Service DNS : concepts

Soumis par VieuxProf
01-01-1999
Dernière mise à jour : 03-02-2008

- Le protocole DNS (Domain Name Server) est un protocole applicatif de niveau 7 utilisant UDP (port 53) pour échanger des informations entre clients et serveurs. Il permet la transformation de noms symboliques en adresses IP sur un réseau.

- Pour l'internet, il s'appuie sur une base de données distribuée sur une hiérarchie de serveurs dont les informations sont actualisées par le mécanisme de propagation des caches.

- Un domaine, caractérisé par un nom unique, est un espace de responsabilité pour les sous-domaines et les machines qui le composent. Il est géré par un serveur DNS qui exerce une autorité déléguée par les serveurs de niveau supérieur. Chacun des hôtes du domaine est identifié par son FQDN (Fully Qualified Domain Name) qui est de la forme : 'mamachine.monsousdomaine.mondomaine.TLD'.

- Les serveurs à la racine de l'arbre (root-servers) délèguent aux serveurs de 1er niveau (root-level noté par ".") la responsabilité des domaines "top-level" (TLD) qui gèrent les 7 extensions .com, .edu, .gov, .mil, .net, .org, .int aux Etats Unis et les extensions associées aux codes ISO des pays hors USA (.ca, .es, .fr, etc.).

- A réception d'une requête de résolution de nom, un serveur DNS peut :

- renvoyer directement la réponse si la machine recherchée appartient au domaine dont il est responsable ou s'il possède l'information requise dans son cache

- contacter un autre serveur (serveur faisant autorité pour le domaine recherché) afin d'obtenir la réponse, la mémoriser dans son cache et l'envoyer au client

- renvoyer l'adresse d'un serveur à partir duquel le client doit pouvoir résoudre le nom

- Chaque domaine doit posséder, si possible sur des réseaux différents, un serveur DNS primaire où se trouve la base des noms et des adresses du domaine considéré, et un ou plusieurs DNS secondaires possédant une copie de la base transférée depuis le serveur primaire.

{mospagebreak title=Requêtes itératives}

Exemple de requête DNS itérative :

La machine 'monclient' souhaite résoudre l'adresse IP de la machine 'machinecible.sousdomaine.domaine.fr'. Les serveurs faisant autorité sur '.fr', 'domaine.fr' et 'sousdomaine.domaine.fr' sont respectivement 'ns.inria.fr', 'ns.domaine.fr' et 'ns.sousdomaine.domaine.fr'.

- La machine 'monclient' interroge le serveur DNS interne 'serveurlocal'. (1)

- Si 'serveurlocal' possède l'information recherchée dans son cache ou si la résolution demandée concerne un domaine sous son autorité, il renvoie directement la réponse et la recherche est terminée. (2)

- Si 'serveurlocal' connaît 'ns.sousdomaine.domaine.fr' ou 'ns.domaine.fr', il interroge le serveur de plus bas niveau et obtient l'adresse IP de 'machinecible'. Il mémorise l'information dans son cache, renvoie la réponse à 'monclient' et la recherche est terminée. (6+2 ou 5+6+2)

- Si 'serveurlocal' connaît 'ns.inria.fr' (TLD) mais ne connaît pas 'ns.sousdomaine.domaine.fr' ni 'ns.domaine.fr', il interroge 'ns.inria.fr' qui lui renvoie l'adresse de 'ns.domaine.fr'. Il interroge alors 'ns.domaine.fr' qui lui renvoie l'adresse de 'ns.sousdomaine.domaine.fr'. Il interroge ensuite 'ns.sousdomaine.domaine.fr' qui lui renvoie l'adresse de 'machinecible'. Il mémorise à chaque étape l'information dans son cache puis renvoie la réponse à 'monclient'. (4+5+6+2)

- Si 'serveurlocal' ne connaît pas 'ns.inria.fr', il interroge un root-server qui lui renvoie cette adresse puis redescend itérativement la hiérarchie comme précédemment. Il mémorise à chaque étape l'information dans son cache puis renvoie la réponse à 'monclient'. (3+4+5+6+2)