourrait rendre impossible tout accès aux ressources de la toile, aussi bien aux sites qu'à la messagerie.

Ce protocole doit être vu à deux niveaux :

- la définition des associations entre FQDN et IP qui est du ressort de l'administrateur du Domaine DNS et nécessite une organisation des serveurs autour de rôles précis,
- la consultation de ces associations par les postes utilisateurs et entre les serveurs, qui relève des interrogations.

Préalablement à l'étude de ces deux points de vue, nous présenterons ci-dessous quelques principes et définitions.

Le système DNS pose des problèmes de sécurité qui peuvent engendrer des dysfonctionnements graves : détournement de communication, identification des adresses de serveurs, etc. C'est pourquoi le protocole DNSSEC est venu compléter l'offre. Un bref aperçu sera donné en fin de document.

I Principe et définitions

DNS (Domain Name Server ou Domain Naming Service) fonctionne :

- à partir de domaines de référence (domaines racines de type .fr, .com, .org, .net etc) rattachés à une racine universelle (ROOT),
- de sous-domaines gérés par les entreprises ou propriétaires d'un nom de domaine (yahoo, google, gouvernement des états, académies, etc).

Les informations d'un domaine sont enregistrées dans un fichier de zone qui contient les associations entre noms lisibles et adresses IP. Le fichier de déclaration devient une autorité de nommage.

DNS est donc une organisation hiérarchique de domaines, gérée par des serveurs faisant autorité sur ces différents domaines (ils sont détenteurs des associations et seuls autorisés à modifier ces associations).

Le client DNS est une machine susceptible d'interroger le ou les serveurs DNS paramétrés dans son environnement IP grâce à un logiciel client DNS (généralement son OS).

1.1 La norme

Pour pouvoir s’y retrouver entre toutes les machines disponibles sur l’internet ou dans un réseau

local, le protocole applicatif DNS (Domain Name System) a été promu RFC en 1984 [RFC 897, mises à jour par RFC 881; puis RFC 921]. Voir la liste des RFC faisant référence à DNS à l'adresse http://www.dns.net/dnsrd/rfc/.

Les équivalences IP/Nom Symbolique existaient auparavant dans les fichiers hosts (pour IP/FQDN) ou lmhosts (pour IP/Nom Netbios, remplacé par WINS), mais devaient être enregistrées manuellement sur chaque machine. DNS réalise donc la centralisation des associations IP/FQDN.

1.2 L'organisation : Domaines et Zones

Remarque : il ne faut pas confondre URL (Universal Resource Locator) et FQDN. Une URL est l'adresse FQDN de la machine (www.jrostand.fr) complétée par le protocole à utiliser (http://...).

Arborescence, racine et Top Level Domain

L'organisation du système DNS repose sur une arborescence commençant par une racine (ROOT) gérée par l'ICANN (Internet Corporation for Assigned Names and Numbers). En France, c'est l'INRIA qui héberge les serveurs racines.

Sous cette racine, différents domaines officiels ou de premier niveau (Top Level Domain - c'est à dire correspondant au système américain), ainsi que des domaines nationaux ont été créés pour permettre une certaine cohérence.

Pour chacun de ces domaines de référence, des serveurs de noms dédiés gérés par des organismes officiels (AFNIC en France, dont est extrait le schéma suivant) permettent l'inscription des noms choisis par les entreprises, associations, organismes, individus, etc.

Domaine, zone, fichiers et associations

L'organisation de DNS repose sur les domaines et les associations. Les éléments de vocabulaire suivants permettent de s'y retrouver.

- Un domaine est une arborescence et/ou sous-arborescence. Un domaine peut donc posséder des sous-domaines.
- Chaque nœud de l'arborescence correspond à une zone, dont le nom complet (FQDN) remonte jusqu'à la racine de l'arbre. Chaque zone est enregistrée dans un fichier de zone. Un domaine et ses sous-domaines donnent lieu à autant de fichiers de zone.
- Les feuilles correspondent à des machines et feront l'objet d'associations avec leurs adresses IP dans un fichier de zone.

On voit par exemple, sur le schéma ci-dessous la machine culture.gouv.fr. dans la zone gouv.fr. du

domaine gouv.fr.

Associations

À l'intérieur d'un fichier de zone, on créera des associations (on parle aussi d'enregistrement de ressource – ***Resource Record [RR]***) entre les noms symboliques des machines rendant des services pour la zone (le service Web généralement associé au nom www, la messagerie sous le nom smtp, etc) et leur adresse IP. Par exemple, dans le domaine yahoo.com, on pourrait trouver les associations suivantes (valeurs fictives):

```
fr    A  217.12.3.11  # association classique d'un FQDN (fr.yahoo.com) à son adresse IP
uk    A  217.12.3.45
   MX    mail #enregistrement d'un serveur de messagerie dans le domaine par son FQDN (mail.yahoo.com)
mail  A     217.12.3.119
```

Une liste plus complète des type d'associations est présentée en annexe.

Hiérarchie

Les serveurs DNS ont des rôles différents selon qu'ils sont :

- le point de départ d'une zone (principal ou maître),
- une recopie (secondaire ou esclave)
- un sous-domaine (délégué).

II Mise en œuvre côté serveur

2.1 Rôle des serveurs

Pour assurer le service permettant de répondre à une demande d'équivalence FQDN / IP, un applicatif réseau sera hébergé sur un ou plusieurs serveurs DNS. Tout serveur DNS, quel que soit son rôle, sera enregistré dans une association NS du fichier de zone.

SOA

Pour une zone donnée, un seul serveur contiendra l'enregistrement initial de toutes les associations de nom de son domaine. Ce serveur maître est dit SOA [Start Of Authority]. Il est le seul habilité à effectuer des modifications dans le fichier de zone.

Une même machine peut être SOA pour plusieurs zones et jouer d'autres rôles DNS (cache, secondaire, etc).

Secondaires

Pour assurer une certaine tolérance aux pannes, le serveur SOA pourra être complété par un ou plusieurs serveurs secondaires qui recevront à intervalle défini une copie en lecture seule du fichier de zone.

Ces secondaires assureront un fonctionnement continu en cas de panne du serveur maître et rapprocheront le service DNS du lieu de son utilisation, évitant les échanges réseaux coûteux et inutiles (répartition de charge).

Une machine serveur secondaire pour une zone peut aussi être maître d'une autre zone (par exemple d'une sous-zone de niveau inférieur : par exemple DNS secondaire de la zone jrostand.fr et DNS primaire de la zone btsinfo.jrostand.fr). Voir les délégations présentées ci-dessous.

La norme préconise, pour une zone, de toujours disposer d'un maître et d'un secondaire.

Délégation

Pour ne pas saturer un serveur maître dans la gestion de l'ensemble des sous-domaines (imaginez le travail que devrait fournir le DNS gérant le domaine .com s'il avait en charge la gestion de tous les noms de domaine et de sous-domaines finissant par .com), le maître peut déléguer la gestion de sous-zones à d'autres machines. Ainsi, dans le domaine .gouv.fr., une délégation sera faite pour le sous-domaine education, qui sera géré par le SOA de la zone education.gouv.fr.

Ainsi encore, un SOA se contente de connaître les sous-domaines immédiatement inférieurs et renvoie vers ces sous-domaines pour la suite de l'arborescence.

Le SOA de .com connaît la machine SOA de yahoo.com, de microsoft.com, de google.com, mais ne gère pas les noms de machines ou les sous-domaines de ces zones.

Cache

Tout serveur DNS enregistre dans une zone de cache les associations qu'il a déjà pu résoudre. L'information est conservée pendant sa durée de vie (définie dans les paramètres du SOA).

Un serveur peut ne servir que de cache, de manière à soulager le réseau sans avoir à gérer de zone particulière. Notamment, les serveurs DNS indiqués par les fournisseurs d'accès ne sont pas gestionnaires de zone mais simplement serveurs cache.

Ces serveurs de cache ne font pas autorité sur les indications qu'ils fournissent, puisqu'ils ne sont pas détenteurs des fichiers de zone.

Zone inversée

Pour faciliter certaines tâches, notamment l'exploration réseau (détection de pannes, cartographie),

les manipulations d'administration distante, etc, il est possible de créer une zone inversée associant à une adresse IP (écrite à l'envers) un nom FQDN.

Un fichier de zone inverse ou indirecte (rattachée au domaine inaddr-arpa pour IPv4 ou ip6-arpa pour IPv6) doit absolument être associé à un fichier de zone standard et à un serveur DNS pour cette zone.

L'enregistrement correspondant est de la forme :

```
<IP_A_L_Envers>  PTR nom_FQDN.
```

2.2 Synchronisation Maître / Secondaire

Les serveurs DNS secondaires (ou esclaves) ne disposent que d'une copie en lecture du fichier de zone. Aussi, lorsque des modifications ont lieu dans ce fichier de zone (sur le maître), il est nécessaire de répercuter les informations sur le secondaire.

Possédant une copie conforme du fichier original, les serveurs secondaires font autorité sur les informations qu'ils diffusent. Ils ne sont cependant pas SOA et ne possèdent donc pas le droit de modifier le fichier.

C'est ce secondaire qui est à l'origine de la demande d'actualisation, conformément au délai de renouvellement inscrit dans l'enregistrement SOA. À intervalle défini, il va donc lancer une demande de renouvellement du fichier en envoyant le numéro de série de la copie dont il dispose actuellement (soit Nser ce numéro).

Le SOA peut toutefois être à l'initiative d'une alerte pour dire aux secondaires que des mises à jours majeures ont eu lieu (modification des NS par exemple).

Le serveur SOA conserve plusieurs versions du fichier de zone. Pour répondre à la demande d'un secondaire, il aura le choix de renvoyer une copie complète du fichier (ce qui peut être lourd lorsque les délais sont courts et /ou les secondaires nombreux) ou simplement les modifications apparues depuis la version du secondaire.

- Si le numéro de série du secondaire est trop ancien, le maître ne disposant pas des étapes intermédiaires renvoie l'intégralité du fichier. On parle de AXFR. C'est le mode d'échange des versions DNS de Windows NT et de BIND (Linux) jusqu'à la version 7.
- Si le maître dispose des fichiers intermédiaires entre le numéro de série Nser du secondaire et la dernière mise à jour, il pourra transmettre les seules modifications qui ont eu lieu (on parle de mise à jour incrémentielle ou IXFR, depuis BIND 8 et Windows 2000) ou, si ces modifications sont plus lourdes que le fichier lui-même, d'envoyer une copie complète du fichier dans sa dernière version.

III Recherche DNS : relation client/serveur

3.1 Fonctionnement classique

La fonction ***resolver*** d'un service DNS est le système permettant à un client ou à un serveur d'effectuer une demande de la forme :

```
 Query 'nomrecherché' ?RR ; quel est l'enregistrement de ressource
correspondant à 'nomrecherché' ?
```

Le resolver effectuera une demande selon l'un des deux modes suivants :

- L'approche itérative : le client demande une réponse ou l'adresse d'un autre serveur. Le service sollicité répondra 'voici l'adresse correspondante' en cas de succès de la requête, ou 'je n'ai pas la réponse, demande à tel serveur'. C'est en général le mode de fonctionnement utilisé dans le dialogue entre serveurs DNS.
- L'approche récursive : elle consiste à demander une réponse obligatoire du type 'voici l'adresse demandée' ou 'l'adresse n'existe pas'. Pour parvenir à un tel résultat, le serveur sollicité ira demander une réponse plus haut. Les postes utilisateur fonctionnent selon ce mode (ils n'interrogent qu'un serveur qui doit leur trouver une réponse si elle existe).

Pour répondre à une requête DNS, un serveur va avant tout étudier les fichiers de zone dont il dispose. Si le FQDN recherché ne relève pas des zones dont il gère le suivi, il va vérifier qu'il ne contient pas une équivalence dans les données de cache.

Pour fournir l'adresse d'un autre serveur à interroger ou pour trouver une réponse, le serveur sollicité pourra s'adresser :

- soit vers les serveurs RACINE, (A.ROOT-SERVER jusqu'à M.ROOT-SERVER) qui sont renseignés à l'installation du service ou mis à jour auprès des services de gestion des noms comme l'AFNIC,
- soit vers des serveurs spécifiés par l'administrateur (on parle de forwarders ou redirecteurs) dans le fichier de zone.

3.2 Fonctionnement non hiérarchique

Un problème avec DNS est que l'ensemble de l'architecture repose sur les serveurs et que cela génère des besoins en performance importants à mesure que les noms de domaines se multiplient.

Au sein d'un réseau, la mise en place d'un serveur seul autorisé à interroger l'extérieur ne fait que reporter sur ce serveur interne le problème de disponibilité et de saturation.

Des techniques visant à mieux répartir le travail entre les serveurs et les postes ont été développées et sont en cours de standardisation et/ou de déploiement : le serveur est le seul interrogé en mode récursif (il va chercher au-dessus de lui) quand aucun poste du réseau local ne sait répondre à une demande en mode itératif. (il ne répond que s'il a l'information en cache).

- Multicast DNS : les équipements d'un réseau s'informent les uns les autres en partageant leur cache, les messages étant adressées sur une adresse multicast (224.0.0.251). mDNS défini par Apple est en passe de devenir le standard (au détriment du protocole LLMNR Link-Local Multicast Name Resolution de Microsoft).
- Anycast DNS : l'échange vers un serveur est remplacé par une trame de diffusion (en UDP).

Ces techniques rentrent dans un cadre plus large de fonctionnement d'un réseau local sans configuration (ZeroConf - Zero Configuration Networking et UPnP – Universal Plug And Play) qui concernent également le remplacement du serveur DHCP par un adressage d'auto-configuration (link-

local [169.254.0.0/16 ou FE80:: en IPv6]).

IV La sécurité : DNSSEC

Comme tout outil informatique, et plus particulièrement parce qu'ils sont au cœur du fonctionnement d'internet ou des accès aux machines de l'entreprise, les serveurs DNS sont vulnérables à de nombreuses attaques.

Au delà des pannes matérielles dont on doit naturellement se prémunir (grâce aux onduleurs, à la sauvegarde et aux outils de tolérance disque ou processeur), la perte, la falsification ou la détérioration des fichiers de zone et de cache, l'empêchement du fonctionnement du service ou la modification ou destruction des réponses sont autant de fragilité du système.

Pour assurer la sécurité du service DNS, on pourra, par exemple, crypter les fichiers de zone (des outils existent sous Linux/Unix) ou sécuriser les échanges maître/secondaire par des techniques de cryptage ou des liaisons sécurisées.

La multiplication des secondaires sera un facteur de disponibilité mais malheureusement de ralentissement.

DNSSEC

Pour aller encore plus loin, le protocole complémentaire DNSSEC permet de signer chaque enregistrement de la zone et de garantir des échanges sûrs :

- entre le serveur et une machine utilisateur : les enregistrements demandés sont accompagnés d'une signature électronique qui en garantit la validité
- entre primaire et secondaire : les mises à jour sont chiffrées et signées, empêchant une lecture intermédiaire ou une modification par un tiers
- entre supérieur et délégué : les mises à jour du délégué sont garanties par une signature électronique vers le supérieur

V Les enregistrements DNS (extraits) avec l'aide de Microsoft

Enregistrement	Explication
A [adresse]	correspond à un nom d'hôte (ordinateur ou autre périphérique réseau) avec une adresse IP dans une zone DNS. Un FQDN peut être associé à plusieurs adresses grâce à un enregistrement A.
AAAA [adresse]	Équivalent de A pour une adresse IPv6 (quatre fois plus volumineuse qu'IPv4)

Enregistrement	Explication
CN [Canonical Name]	Utilisé pour masquer les détails de l'organisation du réseau aux clients qui s'y connectent ou faire des renvois vers des adresses plus complexes (par exemple pour les noms de domaines déposés par des particulier). Par exemple, rostand.ac-caen.fr serait un alias (CN) du nom réel de l'ordinateur : www.rostand.etab.ac-caen.fr. Permet le déplacement de machines dans des domaines sans changer le nom FQDN. Si un nom est associé à un enregistrement CN, il ne peut être associé à un enregistrement A
MX [Mail eXchange]	spécifie un serveur de messagerie pour un nom de domaine DNS. On décrit d'abord l'enregistrement de messagerie en donnant le nom FQDN de la machine (IN MX nomFDQN), puis l'on enregistrera l'association nom FQDN et adresse IP (nomFQDN. A @IP)
NS [Name Server]	repère toutes les machines assurant le service DNS (on peut en avoir plusieurs avec duplication pour des raisons d'efficacité ou de sécurité). Doit être présent dans les fichiers de zone et de zone inverse. Fonctionne comme MX en deux temps.
RT [Routing]	
PTR [Pointer]	Réciproque de A, utilisé pour mapper une adresse IP avec un nom d'hôte (ordinateur ou autre périphérique réseau) dans une zone indirecte DNS (celles du domaine DNS In-addr.arpa).
SOA [Start Of Authority]	Enregistrement de déclaration de zone, indiquant le nom de la zone, le nom de l'administrateur responsable et fournissant en paramètre le délai de rafraîchissement, de reprise, de mise en échec des secondaires ainsi que la durée de vie des données en cache
TXT	associe des informations textuelles générales avec un élément de la base de données DNS. Il est généralement utilisé pour identifier l'emplacement d'un hôte (ordinateur ou autre périphérique réseau), par exemple, Emplacement: bâtiment 26S, salle 2499. La chaîne de texte doit contenir moins de 256 caractères, mais plusieurs enregistrements de ressources TXT sont autorisés.